UNIVERSIDAD DE SEVILLA

Departamento de Matemática Aplicada I

DESARROLLO COCÍCLICO DE DISEÑOS Y APLICACIONES

Memoria presentada por
María Dolores Frau García
para optar al grado de
Doctor en Matemáticas
por la Universidad de Sevilla

Vº Bº
de los Directores,

Fdo.: Víctor Álvarez Solano
Pedro Real Jurado

Sevilla, Mayo de 2003

Desarrollo Cocíclico de Diseños y Aplicaciones

María Dolores Frau García

Mayo de 2003

UNIVERSIDAD de SEVILLA

RECTORADO

UNIVERSIDAD DE SEVILLA
REGISTRO GENERAL
TERCER CICLO
SALIDA
74102 Nº. 200302000006415
19-09-2003 10:24:40

Sevilla, 19 de septiembre 2003
Ref: Negociado de Tesis EL/CH
Asunto: Enviando Tesis Doctorales Leídas

ILMO.SR. DIRECTOR DE LA
BIBLIOTECA DE LA E.T.S.
INGENIERIA INFORMÁTICA
UNIVERSIDAD DE SEVILLA

Adjunto le remito ejemplares de Tesis Doctorales leídas en Departamentos vinculados a esa Facultad a fin de que pasen a formar parte de fondos bibliográficos de consulta de ese Centro.

AUTORES DE LAS TESÍS LEIDAS

1. CARRILLO MONTERO, VICENTE
2. CASCADO CABALLERO, DANIEL
3. FRAU GARCÍA, MARÍA DOLORES

LA JEFA DE SECCIÓN DE DOCTORADO

Fdo.: Yolanda Díaz Rolando

UNIVERSIDAD DE SEVILLA
SECRETARIA

Que la presente Tesis Doctoral
al folio 055 número 195 del libro
correspondiente
Sevilla, 28 de Mayo de 2003
El Jefe del Negociado de Tesis

A mis padres

UNIVERSIDAD DE SEVILLA

El Tribunal que suscribe, reunido los abajo firmantes,
en el acto de juzgar la Tesis Doctoral de

D. MARIA DOLORES FRAU GRACIA

titulada DESARROLLO COCICLICO DE DISEÑOS Y APLICACIONES

acordó otorgarle la calificación de SOBRESALIENTE CUM LAUDE

POR UNANIMIDAD

Sevilla, 11 de JULIO 2003

El Vocal, El Vocal, El Vocal,

El Presidente El Secretario, El Doctorado,

Agradecimientos

Quisiera dedicar, aunque sólo sean unas pequeñas letras a todos aquellos que han estado junto a mí en el sentido más entrañable de la palabra, durante todo este tiempo. Gracias a todos los que de algún modo me habéis apoyado, habéis confiado en mí (en muchas ocasiones más que yo misma) y habéis hecho que los momentos difíciles fuesen más llevaderos.

Quisiera hacer mención especial en estos agradecimientos a mis directores de tesis, Pedro y Víctor, que no sólo han mostrado tener una paciencia infinita, sino que me han ayudado en todo lo que ha estado en su mano: dándome sus más sabios consejos, compartiendo conmigo sus conocimientos, aportando siempre brillantes ideas... Sin ellos, desde luego, no habría sido posible esta memoria, por eso les doy las gracias.

También quisiera dar las gracias a mis compañeros y, sobre todo, amigos *Mateuitos*; siempre dispuestos a ayudar y siempre ahí, al lado, mostrando su apoyo, en los buenos momentos (que han sido muchos) y en los no tan buenos. Quisiera destacar la inestimable ayuda prestada por Natalia, con la que he compartido, no sólo despacho, sino también momentos de nerviosismo, desahogo, alegrías... Ha sido maravilloso poder trabajar junto a todos ellos, en un ambiente tan cordial. Gracias por haberme acogido como a uno más de la familia.

Tampoco puedo olvidar al resto de compañeros del departamento de Matemática Aplicada I, en especial gracias a los miembros del grupo C.H.A.T.A., que me han ayudado continuamente, sobre todo en los inicios de mi bagaje investigador. En particular agradezco su ayuda a Andrés, que ha estado dispuesto en todo momento a sentarse junto a mí, lápiz en mano, a explicarme cualquier cosa y del que he podido aprender mucho.

Sin duda, y aunque los haya dejado para el final, las personas a las que más agradezco su apoyo, su ayuda, su paciencia y cariño son mi familia, que han conseguido que esta tesis haya salido adelante. En especial, gracias a Víctor que, si en el terreno profesional ha sido excelente trabajar con él, en el personal ha sido muchísimo mejor. No tengo palabras para agradecer tanta comprensión, tantísima paciencia, tanto amor... Gracias por soportar heroicamente mis cambios de humor, por ser siempre tan animoso y contagiarme de tu alegría en todo instante, por hacer lo imposible para que los momentos más duros se tornasen incluso agradables, por compartir mis ilusiones, mis deseos, mis alegrías y también mis bajones de ánimo y, ante todo, gracias por ser como eres. Y también, gracias al pequeñín que llevo dentro y que con sus diminutas pataditas me ha trasmitido la fuerza necesaria para dar el último empujón a esta memoria, que en ocasiones parecía no tener fin y, que gracias a Pablo, se ha podido terminar. Gracias Papá, Mamá, Juan, Espe, Mari Carmen, Eduardo, Francis, Salu, Paqui y Migue por haberme animado continuamente, por comprenderme, por compartir conmigo el deseo de ver finalizado este trabajo y por quererme tanto.

Gracias a todos.

Resumen

Al amparo de la Teoría de Perturbación Homológica [111, 14, 51, 47, 68, 48, 106, 98], establecemos una nueva aproximación de la Teoría de desarrollo cocíclico de diseños [23, 24], a la hora de caracterizar matrices cocíclicas de Hadamard; que damos en llamar *método de la reducción homológica.*

Esta técnica aporta dos innovaciones con respecto a los métodos ya conocidos de Horadam, de Launey y Flannery [26, 40, 41]: por una parte, reduce la complejidad del proceso de obtención de una base de 2-cociclos para grupos con modelos homológicos conocidos; por otra, el trabajar directamente con una base de 2-cobordes permite aplicar el test de Hadamard cocíclico, así como establecer cotas superiores e inferiores para el número de generadores a utilizar con vistas a formar matrices cocíclicas de Hadamard.

Para ilustrar el funcionamiento del método, aplicamos la técnica a ciertas familias de productos iterados de extensiones centrales y productos semidirectos de grupos abelianos finitos, para los cuales previamente habremos establecido unos modelos (co)homológicos, progresando sobre los que se determinaran en [99, 100, 4, 1].

Introducción

En uno de sus múltiples libros de divulgación científica [116], Ian Stewart escribe que *"... una característica de la Ciencia de finales del siglo XX es que se están desvaneciendo las fronteras tradicionales de las materias. Esto también es aplicable a las Matemáticas. Ya no es lógico dividirlas en Álgebra, Cálculo, Geometría, etc. Cada una de estas áreas se introduce en cada una de las restantes. Muchas áreas de la investigación matemática se ven ahora enriquecidas por el contacto activo y directo con las ciencias aplicadas. A menudo sucede que las áreas más interesantes no son aquellas en las que se han utilizado tradicionalmente las Matemáticas, y las aplicaciones más interesantes utilizan elementos de las Matemáticas que normalmente no se había considerado útiles..."*

Más adelante prosigue *"... Las Matemáticas de hoy han logrado resolver problemas que tenían desconcertados a los grandes cerebros de los siglos anteriores. Sus más abstractas teorías están siendo aplicadas para dar respuesta a cuestiones fundamentales de la Física, la Química, la Biología, la Informática y la Ingeniería..."*

No hay descripción más acertada del contexto en el que se desenvuelve esta memoria: partiendo de un campo tan abstracto y teórico como es el del Álgebra Homológica, vamos a desarrollar una maquinaria para diseñar códigos correctores de errores óptimos (en un sentido a precisar después), que se sustenta en la obtención de *matrices cocíclicas de Hadamard* en dimensiones apropiadas; mecanismo que, de paso, podría servir para cercar la centenaria conjetura sobre la existencia de matrices de Hadamard en cualquier orden múltiplo de 4.

Quizás no seamos conscientes de ello, pero nuestra vida cotidiana está salpicada constantemente por una lluvia incesante de transmisión de información: instrumentos como la televisión, radio, aparatos de audio, lectores compactos, teléfonos móviles, ordenadores... se han vuelto indispensables para la mayor parte de la población.

Esto hace de la *teoría de códigos* [110] una herramienta fundamental hoy día, puesto que la información que se pretende transferir en cualquier situación suele estar expuesta a multitud de interferencias que pueden provocar distorsiones en el mensaje. De manera que es esencial poder detectar si se ha producido algún error y, en su caso,

reconstruir la información enviada originalmente a partir de los datos recibidos; bajo ciertas condiciones determinadas por *códigos detectores* y/o *correctores de errores.*

El objeto de la teoría de códigos es, precisamente, el diseño de códigos con una tasa de transferencia de información razonable, un bajo coste de codificación y decodificación y ciertas capacidades de detección y corrección de errores que eviten la necesidad de retransmisión.

El resultado crucial en teoría de códigos, que enunciara Shannon en 1948 [110], relaciona la capacidad de un canal con la existencia de "buenos códigos", de modo que siempre que la tasa de transmisión de información permanezca por debajo de la capacidad del canal, se puede encontrar códigos de fiabilidad arbitraria, tan buena como uno desee.

Un buen código corrector de errores ha de satisfacer tres condiciones: que tenga una elevada *distancia mínima* (para que pueda detectar y corregir un mayor número de errores), un cuantioso número de palabras (para no restringir la potencial cantidad de información a ser transmitida), y que no por ello el problema de reconstruir mensajes se traduzca en un problema de alto coste computacional.

Las dos primeras condiciones parecen difíciles de sostener de manera simultánea, dado que mientras más palabras constituyan el código, la distancia entre ellas será menor, luego, parece natural que la distancia mínima del código también disminuya. En realidad, este problema de la determinación del código de tamaño máximo de distancia mínima dada ha derivado en la caracterización de ciertos tipos específicos de códigos, y el establecimiento de condiciones bajo las cuales estos códigos se vuelven *óptimos*, en el sentido anterior.

En particular, Plotkin demostró en [93] que si C es un código binario formado por palabras de longitud v y distancia mínima dada d; entonces, el número b de palabras que componen el código verifica las cotas:

1. Si d es par y $v < 2d$, es $b \leq 2\left[\frac{d}{2d-v}\right]$.
2. Si d es par y $v = 2d$, es $b = 2d$.
3. Si d es impar y $v < 2d+1$, es $b \leq 2\left[\frac{d+1}{2d+1-v}\right]$.
4. Si d es impar y $v = 2d+1$, es $b \leq 2v+2$.

MacWilliams y Sloane probaron en [89] que la existencia de códigos óptimos para 1. y 2. implicaba la existencia de códigos óptimos para 3. y 4.

Levenshtein probó en [85] que estas acotaciones eran las más finas posibles, dado que existían códigos óptimos alcanzando dichas cotas, en función de la existencia de *matrices de Hadamard* de determinadas dimensiones.

Una matriz H cuadrada de orden n con todas sus entradas en $\mathbb{F}_2 = \{1, -1\}$ se dice *matriz de Hadamard de orden n* cuando verifica que $H \cdot H^t = n \cdot I$, i.e., si sus filas (respectivamente, columnas) son ortogonales dos a dos.

Este tipo de matrices da lugar a la denominada *conjetura de Hadamard* (también conocida como conjetura de Paley) que versa sobre la existencia de matrices de Hadamard de dimensión cualquier múltiplo de 4.

Históricamente, este tipo de matrices fueron ya consideradas por Sylvester [120] en 1867, en relación con un problema sobre teselaciones.

Sin embargo, las matrices de Hadamard no cobraron entidad propia hasta que el mismo Hadamard encontró la relación entre estas matrices y el problema de hallar la matriz A cuadrada de orden n de entradas reales $|a_{ij}| \leq k$, para un cierto $k > 0$, de determinante máximo [52]. Hadamard demostró que el determinante de una matriz A como la anteriormente descrita viene acotado en valor absoluto por el número $k^n n^{\frac{1}{2n}}$. Es obvio que para $k = 1$ las matrices de Hadamard alcanzan la cota indicada, dado que

$$(\det(H))^2 = \det(H)\det(H^t) = \det(HH^t) = \det(nI) = n^n.$$

Más aún, demostró que las matrices que llevan su nombre son las únicas que alcanzan esta cota. Evidentemente, para $k \neq 1$, basta tomar $k \cdot H$ para H matriz de Hadamard de orden n.

A parte de los trabajos de Sylvester y Hadamard ya mencionados, entre los más importantes, orientados a la construcción de matrices de Hadamard de orden cualquiera prefijado, cabe destacar el de Scarpis [102], quien probó que cuando p es un número primo congruente con 3 (módulo 4), entonces existe una matriz de Hadamard de orden $p + 1$, mientras que si p es primo congruente con 1(módulo 4), existe una matriz de Hadamard de orden $2(p + 1)$.

Más tarde, Paley generalizó el trabajo de Scarpis, proponiendo una manera de construir infinitas matrices de Hadamard asociadas a cada número primo p, una para cada potencia p^k de dicho número [92]. La construcción de las matrices de Paley a partir de un número primo impar p utiliza la *matriz de Jacobsthal*, y requiere encontrar los *residuos cuadráticos* módulo p^k, esto es, los cuadrados no nulos módulo p^k.

Williamson generalizó el trabajo de Paley y consideró métodos innovadores que le permitieron tanto a él como, más tarde, a Baumert, Golomb y Hall, encontrar matrices de Hadamard para algunos órdenes hasta entonces no estudiados. El método de Williamson [129], consiste en la búsqueda de matrices de Hadamard a partir de matrices por bloques, restringidas a ciertas condiciones con el fin de reducir la complejidad del problema.

Más tarde, Cooper, Wallis y Turyn generalizaron el trabajo de Williamson en [21, 124, 122].

Más recientemente, se ha tratado de caracterizar cuándo las *matrices desarrolladas* sobre un grupo G pueden conformar matrices de Hadamard.

Una matriz M cuadrada de orden v y entradas ± 1 se dice *desarrollada* sobre un grupo finito G de v elementos si proviene de la tabla de multiplicar del grupo G. En el sentido de que dada una ordenación de los elementos de G, existe una aplicación de conjuntos $g : G \to \mathbb{F}_2$, de modo que $M = (g(ab)) \quad \forall a, b \in G$; i.e., cada fila de la matriz consiste en una cierta permutación de los elementos del conjunto G.

Desafortunadamente, las matrices binarias así construidas se caracterizan por tener el mismo número de entradas positivas y negativas en cada fila, y toda matriz de Hadamard con esta propiedad (matriz de Hadamard *regular*) se caracteriza por tener orden un cuadrado perfecto, $4t^2$ [125]. De hecho, la existencia de una matriz de Hadamard regular de orden $4n$ equivale a la existencia de un diseño simétrico de $4n$ puntos, con $n = m^2$ un cuadrado perfecto [10].

Sin embargo, una versión más avanzada de matriz desarrollada está permitiendo encontrar matrices de Hadamard en multitud de órdenes, y se especula que pueda determinar matrices en todos los órdenes múltiplos de 4. Este método se basa en la construcción de matrices desarrolladas *cocíclicamente* [26], por medio de la maquinaria que provee la *Teoría de desarrollo cocíclico de diseños* [24].

Sea v un número natural, S un conjunto finito y Π_F y Π_C sendos grupos de permutaciones sobre S. Un $(v, \Pi_F, \Pi_C, \beta, S)$-diseño consiste en una matriz cuadrada, X, de orden v con entradas en S, de modo que cada par de líneas paralelas (filas o columnas) satisfacen un cierto conjunto de relaciones dado, β, las cuales son invariantes bajo

1. permutación de filas o columnas de X,
2. la aplicación de cualquier permutación $\pi \in \Pi_F$ sobre cualquier fila de X, y
3. la aplicación de cualquier permutación $\pi \in \Pi_C$ sobre cualquier columna de X.

Usualmente, se tiene que $\Pi_F = \Pi_C = \Pi$. En este caso se habla simplemente de (v, Π, β, S)-diseños.

Como ejemplo de este tipo de diseños podemos destacar los $PCD(v, \Lambda)$ (del inglés, *pairwise combinatorial design*), que describimos a continuación.

Para ello, consideremos un subconjunto Λ, no vacío, de matrices $2 \times n$ $(n \geq 1)$ con entradas en S. Sea Π_Λ el mayor subgrupo de Π_S (permutaciones de S), de modo que para cualquier matriz $M \in \Lambda$ la matriz que se obtiene al aplicar a la segunda fila de M cualquier permutación de Π_Λ también está en Λ:

$$\pi \in \Pi_\Lambda \Leftrightarrow \forall\, M = \begin{pmatrix} x_1 & \cdots & x_n \\ y_1 & \cdots & y_n \end{pmatrix} \in \Lambda, \qquad \begin{pmatrix} x_1 & \cdots & x_n \\ \pi(y_1) & \cdots & \pi(y_n) \end{pmatrix} \in \Lambda.$$

Bajo estas premisas, un $PCD(v, \Lambda)$ es un $(v, \Pi_\Lambda, \beta, S)$-diseño, donde el conjunto β de relaciones consiste en que cualquier par de líneas paralelas del diseño constituye un elemento de Λ.

Cualquier matriz de Hadamard de orden v constituye un ejemplo de $PCD(v, \Lambda)$, en el que

- $S = \mathbb{F}_2 = \{1, -1\}$,
- Λ es el conjunto de matrices $2 \times n$ sobre $\mathbb{F}_2$ con sus dos filas ortogonales,
- $\Pi_\Lambda = \{\pi_{+1}, \pi_{-1}\}$, donde $\pi_{\pm 1}$ es la permutación resultante de multiplicar por ± 1.

Una propiedad importante de los $(v, \Pi_F, \Pi_C, \beta, S)$-diseños es que admiten ser extendidos a diseños n-dimensionales en determinadas circunstancias, por medio de las *funciones abelianas de extensión.*

Estas funciones abelianas de extensión se pueden caracterizar desde el punto de vista (co)homológico. De hecho, Horadam identificó las funciones abelianas de extensión como 2-cociclos propios de $H^2(G, C)$, lo que dio lugar a que toda matriz desarrollada por una función de extensión abeliana recibiera el nombre de *matriz cocíclicamente desarrollada* (o más brevemente *matriz cocíclica*).

Horadam y de Launey establecieron en [26] un algoritmo cuadrático para determinar si una matriz cocíclica normalizada es o no de Hadamard, en función de si la suma de los elementos de cualquier fila, salvo la primera (de entradas sólo +1), es o no nula. Llamamos a este procedimiento *test de hadamard cocíclico.*

Así, para encontrar las matrices cocíclicas de Hadamard sobre un grupo G, es necesario encontrar un sistema generador de los 2-cociclos normalizados sobre G. A partir de él, basta generar todas las matrices cocíclicas normalizadas mediante el *producto Hadamard* (i.e., punto a punto) de los generadores, para después aplicarles el test de Hadamard cocíclico.

Topamos con un problema característico del *Álgebra Homológica*: la determinación de los generadores de 2-cobordes y 2-cociclos representativos para un grupo dado G.

El Álgebra Homológica [19, 87, 126], como disciplina con entidad independiente de la Topología Algebraica, terminó de fraguarse en la década que comprende los años de 1950 a 1960, después de las aportaciones de multitud de matemáticos, con especial mención para Eilenberg y Mac Lane, y el lenguaje de categorías y funtores que elaboraron [33].

En sus orígenes, encontramos los estudios acerca de los *espacios esféricos* [73, 31, 32, 29], y la inquietud por determinar la *homología* [30, 87] de espacios dados. Más concretamente, cada n-símplice de un espacio topológico X dado tiene un borde que consiste en $(n-1)$-símplices. Si llamamos K_n al grupo abeliano libre generado por todos los n-símplices, el operador ∂ que asigna a cada n-símplice la suma alternada de sus símplices borde constituye un homomorfismo $\partial : K_n \to K_{n-1}$. Dado que $\partial\partial = 0$, tiene sentido considerar el cociente $H_n(X) = \operatorname{Ker} \partial_n / \operatorname{Im} \partial_{n-1}$, que es el que se conoce como n-módulo de homología de X.

Esta noción transcendió a otras categorías, como la de grupos, módulos y álgebras.

Restringiéndonos a la categoría de grupos abelianos, el conjunto $\mathrm{Hom}(A, C)$ de todos los homomorfismos de grupos de A en C constituye un nuevo grupo conmutativo, bajo el producto punto a punto. Más aún, $\mathrm{Hom}(-,-)$ constituye un funtor covariante fijada la primera componente y contravariante fijada la segunda, de modo que a cada $\alpha : A \to A'$ se le asocia $\bar{\alpha} : \mathrm{Hom}(A', C) \to \mathrm{Hom}(A, C)$ con $\bar{\alpha}(f) = f\alpha$.

A partir de un complejo (K, ∂), se puede generar otro complejo

$$\mathrm{Hom}(K_0, C) \xrightarrow{\bar{\partial}} \mathrm{Hom}(K_1, C) \xrightarrow{\bar{\partial}} \mathrm{Hom}(K_2, C) \to \cdots$$

El grupo cociente $H^n(K, C) = \mathrm{Ker}\, \partial_n / \mathrm{Im}\, \partial_{n+1}$ constituye el n-módulo de *cohomología* de K con coeficientes en C.

Pronto surgió la necesidad de calcular explícitamente estos invariantes para según qué objetos, y se recurrió a las *sucesiones espectrales* [84] como herramientas auxiliares; que facilitaron la determinación de la homología de espacios fibrados (sucesiones espectrales de Leray-Serre [84, 109] y Eilenberg-Moore [36, 37, 101]), la cohomología de G-módulos para G grupo de subgrupo normal conocido (sucesiones espectrales de Lyndon [86], Hochschild-Serre [108, 60]), etc.

Aún así, el Álgebra Homológica seguía considerándose como un campo de corte eminentemente teórico, que resultaba útil en la demostración de teoremas de existencia no constructivos en Álgebra y Topología Algebraica; pero se tornaba un paraje hinóspito cuando se trataba de realizar cálculos explícitos, plagado de algoritmos teóricos impracticables en tiempo real.

La teoría de *homotopía racional* [96, 97, 117, 118, 119] introdujo la posibilidad de buscar objetos algebraicos "simples" (llamados *modelos* [9, 53, 54, 55]), topológicamente equivalentes a espacios topológicos más complejos.

Dos décadas más tarde, a finales de 1980 y principios de 1990, con el antecedente de los trabajos de Shih y Brown [111, 14], esta idea cristalizó en la *Teoría de Perturbación Homológica* [51, 47, 68, 48, 106, 98]; la cual trata de reducir el problema del cálculo (co)homológico en términos de *contracciones* y *perturbaciones* de las mismas.

Si a esta técnica le unimos estudios adecuados acerca de la preservación de estructuras algebraicas en contracciones y perturbaciones (ver por ejemplo [98, 44, 20, 75]),

resulta que muchos de los algoritmos impracticables del Álgebra Homológica pasan a ser procedimientos que, aunque no obstante en general todavía de elevada complejidad, pueden implementarse en máquina y dar lugar a cálculos explícitos en baja dimensión, para una aplicación ulterior, como es nuestro caso [45, 2].

En este sentido, son varios los programas que intentan formalizar una plataforma informática básica para el cálculo en Álgebra Homológica: Axiom [78, 81], GAP [103], MAGMA [12, 18], Kenzo [27, 106, 101, 107], etc.

Desde esta perspectiva se puede abordar con garantías el problema que planteábamos antes: la determinación de un sistema de generadores de 2-cobordes y 2-cociclos representativos de un grupo G.

Sea $(C, +)$ un grupo aditivo abeliano finito y $(G, \bullet)$ un grupo multiplicativo (no necesariamente abeliano) finito de v elementos, ordenados de la siguiente forma $G = \{a_1 = 1, a_2, \ldots, a_v\}$. Sea $M = (f(a,b))$ una matriz cocíclica sobre G desarrollada sobre un 2-cociclo $f : G \times G \to C$.

Denotemos por $B(G)$ al subgrupo de 2-cobordes, formado por las funciones del tipo

$$f(a,b) = \alpha(a)\alpha(b)\alpha(ab)^{-1}, \quad a, b \in G,$$

para una aplicación de conjuntos $\alpha : G \to C$ prefijada.

El grupo $Z(G)$ de todos los 2-cociclos consiste en la suma $B(G) \oplus H^2(G; C)$.

Un sistema de generadores de $B(G)$ se puede determinar mediante una reducción por filas en $\mathbb{Z}$ de una matriz $v \times v^2$, donde la fila i está asociada a la función característica $\alpha_i : G \to \mathbb{Z}$ que lleva $\alpha_i(a_j) = \delta_{ij}$, con δ la función de Kronecker.

Obtener un sistema de generadores de $H^2(G; C)$ no resulta tan sencillo, en general. De hecho, el problema de la determinación explícita de un conjunto completo de representantes de n-cociclos, en general, no parece haber sido tradicionalmente el centro de los estudios de los cohomologistas, al menos, hasta la última década del siglo XX.

Horadam y de Launey plantean la cuestión a través de la descomposición que provee el *Teorema de Coeficientes Universales* [59] de $H^2(G; C)$,

$$H^2(G; C) \cong \mathrm{Ext}_{\mathbb{Z}}(G/[G,G], C) \oplus \mathrm{Hom}(H_2(G), C),$$

lo cual da lugar a matrices de tamaño desproporcionado para órdenes no demasiado elevados del grupo G.

Una segunda alternativa surge del trabajo de Flannery, quien calcula $H_2(G)$ a partir de la fórmula de Hopf, e identifica $H^2(G;C)$ como suma de las imágenes de sendos morfismos de *inflación* y *transgresión*; las cuales constituyen copias isomorfas de $\mathrm{Ext}(G/[G,G],C)$ y $\mathrm{Hom}(H_2(G),C)$, respectivamente.

Nuestro trabajo progresa sobre el desarrollado por Horadam y de Launey, con el objetivo primordial de rebajar el coste de construcción del término $\mathrm{Hom}(H_2(G),C)$, sin sacrificar la posibilidad de utilizar el test de Hadamard cocíclico. La idea será utilizar un *modelo homológico* conocido de G, de modo que el tamaño de las matrices a manejar permanece constante, independientemente del orden del grupo G considerado.

En particular, nos centraremos en el caso de grupos G que sean productos iterados de extensiones centrales y productos semidirectos de grupos abelianos finitos.

En realidad, la memoria tiene tres frentes distinguidos:

- Uno de corte más teórico, cuyos resultados principales son, de un lado, la determinación de modelos (co)homológicos para productos iterados de extensiones centrales y productos semidirectos de grupos abelianos finitos; y, de otro, el establecimiento de un método eficiente de construcción de matrices cocíclicas de Hadamard.

- Otro, de programación de algoritmos en *Mathematica*, que permitirá encontrar resultados experimentales con el ordenador, a demostrar posteriormente. Esto explica que la memoria esté salpicada de rutinas en *Mathematica*, puesto que en verdad éstas han sido fundamentales a la hora de establecer buena parte de los resultados que se recogen en el capítulo 3.

- Un tercero, sobre las aplicaciones que se derivan del trabajo realizado.

Estos contenidos se entremezclan a lo largo de tres capítulos.

El primero de ellos, de fundamentos, sirve para situar la memoria en su contexto, y describe con más detalle varios tópicos que ya hemos presentado en esta introducción,

como son: los códigos correctores de errores, las matrices de Hadamard, los diseños, la Teoría de desarrollo cocíclico de diseños, las matrices cocíclicas de Hadamard y los grupos de Hadamard. Aquí encontramos las aplicaciones potenciales de la tesis.

El capítulo 2 se centra en el problema del cálculo de la (co)homología de grupos finitos. En la sección inicial se describe cuál es el procedimiento general para realizar cálculos en (co)homología desde el punto de vista de la Teoría de Perturbación Homológica, a saber: se busca un *modelo homológico* (DG-módulo de tipo finito que admite una equivalencia de homotopía particular, denominada *contracción*, desde el grupo original), y posteriormente se determina su (co)homología mediante el *algoritmo de Veblen* (mecanismo matricial basado en la forma normal de Smith de la matriz diferencial).

En el segundo apartado, se hace un repaso de los resultados clásicos de [34, 35] acerca de la (co)homología de grupos abelianos, y se establecen las contracciones elementales sobre las que fundamentar los resultados posteriores. Para concluir, se comenta el modo en que se ha implementado las rutinas correspondientes en *Mathematica*.

La tercera sección está dedicada a las extensiones centrales $A_f \rtimes G$ con A abeliano, progresando sobre el trabajo de Rubio en [99, 100], el cual incluye una versión más general del modelo homológico que para estos grupos se describe en el Teorema 2.3.5. A partir de este resultado, se determina un modelo cohomológico en el Teorema 2.3.6. Posteriormente, se comenta la implementación de las contracciones, realizada en *Mathematica*, así como algunos ejemplos concretos de ejecución.

El siguiente apartado corresponde al estudio de modelos (co)homológicos para productos semidirectos $A \ltimes_\chi G$ con G abeliano. En el Teorema 2.4.3 se describe el modelo cohomológico, que construimos progresando sobre el modelo homológico del Teorema 2.4.2, el cual procede de [3, 4, 1], salvo por la simplificación de morfismos que recoge la Proposición 2.4.1. A continuación, se detalla la codificación de las rutinas correspondientes y se muestran algunos cálculos.

En la cuarta sección se combinan los resultados anteriores hasta obtener modelos (co)homológicos para productos iterados de extensiones centrales y productos semidirectos de grupos abelianos finitos, en los teoremas 2.5.1 y 2.5.2, respectivamente. A la hora de adaptar las implementaciones previas a este caso, se diseña una manera

estándar de introducir un producto iterado, en forma de árbol binario de productos de grupos de los estudiados en las secciones precedentes. Incluimos también algunos ejemplos de ejecución.

La última sección está destinada al análisis de las estructuras multiplicativas subyacentes en los modelos hallados a lo largo del capítulo. En el estudio distinguimos dos etapas: primero, las estructuras de (co)álgebras estrictas (esto es, asociativas); para después atacar el de las estructuras asociativas salvo homotopía, más comúnmente conocidas como A_∞-estructuras.

Las estructuras sobre los modelos homológicos de productos directos de grupos abelianos fueron estudiadas décadas atrás, aunque nosotros las revisamos desde el punto de vista de los tipos de contracciones de [98] y las A_∞-estructuras, según los lemas 2.6.3, 2.6.4, 2.6.5 y 2.6.6.

En las extensiones centrales $A_f \rtimes G$, el estudio es más elaborado. Las notas 2.6.7, 2.6.8 y 2.6.9 descartan la existencia de una estructura de álgebra natural en el modelo homológico $hA\tilde{\otimes}hG$ construido. Utilizando el ardid tensorial, en el Teorema 2.6.10 se prueba que dicho modelo posee la estructura de A_∞-coálgebra naturalmente heredada de $\bar{B}(\mathbb{Z}[A_f \rtimes G])$. El Teorema 2.6.12 va más lejos, y garantiza que el DG-módulo $hA\tilde{\otimes}hG$ posee la estructura de A_∞-producto tensorial torcido, según el producto de la DGA-álgebra conmutativa hA y la A_∞-estructura de coálgebra sobre hG naturalmente heredada de $\bar{B}(\mathbb{Z}[G])$. Una versión general de este resultado se enuncia en el Teorema 2.6.11.

El caso de los productos semidirectos es sensiblemente más complejo. Nuevamente, el modelo homológico $hA\tilde{\otimes}hG$ obtenido no posee la estructura natural de álgebra, tal como se recoge en las notas 2.6.13 y 2.6.14. El análogo del Teorema 2.6.10 en la modalidad de productos semidirectos, que ya se demostrara a nivel de resoluciones en [1], se enuncia aquí en el Teorema 2.6.15 a nivel de complejos reducidos. Sin embargo, no es posible extrapolar tal cual el Teorema 2.6.12 al caso de productos semidirectos, puesto que los productos tensoriales torcidos implicados no son principales. El Teorema 2.6.16 y el Lema 2.6.17 permiten demostrar el Teorema 2.6.18, que extiende el Teorema 2.6.11 para el caso de productos tensoriales torcidos no principales. Desafortunadamente, este resultado no puede llegar a aplicarse al caso de productos semidirectos, puesto que no se dan las condiciones apropiadas.

Al comienzo del capítulo 3 se describe el *método de la reducción homológica* (Algoritmo 3.1.4), a aplicar sobre los modelos encontrados en el capítulo anterior para determinar matrices cocíclicas de Hadamard sobre distintos productos iterados de extensiones centrales y productos semidirectos de grupos abelianos finitos. Este método se fundamenta en las proposiciones 3.1.1, 3.1.2 y 3.1.3.

En la segunda sección del capítulo se describen los resultados cosechados por Horadam, Baliga y Flannery en la búsqueda de matrices cocíclicas de Hadamard sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$ y D_{4t}, según sus aproximaciones.

Con vistas a comparar esos procedimientos con el método de la reducción homológica que nosotros proponemos, en la sección tercera atacamos la determinación de matrices cocíclicas de Hadamard sobre estas familias de grupos.

El ambos casos, la primera etapa consiste en fijar una base de 2-cobordes (proposiciones 3.3.1 y 3.3.18), sobre las que construir sendas bases de 2-cociclos normalizados (corolarios 3.3.2 y 3.3.19).

Posteriormente, atendiendo a las nociones de *filas en posición Hadamard*, *configuración* y *2-coborde generalizado* (definiciones 3.3.3, 3.3.4 y 3.3.5), se encadena una serie de resultados (proposiciones 3.3.8, 3.3.9, 3.3.10, 3.3.14, 3.3.15 y 3.3.16, y corolarios 3.3.11, 3.3.12 y 3.3.13), que desembocan en el Teorema 3.3.17, que da cotas superior e inferior para el número de generadores a considerar a la hora de formar una matriz cocíclica de Hadamard sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$. Aportamos una tabla con matrices cocíclicas de Hadamard sobre estos grupos para valores impares de t comprendidos en el intervalo $3 \leq t \leq 13$.

En el caso de grupos diédricos, las definiciones 3.3.21 y 3.3.22 y la Proposición 3.3.20 cristalizan en el Teorema 3.3.23, que caracteriza cuándo una configuración de 2-cociclos deja en posición Hadamard (i.e., con el mismo número de $+1$ y -1) una fila dada. Por otra parte, las proposiciones 3.3.24, 3.3.25 y 3.3.26 conducen al Teorema 3.3.27, que permite reducir a la cuarta parte el coste computacional en la evaluación del test de Hadamard para las configuraciones en D_{4t} que aportan matrices cocíclicas de Hadamard con mayor densidad. En cuanto a cotas acerca del número de generadores d a combinar en estas configuraciones a la hora de construir matrices cocíclicas de Hadamard, el Teorema 3.3.29 establece que $t+1 \leq d \leq 3t$, a partir de la condición que da el Lema 3.3.28. Todos estos resultados se ponen en práctica para

determinar matrices cocíclicas de Hadamard explícitas, basándonos en un algoritmo genético que hemos diseñado a la medida de los grupos D_{4t}.

Esta sección se ultima con una tabla comparativa de matrices cocíclicas de Hadamard sobre diversas familias de productos iterados de extensiones centrales y productos semidirectos de grupos. En particular, determinamos todas las matrices cocíclicas de Hadamard que existen sobre $\mathbb{Z}_4 \times \mathbb{Z}_2^2$, dato que a nuestro parecer se desconocía hasta el momento [63]; así como sobre ciertas extensiones centrales $\mathbb{Z}_{2tf_1} \rtimes \mathbb{Z}_2$ y productos iterados de extensiones centrales y productos semidirectos $(\mathbb{Z}_{t\ f} \rtimes \mathbb{Z}_2) \ltimes_{\bar{\chi}} \mathbb{Z}_2$, con $1 \leq t \leq 5$.

Hemos de incidir nuevamente en la importancia de la labor de implementación que se realiza en este trabajo, puesto que la mayor parte de los resultados anteriores fueron primigeniamente establecidos de manera experimental con el ordenador.

A continuación, abrimos una sección que se centra en el uso de las matrices de Hadamard para la construcción de códigos correctores de errores. Incluimos aquí una reseña de los trabajos [7, 66, 67], en los que se redescubren muchos de los códigos más usuales como verdaderos *códigos cocíclicos*, provenientes de matrices cocíclicas de Hadamard. Terminamos la sección describiendo una aplicación inusual de los códigos, concerniente al diseño de criptosistemas de clave pública.

Finalizamos la memoria con una última sección, dedicada a conclusiones y problemas abiertos; el más destacable de los cuales sería establecer un nexo entre diseños n-dimensionales y n-cohomología, con $n > 2$, paralelo al existente entre 2-diseños y 2-cohomología.

Contenido

Capítulo 1.

Fundamentos

Capítulo 1.

Fundamentos

En la sociedad que nos ha tocado vivir, instrumentos como la televisión, radio, aparatos de audio, lectores compactos, teléfonos móviles,... se han vuelto indispensables para la mayor parte de la población. Todos ellos tienen una cosa en común: su utilidad en la transmisión de información. En otros ámbitos muy dispares como el mundo de la banca, el militar, la investigación espacial,... la transmisión de información sigue siendo uno de los problemas prioritarios. Esto hace de la *teoría de códigos* una herramienta fundamental hoy día, puesto que la información que se pretende transferir en cualquier situación suele estar expuesta a multitud de interferencias que pueden provocar distorsiones en el mensaje. De manera que es esencial poder detectar si se ha producido algún error y, en su caso, reconstruir la información enviada originalmente a partir de los datos recibidos; bajo ciertas condiciones determinadas por *códigos detectores* y/o *correctores de errores.*

La teoría de códigos es un tema relativamente reciente cuyos comienzos se inspiran en los trabajos que realizaron Golay, Hamming y Shannon de forma independiente a finales de la década de 1940. Aunque su origen se remonta a problemas relacionados más propiamente con la ingeniería, el enorme avance que se ha producido en este campo a lo largo de su breve historia se debe en gran medida a las técnicas matemáticas cada vez más sofisticadas que, en algunos casos, se han ido desarrollando de forma paralela.

Una de las aplicaciones del trabajo expuesto en esta memoria es precisamente la construcción de *códigos óptimos.* Esto hace indispensable dedicar una primera sección de este capítulo a la teoría de códigos. No pretendemos realizar un estudio exhaustivo de esta teoría, puesto que un tema tan extenso y apasionante requeriría varios volúmenes y, en realidad, no es ese nuestro objetivo. Sin embargo, sí intenta ser

una introducción a dicha teoría en la que se pongan de manifiesto nociones relevantes relacionadas con los estudios realizados en esta tesis.

Comenzaremos analizando el proceso que ha de seguir la información desde el momento en que se envía hasta que es recibida. Esto nos llevará al estudio de los códigos y, en particular, de las propiedades fundamentales que los caracterizan. Así, introduciremos algunos conceptos útiles para determinar si un código dado es bueno. Nos centraremos en los códigos correctores de errores, ya que tienen multitud de aplicaciones, tales como la retransmisión de imágenes desde el espacio, el almacenaje de información en discos compactos, etc. Estudiaremos cómo pueden detectar y corregir algunos de los errores producidos durante la transmisión de un mensaje. Esto permitirá comprender mejor su utilidad, e incluso, su necesidad. Recopilaremos algunos resultados que permiten determinar el número máximo de palabras que puede llegar a tener un código con determinadas propiedades (*longitud de sus palabras* y *distancia mínima*) para que sea corrector de e errores. Veremos que los *códigos lineales*, bajo ciertas condiciones, pueden llegar a ser óptimos respecto a su número de palabras, corrigiendo un número dado de errores. Eso hará que nos detengamos en recordar algunas nociones relacionadas con dichos códigos, así como en su forma de operar a la hora de codificar y decodificar mensajes. Si nos reducimos a *códigos binarios*, no necesariamente lineales, tendremos otra vertiente a partir de la cual podremos encontrar *códigos óptimos* en el sentido anterior. Así, surgirá la necesidad de buscar *matrices de Hadamard* en todos los órdenes posibles. Textos fuente sobre los que hemos cimentado el desarrollo son [17, 61, 94].

El estudio de la matrices de Hadamard podría decirse que comenzó a mediados del siglo XIX, con los trabajos que realizara Sylvester [120], aunque fue a finales de ese siglo cuando Hadamard determinó en [52] algunas de las propiedades y aplicaciones que caracterizan a estas matrices y comenzó a preguntarse acerca de su existencia en distintos órdenes. Así es como surgió la *conjetura de Hadamard*, según la cual las matrices de Hadamard existen para los órdenes 1, 2 y todos los múltiplos de 4. El interés por encontrar matrices de Hadamard en todos los órdenes posibles no es meramente teórico. En realidad es un interés eminentemente práctico, puesto que las matrices de Hadamard tienen un abanico muy amplio de aplicaciones. Entre ellas se encuentra la construcción de códigos correctores de errores óptimos, ya mencionada.

La segunda sección de este capítulo comprende una introducción al mundo de las matrices de Hadamard. Comienza con su definición para después mencionar algunas

de sus múltiples aplicaciones. Tras hacer una recopilación de las propiedades fundamentales que satisfacen, se presentarán determinados problemas abiertos relacionados con las mismas. Posteriormente, basándonos en la referencia por antonomasia [58], realizaremos un somero seguimiento histórico en lo concerniente a la búsqueda y construcción de las matrices de Hadamard.

Códigos y matrices de Hadamard aparecen de la mano de *diseños*, los cuales constituyen un punto de interés principal en esta memoria.

Así, en la tercera sección de este capítulo se analizará la ligazón existente entre determinados *diseños* y las matrices de Hadamard. Nos centraremos en dos tipos de diseños; los diseños por bloques o t-diseños de parámetros (v, k, λ) y los diseños combinatorios. Dentro del primer tipo destacaremos los *diseños de Hadamard*, los cuales están estrechamente relacionados con las matrices de Hadamard, a través de su *matriz de incidencia* asociada. La segunda parte de la sección la dedicaremos a los diseños combinatorios. En realidad, los diseños por bloques pueden ser considerados también como diseños combinatorios en un sentido mucho más amplio que el que aquí se recogerá. Sin embargo, hemos decidido restringir el concepto de diseños combinatorios, con el fin de poder distinguir entre unos diseños y otros. Veremos ejemplos de diseños combinatorios, de manera que pondremos de manifiesto la relación entre estos diseños y las matrices de Hadamard, así como alguna relación entre determinados diseños combinatorios y diseños por bloques.

En este punto, nuestro interés se centrará en la extensión de diseños 2-dimensionales a diseños n-dimensionales. Concretamente, no en la extensión en sí, sino más bien en un procedimiento que la facilite.

Esto motiva que dediquemos un apartado al estudio desarrollado por de Launey en [23] para extender los diseños 2-dimensionales a diseños n-dimensionales. Este método está basado en el uso de *funciones abelianas de extensión.*

La búsqueda de funciones abelianas de extensión llevó a Horadam y de Launey a lo que se denomina *Teoría de desarrollo cocíclico de diseños* [24], la cual constituye el pilar fundamental de esta memoria.

La cuarta sección de este capítulo está dedicada, precisamente, a este tema. En ella se describirá cómo Horadam y de Launey caracterizaron en [24], a partir del trabajo anterior de de Launey [23], un sistema de generadores para funciones abelianas de

extensión, identificando dichas funciones como verdaderos 2-cociclos.

Una de las aplicaciones inmediatas de la teoría de desarrollo cocíclico de diseños es la construcción de matrices *cocíclicas de Hadamard*, que aparecen naturalmente asociadas a 2-cociclos *ortogonales*. En la quinta sección abordaremos los resultados principales que sentaron al respecto Horadam y de Launey en [26].

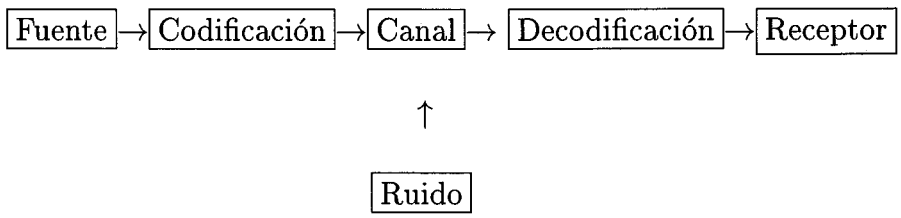
Por último, en la sexta sección, presentaremos la relación existente entre matrices cocíclicas de Hadamard y *grupos de Hadamard* [74], lo cual nos permitirá obtener algunas obstrucciones para el carácter Hadamard de matrices cocíclicas sobre ciertos grupos.

Nuestro propósito en esta memoria es progresar a partir de estos fundamentos para determinar desarrollos cocíclicos de diseños sobre productos iterados de extensiones centrales y productos semidirectos de grupos finitos abelianos; y por ende, matrices cocíclicas de Hadamard y códigos correctores de errores óptimos asociados a ellas.

1.1 Códigos correctores de errores

Un sistema de transmisión de información ha de constar necesariamente de una *fuente* que produzca los mensajes que se desean enviar. La información a emitir está compuesta por *unidades elementales de información* (por ejemplo, si el mensaje es una frase, las unidades elementales de información podrían ser las letras que lo componen). También se requiere un *código*, suficientemente amplio como para que a cada unidad elemental de información se le asocie una palabra del código y que cada palabra del código esté relacionada, a lo más, con una unidad elemental. Una vez codificado el mensaje, se puede transmitir. Esto se hace a través del denominado *canal*, que puede ser la atmósfera, una línea telefónica, el papel sobre el que se encuentra impreso el mensaje, etc. Mientras el mensaje viaja a través del canal puede verse sometido a *ruidos* que provoquen distorsiones en el mensaje, como consecuencia de inclemencias meteorológicas, interferencias, impresión defectuosa,... El mensaje codificado y modificado por los ruidos llega al *receptor*, que tendrá que conocer el código en que se ha enviado la información para, si es posible, detectar y corregir los *errores* producidos en la transmisión y recuperar la información enviada inicialmente mediante la decodificación del mensaje ya corregido.

Gráficamente, esta situación se podría plasmar de la siguiente manera:



En el diagrama anterior, el *ruido* se destapa como un elemento muy importante e imposible de obviar, que origina la necesidad de desarrollar una teoría de detección y corrección de errores en la transmisión de información.

En la práctica, se trata de combinar el uso de canales de comunicación con un bajo nivel de ruidos y *sistemas de filtros* para paliar el efecto de los mismos. Estos aspectos competen más propiamente al campo de la Ingeniería que al matemático, por lo que los mantendremos al margen. En cambio, una vez que se ha elegido un canal en concreto, es necesario construir un código para el proceso de de/-codificación; el cual habría de satisfacer ciertas condiciones, como son una fácil transmisión y máxima transferencia de información por unidad de tiempo, una buena capacidad de detección y corrección de errores y una rápida de-/codificación.

En lo que concierne a la transferencia de información por el canal, surge la noción de *capacidad* de un canal, que corresponde a la magnitud que mide la habilidad del canal para transmitir información.

Hay que tener en cuenta que el concepto de *información* que aquí manejamos tiene un fuerte carácter probabilístico, en tanto en cuanto puede interpretarse como la información $I(\mathcal{U}|\mathcal{W})$ que puede deducirse de la variable aleatoria $\mathcal{W}$ de los mensajes recibidos, con respecto a la variable aleatoria $\mathcal{U}$ de los mensajes inicialmente enviados. Incidamos brevemente en este aspecto, que se recoge en [127] con mayor profundidad.

Esta noción probabilística de información fue introducida en los trabajos de Hartley hacia 1928, y posteriormente interpretada en función del concepto de *entropía* o *incertidumbre*, $H(\mathcal{U})$, de una variable aleatoria $\mathcal{U}$, que mide la incertidumbre del valor a tomar por dicha variable aleatoria; de modo que si $\mathcal{U}$ toma n valores distintos con probabilidades $p_1, \ldots, p_n$, es $H(\mathcal{U}) = -\sum_{k=1}^{n} p_k \log_2 p_k$.

Así, la información $I(\mathcal{U}|\mathcal{W})$ que la variable aleatoria $\mathcal{W}$ arroja sobre la variable

aleatoria $\mathcal{U}$ no es más que la diferencia $H(\mathcal{U}) - H(\mathcal{U}|\mathcal{W})$ de la entropía de $\mathcal{U}$ y la entropía de $\mathcal{U}$ conocida $\mathcal{W}$; esto es, cuánto se reduce la incertidumbre de $\mathcal{U}$ al conocer $\mathcal{W}$.

La capacidad de un canal resulta ser el máximo de entre las informaciones $I(\mathcal{U}|\mathcal{W})$, para $\mathcal{U}$ y $\mathcal{W}$ recorriendo las variables aleatorias asociadas a todas las posibles formas de codificación a la hora de transmitir mensajes por el canal. Este valor, que parece tan etéreo, se puede calcular como la solución de un problema de extremos condicionados de una función de varias variables, dado que $I(\mathcal{U}|\mathcal{W})$ es una función que depende exclusivamente de la distribución de probabilidades $p_1, \ldots, p_n$ de $\mathcal{U}$.

En el caso de un canal *binario simétrico* de *fiabilidad* p, en el que se transmiten dos cifras (0 y 1), siendo la probabilidad p de recibir correctamente un dígito independiente del dígito enviado en cuestión; la capacidad es $C(p) = 1 + p\log_2 p + (1-p)\log_2(1-p)$. A modo de curiosidad, notemos que en el caso de este canal la unidad básica de información teórica (comúnmente, *bit*) en la que se mide la magnitud información corresponde a un dígito 0 ó 1, y he aquí la procedencia del término tan utilizado en la jerga del mundo informático.

Centrémonos ahora en el propio código. La actuación de un código corrector puede dividirse en dos etapas:

1. Una primera de *detección*, en la que comprueba si se ha producido algún error en la transmisión. Sirva de ejemplo los códigos de barra que se utilizan para marcar los productos en un supermercado, que consisten en añadir cierta *redundancia* a la etiqueta propia de cada artículo, para facilitar su posterior identificación.

2. La segunda, de *corrección*, donde se corrigen los errores detectados durante la primera etapa.

La corrección suele ser, desde el punto de vista computacional, mucho más costosa que la detección. Esto hace que en multitud de ocasiones interese trabajar con códigos simplemente detectores, ya que puede llegar a ser más pragmático reenviar el mensaje que tratar de corregir los errores cometidos durante la transmisión. En el ejemplo anterior, cuando en el supermercado la lectura del código de barras detecta errores, la persona situada en la caja vuelve a pasar el código por el lector, es decir, *reenvía el mensaje*. Sin embargo, esto no resta interés al estudio de códigos correctores: en

primer lugar, porque a veces es prácticamente imposible reenviar el mensaje, por ejemplo, en el caso de mensajes enviados al espacio, durante la lectura de un disco compacto, etc; en segundo lugar, porque si el canal fuese muy malo, se perdería mucho tiempo retransmitiendo el mensaje una y otra vez hasta conseguir que el receptor percibiese el mensaje sin errores.

Una táctica frecuente a la hora de detectar errores es, de hecho, la de añadir *redundancia* a las palabras enviadas, a modo que comprobación. El siguiente ejemplo puede resultar clarificador.

Consideremos un código formado por las 2^{11} palabras de longitud 11 sobre $\mathbb{Z}_2$ (en el que por ser completo no se puede detectar ningún error), y que se transmiten 10^7 dígitos por segundo en un canal binario simétrico de fiabilidad $p = 1 - 10^{-8}$. De este modo, según el principio de inclusión-exclusión, la probabilidad de que una palabra se transmita incorrectamente es aproximadamente igual a $11p^{10}(1-p) \simeq \frac{11}{10^8}$; de donde resulta que una media de $\frac{11}{10^8} \cdot \frac{10^7}{11} = 0.1$ palabras se transmiten erróneamente cada segundo. Esto es, del orden de 1 palabra cada 10 segundos, 6 en un minuto, 360 en una hora ó 8640 en un día...

Añadamos ahora un dígito *de paridad* a cada una de las palabras del código, de modo que todas ellas contengan un número par de unos. Como es obvio, las palabras recibidas con exactamente un error son detectadas de manera automática. Y la probabilidad de que se produzcan al menos dos errores en la transmisión es $1-p^{12}-12p^{11}(1-p)$, que viene a ser en nuestro caso del orden de $\frac{66}{10^{16}}$. De modo que aproximadamente $\frac{66}{10^{16}} \cdot \frac{10^7}{12} = 5.5 \cdot 10^{-9}$ palabras son transmitidas erróneamente cada segundo sin ser detectadas, lo que se traduce en cerca de ¡una palabra cada 2000 días!

Sin embargo, aunque el añadir redundancia mejora la capacidad detectora de un código, evidentemente, por otro parte, reduce la tasa de transferencia de información.

En cualquier caso, esto no es suficiente: una vez que se han detectado palabras con errores, hay que discernir las posiciones en las que éstos se producen, y para ello, en principio, se requiere la retransmisión del mensaje, con el gasto de tiempo y/o memoria que ello conlleva. Dado que, incluso, a veces es impracticable retransmitir el mensaje (piénsese en los casos ya citados de lectores de discos compactos o transmisiones espaciales), parece natural tratar de incorporar al código ciertas capacidades de corrección, aún a coste de incrementar la longitud de las palabras del mismo y por

tanto reducir la tasa de transferencia de información.

De hecho, el objeto de la teoría de códigos es el diseño de códigos con una tasa de transferencia de información razonable, un bajo coste de de-/codificación y ciertas capacidades de detección y corrección de errores que eviten la necesidad de retransmisión. Así, existen códigos generados a partir de estructuras algebraicas complejas que tras un preprocesamiento más o menos costoso, pero abordable, permiten corregir los errores en un tiempo razonable.

En cuanto a la corrección de errores, parece natural utilizar la técnica del *vecino más próximo*, en el sentido de que recibida una palabra con errores, se busca aquella palabra del código que se le parezca más ó *diste* menos (i.e., que difiera en menos dígitos) y se asume que ésta fue la palabra transmitida inicialmente.

Con frecuencia, se suele utilizar *códigos bloque*, en el sentido de que la información se envía mediante palabras de longitud fija v, de manera que cada palabra está formada por una sucesión de v "letras" (frecuentemente, dígitos), que recaen sobre un "alfabeto" Q de tamaño q (la mayoría de las veces, un cuerpo finito $\mathbb{Z}_q$, y, en particular, $q = 2$).

En estas circunstancias, el *espacio de Hamming* $H(v, q)$ consiste en el conjunto de todas las palabras de longitud v sobre el alfabeto Q. Este espacio se puede dotar de una métrica de manera natural: si una palabra w se transmite a través de un canal con ruido, algunas de las letras de la palabra podrán sufrir un cambio; mientras más letras hayan sido cambiadas, más distará la palabra recibida de la emitida. Así, tiene sentido definir la *distancia Hamming*, que mide el número de posiciones en que difieren las letras de dos palabras dadas $c = (c_1, \ldots, c_v)$ y $w = (w_1, \ldots, w_v)$:

$$d(c, w) = |\{i : c_i \neq w_i, 1 \leq i \leq v\}|.$$

Gracias a la introducción de esta métrica, la técnica del vecino más próximo se puede formalizar mediante argumentos probabilísticos. Denotemos por $p(u, w)$ la probabilidad de que se envíe la palabra u y se reciba la palabra w. Si se utiliza un canal binario simétrico de fiabilidad p, asumiendo que el ruido se produce de manera aleatoria y que la emisión de cada dígito es un suceso independiente, si u y w difieren en d de entre n posiciones, resulta que $p(u, w) = p^{n-d}(1-p)^d$.

Dadas dos palabras u_1 y u_2 que difieran de w en d_1 y d_2 dígitos, respectivamente;

es fácil probar que $p(u_1, w) \leq p(u_2, w)$ si y sólo si $d_1 \leq d_2$, de donde es más probable que la palabra que se enviara originalmente cuando se recibió w fuera la más similar a w de entre todas las del código.

De este modo, la probabilidad $p(C, u)$ de que se envíe una palabra u y que el receptor concluya que efectivamente fue esa la palabra enviada resulta ser la suma de las probabilidades $p(u, w)$ para aquellas palabras w que distan de u menos que de cualquier otra palabra del código C:

$$p(C, u) = \sum_{w \in B(u,C)} p(u, w),$$

donde $B(u, C) = \{w : \ d(u, w) < d(y, w) \ \forall\, y \in C, \ y \neq u\}$.

En el caso en que la distancia entre las palabras del código sea suficiente como para que las distorsiones del medio no lleguen a confundirlas, y suponiendo que en la transmisión no se producen demasiados errores, la información recibida puede rectificarse sin problemas para recuperar el mensaje original mediante esta idea del vecino más próximo. Pero, en algunas ocasiones, las distorsiones sufridas como consecuencia de los errores producidos en la transmisión pueden alterar convenientemente las letras de una palabra, de manera que la palabra más cercana no corresponda a la palabra enviada, confundiendo así dos palabras distintas del código. Es bajo esta idea donde subyace la noción de *código*, que será un subconjunto de al menos dos palabras de $H(v, q)$, de modo que la transmisión se circunscribe a este grupo de palabras.

La dificultad estriba en determinar, según el medio, códigos correctores en los que la palabra del código más próxima a la palabra recibida sea siempre única y coincida con la palabra transmitida originalmente.

A la hora de medir la fiabilidad de un código C se recurre a la *probabilidad media de error*, $\bar{e}(C)$, y la *probabilidad máxima de error*, $e(C)$; de modo que si denotamos $p(u) = 1 - p(u, u)$ la probabilidad de que enviando u se reciba una palabra distinta de u, resulta ser

$$\bar{e}(C) = \frac{1}{|C|} \sum_{u \in C} p(u), \qquad e(C) = \max_{u \in C} p(u).$$

Obviamente, es $e(C) \geq \bar{e}(C)$.

El resultado crucial en teoría de códigos, que enunciara Shannon en 1948 [110], relaciona la capacidad de un canal con la existencia de buenos códigos, de modo

que siempre que la tasa de transmisión de información permanezca por debajo de la capacidad del canal, se puede encontrar códigos de fiabilidad arbitraria, tan buena como uno desee.

Más concretamente, si nos reducimos a un canal simétrico binario de capacidad C, dados $0 < R < C$, $1 \leq M_n \leq 2^{nR}$, $n \in \mathbb{N}$ y $\epsilon > 0$ cualesquiera, existe una sucesión de códigos C_n (que constan de M_n palabras de longitud n, respectivamente) y un natural $n_0(\epsilon)$ de modo que para $n \geq n_0(\epsilon)$ es $e(C_n) \leq \epsilon$.

La cuestión radica, pues, en encontrar los códigos apropiados para según qué canales. Un resultado análogo al anterior [39], garantiza que esta búsqueda se puede reducir a *códigos lineales*, los cuales surgen de forma natural en la determinación de *códigos óptimos*, en un sentido a precisar a continuación.

Un código C se dice corrector de e errores cuando dada cualquier palabra w, existe una y sólo una palabra c del código que dista menos que e de w. Un código de estas características garantiza una transmisión idónea para medios que no produzcan más de e distorsiones.

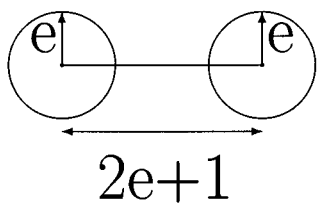
La *distancia mínima* de un código se define como la menor de las distancias entre sus palabras; de forma que si la distancia mínima de un código es d, cualesquiera dos palabras del código difieren al menos en d posiciones (o letras).

Es fácil razonar que cualquier código de distancia mínima d es capaz de detectar hasta $d-1$ errores, puesto que si se envía una palabra y en la transmisión se producen menos de d errores, se recibe una palabra no perteneciente al código. Sin embargo, si se produjesen d errores o más, la palabra recibida podría coincidir con alguna otra palabra del código, impidiendo así la detección de hipotéticos errores.

Para que un código pueda corregir hasta e errores es necesario y suficiente que las bolas de centro las palabras del código y radio e sean disjuntas dos a dos. De este modo, cuando se recibe una palabra que dista menos que e de alguna palabra del código, la palabra recibida estará contenida en la bola centrada en dicha palabra del código y radio e. Así, si la distancia mínima del código es d, se cumplirá la relación $d \geq 2e + 1$, es decir, el código podrá corregir hasta $e = \lfloor \frac{d-1}{2} \rfloor$ errores [1]. La corrección de los errores introducidos durante una transmisión se realiza asumiendo

[1] Como es usual, la notación $\lfloor x \rfloor$ hace referencia a la parte entera por defecto de x.

que la palabra enviada fue la situada en el centro de la bola considerada.



Luego, un buen código corrector de errores ha de satisfacer tres condiciones: que tenga una elevada distancia mínima (para que pueda detectar y corregir un mayor número de errores), un cuantioso número de palabras (a efectos de poder elaborar gran cantidad de información diversa), y que no por ello el problema de reconstruir mensajes se traduzca en un problema de alto coste computacional.

Las dos primeras condiciones parecen difíciles de sostener de manera simultánea, dado que mientras más palabras constituyan el código, la distancia entre ellas será menor, luego, parece natural que la distancia mínima del código también disminuya. En realidad, este problema de la determinación del código de tamaño máximo en $H(v,q)$ de distancia mínima dada d ha sido tratado en multitud de ocasiones, lo que ha derivado en la consecución de diversos resultados parciales (ver, por ejemplo [17]), algunos de los cuales se exponen en la siguiente sección.

1.1.1 Códigos óptimos

Comencemos introduciendo una cota inferior del número de palabras que puede tener un código de distancia mínima d.

Cota de Varshamov-Gilbert [17] . Dado un natural d, en el espacio Hamming $H(v,q)$ existe un código de distancia mínima mayor o igual que d que consta de al menos k palabras, con

$$k = \frac{q^v}{\sum_{i=0}^{d-1} \binom{v}{i} (q-1)^i}.$$

En general, este resultado dista considerablemente del número máximo de palabras posible para un código de las mismas características.

A continuación recopilamos varios resultados destacables en relación a las cotas superiores del número de palabras de un código de $H(v,q)$.

Cota de Hamming [17] . Sean dos naturales d y e con $d \geq 2e+1$. Todo código en $H(v,q)$ de distancia mínima d o superior tiene a lo más k palabras, con

$$k = \frac{q^v}{\sum_{i=0}^{e} \binom{v}{i} (q-1)^i}.$$

La cota se alcanza si y sólo si cualquier palabra de $H(v,q)$ dista a lo más e de una, y sólo una, palabra del código en cuestión. En este caso, el código recibe el nombre de *código perfecto corrector de e errores.*

Cota de Singleton [17]. Un código en $H(v,q)$ de distancia mínima d consta a lo más de q^{v-d+1} palabras.

La cota se alcanza si y sólo si dadas $v-d+1$ posiciones y $v-d+1$ letras del alfabeto existe una y sólo una palabra en el código que presenta esas letras en las posiciones determinadas. En este caso, se habla de un *código de distancia máxima de separación.*

Cota de Plotkin [17] . Sea $t = 1 - \frac{1}{q}$, con $d > tv$. Entonces, un código en $H(v,q)$ de distancia mínima d consta a lo más de $\frac{d}{d-tv}$ palabras.

La cota se alcanza si y sólo si la distancia entre cualquier par de palabras del código es d y el número de palabras del código que contienen una letra dada en una posición prefijada es constante igual a $\frac{d}{q(d-tv)}$.

Bajo ciertas condiciones se pueden construir códigos que alcanzan las cotas anteriores; como por ejemplo los llamados *códigos lineales* y los *códigos de Hadamard* que estudiaremos a continuación.

1.1.2 Códigos lineales

En lo que sigue asumimos que el alfabeto viene dado por un cuerpo $\mathbb{Z}_q$, de modo que el espacio Hamming $H(v,q)$ adquiere de forma natural la estructura de un $\mathbb{Z}_q$-espacio vectorial de dimensión v. Un *código lineal* consiste en un subespacio vectorial de $H(v,q)$.

En los códigos lineales se puede definir el *peso* de una palabra como la distancia de la palabra en cuestión a la *palabra nula* (que consta de v ceros), es decir, mide el número de entradas no nulas de una palabra. El *peso mínimo* de un código es el menor de entre los pesos de las palabras del código, salvo la palabra nula.

Así, la distancia entre dos palabras se puede reinterpretar como el peso de la palabra diferencia de ambas, por lo que es inmediato deducir que las magnitudes distancia mínima y peso mínimo de un código coinciden. De este modo se rebaja la complejidad cuadrática en la determinación de la distancia mínima a una simplemente lineal. (Téngase en cuenta que un código lineal no deja de ser subespacio vectorial).

En un código lineal formado por palabras de longitud v, las k primeras letras de cualquier palabra suelen corresponder al mensaje en sí y los restantes $v-k$ símbolos, correspondientes a una cierta *redundancia*, permiten comprobar que la palabra no ha sufrido errores. Se dice que la dimensión del código es k. Al estar considerando un alfabeto de q letras, el número de palabras del código será q^k.

Por ser los códigos lineales subespacios vectoriales, pueden caracterizarse mediante diversas matrices. La *matriz generadora*, G, de un código se puede construir a partir de una base de palabras del código, de manera que cada una de las filas de la matriz sea una de estas palabras. Definida así, la matriz generadora permite obtener todas las palabras del código mediante las posibles combinaciones lineales de sus filas.

Además, la codificación, es decir, determinar cuál es la palabra del código asociada a un mensaje elemental $x = (x_1, \cdots, x_k)$, es un problema sencillo y, desde un punto de vista computacional, resoluble de manera eficiente (sobre todo en el caso $q = 2$) desde el momento en que dicha palabra se puede obtener mediante la siguiente aplicación biyectiva sobre C

$$\begin{array}{ccc} \mathbb{Z}_q^k & \rightarrow & C \\ (x_1, \cdots, x_k) & \rightarrow & xG = (x'_1, \cdots, x'_v) \end{array}$$

Atendiendo a la dualidad propia del álgebra lineal, el código vendrá igualmente caracterizado por cualquier variedad ortogonal, de matriz generadora H, tal que $GH^T = 0$. Una tal matriz H se denomina *matriz de paridad* o *matriz de comprobación* del código C. Esta matriz permite comprobar si un vector dado u de $\mathbb{Z}_q^v$ es una palabra del código, para ello sólo es necesario tener en cuenta que $Hc^T = 0$ para toda palabra c del código. Es decir, si se recibe la palabra w tal que $Hw^T \neq 0$, es seguro que se ha producido algún error en la transmisión, puesto que en ese caso w no puede ser una palabra del código.

Dada una matriz generadora de un código de dimensión k y palabras de longitud v, se puede obtener otra equivalente mediante una sucesión finita de entre las siguientes transformaciones: la permutación de filas, la sustitución de una fila por su suma con otra y la multiplicación de una fila por cualquier escalar de $\mathbb{Z}_q$. En el caso en que se permuten dos columnas de una matriz generadora del código, se obtiene una matriz generadora de otro código equivalente al primero en el sentido de que ambos tienen igual dimensión, distancia mínima y palabras de igual longitud. Estas operaciones permiten realizar una reducción escalonada por filas de la matriz generadora de un código, dando lugar a una nueva matriz generadora (eventualmente, de un código equivalente) de la forma $G_{k\times v} = (I_k|A)$, con A una matriz de orden $k \times (v-k)$. Cuando la matriz generadora de un código adquiere esta estructura se dice que está en forma estándar.

En la práctica, la bondad de tener una matriz generadora en forma estándar se traduce en la simplificación del cálculo de una matriz de comprobación asociada. Así, una matriz de la forma $H = (-A^T|I_{v-k})^T$ resulta ser una matriz de comprobación asociada a G, puesto que se trata de una matriz de orden $v \times (v-k)$ con todas sus filas linealmente independientes y verificando por construcción la relación $GH^T = 0$ anteriormente indicada.

Según lo visto hasta ahora, la detección de errores en la transmisión de un mensaje mediante un código lineal se consigue a través de la matriz H del código, pero, ¿cómo se realiza la corrección de los mismos?

Sea C un código de distancia mínima d, de modo que puede corregir hasta $e = \lfloor \frac{d-1}{2} \rfloor$ errores. En ese caso, al enviar la palabra c del código, se recibirá una palabra $w = c + u$, donde u representa la distorsión y, por tanto, ha de tener a lo sumo peso e.

La *decodificación* es el procedimiento que permite recuperar la palabra enviada a partir de la recibida. Se basa en la técnica del vecino más próximo, es decir, en asumir que la palabra enviada es la más próxima a la recibida. Una primera solución al problema de la decodificación podría consistir en la comparación de la palabra recibida con las q^l palabras del código y considerar la más cercana como la palabra enviada; pero cuando el código consta de un elevado número de palabras, el proceso resulta ser muy largo. En el caso de códigos lineales el proceso puede simplificarse considerando vectores del tipo $s = wH^T$, con "s" *síndrome* asociado a w. Teniendo en cuenta que $wH^T = (c+u)H^T = cH^T + uH^T = uH^T$, el síndrome viene unívocamente determinado por la distorsión u; en el sentido de que si u' es otro vector de peso a lo sumo e con $u'H^T = uH^T$, necesariamente ha de ser $u = u'$ (puesto que $u - u'$ no puede ser una palabra de C de peso a lo sumo $2e$, ya que el peso mínimo de C es $2e + 1$). De este modo, conocida una tabla que asocie posibles vectores errores (aquellas palabras de peso a lo sumo e) con sus síndromes correspondientes, se puede recuperar la palabra enviada c mediante la simple operación $c = w - u$, u error que origina el síndrome wH^T.

Más aún, dado un código lineal C cuyas palabras tienen longitud v, cualquier palabra w del espacio Hamming $H(q, v)$ genera una *clase* $[w]$ *módulo* C, que consiste en el conjunto de todas las palabras del espacio Hamming que pueden obtenerse a partir de la suma de w con cualquier palabra del código,

$$w + v \quad \forall v \in C.$$

De manera que si C tiene dimensión k habrá exactamente $2^{(v-k)}$ clases distintas, cada una de ellas formada por 2^k palabras exactamente. Cada una de dichas clases tendrá, por construcción, un único síndrome asociado, de forma que a dos clases distintas les corresponderán síndromes diferentes. Cabe destacar una clase particular, que estaría constituida por el propio código C, que evidentemente, ha de tener asociada el síndrome nulo.

Para recuperar una palabra enviada, c, será necesario restarle a la palabra recibida, w, el error producido en la transmisión, u. Una vez que se conoce el síndrome asociado a la palabra recibida, se sabe que el error producido ha de ser una de las palabras de la clase que tiene asociado el síndrome calculado. Se suele asumir que el error es la palabra de menor peso que se encuentra en dicha clase [2].

[2] En el caso en que haya más de una palabra en la clase con error mínimo, se puede optar por elegir una de ellas al azar o, si es factible, se puede pedir que el mensaje sea retransmitido nuevamente.

Veamos ahora cómo se comportan los códigos lineales con respecto a las cotas de Varshamov-Hilbert y de Hamming que enunciáramos previamente.

Se sabe que si q es una potencia de un primo, existe un código lineal que alcanza la cota de Varshamov-Gilbert (ver [17]).

Por otro lado, sirviéndose de las matrices de comprobación se puede construir códigos lineales perfectos correctores de 1 error, i.e., verificando la cota de Hamming, ya que un código lineal C tiene peso mínimo al menos d si y sólo si cualesquiera $d-1$ columnas de una matriz de comprobación de C son linealmente independientes.

Luego, para que un código lineal sea corrector de 1 error cualesquiera dos columnas de una matriz de comprobación deben ser linealmente independientes.

A modo de ejemplo reseñamos a continuación uno de los códigos lineales más conocidos, destacable por su simplicidad a la hora de codificar y decodificar mensajes, corrigiendo hasta un error (como veremos posteriormente): el *código Hamming*. Para introducirlo, consideremos la relación de equivalencia que define la proporcionalidad sobre el conjunto de vectores columnas no nulos de longitud fija, digamos, l. Como cada clase contiene $q-1$ vectores, y en total hay q^l-1 vectores no nulos, resulta que la relación de proporcionalidad define exactamente $v=\frac{q^l-1}{q-1}$ clases distintas. Así, un *código Hamming* de dimensión $k=v-l$ y palabras de longitud v es aquel cuya matriz de comprobación es una matriz $v\times(v-k)$ constituida por vectores columnas representantes de cada una de las v clases existentes.

Se tiene, por tanto, que los códigos de Hamming son códigos perfectos correctores de 1 error. Más aún, todo código lineal perfecto corrector de 1 error es un código Hamming.

1.1.3 Códigos de Hadamard

Particularizando la cota de Plotkin para códigos binarios no necesariamente lineales, Plotkin mismo demostró en [93] la validez del siguiente resultado.

Sea C un código, formado por palabras de longitud v y distancia mínima dada d, sobre el alfabeto $\mathbb{Z}_2$. Entonces, el número b de palabras que componen el código verifica las cotas siguientes:

1. Si d es par y $v < 2d$, es $b \leq 2\left[\frac{d}{2d-v}\right]$.
2. Si d es par y $v = 2d$, es $b = 2d$.
3. Si d es impar y $v < 2d+1$, es $b \leq 2\left[\frac{d+1}{2d+1-v}\right]$.
4. Si d es impar y $v = 2d+1$, es $b \leq 2v+2$.

MacWilliams y Sloane probaron en [89] que la existencia de códigos óptimos para 1. y 2. implicaba la existencia de códigos óptimos para 3. y 4.

Levenshtein probó en [85] que estas acotaciones eran las más finas posibles, dado que existían códigos óptimos alcanzando dichas cotas, en función de la existencia de *matrices de Hadamard* (matrices ortogonales de entradas ± 1) de determinadas dimensiones. Más concretamente, la existencia de una matriz de Hadamard de dimensión $4t$ implica la existencia de los siguientes códigos binarios óptimos para las cotas de Plotkin[11, 85]:

a) Un código de $8t$ palabras de longitud $4t$ y distancia mínima $2t$.

b) Un código de $4t$ palabras de longitud $4t-1$ y distancia mínima $2t$.

c) Un código de $8t$ palabras de longitud $4t-1$ y distancia mínima $2t-1$.

d) Un código de $2t$ palabras de longitud $4t-2$ y distancia mínima $2t$.

Esta asombrosa relación se explica del siguiente modo. Sea H una matriz de Hadamard de dimensión $4t$, la cual, sin pérdida de generalidad, se puede asumir normalizada (i.e., con la primera fila y columna de unos). Denotemos por $J = (j_{ij})$ a la matriz cuadrada de la misma dimensión formada toda ella por 1 ($h_{ij} = 1\ \forall i, j$). Entonces, las $8t$ filas de las dos matrices $W_{4t}^{(1)} = \frac{1}{2}(J+H)$ y $W_{4t}^{(2)} = \frac{1}{2}(J-H)$ forman un código binario de distancia mínima $2t$, siendo la longitud de cada palabra constante e igual a $4t$.

Para construir los otros códigos, llamemos K a la matriz que se obtiene de H al eliminar su primera columna, y L la matriz que se obtiene al prescindir de la primera columna de la matriz resultante de eliminar de K todas las filas que comienzan por $+1$. Entonces, las $4t$ filas de $W_{4t}^{(3)} = \frac{1}{2}(J+K)$, las $8t$ filas de $W_{4t}^{(3)}$ y $W_{4t}^{(4)} = \frac{1}{2}(J-K)$, y las $2t$ filas de $W_{4t}^{(5)} = \frac{1}{2}(J+L)$ forman los restantes códigos, respectivamente.

Los códigos a) y c) anteriores son óptimos en el sentido de las segunda y cuarta cotas de Plotkin, respectivamente. Los otros dos códigos son casos óptimos particulares de la primera cota, en los que es $v = 2d - 1$ y $v = 2d - 2$, según el caso.

Faltaría probar que para $d \leq v < 2d$, con d par, existe un código óptimo de $b = 2\left[\frac{d}{2d-v}\right]$ palabras de longitud v sobre un alfabeto de $q = 2$ letras y distancia mínima d.

La construcción de un código de estas características pasa por una *suma* apropiada de los códigos anteriores. Esta suma se define del siguiente modo. Sean C_1 y C_2 sendos códigos de b_i palabras, de longitud constante v_i, en el alfabeto $\mathbb{Z}_q$ y de distancias mínimas d_i, con $i = 1, 2$ respectivamente. Consideremos, sin pérdida de generalidad, que $b_2 \geq b_1$. En estas circunstancias, dados dos números naturales, a_1, a_2, se puede generar el *código suma* $C = a_1C_1 \oplus a_2C_2$ cuyas palabras serán de la forma $(c_1^j|\overset{a_1}{\cdots}|c_1^j|c_2^j|\overset{a_2}{\cdots}|c_2^j)$, siendo c_i^j la palabra j-ésima de C_i, para $1 \leq j \leq b_1$. El código C así construido constará, por tanto, de b_1 palabras de longitud constante $a_1v_1 + a_2v_2$ y distancia mínima $d \geq a_1d_1 + a_2d_2$. Queda claro que esta construcción es independiente de las últimas $b_2 - b_1$ palabras de C_2.

Así, sean $r = \left[\frac{d}{2d-n}\right]$, $a_1 = d(2r+1) - v(r+1)$ y $a_2 = rv - d(2r-1)$.

Consideremos el código C definido por:

- Si v es par, $C = \frac{a_1}{2}W_{4r}^{(5)} \oplus \frac{a_2}{2}W_{4(r+1)}^{(5)}$.
- Si v es impar y r es par, $C = a_1W_{2r}^{(3)} \oplus \frac{a_2}{2}W_{4(r+1)}^{(5)}$.
- Si v y r son ambos impares, $C = \frac{a_1}{2}W_{4r}^{(5)} \oplus a_2W_{2(r+1)}^{(3)}$.

El código C así construido es óptimo para la primera cota de Plotkin.

Resumiendo, una condición suficiente para la existencia de códigos binarios óptimos en el sentido de la cota de Plotkin, para v y d dados, es la existencia de matrices de Hadamard de dimensiones $2r$ (r par), $2(r+1)$ (r impar), $4r$ y $4(r+1)$, con $r = \left[\frac{d}{2d-n}\right]$.

De hecho, a partir de matrices de Hadamard se han construido códigos sumamente útiles, incluso para la investigación espacial.

Códigos de Reed-Muller

El código de Reed-Muller de orden r, $RM(r,m)$, viene definido de forma recursiva:

1. $RM(0,m) = \{00\ldots0, 11\ldots1\}$.
2. $RM(r,m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}) : \mathbf{u} \in RM(r,m-1), \mathbf{v} \in RM(r-1,m-1)\}$, $0 \leq r \leq m$.

Así, $RM(m,m)$ contiene todas las posibles palabras de longitud 2^m.

Se puede comprobar que la distancia mínima del código $RM(r,m)$ es $d = 2^{m-r}$; el número de palabras es 2^a, con $a = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{m} = 2^m$; y la longitud de cada palabra es 2^m.

Alguno de estos códigos se puede construir, también, a partir de matrices de Hadamard. De hecho, cualquier código Reed-Muller $RM(1,m)$ se obtiene a partir de una matriz de Hadamard H de orden 2^m construida según el *método de Sylvester*: las palabras de $RM(1,m)$ resultan ser las filas de la matriz que se obtiene de

$$\begin{bmatrix} H \\ -H \end{bmatrix}.$$

al reemplazar las entradas -1 por 0.

En particular, el código de Reed-Muller $RM(1,5)$, de distancia mínima 16 y 64 palabras de longitud 32, puede obtenerse a partir de una matriz de Hadamard de orden 32, mediante el procedimiento anteriormente descrito.

Este código ha sido especialmente útil en la transmisión de fotografías desde sondas espaciales, dado que es muy apropiado para enviar información a través de canales sometidos a muchos ruidos (gracias a su elevada distancia mínima) y tiene un algoritmo de decodificación muy rápido y eficiente.

En 1965 la sonda espacial *Mariner* 4 fue la primera sonda espacial que fotografió otro planeta, realizando 22 fotografías de Marte. Cada una de las fotografías estaba compuesta por 200×200 elementos pictográficos. A cada uno de estos elementos se le asociaba una 6-tupla binaria que representaba el nivel de brillo desde el blanco (000000) hasta el negro (111111). Así, el número total de bits (dígitos binarios)

por fotografía era de 240.000. Los datos eran retransmitidos a razón de $8\frac{1}{3}$ bits por segundo, por lo que requería de 8 horas para enviar cada fotografía.

Más tarde, a finales de los años 60 y principios de los 70, las sondas Mariner 6, 7 y 9, mejoraron las fotografías de Marte por varias razones. En primer lugar, cada fotografía fue descompuesta en 700×832 unidades elementales. Además, el Mariner 9 fue la primera nave puesta en órbita alrededor de Marte, tomando las fotografías de este planeta desde distintos puntos de la órbita. Pero lo fundamental, desde nuestro estudio, es que comenzó a utilizarse un código corrector de errores más potente para enviar la información: el $RM(1,5)$. En lugar de utilizar 6 símbolos para enviar cada unidad elemental de información, este código utiliza 32 (siendo 26 de ellos redundantes). La velocidad de transmisión aumentó a 16.200 bits por segundo.

Códigos de Golay

Otros códigos binarios muy importantes, tanto en la práctica como en el terreno teórico, son los *códigos de Golay*. De entre los códigos de Golay, los más usuales son el G_{23} y el G_{24} (comúnmente conocido como código de Golay *extendido*[3]), que se obtiene del anterior al añadir un dígito de paridad. La matriz generadora de este último es:

$$\left(\begin{array}{c|cccccccccccc|c}
1 & 1 & & & & & & & & & & & & \\
1 & & 1 & & & & & & & & & & & \\
1 & & & 1 & & & & & & & & & & \\
1 & & & & 1 & & & & & & & & & \\
1 & & & & & 1 & & & & & & & & \\
1 & & & & & & 1 & & & & & & & \\
1 & & & & & & & 1 & & & & & & \\
1 & & & & & & & & 1 & & & & & \\
1 & & & & & & & & & 1 & & & & \\
1 & & & & & & & & & & 1 & & & \\
1 & & & & & & & & & & & 1 & & \\
1 & & & & & & & & & & & & 1 & \\
\hline
 & & & & & & & & & & & & & 1
\end{array}\right.
\left|\begin{array}{cccccccccccc}
1 & 1 & & 1 & 1 & 1 & & & & 1 & & \\
 & 1 & 1 & & 1 & 1 & 1 & & & & & 1 \\
1 & & 1 & 1 & & 1 & 1 & 1 & & & & \\
 & 1 & & 1 & 1 & & 1 & 1 & 1 & & & \\
1 & & 1 & & 1 & 1 & & 1 & 1 & 1 & & \\
 & & 1 & & 1 & 1 & & 1 & 1 & 1 & 1 & \\
 & & & 1 & & 1 & 1 & & 1 & 1 & 1 & 1 \\
1 & & & & 1 & & 1 & 1 & & 1 & 1 & \\
1 & 1 & & & & 1 & & 1 & 1 & & & 1 \\
1 & 1 & 1 & & & & 1 & & 1 & 1 & & \\
 & 1 & 1 & 1 & & & & 1 & & 1 & 1 & \\
1 & & 1 & 1 & 1 & & & & 1 & & 1 & 1 \\
\hline
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right)$$

[3]Sobre la *extensión* de códigos consultar [89].

Donde la submatriz 11×11 de la derecha se construye, mediante ciertas transformaciones, a partir de una matriz de Hadamard obtenida según la construcción de Paley de orden 12:

$$M_{12} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - \\ 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 \\ 1 & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - \\ 1 & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - \\ 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 \\ 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 \\ 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - \\ 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 \\ 1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - \end{pmatrix}$$

El código extendido de Golay es un código lineal de distancia mínima $d = 8$, constituido por $2^{12} = 4096$ palabras de longitud 24. Se podría hablar mucho a cerca de este código y sus propiedades, pero no entraremos en detalles para no extendernos en exceso. Sin embargo, es necesario destacar que se trata de un código de elevado número de palabras y con capacidad para corregir hasta 3 errores. Estas características hacen de él un código bueno y único, ya que no existe otro con estos parámetros. De hecho, el código extendido de Golay fue utilizado a principio de la década de los 80 en misiones espaciales del Voyager para enviar fotografías a color de alta resolución de Júpiter y Saturno.

El código de Golay G_{23} se obtiene a partir de una matriz generadora del código G_{24} sin más que eliminar el último símbolo de cada una de las palabras del código. El código G_{23} se caracteriza por tener distancia mínima $d = 7$, y el mismo número de palabras que el anterior, pero cada una de ellas de 23 letras.

1.2 Matrices de Hadamard

Como vimos en la sección anterior, las matrices de Hadamard permiten construir códigos correctores de errores de gran aplicabilidad. Esto induce a buscar matrices

de Hadamard en todos los órdenes posibles, con el fin de construir nuevos códigos a partir de ellas que mejoren los anteriores.

Comenzaremos esta sección recordando qué son las matrices de Hadamard, algunas de sus propiedades, así como problemas abiertos relacionados con estas matrices. Posteriormente, haremos un breve recorrido histórico acerca de los diversos métodos que se han diseñado para su construcción. Nos basaremos en [58], que es la referencia por antonomasia.

Una matriz H cuadrada de orden n con todas sus entradas en $\mathbb{F}_2 = \{1, -1\}$ se dice *matriz de Hadamard de orden n* cuando verifica que $H \cdot H^T = n \cdot I$, i.e., si sus filas (respectivamente, columnas) son ortogonales dos a dos.

Este tipo de matrices da lugar a la denominada *conjetura de Hadamard* (también conocida como conjetura de Paley) que versa sobre la existencia de matrices de Hadamard de dimensión cualquier múltiplo de 4 y que, como otros tantos problemas clásicos en matemáticas, pese a la aparente simpleza de su enunciado, esconde un resultado que permanece desde hace siglos sin demostración o contraejemplo conocidos.

Al contrario que otras conjeturas, en las que si cabe han sido más relevantes las teorías desarrolladas sucesivamente para su resolución que los propios postulados enunciados en las conjeturas mismas (como el Teorema de Fermat o la conjetura de Goldbach, que propiciaron el nacimiento de la teoría algebraica de números), la existencia de matrices de Hadamard en cualquier orden $4t$ es fundamental por sus aplicaciones en muy diversos campos, tales como las teorías de diseños combinatorios (diseños ortogonales, SBIBD, ...), códigos correctores de errores, diseños de pesadas múltiples, cálculo de matrices con determinante máximo, ...

Un problema secundario relacionado con la conjetura de Hadamard, asimismo de gran complejidad, es el de la determinación del número de matrices de Hadamard "esencialmente distintas" que existen para un orden determinado. La *equivalencia Hadamard* de matrices es la noción que se corresponde con esta idea de "diferencia sustancial" entre dos matrices H_1 y H_2, en el sentido de que han de diferir una de otra en el producto de sendas matrices de permutación signadas P_1 y P_2,

$$P_1 H_1 = H_2 P_2;$$

es decir, que se pueden obtener una de otra mediante la permutación y/o negación de filas y/o columnas.

Dada una matriz de Hadamard, se puede negar cada fila cuyo primer elemento sea -1, y así obtener una matriz equivalente cuya primera columna está formada sólo por unos. De forma análoga, la primera fila se puede convertir en una fila toda de unos, negando las columnas que comiencen por -1. Toda matriz de esta forma se dice matriz de Hadamard *normalizada.*

Aunque considerar que las matrices de Hadamard existen en cualquier orden múltiplo de cuatro es una mera conjetura, lo que sí se puede probar de forma sencilla es que, en caso de existir, estas matrices han de tener orden 1, 2 ó 4t. De hecho, salvo equivalencia Hadamard, las matrices de Hadamard de orden 1 y 2 son respectivamente:

$$H_1 = (1) \quad , \quad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Para probar que las matrices de Hadamard de orden $n \geq 3$ son de orden un múltiplo de 4 basta considerar, sin pérdida de generalidad gracias a la equivalencia Hadamard, una matriz de Hadamard cuyas primeras filas sean de la forma:

$$\begin{array}{cccccccccccccccc}
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\
1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & -1 & -1 & \cdots & -1 & -1 & -1 & \cdots & -1 \\
1 & 1 & \cdots & 1 & -1 & -1 & \cdots & -1 & 1 & 1 & \cdots & 1 & -1 & -1 & \cdots & -1 \\
 & & i & & & & j & & & & k & & & & l &
\end{array}$$

Teniendo en cuenta la ortogonalidad de las filas resulta que:

$$i + j - k - l = 0$$

$$i - j + k - l = 0$$

$$i - j - k + l = 0$$

De lo que se deduce que $i = j = k = l$. Por otra parte, como $i+j+k+l = n$, resulta que, efectivamente, es $n = 4i$ un múltiplo de 4.

En definitiva, dada una matriz H de Hadamard de dimensión $n > 2$, entonces, n es par y cualesquiera dos filas distintas de H coinciden en exactamente $n/2$ de sus columnas. Más aún, si $n > 2$, entonces n es múltiplo de 4 y cualesquiera tres filas distintas de H coinciden en exactamente $n/4$ columnas.

Se conocen numerosos métodos para construir matrices de Hadamard, de los cuales veremos algunos más adelante. Con ellos se consigue obtener familias infinitas de matrices de Hadamard, dando lugar a infinitos órdenes (múltiplos de 4) en los que existen estas matrices. Sin embargo, aún hay infinitos órdenes en los que todavía no se conocen matrices de Hadamard. Por otra parte, no se conoce ningún orden divisible por 4 para el que se haya demostrado que no existen matrices de Hadamard. Actualmente (según [26]) el menor orden para el que no se ha conseguido encontrar matrices de Hadamard es $428 = 4 \cdot 107$.

1.2.1 Métodos de construcción

Históricamente, este tipo de matrices fueron ya consideradas por Sylvester [120] en 1867, en relación con un problema sobre teselaciones. A él se atribuye la forma más sencilla de construir matrices de Hadamard, basada en el producto de Kronecker de dos matrices, definido de la siguiente forma:

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{pmatrix}$$

Dado que el producto de Kronecker verifica que $(A \otimes B)(C \otimes D) = AC \otimes BD$, si H_1 y H_2 son matrices de Hadamard de órdenes n_1 y n_2, respectivamente, entonces

$$(H_1 \otimes H_2)(H_1 \otimes H_2)^T = (H_1 \otimes H_2)(H_1^T \otimes H_2^T) = H_1 H_1^T \otimes H_2 H_2^T =$$

$$n_1 I_{n_1} \otimes n_2 I_{n_2} = n_1 n_2 I_{n_1 n_2},$$

por lo que, efectivamente, $H_1 \otimes H_2$ es así mismo una matriz de Hadamard.

Esto permite calcular una familia infinita de matrices de Hadamard mediante el uso reiterado del producto de Kronecker. En particular, partiendo de la matriz de Hadamard de orden 2, se obtiene una matriz de Hadamard de orden 2^n para cualquier entero positivo n. Estas son las llamadas *matrices de Sylvester.*

Sin embargo, las matrices de Hadamard no cobraron entidad propia hasta que el mismo Hadamard encontró la relación entre estas matrices y el problema de hallar la matriz A cuadrada de orden n de entradas reales $|a_{ij}| \leq k$, para un cierto $k > 0$, de

determinante máximo [52]. Hadamard demostró que el determinante de una matriz A como la anteriormente descrita viene acotado en valor absoluto por el número $k^n n^{\frac{1}{2n}}$. Es obvio que para $k = 1$ las matrices de Hadamard alcanzan la cota indicada, dado que

$$(\det(H))^2 = \det(H)\det(H^T) = \det(HH^T) = \det(nI) = n^n.$$

Más aún, demostró que las matrices que llevan su nombre son las únicas que alcanzan esta cota. Evidentemente, para $k \neq 1$, basta tomar $k \cdot H$ para H matriz de Hadamard de orden n.

A parte de los trabajos de Sylvester y Hadamard ya mencionados, entre los más importantes, orientados a la construcción de matrices de Hadamard de orden cualquiera prefijado, cabe destacar el de Scarpis (1898), quien probó que cuando p es un número primo congruente con 3 (módulo 4), entonces existe una matriz de Hadamard de orden $p+1$, mientras que si p es primo congruente con 1(módulo 4), existe una matriz de Hadamard de orden $2(p+1)$.

Más tarde, Paley (1933) generalizó el trabajo de Scarpis, proponiendo una manera de construir infinitas matrices de Hadamard asociadas a cada número primo, una para cada potencia de dicho número. La construcción de las matrices de Paley a partir de un número primo impar p requiere encontrar los llamados *residuos cuadráticos* (o simplemente *residuos*) módulo p^k, esto es, los cuadrados no nulos módulo p^k. En realidad, como $(p^k - a)^2 \equiv (-a)^2 \equiv a^2 \ (mod\, p^k)$, basta considerar los cuadrados de los $\frac{p^k-1}{2}$ primeros números. Los restantes $\frac{p^k-1}{2}$ números módulo p^k son los llamados no-residuos (el cero no se considera residuo ni no-residuo). Las matrices se construyen a partir de la *matriz de Jacobsthal* $Q = (q_{ij})$, que es una matriz $p^k \times p^k$ cuyas entradas son $q_{ij} = \chi(i-j)$, donde χ es la *función de Legendre* definida de la siguiente forma:

- $\chi(i) = 0$, si i es un múltiplo de p^k.
- $\chi(i) = 1$, si i es un residuo módulo p^k.
- $\chi(i) = -1$, si i es un no-residuo módulo p^k.

De este modo, las matrices

$$H_I = \begin{pmatrix} 1 & \mathbf{1} \\ -\mathbf{1^T} & I+Q \end{pmatrix} \quad \text{y} \quad H_{II} = \begin{pmatrix} 0 & \mathbf{1} \\ \mathbf{1^T} & Q \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} + I \otimes \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$$

resultan ser matrices de Hadamard de dimensión $p^k + 1$ y $2(p^k + 1)$, según sea $p^k \equiv 3\ (mod\, 4)$ ó $p^k \equiv 1\ (mod\, 4)$, respectivamente.

Williamson (1944) generalizó el trabajo de Paley y consideró métodos innovadores que le permitieron tanto a él como, más tarde, a Baumert, Golomb y Hall, encontrar matrices de Hadamard para algunos órdenes hasta entonces no estudiados. El método de Williamson consiste en la búsqueda de matrices de Hadamard a partir de matrices por bloques, restringidas a ciertas condiciones con el fin de reducir la complejidad del problema.

Más tarde, Cooper, Wallis y Turyn generalizaron el trabajo de Williamson.

Se han estudiado otros muchos métodos para obtener matrices de Hadamard, por ejemplo Dade y Goldberg (1959) utilizaban permutaciones de grupos para este fin, Bush (1971) trataba de construir estas matrices mediante planos proyectivos finitos, Wallis (1976) utilizó diseños ortogonales, ...

Cabe destacar otro de los numerosos intentos de búsqueda de las matrices de Hadamard, el cual se fundamenta en el estudio de *matrices desarrolladas* sobre un grupo G.

Una matriz M cuadrada de orden v y entradas ± 1 se dice *desarrollada* sobre un grupo finito G de v elementos si proviene de la tabla de multiplicar del grupo G. En el sentido de que dada una ordenación de los elementos de G, existe una aplicación de conjuntos $g : G \to \mathbb{F}_2$, de modo que $M = (g(ab))\ \ \forall a, b \in G^{\bullet}$; i.e., cada fila de la matriz consiste en una cierta permutación de los elementos del conjunto G. Pero, las matrices binarias así construidas se caracterizan por tener el mismo número de entradas positivas y negativas en cada fila, y toda matriz de Hadamard con esta propiedad (matriz de Hadamard *regular*) se caracteriza por tener orden un cuadrado perfecto, $4t^2$ [125]. De hecho, la existencia de una matriz de Hadamard regular de orden $4n$ equivale a la existencia de un diseño simétrico de $4n$ puntos, con $n = m^2$ un cuadrado perfecto [10].

Actualmente, la aproximación que se estima con mayores probabilidades de éxito en la labor de construir matrices de Hadamard de todos los órdenes múltiplos de 4, se basa en la construcción de matrices desarrolladas *cocíclicamente*. Horadam y de Launey en los años 90 fueron pioneros en la búsqueda de *matrices de Hadamard cocíclicas* [26]. Estas matrices se obtienen a partir de 2-cociclos, como veremos más

adelante. Ambos autores han generado gracias a este procedimiento matrices de Hadamard hasta completar todos los órdenes por debajo de 100 y conjeturan que éste método permite generar matrices de Hadamard de cualquier orden $4t$.

Profundizaremos en esta idea posteriormente. Pero antes, veremos que la existencia de ciertos *diseños* permite construir matrices de Hadamard de determinados órdenes y viceversa.

1.3 Diseños

1.3.1 Diseños por bloques

En este apartado, sirviéndonos de [5] y [17], recopilamos algunas cuestiones referentes a diseños por bloques, con el fin de relacionarlos con las matrices de Hadamard.

Dados t, k, v y λ números enteros tales que $0 \leq t \leq v$ y $\lambda > 0$, un $t-(v,k,\lambda)$ *diseño* o simplemente t-diseño de parámetros (v,k,λ), es una terna $(X, \mathcal{B}, \mathcal{I})$, donde X es un conjunto de v puntos, $X = \{p_1, \ldots, p_v\}$; $\mathcal{B}$ es un conjunto de *bloques* $\{B_1, \ldots, B_b\}$, disjunto de X; e $\mathcal{I}$ es una relación $\mathcal{I} \subset X \times \mathcal{B}$; tal que verifica que todo bloque está relacionado con exactamente k puntos, y cualesquiera t puntos dados están relacionados con exactamente λ bloques de forma simultánea.

Especial mención requieren los 2-diseños ($t = 2$), por su estrecha relación con las matrices de Hadamard. En la literatura, los 2-diseños son frecuentemente denominados *BIBD* (del inglés, *balanced incomplete block design*). Un diseño 2-dimensional más genérico en el que los bloques no tienen igual longitud recibe el nombre de *PBD* (del inglés, *pairwise-balanced designs*). Aunque estos diseños son bastante útiles, especialmente en técnicas de construcción recursiva, nosotros nos vamos a restringir a los diseños cuyos bloques tienen el mismo cardinal.

Aquí vamos a considerar sólo diseños en los que cada bloque aparece una sola vez

en la colección $\mathcal{B}$. Así, el número b de bloques de un $t-(v,k,\lambda)$ diseño será:

$$b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}.$$

Basta observar que el número de pares (T,B) distintos formados por un subconjunto T de t elementos de X y un bloque B de $\mathcal{B}$ viene dado, de un lado, por $\binom{v}{t}$ elecciones de T y λ bloques de B para cada una de estas opciones; y, de otro, por b bloques B y $\binom{k}{t}$ t-subconjuntos T para cada uno de estos bloques.

Cuando el número de bloques, b, coincide con el número de puntos, v, se tiene un diseño simétrico, comúnmente conocido como *SBIBD*.

Asumir que $\mathcal{I}$ representa una relación de pertenencia entre puntos y bloques, de modo que cada bloque queda identificado como un subconjunto de X con k elementos (aquellos con los que está relacionado), es una buena representación de la idea formal de diseño, pero ésta es tan solo una situación muy particular, cuando $\mathcal{I}$ es la relación de pertenencia. Sin embargo, este concepto es mucho más amplio, como se pone de manifiesto, por ejemplo, en la construcción de los *diseños complementarios*.

Esta *estructura complementaria* se puede definir dado un t-diseño $(X,\mathcal{B},\mathcal{I})$ de parámetros (v,k,λ) con $v-k \geq t$ en el siguiente sentido: se sustituye la relación $\mathcal{I}$ por su complementaria $\widetilde{\mathcal{I}} = X \times \mathcal{B} \backslash I$, de modo que un punto x está relacionado con un bloque B si $(x,B) \notin \mathcal{I}$. Así, el t-diseño de parámetros (v,k,λ) con $(v-k) \geq t$ conforma un *diseño complementario*, que no es más que un $t-(v,v-k,\widetilde{\lambda})$ diseño $(\widetilde{X},\widetilde{\mathcal{B}})$, con

$$\widetilde{\lambda} = \lambda \frac{\binom{v-k}{t}}{\binom{k}{t}}.$$

A partir de ahora, consideraremos en todo momento este concepto más amplio de relación de "pertenencia", $\mathcal{I}$, entre puntos y bloques, de manera que hablaremos sencillamente de t-diseños $(X,\mathcal{B})$.

Otro tipo de diseño que se obtiene a partir de un t-diseño $(X, \mathcal{B})$ de parámetros (v, k, λ) es el siguiente: dado $s \leq t$, sea S un s-subconjunto de X, $X' = X \backslash S$ y $\mathcal{B}' = \{B \backslash S : S \subseteq B, B \in \mathcal{B}\}$. Entonces, el par $(X', \mathcal{B}')$ constituye un $(t-s)-(v-s, k-s, \lambda)$ diseño, llamado *diseño derivado* de $(X, \mathcal{B})$ con respecto a S.

Todo t-diseño admite una representación matricial, en forma de *matriz de incidencia* $A = (a_{ij})$, para $1 \leq i \leq b$ y $1 \leq j \leq v$, de modo que la entrada a_{ij} es 1 si $p_j \in B_i$ y 0 en otro caso. Está claro que para t-diseños, con $t > 0$, habrá exactamente k entradas no nulas por fila (y un número constante, r, de entradas no nulas por columna). Recíprocamente, toda matriz con esta propiedad da origen de forma natural a un 1-diseño.

La existencia de diseños para toda entrada de enteros es un resultado hasta ahora no demostrado, en gran medida similar a la conjetura de Hadamard. En realidad, 3-diseños, 2-diseños y matrices de Hadamard se encuentran intrínsecamente relacionados.

De hecho, dada una matriz de Hadamard $H = (h_{ij})$ de orden $4n > 4$, que podemos tomar bajo equivalencia Hadamard con su primera fila toda de $+1$, se puede definir los conjuntos $B_i^+ = \{j : h_{ij} = +1\}$ y $B_i^- = \{j : h_{ij} = -1\}$, para $2 \leq i \leq 4n$; que conforman una familia $\mathcal{B}$ de $2(4n-1)$ conjuntos de $2n$ elementos (puesto que cada columna tiene el mismo número de entradas positivas que negativas). Si llamamos $X = \{1, \ldots, 4n\}$, recordando que en toda matriz de Hadamard de orden $4n > 4$ se verifica que cualesquiera tres columnas distintas coinciden en exactamente n filas, entonces se tiene que $(X, \mathcal{B})$ constituye un $3-(4n, 2n, n-1)$ diseño.

Por otra parte, dado un $3-(4n, 2n, n-1)$ diseño, tomando el diseño derivado con respecto a un punto cualquiera de entre los $4n$ de X, se tiene un $2-(4n-1, 2n-1, n-1)$ diseño.

Además, a partir de un $2-(4n-1, 2n-1, n-1)$ diseño, dada su matriz de incidencia A, se puede construir otra matriz H sustituyendo los 0 por -1 y añadiendo una primera fila y primera columna todas de $+1$. Teniendo en cuenta que cualquier fila de A contiene exactamente $2n-1$ entradas positivas, toda fila de H coincidirá en exactamente $2n$ columnas (todas aquellas con entradas positivas) con la primera fila de H. Por otro lado, cualesquiera dos filas de A tienen la entrada 1 común en $n-1$ posiciones, y la 0 en n posiciones (puesto que el complementario del diseño es un

$2-(4n-1, 2n, n)$ diseño). Así, las correspondientes filas de H coinciden exactamente en $2n$ columnas, de donde $HH^T = 4nI$, es decir, la matriz H así construida es una matriz de Hadamard.

De modo que, para $n > 1$, los apartados siguientes son equivalentes:

1. Existe una matriz de Hadamard de dimensión $4n$.
2. Existe un $3-(4n, 2n, n-1)$ diseño.
3. Existe un $2-(4n-1, 2n-1, n-1)$ diseño.

Este tipo de 2-diseños y 3-diseños se denominan *diseños de Hadamard.*

1.3.2 Diseños combinatorios

En el apartado anterior introducíamos un tipo de diseños cuya definición dependía intrínsecamente de bloques. A continuación vamos a trabajar con otro tipo de diseños cuya definición es "más combinatoria", en función de permutaciones sobre un conjunto dado.

Sea v un número natural, S un conjunto finito y Π_F y Π_C sendos grupos de permutaciones sobre S. Un $(v, \Pi_F, \Pi_C, \beta, S)$-diseño consiste en una matriz cuadrada, X, de orden v con entradas en S, de modo que cada par de líneas paralelas (filas o columnas) satisfacen un cierto conjunto de relaciones dado, β, las cuales son invariantes bajo

1. permutación de filas o columnas de X,
2. la aplicación de cualquier permutación $\pi \in \Pi_F$ sobre cualquier fila de X, y
3. la aplicación de cualquier permutación $\pi \in \Pi_C$ sobre cualquier columna de X.

Usualmente, se tiene que $\Pi_F = \Pi_C = \Pi$. En este caso se habla simplemente de (v, Π, β, S)-diseños.

Como ejemplo de este tipo de diseños podemos destacar los $PCD(v, \Lambda)$ (del inglés, *pairwise combinatorial design*), que describimos a continuación.

Para ello, consideremos un subconjunto Λ, no vacío, de matrices $2 \times n$ ($n \geq 1$) con entradas en S. Sea Π_Λ el mayor subgrupo de Π_S (permutaciones de S), de modo que para cualquier matriz $M \in \Lambda$ la matriz que se obtiene al aplicar a la segunda fila de M cualquier permutación de Π_Λ también está en Λ:

$$\pi \in \Pi_\Lambda \Leftrightarrow \forall\, M = \begin{pmatrix} x_1 & \cdots & x_n \\ y_1 & \cdots & y_n \end{pmatrix} \in \Lambda, \qquad \begin{pmatrix} x_1 & \cdots & x_n \\ \pi(y_1) & \cdots & \pi(y_n) \end{pmatrix} \in \Lambda.$$

Bajo estas premisas, un $PCD(v, \Lambda)$ es un $(v, \Pi_\Lambda, \beta, S)$-diseño, donde el conjunto β de relaciones consiste en que cualquier par de líneas paralelas del diseño constituye un elemento de Λ.

Es conveniente observar que esta noción es en cierto modo comparable a la de PBD. El paralelismo entre los dos conceptos proviene del hecho de que un PBD es un diseño en el que cada par de puntos está relacionado con λ bloques, mientras que un PCD es un diseño en el que cada par de líneas paralelas está en Λ.

Cualquier matriz de Hadamard de orden v constituye un ejemplo de $PCD(v, \Lambda)$, en el que

- $S = \mathbb{F}_2 = \{1, -1\}$,
- Λ es el conjunto de matrices $2 \times n$ sobre $\mathbb{F}_2$ con sus dos filas ortogonales,
- $\Pi_\Lambda = \{\pi_{+1}, \pi_{-1}\}$, donde $\pi_{\pm 1}$ es la permutación resultante de multiplicar por ± 1.

Un $SBIBD(v, k, \lambda)$ se puede caracterizar como un PCD de modo que

- $S = \{0, 1\}$,
- Λ es el conjunto de matrices $2 \times n$ con entradas en S tal que cada fila contiene exactamente k unos (y, necesariamente, $v - k$ ceros), y el producto escalar de cada par de filas, siempre que sean distintas, es igual a λ.
- Π_Λ se reduce a la aplicación identidad.

Una propiedad importante de los $(v, \Pi_F, \Pi_C, \beta, S)$-diseños es que admiten ser extendidos a diseños n-dimensionales en determinadas circunstancias, por medio de lo que se dio en llamar *funciones abelianas de extensión.*

Un $(v, \Pi_F, \Pi_C, \beta, S)^n$-diseño ó *diseño n-dimensional propio*, es una matriz n-cúbica de orden v con entradas en S de modo que cualquier sección suya (submatriz 2-dimensional obtenida al fijar $n-2$ de las dimensiones) da lugar, eventualmente traspuesta, a un $(v, \Pi_F, \Pi_C, \beta, S)$-diseño.

Sea una función de conjuntos $f : G \times G \to H$, siendo H un grupo multiplicativo. Se dice que f es una *función de extensión* si

$$f(a,b)f(ab,c) = f(b,c)f(a,bc) \qquad \forall a,b,c \in G. \tag{1.1}$$

Si además verifica

$$f(a_i,b_i)f(a_j,b_j) = f(a_j,b_j)f(a_i,b_i) \qquad \forall a_i,a_j,b_i,b_j \in G,$$

entonces, f es una función *abeliana* de extensión (AEF).

En el caso en que

$$f(1,1) = 1,$$

se dice que f está *normalizada.*

Una matriz M está *desarrollada por una función de extensión sobre un grupo* cuando proviene del desarrollo sobre un grupo y una función de extensión; es decir, $M = (f(a_i,a_j)g(a_ia_j))$, con $f : G \times G \to C$ función de extensión y $g : G \to S$ aplicación de conjuntos (que se suele denominar función de desarrollo sobre G). En lo que sigue, G será un grupo multiplicativo finito de v elementos y C un conjunto finito.

Un (v, Π, β, S)-diseño se dice desarrollado por una función de extensión f cuando viene dado por una matriz desarrollada por una función f de extensión sobre un grupo. Cuando f verifica que $f(a_i,a_j) \in \Pi$ para todo $a_i, a_j \in G$, se dice que f es *apropiada.*

Sea X un (v, Π, β, S)-diseño desarrollado por una función de extensión apropiada $f : G \times G \to S$ tal que $X = (f(a_i,a_j)g(a_ia_j))$. Entonces,

$$[\prod_{i=2}^{v} f(\sum_{j=1}^{i-1} a_i, a_j)](g(\prod_{j=1}^{v} a_j))$$

es un $(v, \Pi, \beta, S)^n$-diseño n-dimensional propio.

Este método de construcción de diseños n-dimensionales a partir de diseños 2-dimensionales no es más que una generalización del ideado por Hammer y Seberry en [56] para extender matrices de Hadamard 2-dimensionales desarrolladas sobre un grupo a matrices de Hadamard n-dimensionales propias.

El problema radica en encontrar y caracterizar funciones de extensión apropiadas para G, C y S dados. La *teoría de desarrollo cocíclico* de diseños elaborada por Horadam y de Launey a mediados de los noventa responde a estas cuestiones.

1.4 Teoría de desarrollo cocíclico de diseños

Las funciones abelianas de extensión definidas en la sección anterior se pueden caracterizar desde el punto de vista (co)homológico. De hecho, tal y como fundamentaran Horadam y de Launey en [24], estas funciones se pueden reinterpretar en términos del primer y segundo grupo de homología.

Sea $(C, +)$ un grupo aditivo abeliano finito y $(G, \bullet)$ un grupo multiplicativo (no necesariamente abeliano) finito de v elementos, ordenados de la siguiente forma $G = \{a_1 = 1, a_2, \ldots, a_v\}$. Por ser C abeliano, cualquier aplicación $f : G \times G \to C$ es una función abeliana de extensión cuando satisface las v^3 ecuaciones

$$f(a,b) + f(ab,c) - f(b,c) - f(a,bc) = 0 \qquad a,b,c \in C,$$

para las v^2 variables $(a,b) \in G \times G$. De aquí que cualquier función abeliana de extensión $f : G \times G \to C$ se pueda interpretar como un homomorfismo de grupos $\phi(f)$ de $U(G) = \mathbb{Z}[G \times G]/R$ en C, siendo R el subgrupo de $Z[G \times G]$ que generan las citadas relaciones,

$$R = < (b,c) - (ab,c) + (a,bc) - (a,b) : \quad a,b,c \in G > .$$

De manera que

$$\begin{array}{rcl} \phi : AEF & \to & \mathrm{Hom}(U(G), C) \\ f & \to & \phi(f), \end{array} \tag{1.2}$$

con

$$\phi(f)(\sum_{a,b) \in G \times G} \lambda_{a,b}[a,b]) = \sum_{(a,b) \in G \times G} \lambda_{a,b} f((a,b)),$$

que está bien definido por ser f una función abeliana de extensión.

Por tanto, para caracterizar completamente al conjunto de funciones abelianas de extensión, que conforma un grupo mediante el producto punto a punto, bastará determinar una presentación de $U(G)$, con varias indeterminadas sujetas a un conjunto minimal de relaciones; el cual se puede obtener a partir de R mediante reducción por filas en los enteros de la matriz $v^3 \times v^2$ correspondiente. Esto sólo es factible en la práctica cuando el orden v del grupo G es pequeño, disparándose la complejidad del proceso en otro caso. En general, se hace necesario buscar aproximaciones alternativas.

Se definen las funciones abelianas de extensión *principales* como aquellas en que

$$f(a,b) = \alpha(a) + \alpha(b) - \alpha(ab),$$

para cierta aplicación de conjuntos $\alpha : G \to C$.

Denotemos por $B(G)$ al subgrupo de $U(G)$ formado por los elementos del tipo

$$\sum_{(a,b)\in G\times G} (\lambda_a + \lambda_b - \lambda_{ab})(a,b),$$

con $\lambda_g \in \mathbb{Z}$ fijo para cada $g \in G$.

El conjunto de homomorfismos $\mathrm{Hom}(B(G), C)$ coincide con el conjunto de las funciones abelianas de extensión principales, de manera que la clase de equivalencia correspondiente a estas funciones abelianas de extensión principales es un subgrupo de las funciones abelianas de extensión.

Un sistema de generadores de $B(G)$ se puede determinar mediante una reducción por filas en $\mathbb{Z}$ de una matriz $v \times v^2$, donde la fila i está asociada a la función característica $\alpha_i : G \to \mathbb{Z}$ que lleva $\alpha_i(a_j) = \delta_{ij}$, con δ la función de Kronecker.

Horadam identificó las funciones abelianas de extensión como 2-cociclos propios de $H^2(G, C)$. Más aún, comprobó que el grupo de las funciones abelianas de extensión principales coincidía con el grupo de los 2-cobordes.

En definitiva, se tiene que

$$\mathrm{Hom}(U(G), C)/\mathrm{Hom}(B(G), C) \cong H^2(G; C).$$

Luego, $\mathrm{Hom}(U(G), C)$ se obtiene como la suma directa $\mathrm{Hom}(B(G), C) \oplus H^2(G; C)$. Por tanto, determinar un sistema de generadores de funciones abelianas de extensión consiste en encontrar un conjunto de 2-cociclos representativos en cohomología y un sistema de generadores de 2-cobordes.

Lamentablemente, la determinación de n-cociclos representativos es un problema abierto hoy día en Álgebra Homológica. No obstante, en este caso basta calcular $H^2(G; C)$ y un sistema generador de 2-cobordes.

Para ello se puede recurrir, como es preceptivo, al *Teorema de Coeficientes Universales* [59], de modo que

$$H^2(G; C) \cong \mathrm{Ext}_{\mathbb{Z}}(H_1(G), C) \oplus \mathrm{Hom}(H_2(G), C),$$

donde $H_1(G) = G/[G, G]$ es el abelianizado de G (asimismo finito por serlo G) y $H_2(G)$ es el segundo grupo de homología de G.

En el capítulo tercero de la memoria abordaremos métodos para calcular lo más eficientemente posible estos dos sumandos en que factoriza $H^2(G; C)$.

1.5 Matrices cocíclicas de Hadamard

Dado que toda función de extensión abeliana se puede interpretar como un 2-cociclo, el concepto de matriz desarrollada por una función de extensión abeliana sobre un grupo visto en el apartado 1.3.2 recibe también el nombre de *matriz cocíclicamente desarrollada* (o más brevemente *matriz cocíclica*).

Así, una matriz binaria cuadrada M de orden v se dice desarrollada cocíclicamente sobre G cuando proviene de la tabla de multiplicar del grupo G y un cociclo f

$$M = [f(a, b)g(ab)] \; \forall a, b, c \in G,$$

siendo $g : G \to \mathbb{F}_2$ una función de desarrollo sobre G.

Por otra parte, si $g \equiv 1$, se dice que M es una matriz *cocíclica pura*.

Horadam y de Launey establecieron una condición necesaria y suficiente para determinar si una matriz cocíclica pura es de Hadamard:

Test de Hadamard cocíclico [26]. Una matriz cocíclica pura es de Hadamard si y sólo si la suma de los elementos de cualquier fila, salvo la primera (de entradas sólo +1), es nula.

Este resultado es inmediato si se hace el producto escalar de dos filas b y d, con $b, d \in G\backslash\{1\}$. Ya que si $a = db^{-1}$ y teniendo en cuenta que en $\mathbb{Z}_2$ todo elemento es su propio inverso, se tiene que

$$\sum_{c\in G} f(b,c)f(d,c) = \sum_{c\in G} f(b,c)f(ab,c) \overset{(1.1)}{=} \sum_{c\in G} f(a,b)f(a,bc) =$$
$$= f(a,b)\sum_{c\in G} f(a,bc) = \pm\sum_{c\in G} f(a,c),$$

lo que da lugar al resultado anterior.

De esta forma, tenemos un algoritmo cuadrático para determinar si una matriz cocíclica pura es o no de Hadamard.

Para averiguar si una matriz cocíclica (no pura) es de Hadamard es necesario recurrir a la relación de *equivalencia Hadamard* recogida en (1.2), según la cual dos matrices binarias son *Hadamard equivalentes* si se puede obtener una de otra mediante permutación de filas (o columnas) o negación de algunas filas (o columnas).

Es fácil demostrar que toda matriz cocíclica es Hadamard equivalente a una matriz cocíclica pura, puesto que

$$M = (f(a,b)g(ab)) \sim_h M^* = (f^*(a,b)),$$

siendo $f^*(a,b) = g(a)^{-1}g(b)^{-1}g(ab)f(a,b)$.

Dado que la relación de equivalencia Hadamard preserva la ortogonalidad entre filas y columnas, el problema de estudiar todas las matrices cocíclicas para comprobar si son de Hadamard se reduce a tener que generar sólo las matrices cocíclicas puras.

Todavía se puede reducir un poco más, puesto que basta con estudiar las matrices cocíclicas puras normalizadas, ya que cambiar el signo no varía el carácter de la matriz (según la equivalencia Hadamard):

$$M(f(a,b)g(ab)) \sim_h M(-f(a,b)g(ab)).$$

Por tanto, en lugar de buscar entre todas las matrices desarrolladas cocíclicamente sobre un grupo G, basta restringir la búsqueda entre las matrices cocíclicas puras

normalizadas. (Nótese que el hecho de que sean matrices cocíclicas puras, hace que sólo dependan de la función cocíclica f y no del grupo G).

Así, para encontrar las matrices cocíclicas de Hadamard, es necesario encontrar un sistema generador de los 2-cociclos normalizados. A partir de él, basta generar todas las matrices cocíclicas normalizadas mediante el *producto Hadamard* (i.e., punto a punto, que notaremos por $\bullet$) de los generadores, para después aplicarles el test de Hadamard.

1.6 Grupos de Hadamard

Las matrices cocíclicas de Hadamard, o equivalentemente, los 2-cociclos ortogonales, están íntimamente ligados a los grupos que Ito [74] ha denominado *grupos de Hadamard.*

Para precisar esta relación, primero hemos de describir de manera detallada la relación existente entre 2-cociclos y *extensiones centrales.*

Una *extensión de grupos* es una sucesión exacta corta

$$1 \rightarrowtail F \overset{i}{\rightarrowtail} E \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$$

con F, E, G grupos no necesariamente abelianos; siendo $i(F)$ un subgrupo normal de E, por lo que $E/i(F) \cong G$.

Una tal extensión *escinde* si existe un inverso $q : G \to E$ de p a derecha, de modo que $p \circ q = 1_G$.

Por otra parte, $1 \rightarrowtail F \overset{i}{\rightarrowtail} E \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$ y $1 \rightarrowtail F \overset{i}{\rightarrowtail} E' \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$ son dos extensiones *equivalentes* cuando existe un isomorfismo $\beta : E \to E'$ haciendo conmutativos los diagramas siguientes

$$\begin{array}{ccccccccc} 1 & \rightarrowtail & F & \overset{i}{\rightarrowtail} & E & \overset{p}{\twoheadrightarrow} & G & \twoheadrightarrow & 1 \\ & & \| & & \downarrow \beta & & \| & & \\ 1 & \rightarrowtail & F & \overset{i'}{\rightarrowtail} & E' & \overset{p'}{\twoheadrightarrow} & G & \twoheadrightarrow & 1 \end{array}$$

Nos vamos a centrar ahora en aquellas extensiones de grupos en las que $F = C$ es abeliano.

Dotar a C de estructura de G-módulo consiste en dar:

- Bien una acción asociativa, distributiva con elemento unidad $\kappa : G \times C \to C$, notando $\kappa(g,c) = g \cdot c$ ó simplemente gc; esto es, de manera que $g(cc') = (gc)(gc')$, $(gg')c = g(g'c)$ y $1 \cdot c = c$, $\forall\, g, g' \in G$, $\forall\, c, c' \in C$.
- Bien un homomorfismo $\varphi : G \to \mathrm{Aut}(C)$, que daría lugar a la acción $\kappa(g,c) = \varphi(g)(c)$.

En particular, todo grupo C adquiere la estructura *trivial* de G-módulo con la acción $\varphi(g) = 1$, $\forall\, g \in G$.

Toda extensión $1 \rightarrowtail C \overset{i}{\rightarrowtail} E \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$ da lugar a una estructura de G-módulo sobre C, del siguiente modo.

La conjugación en E da pie a un homomorfismo $\theta : E \to \mathrm{Aut}(C)$, el cual viene caracterizado por $\theta(e)(c) = i^{-1}(e \cdot i(c) \cdot e^{-1})$. En particular, por ser C abeliano, se tiene que $\theta(i(C)) = 1$, de modo que θ induce un homomorfismo $\varphi : G \cong E/i(C) \to \mathrm{Aut}(C)$, con $\varphi \circ p = \theta$; siendo $\varphi(p(e))(c) = i^{-1}(e \cdot i(c) \cdot e^{-1})$.

Este homomorfismo φ dota a C de estructura de G-módulo, y viene caracterizado por completo por la extensión dada. En verdad, φ informa acerca del modo en que C aparece como subgrupo normal en la extensión.

Un resultado clásico [87] reza que una extensión $1 \rightarrowtail C \overset{i}{\rightarrowtail} E \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$ escinde si y sólo si es equivalente al *producto semidirecto* $1 \rightarrowtail C \overset{i}{\rightarrowtail} C \ltimes_\varphi G \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$, viniendo dada la ley de grupo de $C \ltimes_\varphi G$ por

$$(c,g) \cdot (c',g') = (c(gc'), gg'), \qquad gc = \varphi(g)(c).$$

Una extensión $1 \rightarrowtail C \overset{i}{\rightarrowtail} E \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$ se dice *central* cuando $i(C)$ está en el centro de E, $i(c) \cdot e = e \cdot i(c)$ $\forall\, c \in C, e \in E$.

Existe una biyección entre las extensiones centrales $1 \rightarrowtail C \overset{i}{\rightarrowtail} E \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$ de C por G, salvo equivalencia, y las clases de 2-cohomología de G con coeficientes en C. En esta correspondencia, el producto semidirecto va en el 2-cociclo neutro $f(g,h) = 1$.

Más concretamente, dado un 2-cociclo $f : G \times G \to C$, se puede definir la extensión central $E_f = C_f \rtimes G = \{(c,g) : \ c \in C, g \in G\}$ de modo que $(c,g) \cdot (d,h) =$

$(c \cdot d \cdot f(g,h), gh)$. Este grupo determina la sucesión exacta corta

$$1 \rightarrowtail C \overset{i}{\rightarrowtail} E_f \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$$

con i y p la inclusión y proyección canónicas de C y sobre G, respectivamente; dado que $i(C) = C \times \{1\}$ queda dentro del centro de E_f:

$$(c,1) \cdot (d,h) = (cd \cdot f(1,h), h) = (dc \cdot f(h,1), h) = (d,h) \cdot (c,1),$$

puesto que $cd = dc$ por ser C abeliano y $f(1,h) = f(h,1)$ por ser f 2-cociclo.

Más aún, $R_f = \{1\} \times G$ es un complemento de $i(C)$ en E_f, de modo que $E_f/i(C) \cong R_f$.

Recíprocamente, toda sucesión exacta corta $1 \rightarrowtail C \overset{i}{\rightarrowtail} E \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$ en la que $i(C)$ recae en el centro de C, determina una clase de 2-cociclos en $H^2(G,C)$ del modo siguiente.

Sea $T = \{t_g \in E : \ g \in G\}$ un complemento de $i(C)$ en E, de modo que $E/i(C) \cong < T >$ y $p(t_g) = g$, asumiendo por comodidad que $t_1 = 1$. Entonces, la aplicación $f(g,h) = i^{-1}(t_g t_h t_{gh}^{-1})$ define un 2-cociclo propio de $H^2(G,C)$.

Más aún, la aplicación de $E_f = C \times_f G$ en E dada por $(c,g) \to i(c)t_g$ establece un isomorfismo, el cual lleva R_f sobre T.

Otra elección T' para el complemento T genera un 2-cociclo f' cohomólogo a f, de modo que $f' = f \circ \partial\phi$, con $\phi(g) = (i^{-1}((t'_g)^{-1} t_g)$.

Esta correspondencia permitió demostrar a Flannery en las Proposiciones 3.3 y 3.4 de [42] que una extensión central $E = C_f \rtimes \mathbb{Z}_2$ es un grupo de Hadamard precisamente cuando algún 2-cociclo de la clase de 2-cohomología correspondiente es ortogonal.

Entendemos aquí por 2-cociclo *ortogonal* todo aquel cuya matriz cocíclica asociada sea de Hadamard, y por *grupo de Hadamard* un grupo E de orden $8t$, para $t \geq 1$, que contiene a un subgrupo central $< e^* > \cong \mathbb{Z}_2$; de modo que existe un complemento D de $< e^* >$ en E, con $|D \cap Dx| = 2t$ para todo $x \in E \setminus < e^* >$.

Un tal complemento D recibe el nombre de *subconjunto Hadamard de* E. Se tiene que D es subconjunto de Hadamard de E si y sólo si lo es asimismo Dy (respectivamente, yD) para cualquier $y \in E$; de modo que siempre se puede asumir que en tal caso $1 \in D$.

Hay que destacar que el hecho de que un 2-cociclo f sea ortogonal, no implica de ningún modo que alguno de sus 2-cociclos cohomólogos haya de ser también ortogonal.

Es conveniente recordar que existe un test bastante rápido (de complejidad cuadrática en función del tamaño de la matriz) que decide si una matriz cocíclica normalizada es Hadamard o no: lo será en caso de que todas las filas (respectivamente, columnas) a excepción de la primera tengan el mismo número de entradas positivas que negativas.

Basándose en este test Flannery probó en [42] el siguiente resultado.

Proposición 1.6.1 *[42] Sea E un grupo Hadamard de orden $8t$, $t \geq 1$, con subgrupo central dado $\mathbb{F}_2 \overset{i}{\cong} < e^* >$, y notemos $G = E/ < e^* >$. Si $[f] \in H^2(G, \mathbb{F}_2)$ corresponde a la clase de equivalencia asociada a la extensión $1 \rightarrowtail \mathbb{F}_2 \overset{i}{\rightarrowtail} E \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$, entonces $[f]$ contiene un 2-cociclo ortogonal.*

En efecto, si se fija un complemento $D = \{t_g : g \in G\}$ de $< e^* >$ en E y se construye el 2-cociclo f correspondiente de la extensión central $1 \rightarrowtail \mathbb{F}_2 \overset{i}{\rightarrowtail} E \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$ se tiene que $f(g,h) = 1$ si y sólo si $t_g t_h \in D$, de manera que el número de entradas positivas en la fila g de una matriz asociada a f es $|D \cap t_h^{-1} D| = 2t$, exactamente la mitad.

El recíproco también fue demostrado por Flannery en [42].

Proposición 1.6.2 *[42] Sea G un grupo de orden $4t$, $t \geq 1$, y $f \in H^2(G, \mathbb{Z}_2)$ un 2-cociclo ortogonal. Entonces, la extensión central naturalmente asociada a f, salvo equivalencia, constituye un grupo de Hadamard.*

A partir de la extensión $1 \rightarrowtail \mathbb{F}_2 \overset{i}{\rightarrowtail} E_f \overset{p}{\twoheadrightarrow} G \twoheadrightarrow 1$, basta tomar $e^* = (1, -1)$ y $D = \{(g, 1) : g \in G\}$. Como $(g,1) \cdot (h,u) = (gh, u \cdot f(g,h))$, el número de pares $(g,1)$ en D que hacen $(g,1) \cdot (h,u) \in D$ es $2t$ (precisamente, aquellos elementos u de G que corresponden a las columnas de las $2t$ entradas de la fila g que tienen el mismo signo que u, en la matriz que representa a f). Por tanto, $|D \cap D(h,u)| = 2t$ y E_f constituye un grupo de Hadamard.

Algunas restricciones acerca de existencia de grupos de Hadamard las encontramos en las proposiciones 5, 6 y 7 de [74], que vienen a decir que un grupo de Hadamard que escinda sobre su subgrupo central distinguido ha de tener orden $2m^2$, y que los 2-subgrupos de Sylow de grupos de Hadamard de orden $2^k m$, con $k \geq 3$ y m impar, no pueden ser ni cíclicos ni diédricos.

En realidad, como apuntara Flannery en [42], la primera condición equivale a las bien conocidas de que para que una matriz generada sobre un grupo pueda llegar a ser Hadamard es necesario que el grupo tenga orden un cuadrado perfecto [125]; o que la existencia de una matriz de Hadamard regular de orden $4n$ equivale a la existencia de un diseño simétrico de $4n$ puntos, con $n = m^2$ un cuadrado perfecto [10].

Las otras dos condiciones a veces permiten afinar la búsqueda de matrices cocíclicas de Hadamard sobre grupos dados.

A diferencia del método de construcción que veíamos en 1.2.1 basado en el estudio de matrices desarrolladas sobre un grupo, las matrices cocíclicas de Hadamard pueden tener un orden 4t cualquiera (no necesariamente un cuadrado perfecto). Más aún, Horadam y de Launey conjeturan que con este procedimiento, se pueden obtener matrices de Hadamard de cualquier orden múltiplo de 4.

En el capítulo 3 atacaremos esta cuestión para grupos que sean productos iterados de extensiones centrales y productos semidirectos de grupos abelianos finitos, teniendo siempre presente las obstrucciones acerca del carácter Hadamard a que dan lugar los 2-subgrupos de Sylow de un hipotético grupo de Hadamard.

Para ello, se antoja indispensable realizar un estudio previo de la (co)homología de estos grupos, el cual abordamos en el capítulo que se abre a continuación.

Capítulo 2.

(Co)homología de grupos vía perturbación homológica

Capítulo 2.

(Co)homología de grupos vía perturbación homológica

2.1 Generalidades

La noción de *homología* aparece ligada al nacimiento del *Álgebra Homológica*, a raíz de los trabajos que a lo largo de las primeras cuatro décadas del siglo pasado se desarrollaron en relación con los espacios esféricos [73, 31, 32, 29].

Formalmente, dado un objeto K de una categoría (léase módulo, por ejemplo), graduado en los naturales, y una *diferencial* d para K (esto es, un morfismo de grado menos 1, $d_* : K_* \to K_{*-1}$, verificando $dd = 0$), la homología $H_*(K)$ de K viene dada por los cocientes $\text{Ker } d_*/\text{Im } d_{*+1}$.

Más aún, dado otro objeto C, el objeto $\text{Hom}(K, C)$ dotado de la *codiferencial* $\partial_* : \text{Hom}(K_*, C) \to \text{Hom}(K_{*+1}, C)$, con $\partial_*(f) = fd_{*+1}$, permite definir la *cohomología* $H^*(K, C)$ de K con coeficientes en C mediante los cocientes $\text{Ker } \partial_*/\text{Im } \partial_{*-1}$.

Esta definición es apropiada para módulos, pero no para grupos o álgebras, en general, dado que estos objetos poseen una estructura más rica (leyes internas de grupo y álgebra, respectivamente) que en principio no parecen intervenir en la caracterización anterior.

De hecho, la (co)homología de grupos se define a partir de la homología de *álgebras*, y su cálculo se remite al establecimiento de *resoluciones* apropiadas [87].

Más concretamente, sea A un *álgebra diferencial graduada aumentada* sobre un anillo Λ con $1 \neq 0$ (brevemente, DGA-álgebra), que no es más que un DG-módulo

dotado de un producto asociativo con unidad $*_A : A \otimes A \to A$, y una aumentación $\xi : A_0 \to \Lambda$, ambos compatibles con la diferencial (en tanto en cuanto $d\xi = 0$ y $d*_A = *_A(d \otimes 1 + 1 \otimes d)$). Con normalidad, se utilizará $a *_A b$ para $*_A(a \otimes b)$.

Hemos de hacer notar que el anillo base Λ adquiere la estructura de A-módulo a izquierda mediante el *pullback* de la aumentación ξ, de modo que $a *_A \lambda = \xi(a) \cdot \lambda$.

Por otra parte, una *resolución* $\epsilon : (X, d) \to A$ de A es una sucesión exacta del tipo

$$\cdots X_2 \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{\epsilon} A \to 0.$$

El objeto $(\bar{X}, \bar{d}) = (X \otimes_A \Lambda, d \otimes_A 1_\Lambda)$ se denomina *complejo reducido* de la resolución. Recordemos que el producto tensorial de A-módulos, $B \otimes_A C$, sobre la DGA-álgebra A viene dado por el conúcleo del homomorfismo $p : B \otimes A \otimes C \to B \otimes C$ con

$$p(b \otimes a \otimes c) = (b *_A a) \otimes c - b \otimes (a *_A c).$$

En estas circunstancias, la homología de A se define como la homología de $X \otimes_A \Lambda$, para cualquier resolución X de A. Análogamente, la cohomología de A se define como la cohomología de $\mathrm{Hom}_A(X, \Lambda)$, para cualquier resolución X de A.

En el caso de un grupo G, la (co)homología viene dada por la (co)homología correspondiente del álgebra libre sobre Λ de base el grupo, $\Lambda[G]$.

Debemos hacer hincapié en el hecho de que las resoluciones, en su mayor parte, admiten ser comparadas (ver [87, 126] para varios teoremas clásicos de comparación de resoluciones), y factorizadas (según un patrón recursivo [78, 79, 80]) en función de la *resolución bar*. Más aún, en [1] se demuestra que existe una factorización equivalente a nivel de los complejos reducidos de las resoluciones, en la que la *construcción bar* desempeña un papel fundamental.

Notemos por $\bar{A}$ al $\mathrm{Ker}\,\xi_A$, que coincidirá con el cociente A/Λ en caso de ser A conexa (i.e., $A_0 = \Lambda$).

La construcción bar (normalizada) de A, $\bar{B}(A)$, se define como el DG-módulo tensorial suspendido $T(S(\bar{A})) = \bigoplus_{n \geq 0}(S(\bar{A}) \otimes \overset{n}{\cdots} \otimes S(\bar{A}))$, cuya diferencial total $d_{\bar{B}}$ es suma de las diferenciales simplicial

$$d_s([a_1|\cdots|a_n]) = \sum_{i=1}^{n-1}(-1)^{e_i}[a_1|\cdots|a_i *_A a_{i+1}|\cdots|a_n],$$

y tensorial

$$d_t([a_1|\cdots|a_n]) = -\sum_{i=1}^{n}(-1)^{e_{i-1}}[a_1|\cdots|a_{i-1}|da_i|a_{i+1}|\cdots|a_n],$$

donde $e_i = i + |a_1| + \cdots + |a_i|$ y $[a_1|\cdots|a_n] = S(a_1)\otimes\cdots\otimes S(a_n)$.

La aumentación $\xi_{\bar{B}} : \bar{B}(A) \to \Lambda$ viene dada por

$$\xi_{\bar{B}}(\lambda) = \lambda, \quad \lambda \in \Lambda; \qquad \xi_{\bar{B}}(u) = 0, \quad |u|_{\bar{B}} > 0.$$

Debemos recalcar que en el caso A no conexo, en grado 0 aparecen elementos que no son escalares y, aún así, pueden no estar en $\operatorname{Ker}\xi_A$. Si a es uno de estos elementos, está claro que $a \notin \operatorname{Ker}\xi_A$, pero en cambio $a - \xi_A(a) \in \operatorname{Ker}\xi_A = \bar{A}$.

Esta factorización de hecho define un isomorfismo entre las dos definiciones posibles de $\bar{B}(A)$; la anterior, $(T(S(\operatorname{Ker}\xi_A)), d_{\bar{B}})$; y el cociente $(T(S(A))/s(T(S(A))), d_{\bar{B}})$, en el que se identifica a 0 cualquier tupla que contenga alguna entrada escalar.

En el sentido $T(S(\operatorname{Ker}\ \xi_A)) \to T(S(A))/s(T(S(A)))$ es la simple inclusión, dado que los escalares no están en $\operatorname{Ker}\ \xi_A$.

La aplicación inversa asocia a cada $[a_1|\cdots|a_n]$, $[a_1 - \xi_A(a_1)|\cdots|a_n - \xi_A(a_n)]$. Esta aplicación está bien definida, porque $a_i - \xi_A(a_i) \in \operatorname{Ker}\ \xi_A$ para todo $1 \leq i \leq n$.

Generalmente se suele utilizar la primera de las caracterizaciones, aunque en el caso de álgebras libres $\Lambda[G]$ sobre grupos G nosotros tendremos que recurrir a la segunda, mediante el isomorfismo anterior.

Ahora, podemos caracterizar la resolución bar de A, $B(A)$, como el *producto tensorial torcido* $A \otimes_\theta \bar{B}(A)$ inducido por la *cocadena de torsión* $\theta : \bar{B}(A) \to A$, llamada *universal*, que actúa de manera no trivial únicamente sobre los elementos de dimensión simplicial uno,

$$\theta([a_1|\cdots|a_n]) = \begin{cases} a_1, & \text{si } n = 1, \\ 0, & \text{si } n \neq 1. \end{cases}$$

Así, la diferencial $d_{B(A)}$ queda definida como

$$d_B(a\otimes[a_1|\cdots|a_n]) = da\otimes[a_1|\cdots|a_n]+(-1)^{|a|}a\otimes d_{\bar{B}}([a_1|\cdots|a_n])+(a*_A a_1)[a_2|\cdots|a_n].$$

De este modo, la homología del álgebra A quedaría

$$H_*(A) = H_*((A \otimes_\theta \bar{B}(A)) \otimes_A \Lambda) = H_*(\bar{B}(A)),$$

dado que:

- De un lado, $(A \otimes \bar{B}(A)) \otimes_A \Lambda \cong \bar{B}(A)$ a nivel de módulos, puesto que el factor A es "absorbido" por el factor Λ, por definición de la operación $\otimes_A$ y la estructura de A-módulo de Λ.
- De otro, la diferencial de $(A \otimes_\theta \bar{B}(A)) \otimes_A \Lambda)$ es $d = d_B \otimes_A 1_\Lambda$; por tanto,

$$d = (d_A \otimes 1) \otimes_A 1 + (1 \otimes d_{\bar{B}}) \otimes_A 1 + [(1 *_A \theta \otimes 1)(1 \otimes \Delta)] \otimes_A 1 =$$

$$= (1 \otimes d_{\bar{B}}) \otimes_A 1 \cong d_{\bar{B}},$$

puesto que la estructura de A-módulo de Λ hace que los sumandos $(d_A \otimes 1) \otimes_A 1$ y $[(1 *_A \theta \otimes 1)(1 \otimes \Delta)] \otimes_A 1$ sean nulos ($\xi d = 0$ e $\operatorname{Im}\theta \subseteq \operatorname{Ker}\xi$).

Por su parte, la cohomología del álgebra A quedaría

$$H^*(A) = H^*(\operatorname{Hom}_A(A \otimes_\theta \bar{B}(A), \Lambda)) = H^*(\operatorname{Hom}_\Lambda(\bar{B}(A), \Lambda)),$$

dado que $\operatorname{Hom}_A(A \otimes_\theta \bar{B}(A), \Lambda) \cong \operatorname{Hom}_\Lambda(\bar{B}(A), \Lambda)$:

- De un lado, las aplicaciones A-lineales de $A \otimes \bar{B}(A)$ en Λ vienen dadas por las Λ-lineales de $\bar{B}(A)$ en Λ, teniendo en cuenta la estructura de A-módulo de Λ.
- De otro, dada $f : A \otimes_\theta \bar{B}(A) \to \Lambda$ A-lineal, resulta que $\partial f = f d_B \cong \bar{f} d_{\bar{B}}$, con $\bar{f} = f \otimes_A 1$.

En conclusión, dado un grupo G, resulta que $H_*(G) = H_*(\Lambda[G]) = H_*(\bar{B}(\Lambda[G]))$ y $H^*(G) = H^*(\Lambda[G]) = H^*(\operatorname{Hom}(\bar{B}(\Lambda[G]), \Lambda))$.

Nuestro interés se centra en la (co)homología **entera** de grupos finitos, i.e., el caso $\Lambda = \mathbb{Z}$. En adelante, para denotar el anillo base, utilizaremos Λ para resultados sobre DGA-álgebras en general y escribiremos tácitamente $\mathbb{Z}$ en el caso de grupos.

Para calcular explícitamente la (co)homología de un grupo G, grado a grado, se suele hacer uso del *algoritmo de Veblen* [123], que describimos a continuación. Hemos

de hacer notar que, aunque vamos a describir este procedimiento tomando como partida la construcción bar del grupo, es igualmente válido para cualquier *modelo homológico*[1] del grupo que consista en un DG-módulo libre de tipo finito (i.e. finito en cada grado).

Según acabamos de ver, $H_p(G) = H_p(\bar{B}(\mathbb{Z}[G])) = \text{Ker } d_p/\text{Im } d_{p+1}$, donde d_p representa la diferencial propia de la construcción Bar, $d_p : \bar{B}_p(\mathbb{Z}[G]) \to \bar{B}_{p+1}(\mathbb{Z}[G])$.

El primer paso consiste en descomponer $\bar{B}_p(\mathbb{Z}[G])$ en tres sumandos

$$\bar{B}_p(\mathbb{Z}[G]) = U_p \oplus V_p \oplus W_p,$$

de manera que

$$d_p(U_p) \subseteq W_{p-1} \qquad \text{y} \qquad d_p(V_p) = d_p(W_p) = 0;$$

es decir, que $V_p \oplus W_p = \text{Ker}\, d_p$, mientras que $W_p \supseteq \text{Im } d_{p+1} = d_{p+1}(U_{p+1})$.

Dado que $\text{Im } d_{p+1} \subseteq W_p \subseteq \text{Ker } d_p$ se tiene que

$$H_p(\bar{B}(\mathbb{Z}[G])) = \text{Ker } d_p/\text{Im } d_{p+1} = \frac{\text{Ker } d_p}{W_p} \oplus \frac{W_p}{\text{Im } d_{p+1}} = \frac{V_p \oplus W_p}{W_p} \oplus \frac{W_p}{\text{Im } d_{p+1}},$$

de forma que el primer sumando corresponde a la parte libre de $H_p(G)$ y el segundo a la parte de torsión.

Considerando $\beta = \{\mathbf{e_1}, \ldots, \mathbf{e_n}\}$ y $\beta' = \{\mathbf{e'_1}, \ldots, \mathbf{e'_m}\}$, sendas bases de $\bar{B}_p(\mathbb{Z}[G])$ y $\bar{B}_{p-1}(\mathbb{Z}[G])$, se puede construir la matriz de la diferencial de grado p

$$M_p(d) = \begin{pmatrix} d(\mathbf{e_1}) \\ \vdots \\ d(\mathbf{e_n}) \end{pmatrix}_{n \times m}$$

Utilizando la *forma normal de Smith* se puede transformar la matriz anterior en una matriz diagonal

$$D_p = \left(\begin{array}{ccc|c} b_1 & & & \\ & \ddots & & 0 \\ & & b_l & \\ \hline & 0 & & 0 \end{array}\right)_{n \times m}$$

[1] A precisar posteriormente.

donde $1 \leq b_1|b_2|\cdots|b_l$.

De manera que $D_p = P \cdot M_p(d) \cdot Q$, siendo P y Q las matrices de paso

$$\begin{array}{ccc} \beta & \xrightarrow{M_p(d)} & \beta' \\ {\scriptstyle P}\uparrow & \# & \downarrow{\scriptstyle Q} \\ \bar{\beta} & \xrightarrow{D_p} & \bar{\beta}' \end{array}$$

Así:

- W_{p-1} está generado por el conjunto de los l primeros vectores de β', $\{\mathbf{e'_1}, \ldots, \mathbf{e'_l}\}$.
- $\operatorname{Im} d_p$ viene generado por $\{b_1\mathbf{e'_1}, \ldots, b_l\mathbf{e'_l}\}$.
- $\operatorname{Ker} d_p$ está generado por $\{\mathbf{e_{l+1}}, \ldots, \mathbf{e_n}\}$.

Como el cálculo de la homología en grado p requiere conocer $\operatorname{Ker} d_p$, $\operatorname{Im} d_{p+1}$ y W_p, será necesario, en general, calcular las matrices diagonales D_p y D_{p+1}.

Si $s = n - l$ es el número de generadores de $\operatorname{Ker} d_p$ y r la dimensión de la $\operatorname{Im} d_{p+1}$, la homología en grado p de $\bar{B}(\mathbb{Z}[G])$ será $H_p(\bar{B}(\mathbb{Z}[G])) = \mathbb{Z}^{s-r} \oplus \mathbb{Z}_{b_1} \oplus \cdots \oplus \mathbb{Z}_{b_r}$. Donde $\mathbb{Z}^{s-r}$ corresponde a la parte libre y $\mathbb{Z}_{b_1} \oplus \cdots \oplus \mathbb{Z}_{b_r}$ a la parte de torsión.

El procedimiento anterior puede dualizarse para calcular la cohomología de un grupo G en grado p:

$$H^p(G) = H^p(\operatorname{Hom}(\bar{B}(\mathbb{Z}[G]), \mathbb{Z})) = \operatorname{Ker} \partial_p / \operatorname{Im} \partial_{p-1},$$

siendo ∂_p la codiferencial $\partial_p : \operatorname{Hom}(\bar{B}(\mathbb{Z}[G]), \mathbb{Z})_p \to \operatorname{Hom}(\bar{B}(\mathbb{Z}[G]), \mathbb{Z})_{p+1}$.

Al igual que hiciéramos antes con $\bar{B}_p(\mathbb{Z}[G])$, descomponemos ahora $\operatorname{Hom}(\bar{B}(\mathbb{Z}[G]), \mathbb{Z})_p$ en la forma:

$$\operatorname{Hom}(\bar{B}(\mathbb{Z}[G]), \mathbb{Z})_p = U_p \oplus V_p \oplus W_p,$$

de modo que

$$\partial_p(U_p) \subseteq W_{p+1} \qquad \partial_p(V_p) = \partial_p(W_p) = 0.$$

Consecuentemente,

$$H^p(\mathrm{Hom}(\bar{B}(\mathbb{Z}[G]),\mathbb{Z})) = \mathrm{Ker}\ \partial_p/\mathrm{Im}\ \partial_{p-1} = \frac{V_p \oplus W_p}{\mathrm{Im}\ \partial_{p-1}} =$$

$$= \frac{V_p \oplus W_p}{W_p} \oplus \frac{W_p}{\mathrm{Im}\ \partial_{p-1}} = V_p \oplus \frac{W_p}{\mathrm{Im}\ \partial_{p-1}}.$$

Así, considerando $\beta = \{\mathbf{e_1}, \ldots, \mathbf{e_m}\}$, $\beta' = \{\mathbf{e'_1}, \ldots, \mathbf{e'_n}\}$ y $\beta'' = \{\mathbf{e''_1}, \ldots, \mathbf{e''_q}\}$, sendas bases de $\mathrm{Hom}(\bar{B}(\mathbb{Z}[G]),\mathbb{Z})_{p-1}$, $\mathrm{Hom}(\bar{B}(\mathbb{Z}[G]),\mathbb{Z})_p$ y $\mathrm{Hom}(\bar{B}(\mathbb{Z}[G]),\mathbb{Z})_{p+1}$, respectivamente; para determinar W_p se calcula la forma normal de Smith de la matriz de la codiferencial de grado $p-1$:

$$M(\partial_{p-1}) = \left(\begin{array}{ccc|c} c_1 & & & \\ & \ddots & & 0 \\ & & c_k & \\ \hline & 0 & & 0 \end{array}\right)_{q\times n}$$

Análogamente, para determinar V_p se requiere la forma normal de Smith de la matriz

$$M(\partial_p) = \left(\begin{array}{ccc|c} b_1 & & & \\ & \ddots & & 0 \\ & & b_l & \\ \hline & 0 & & 0 \end{array}\right)_{n\times m}$$

siendo la dimensión de V_p igual a $n-l-k$.

Por tanto, $H^p(\bar{B}(\mathbb{Z}[G])) = \mathbb{Z}^{n-l-k} \oplus \mathbb{Z}_{c_1} \oplus \cdots \oplus \mathbb{Z}_{c_k}$.

En definitiva, el algoritmo de Veblen permite determinar la (co)homología de un grupo grado a grado, con sólo calcular las formas normales de Smith de las (co)diferenciales implicadas. Lamentablemente, el tamaño de estas matrices crece ostensiblemente según el orden del grupo, y exponencialmente con la dimensión: si $|G| = r$, $\bar{B}_p(\mathbb{Z}[G])$ posee $(r-1)^p$ generadores, de donde $M(d_p)$ es una matriz de tamaño $(r-1)^p \times (r-1)^{p-1}$.

Las *contracciones* de DG-módulos se revelan como una útil herramienta a la hora de simplificar el problema del cálculo explícito de la (co)homología de grupos; dado que permiten reducir el estudio de la (co)homología de un grupo G al estudio análogo

sobre un *modelo homológico*, es decir, de otro grupo con un número menor y finito de generadores en cada grado, pero con igual (co)homología.

Más concretamente, una contracción de DGA-módulos, $C : \{N, M, f, g, \phi\}$, consiste en una *equivalencia de homotopía* particular entre dos DG-módulos N y M,

$$fg = 1_M,\ 1_N - gf = \phi d + d\phi;$$

verificando ciertas propiedades adicionales:

$$f\phi = 0,$$

$$\phi g = 0,$$

$$\phi\phi = 0.$$

En ocasiones notaremos una contracción simplemente por $N \overset{c}{\Rightarrow} M$.

El morfismo f es suprayectivo, mientras que g es inyectivo, por lo que se suelen denominar *proyección* e *inyección* de la contracción, respectivamente. Por el mismo motivo, N se conoce como *DG-módulo mayor* y M como *DG-módulo menor.*

De modo que, una contracción hace posible descomponer N (que en nuestro caso será $\bar{B}(\mathbb{Z}[G])$), como suma directa de M (que en nuestro caso denotaremos por hG), y un DGA-módulo acíclico (i.e., de homología nula); siendo, por tanto, las homologías de N (léase, $\bar{B}(\mathbb{Z}[G])$) y M (léase, hG) idénticas. Así, una contracción permite obtener un DGA-módulo finitamente generado con la misma homología que el DG-módulo original, pero con un número menor de generadores, en general. En el caso de que, además, el número de generadores que presenta hG en cada grado sea finito, se ha determinado un *modelo homológico* para N.

A veces la búsqueda de un modelo homológico requiere llevar a cabo ciertas modificaciones en las estructuras de una contracción conocida, pero de manera que se mantengan sus propiedades esenciales. En lo que respecta a la modificación de estructuras diferenciales, esto se traduce en introducir *perturbaciones.*

Una *perturbación* de un DGA-módulo N consiste en un morfismo de módulos graduados $\delta : N \to N$ de grado -1, de modo que $(d_n + \delta)^2 = 0$ y $\xi_N \delta = 0$. Es decir, una perturbación δ de un DGA- módulo N verifica que $|\delta| = -1$, $d_N\delta + \delta d_N + \delta^2 = 0$ y que la aumentación $\xi_N : (N, d_N + \delta) \to \Lambda$ sigue siendo un morfismo de DG-módulos.

Una *perturbación* o *dato de perturbación* de una contracción $c : \{N, M, f, g, \phi\}$ es una perturbación δ del DGA-módulo N que verifica que la composición $\phi\delta$ es puntualmente nilpotente, es decir, para todo elemento no nulo $x \in N$ existe un entero positivo n (dependiendo de x, en general), de modo que $(\phi\delta)^n(x) = 0$.

Recogemos a continuación un resultado fundamental en la teoría de perturbación.

Teorema 2.1.1 (Lema Básico de Perturbación) *[13, 111].*
Sean $c : \{N, M, f, g, \phi\}$ una contracción y $\delta : N \to N$ una perturbación de dicha contracción. Entonces, queda definida una nueva contracción,

$$c_\delta : \{(N, d_N + \delta, \xi_N, \eta_N),\ (M, d_M + d_\delta, \xi_M, \eta_M),\ \ f_\delta,\ g_\delta,\ \phi_\delta\},$$

siendo:

$$\begin{aligned} d_\delta &= f\,\delta\,(1+\phi\delta)^{-1}\,g, \\ f_\delta &= f\,(1-\delta\,(1+\phi\delta)^{-1}\,\phi), \\ g_\delta &= (1+\phi\delta)^{-1}\,g, \\ \phi_\delta &= (1+\phi\delta)^{-1}\,\phi; \end{aligned}$$

$$\text{con} \quad (1+\phi\delta)^{-1} = \sum_{i\geq 0}(-1)^i\,(\phi\,\delta)^i = 1 - \phi\,\delta + \phi\,\delta\,\phi\,\delta - \cdots + (-1)^i(\phi\,\delta)^i + \cdots.$$

Es evidente que, debido a la nilpotencia puntual de $\phi\delta$, la suma $(1+\phi\delta)^{-1}(x)$ es finita, para cada $x \in N$. Por otra parte, resulta obvio que el morfismo d_δ constituye una perturbación del DGA-módulo (M, d_M, ξ_M, η_M).

Este resultado se puede extender hasta contemplar las más ricas estructuras de (co)álgebras, dando lugar a distintas versiones, dependiendo del grado de compatibilidad de los morfismos de la contracción con respecto a las estructuras subyacentes (ver [48, 72, 98]).

En el plano de la cohomología se tienen las mismas herramientas. De manera que, dada una contracción $\bar{B}(\mathbb{Z}[G]) \Rightarrow hG$, se puede aplicar el funtor Hom (que preserva contracciones), dando lugar a una nueva contracción

$$\mathrm{Hom}(\bar{B}(\mathbb{Z}[G], \mathbb{Z}) \Rightarrow \mathrm{Hom}(hG, \mathbb{Z}).$$

Así se puede obtener un *modelo cohomológico*, $\mathrm{Hom}(hG, \mathbb{Z})$, para el grupo G.

Explícitamente, dada una contracción

$$c : \{N, M, f, g, \phi\},$$

al aplicar el funtor Hom se obtiene la contracción

$$c^* : \{N^*, M^*, g^*, f^*, \phi^*\},$$

donde seguimos las notaciones de $h^* = \mathrm{Hom}(h, \Lambda)$ y $L^* = \mathrm{Hom}(L, \Lambda)$, usuales en el Álgebra Lineal.

No obstante, el problema del cálculo de la (co)homología conlleva, aún así, un elevado coste computacional; el cual se puede tratar de reducir mediante el estudio de estructuras algebraicas subyacentes en la contracción dada, y la eventual aplicación de resultados específicos para objetos con estructura algebraica enriquecida. Sobre esta idea volveremos en la sección 6 del presente capítulo.

En las secciones que siguen fijaremos $\Lambda = \mathbb{Z}$, pues en ellas trataremos la (co)homología entera de ciertos grupos finitos.

La determinación de la (co)homología de grupos es un problema clásico dentro del Álgebra Homológica. Desde sus albores, han sido muchos los matemáticos que han tratado de hallar versiones explícitas más o menos satisfactorias de los anillos de (co)homología para diversas familias de grupos.

Fueron Eilenberg y Mac Lane los primeros que, centrados en la caracterización de la (co)homología de los espacios $K(\Pi, n)$ [34, 35] (posteriormente en su nombre llamados *espacios de Eilenberg-Mac Lane*, que satisfacen que sus anillos de (co)homología $H(\Pi, n)$ son, precisamente, los de cualquier espacio X conexo por caminos de grupos de homotopía $\pi_n(X) = \Pi$ y $\pi_i(X) = 0$ para $i \neq n$), se adentraron en el estudio de la (co)homología de grupos abelianos finitamente generados. Esta serie de trabajos constituye un verdadero pilar en el Álgebra Homológica, y de hecho, son objeto de frecuente consulta, dada la cantidad de herramientas y procederes que en ellos se describen. Entrelazando esta información ambos autores diseñaron una maquinaria para caracterizar la (co)homología de grupos abelianos, que abordaremos nosotros en la próxima sección, con ciertos matices.

En una línea similar, Huebschmann describe en [70] un modelo cohomológico para

grupos abelianos finitamente generados, que también depende de una presentación inicial del grupo en cuestión. Aún ahora, no sabemos de ninguna descripción de la (co)homología de un grupo abeliano que no necesite de una presentación del grupo. Resultados en esta línea sí se han alcanzado en lo que toca a homología de grupos abelianos [22, 57].

En cuanto a la determinación de la (co)homología de otras familias de grupos, han sido generosamente trabajados grupos nilpotentes [77, 68, 69] (en particular, libres de torsión), grupos metacíclicos [71], fibrados en general [50, 83], p-grupos [79, 45], etc. Nuestro interés se centrará en el estudio de la (co)homología de productos iterados de extensiones centrales y productos semidirectos de grupos abelianos finitos; la cual vendrá dada en función de la (co)homología de los grupos factores correspondientes.

2.2 (Co)homología de grupos abelianos

2.2.1 Modelo homológico

Cualquier grupo abeliano G, como es bien conocido, admite una descomposición primaria en la forma

$$G = \mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{r_t}},$$

con $2 \leq p_1 \leq \cdots \leq p_t$ primos.

La (co)homología de los grupos fundamentales $\mathbb{Z}$ y $\mathbb{Z}_n$ fue tratada ya a mediados del siglo pasado. En particular, Eilenberg y Mac Lane dieron en [35] sendos *modelos homológicos* para estos grupos, en función de álgebras *exteriores* y *polinomiales modificadas*.

En primer lugar, veamos la contracción que permite determinar la homología de $\mathbb{Z}$ a partir la de la homología de un *álgebra exterior*. Recuérdese que un álgebra exterior $E(u, 2n+1)$, con $n \geq 0$, consiste en una DGA-álgebra libre con generadores 1 y u; siendo u de grado $2n+1$ y verificando que $u \cdot u = 0$. Su diferencial es nula y la aumentación y coaumentación vienen dadas por la identidad en el anillo base.

La contracción en cuestión es:

$$C_{\mathbb{Z}} : \{\bar{B}(\mathbb{Z}[\mathbb{Z}]),\ E(u,1),\ f_{\mathbb{Z}},\ g_{\mathbb{Z}},\ \phi_{\mathbb{Z}}\}; \tag{2.1}$$

donde los morfismos de la contracción son la "proyección"

$$f_{\mathbb{Z}}([\bar{n}_1|\cdots|\bar{n}_q]) = \begin{cases} n_1\, u, & \text{si } q = 1; \\ 0, & \text{si } q > 1; \end{cases}$$

la "inyección" dada por

$$g_{\mathbb{Z}}(u) = [\bar{1}];$$

y el operador de homotopía dado por

$$\phi_{\mathbb{Z}}([\bar{n}_1|\cdots|\bar{n}_k]) = \begin{cases} -\sum_{i=1}^{n_1-1} [\bar{1}|\bar{i}|\bar{n}_2|\cdots|\bar{n}_k], & \text{si } n_1 > 1; \\ 0, & \text{si } n_1 = 1; \\ \sum_{i=1}^{|n_1|} [\bar{1}|\overline{-i}|\bar{n}_2|\cdots|\bar{n}_k], & \text{si } n_1 < 1. \end{cases}$$

Además, en esta contracción, la diferencial sobre el modelo homológico $E(u,1)$ es nula, de donde constituye exactamente la propia homología de $\mathbb{Z}$: $H(\mathbb{Z}) = E(u,1)$.

No obstante, nosotros no utilizaremos exactamente la contracción anterior: consideraremos un operador de homotopía alternativo, que procede de la *comparación canónica* de la resolución a que da lugar la contracción previa con la *resolución bar* (ver [1] para mayor detalle). Este punto es crucial para que los argumentos sobre filtraciones que están por venir puedan extrapolarse también al caso de grupos abelianos no necesariamente finitos (aunque no hemos de olvidar que nuestro interés reside exclusivamente en grupos finitos, para la búsqueda de matrices cocíclicas de Hadamard a que dan lugar). Una fórmula explícita para este operador de homotopía (que notaremos también como $\phi_{\mathbb{Z}}$), es:

$$\phi_{\mathbb{Z}}([\bar{n}_1|\cdots|\bar{n}_k]) = \begin{cases} (-1)^k \sum_{i=1}^{n_k-1} [\bar{n}_1|\cdots|\bar{n}_{k-1}|\bar{i}|\bar{1}], & \text{si } n_k > 1, \\ 0, & \text{si } n_k = -1, 0, 1, \\ (-1)^k \sum_{i=1}^{-1-n_k} [\bar{n}_1|\cdots|\bar{n}_{k-1}|\overline{-i}|\bar{1}], & \text{si } n_k < -1. \end{cases}$$

Eilenberg y Mac Lane también construían en [35] un modelo homológico para $\mathbb{Z}_n$,

$$C_{\mathbb{Z}_n} = \{\bar{B}(\mathbb{Z}[\mathbb{Z}_n]), (E(u,1) \otimes \Gamma(w,2), d_n), f_{\mathbb{Z}_n}, g_{\mathbb{Z}_n}, \phi_{\mathbb{Z}_n}\}, \tag{2.2}$$

en función del producto de un álgebra exterior y un *álgebra polinomial modificada* (también conocida como *álgebra de potencias divididas*).

Recordemos que un *álgebra polinomial modificada* $\Gamma(w, 2n)$, con $n \geq 1$, es la DGA-álgebra libre con generadores

$$\gamma_o(w) = 1; \gamma_1(w) = w, \ldots, \gamma_k(w), \ldots; \text{con } |\gamma_k(w)| = 2n,$$

cuyo producto viene dado por

$$\gamma_k(w)\gamma_h(w) = \frac{(k+h)!}{k!h!}\gamma_{k+h}(w).$$

También tiene diferencial nula y la aumentación y coaumentación siguen siendo la identidad en el anillo base. A veces se suele denotar $\gamma_k(w)$ simplemente como $w^{(k)}$.

La diferencial asociada al modelo homológico de $\mathbb{Z}_n$, $E(u,1) \otimes \Gamma(w,2)$, viene dada por las relaciones $d_n(\gamma_j(v)) = n \cdot u\gamma_{j-1}(v))$ y $d_n(u\gamma_j(v)) = 0$.

Y los morfismos de la contracción anterior son:

$$\begin{array}{lcl} f_{\mathbb{Z}_n}[\bar{x}_1|\bar{y}_1|\cdots|\bar{x}_m|\bar{y}_m] & = & [\prod_{i=1}^m s_2(x_i,y_i)]\gamma_m(w), \\ f_{\mathbb{Z}_n}[\bar{x}_1|\bar{y}_1|\cdots|\bar{x}_m|\bar{y}_m|\bar{z}] & = & [s_1(z)\prod_{i=1}^m s_2(x_i,y_i)]u\gamma_m(w), \end{array}$$

siendo

$$s_1(i) = i,\ 0 \leq i \leq n, \qquad s_2(i,j) = \begin{cases} 0 & i+j < n, \\ 1 & i+j \geq n; \end{cases}$$

$$\begin{array}{lcl} g_{\mathbb{Z}_n}(u) & = & [\bar{1}], \\ g_{\mathbb{Z}_n}(\gamma_k(v)) & = & \sum_{x_1,\ldots,x_k \in \mathbb{Z}_n}[\bar{1}|\bar{x}_1|\cdots|\bar{1}|\bar{x}_k], \\ g_{\mathbb{Z}_n}(u\gamma_k(v)) & = & \sum_{x_1,\ldots,x_k \in \mathbb{Z}_n}[\bar{1}|\bar{x}_1|\cdots|\bar{1}|\bar{x}_k|\bar{1}]; \end{array}$$

y $\phi([\bar{x}_1|\cdots|\bar{x}_k]) = -\varphi([\bar{x}_1|\cdots|\bar{x}_k])$, con

$$\begin{array}{lcl} \varphi_{\mathbb{Z}_n}[\,] & = & 0, \\ \varphi_{\mathbb{Z}_n}[\bar{x}] & = & C(x), \\ \varphi_{\mathbb{Z}_n}[\bar{x}|\bar{y}|\sigma] & = & [C(x)|\bar{y}|\sigma] + s_2(x,y)[\sum_{l \in \mathbb{Z}_n}[\bar{1}|\bar{l}]|\varphi_{\mathbb{Z}_n}\sigma]; \end{array}$$

donde

$$C(x) = \sum_{i=1}^{x-1}[\bar{1}|\bar{i}].$$

Recuérdese que las tuplas de $\bar{B}(\mathbb{Z}[\mathbb{Z}_n])$ no pueden contener la entrada 0, puesto que trabajamos la construcción bar normalizada que corresponde al grupo.

Los grupos abelianos más sencillos que se pueden construir a partir de $\mathbb{Z}$ y de $\mathbb{Z}_n$, consisten en el producto directo $A \times G$ de dos grupos dados $A, G \in \{\mathbb{Z}_n, \mathbb{Z}\}$, con la ley de grupo usual, componente a componente:

$$(a_1, g_1)(a_2, g_2) = (a_1 a_2, g_1 g_2).$$

Para calcular la homología de este grupo se puede recurrir al cálculo de la homología del álgebra asociada $\mathbb{Z}[A \times G] \cong \mathbb{Z}[A] \otimes \mathbb{Z}[G]$; esto es, estudiar la homología de la construcción bar asociada $\bar{B}(\mathbb{Z}[A] \otimes \mathbb{Z}[G])$. Teniendo en cuenta que los modelos homológicos de A y G son conocidos, un modelo homológico para $\bar{B}(\mathbb{Z}[A \times G])$ queda caracterizado según la contracción establecida por Eilenberg-Mac Lane en [35], la cual relaciona la construcción bar del producto de dos álgebras (en nuestro caso, $\mathbb{Z}[A]$ y $\mathbb{Z}[G]$), con el producto de las construcciones bares de cada una de ellas:

$$C_{\bar{B}\otimes} : \{\bar{B}(\mathbb{Z}[A] \otimes \mathbb{Z}[G]), \bar{B}(\mathbb{Z}[A]) \otimes \bar{B}(\mathbb{Z}[G]), f_{\bar{B}\otimes}, g_{\bar{B}\otimes}, \phi_{\bar{B}\otimes}\}. \tag{2.3}$$

La aplicación $f_{\bar{B}\otimes}$ queda caracterizada por su actuación sobre elementos homogéneos $[a_1 \otimes g_1 | \cdots | a_n \otimes g_n]$ de $\bar{B}(\mathbb{Z}[A] \otimes \mathbb{Z}[G])$, con cada $a_i \in \mathbb{Z}[A]$ y $g_i \in \mathbb{Z}[G]$ homogéneos:

$$f_{\bar{B}\otimes}([a_1 \otimes g_1 | \cdots | a_n \otimes g_n]) = \sum_{i=0}^{n} [a_1 | \cdots | a_i] \otimes [g_{i+1} | \cdots | g_n],$$

donde para $i = 0$ el término $[a_1 | \cdots | a_i] = [\,] = 1 \in \bar{B}(\mathbb{Z}[A])$; y análogamente, para $i = n$, $[g_{i+1} | \cdots | g_n] = [\,] = 1 \in \bar{B}(\mathbb{Z}[G])$.

Teniendo en cuenta las propiedades del producto tensorial, resulta que $\bar{B}(\mathbb{Z}[A])$ y $\bar{B}(\mathbb{Z}[G])$ quedan identificadas como subálgebras de $\bar{B}(\mathbb{Z}[A] \otimes \mathbb{Z}[G])$, siendo:

$$[a_1 | \cdots | a_n] = [a_1 \otimes 1 | \cdots | a_n \otimes 1], \quad [g_1 | \cdots | g_n] = [1 \otimes g_1 | \cdots | 1 \otimes g_n].$$

De este modo, la aplicación $g_{\bar{B}\otimes}$ queda definida por la fórmula:

$$g_{\bar{B}\otimes}(u \otimes v) = u \star v, \qquad u \in \bar{B}(\mathbb{Z}[A]),\ v \in \bar{B}(\mathbb{Z}[G]),$$

donde $\star$ representa el *producto shuffle*, definido en [34] por medio de (p, q)-*shuffles* o mezclas.

Un (p, q)-*shuffle* consiste en una partición del conjunto de los primeros $p + q$ enteros[2]; de modo que resulten dos subconjuntos ordenados y disjuntos, $\alpha_1 < \cdots < \alpha_p$

[2]Se entiende, pues, que se trata del conjunto $\{0, \ldots, p + q - 1\}$.

y $\beta_1 < \cdots < \beta_q$ de p y q enteros, respectivamente. En definitiva, se trata de una permutación π del conjunto de los $p+q$ primeros enteros de modo que $\pi(i) < \pi(j)$ cuando, bien $0 \leq i < j \leq p-1$; bien, $p \leq i < j < p+q$. De este modo, quedan determinadas dos sucesiones de enteros:

$$\alpha_i = \pi(i-1), \quad i = 1, \ldots, p; \qquad \beta_j = \pi(p+j-1), \quad j = 1, \ldots, q,$$

que se corresponden con los subconjuntos de la definición primigenia. Notaremos cada (p,q)-shuffle por un par (α, β), en referencia a las sucesiones α_i y β_j.

El producto shuffle se puede definir entonces en la forma

$$[a_1|\cdots|a_p] \star [b_1|\cdots|b_p] = \sum (-1)^{sg(\pi,a,b)} [c_{\pi(1)}|\cdots|c_{\pi(p+q)}] \tag{2.4}$$

en el que la suma está definida para todos los $\pi \in \{(p,q) - shuffles\}$, siendo el signo $sg(\pi,a,b) = \sum_{(i,j),\pi(i)>\pi(j)} |[a_i]|_{\bar{B}}|[b_j]|_{\bar{B}}$, y $(c_1, \ldots, c_{p+q}) = (a_1, \ldots, a_p, b_1, \ldots, b_q)$.

Por último, el operador de homotopía viene dado por

$$\phi_{\bar{B}\otimes} = \lambda^{-1} SHI_{\otimes} \lambda,$$

donde:

- el morfismo $SHI_{\otimes}$ actúa del siguiente modo:

$$SHI_{\otimes} : \bar{B}(\mathbb{Z}[A]) \times \bar{B}(\mathbb{Z}[G]) \to \bar{B}(\mathbb{Z}[A]) \times \bar{B}(\mathbb{Z}[G]),$$

$$SHI_{\otimes}([a_1|\cdots|a_n] \times [g_1|\cdots|g_n]) = \sum_{q=0}^{n-1} \sum_{p=0}^{n-p-q} [a_1 \otimes g_1|\cdots|a_{n-p-q-1} \otimes g_{n-p-q-1}|$$
$$|g_{n-p-q}\cdots g_{n-q}|([a_{n-p-q}|\cdots|a_{n-q}] \star [g_{n-q+1}|\cdots|g_n])],$$

- el isomorfismo de DG-módulos λ actúa del siguiente modo:

$$\lambda : \bar{B}(\mathbb{Z}[A] \otimes \mathbb{Z}[G]) \to \bar{B}(\mathbb{Z}[A]) \times \bar{B}(\mathbb{Z}[G]),$$

$$\lambda[a_1 \otimes g_1|\cdots|a_n \otimes g_n] = [a_1|\cdots|a_n] \times [g_1|\cdots|g_n],$$

con a_i y g_i elementos homogéneos de A y G, respectivamente.

A partir de las fórmulas anteriores, se puede determinar que los morfismos $g_{\bar{B}\otimes}$ y $\phi_{\bar{B}\otimes}$ actúan en tiempo exponencial, mientras que $f_{\bar{B}\otimes}$ lo hace en tiempo lineal.

Por otra parte, para escribir el modelo homológico de $\bar{B}(\mathbb{Z}[A]) \otimes \bar{B}(\mathbb{Z}[G])$ en función de los modelos homológicos de $\bar{B}(\mathbb{Z}[A])$ y de $\bar{B}(\mathbb{Z}[G])$, se puede utilizar la *contracción producto tensorial* de dos contracciones conocidas. Dadas dos contracciones $c_i : \{N_i,\ M_i,\ f_i,\ g_i,\ \phi_i\}\quad i = 1, 2$, la *contracción producto tensorial* de ambas viene dada por:

$$c_1 \otimes c_2 : \{N_1 \otimes N_2,\ M_1 \otimes M_2, f_1 \otimes f_2,\ g_1 \otimes g_2,\ \phi_1 \otimes g_2 f_2 + 1_N \otimes \phi_2\}. \tag{2.5}$$

Así, se obtiene la contracción:

$$c : \{\bar{B}(\mathbb{Z}[A]) \otimes \bar{B}(\mathbb{Z}[G]), hA \otimes hG, f_A \otimes f_G, g_A \otimes g_G, \phi_A \otimes g_G f_G + 1 \otimes \phi_G\}, \tag{2.6}$$

donde hA y hG son los modelos homológicos de A y G, respectivamente; es decir, $hA, hG \in \{E, E \otimes \Gamma\}$, $f_A, f_G \in \{f_{\mathbb{Z}}, f_{\mathbb{Z}_n}\}$, $g_A, g_G \in \{g_{\mathbb{Z}}, g_{\mathbb{Z}_n}\}$ y $\phi_A, \phi_G \in \{\phi_{\mathbb{Z}}, \phi_{\mathbb{Z}_n}\}$.

De otro lado, dadas dos contracciones en las que el módulo menor de la primera es el mayor de la segunda, éstas se pueden concatenar para producir una nueva contracción; de modo que a partir de las contracciones $c_i : \{N_i, M_i, f_i, g_i, \phi_i\}$, $i = 1, 2$, con $N_2 = M_1$, la *contracción composición de ambas*, viene dada por:

$$c_2 \circ c_1 : \{N_1,\ M_2,\ f_2 f_1,\ g_1 g_2,\ \phi_1 + g_1 \phi_2 f_1\}.$$

Luego, si componemos las contracciones (2.3) y (2.6), tenemos la contracción que proporciona un modelo homológico para el producto directo $A \times G$:

$$c_{A\times G} : \{\bar{B}(\mathbb{Z}[A] \otimes \mathbb{Z}[G]),\ hA \otimes hG,\ f_{A\times G},\ g_{A\times G},\ \phi_{A\times G}\}, \tag{2.7}$$

siendo:

$$f_{A\times G} = (f_A \otimes f_G) f_{\bar{B}\otimes},$$
$$g_{A\times G} = g_{\bar{B}\otimes}(g_A \otimes g_G),$$
$$\phi_{A\times G} = \phi_{\bar{B}\otimes} + g_{\bar{B}\otimes}(\phi_A \otimes g_G f_G + 1 \otimes \phi_G) f_{\bar{B}\otimes}.$$

Este mecanismo admite ser iterado, de modo que, dado un grupo

$$(\cdots((A_1 \times A_2) \times A_3) \cdots \times A_t), \quad \text{con cada } A_i \in \{\mathbb{Z}, \mathbb{Z}_{n_i}\},$$

por composición de $t - 1$ contracciones de productos directos del tipo anterior, y siguiendo el siguiente esquema

$$\bar{B}(\mathbb{Z}[(\cdots((A_1 \times A_2) \times A_3) \cdots \times A_t)]) \cong \bar{B}(\mathbb{Z}[A_1] \otimes \cdots \otimes \mathbb{Z}[A_t]) \Longrightarrow$$

$$\overset{\text{composición reiterada de } C_{\bar{B}\otimes}}{\Longrightarrow} (\bigotimes_{i=1}^{t} \bar{B}(\mathbb{Z}[A_i])) \overset{\text{producto tensorial de } C_{\mathbb{Z},\mathbb{Z}_n}}{\Longrightarrow} \bigotimes_{i=1}^{t} hA_i;$$

obtenemos la contracción:

$$c_\times : \{(\cdots((A_1 \times A_2) \times A_3)\cdots) \times A_t), hA_1 \otimes \cdots \otimes hA_t, f_\times, g_\times, \phi_\times\}, \tag{2.8}$$

con $A_i \in \{\mathbb{Z}, \mathbb{Z}_{n_i}\}$ y $hA_i \in \{E, E \otimes \Gamma\}$ y cuyos morfismos quedan definidos en la forma

$$f_\times = (f_{\mathbb{Z}_{n_1}} \otimes \cdots \otimes f_{\mathbb{Z}_{n_t}})(1^{\otimes t-2} \otimes f_{B\otimes}) \cdots f_{B\otimes}$$

$$g_\times = g_{B\otimes} \cdots (1^{\otimes t-2} \otimes g_{B\otimes})(g_{\mathbb{Z}_{n_1}} \otimes \cdots \otimes g_{\mathbb{Z}_{n_t}})$$

$$\phi_\times = \sum_{i=0}^{t-1} (1^{\otimes i-1} \otimes g_{B\otimes})(1^{\otimes i} \otimes \phi_{B\otimes})(1^{\otimes i-1} \otimes f_{B\otimes}) +$$

$$+ g_{B\otimes} \cdots (1^{\otimes t-2} \otimes g_{B\otimes}) \sum_{i=0}^{t-1} [1^{\otimes i} \otimes \phi_{A_{i+1}} \otimes (g_{A_{i+2}} f_{A_{i+2}} \otimes \cdots \otimes g_{A_t} f_{A_t})](1^{\otimes t-2} \otimes f_{B\otimes}) \cdots f_{B\otimes}.$$

La diferencial correspondiente al modelo es:

$$d_\times = (\sum_{i=1}^{t} 1^{\otimes i-1} \otimes d_{hA_i} \otimes 1^{\otimes t-i}).$$

2.2.2 Modelo cohomológico

A la hora de determinar un modelo cohomológico para un grupo abeliano, progresaremos sobre un modelo homológico, aplicando el funtor Hom a la contracción correspondiente.

De cualquier modo, al igual que en el apartado anterior, comenzaremos estudiando el modelo cohomológico de los grupos más sencillos, $\mathbb{Z}$ y $\mathbb{Z}_n$.

Antes de proseguir, hemos de hacer notar que dada un álgebra A y una coálgebra C, el complejo $\mathrm{Hom}(C, A)$ adquiere asimismo la estructura de álgebra mediante el $\cup$-producto: dados $f, g \in \mathrm{Hom}(C, A)$, se define $f \cup g = (f *_A g)\Delta \in \mathrm{Hom}(C, A)$.

Consideremos el grupo $\mathbb{Z}$. De un lado, se tiene que $E^*(u) = \mathrm{Hom}(E(u, 1), \mathbb{Z}) \cong E(u^*)$ a nivel de DG-álgebras. En efecto, considerando el coproducto $\Delta_E(u) = u \otimes 1 + 1 \otimes u$ propio de $E(u)$, resulta que $\mathrm{Hom}(E(u), \mathbb{Z})$ adquiere la estructura de DG-álgebra

con el producto $\cup$; que actúa de manera trivial, puesto que $u^* \cup u^* = (u^* *_{\mathbb{Z}} u^*)\Delta_E = 0$, al ser $u^*(1) = 0$.

Así, al aplicar el funtor Hom sobre la contracción (2.1), se obtiene

$$c^*_{\mathbb{Z}} : \{\mathrm{Hom}(\bar{B}(\mathbb{Z}[\mathbb{Z}]), \mathbb{Z}), E(u,1), g^*_{\mathbb{Z}},\ f^*_{\mathbb{Z}},\ \phi^*_{\mathbb{Z}}\},$$

siendo

$$g^*_{\mathbb{Z}} = \mathrm{Hom}(g_{\mathbb{Z}}, \mathbb{Z})\ , \quad f^*_{\mathbb{Z}} = \mathrm{Hom}(f_{\mathbb{Z}}, \mathbb{Z})\ , \quad \phi^*_{\mathbb{Z}} = \mathrm{Hom}(\phi_{\mathbb{Z}}, \mathbb{Z})\ .$$

Del mismo modo, se tiene el isomorfismo $\Gamma^*(w) = \mathrm{Hom}(\Gamma(w), \mathbb{Z}) \cong P(w^*, 2)$; donde $P(x, 2n)$, con n un entero positivo, denota un *álgebra polinomial*: una DGA-álgebra de diferencial nula, con generadores 1 en grado 0 y x en grado $2n$, y producto $x^i x^j = x^{i+j}$. La aumentación y coaumentación coinciden con $1_{\mathbb{Z}}$.

Por otra parte, el funtor Hom respeta los productos tensoriales de estas álgebras básicas (exteriores, polinomiales y polinomiales modificadas), que son libres y de tipo finito (finitamente generadas en cada grado); de modo que

$$(A \otimes B)^* \overset{F}{\cong} A^* \otimes B^*, \tag{2.9}$$

para $A, B \in \{E(u), \Gamma(w), P(v)\}$. Este isomorfismo F se puede ver como composición de otros dos más sencillos:

$$(A \otimes B)^* \overset{\xi}{\cong} \mathrm{Hom}(A, B^*) \quad \text{y} \quad \mathrm{Hom}(A, C) \overset{\eta}{\cong} A^* \otimes C,$$

siendo

$$\begin{array}{rccll} \xi : & (A \otimes B)^* & \to & \mathrm{Hom}(A, B^*) & \\ & f & \mapsto & \xi(f) & / \ \xi(f)(a) \in B^*, \\ & & & & \text{con } \xi(f)(a)(b) = f(a \otimes b) \in \mathbb{Z}, \end{array}$$

$$\begin{array}{rccll} \xi^{-1} : & \mathrm{Hom}(A, B^*) & \to & (A \otimes B)^* & \\ & g & \mapsto & \xi^{-1}(g) & / \ \xi^{-1}(g)(a \otimes b) = g(a)(b) \in \mathbb{Z}, \end{array}$$

$$\begin{array}{rccll} \eta : & \mathrm{Hom}(A, C) & \to & A^* \otimes C & \\ & g & \mapsto & \eta(g) & / \ \eta(g) = \sum\limits_{i \in \mathbb{N}} a_i^* \otimes g(a_i), \\ & & & & \text{dado que por ser } A \text{ libre y de tipo finito} \\ & & & & \text{es de la forma } A = \bigoplus\limits_{i \in \mathbb{N}} \mathbb{Z}[a_i] \end{array}$$

y

$$\begin{array}{rccl} \eta^{-1}: & (A^* \otimes C) & \to & \mathrm{Hom}(A, C) \\ & f \otimes c & \mapsto & \eta^{-1}(f \otimes c) \quad / \, \eta^{-1}(f \otimes c)(a) = f(a) \cdot c \in C. \end{array}$$

Así, al aplicar el funtor Hom sobre la contracción (2.2), se tiene

$$c^*_{\mathbb{Z}_n} : \{\mathrm{Hom}(\bar{B}(\mathbb{Z}[\mathbb{Z}_n]), \mathbb{Z}), E(u,1) \otimes P(v,2), g^*_{\mathbb{Z}_n}, f^*_{\mathbb{Z}_n}, \phi^*_{\mathbb{Z}_n}\},$$

en la que

$$g^*_{\mathbb{Z}_n} = \mathrm{Hom}(g_{\mathbb{Z}_n}, \mathbb{Z}) \, , \quad f^*_{\mathbb{Z}_n} = \mathrm{Hom}(f_{\mathbb{Z}_n}, \mathbb{Z}) \, , \quad \phi^*_{\mathbb{Z}_n} = \mathrm{Hom}(\phi_{\mathbb{Z}_n}, \mathbb{Z}) \, .$$

A partir de los modelos cohomológicos de $\mathbb{Z}$ y $\mathbb{Z}_n$ presentados, se puede obtener un modelo cohomológico para cualquier otro grupo abeliano finitamente generado $G = A_1 \times \cdots \times A_t$, con $A_i \in \{\mathbb{Z}, \mathbb{Z}_n\}$, a partir de la contracción (2.8) y el isomorfismo (2.9):

$$\mathrm{Hom}((\cdots((A_1 \times A_2) \times A_3), \cdots) \times A_t), \mathbb{Z}) \overset{c^*_\times}{\Longrightarrow} \mathrm{Hom}(hA_1 \otimes \cdots \otimes hA_t, \mathbb{Z}) \overset{F}{\cong} hA_1^* \otimes \cdots \otimes hA_t^* \tag{2.10}$$

2.2.3 Computación

Toda la labor de implementación de los algoritmos que se describen en esta memoria se ha realizado utilizando el paquete simbólico *Mathematica 4.0*. El motivo lo encontramos en el hecho de que este programa es el más afín de entre los que se nos ofrecían, amén de su versatilidad y la amplia librería de comandos y paquetes ya programados de que dispone.

A lo largo de la memoria iremos intercalando la descripción teórica de los algoritmos con su correspondiente implementación en *Mathematica* y unas pruebas de ejecución a modo de ejemplos (con la sola excepción de este apartado, toda vez que la (co)homología de grupos abelianos es bien conocida).

En particular, ahora nos centraremos en un módulo que calcula la homología de un producto directo de grupos abelianos finitos, sobre el que posteriormente nos basaremos para implementar rutinas de cálculo (co)homológico para productos iterados de extensiones centrales y productos semidirectos de grupos de este tipo. Aclaremos primero el modo en que vamos a codificar las distintas estructuras.

Todo grupo G de orden n se codifica etiquetando sus elementos en la forma $\{1,\ldots,n\}$ y definiendo su operación producto $*$, respecto de la cual 1 será la unidad. En particular, la ley de grupo para $\mathbb{Z}_n$ vendrá dada en la forma

```
prod[x_,y_,]:=1+Mod[x+y-2,1];
```

Un elemento básico $\lambda\cdot(a_{n-1},\ldots,a_0)$ de $C_*(\bar{W}(H))$ se codifica en la forma $\lambda * \{h_{n-1},\ldots,h_0\}$, mientras que un elemento genérico de $C_*(\bar{W}(A))\otimes C_*(\bar{W}(G))$ viene dado por $\lambda * \{\{a_{n-1},\ldots,a_0\},\{g_{n-1},\ldots,g_0\}\}$.

Aquí hemos de andar con cuidado, dado que las operaciones suma y producto son "listables" en *Mathematica* (esto es, las listas se tratan como vectores, y las operaciones suma y producto como operaciones componentes a componentes). Por tanto, hemos de modificar dicho atributo para hacer de la adición y la multiplicación sendos operadores no "listables", lo que facilita sobremanera el tratamiento de la combinación lineal de listas:

```
ClearAttributes[Plus,Listable];
ClearAttributes[Times,Listable];
```

Las operaciones correspondientes con el carácter "listable" las recuperamos así:

```
SetAttributes[sumlist,Listable];SetAttributes[prodlist,Listable];
sumlist[a_,b_]:=a+b; prodlist[a_,b_]:=a*b;
```

Para filtrar los elementos degenerados en $C_*(\bar{W}(A)\times\bar{W}(G))$ (con sendos elementos neutros simultáneamente en las mismas componentes de $\bar{W}(A)$ y $\bar{W}(A)$) y los de $C_*(\bar{W}(A))\otimes C_*(\bar{W}(G))$ (en los que aparece un elemento neutro en alguna de las componentes de uno de los factores); definimos linealmente sendas aplicaciones de control,

```
nul1[x_+y_]:=nul1[x]+nul1[y]; nul1[x_*y_]:=Expand[x*nul1[y]];
nul1[0]:=0;
nul1[l_]:=Module[{k, n,i}, k=l; n=Length[l[[1]]]; i=1;
      While[i<=n, If[(l[[1,i]]==1)&&(l[[2,i]]==1), k=0; i=n+1,
        i=i+1]];
      k];
nul2[x_+y_]:=nul2[x]+nul2[y]; nul2[x_*y_]:=Expand[x*nul2[y]];
```

```
nul2[0]:=0;
nul2[l_]:=Module[{k,n1,n2}, n1=Length[Select[l[[1]],#==1&,1]];
      n2=Length[Select[l[[2]],#==1&,1]]; If[n1+n2==0, k=l, k=0];
      k];
```

Los elementos correspondientes al modelo homológico $E(u) \otimes \Gamma(w)$ de $\mathbb{Z}_n$ los codificaremos como combinaciones lineales de listas de una sola entrada, que se corresponderán con los generadores del módulo $E(u)\tilde{\otimes}\Gamma(w)$; de modo que $\{m\}$ hace referencia al generador $u^{m\,(mod\,2)} \otimes \gamma_{\lfloor \frac{m}{2} \rfloor}(w)$.

A continuación codificamos los morfismos que componen las contracciones en que factoriza el modelo homológico de productos directos que hemos descrito previamente: primero, los correspondientes a la contracción Eilenberg-Zilber; después, los que definen el modelo como producto de contracciones de modelos homológicos para grupos $\mathbb{Z}_n$.

Las aplicaciones `aw`,`eml` y `shi` a describir a continuación se aplican sobre elementos de entrada no degenerados. Esto significa que, en caso necesario, se ha de aplicar `nul1` ó `nul2`, según corresponda, antes de llamar a dichas funciones.

```
aw[x_+y_]:=aw[x]+aw[y]; aw[x_*y_]:=Expand[x*aw[y]];
aw[0]=0;
aw[l_]:=Module[{n,l1,l2}, l1=l[[1]]; l2=l[[2]]; n=Length[l1];
      Apply[Plus,Table[{Drop[l1,-(n-i)],Drop[l2,i]},
        {i,n+1-Position[Append[Reverse[l2],1],1,1,1][[1,1]],
          -1+Position[Append[l1,1],1,1,1][[1,1]]}]];
```

A la hora de codificar la aplicación EML, hemos convenido utilizar una rutina axiliar `aumnent[p][k]`, de modo que para hacer un (p,q)-shuffle se seleccionan aquellas posiciones de la lista de longitud p en las que insertar los q elementos de la lista original, y se disponen entre llaves.

```
aument[p_][k_]:=Table[Append[k,{j}],{j, Last[k][[1]],p+1}];
apaument[p_][k_]:=Flatten[Map[aument[p],k],1];
shuf[p_,0]:={{}}; shuf[0,q_]:={Table[{1},{i,q}]};
shuf[p_,1]:=Table[{{q}},{q,1,p+1}];
shuf[p_,q_]:=Nest[apaument[p],shuf[p,1],q-1];
insertar[l_,{ele_,pos_}]:=Insert[l, ele, pos];
```

```
eml[x_+y_]:=eml[x]+eml[y]; eml[x_*y_]:=Expand[x*eml[y]]; eml[0]=0;
eml[l_]:=Module[{k,n1,n2,l1,l2}, l1=l[[1]]; l2=l[[2]]; n1=Length[l1];
      n2=Length[l2]; k=shuf[n1, n2]; Expand[Apply[Plus,
        Table[(-1)^(n2*(n1+1)+Apply[Plus,Flatten[k[[i]],1]])*
          {Insert[l1,1,k[[i]]],Fold[insertar,Table[1, {j, n1}],
            Table[{l2[[n2+1-j]],k[[i,n2+1-j]]}, {j,n2}]]},
      {i, Length[k]}]]];
```

La función unir yuxtapone dos elementos de $C_*(\bar{W}(A) \times \bar{W}(G))$, y se utiliza a la hora de definir shi:

```
unir[l_,x_+y_]:=unir[l,x]+unir[l, y];
unir[l_,x_*y_]:=Expand[x*unir[l,y]]; unir[l_,0]=0; unir[0,k_]:=0;
unir[l_,k_]:={Join[l[[1]],k[[1]]],Join[l[[2]],k[[2]]]};
shi[x_+y_]:=shi[x]+shi[y]; shi[x_*y_]:=Expand[x*shi[y]]; shi[0]=0;
shi[l_]:=Module[{n,k1,k2}, k1=l[[1]]; k2=l[[2]]; n=Length[k1];
      If[n<=1, 0, Expand[Apply[Plus,Table[Apply[Plus,
        Table[(-1)^(n-p-q)*unir[nul1[{Append[Drop[k1,-p-q-1],1],
          Append[Drop[k2,-p-q-1],Fold[prodg[niv],1,Reverse[Take[
            k2,{n-p-q,n-q}]]]]}],eml[nul2[{Take[k1,{n-p-q,n-q}],
      Drop[k2,n-q]}]]],{p,0,n-q-1}]], {q,0,n - 1}]]]]];
```

Los morfismos que definen un modelo homológico de $\mathbb{Z}_n$ son:

```
sumarunalista[l_]:=Apply[Plus,l];
s[n_,l_]:=Module[{m, k}, m=Length[l];If[Length[Select[Map[
      sumarunalista,Partition[sumlist[-1,l],2]],#1<n&]]==0,
        If[Mod[m,2]==1, k=Last[l]-1, k=1], k=0];
      k];
fzn[n_][x_+y_]:=fzn[n][x]+fzn[n][y];
fzn[n_][x_*y_]:=Expand[x*fzn[n][y]];
fzn[n_][0]:=0;
fzn[n_][l_]:=s[n, l]*{Length[l]};
base1[n_][l_]:=Table[Join[{2,i},l], {i,2,n}];
base2[n_][l_]:=Flatten[Map[base1[n],l],1];
gzn[n_][x_+y_]:=gzn[n][x]+gzn[n][y];
gzn[n_][x_*y_]:=Expand[x*gzn[n][y]];
```

```
gzn[n_][0]:=0;
gzn[n_][l_]:=Module[{k}, If[Mod[l[[1]],2]==1, k={{2}}, k ={{}}];
      Apply[Plus,Nest[base2[n],k,Floor[l[[1]]/2]]]];
fi2[n_][x_+y_]:=fi2[n][x]+fi2[n][y];
fi2[n_][x_*y_]:=Expand[x*fi2[n][y]];
fi2[n_][0]:=0; fi2[n_][{}]=0;
fi2[n_][l_]:=Module[{k}, k=Apply[Plus,Table[Join[
        {2,i},Rest[l]],{i,2,l[[1]]-1}]];
      If[l[[1]]+Append[l,0][[2]]<n+2, , k=k+pegar[Apply[Plus,Table[
        {2,i},{i,2,n}]], fi2[n][Drop[l, 2]]]];
      k];
fizn[n_][l_]:=Expand[-fi2[n][l]];
difzn[n_][{0}]:=0;
difzn[n_][l_]:=Mod[1+l[[1]],2]*n*{l[[1]]-1};
```

El último eslabón que resta para engarzar el modelo homológico de un producto directo es la codificación de una contracción producto tensorial de dos modelos homológicos de grupos abelianos finitos, cuyos morfismos llamamos `fmodban`, `gmodban` y `fimodban`. La función auxiliar bilineal `pegar` transforma pares de elementos de $C_*(\bar{W}(A))$ y $C_*(\bar{W}(G))$ en un elemento de $C_*(\bar{W}(A)) \otimes C_*(\bar{W}(G))$.

```
pegar[x_+y_,z_]:=pegar[x,z]+pegar[y,z]; pegar[0,z_]:=0;
pegar[x_*y_,z_]:=Expand[x*pegar[y,z]];
pegar[z_,x_+y_]:=pegar[z,x]+pegar[z,y];
pegar[z_,x_*y_]:=Expand[x*pegar[z,y]]; pegar[z_,0]:=0;
pegar[l_,k_]:=Join[l,k];
fmodban[x_+y_]:=fmodban[x]+fmodban[y]; fmodban[0]:=0;
fmodban[x_*y_]:=Expand[x*fmodban[y]];
fmodban[l_]:=pegar[fa[l[[1]]],fg[l[[2]]]];
union[x_+y_,z_]:=union[x,z]+union[y,z];
union[x_*y_,z_]:=Expand[x*union[y, z]]; union[0,z_]:=0;
union[z_,x_+y_]:=union[z,x]+union[z,y];
union[z_,x_*y_]:=Expand[x*union[z,y]]; union[z_,0]:=0;
union[l_,k_]:={l, k};
gmodban[x_+y_]:=gmodban[x]+gmodban[y]; gmodban[0]:=0;
gmodban[x_*y_]:=Expand[x*gmodban[y]];
gmodban[l_]:=union[ga[l[[1]]],gg[l[[2]]]];
```

```
fimodban[x_+y_]:=fimodban[x]+fimodban[y];
fimodban[x_*y_]:=Expand[x*fimodban[y]]; fimodban[0]:=0;
fimodban[l_]:=Expand[(-1)^Length[l[[1]]]*union[l[[1]],fig[l[[2]]]]+
      union[fia[l[[1]]],gg[fg[l[[2]]]]]];
```

En este código, previamente se han definido las aplicaciones `fa`, `ga`, `phia`, `fg`, `gg` y `phig`, como las `fzn`, `gzn` y `phizn` correspondientes, en función de los índices de los $\mathbb{Z}_n$ que intervienen.

Por último, la diferencial `dif` del modelo homológico resulta de

```
dif[l_]:=Expand[pegar[da[l[[1]]],l[[2]]]+
      (-1)^l[[1]]*pegar[l[[1]],dg[l[[2]]]]];
```

donde `da` y `dg` representan las diferenciales `difzn` correspondientes.

A la hora de hacer cálculos explícitos de (co)homología basta aplicar el algoritmo de Veblen, cuyo paso fundamental es la determinación de la forma normal de Smith de las matrices que proporciona la diferencial.

En lugar de programar nosotros mismos una rutina a tal efecto, aprovechamos las librerías conocidas de *Mathematica* y hacemos uso del programa `IntegerSmithNormalForm` que David Jabon diseñara en 1994.

Para determinar la homología en grado i habrá que utilizar las diferenciales d_i y d_{i+1}. En la rutina que sigue, suponemos que el modelo homológico está compuesto por `numgru` álgebras del tipo $E \otimes \Gamma$. Las variables `b1`, `b2` y `b3` denotan el número de generadores en el modelo homológico en dimensiones $i-1$, i e $i+1$, respectivamente; que son las combinaciones con repetición de `numgru` elementos tomados de $i-1$, i e $i+1$ en $i-1$, i e $i+1$ veces, respectivamente. La diferencial del modelo se denota como `dif`. El comando `basemod[q,p]` genera una base en grado q en un producto de p álgebras $E \otimes \Gamma$, ordenada según la lista $\{\{q,0,\ldots,0\},\{q-1,1,0,\ldots,0\},\ldots,\{0,\ldots,0,q\}\}$. La función que asigna a una de estas tuplas su correspondiente posición en la base es `conversion`.

```
juntar[l_][k_]:=Join[l,k];
basemod[0,p_]:={Table[0, {i,p}]};
basemod[q_Integer,1]:={{q}};
```

```
basemod[q_Integer,p_Integer]:=Flatten[Table[Map[juntar[{q- i}],
      basemod[i,p-1]], {i,0,q}],1];
conversion[0,p_][l_]:=1;
conversion[q_,p_][l_]:=Sum[Binomial[p+i-2,i],{i,0,q-l[[1]]-1}]+
      conversion[q-l[[1]],p-1][Rest[l]];
coef[l_]:=If[VectorQ[l],{1,l},{l[[1]],l[[2]]}];
b2=Binomial[numgru+i-1,i];
b1=Binomial[numgru+i-2,i-1];
A=Table[Table[0, {i,b1}], {j,b2}];
primbase=basemod[i,numgru];
Module[{k,k1,k2}, Do[ k={-1}+dif[primbase[[i]]];
      k2=Table[coef[k[[k1]]], {k1,2,Length[k]}];
      Do[
A=ReplacePart[A,k2[[j,1]],{i,conversion[i-1,numgru][k2[[j,2]]]}],
{j, Length[k2]}], {i, b2}]; ];
SetAttributes[Plus,Listable]; SetAttributes[Times,Listable];
fnsa1=ExtendedSmithForm[A];
ClearAttributes[Plus,Listable]; ClearAttributes[Times,Listable];
nucleo=b2-Select[Table[fnsa1[[1,ji,ji]], {ji,b1}],#1>0&];
Print["El núcleo de d_",i," tiene dimension ",nucleo];
b3=Binomial[numgru+i,i+1];
B=Table[Table[0, {i,b2}], {j,b3}];
segbase=basemod[i+1,numgru];
Module[{k,k1,k2}, Do[ k={-1}+dif[segbase[[i]]];
      k2=Table[coef[k[[k1]]], {k1,2,Length[k]}];
      Do[
B=ReplacePart[B,k2[[j,1]],{i,conversion[i,numgru][k2[[j,2]]]}],
{j, Length[k2]}], {i, b3}]; ];
SetAttributes[Plus,Listable]; SetAttributes[Times,Listable];
fnsa2=ExtendedSmithForm[B];
ClearAttributes[Plus,Listable]; ClearAttributes[Times,Listable];
homologia=Select[Table[fnsa2[[1,ji,ji]], {ji, b2}],#1>0&];
Print["La homología en grado ",i," es
Z^",nucleo-Length[Select[homologia,#1>1&],"  +  ",
      "Z_",Select[homologia,#1>1&]];
```

En el capítulo 3 este procedimiento se restringirá a el cálculo de las homologías en grados 1 y 2 de grupos finitos, para la búsqueda de matrices cocíclicas de Hadamard.

Cronológicamente, primero abordaremos la caracterización de modelos (co)homológicos para extensiones centrales y productos semidirectos de grupos abelianos finitos, por separado, para después atacar el problema de productos iterados de los mismos.

2.3 (Co)homología de extensiones centrales

En el artículo [83] Lambe y Stasheff describen, bajo ciertas condiciones, un procedimiento para construir un modelo homológico de una fibración (iterada) a partir de modelos homológicos conocidos de los factores integrantes de la fibración.

Más concretamente, según [8] toda fibración $F \to E \to B$ posee una factorización en forma de producto cartesiano torcido $B \times_\tau F$ (normalmente no principal). En estas circunstancias, Lambe y Stasheff demuestran que dada una fibración iterada $X = E_n \to E_{n-1} \to \cdots E_0 \to E_{-1} = *$ de modo que la cocadena de torsión τ_i a la que da lugar cada fibración simple $F_i \to E_i \to E_{i-1}$ se anula sobre 1-símplices, entonces X presenta un modelo homológico en función de modelos homológicos hF_i de las fibras F_i; el cual posee una A_∞-estructura de coálgebra naturalmente heredada de $C_*(X)$.

La idea que ellos siguen es, de manera recursiva, perturbar el producto de las contracciones que establecen los modelos homológicos según la diferencial obtenida al aplicar el Teorema de Eilenberg-Zilber torcido al producto cartesiano torcido asociado a la fibración correspondiente. La condición de parada de la perturbación resulta de la condición de anulación sobre 1-símplices de las cocadenas de torsión que entran en juego.

En este mismo artículo, ambos autores proponen un modelo homológico para extensiones centrales $G \ltimes_f A \equiv 1 \rightarrowtail A \rightarrowtail K \twoheadrightarrow G \twoheadrightarrow 1$ de 2-cociclo $f : G \times G \to A$, mediante el producto cartesiano torcido que surge al tomar el *pullback* del fibrado universal $\bar{W}(G) \to W^2(A) \to \bar{W}^2(A)$ vía la aplicación $k_f : \bar{W}(G) \to \bar{W}^2(A)$ que genera f; de modo que la función de torsión de tal producto cartesiano resulta ser la composición de k_f con la cocadena universal $\bar{W}^2(A) \xrightarrow{t} \bar{W}(A)$. Aquí, $\bar{W}$ denota el funtor *clasificante geométrico*, a describir posteriormente, el cual asocia a cada

conjunto simplicial X otro nuevo conjunto simplicial $\bar{W}(X)$.

En [100] se recoge una aproximación similar, pero por medio de un isomorfismo simplicial del clasificante geométrico de la extensión central $A_f \rtimes G$ al clasificante geométrico de un producto cartesiano torcido $A \times_\tau G$ adecuado. Ésta será la aproximación que tratemos nosotros aquí, pormenorizando las estructuras subyacentes en los objetos que intervienen en la determinación del modelo homológico.

Teniendo en cuenta la biyección que describimos en la sexta sección del capítulo primero, vamos a tratar las extensiones centrales $A_f \rtimes G$ de A por G a partir de 2-cociclos normalizados $f : G \times G \to A$,

$$f(a,b) + f(ab,c) = f(a,bc) + f(b,c), \qquad f(a,1) = f(1,a) = 0;$$

de modo que la ley de grupo vendrá dada por

$$(a,g)(a',g') = (a + a' + f(g,g'), gg').$$

2.3.1 Modelo homológico

En esta sección vamos a describir un modelo homológico para ciertas extensiones centrales $A_f \rtimes G$, progresando sobre el trabajo de Rubio en [100]. Hemos de aclarar que aunque en [100] se determina la existencia de un modelo homológico para $A_f \rtimes G$, sólo se describe explícitamente el isomorfismo simplicial (2.12), dirigiendo al interesado en el resto de detalles a [99], donde se realiza un tratamiento para fibraciones en general. Siguiendo la argumentación que ahí se expone, nosotros vamos a reproducir una demostración completa para el caso particular de extensiones con A abeliano y G grupo con modelo homológico conocido. El motivo no es otro que progresar sobre éste para describir, a continuación, un modelo cohomológico para extensiones centrales $A_f \rtimes G$ de grupos A y G abelianos finitos.

Para ello, será necesario hacer un pequeño recorrido entre diversos isomorfismos y contracciones, que describiremos a lo largo de la presente sección:

1. Isomorfismo $\bar{B}(\mathbb{Z}[A_f \rtimes G]) \cong C_*(\bar{W}(A_f \rtimes G))$.

2. Isomorfismo $C_*(\bar{W}(A_f \rtimes G)) \cong C_*(\bar{W}(A) \times_\tau \bar{W}(G))$.

3. Contracción $C_*(\bar{W}(A) \times_\tau \bar{W}(G)) \Rightarrow C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G))$.

4. Contracción $C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G)) \Rightarrow hA \tilde{\otimes} hG$.

Abordaremos este estudio desde el punto de vista de la *Teoría de Perturbación Homológica* [111, 14, 106, 83, 47, 48, 107, 98]. Será necesario introducir asimismo algunas nociones básicas relacionadas con la *Topología Simplicial* [91]. En particular, haremos uso de la definición de homología de un grupo discreto a partir del *espacio clasificante* o *clasificante geométrico* canónicamente asociado a su versión simplicial (ver [91]).

Comencemos recordando la definición clásica de *conjunto simplicial*, que no es más que un conjunto K graduado en $\mathbb{Z}^+$, $K = \{K_0, K_1, \ldots, K_n, \ldots\}$, junto con dos familias de funciones $\partial_i : K_q \to K_{q-1}$ y $s_i : K_q \to K_{q+1}$, $0 \leq i \leq q$; verificándose las identidades:

$$\begin{aligned}
\partial_i \partial_j &= \partial_{j-1} \partial_i, \quad \text{si } i < j; \\
s_i s_j &= s_{j+1} s_i, \quad \text{si } i \leq j; \\
\partial_i s_j &= s_{j-1} \partial_i, \quad \text{si } i < j; \\
\partial_i s_j &= s_j \partial_{i-1}, \quad \text{si } i > j+1; \\
\partial_j s_j &= 1_K = \partial_{j+1} s_j.
\end{aligned}$$

Los elementos de K_q se llaman *q-símplices*. Las aplicaciones ∂_i y s_i se denominan operadores de *cara* y de *degeneración*, respectivamente. Un símplice x se dice *degenerado* cuando $x = s_i z$, para algún símplice z y operador de degeneración s_i; en caso contrario, el símplice x se denomina *no degenerado*.

El *clasificante geométrico* $\bar{W}(G)$ de un grupo simplicial $(G, +)$ consiste en el conjunto simplicial definido como sigue:

$$\begin{aligned}
\bar{W}_0(G) &= \{[\,]\}; \\
\bar{W}_n(G) &= G_{n-1} \times \cdots \times G_0, \quad n > 0; \\
s_0[\,] &= [e_0]; \\
\partial_i[g_0] &= [\,], \quad i = 0, 1; \\
\partial_0[g_n, \ldots, g_0] &= [g_{n-1}, \ldots, g_0], \\
\partial_{i+1}[g_n, \ldots, g_0] &= [\partial_i g_n, \ldots, \partial_1 g_{n-i+1}, g_{n-i-1} + \partial_0 g_{n-i}, g_{n-i-2}, \ldots, g_0], \\
s_0[g_{n-1}, \ldots, g_0] &= [e_n, g_{n-1}, \ldots, g_0], \\
s_{i+1}[g_n, \ldots, g_0] &= [s_i g_n, \ldots, s_0 g_{n-i}, e_{n-i}, g_{n-i-1}, \ldots, g_0];
\end{aligned}$$

donde [ ] denota el único elemento de $\bar{W}_0(G)$, e_n corresponde al elemento identidad de G_n y $[g_{n-1}, \ldots, g_0]$ es un elemento genérico de $\bar{W}_n(G)$, para $n > 0$.

Cuando se trata de un grupo discreto G, por abuso del lenguaje, se considera que el clasificante asociado a G es el clasificante geométrico ${}^sG$ asociado al grupo simplicial canónicamente asociado a G; que no es más que el grupo simplicial dado por ${}^sG_n = G$ para todo $n \geq 0$, y con el homomorfismo identidad por operadores simpliciales de cara y de degeneración.

La homología de un grupo simplicial (o discreto) puede definirse como la homología del objeto $\bar{W}(G)$, como veremos a continuación.

Por otra parte, dado un conjunto simplicial K, el Λ módulo simplicial libre generado por K, $\Lambda[K]$, se define como el módulo simplicial dado por

$$\Lambda[K]_n = \Lambda[K_n],$$

de manera que sus operadores de cara y de degeneración son los morfismos de Λ-módulos inducidos por los operadores propios de K.

Se denomina complejo de cadenas asociado a un conjunto simplicial K, y se denota $C_*(K)$, al DG-módulo asociado a $\Lambda[K]$, cuya diferencial consiste en la suma alternada de los operadores de cara. En este caso, la homología de K, $H_*(K)$, viene dada por

$$H_n(K) = H_n(C_*(K)), \qquad \forall n \geq 0.$$

Hemos de hacer hincapié en el hecho de que la homología de un grupo simplicial (o discreto) G se puede obtener como la homología del complejo de cadenas asociado al clasificante geométrico de G, $C_*(\bar{W}(G))$, dado que éste es isomorfo a $\bar{B}(\mathbb{Z}[G])$ (ver [91, 15]).

Concretamente, si el grupo G es abeliano, $C_*(\bar{W}(G))$ y $\bar{B}(\mathbb{Z}[G])$ resultan ser trivialmente isomorfos:

$$\begin{array}{ccc} \bar{B}(\mathbb{Z}[G]) & \to & C_*(\bar{W}(G)) \\ [g_n, \ldots, g_0] & \mapsto & (g_n, \ldots, g_0). \end{array}$$

Si el grupo G no es abeliano, como es nuestro caso, entonces se tiene el siguiente

isomorfismo (ver [4]):

$$\begin{array}{rccc} \varphi_1: & \bar{B}(\mathbb{Z}[G]) & \to & C_*(\bar{W}(G)) \\ & [g_0,\ldots,g_n] & \mapsto & (-1)^{\lceil \frac{n}{2} \rceil + 1}(g_n,\ldots,g_0). \end{array} \tag{2.11}$$

Sean ahora B un conjunto simplicial y G un grupo simplicial. Una *función de torsión* ó *torsión geométrica* $\tau : B_* \longrightarrow G_{*-1}$ es una familia de aplicaciones verificando las condiciones siguientes:

$$\begin{array}{rcl} \partial_0\tau(b) & = & [\tau(\partial_0 b)]^{-1}\tau(\partial_1 b); \\ \partial_i\tau(b) & = & \tau(\partial_{i+1}b), \quad \text{para } i > 0; \\ s_i\tau(b) & = & \tau(s_{i+1}b), \quad \text{para } i \geq 0; \\ \tau(s_0 b) & = & e_n; \end{array}$$

donde e_n es el elemento neutro del grupo G_n correspondiente.

Sean F y B dos conjuntos simpliciales y G un grupo simplicial que actúa a izquierda de F, es decir, de modo que existe un morfismo simplicial $* : G \times F \to F$ verificando $e_q * x = x$ y $g_1 * (g_2 * x) = (g_1 g_2) * x$, con $x \in F$ y $g_1, g_2 \in G$. Dada una función de torsión $\tau : B \to G$, se puede definir el *producto cartesiano torcido (PCT) de fibra F, base B, grupo estructural G, de acción $*$ de G sobre F y función de torsión τ* como el conjunto simplicial $F \times_\tau B$ dado por:

$$\begin{array}{rcll} (F \times_\tau B)_n & = & F_n \times B_n; & \\ \partial_0(f,b) & = & (\tau b * \partial_0 f, \partial_0 b); & \\ \partial_i(f,b) & = & (\partial_i f, \partial_i b), & \text{para } i > 0; \\ s_i(f,b) & = & (s_i f, s_i b), & \text{para } i \geq 0. \end{array}$$

En el caso de que $F = G$, se habla de *producto cartesiano torcido principal*, o simplemente (PCTP).

A partir de una extensión central $A_f \rtimes G$, consideremos el producto tensorial torcido $\bar{W}(A) \times_\tau \bar{W}(G)$ definido por la función de torsión

$$\tau : \bar{W}(G) \to \bar{W}(A),$$

que actúa trivialmente en grado 1 ($\tau[g_0] = 0$) y para $n > 1$ viene dada por

$$\tau[g_{n-1},\ldots,g_0] = [-f(g_{n-2},g_{n-1}), -f(g_{n-3},g_{n-2}g_{n-1}) + f(g_{n-3},g_{n-2}),\ldots,$$

$$-f(g_0, g_1 \cdots g_{n-1}) + f(g_0, g_1 \cdots g_{n-2})];$$

con grupo estructural G de acción κ determinada por la ley interna de $\bar{W}(A)$,

$$\kappa : \bar{W}(A) \times \bar{W}(A) \to \bar{W}(A),$$

que consiste en la operación de A componente a componente (nótese que esta operación es asociativa por ser A un grupo abeliano).

En estas circunstancias, se tiene el siguiente resultado.

Teorema 2.3.1 *[100] Existe un isomorfismo simplicial*

$$\varphi_2 : \bar{W}(A_f \rtimes G) \longrightarrow \bar{W}(A) \times_\tau \bar{W}(G), \tag{2.12}$$

dado por

$$\varphi_2[(a_{n-1}, g_{n-1}), \ldots, (a_0, g_0)] =$$

$$= ([a_{n-1}, a_{n-2} + f(g_{n-2}, g_{n-1}), \ldots, a_{n-i} + f(g_{n-i}, g_{n-i+1} \cdots g_{n-1}),$$

$$\ldots, a_0 + f(g_0, g_1 \cdots g_{n-2} g_{n-1})], [g_{n-1}, \ldots, g_0]).$$

La aplicación inversa φ_2^{-1} resulta ser

$$\varphi_2^{-1}([a_{n-1}, \ldots, a_0], [g_{n-1}, \ldots, g_0]) =$$

$$[(a_{n-1}, g_{n-1}), (a_{n-2} - f(g_{n-2}, g_{n-1}), g_{n-2}), \ldots, (a_{n-i} - f(g_{n-i}, g_{n-i+1} \cdots g_{n-2} g_{n-1}), g_{n-i}),$$

$$\ldots, (a_0 - f(g_0, g_1 \cdots g_{n-2} g_{n-1}), g_0)].$$

El siguiente paso para encontrar el modelo homológico de una extensión central hace uso del teorema de Eilenberg-Zilber, que permite relacionar estructuras geométrico combinatorias (módulos simpliciales) y estructuras algebraicas (los complejos de cadenas asociados) a partir de los morfismos que describimos a continuación.

Sean K y L dos Λ-módulos simpliciales aumentados. Consideremos los morfismos Alexander-Whitney,

$$AW : (K \times L)_N \to K_N \otimes L_N;$$

Eilenberg-Mac Lane,

$$EML : K_N \otimes L_N \to (K \times L)_N;$$

y Shih[3],

$$SHI : (K \times L)_N \to (K \times L)_N;$$

aplicaciones que vienen dadas en grados positivos por las fórmulas:

$$\begin{aligned} AW(a_n \times b_n) &= \sum_{i=0}^{n} \partial_{i+1} \cdots \partial_n a_n \otimes \partial_0 \cdots \partial_{i-1} b_n, \\ EML(a_p \otimes b_q) &= \sum_{(\alpha,\beta)\in\{(p,q)-shuffles\}} (-1)^{sg(\alpha,\beta)} (s_{\beta_q} \cdots s_{\beta_1} a_p \times s_{\alpha_p} \cdots s_{\alpha_1} b_q), \\ SHI(a_n \times b_n) &= \sum (-1)^{m+sg(\alpha,\beta)} (s_{\beta_q+m} \cdots s_{\beta_1+m} s_{m-1} \partial_{n-q+1} \cdots \partial_n a_n \times \\ &\qquad \times s_{\alpha_{p+1}+m} \cdots s_{\alpha_1+m} \partial_m \cdots \partial_{m+p-1} b_n); \end{aligned}$$

donde $m = n - p - q$, $sg(\alpha, \beta) = \sum_{i=1}^{p} (\alpha_i - (i-1))$, y la última suma se toma sobre índices $0 \leq q \leq n-1$, $0 \leq p \leq n-q-1$ y $(\alpha, \beta) \in \{(p+1, q)\text{-shuffles}\}$.

En grado 0, los homomorfismos AW y EML se definen como $AW(a_0 \times b_0) = a_0 \otimes b_0$ y $EML(a_0 \otimes b_0) = (a_0 \times b_0)$; por otro lado, el operador de homotopía, SHI, coincide con la aplicación idénticamente nula actuando sobre elementos de grado 0.

En estas condiciones, se tienen los siguientes resultados.

Teorema 2.3.2 (de Eilenberg-Zilber) *[38, 35] Sean X e Y dos conjuntos simpliciales. Entonces, el conjunto de datos*

$$EZ_{C_*(X),C_*(Y)} : \{C_*(X \times Y),\ C_*(X) \otimes C_*(Y),\ AW,\ EML,\ SHI\} \tag{2.13}$$

conforma una contracción.

Si se introduce una perturbación en $C_*(X \times Y)$ mediante una función de torsión τ, en [14] se prueba la existencia de la llamada *contracción Eilenberg-Zilber torcida*, que notaremos simplemente por $EZ^{\tau}_{F,B}$.

Teorema 2.3.3 (de Eilenberg-Zilber Torcido) *[14]*
Si $F \times_\tau B$ es un producto cartesiano torcido según una función de torsión τ, entonces el complejo de cadenas $C_*(F \times_\tau B)$ admite una contracción hasta un producto tensorial "torcido" $C_*(F) \otimes_{t(\tau)} C_*(B)$.

[3]Obsérvese que éste es el mismo morfismo que aparecía en la factorización del operador de homotopía de la contracción (2.3).

De manera que τ induce una perturbación que da lugar a una diferencial modificada d_δ en $C_*(F) \otimes_{t(\tau)} C_*(B)$.

Así se puede obtener el morfismo t de módulos graduados de grado -1 definido por la composición $t = p \circ d_\delta \circ i$,

$$C_*^N(B) \xrightarrow{i} C_*^N(G) \otimes C_*^N(B) \xrightarrow{d_\delta} C_*^N(G) \otimes C_*^N(B) \xrightarrow{p} C_*^N(G),$$

donde

$$i(x) = e_0 \otimes x, \quad e_0 \text{ elemento neutro de } G_0;\ p(y \otimes x) = y \cdot \xi_{C_*^N(B)} x. \tag{2.14}$$

Sean A una DGA-álgebra y C una DGA-coálgebra. Se denomina *cocadena de torsión* (ó, también, *cocadena de Brown*), a un morfismo de módulos graduados de grado -1, $t : C \to A$, de modo que:

$$d_A t + t d_C + t \cup t = 0, \quad \xi_A t = 0, \quad t\eta_C = 0;$$

donde $t \cup t = \pm(t *_A t)\Delta_C$.

Dados M un DGA-módulo a derecha sobre una DGA-álgebra A, N un DGA-comódulo a izquierda sobre una DGA-coálgebra C y $t : C \to A$ una cocadena de torsión, se puede definir:

$$d_t : M \otimes N \longrightarrow M \otimes N$$

mediante

$$d_t(x \otimes y) = d(x \otimes y) + t \cap x \otimes y,$$

donde

$$t \cap x \otimes y = (1_M *_M t \otimes 1_N)(1_M \otimes \Delta_N)(x \otimes y);$$

de manera que d_t es una diferencial y $M \otimes N$, dotado de esta diferencial y de la aumentación y coaumentación definidas para el producto tensorial, es un DGA-módulo, $M \otimes_t N$, conocido como *producto tensorial torcido por la cocadena t*.

Análogamente, podría haberse tomado M DGA-módulo a izquierda de A y N DGA-comódulo a derecha de C, de modo que aparece $d_t = 1 \otimes d + d \otimes 1 + t\cap$, diferencial sobre $N \otimes M$, con

$$t\cap = (1_N \otimes t *_M 1_M)(\Delta_N \otimes 1_M).$$

Hemos de hacer notar que para que d_t constituya de hecho una diferencial en los productos tensoriales torcidos anteriores, es necesario que el signo de $t \cup t = \pm(t *_A t)\Delta_C$ sea positivo en el caso de tomar $N \otimes_t M$, y negativo en el caso de tomar $M \otimes_t N$.

Esto no es óbice para definir una cocadena de torsión salvo signo, dado que si t es cocadena de torsión para $C \otimes_t A$, entonces $-t$ es cocadena de torsión para $A \otimes_t C$; y recíprocamente:

$$d_A t + t d_C + (t *_A t)\Delta_C = 0 \Rightarrow d_A(-t) + (-t)d_C + ((-t) *_A (-t))\Delta_C = 0.$$

De este modo, el morfismo $t(\tau) : C_*(B) \to C_*(G)$ definido anteriormente resulta ser una cocadena de torsión inducida por la función de torsión τ (ver [111]).

En nuestro caso, la fibra viene dada por $\bar{W}(A)$ y la base por $\bar{W}(G)$, de manera que partimos de la contracción de Eilenberg-Zilber

$$EZ_{C_*(\bar{W}(A)),C_*(\bar{W}(G))} : \{C_*(\bar{W}(A) \times \bar{W}(G)),\ C_*(\bar{W}(A)) \otimes C_*(\bar{W}(G)),\ AW,\ EML,\ SHI\}.$$

Si se toma como dato de perturbación:

$$\begin{array}{rccl} \delta & : C_*(\bar{W}(A) \times \bar{W}(G)) & \to & C_*(\bar{W}(A) \times \bar{W}(G)) \\ & (\bar{a}, \bar{g}) & \mapsto & (\tau(\bar{g}) + \partial_0 \bar{a}, \partial_0 \bar{g}) - (\partial_0 \bar{a}, \partial_0 \bar{g}), \end{array} \tag{2.15}$$

según (2.3.3) se tiene la siguiente contracción

$$EZ^{\tau}_{\bar{W}(A),\bar{W}(G)} : \{C_*(\bar{W}(A) \times_\tau \bar{W}(G)), C_*(\bar{W}(A) \otimes_{t(\tau)} C_*(\bar{W}(G)), AW_\tau, EML_\tau, SHI_\tau\},$$

siendo los morfismos AW_τ, EML_τ y SHI_τ los obtenidos a partir de AW, EML y SHI mediante el Lema Básico de Perturbación (Teorema 2.1.1).

La diferencial generada en $C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G))$ mediante la contracción (2.15) resulta ser:

$$d_t = 1 \otimes d + d \otimes 1 + t\cap,$$

con

$$t\cap = (1 * t \otimes 1)(1 \otimes \Delta).$$

Denotamos por d_δ la diferencial obtenida según el Lema Básico de Perturbación en $C_*(\bar{W}(A)) \times_t C_*(\bar{W}(G))$,

$$d_\delta = AW\delta \sum_{i \geq 0} (-1)^i (SHI\ \delta)^i EML. \tag{2.16}$$

En estas circunstancias Shih demostró el siguiente resultado.

Teorema 2.3.4 *[111] Dado un producto cartesiano torcido $F \times_\tau B$ con grupo estructural G, el morfismo $t : C^N_*(B) \longrightarrow C^N_*(G)$ definido previamente es una cocadena de torsión, verificando además que $d_\delta = t \cap$.*

Llegados a este punto, sólo nos resta un último paso para determinar un modelo homológico para la extensión central $A_f \rtimes G$. Para llevarlo a cabo, basta conocer las contracciones que dan el modelo homológico de los grupos A y G en que factoriza dicha extensión central,

$$c_G : \{C_*(\bar{W}(G)), hG, f_G, g_G, \phi_G\} \quad \text{y} \quad c_A : \{C_*(\bar{W}(A)), hA, f_A, g_A, \phi_A\}.$$

Teniendo en cuenta la contracción (2.5), resulta

$$c_\otimes : \{C_*(\bar{W}(A)) \otimes C_*(\bar{W}(G)), hA \otimes hG, f_A \otimes f_G, g_A \otimes g_G, 1 \otimes \phi_G + \phi_A \otimes g_G f_G\}.$$

Si perturbamos según el dato $t\cap$, obtenemos una nueva contracción

$$c_{t\cap} : \{C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G)), hA \tilde{\otimes} hG, f_{t\cap}, g_{t\cap}, \phi_{t\cap}\},$$

donde:

$$f_{t\cap} = (f_A \otimes f_G)(1 - t\cap \sum_{i\geq 0}(-1)^i((1 \otimes \phi_G + \phi_A \otimes g_G f_G)t\cap)^i(1 \otimes \phi_G + \phi_A \otimes g_G f_G),$$

$$g_{t\cap} = \sum_{i\geq 0}(-1)^i((1 \otimes \phi_G + \phi_A \otimes g_G f_G)t\cap)^i(g_A \otimes g_G),$$

$$\phi_{t\cap} = \sum_{i\geq 0}(-1)^i((1 \otimes \phi_G + \phi_A \otimes g_G f_G)t\cap)^i(1 \otimes \phi_G + \phi_A \otimes g_G f_G).$$

Veamos que el proceso de perturbación es convergente (esto es, que $\phi\, t\cap$ es puntualmente nilpotente).

Para demostrar esta convergencia, podemos basarnos en un argumento clásico, ya utilizado por May en [90]. Supongamos en primer lugar que la cocadena de torsión t se anula sobre elementos de grado 1. En este caso, Δ tiene que "romper" los elementos de manera que deje al menos 2 a la izquierda, para que la actuación de t no sea nula. Por tanto, $t\cap = (1 * t \otimes 1)(1 \otimes \Delta)$, disminuirá al menos en 2 la gradación simplicial en la segunda componente, propia de G. Por otra parte, es claro que $1 \otimes \phi_G$ aumenta en uno dicho grado simplicial, mientras que $\phi_A \otimes g_G f_G$ no lo modifica. De donde el

proceso converge, pues la composición $(1 \otimes \phi_G + \phi_A \otimes g_G f_G)t\cap$ disminuye al menos en uno la gradación simplicial en cada paso.

Veamos que efectivamente t sobre un elemento de grado 1 es cero. Recordemos que $t = pd_\delta i$. Si t actúa sobre un elemento (g_0) de grado 1, en primer lugar actúa la inyección i, de modo que:

$$i(g_0) = (( ) \otimes (g_0)).$$

A continuación, teniendo en cuenta la expresión de d_δ dada en (2.16) , actúa EML:

$$EML(( ) \otimes (g_0)) = ((0), (g_0)).$$

El siguiente morfismo que actúa es δ, de modo que, como τ y ∂_0 bajan un grado, lleva el elemento de grado 1 a grado cero. Así:

$$\delta((0), (g_0)) = (( ), ( )) - (( ), ( )) = 0.$$

Con todo esto, el proceso seguido hasta encontrar un modelo homológico de una extensión central $A_f \rtimes G$ se puede resumir en el siguiente esquema:

$$\bar{B}(\mathbb{Z}[A_f \rtimes G]) \overset{\varphi_1}{\Rightarrow} C_*(\bar{W}(A_f \rtimes G)) \overset{\varphi_2}{\Rightarrow} C_*(\bar{W}(A) \times_\tau \bar{W}(G)) \overset{EZ^\tau_{\bar{W}(A),\bar{W}(G)}}{\Rightarrow}$$
$$\overset{EZ_{\bar{W}(A),\bar{W}(G)}}{\Rightarrow} C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G)) \overset{C_{t\cap}}{\Rightarrow} hA \tilde{\otimes} hG$$

De manera que la contracción llevada a cabo:

$$c_{A_f \rtimes G} : \{\bar{B}(\mathbb{Z}[A_f \rtimes G]), hA \tilde{\otimes} hG, f, g, \phi\}, \tag{2.17}$$

viene dada por los morfismos siguientes:

$$f = f_{t\cap} AW_\tau \varphi_2 \varphi_1$$
$$g = \varphi_1^{-1} \varphi_2^{-1} EML_\tau g_{t\cap}$$
$$\phi = \varphi_1^{-1} \varphi_2^{-1} SHI_\tau \varphi_2 \varphi_1 + \varphi_1^{-1} \varphi_2^{-1} EML_\tau \phi_{t\cap} AW_\tau \varphi_2 \varphi_1.$$

Y la diferencial del homológico será $\tilde{d} = d_{hA} \otimes 1 + 1 \otimes d_{hG} + d_\infty$, donde d_∞ viene definido según el lema de perturbación de la siguiente forma:

$$d_\infty = (f_A \otimes f_G)t \cap \sum_{i \geq 0} (-1)^i ((1 \otimes \phi_G + \phi_A \otimes g_G f_G)t\cap)^i (g_A \otimes g_G).$$

Así, se ha probado la validez del resultado siguiente, que no es sino un caso particular del trabajo más general de [99, 100].

Teorema 2.3.5 *La contracción (2.17) establece un modelo homológico para la extensión central $A_f \rtimes G$, con A abeliano (no necesariamente finito) y G grupo con modelo homológico conocido.*

Nosotros nos centraremos en el caso A y G ambos abelianos finitos.

Abordemos ahora el estudio de un modelo cohomológico para estos grupos.

2.3.2 Modelo cohomológico

A la hora de diseñar un modelo cohomológico para $A_f \rtimes G$, con A y G abelianos finitos, procedemos según los pasos siguientes:

1. Aplicamos primero el funtor Hom a la contracción (2.17), para obtener

$$c^*_{A_f \rtimes G} : \{\mathrm{Hom}(\bar{B}(\mathbb{Z}[A_f \rtimes G]), \mathbb{Z}), \mathrm{Hom}(hA \tilde{\otimes} hG, \mathbb{Z}), g^*, f^*, \phi^*\}. \qquad (2.18)$$

   Nótese que si $\tilde{d} = d_{hA} \otimes 1 + 1 \otimes d_{hG} + d_\infty$ es la diferencial sobre $hA \tilde{\otimes} hG$, entonces $\tilde{\partial}$ definida como $\tilde{\partial}(f) = f \circ \tilde{d}$ es la diferencial sobre $\mathrm{Hom}(hA \tilde{\otimes} hG, \mathbb{Z})$. En particular, es fácil ver que $\tilde{\partial} = \partial + \partial_\infty$, donde $\partial(f) = f \circ (d_{hA} \otimes 1 + 1 \otimes d_{hG})$ y $\partial_\infty(f) = f \circ d_\infty$; de donde $\tilde{\partial}$ surge por la perturbación de la diferencial usual ∂ según el dato ∂_∞.

2. A partir del isomorfismo F de (2.9), formamos la isocontracción banal

$$c_F : \{\mathrm{Hom}(hA \otimes hG, \mathbb{Z}), \bigotimes_{i \in I} (E(u_i) \otimes P(v_i)), F, F^{-1}, 0\}, \qquad (2.19)$$

   donde cada $\mathbb{Z}_{n_i}$ en que se descomponen A y G aporta una pareja $E(u_i) \otimes P(v_i)$. Más concretamente, sea $A = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_s}$ y $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$, y denotemos por $A_{k_i} = A_{k_i}(v_{k_i}, 1)$ al par $E(u_{k_i}, 1) \otimes \Gamma(w_{k_i}, 2)$ que corresponde al factor $\mathbb{Z}_{k_i}$ en el modelo homológico de $A_f \rtimes G$; de modo que $v^j_{k_i} = u^{j \,(mod\, 2)}_{k_i} \otimes w^{\lfloor \frac{j}{2} \rfloor}_{k_i}$. En estas circunstancias, una versión más explícita del isomorfismo (2.9) es

$$\begin{array}{rccc} F: & \mathrm{Hom}(A_{m_1} \otimes \cdots \otimes A_{n_t}, \mathbb{Z}) & \to & A^*_{m_1} \otimes \cdots \otimes A^*_{n_t} \\ & f & \mapsto & \sum_{f(v_{m_1}, \ldots, v_{n_t}) \neq 0} f(v_{m_1}, \ldots, v_{n_t}) \cdot v^*_{m_1} \otimes \cdots \otimes v^*_{n_t}, \\ & f_{m_1} *_{\mathbb{Z}} \cdots *_{\mathbb{Z}} f_{n_t} & \leftarrow\!\shortmid & f_{m_1} \otimes \cdots \otimes f_{n_t}. \end{array}$$

3. Ahora sólo queda perturbar la contracción (2.19) anterior según ∂_∞ y componer el resultado con (2.18), para así obtener

$$c : \{\mathrm{Hom}(\bar{B}(\mathbb{Z}[A_f \rtimes G]), \mathbb{Z}), \tilde{\bigotimes_{i\in I}}(E(u_i) \otimes P(v_i)), f, g, \phi\}. \tag{2.20}$$

Dado que (2.19) es una isocontracción, el proceso de perturbación se reduce a modificar la diferencial usual de $A^*_{m_1} \otimes \cdots \otimes A^*_{n_t}$, resultando

$$\tilde{d}^* = \left(\sum_{i=1}^{s} 1^{\otimes i-1} \otimes d_{A^*_{m_i}} \otimes 1^{\otimes s-i}\right) + \left(\sum_{j=1}^{t} 1^{\otimes j-1} \otimes d_{A^*_{n_j}} \otimes 1^{\otimes t-j}\right) + F \circ \partial_\infty \circ F^{-1}.$$

De este modo, queda probado el siguiente resultado.

Teorema 2.3.6 *La contracción (2.20) establece un modelo cohomológico para la extensión central $A_f \rtimes G$, con A y G grupos abelianos (no necesariamente finitos).*

Evidentemente, este esquema también funciona en el caso A y G grupos abelianos en general, no necesariamente finitos: basta considerar el modelo homológico correspondiente de cada factor $\mathbb{Z}$ ó $\mathbb{Z}_{n_i}$ en que se descompongan A y G, respectivamente. Para otros grupos A y G que no sean abelianos, pero tengan modelos homológicos conocidos, todo depende de la validez de los pasos segundo y tercero. Volveremos sobre esto más adelante, cuando tratemos el caso de productos iterados de extensiones centrales y productos semidirectos de grupos abelianos.

2.3.3 Computación y ejemplos

Lo primero que codificamos es el isomorfismo `isobar[1]`, $\bar{B}(\mathbb{Z}[H]) \simeq C_*(\bar{W}(H))$, para el caso de grupos discretos H no conmutativos. Recordemos que si H es conmutativo, $\bar{B}(\mathbb{Z}[H]) = C_*(\bar{W}(H))$, relación que notaremos con el morfismo identidad `isobar[0]`.

```
isobar[arb_][x_+y_]:=isobar[arb][x]+isobar[arb][y];
isobar[arb_][x_*y_]:=Expand[x*isobar[arb][y]]; isobar[arb_][0]:=0;
isobar[1][l_]:=(-1)^(Ceiling[Length[l]/2]+1)*Reverse[l];
isobar[0][l_]:=1;
```

El siguiente paso es implementar las aplicaciones `isoec` e `invisoec`, que conforman el isomorfismo de $C_*(\bar{W}(A_f \rtimes G))$ a $C_*(\bar{W}(A) \times_\tau \bar{W}(G))$. Los índices 4 y 5 que se utilizan en adelante hacen referencia a la forma en que viene dada la extensión central, $A_f \rtimes G$ ó $G \ltimes_f A$, respectivamente. Por motivos técnicos a explicar posteriormente, el 2-cociclo f se denota como `chi`.

Por otra parte, `carda` y `cardg` hacen referencia al cardinal de los grupos A y G, respectivamente. Los elementos del grupo $A \times G$ se ordenan de manera natural según las filas de la matriz $A \times G$,

$$\{(a_1, g_1), (a_1, g_2), \ldots, (a_1, g_n), \ldots, (a_m, g_n)\},$$

y siguiendo la notación que hemos establecido se numeran desde 1 a $|A| \cdot |G|$, siendo 1 el elemento unidad. De este modo, el elemento i de $A \times G$ corresponde al par $(\lceil \frac{i}{|G|} \rceil, 1 + [i - 1 \ (mod\, |G|)])$.

```
isoec[ind_][x_+y_]:=isoec[ind][x]+isoec[ind][y];
isoec[ind_][x_*y_]:=Expand[x*isoec[ind][y]]; isoec[ind_][0]:=0;
isoec[ind_][{}]:={{},{}};
isoec[4][l_]:=Module[{k,n,x1,x2}, n=Length[l]; k ={}; Do[
        x1=Ceiling[l[[i]]/cardg]; x2=1+Mod[l[[i]]-1,cardg];
      k=Append[k,{x1,x2}], {i,n}]; k=Transpose[k]; {Prepend[Table[
      proda[k[[1,i]],chi[k[[2,i]],Fold[prodg,1,Reverse[
      Take[k[[2]],i-1]]]]],{i,2,n}],k[[1,1]]],k[[2]]}];
isoec[5][l_]:=Module[{k,n,x1,x2}, n=Length[l]; k={}; Do[
        x1=Ceiling[l[[i]]/cardg]; x2=1+Mod[l[[i]]-1,cardg];
      k=Append[k,{x1,x2}],{i,n}]; k=Transpose[k];
      {k[[1]],Prepend[Table[prodg[k[[2, i]],chi[k[[1, i]],
      Fold[proda,1,Reverse[Take[k[[1]],i-1]]]]],{i,2,n}],k[[2,1]]]}];
invisoec[ind_][x_+y_]:=invisoec[ind][x]+invisoec[ind][y];
invisoec[ind_][x_*y_]:=Expand[x*invisoec[ind][y]];
invisoec[ind_][0]:=0;
invisoec[ind_][{{},{}}]:={};
invisoec[4][l_]:=Module[{k}, k=Prepend[Table[{proda[l[[1,i]],inversos[
       [chi[l[[2,i]],Fold[prodg,1,Reverse[Take[l[[2]],i-1]]]]]]],
      l[[2,i]]}, {i,2,Length[l[[1]]]}],{l[[1,1]],l[[2, 1]]}];
      Table[(k[[i,1]]-1)*cardg+k[[i,2]], {i, Length[k]}]];
invisoec[5][l_]:=Module[{k}, k=Prepend[Table[{l[[1,i]],prodg[l[[2,i]],
```

```
      inversos[[chi[l[[1,i]],Fold[proda,1,Reverse[Take[
    l[[1]],i-1]]]]]]]},{i,2,Length[l[[2]]]}],{l[[1,1]],l[[2,1]]}];
    Table[(k[[i,1]]-1)*cardg+k[[i,2]], {i,Length[k]}]];
```

A continuación definimos los morfismos que corresponden a la función de torsión τ y la perturbación asociada δ_τ, que llamamos `tauec` y `deltauec`. La función `deltauecsimple` devuelve aquellos términos en la imagen de $delta_\tau$ en los que interviene la función de torsión τ.

```
tauec[4][l_]:=Module[{k}, If[Length[l]<=1, k=0,
    k=Prepend[Table[proda[inversos[[chi[l[[i+2]],
      Fold[prodg,1,Reverse[Take[l,i+1]]]]]],
      chi[l[[i+2]],Fold[prodg,1,Reverse[Take[l,{2,i+1}]]]]],
    {i,Length[l]-2}],inversos[[chi[l[[2]],l[[1]]]]]]]; k];
tauec[5][l_]:=Module[{k}, If[Length[l]<=1, k=0,
    k=Prepend[Table[prodg[inversos[[chi[l[[i+2]],
      Fold[proda,1,Reverse[Take[l,i+1]]]]]],
      chi[l[[i+2]],Fold[proda,1,Reverse[Take[l,{2,i+1}]]]]],
    {i,Length[l]-2}],inversos[[chi[l[[2]],l[[1]]]]]]]; k];
deltauec[ind_][x_+y_]:=deltauec[ind][x]+deltauec[ind][y];
deltauec[ind][x_*y_]:=Expand[x*deltauec[ind][y]]; deltauec[ind_][0]=0;
deltauecsimple[ind_][x_+y_]:=deltauecsimple[ind][x]+
    deltauecsimple[ind][y];
deltauecsimple[ind_][x_*y_]:=Expand[x*deltauecsimple[ind][y]];
deltauecsimple[ind_][0]=0;
prodalista[ind_][0,l_]:=l;
prodalista[4][k_,l_]:=Table[proda[k[[i]],l[[i]]], {i,Length[k]}];
prodalista[5][k_,l_]:=Table[prodg[k[[i]],l[[i]]], {i,Length[k]}];
deltauecsimple[ind_][{{},{}}]:=0;
deltauecsimple[4][l_]:={prodalista[4][tauec[4][l[[2]]],Rest[l[[1]]]],
    Rest[l[[2]]]};
deltauecsimple[5][l_]:={Rest[l[[1]]],prodalista[5][tauec[5][l[[1]]],
    Rest[l[[2]]]]};
deltauec[4][l_]:=Module[{n,l1,l2,k}, l1=l[[1]]; l2=l[[2]];
    n=Length[l1]; If[n< 2||l2[[1]]==1, k=0,
      k=deltauecsimple[4][l]-{Rest[l1],Rest[l2]}]; k];
deltauec[5][l_]:=Module[{n,l1,l2,k}, l1=l[[1]]; l2=l[[2]];
```

```
n=Length[l2]; If[n<2||l1[[1]]==1, k=0,
  k=deltauecsimple[5][l]-{Rest[l1],Rest[l2]}]; k];
```

La aplicación `difteztec` representa la diferencial de $C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G))$, según el Teorema de Eilenberg-Zilber Torcido. La función auxiliar `orlar[ind]` permite seleccionar la mitad de los sumandos que devuelve EML, justamente aquellos que tienen por primeros elementos un 1 en la primera componente (propia de A), y un elemento distinto de 1 en la segunda componente (propia de G); en función del índice 4 ó 5 "ind".

```
orlar[ind_][x_+y_,ele_]:=orlar[ind][x,ele]+orlar[ind][y,ele];
orlar[ind_][x_*y_,ele_]:=x*orlar[ind][y,ele]; orlar[ind_][0,ele_]:=0;
orlar[3][l_,ele_]:={Append[l[[1]],ele],Prepend[l[[2]],1]};
orlar[4][l_,ele_]:={Prepend[l[[1]],1],Prepend[l[[2]],ele]};
orlar[5][l_,ele_]:={Prepend[l[[1]],ele],Prepend[l[[2]],1]};
compo[ind_][x_+y_]:=compo[ind][x]+compo[ind][y];
compo[ind_][x_*y_]:=x*compo[ind][y]; compo[ind_][0]:=0;
compo[ind_][l_]:=deltauec[ind][shi[1]];
sumatorio[l_]:=Apply[Plus,Table[(-1)^(i+1)*l[[i]], {i, Length[l]}]];
difteztec[ind_][x_+y_]:=difteztec[ind][x]+difteztec[ind][y];
difteztec[ind_][x_*y_]:=Expand[x*difteztec[ind][y]];
difteztec[ind_][0]:=0;
difteztec[4][l_]:=Module[{p,q,l1,l2,k}, l1=l[[1]]; l2=l[[2]];
p=Length[l1];
      q=Length[l2]; If[q==0||l2[[1]]==1, k=0,
        k=aw[sumatorio[NestWhileList[compo[4],(-1)^p*
        deltauecsimple[4][orlar[4][eml[nul2[{l1,Rest[l2]}]],l2[[1]]]],
        (#1=!=0)&]]]-(-1)^p*{l1, Rest[l2]}]; k];
difteztec[5][l_]:=Module[{p,q,l1,l2,k}, l1=l[[1]]; l2=l[[2]];
p=Length[l1];
      q=Length[l2]; If[p==0||l1[[1]]==1, k=0,
        k=aw[sumatorio[NestWhileList[compo[5],
        deltauecsimple[5][orlar[5][eml[nul2[{Rest[l1],l2}]],
        l1[[1]]]],(#1=!=0)&]]]-{Rest[l1],l2}]; k];
```

Ahora codificamos las aplicaciones `awec`, `emlec` y `shiec` propias de la contracción Eilenberg-Zilber torcida asociada a `deltauec`.

```
awec[ind_][x_+y_]:=awec[ind][x]+awec[ind][y];
awec[ind_][x_*y_]:=Expand[x*awec[ind][y]]; awec[ind_][0]:=0;
awec[ind_][l_]:=aw[sumatorio[NestWhileList[compo[ind],nul1[l],
      (#1=!=0)&]]];
emlec[ind_][x_+y_]:=emlec[ind][x]+emlec[ind][y];
emlec[ind_][x_*y_]:=Expand[x*emlec[ind][y]]; emlec[ind_][0]:=0;
emlec[4][l_]:=Module[{k,l1,l2}, l1=l[[1]]; l2=l[[2]]; k=eml[nul2[l]];
      If[Length[l2]==0||l2[[1]]==1, , k=k-shi[sumatorio[
        NestWhileList[compo[4],(-1)^Length[l1]*
        deltauecsimple[4][orlar[4][eml[nul2[{l1,Rest[l2]}]],
        l2[[1]]]],(#1=!=0)&]]]; k];
emlec[5][l_]:=Module[{k,l1,l2}, l1=l[[1]]; l2=l[[2]]; k=eml[nul2[l]];
      If[Length[l1]==0||l1[[1]]==1, , k=k-shi[sumatorio[
        NestWhileList[compo[5],deltauecsimple[5][orlar[5][
        eml[nul2[{Rest[l1],l2}]],l1[[1]]]],(#1=!=0)&]]]; k];
shiec[ind_][x_+y_]:=shiec[ind][x]+shiec[ind][y];
shiec[ind_][x_*y_]:=Expand[x*shiec[ind][y]]; shiec[ind_][0]:=0;
shiec[ind_][l_]:=shi[sumatorio[NestWhileList[compo[ind],nul1[l],
      (#1=!=0)&]]];
```

Para construir la diferencial del modelo, `difmodec`, así como los morfismos `fmodec`, `gmodec` y `fimodec` de la contracción final, es necesario predefinir los modelos homológicos hA y hG y las aplicaciones `fa`, `ga`, `fia` y `fg`, `gg`, `fig` que dan las contracciones a hA y hG, respectivamente. Vendrán dadas en función de los modelos de $\mathbb{Z}_n$ codificados con antelación.

```
compomodec[ind_][x_+y_]:=compomodec[ind][x]+compomodec[ind][y];
compomodec[ind_][x_*y_]:=Expand[x*compomodec[ind][y]];
compomodec[ind_][0]:=0;
compomodec[ind_][l_]:=difteztec[ind][fimodban[l]];
difmodec[ind_][x_+y_]:=difmodec[ind][x]+difmodec[ind][y];
difmodec[ind_][x_*y_]:=Expand[x*difmodec[ind][y]];
difmodec[ind_][0]:=0;
difmodec[ind_][l_]:=fmodban[sumatorio[NestWhileList[compomodec[ind],
      difteztec[ind][gmodban[l]],(#1=!=0)&]]];
fmodec[ind_][x_+y_]:=fmodec[ind][x]+fmodec[ind][y];
fmodec[ind_][x_*y_]:=Expand[x*fmodec[ind][y]]; fmodec[ind_][0]:=0;
```

```
fmodec[ind_][l_]:=fmodban[sumatorio[NestWhileList[
      compomodec[ind],l,(#1=!=0)&]]];
gmodec[ind_][x_+y_]:=gmodec[ind][x]+gmodec[ind][y];
gmodec[ind_][x_*y_]:=Expand[x*gmodec[ind][y]]; gmodec[ind_][0]:=0;
gmodec[ind_][l_]:=gmodban[l]-fimodban[sumatorio[NestWhileList[
      compomodec[ind],difteztec[ind][gmodban[l]],(#1=!=0)&]]];
fimodec[ind_][x_+y_]:=fimodec[ind][x]+fimodec[ind][y];
fimodec[ind_][x_*y_]:=Expand[x*fimodec[ind][y]]; fimodec[ind_][0]:=0;
fimodec[ind_][l_]:=fimodban[sumatorio[NestWhileList[
      compomodec[ind],l,(#1=!=0)&]]];
```

Para calcular homología basta utilizar la rutina que codifica el algoritmo de Veblen, que describiéramos en la sección previa.

Apliquemos el procedimiento para determinar la homología en dimensión 1 y 2 de los grupos $\mathbb{Z}_{2tf} \rtimes \mathbb{Z}_2$, para $t \in \mathbb{N}$ y $f(-1,-1) = \lceil \frac{t}{2} \rceil + 1$. En la salida incluimos las matrices que representan las diferenciales d_i respecto de las bases del modelo que da `basemod[i,2]`.

t	1	2	3	4	5
$M(d_2)$	$\begin{pmatrix} 2 & 0 \\ 0 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 \\ 0 & 0 \\ 2 & 2 \end{pmatrix}$	$\begin{pmatrix} 6 & 0 \\ 0 & 0 \\ 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 8 & 0 \\ 0 & 0 \\ 5 & 2 \end{pmatrix}$	$\begin{pmatrix} 10 & 0 \\ 0 & 0 \\ 6 & 2 \end{pmatrix}$
$M(d_3)$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & -2 & 0 \\ -1 & 2 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & -2 & 0 \\ -1 & 3 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & -2 & 0 \\ -1 & 5 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & -2 & 0 \\ -1 & 6 & 0 \end{pmatrix}$
H_1	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_4$	$\mathbb{Z}_{12}$	$\mathbb{Z}_{16}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$
H_2	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2$

A continuación, vamos a abordar la problemática análoga para el caso de productos semidirectos $A \ltimes_\chi G$.

2.4 (Co)homología de productos semidirectos

Tal como definiéramos en el capítulo primero, dados dos grupos A y G y una acción $\chi : G \times A \to A$ de G en A, el *producto semidirecto* $A \ltimes_\chi G$ de A y G consiste en el grupo resultante de considerar en $A \times G$ la operación producto definida por la regla:

$$(a, g) \cdot (a', g') = (a + \chi(g, a'), gg').$$

Se dice que la acción χ es distributiva o conforma una *acción de grupos* cuando satisface que

$$\chi(g, a + a') = \chi(g, a) + \chi(g, a') \qquad \forall\, g \in G,\ a, a' \in A.$$

Todos los productos semidirectos que consideremos estarán dotados de una acción de grupos.

Como ejemplo clásico de producto semidirecto de grupos podemos destacar el *grupo diédrico* $D_{2m} = \mathbb{Z}_m \ltimes \mathbb{Z}_2$, para $m \geq 2$, con

$$\chi : \mathbb{Z}_2 \times \mathbb{Z}_m \to \mathbb{Z}_m$$

tal que

$$\chi(a, b) = \begin{cases} b & \text{si} \quad a = 1, \\ -b & \text{si} \quad a = -1. \end{cases}$$

Es fácil comprobar que, así definida, χ constituye una acción de grupos.

Para simplificar la lectura en lo que sigue, notaremos $\chi(g, a)$ simplemente por ga.

2.4.1 Modelo homológico

En esta sección se describen los modelos homológicos para productos semidirectos $A \ltimes_\chi G$ que se hallaran en [3, 4, 1], con A grupo con modelo homológico conocido y G abeliano, no necesariamente finito.

Se seguirá un esquema análogo al utilizado en el estudio del modelo homológico de extensiones centrales descrito en la sección anterior:

1. Isomorfismo $\bar{B}(\mathbb{Z}[A \ltimes_\chi G]) \cong C_*(\bar{W}(A \ltimes_\chi G))$.
2. Isomorfismo $C_*(\bar{W}(A \ltimes_\chi G)) \cong C_*(\bar{W}(A) \times_\tau \bar{W}(G))$.
3. Contracción $C_*(\bar{W}(A) \times_\tau \bar{W}(G)) \Rightarrow C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G))$.
4. Contracción $C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G)) \Rightarrow hA \tilde{\otimes} hG$.

El primer paso viene dado por el isomorfismo φ_1 de (2.11), que relaciona la construcción bar de un grupo con el complejo de cadenas del clasificante geométrico asociado a dicho grupo.

Para el segundo paso, consideremos el producto cartesiano torcido $\bar{W}(A) \times_\tau \bar{W}(G)$ definido por la función de torsión τ_*,

$$\begin{array}{rccc} \tau_n : & \bar{W}_n(G) & \to & G_{n-1} \\ & [g_{n-1}, \ldots, g_0] & \mapsto & g_{n-1}; \end{array}$$

con grupo estructural G de acción κ determinada por

$$\begin{array}{rccc} \kappa : & G \times \bar{W}(A) & \to & \bar{W}(A) \\ & (g, [a_{n-1}, \ldots, a_0]) & \mapsto & [g \cdot a_{n-1}, \ldots, g \cdot a_0]. \end{array}$$

En estas circunstancias, tal y como se puede ver en [3], existe un isomorfismo simplicial $\varphi_2 : \bar{W}(A \ltimes_\chi G) \cong \bar{W}(A) \times_\tau \bar{W}(G)$ definido por:

$$\varphi_2[(a_{n-1}, g_{n-1}), \ldots, (a_0, g_0)] = \tag{2.21}$$

$$= ([g_{n-1}^{-1} a_{n-1}, \ldots, \partial_0^{i-1} g_{n-1}^{-1} \cdots \partial_0 g_{n-i+1}^{-1} g_{n-i}^{-1} a_{n-i}, \ldots, \partial_0^{n-1} g_{n-1}^{-1} \cdots \partial_0 g_1^{-1} g_0^{-1} a_0],$$

$$[g_{n-1}, \ldots, g_0]);$$

cuya aplicación inversa φ_2^{-1} resulta ser

$$\varphi_2^{-1}([a_{n-1}, \ldots, a_0], [g_{n-1}, \ldots, g_0]) =$$

$$= [(g_{n-1} a_{n-1}, g_{n-1}), \ldots, (g_{n-i} \partial_0 g_{n-i+1} \cdots \partial_0^{n-i+1} g_{n-1} a_{n-i}, g_{n-i}),$$

$$(g_0 \partial_0 g_1 \cdots \partial_0^{n-1} g_{n-1} a_0, g_0)].$$

El tercer paso proviene de aplicar el Teorema de Eilenberg-Zilber torcido, puesto que τ induce una perturbación en

$$EZ_{C_*(\bar{W}(A)), C_*(\bar{W}(G))} : \{C_*(\bar{W}(A) \times \bar{W}(G)), C_*(\bar{W}(A)) \otimes C_*(\bar{W}(G)), AW, EML, SHI\},$$

dando lugar a la contracción

$$EZ^{\tau}_{\bar{W}(A),\bar{W}(G)} : \{C_*(\bar{W}(A) \times_\tau \bar{W}(G)), C_*(\bar{W}(A)) \otimes_{t(\tau)} C_*(\bar{W}(G)), AW_\tau, EML_\tau, SHI_\tau\}.$$

La diferencial del modelo pequeño aparece modificada por $d_\delta = t\cap = (1\otimes t * 1)(\Delta\otimes 1)$, donde $t : C_*(\bar{W}(G)) \to C_*(G)$ es la cocadena de torsión asociada a τ.

A la hora de buscar una fórmula explícita para t (que ya diera Armario en [4]), recurrimos a la composición (2.14). En contraposición con las extensiones centrales, en este caso hemos de tener en cuenta que el producto tensorial torcido con el que estamos trabajando no es principal: la fibra es $\bar{W}(A)$; la base, $\bar{W}(A)$; y el grupo estructural, G. Por tanto, t vendrá dada por la composición siguiente:

$$C^N_*(\bar{W}(G)) \xrightarrow{i} C^N_*(G) \otimes C^N_*(\bar{W}(G)) \xrightarrow{d_{\delta'}} C^N_*(G) \otimes C^N_*(\bar{W}(G)) \xrightarrow{p} C^N_*(G)$$

donde $i(x) = e \otimes x$, e elemento neutro de G, $p(g \otimes x) = y \cdot \xi(x)$ y $d_{\delta'}$ es el morfismo que nos proporciona el lema de perturbación cuando la contracción $EZ_{G,\bar{W}(G)} : \{C^N_*(G \times \bar{W}(G)), C^N_*(G) \otimes C^N_*(\bar{W}(G)), AW_{G,\bar{W}(G)}, EML_{G,\bar{W}(G)}, SHI_{G,\bar{W}(G)}\}$ es perturbada según el morfismo $\delta'(g,\bar{g}) = (\tau\bar{g} \cdot g, \partial_0\bar{g}) - (g, \partial_0\bar{g})$.

Comprobemos, en primer lugar, que la composición $SHI_{G,\bar{W}(G)}\ \delta'\ EML_{G,\bar{W}(G)}\ i$ es nula cuando trabajamos con el complejo de cadenas. De manera que, la fórmula de $d_{\delta'}$ sobre la imagen de i se reduce a $AW_{G,\bar{W}(G)}\ \delta'\ EML_{G,\bar{W}(G)}$. Si denotamos por e al elemento neutro de G, se tiene:

$$\begin{aligned}
(g_{n-1},\dots,g_0) &\xrightarrow{i} && e \otimes (g_{n-1},\dots,g_0)\\
&\xrightarrow{EML_{G,\bar{W}(G)}} && e \times (g_{n-1},\dots,g_0)\\
&\xrightarrow{\delta} && \begin{array}{l} g_{n-1} \times (g_{n-2},\dots,g_0)\\ -e \times (g_{n-2},\dots,g_0)\end{array}\\
&\xrightarrow{SHI_{G,\bar{W}(G)}} && 0
\end{aligned}$$

Analicemos que efectivamente $SHI(g_{n-1} \times (g_{n-2},\dots,g_0) - e \times (g_{n-2},\dots,g_0)) = 0$. Estudiemos en primer lugar qué ocurre con el primer sumando. Estamos trabajando con G, un grupo discreto, sin embargo, consideramos que se trata de un grupo simplicial en el que los operadores de cara y de degeneración son la identidad. Por tanto,

cuando hacemos que actúe SHI, estamos considerando que g_{n-2} no está en grado cero y que, por consiguiente, $g_{n-2} = s_j g_{n-2}\ \forall j$. Por otra parte, teniendo en cuenta la expresión de SHI, sobre $(g_{n-2}, \ldots, g_0)$ actuará algún s_j, de manera que se tendrá un elemento degenerado, pues sobre las dos componentes actúa el mismo operador de degeneración. Análogamente ocurre con el segundo sumando $e \times (g_{n-2}, \ldots, g_0)$.

Hagamos actuar, ahora, la composición $p\ AW_{G,\bar{W}(G)}$ sobre la imagen de $(g_n, \ldots, g_0)$ por el morfismo $\delta'\ EML_{G,\bar{W}(G)}\ i$.

$$\xrightarrow{AW_{G,\bar{W}(G)}} \sum_{i=0}^{n-1} \partial_{n-i}^{n-i}(g_{n-1} - e) \otimes \partial_0^i(g_{n-1}, \ldots, g_0)\ .$$

Nótese que $g_{n-1} - e$ es un elemento degenerado, salvo cuando lo consideramos en grado cero. Para bajarlo a grado cero se requiere aplicar los n operadores cara sobre dicho elemento. Esto se tiene si nos restringimos únicamente al primer sumando, $i = 0$.

Por otra parte, para proyectar con p y obtener un resultado no nulo, serán necesario que la segunda componente del producto cartesiano sea el único elemento en grado cero, [ ]. Esto sólo es posible si $n = 1$.

$$\xrightarrow{p} \begin{array}{ll} g_n - e & \text{si } n = 1 \\ 0 & \text{si } n \neq 1 \end{array}$$

En resumen, $t : C_*(\bar{W}(G)) \to C_*(G)$, viene dada explícitamente por:

$$t[g_{n-1}, \ldots, g_0] = \begin{cases} g_0 - e_0, & \text{si } n = 1; \\ 0, & \text{si } n \geq 2. \end{cases}$$

Obsérvese que en este punto se encuentra una diferencia fundamental a la hora del cálculo de homología entre extensiones centrales y producto semidirectos:

- De un lado, la cocadena propia de extensiones centrales verificaba la condición de May, en tanto en cuanto se anulaba para elementos de grado 1. Sin embargo, la cocadena propia de productos semidirectos sólo actúa de forma no nula precisamente sobre los elementos de grado 1.

- De otro, en el caso de productos semidirectos sí tenemos una fórmula explícita de la cocadena, mientras que carecemos de ella en extensiones centrales.

Pero no sólo $t\cap$ admite una expresión reducida.

Proposición 2.4.1 *En la contracción*

$$EZ^{\tau}_{\bar{W}(A),\bar{W}(G)} : \{C_*(\bar{W}(A) \times_\tau \bar{W}(G)), C_*(\bar{W}(A)) \otimes_{t(\tau)} C_*(\bar{W}(G)), AW_\tau, EML_\tau, SHI_\tau\}$$

anterior, se tiene que $SHI_\tau = SHI$, $EML_\tau = EML$ *y* $AW_\tau = AW - AW\delta SHI$.

Demostración.

En [4] se demostraba que $EML_\tau = EML$, probando que $SHI\delta EML = 0$.

Aquí vamos a seguir una línea argumentativa diferente, que no sólo va a permitir demostrar ese resultado, sino también que $AW_\tau = AW - AW\delta SHI$ y $SHI_\tau = SHI$.

El dato de perturbación δ de $EZ^{\tau}_{\bar{W}(A),\bar{W}(G)}$ viene dado por

$$\begin{array}{rccl} \delta & : C_*(\bar{W}(A) \times \bar{W}(G)) & \to & C_*(\bar{W}(A) \times \bar{W}(G)) \\ & (\bar{a}, \bar{g}) & \mapsto & \tau\bar{g} \cdot \partial_0\bar{a}, \partial_0\bar{g}) - (\partial_0\bar{a}, \partial_0\bar{g}), \end{array}$$

esto es,

$$\delta((a_{n-1}, \ldots, a_0), (g_{n-1}, \ldots, g_0)) = ((g_{n-1}a_{n-2}, \ldots, a_0), (g_{n-2}, \ldots, g_0)) - \\ -((a_{n-2}, \ldots, a_0), (g_{n-2}, \ldots, g_0));$$

de donde $\delta = \partial_0\bar{\kappa} - \partial_0$, con $\bar{\kappa} : C_*(\bar{W}(A) \times \bar{W}(G)) \to C_*(\bar{W}(A) \times \bar{W}(G))$ dado por

$$\bar{\kappa}((a_{n-1}, \ldots, a_0), (g_{n-1}, \ldots, g_0)) = ((g_{n-1}a_{n-1}, \ldots, g_{n-1}a_0), (g_{n-1}, \ldots, g_0)).$$

y $\partial_0 = (\partial_0, \partial_0)$ el operador simplicial propio de $C_*(\bar{W}(A) \times \bar{W}(G))$.

Por otro lado, una fórmula explícita para SHI es

$$SHI((a_{n-1}, \ldots, a_0), (g_{n-1}, \ldots, g_0)) = \sum_{q=0}^{n-1} \sum_{p=0}^{n-q-1} \pm((a_{n-1}, \ldots, a_{p+q+1}, 0), \\ , (g_{n-1}, \ldots, g_{p+q+1}, g_{p+q} \cdots g_q))||$$

$$||((a_{p+q},\dots,a_q),(1,\dots,1))\star((0,\dots,0),(g_{q-1},\dots,g_0)),$$

con $\star$ el producto shuffle.

De este modo, la composición de $\bar{\kappa}$ y SHI resulta ser:

$$SHI\bar{\kappa}((a_{n-1},\dots,a_0),(g_{n-1},\dots,g_0)) = \bar{\kappa}SHI((a_{n-1},\dots,a_0),(g_{n-1},\dots,g_0))-$$

$$-\sum_{q=0}^{n-1}[(0,g_{n-1}\cdots g_q)||((g_{n-1}\cdots g_q a_{n-1},\dots,g_{n-1}\cdots g_q a_q),(1,\dots,1))\star$$

$$\star((0,\dots,0),(g_{q-1},\dots,g_0))+$$

$$+(0,g_{n-1}\cdots g_q)||((g_{n-1}a_{n-1},\dots,g_{n-1}a_q),(1,\dots,1))\star((0,\dots,0),(g_{q-1},\dots,g_0))];$$

de modo que

$$\partial_0\bar{\kappa}SHI((a_{n-1},\dots,a_0),(g_{n-1},\dots,g_0)) = \partial_0 SHI\bar{\kappa}((a_{n-1},\dots,a_0),(g_{n-1},\dots,g_0))+$$

$$+\sum_{q=0}^{n-1}[((g_{n-1}\cdots g_q a_{n-1},\dots,g_{n-1}\cdots g_q a_q),(1,\dots,1))\star((0,\dots,0),(g_{q-1},\dots,g_0))-$$

$$-((g_{n-1}a_{n-1},\dots,g_{n-1}a_q),(1,\dots,1))\star((0,\dots,0),(g_{q-1},\dots,g_0))].$$

Teniendo en cuenta ahora que $EML \simeq -\star-$ y la relación $\partial_0 SHI = -SHI\partial_0 + EML\,AW$ que se recoge en [35], finalmente podemos concluir que $SHI\delta SHI = 0$:

- $SHI\partial_0 SHI = -SHI\,SHI\partial_0 + SHI\,EML\,AW = 0.$
- $SHI\partial_0\bar{\kappa}SHI = SHI\partial_0 SHI\bar{\kappa} + SHI\,EML(\,,\,) - SHI\,EML(\,,\,) = 0.$
- De donde $SHI\partial_0 SHI = SHI\partial_0\bar{\kappa}SHI - SHI\partial_0 SHI = 0.$

Así,

$$EML_\tau = \sum_{\imath\geq 0}(-1)^i(SHI\delta)^i EML = EML + SHI\delta EML.$$

Pero es fácil ver que

$$\delta EML = \partial_0\bar{\kappa}EML - \partial_0 EML = EML(\,,\,) - EML(\,,\,),$$

por lo que $SHI\delta EML = 0$ y $EML_\tau = EML$.

Del mismo modo, $SHI_\tau = \sum_{\imath\geq 0}(-1)^i(SHI\delta)^i SHI = SHI$.

Por último, $AW_\tau = \sum_{i\geq 0}(-1)^i AW(\delta SHI)^i = AW - AW\delta SHI$, de modo que

$$AW_\tau((a_{n-1},\ldots,a_0),(g_{n-1},\ldots,g_0)) = (2AW - AW\bar{\kappa})((a_{n-1},\ldots,a_0),(g_{n-1},\ldots,g_0)) -$$
$$-\sum_{q=0}^{n-1}[((g_{n-1}\cdots g_q a_{n-1},\ldots,g_{n-1}\cdots g_q a_q,0,\ldots,0),(1,\ldots,1,g_{q-1},\ldots,g_0)) -$$
$$-((g_{n-1}a_{n-1},\ldots,g_{n-1}a_q,0,\ldots,0),(1,\ldots,1,g_{q-1},\ldots,g_0))].$$

■

El último paso se fundamenta en sendos modelos homológicos conocidos para A y G:

$$c_A : \{C_*(\bar{W}(A)), hA, f_A, g_A, \phi_A\} \quad \text{y} \quad c_G : \{C_*(\bar{W}(G)), hG, f_G, g_G, \phi_G\}.$$

Teniendo en cuenta la contracción (2.5), se tiene:

$$c_\otimes : \{C_*(\bar{W}(A)) \otimes C_*(\bar{W}(G)), hA \otimes hG, f_A \otimes f_G, g_A \otimes g_G, 1 \otimes \phi_G + \phi_A \otimes g_G f_G\}.$$

Si perturbamos con $t\cap$ obtenemos:

$$c_{t\cap} : \{C_*(\bar{W}(A)) \otimes_{t(\tau)} C_*(\bar{W}(G)), h(A)\tilde{\otimes}h(G), f_{t\cap}, g_{t\cap}, \phi_{t\cap}\},$$

donde:

$$f_{t\cap} = (f_A \otimes f_G)t\cap \sum_{i\geq 0}(-1)^i((1\otimes\phi_G + \phi_A \otimes g_G f_G)t\cap)^i(1\otimes\phi_G + \phi_A\otimes g_G f_G)$$

$$g_{t\cap} = \sum_{i\geq 0}(-1)^i((1\otimes\phi_G + \phi_A \otimes g_G f_G)t\cap)^i(g_A\otimes g_G)$$

$$\phi_{t\cap} = \sum_{i\geq 0}(-1)^i((1\otimes\phi_G + \phi_A \otimes g_G f_G)t\cap)^i(1\otimes\phi_G + \phi_A\otimes g_G f_G).$$

El hecho de que t no se anule para elementos de grado 1 imposibilita que utilicemos la misma línea argumentativa que en el caso de extensiones centrales para garantizar que este proceso de perturbación es convergente.

No obstante, para aquellos casos en los que G es un grupo abeliano[4] (no necesariamente finito), en [3, 4, 1] se diseñó una filtración sobre $C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G))$,

[4]Para el cual se describiera en la sección anterior un modelo homológico (ver (2.8)), en función de álgebras exteriores y polinomiales modificadas (ver (2.1) y (2.2)).

de suerte que $t\cap$ disminuía en una unidad el grado de filtración, mientras que la homotopía $1 \otimes \phi_G + \phi_A \otimes g_G f_G$ lo respetaba. Lo cual permitía demostrar la finitud del proceso de perturbación.

Concretamente, si $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k} \oplus \mathbb{Z}^v$, esta filtración venía dada por la familia $\{C_*(\bar{W}(A)) \otimes F_q(C_*(\bar{W}(G))\}_{q\geq 0}$; donde $F_q(C_*(\bar{W}(G))$ es el sub-DG-módulo de $\bar{B}(\mathbb{Z}[\mathbb{Z}_{n_1}] \otimes \cdots \otimes \mathbb{Z}[\mathbb{Z}_{n_k}] \otimes \mathbb{Z}[\mathbb{Z}] \otimes \overset{v}{\cdots} \otimes \mathbb{Z}[\mathbb{Z}])$ generado por aquellos elementos homogéneos $[x_1^1 \otimes \cdots \otimes x_1^{k+v} | \cdots | x_n^1 \otimes \cdots \otimes x_n^{k+v}]$ de modo que $\sum_{i,j} |x_i^j| \leq q$.

Resumiendo, el proceso seguido hasta encontrar un modelo homológico de un producto semidirecto, tal como recogen [3, 4, 1], es:

$$\bar{B}(\mathbb{Z}[A \ltimes_\chi G]) \overset{\varphi_1}{\Rightarrow} C_*(\bar{W}(A \ltimes_\chi G)) \overset{\varphi_2}{\Rightarrow} C_*(\bar{W}(A) \times_\tau \bar{W}(G)) \overset{EZ^\tau_{\bar{W}(A),\bar{W}(G)}}{\Rightarrow}$$

$$\overset{EZ_{\bar{W}(A),\bar{W}(G)}}{\Rightarrow} C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G)) \overset{C_{t\cap}}{\Rightarrow} hA \tilde{\otimes} hG$$

Teorema 2.4.2 *[3, 4, 1] La contracción*

$$c_{A \ltimes_\chi G} : \{\bar{B}(\mathbb{Z}[A \ltimes_\chi G]), hA \tilde{\otimes} hG, f, g, \phi\}, \tag{2.22}$$

establece un modelo homológico para $A \ltimes_\chi G$, siendo los morfismos:

$$f = f_{t\cap} AW_\tau \varphi_2 \varphi_1$$

$$g = \varphi_1^{-1}\varphi_2^{-1} EML_\tau g_{t\cap}$$

$$\phi = \varphi_1^{-1}\varphi_2^{-1} SHI_\tau \varphi_2 \varphi_1 + \varphi_1^{-1}\varphi_2^{-1} EML_\tau \phi_{t\cap} AW_\tau \varphi_2 \varphi_1.$$

La diferencial del homológico es $d_{hA} \otimes 1 + 1 \otimes d_{hG} + d_\infty$, donde d_∞ viene definido según el lema de perturbación de la siguiente forma:

$$d_\infty = (f_A \otimes f_G) t \cap \sum_{i\geq 0} (-1)^i ((1 \otimes \phi_G + \phi_A \otimes g_G f_G) t \cap)^i (g_A \otimes g_G).$$

2.4.2 Modelo cohomológico

A la hora de diseñar un modelo cohomológico para $A \ltimes_\chi G$, con A y G grupos abelianos finitos, procedemos según los pasos siguientes:

1. Aplicamos primero el funtor Hom a la contracción (2.22), para obtener

$$c^*_{A\ltimes_\chi G} : \{\mathrm{Hom}(\bar{B}(\mathbb{Z}[A\ltimes_\chi G]),\mathbb{Z}),\mathrm{Hom}(hA\tilde{\otimes}hG,\mathbb{Z}),g^*,f^*,\phi^*\}. \tag{2.23}$$

Nótese que si $\tilde{d}=d_{hA}\otimes 1+1\otimes d_{hG}+d_\infty$ es la diferencial sobre $hA\tilde{\otimes}hG$, entonces $\tilde{\partial}$ definida como $\tilde{\partial}(f)=f\circ\tilde{d}$ es la diferencial sobre $\mathrm{Hom}(hA\tilde{\otimes}hG,\mathbb{Z})$. En particular, es fácil ver que $\tilde{\partial}=\partial+\partial_\infty$, donde $\partial(f)=f\circ(d_{hA}\otimes 1+1\otimes d_{hG})$ y $\partial_\infty(f)=f\circ d_\infty$; de donde $\tilde{\partial}$ surge por la perturbación de la diferencial usual ∂ según el dato ∂_∞.

2. Formamos la isocontracción banal (2.19),

$$c_F : \{\mathrm{Hom}(hA\otimes hG,\mathbb{Z}),\bigotimes_{i\in I}(E(u_i)\otimes P(v_i)),F,F^{-1},0\},$$

donde cada $\mathbb{Z}_{n_i}$ en que se descomponen A y G aporta una pareja $E(u_i)\otimes P(v_i)$; asociada al isomorfismo F de (2.9),

$$\begin{array}{rccc} F: & \mathrm{Hom}(A_{m_1}\otimes\cdots\otimes A_{n_t},\mathbb{Z}) & \to & A^*_{m_1}\otimes\cdots\otimes A^*_{n_t} \\ & f & \mapsto & \sum_{f(v_{m_1},\ldots,v_{n_t})\neq 0} f(v_{m_1},\ldots,v_{n_t})\cdot v^*_{m_1}\otimes\cdots\otimes v^*_{n_t}, \\ & f_{m_1}*_{\mathbb{Z}}\cdots *_{\mathbb{Z}} f_{n_t} & \leftarrow\!\shortmid & f_{m_1}\otimes\cdots\otimes f_{n_t}; \end{array}$$

donde $A=\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_s}$ y $G=\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_t}$, y $A_{k_i}=A_{k_i}(v_{k_i},1)$ denota al par $E(u_{k_i},1)\otimes\Gamma(w_{k_i},2)$ que corresponde al factor $\mathbb{Z}_{k_i}$ en el modelo homológico de $A_f\rtimes G$. De modo que $v^j_{k_i}=u^{j\,(mod\,2)}_{k_i}\otimes w^{\lfloor\frac{j}{2}\rfloor}_{k_i}$.

3. Ahora sólo queda perturbar la contracción (2.19) anterior según ∂_∞ y componer el resultado con (2.23), para así obtener

$$c : \{\mathrm{Hom}(\bar{B}(\mathbb{Z}[A\ltimes_\chi G]),\mathbb{Z}),\tilde{\bigotimes_{i\in I}}(E(u_i)\otimes P(v_i)),f,g,\phi\}. \tag{2.24}$$

Dado que (2.19) es una isocontracción, el proceso de perturbación se reduce a modificar la diferencial usual de $A^*_{m_1}\otimes\cdots\otimes A^*_{n_t}$, resultando

$$\tilde{d^*}=\left(\sum_{i=1}^{s}1^{\otimes i-1}\otimes d_{A^*_{m_i}}\otimes 1^{\otimes s-i}\right)+\left(\sum_{j=1}^{t}1^{\otimes j-1}\otimes d_{A^*_{n_j}}\otimes 1^{\otimes t-j}\right)+F\circ\partial_\infty\circ F^{-1}.$$

De este modo, queda probado el siguiente resultado.

Teorema 2.4.3 *La contracción (2.24) establece un modelo cohomológico para el producto semidirecto $A\ltimes_\chi G$, con A y G grupos abelianos finitos.*

Nuevamente, este esquema también funciona en el caso A y G grupos abelianos en general, no necesariamente finitos: basta considerar el modelo homológico correspondiente de cada factor $\mathbb{Z}$ ó $\mathbb{Z}_{n_i}$ en que se descompongan A y G, respectivamente. Para otros grupos A y G que no sean abelianos, pero tengan modelos homológicos conocidos, todo depende de la validez del paso segundo. Este aspecto saldrá a relucir a continuación, cuando abordemos la determinación de modelos (co)homológicos para productos iterados de extensiones centrales y productos semidirectos de grupos abelianos finitos.

2.4.3 Computación y ejemplos

El primer paso es implementar las aplicaciones `isops` e `invisops`, que conforman el isomorfismo de $C_*(\bar{W}(A \ltimes_\chi G))$ a $C_*(\bar{W}(A) \times_\tau \bar{W}(G))$. Los índices 2 y 3 que se utilizan en adelante hacen referencia a la forma en que viene dado el producto semidirecto, $A \ltimes_\chi G$ ó $G_\chi \rtimes A$, respectivamente. La acción la denotamos por `chi`.

```
isops[ind_][x_+y_]:=isops[ind][x]+isops[ind][y];
isops[ind_][x_*y_]:=Expand[x*isops[ind][y]]; isops[ind_][0]:=0;
isops[ind_][{}]:={{},{}};
isops[2][l_]:=Module[{k,n,x1,x2}, n=Length[l]; k={}; Do[
      x1=Ceiling[l[[i]]/cardg]; x2=1+Mod[l[[i]]-1,cardg];
      k=Append[k,{x1,x2}],{i, n}]; k=Transpose[k];
      {Table[chi[Fold[prodg,1,Table[inversos[[k[[2,j]]]],
      {j,i}]],k[[1,i]]],{i,n}],k[[2]]}];
isops[3][l_]:=Module[{k,n,x1,x2}, n=Length[l]; k={}; Do[
      x1=Ceiling[l[[i]]/cardg]; x2=1+Mod[l[[i]]-1,cardg];
      k=Append[k,{x1,x2}],{i,n}]; k=Transpose[k];
      {k[[1]],Table[chi[Fold[proda,1,Table[
      inversos[[k[[1,j]]]],{j,i}]],k[[2,i]]],{i,n}]}];
invisops[ind_][x_+y_]:=invisops[ind][x]+invisops[ind][y];
invisops[ind_][x_*y_]:=Expand[x*invisops[ind][y]];
invisops[ind_][0]:=0; invisops[ind_][{{},{}}]:={};
invisops[2][l_]:=Module[{k}, k=Table[{chi[Fold[prodg,1,Reverse[
      Take[l[[2]],i]]],l[[1,i]]],l[[2,i]]},{i,Length[l[[1]]]}];
      Table[(k[[i,1]]-1)*cardg+k[[i,2]],{i,Length[k]}]];
```

```
invisops[3][l_]:=Module[{k}, k=Table[{l[[1,i]],chi[Fold[proda,1,
    Reverse[Take[l[[1]],i]]],l[[2,i]]]},{i,Length[l[[2]]]}];
    Table[(k[[i,1]]-1)*cardg+k[[i,2]],{i,Length[k]}]];
```

A continuación definimos los morfismos que corresponden a la función de torsión τ y la perturbación asociada δ_τ, que llamamos `taups` y `deltaups`. La función `deltaupssimple` devuelve aquellos términos en la imagen de $delta_\tau$ en los que interviene la función de torsión τ. Nótese que `deltaups` es nula actuando sobre elementos de grado 0 ó 1.

```
deltaups[ind_][x_+y_]:=deltaups[ind][x]+deltaups[ind][y];
deltaups[ind_][x_*y_]:=Expand[x*deltaups[ind][y]];
deltaups[ind_][0]:=0;
deltaupssimple[ind_][x_+y_]:=deltaupssimple[ind][x]+
    deltaupssimple[ind][y];
deltaupssimple[ind_][x_*y_]:=Expand[x*deltaupssimple[ind][y]];
deltaupssimple[ind_][0]:=0; deltaupssimple[ind_][{{},{}}]:=0;
deltaupssimple[2][l_]:={Table[chi[l[[2,1]],l[[1,i+1]]],
    {i,Length[l[[1]]]-1}],Rest[l[[2]]]};
deltaupssimple[3][l_]:={Rest[l[[1]]],Table[chi[l[[1,1]],l[[2,i+1]]],
    {i,Length[l[[2]]]-1}]};
deltaups[2][l_]:=Module[{n,l1,l2,k}, l1=l[[1]]; l2=l[[2]];
    n=Length[l1]; If[n<2||l2[[1]]==1, k=0,
    k=deltaupssimple[2][l]-{Rest[l1],Rest[l2]}]; k];
deltaups[3][l_]:=Module[{n,l1,l2,k}, l1=l[[1]]; l2=l[[2]];
    n=Length[l2]; If[n<2||l1[[1]]==1, k=0,
    k=deltaupssimple[3][l]-{Rest[l1],Rest[l2]}]; k];
```

La aplicación `difteztps` representa la diferencial de $C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G))$, según el Teorema de Eilenberg-Zilber Torcido. La función auxiliar `orlar[ind]` permite seleccionar la mitad de los sumandos que devuelve EML, justamente aquellos que tienen por primeros elementos un 1 en la primera componente (propia de A), y un elemento distinto de 1 en la segunda componente (propia de G); en función del índice 2 ó 3 "ind". Crearemos `difteztps` a través de la cocadena de torsión, que se codifica fácilmente en este caso.

```
compops[ind_][x_+y_]:=compops[ind][x]+compops[ind][y];
```

```
compops[ind_][x_*y_]:=Expand[x*compops[ind][y]]; compops[ind_][0]:=0;
compops[ind_][l_]:=deltaups[ind][shi[l]];
difteztps[ind_][x_+y_]:=difteztps[ind][x]+difteztps[ind][y];
difteztps[ind_][x_*y_]:=Expand[x*difteztps[ind][y]];
difteztps[ind_][0]:=0;
difteztps[2][l_]:=Module[{p,q,l1,l2,k}, l1=l[[1]]; l2=l[[2]];
      p=Length[l1]; q=Length[l2]; If[q==0||l2[[1]]==1, k=0,
      k=(-1)^p*({Table[chi[l2[[1]],l1[[i]]],{i,p}],
      Rest[l2]}-{l1,Rest[l2]})]; k];
difteztps[3][l_]:=Module[{p,q,l1,l2,k}, l1=l[[1]]; l2=l[[2]];
      p=Length[l1]; q=Length[l2]; If[p==0||Last[l1]==1, k=0,
      k=(-1)^p*({Drop[l1,-1],Table[chi[Last[l1],l2[[i]]],
      {i,q}]}-{Drop[l1,-1],l2})]; k];
```

Ahora codificamos las aplicaciones `awps`, `emlps` y `ships` propias de la contracción Eilenberg-Zilber torcida asociada a `deltaups`.

```
awps[ind_][x_+y_]:=awps[ind][x]+awps[ind][y];
awps[ind_][x_*y_]:=Expand[x*awps[ind][y]]; awps[ind_][0]:=0;
awps[ind_][l_]:=aw[sumatorio[NestWhileList[compops[ind],nul1[l],
      (#1=!=0)&]]];
emlps[ind_][x_+y_]:=emlps[ind][x]+emlps[ind][y];
emlps[ind_][x_*y_]:=Expand[x*emlps[ind][y]]; emlps[ind_][0]:=0;
emlps[2][l_]:=Module[{k,l1,l2}, k=eml[nul2[l]]; l1=l[[1]]; l2=l[[2]];
      If[Length[l2]==0||l2[[1]]==1, , k=k-shi[sumatorio[
      NestWhileList[compops[2],(-1)^Length[l1]*
      deltaupssimple[orlar[4][eml[nul2[{l1,Rest[l2]}]],l2[[1]]]],
      (#1=!=0)&]]]; k];
emlps[3][l_]:=Module[{k,l1,l2}, k=eml[nul2[l]]; l1=l[[1]]; l2=l[[2]];
      If[Length[l1]==0||l1[[1]]==1, , k=k-shi[sumatorio[
      NestWhileList[compops[3],deltaupssimple[3][orlar[5][
      eml[nul2[{Rest[l1],l2}]],l1[[1]]]],(#1=!=0)&]]]; k];
ships[ind_][x_+y_]:=ships[ind][x]+ships[ind][y];
ships[ind_][x_*y_]:=Expand[x*ships[ind][y]]; ships[ind_][0]:=0;
ships[ind_][l_]:=shi[sumatorio[NestWhileList[
      compops[ind],nul1[l],(#1=!=0)&]]];
```

Para construir la diferencial del modelo, `difmodps`, así como los morfismos `fmodps`, `gmodps` y `fimodps` de la contracción final, es necesario predefinir los modelos homológicos hA y hG y las aplicaciones `fa`, `ga`, `fia` y `fg`, `gg`, `fig` que dan las contracciones a hA y hG, respectivamente. Vendrán dadas en función de los modelos de $\mathbb{Z}_n$ codificados con antelación.

```
compomodps[ind_][x_+y_]:=compomodps[ind][x]+compomodps[ind][y];
compomodps[ind_][x_*y_]:=Expand[x*compomodps[ind][y]];
compomodps[ind_][0]:=0;
compomodps[ind_][l_]:=difteztps[ind][fimodban[l]];
difmodps[ind_][x_+y_]:=difmodps[ind][x]+difmodps[ind][y];
difmodps[ind_][x_*y_]:=Expand[x*difmodps[ind][y]];
difmodps[ind_][0]:=0;
difmodps[ind_][l_]:=fmodban[sumatorio[NestWhileList[
      compomodps[ind],difteztps[ind][gmodban[l]],(#1=!=0)&]]];
fmodps[ind_][x_+y_]:=fmodps[ind][x]+fmodps[ind][y];
fmodps[ind_][x_*y_]:=Expand[x*fmodps[ind][y]]; fmodps[ind_][0]:=0;
fmodps[ind_][l_]:=fmodban[sumatorio[NestWhileList[
      compomodps[ind],l,(#1=!=0)&]]];
gmodps[ind_][x_+y_]:=gmodps[ind][x]+gmodps[ind][y];
gmodps[ind_][x_*y_]:=Expand[x*gmodps[ind][y]]; gmodps[ind_][0]:=0;
gmodps[ind_][l_]:=gmodban[l]-fimodban[sumatorio[NestWhileList[
      compomodps[ind],difteztps[ind][gmodban[l]],(#1=!=0)&]]];
fimodps[ind_][x_+y_]:=fimodps[ind][x]+fimodps[ind][y];
fimodps[ind_][x_*y_]:=Expand[x*fimodps[ind][y]]; fimodps[ind_][0]:=0;
fimodps[ind_][l_]:=fimodban[sumatorio[NestWhileList[
      compomodps[ind],l,(#1=!=0)&]]];
```

Para calcular homología basta utilizar la rutina que codifica el algoritmo de Veblen.

Apliquemos el procedimiento para determinar la homología en dimensión 1 y 2 de los grupos diédricos $D_{4t} = \mathbb{Z}_{2t} \ltimes_{\chi} \mathbb{Z}_2$, para $1 \leq t \leq 5$.

En la salida incluimos las matrices que representan las diferenciales d_i respecto de

las bases del modelo que da `basemod[i,2]`.

t	1	2	3	4	5
$M(d_2)$	$\begin{pmatrix} 2 & 0 \\ 0 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 \\ -2 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 6 & 0 \\ -4 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 8 & 0 \\ -6 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 10 & 0 \\ -8 & 0 \\ 0 & 2 \end{pmatrix}$
$M(d_3)$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 2 & 4 & 0 \\ -2 & -4 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 4 & 6 & 0 \\ -4 & -6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 6 & 8 & 0 \\ -6 & -8 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 \\ 8 & 10 & 0 \\ -8 & -10 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
H_1	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$
H_2	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	$\mathbb{Z}_2$

2.5 (Co)homología de productos iterados

Vamos a determinar ahora modelos (co)homológicos para productos iterados de extensiones centrales y productos semidirectos de grupos abelianos, los cuales representaremos mediante árboles binarios de $t+1$ hojas $A_i \in \{\mathbb{Z}, \mathbb{Z}_{n_i}\}$ y t vértices internos (o padres), correspondientes a productos $\tilde{\times}_i \in \{\times, \rtimes_{f_i}, \ltimes_{\chi_i}\}$; donde asumimos que en todo producto $A_f \rtimes G$ (respectivamente, $A \ltimes_\chi G$), es A (respectivamente, G) abeliano.

Con asiduidad, adoptaremos la notación simplificada $A_1 \tilde{\times}_1 A_2 \tilde{\times}_2 A_3 \cdots \tilde{\times}_t A_{t+1}$, sin especificar el modo en que se asocian los productos, de no ser estrictamente necesario. De ser otro el caso, ordenaríamos los productos por orden inverso en la prioridad en que se asocian, $\tilde{\times}_{i_1}, \ldots, \tilde{\times}_{i_t}$, significando esto que $\tilde{\times}_{i_1}$ es el último producto en efectuarse (vértice raíz del árbol) y $\tilde{\times}_{i_t}$ es el último vértice padre del penúltimo nivel del árbol binario (nótese que en el último nivel sólo hay hojas, por definición).

2.5.1 Modelo homológico

Los modelos homológicos de productos directos, extensiones centrales y productos semidirectos de grupos estudiados en las secciones precedentes, permiten diseñar un modelo homológico para cualquier producto iterado $A_1 \tilde{\times}_1 \cdots \tilde{\times}_t A_{t+1}$ de grupos abelianos. Concretamente, vamos a determinar un modelo homológico para $A_1 \tilde{\times}_1 \cdots \tilde{\times}_t A_{t+1}$

de manera recursiva, procediendo desde la operación raíz $\tilde{\times}_{i_1}$ hasta la primera operación $\tilde{\times}_{i_t}$.

En efecto, el grupo dado por el producto $\tilde{\times}_{i_j}$ presenta un modelo homológico en función de los modelos homológicos de los factores, según las contracciones simples (2.8), (2.17) y (2.22) tratadas en las secciones anteriores:

- Toda extensión central $A_f \rtimes G$ con A abeliano admite un modelo homológico, en función de un modelo homológico de G. Todas las extensiones centrales a que da lugar $A_1 \tilde{\times}_1 A_2 \tilde{\times}_2 A_3 \cdots \tilde{\times}_t A_{t+1}$ tienen, pues, modelo homológico.
- Todo producto semidirecto $A \ltimes_\chi G$ con G abeliano admite un modelo homológico, en función de un modelo homológico de A. Todos los productos semidirectos a que da lugar $A_1 \tilde{\times}_1 A_2 \tilde{\times}_2 A_3 \cdots \tilde{\times}_t A_{t+1}$ tienen, pues, modelo homológico.

Teorema 2.5.1 *La composición de reiterada de las contracciones (2.8), (2.17) y (2.22) proporciona un modelo homológico*

$$c_{\tilde{\times}} : \{\bar{B}(\mathbb{Z}[A_1 \tilde{\times}_1 \cdots \tilde{\times}_t A_{t+1}]), \bigotimes_{1 \leq i \leq t+1} (E(u_i) \tilde{\otimes} \Gamma(w_i)), f, g, \phi\}. \tag{2.25}$$

para productos iterados $A_1 \tilde{\times}_1 \cdots \tilde{\times}_t A_{t+1}$ de grupos abelianos.

2.5.2 Modelo cohomológico

A la hora de diseñar un modelo cohomológico para un producto iterado $A_1 \tilde{\times}_1 \cdots \tilde{\times}_t A_{t+1}$ de grupos abelianos finitos, procedemos según los pasos descritos en las secciones precedentes, tomando el funtor Hom en (2.25) y componiendo con la perturbación adecuada de la isocontracción (2.19) correspondiente; hasta obtener:

$$c^* : \{\mathrm{Hom}(\bar{B}(\mathbb{Z}[A_1 \tilde{\times}_1 \cdots \tilde{\times}_t A_{t+1}]), \mathbb{Z}), \bigotimes_{1 \leq i \leq t+1} (E(u_i) \tilde{\otimes} P(v_i)), F \circ g^*, F \circ f^*, \phi^*\}. \tag{2.26}$$

Teorema 2.5.2 *La contracción (2.26) establece un modelo cohomológico para un producto iterado $A_1 \tilde{\times}_1 \cdots \tilde{\times}_t A_{t+1}$ de grupos abelianos finitos.*

2.5.3 Computación y ejemplos

Los programas que hemos visto anteriormente para extensiones centrales y productos semidirectos pueden ser actualizados con leves modificaciones para adaptarse al caso de productos iterados de los mismos.

El nuevo programa habría de saber el cardinal de cada uno de los grupos abelianos finitos iniciales, amén de los 2-cociclos χ_i y las acciones ${}_j\chi$ implicadas. El programa facilitará como salida los morfismos que integran todas las contracciones en que se descompone el modelo homológico del grupo iterado total. En aras de favorecer la recursividad, todas estas funciones tendrán como primer argumento un índice "niv", que hará referencia al nivel de imbricación en cada etapa.

En particular, todo producto iterado P lo representaremos mediante un árbol binario enraizado, en el que los vértices hoja son los grupos $\mathbb{Z}_n$ en que factoriza P, y cada vértice padre se traduce en un producto de grupos. Este árbol se introduce como una lista de tantas sublistas como niveles tiene, de modo que cada nivel viene dado en una lista independiente. Ha de tenerse en cuenta que en todo el programa cada iteración se representa en la forma $A \times G$, de modo que en el caso de extensiones centrales la imagen del 2-cociclo ha de ser un grupo abeliano, y en el caso de productos semidirectos lo ha de ser el grupo estructural de la acción. Para distinguir cuál de entre A y G es el grupo abeliano en $A \times G$ se seguirá la siguiente numeración: 2 para productos semidirectos con G abeliano (es decir con G el grupo estructural), 3 para productos semidirectos A abeliano, 4 para extensiones centrales con A abeliano y 5 para extensiones centrales con G abeliano (esto es, imagen del 2-cociclo). El 1 se reserva para productos directos.

En "numgru" se guarda el número de $\mathbb{Z}_n$ involucrados, mientras que en la lista "card" se almacenan sus respectivos cardinales n. En "arbol" se guarda la lista de estratos, mientras que "hojimb" es la lista de pares de hojas (número de grupos) que se utilizan en la primera y segunda componente de cada imbricación, en concordancia con la estratificación dada en el árbol a partir del vértice raíz, de arriba a abajo y de izquierda a derecha.

Por ejemplo, al grupo $\mathbb{Z}_n \times ((\mathbb{Z}_m {}_f\rtimes \mathbb{Z}_t)\ltimes_\chi \mathbb{Z}_s)$ le corresponde el árbol $\{\{1\},\{0,2\},\{3,0\}\}$, y la lista "hojimb" $\{\{1,1\},\{2,1\},\{1,1\}\}$.

Ha de tenerse en cuenta que en todo el programa cada iteración se representa en la forma $A \times G$, de modo que en el caso de extensiones centrales la imagen del 2-cociclo ha de ser un grupo abeliano, y en el caso de productos semidirectos lo ha de ser el grupo estructural de la acción. Para distinguir cuál de entre A y G es el grupo abeliano en $A \times G$ se seguirá la siguiente numeración: 2 para productos semidirectos con G abeliano (es decir con G el grupo estructural), 3 para productos semidirectos A abeliano, 4 para extensiones centrales con A abeliano y 5 para extensiones centrales con G abeliano (esto es, imagen del 2-cociclo). El 1 se reserva para productos directos.

```
Print["Introduzca el árbol binario que representa el grupo, comenzando
por el vértice raíz y continuando por niveles de arriba a abajo y de
izquierda a derecha, según la siguiente leyenda:  0, si el vértice es
hoja; 1, si el vértice da lugar a un producto directo A x G; 2, si el
vértice da lugar a un producto semidirecto A x G, con G grupo
estructural; 3, si el vértice da lugar a un producto semidirecto A x
G, con A grupo estructural; 4, si el vértice da lugar a una extensión
central A x G, con A imagen del 2-cociclo; y 5, si el vértice da lugar
a una extensión central con G imagen del 2-cociclo.  Cada nivel irá
dado en una lista independiente."];
arbol=Input["¿Lista normalizada de vértices padre del árbol
     por niveles?  "];
numgru=1+Length[Select[Flatten[arbol,1],#1=!=0&]];
card={};
Do[Print["Cardinal del grupo ",i," comenzando desde la izquierda..."];
     card=Append[card,Input["Cardinal "]], {i, numgru}];
hojimb=Table[{1,1},{i,Length[Last[arbol]]-Count[Last[arbol],0]}];
Module[{aux,pos}, Do[aux=sumlist[arbol[[i]],1];
     pos=Complement[Range[Length[aux]],Flatten[Position[aux, 1],1]];
     Do[aux[[pos[[j]]]]=hojimb[[j,1]]+hojimb[[j,2]],{j,Length[pos]}];
     hojimb=Join[Partition[aux,2],hojimb],{i,Length[arbol],2,-1}]];
imbestratos=Table[Select[arbol[[i]],#1=!=0&],{i,Length[arbol]}];
imbprec=Append[Table[Apply[Plus,Table[Length[imbestratos[[j]]],
     {j,i-1}]], {i,Length[arbol]}],numgru-1];
```

Las leyes internas de los grupos que corresponden a la imbricación `niv` se codifican según `proda[niv]` y `prodg[niv]`, con atributo "listable". En las listas `inversos[niv]` se almacenan los inversos de los elementos de A ó G, según el nivel

de imbricación `niv`: `A[niv]` en el caso de extensiones centrales del tipo 4 o productos semidirectos del tipo 3, y `G[niv]` en el caso de productos semidirectos del tipo 2 y extensiones centrales del tipo 5.

Para definir estos comandos se realizará un bucle doble anidado. El externo (en `i`), indicará el estrato de `imbestratos`; el interno (en `j`), recorriendo cada una de las imbricaciones del estrato en cuestión. La variable `niv` almacenará el número de la imbricación en curso. La lista `indices` almacenará los cardinales de los grupos $\mathbb{Z}_n$ que estén involucrados en el instante dado, de modo que comenzará siendo igual a `card` y se le irán borrando los índices de aquéllos $\mathbb{Z}_n$ que hayan sido utilizados como vértices hojas. El índice `pos` hará referencia a la posición en `indices` del último $\mathbb{Z}_n$ utilizado aún activo. La idea será construir los cardinales `card_[niv]` y las leyes de grupos `prod_[niv]` correspondientes a los factores A`[niv]` y G`[niv]`. Si alguno de estos dos grupos resultara encerrar una nueva imbricación (necesariamente, en el siguiente estrato), el índice `posest` marcaría el índice correspondiente a esta nueva imbricación. Se aprovecha la ocasión para definir asimismo las aplicaciones de las contracciones asociadas a cada imbricación. En `infoarbol` se guarda una lista de 4 índices por cada imbricación: las dos primeras entradas se refieren al carácter 0, 1, 2, 3, 4 ó 5 de los factores A y G correspondientes a la imbricación, mientras que las entradas tercera y cuarta se refieren al número de imbricación que a éstos les correspondiera ó al índice del factor $\mathbb{Z}_n$ que constituyeran, según sea el caso.

```
infoarbol={};
Module[{indices,i3,i4,a1,g1,niv,pos,posest,arbol2,preg},
      arbol2=Append[arbol,Table[0,{i,2*Length[Last[imbestratos]]}]];
      indices=card; niv=1; Do[pos=0; posest=imbprec[[i+1]];
        Do[a1=hojimb[[niv, 1]]; g1=hojimb[[niv, 2]];
        carda[niv]=Apply[Times,Take[indices,{pos+1,pos+a1}]];
        cardg[niv]=Apply[Times,Take[indices,{pos+a1+1,pos+a1+g1}]];
        Which[imbestratos[[i,j]]==1, , imbestratos[[i,j]]==2,
        Print["¿Ha definido previamente la acción chi[", niv,
        "]:G x A --> A?"];
        preg=Input["Introduzca 1 si la quiere definir ahora."];
        If[preg==1, Do[Do[Print["Introduzca el valor de chi[",
        niv,"][",fil,",",col,"]"]; chi[niv][fil,col]=Input["Valor:"],
        {col,carda[niv]}], {fil, cardg[niv]}]],
        imbestratos[[i,j]]==3,Print["¿Ha definido previamente la
```

```
        acción chi[",niv,"]:A x G --> G?"];
        preg=Input["Introduzca 1 si la quiere definir ahora."];
        If[preg==1, Do[Do[Print["Introduzca el valor de chi[",
        niv,"][",fil,",",col,"]"]; chi[niv][fil,col]=Input["Valor:"],
        {col,cardg[niv]}], {fil,carda[niv]}]],
        imbestratos[[i,j]]==4, Print["¿Ha definido previamente el
        2-cociclo chi[",niv,"]:G x G --> A?"];
        preg=Input["Introduzca 1 si lo quiere definir ahora."];
        If[preg==1, Do[Do[Print["Introduzca el valor de chi[",
        niv,"][",fil,",",col,"]"]; chi[niv][fil,col]=Input["Valor:"],
        {col,cardg[niv]}], {fil,cardg[niv]}]],
        imbestratos[[i,j]]==5, Print["¿Ha definido previamente el
        2-cociclo chi[",niv,"]:A x A --> G?"];
        preg=Input["Introduzca 1 si lo quiere definir ahora."];
        If[preg==1, Do[Do[Print["Introduzca el valor de chi[",
        niv,"][",fil,",",col,"]"]; chi[niv][fil,col]=Input["Valor:"],
        {col,carda[niv]}], {fil,carda[niv]}]]];
        posest=posest+1; Which[a1==1,i3=indices[[pos+1]];
        indices=Drop[indices,{pos+1}]; pos=pos-1;
        posest=posest-1, a1>1, i3=posest];
        pos=pos+a1; posest=posest+1;
        Which[g1==1, i4=indices[[pos+1]]; posest=posest-1;
        indices=Drop[indices,{pos+1}]; pos=pos-1,
        g1>1, i4=posest]; pos=pos+g1;
        infoarbol=Append[infoarbol,{arbol2[[i+1,2*j-1]],
        arbol2[[i+1,2*j]], i3, i4}];
niv=niv+1, {j,Length[imbestratos[[i]]]}], {i,Length[imbestratos]}]];
Module[{ini,ele,lista}, lista=Flatten[imbestratos,1]; Do[
     Which[lista[[niv]]==3||lista[[niv]]==4,
        ini=Table[i,{i,2,carda[niv]}];
        inversos[niv]=Table[1,{i,carda[niv]}];
        While[Length[ini]>0, ele=1+Position[Table[
        proda[niv][ini[[1]],i1],{i1,2,carda[niv]}],1][[1,1]];
        inversos[niv]=ReplacePart[inversos[niv],ele,ini[[1]]];
        inversos[niv]=ReplacePart[inversos[niv],ini[[1]],ele];
        ini=DeleteCases[DeleteCases[ini,ini[[1]]],ele]],
```

```
      lista[[niv]]==2||lista[[niv]]==5,
        ini=Table[i,{i,2,cardg[niv]}];
        inversos[niv]=Table[1,{i,cardg[niv]}];
        While[Length[ini]>0, ele=1+Position[Table[
        prodg[niv][ini[[1]],i1],{i1,2,cardg[niv]}],1][[1,1]];
        inversos[niv]=ReplacePart[inversos[niv],ele,ini[[1]]];
        inversos[niv]=ReplacePart[inversos[niv],ini[[1]],ele];
        ini=DeleteCases[DeleteCases[ini,ini[[1]]],ele]],
      lista[[niv]]==1,]
,{niv,numgru-1}]];
```

A continuación se definen las leyes internas de los grupos asociados a cada imbricación, así como las contracciones que definen los modelos homológicos de los grupos factores correspondientes en que éstos se descomponen.

A la hora de engarzar de manera recursiva las contracciones a que dan lugar los distintos grupos que van apareciendo en cada imbricación, se ha optado por fijar que el comienzo de cada contracción elemental sea el complejo de cadenas del clasificante geométrico del grupo, y no la construcción bar; así, el isomorfismo de la bar al clasificante sólo se ha de usar en la primera imbricación, raíz del árbol que corresponde al grupo inicial.

```
prod[l_,x_,y_,0]:=1+Mod[x+y-2,1];
prod[l_,x_,y_,1]:=Module[{k1,k2,x1,x2,y1,y2}, x1=Ceiling[x/cardg[l]];
      x2=1+Mod[x-1,cardg[l]]; y1=Ceiling[y/cardg[l]];
      y2=1+Mod[y-1,cardg[l]]; k1=proda[l][x1,y1];
      k2=prodg[l][x2,y2]; (k1-1)*cardg[l]+k2];
prod[l_,x_,y_,2]:=Module[{k1,k2,x1,x2,y1,y2}, x1=Ceiling[x/cardg[l]];
      x2=1+Mod[x-1,cardg[l]]; y1=Ceiling[y/cardg[l]];
      y2=1+Mod[y-1,cardg[l]]; k1=proda[l][x1,chi[l][x2,y1]];
      k2=prodg[l][x2,y2]; (k1-1)*cardg[l]+k2];
prod[l_,x_,y_,3]:=Module[{k1,k2,x1,x2,y1,y2}, x1=Ceiling[x/cardg[l]];
      x2=1+Mod[x-1,cardg[l]]; y1=Ceiling[y/cardg[l]];
      y2=1+Mod[y-1,cardg[l]]; k2=prodg[l][x2,chi[l][x1,y2]];
      k1=proda[l][x1,y1]; (k1-1)*cardg[l]+k2];
prod[l_,x_,y_,4]:=Module[{k1,k2,x1,x2,y1,y2}, x1=Ceiling[x/cardg[l]];
      x2=1+Mod[x-1,cardg[l]]; y1=Ceiling[y/cardg[l]];
```

```
      y2=1+Mod[y-1,cardg[l]];
      k1=proda[l][proda[l][x1,y1],chi[l][x2,y2]];
      k2=prodg[l][x2,y2]; (k1-1)*cardg[l]+k2];
prod[l_,x_,y_,5]:=Module[{k1,k2,x1,x2,y1,y2}, x1=Ceiling[x/cardg[l]];
      x2=1+Mod[x-1,cardg[l]]; y1=Ceiling[y/cardg[l]];
      y2=1+Mod[y-1,cardg[l]];
      k2=prodg[l][prodg[l][x2,y2],chi[l][x1,y1]];
      k1=proda[l][x1,y1]; (k1-1)*cardg[l]+k2];
proyeccion[j_][0][l_]:=fzn[j][l];
proyeccion[j_][1][l_]:=fmodban[j][aw[isopd[j][l]]];
proyeccion[j_][2][l_]:=fmodps[j,2][awps[j,2][isops[j,2][l]]];
proyeccion[j_][3][l_]:=fmodps[j,3][awps[j,3][isops[j,3][l]]];
proyeccion[j_][4][l_]:=fmodec[j,4][awec[j,4][isoec[j,4][l]]];
proyeccion[j_][5][l_]:=fmodec[j,5][awec[j,5][isoec[j,5][l]]];
inyeccion[j_][0][l_]:=gzn[j][l];
inyeccion[j_][1][l_]:=invisopd[j][eml[gmodban[j][l]]];
inyeccion[j_][2][l_]:=invisops[j,2][emlps[j,2][gmodps[j,2][l]]];
inyeccion[j_][3][l_]:=invisops[j,3][emlps[j,3][gmodps[j,3][l]]];
inyeccion[j_][4][l_]:=invisoec[j,4][emlec[j,4][gmodec[j,4][l]]];
inyeccion[j_][5][l_]:=invisoec[j,5][emlec[j,5][gmodec[j,5][l]]];
homotopia[j_][0][l_]:=fizn[j][l];
homotopia[j_][1][l_]:=invisopd[j][shi[j][isopd[j][l]]]+
      invisopd[j][eml[fimodban[j][aw[isopd[j][l]]]]];
homotopia[j_][2][l_]:=invisops[j,2][ships[j,2][isops[j,2][l]]]+
      invisops[j,2][emlps[j,2][fimodps[j,2][awps[j,2][isops[j,2][l]]]]];
homotopia[j_][3][l_]:=invisops[j,3][ships[j,3][isops[j,3][l]]]+
      invisops[j,3][emlps[j,3][fimodps[j,3][awps[j,3][isops[j,3][l]]]]];
homotopia[j_][4][l_]:=invisoec[j,4][shiec[j,4][isoec[j,4][l]]]+
      invisoec[j,4][emlec[j,4][fimodec[j,4][awec[j,4][isoec[j,4][l]]]]];
homotopia[j_][5][l_]:=invisoec[j,5][shiec[j,5][isoec[j,5][l]]]+
      invisoec[j,5][emlec[j,5][fimodec[j,5][awec[j,5][isoec[j,5][l]]]]];
dif[x_][m_][l_+k_]:=dif[x][m][l]+dif[x][m][k];
dif[x_][m_][l_*k_]:=Expand[l*dif[x][m][k]];
dif[x_][m_][0]:=0;
dif[x_][0][l_]:=difzn[x][l];
dif[x_][1][l_]:=Module[{l1,l2}, l1=Take[l,hojimb[[x,1]]];
```

```
      l2=Take[l,-hojimb[[x,2]]]; Expand[pegar[da[x][l1],l2]+
      (-1)^Apply[Plus,l1]*pegar[l1,dg[x][l2]]]];
dif[x_][2][l_]:=Module[{l1,l2}, l1=Take[l,hojimb[[x,1]]];
      l2=Take[l,-hojimb[[x,2]]]; Expand[pegar[da[x][l1],l2]+
      (-1)^Apply[Plus,l1]*pegar[l1,dg[x][l2]]+difmodps[x,2][l]]];
dif[x_][3][l_]:=Module[{l1,l2}, l1=Take[l,hojimb[[x,1]]];
      l2=Take[l,-hojimb[[x,2]]]; Expand[pegar[da[x][l1],l2]+
      (-1)^Apply[Plus,l1]*pegar[l1,dg[x][l2]]+difmodps[x,3][l]]];
dif[x_][4][l_]:=Module[{l1,l2}, l1=Take[l,hojimb[[x,1]]];
      l2=Take[l,-hojimb[[x,2]]]; Expand[pegar[da[x][l1],l2]+
      (-1)^Apply[Plus,l1]*pegar[l1,dg[x][l2]]+difmodec[x,4][l]]];
dif[x_][5][l_]:=Module[{l1,l2}, l1=Take[l,hojimb[[x,1]]];
      l2=Take[l,-hojimb[[x,2]]]; Expand[pegar[da[x][l1],l2]+
      (-1)^Apply[Plus,l1]*pegar[l1,dg[x][l2]]+difmodec[x,5][l]]];
proda[niv_][x_,y_]:=prod[infoarbol[[niv,3]],x,y,infoarbol[[niv,1]]];
prodg[niv_][x_,y_]:=prod[infoarbol[[niv,4]],x,y,infoarbol[[niv,2]]];
fa[niv_][l_]:=proyeccion[infoarbol[[niv,3]]][infoarbol[[niv,1]]][l];
ga[niv_][l_]:=inyeccion[infoarbol[[niv,3]]][infoarbol[[niv,1]]][l];
fia[niv_][l_]:=homotopia[infoarbol[[niv,3]]][infoarbol[[niv,1]]][l];
fg[niv_][l_]:=proyeccion[infoarbol[[niv,4]]][infoarbol[[niv,2]]][l];
gg[niv_][l_]:=inyeccion[infoarbol[[niv,4]]][infoarbol[[niv,2]]][l];
fig[niv_][l_]:=homotopia[infoarbol[[niv,4]]][infoarbol[[niv,2]]][l];
da[niv_][l_]:=dif[infoarbol[[niv,3]]][infoarbol[[niv,1]]][l];
dg[niv_][l_]:=dif[infoarbol[[niv,4]]][infoarbol[[niv,2]]][l];
```

Por último, construimos la diferencial del grupo producto iterado, y la proyección de la contracción que va al modelo homológico del mismo (igualmente podríamos codificar los restantes morfismos de dicha contracción). La variable `ar` detecta si se tiene que aplicar `isobar`, en función de que el grupo de entrada sea o no conmutativo.

```
Module[{ar}, If[arbol[[1,1]]==0,
      farbol[l_]:=fzn[card[[1]]][l];
      difarbol[l_]:=dif[card[[1]]][0][l];
      prodarbol[x_,y_]:=1+Mod[x+y-2,card[[1]]],
ar=Select[Flatten[arbol,1],#1>1&]; If[Length[ar]>0, ar=1, ar=0];
farbol[l_]:=Expand[proyeccion[1][arbol[[1,1]]][isobar[ar][l]]];
difarbol[l_]:=Expand[dif[1][arbol[[1,1]]][l]];
```

```
prodarbol[x_,y_]:=prod[1,x,y,arbol[[1,1]]]];
```

Para efectuar cálculos concretos de homología basta llamar a la rutina que realiza el algoritmo de Veblen.

Apliquemos el procedimiento para determinar la homología en dimensión 1 y 2 de los grupos iterados $(\mathbb{Z}_{tf} \rtimes \mathbb{Z}_2) \ltimes_\chi \mathbb{Z}_2$, para $1 \leq t \leq 5$, con $f_2(-1,-1) = \lceil \frac{t}{2} \rceil + 1$ y $\chi(-1,b) = -b$.

En la salida incluimos las matrices que representan las diferenciales d_i respecto de las bases del modelo que da `basemod[i,2]`.

t	1	2	3
$M(d_2)$	$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$
$M(d_3)$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$
H_1	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$
H_2	$\mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2$

t	4	5
$M(d_2)$	$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 0 & 0 \\ -2 & 0 & 0 \\ 1 & 2 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 5 & 0 & 0 \\ 0 & 0 & 0 \\ -3 & 0 & 0 \\ 1 & 2 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$
$M(d_3)$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \\ 2 & 0 & 4 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ -2 & 0 & -4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 2 & 0 \\ 0 & 0 & -1 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 & 0 \\ 3 & 0 & 5 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ -3 & 0 & -5 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 2 & 0 \\ 0 & 0 & -1 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$
H_1	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$
H_2	$\mathbb{Z}_2$	0

2.6 Estudio de estructuras

En esta sección pretendemos estudiar las estructuras algebraicas subyacentes en las contracciones establecidas a lo largo del capítulo, con vistas a recortar la complejidad del proceso de cálculo de la (co)homología de productos iterados de extensiones centrales y productos semidirectos de grupos abelianos finitos.

Para ello, primero revisaremos algunos resultados concernientes a la preservación de estructuras de (co)álgebra en la perturbación de contracciones; y, posteriormente, nos introduciremos en el ámbito de las A_∞-*estructuras*.

2.6.1 Preservación de estructuras de (co)álgebra

En [47, 48, 72] se acuña el término de *contracción de (co)álgebras* para aquellas contracciones $c : \{A, A', f, g, \phi\}$ en las que f y g son morfismos de DGA-(co)álgebras y ϕ una homotopía de (co)álgebras; esto es, verificando la identidad siguiente:

$$\phi *_A = *_A \phi^{[\otimes 2]} \quad \text{(respectivamente, } \Delta_A \phi = \phi^{[\otimes 2]} \Delta_A),$$

donde notamos $\phi^{[\otimes 2]} = 1 \otimes \phi + \phi \otimes gf$.

En [98], se muestra un test para determinar si el operador de homotopía ϕ de una contracción dada, $c : \{A, A', f, g, \phi\}$, es o no una homotopía de (co)álgebras: para que lo sea, es necesario que se verifique que

$$\phi \circ *_A \circ \phi^{[\otimes 2]} = 0 \quad \text{(respectivamente, } \phi^{[\otimes 2]} \circ \Delta_A \circ \phi = 0).$$

No obstante, gran parte de las contracciones que relacionan dos (co)álgebras no llegan a ser contracciones de (co)álgebras, puesto que alguno de entre los morfismos que las componen no verifica la propiedad pertinente. Esto hizo interesante el estudio de la preservación de estas estructuras bajo condiciones más débiles.

A continuación, se expone la clasificación de las contracciones de DGA-(co)álgebras que recoge Real en [98], según el grado de compatibilidad que presenten sus morfismos componentes con respecto de las estructuras multiplicativas subyacentes.

La proyección f es una *casi-proyección de (co)álgebras* cuando se dan las siguientes condiciones:

$$\begin{aligned} f(\phi *_A \phi) &= 0, \\ f(\phi *_A g) &= 0, \\ f(g *_A \phi) &= 0, \\ \text{(respectivamente, } (f \otimes f)\Delta_A \phi &= 0). \end{aligned}$$

La inyección g es una *casi-inyección de (co)álgebras* cuando $\phi(g *_A g) = 0$, en el caso de álgebras; o bien

$$\begin{aligned} (\phi \otimes \phi)\Delta_A g &= 0, \\ (\phi \otimes f)\Delta_A g &= 0, \\ (f \otimes \phi)\Delta_A g &= 0, \end{aligned}$$

en el caso de coálgebras.

El operador de homotopía ϕ es una *casi-homotopía de (co)álgebras* cuando se dan las condiciones:

$$\begin{aligned} \phi(\phi *_A \phi) &= 0, \\ \phi(\phi *_A g) &= 0, \\ \phi(g *_A \phi) &= 0, \end{aligned}$$

en el caso de álgebras; o bien,

$$\begin{aligned} (\phi \otimes \phi)\Delta_A \phi &= 0, \\ (\phi \otimes f)\Delta_A \phi &= 0, \\ (f \otimes \phi)\Delta_A \phi &= 0, \end{aligned}$$

en el caso de coálgebras.

Esto permite caracterizar varios tipos de contracciones de (co)álgebras:

- Una contracción de (co)álgebras es *semicompleta*, si f es una casi-proyección de (co)álgebras, g es un morfismo de DGA-(co)álgebras y ϕ es una casi-homotopía de (co)álgebras.
- Una contracción de (co)álgebras es *casicompleta* si f y g son morfismos de DGA-(co)álgebras y ϕ es una casi-homotopía de (co)álgebras.
- Una contracción de álgebras se dice *completa* si f y g son morfismos de DGA-(co)álgebras y ϕ es una homotopía de (co)álgebras. Esta noción coincide con la de contracción de (co)álgebras propia de [47, 48, 72].

Evidentemente, las contracciones semicompletas engloban a las casicompletas, así como éstas engloban a las completas. Real propone asimismo en [98] sendos tests para diferenciar unas de otras:

- Una contracción de (co)álgebras casicompleta será completa si y sólo si

$$\phi(1 *_A \phi) = 0 \quad \text{(respectivamente, } (1 \otimes \phi)\Delta_A \phi = 0).$$

- Por otra parte, una contracción semicompleta será casicompleta si y sólo si

$$f(1 *_A \phi) = 0 \quad \text{(respectivamente, } (1 \otimes \phi)\Delta_A g = 0).$$

No es difícil probar que los conjuntos de contracciones de (co)álgebras semicompletas y casicompletas son cerrados por composición y producto tensorial de contracciones. Por el contrario, tanto la composición como el producto tensorial de contracciones completas degeneran en general hacia contracciones casicompletas.

En las secciones previas hemos visto algunas contracciones que pueden servir ahora de ejemplo, si atendemos a la estructura de *álgebra de Hopf* que presenta la construcción bar de una DGA-álgebra conmutativa.

Efectivamente, la construcción bar presenta una estructura de coálgebra, naturalmente heredada del módulo tensorial, mediante el coproducto tensorial $\Delta_{\bar{B}}$,

$$\Delta_{\bar{B}}([a_1|\cdots|a_n]) = \sum_{i=0}^{n}[a_1|\cdots|a_i]\otimes[a_{i+1}|\cdots|a_n].$$

En caso de ser A conmutativa, $\bar{B}(A)$ adquiere, además, la estructura de DGA-álgebra de Hopf conmutativa con el *producto shuffle* $\star$. Éste es el caso de álgebras libres sobre grupos conmutativos, $\mathbb{Z}[G]$.

En estas circunstancias, podemos caracterizar algunas de las contracciones ya estudiadas:

- En la contracción (2.1), $\bar{B}(\mathbb{Z}[\mathbb{Z}])$ es una DGA-álgebra de Hopf (con el coproducto tensorial y el producto shuffle), mientras que $E(u,1)$ es también otra DGA-álgebra de Hopf (con el coproducto usual, $\Delta(u) = u\otimes 1 + 1\otimes u$; y el producto nulo, $u\cdot u = 0$).

  Se puede comprobar que, desde el punto de vista de álgebra, se trata de una contracción casicompleta. Sin embargo, desde el punto de vista de coálgebra, tan sólo se tiene que la inyección es un morfismo de DGA-coálgebras.

- En la contracción (2.2), $\bar{B}(\mathbb{Z}[\mathbb{Z}_n])$ y $E(u,1)\otimes\Gamma(w,2)$ resultan ser DGA-álgebras de Hopf, esta última no conmutativa, con el coproducto heredado, $(f\otimes f)\Delta_{\bar{B}}g$, y el producto tensorial natural.

  Desde el punto de vista de álgebra esta contracción es casicompleta. Desde el punto de vista de coálgebra ninguno de los morfismos presenta compatibilidad alguna con la estructura de coálgebra.

- Si consideramos la contracción Eilenberg-Zilber (2.13) con $X = G$ e $Y = G'$ grupos simpliciales, resulta que $C_*(G\times G')$ y $C_*(G)\otimes C_*(G')$ adquieren la

estructura de DGA-álgebras de Hopf; mediante el *producto de Pontrjagin* y el *coproducto de Alexander-Whitney*:

- El producto de Pontrjagin (ó de *Eilenberg-Mac Lane*), $*_{C(G)}$, viene dado por la composición del operador $EML_{G,G'}$ con el morfismo de DG-módulos inducido por el producto de G, $\bullet : C_*(G \times G) \to C_*(G)$,

$$(x_p *_{C(G)} y_q) = \sum_{(\alpha,\beta)} (-1)^{sg(\alpha,\beta)} s_{\beta_q} \cdots s_{\beta_1} x_p \bullet s_{\alpha_p} \cdots s_{\alpha_1} y_q,$$

  donde el índice del sumatorio (α, β) recorre los (p, q)-shuffles.

- El coproducto Alexander-Whitney, $\Delta_K : C_*(K) \to C_*(K) \otimes C_*(K)$, definido sobre un conjunto simplicial K, consiste en la composición de la aplicación diagonal $C_*(K) \to C_*(K \times K)$ y el operador de Alexander-Whitney $AW_{K,K}$,

$$\Delta_K(x_n) = \sum_{i=0}^{n} \partial_{i+1} \cdots \partial_n x_n \otimes \partial_0 \cdots \partial_{i-1} x_n.$$

Se puede comprobar que la contracción así establecida es casicompleta, desde el punto de vista de álgebra; y, desde el punto de vista de coálgebra, la inyección es un morfismo de DGA-coálgebras.

- Consideremos ahora la contracción que provee el Teorema de Eilenberg Zilber Torcido (ver teoremas 2.3.3 y 2.3.4) para el caso de grupos simpliciales $X = G$ e $Y = G'$,

$$EZ_{G,G'} : \{C_*(G \times_\tau G'),\ C_*(G) \otimes_t C_*(G'),\ AW_\tau,\ EML_\tau,\ SHI_\tau\},$$

que resulta de la perturbación de la contracción Eilenberg Zilber usual según el dato (2.15),

$$\begin{array}{rcl} \delta : C_*(\bar{W}(A) \times \bar{W}(G)) & \to & C_*(\bar{W}(A) \times \bar{W}(G)) \\ (\bar{a}, \bar{g}) & \mapsto & (\tau(\bar{g}) + \partial_0 \bar{a}, \partial_0 \bar{g}) - (\partial_0 \bar{a}, \partial_0 \bar{g}). \end{array}$$

En [4] (pág. 63, Teorema 3.2.25) se demuestra que esta contracción es semicompleta, siempre que $G \times_\tau G'$ sea un producto cartesiano torcido principal dotado de la ley de grupos usual.

- En la contracción (2.3), siempre que los grupos G y G' sean conmutativos, tanto $\bar{B}(\mathbb{Z}[G] \otimes \mathbb{Z}[G'])$ (producto shuffle y coproducto tensorial), como $\bar{B}(\mathbb{Z}[G]) \otimes \bar{B}(\mathbb{Z}[G'])$ (producto tensorial y coproducto Alexander-Whitney), son DGA-álgebras de Hopf.

En estas circunstancias, esta contracción es casicompleta desde el punto de vista de álgebra; mientras que, desde el punto de vista de coálgebra, la inyección es un morfismo de DGA-coálgebras.

No obstante, esta clasificación de contracciones de (co)álgebras no es del todo satisfactoria, en tanto en cuanto hay contracciones de una (co)álgebra a un DG-módulo en las que se puede observar cierta preservación de estructuras; que se han dado en llamar A_∞-estructuras, y que no son más que (co)álgebras asociativas salvo homotopía, a describir a continuación.

2.6.2 A_∞-estructuras

En su estudio sobre H-espacios [114], Stasheff se percató de que la asociatividad de las (co)álgebras no era en general una propiedad invariante por homotopía, pero casi. Él mismo estableció una definición formal para ese "casi", definiendo las *A_∞-estructuras* u objetos con *asociatividad fuertemente homotópica.*

Con el paso de los años, estos objetos se han descrito desde diferentes puntos de vista:

1. Geométrico.

   Sea un DG-módulo (M, m_1) (i.e., $m_1 m_1 = 0$), dotado de un producto m_2 compatible con la diferencial (i.e., $m_1 m_2 = m_2(m_1 \otimes 1 + 1 \otimes m_1)$); que, aunque no asociativo en el sentido estricto, sí sea asociativo *salvo homotopía* m_3: de modo que $m_3(m_1 \otimes 1 \otimes 1) + m_1 m_3 = m_2(m_2 \otimes 1) - m_2(1 \otimes m_2)$.

   Este proceso se puede generalizar, de modo que existan homotopías m_i análogas que midan la falta de asociatividad en las diversas formas de agrupar los productos de i elementos dados (nótese que el conjunto completo de formas distintas viene dado por el conjunto de árboles binarios de i hojas). Stasheff diseñó en [114, 115] una sucesión de poliedros K_i, cuyos vértices representan cada forma de multiplicar i elementos, y cuyas aristas representan que los vértices adyacentes son homotópicos; es más, el poliedro en sí es un ciclo en $\mathrm{Hom}(M^{\otimes i}, M)$, que es imagen de un borde, que identifica como la propia homotopía m_i. Se puede desarrollar un procedimiento análogo para coálgebras salvo homotopía.

2. Analítico.

   Una A_∞-álgebra (resp., A_∞-coálgebra) es un DG-módulo (M, m_1) (resp., (M, Δ_1)) dotado de una familia de morfismos $m_i \in \mathrm{Hom}(M^{\otimes i}, M)$ (resp., $\Delta_i \in \mathrm{Hom}(M, M^{\otimes i})$) de grado $i-2$ de modo que, para $i \geq 1$ (donde i indica el número de elementos a multiplicar), es

$$\sum_{n=1}^{i} \sum_{k=0}^{i-n} (-1)^{n+k+nk} m_{i-n+1}(1^k \otimes m_n \otimes 1^{i-n-k}) = 0,$$

$$(\text{resp., } \sum_{n=1}^{i} \sum_{k=0}^{i-n} (-1)^{n+k+nk} (1^{i-n-k} \otimes \Delta_n \otimes 1^k)\Delta_{i-n+1} = 0).$$

3. Algebraico.

   Una A_∞-álgebra (resp., A_∞-coálgebra) es un módulo graduado M dotado de una aplicación lineal $m : T(sM) \to M$ (resp., $\Delta : M \to T(s^{-1}M)$) tal que el morfismo $d = -(smT(s^{-1})^{[]}$ (resp., $d = -(T(s^{-1})\Delta s)^{[]}$) hace de $T(sM)$ (resp., $T(s^{-1}M)$) una DGA-coálgebra (resp., DGA-álgebra) [95].

4. Funtorial.

   Una A_∞-(co)álgebra es la imagen de una (co)álgebra por una contracción [75].

La técnica algebraica cristalizó en los trabajos, primero de Gugenheim [46], a quien se añadió posteriormente Stasheff [51] y por último Lambe [48]; en lo que se da en llamar *ardid tensorial*, de modo que a partir de una contracción $A \overset{\varsigma}{\Rightarrow} M$ de una DGA-(co)álgebra a un DG-módulo, tensorizando y perturbando adecuadamente para obtener la construcción (co)bar, se define bajo ciertas condiciones (comúnmente, A conexo o simplemente conexo) una A_∞-estructura de (co)álgebra sobre el DG-módulo inicial. El recíproco es asimismo válido, y conforma el novedoso enfoque funtorial de [75].

En este traspaso de información, aparecen de manera natural ciertas cocadenas de torsión y productos tensoriales torcidos, canónicamente asociadas a las cocadenas de torsión universales θ de las construcciones bar y cobar, respectivamente.

Más concretamente, en [13] se prueba que dada una cocadena de torsión $\tau : C \to A$ y un A-módulo L existe una cocadena de torsión $\tau^* : C \to E$, donde $E = \mathrm{End}\,(H(L))$ es el álgebra de endomorfismos de la homología de L con diferencial trivial. Más

aún, los productos tensoriales torcidos $C \otimes_\tau L$ y $C \otimes_{\tau^*} H(L)$ son homológicamente equivalentes.

Por otro lado, Kadeishvili prueba en [76] que toda álgebra A induce una A_∞-estructura sobre $H(A)$ y una cocadena de torsión $\tau : \tilde{B}(H(A)) \to A$. Además, si $t : C \to A$ es otra cocadena de torsión, existe una *A_∞-cocadena de torsión* $\tilde{t} : C \to H(A)$, de modo que t es homótopa a $\tau\tilde{t}$.

Aquí entendemos por A_∞-cocadena de torsión una aplicación lineal de grado -1, $t : C \to A$, con C una DGA-coálgebra y A una A_∞-álgebra (respectivamente, A una DGA-álgebra y C una A_∞-coálgebra); de manera que

$$td + \sum_{i=1}^{\infty} m_i t^{\otimes i} \Delta^{(i)} = 0$$

$$(\text{resp.,} \quad dt + \sum_{i=1}^{\infty} \mu^{(i)} t^{\otimes i} \Delta_i = 0),$$

donde $\Delta^{(1)} = 1$, $\mu^{(1)} = 1$, $\Delta^{(2)} = \Delta$, $\mu^{(2)} = \mu$ y en general $\Delta^{(k)} = (1 \otimes \Delta^{(k-1)})\Delta$ y $\mu^{(k)} = \mu(1 \otimes \mu^{(k-1)})$.

De otro modo, $t : C \to A$ es una A_∞-cocadena de torsión si y sólo si posee una única elevación $\tilde{t} : C \to \tilde{B}(A)$ (resp., $\tilde{t} : \tilde{\Omega}(C) \to A$) que constituye un morfismo de DGA-coálgebras (resp., DGA-álgebras), con $t = \theta\tilde{t}$ (resp., $t = \tilde{t}\theta$).

En [48] Gugenheim, Lambe y Stasheff extrapolan los resultados anteriores en función del ardid tensorial, mediante el siguiente planteamiento.

Dada un álgebra M, la aplicación $\rho : M \to \mathrm{End}\,(M)$ definida por $\rho(a)(b) = ab$ resulta ser un morfismo de álgebras, en virtud de la asociatividad del producto en M. En el caso de que M sea una A_∞-álgebra, ρ deja de ser un morfismo de álgebras por la pérdida de la asociatividad en M, aunque no obstante verifica una compatibilidad "homotópica" con respecto al producto, propia de un homomorfismo de A_∞-álgebras: ρ admite una extensión a una aplicación de DG-coálgebras $\tilde{\rho} : \tilde{B}(M) \to \bar{B}(\mathrm{End}(M))$, de modo que $\tilde{\rho} = \rho\tilde{\theta}$, para $\tilde{\theta}$ la cocadena universal en $\tilde{B}(M)$.

Así, cualquier A_∞-cocadena de torsión $t : C \to M$ admite una elevación $\tilde{t} = \rho t : C \to \mathrm{End}(M)$ a una cocadena de torsión en el sentido estricto.

En estas circunstancias, el último teorema recogido en [48] aserta que dada una cocadena de torsión $C \to A$ y una contracción $(f, g, \phi) : A \to M$ para un cierto DGC-

módulo M, existe una A_∞-estructura sobre M (heredada de la contracción mediante el ardid tensorial), una A_∞-cocadena de torsión $\tilde{t} : C \to M$ y sendas cocadenas de torsión (en el sentido estricto) $t^* : C \to \mathrm{End}(M)$ y $\bar{t} : C \to \bar{B}(A)$ de modo que $\tilde{t} = \tilde{\theta} f_\infty \bar{t}$ y $t^* = \rho \tilde{t}$. Además, $f_\infty : \bar{B}(A) \to \tilde{B}(M)$ define un casi-isomorfismo de coálgebras.

Más aún, los productos tensoriales torcidos $C \otimes_t A$ y $C \otimes_{t^*} M$ y el A_∞-producto tensorial torcido $C \otimes_{\tilde{t}} M$ son homológicamente equivalentes entre sí.

Nótese que toda A_∞-cocadena de torsión $t : C \to A$ da lugar a un A_∞-producto tensorial torcido, de manera que la diferencial d_t en el complejo $A \otimes_t C$ viene dada por

$$d_t = 1 \otimes d + \sum_{i=1}^{\infty} (m_i \otimes 1)(1 \otimes t^{\otimes i-1} \otimes 1)(1 \otimes \Delta^{(i)})$$

$$(\text{resp., } d_t = d \otimes 1 + \sum_{i=1}^{\infty} (\mu^{(i)} \otimes 1)(1 \otimes t^{\otimes i-1} \otimes 1)(1 \otimes \Delta_i)).$$

Aunque los autores dejan abierta la posibilidad de extender estos resultados para el caso dual de coálgebras, advierten que el ardid tensorial puede no definir un proceso finito (a causa de que el dato de perturbación tal vez pueda no disminuir la gradación de la filtración canónica asociada; es decir, que en definitiva no dé lugar a un proceso de perturbación convergente).

En [1] se establece este resultado en el contexto de las contracciones, y se generaliza para el primigenio caso de A_∞-álgebras:

Teorema 2.6.1 *[1] Sea $A \otimes_t C$ el producto tensorial torcido según una cocadena de torsión $t : C \to A$ y consideremos una contracción $c(f, g, \phi) : C \Rightarrow C'$. Supongamos que c induce sobre C' una estructura de A_∞-coálgebra, que $t\phi = 0$ y que $(1 \otimes \phi)t\cap$ es puntualmente nilpotente. Entonces, existe una contracción*

$$A \otimes_t C \Rightarrow A \otimes_{\bar{t}} C',$$

donde $\bar{t} = tg$ es una A_∞-cocadena de torsión y $A \otimes_{\bar{t}} C'$ un A_∞-producto tensorial torcido.

Teorema 2.6.2 *[1] Sea $A \otimes_t C$ el producto tensorial torcido según una cocadena de torsión $t : C \to A$ y consideremos una contracción $c(f, g, \phi) : A \Rightarrow A'$. Supongamos*

que c induce sobre A' una estructura de A_∞-álgebra, que $\phi t = 0$ y que $(\phi \otimes 1)t\cap$ es puntualmente nilpotente. Entonces, existe una contracción

$$A \otimes_t C \Rightarrow A' \otimes_{\bar{t}} C,$$

donde $\bar{t} = ft$ es una A_∞-cocadena de torsión y $A' \otimes_{\bar{t}} C$ un A_∞-producto tensorial torcido.

En particular, la A_∞-estructura de coálgebra de que habla el Teorema 2.6.1 viene dada para $i \geq 2$ por

$$\Delta_i = (-1)^{\frac{(i-1)(i-2)}{2}} f^{\otimes i} \left[\sum_{k_2=1}^{2} \sum_{k_3=1}^{k_2+1} \cdots \sum_{k_{i-1}=1}^{k_{i-2}+1} \prod_{j=2}^{i-1} (-1)^{k_j} (1^{\otimes k_j - 1} \otimes \Delta_C \phi \otimes 1^{\otimes j - k_j}) \right] \Delta_C g,$$

donde el símbolo $\prod_{j=2}^{i-1} h_j$ representa la composición $h_{i-1} \circ \cdots \circ h_2$.

Ahora estamos en condiciones de indagar acerca de las estructuras que subyacen en los modelos (co)homológicos determinados a lo largo del presente capítulo.

2.6.3 Estructuras en modelos (co)homológicos de productos directos

Analicemos las estructuras que aparecen en la contracción

$$c_\times : \{(\cdots((A_1 \times A_2) \times A_3) \cdots) \times A_t), hA_1 \otimes \cdots \otimes hA_t, f_\times, g_\times, \phi_\times\}$$

que da lugar al modelo homológico (2.8) de productos directos de grupos abelianos, que resultaba de la composición

$$\bar{B}(\mathbb{Z}[(\cdots((A_1 \times A_2) \times A_3) \cdots \times A_t)]) \cong \bar{B}(\mathbb{Z}[A_1] \otimes \cdots \otimes \mathbb{Z}[A_t]) \Longrightarrow$$

$$\overset{\text{composición reiterada de } C_{\bar{B}\otimes}}{\Longrightarrow} (\bigotimes_{i=1}^{t} \bar{B}(\mathbb{Z}[A_i]) \overset{\text{producto tensorial de } C_{\mathbb{Z},\mathbb{Z}_n}}{\Longrightarrow} \bigotimes_{i=1}^{t} hA_i,$$

con cada $A_i \in \{\mathbb{Z}, \mathbb{Z}_{n_i}\}$.

Dado que tanto las contracciones $C_{\bar{B}\otimes}$ como las $C_{\mathbb{Z},\mathbb{Z}_n}$ son casicompletas, y éste es un carácter hereditario por composición de contracciones, es fácil deducir que (2.8) es casicompleta desde el punto de vista de álgebras; de modo que $\otimes_{i=1}^{t} hA_i$ es una

CDGA-álgebra de Hopf (no conmutativa, de ser finito alguno de los A_i), siendo $f_\times$ y $g_\times$ morfismos de álgebras y $\phi_\times$ una casi-homotopía de álgebras.

Por el contrario, en principio, nada podemos decir desde el punto de vista de coálgebras para esta contracción, dado que los morfismos de $C_{\mathbb{Z}_n}$ no son compatibles con esta estructura.

No obstante, pese a que $C_{\bar{B}\otimes}$ y $C_{\mathbb{Z},\mathbb{Z}_n}$ no son siquiera semicompletas desde el punto de vista de coálgebras, sí es conveniente destacar ciertas relaciones menores de compatibilidad entre los coproductos existentes y los morfismos componentes de dichas contracciones.

Lema 2.6.3 *La contracción* $C_{\mathbb{Z}}(f_{\mathbb{Z}}, g_{\mathbb{Z}}, \phi_{\mathbb{Z}}) : \bar{B}(\mathbb{Z}[\mathbb{Z}]) \Longrightarrow E$ *verifica que:*

1. $(\phi_{\mathbb{Z}} \otimes \phi_{\mathbb{Z}})\Delta\phi_{\mathbb{Z}} = 0.$
2. $(\phi_{\mathbb{Z}} \otimes f_{\mathbb{Z}})\Delta\phi_{\mathbb{Z}} = 0.$
3. $(f_{\mathbb{Z}} \otimes \phi_{\mathbb{Z}})\Delta_{\mathbb{Z}} \neq 0.$
4. $(f_{\mathbb{Z}} \otimes f_{\mathbb{Z}})\Delta = \Delta f_{\mathbb{Z}}$ *salvo en* $\bar{B}_2(\mathbb{Z}[\mathbb{Z}])$.

Así, $f_{\mathbb{Z}}$ no es morfismo de coálgebras porque $(f \otimes f)\Delta([a|b]) \neq \Delta f([a|b])$. Y $\phi_{\mathbb{Z}}$ no es una casi-homotopía de coálgebras porque $(f_{\mathbb{Z}} \otimes \phi_{\mathbb{Z}})\Delta_{\mathbb{Z}} \neq 0$, en general.

Lema 2.6.4 *La contracción* $C_{\mathbb{Z}_n}(f_{\mathbb{Z}_n}, g_{\mathbb{Z}_n}, \phi_{\mathbb{Z}_n}) : \bar{B}(\mathbb{Z}[\mathbb{Z}_n]) \Longrightarrow E \otimes \Gamma$ *verifica que:*

1. $(\phi_{\mathbb{Z}_n} \otimes \phi_{\mathbb{Z}_n})\Delta g_{\mathbb{Z}_n} = 0.$
2. $(\phi_{\mathbb{Z}_n} \otimes f_{\mathbb{Z}_n})\Delta g_{\mathbb{Z}_n} = 0.$
3. $(\phi_{\mathbb{Z}_n} \otimes \phi_{\mathbb{Z}_n})\Delta\phi_{\mathbb{Z}_n} = 0.$
4. $(\phi_{\mathbb{Z}_n} \otimes f_{\mathbb{Z}_n})\Delta\phi_{\mathbb{Z}_n} = 0.$
5. $(f_{\mathbb{Z}_n} \otimes f_{\mathbb{Z}_n})\Delta\phi_{\mathbb{Z}_n} \neq 0.$

De modo que $g_{\mathbb{Z}_n}$ no es una casi-inyección de coálgebras porque $(f_{\mathbb{Z}_n} \otimes \phi_{\mathbb{Z}_n})\Delta\phi_{\mathbb{Z}_n}$ no es nulo. Y $\phi_{\mathbb{Z}_n}$ no es una casi-homotopía de coálgebras porque $(f_{\mathbb{Z}_n} \otimes \phi_{\mathbb{Z}_n})\Delta_{\mathbb{Z}_n} \neq 0$, en general.

Por otra parte, en [98] se recoge un resultado acerca de la transmisión del (co)producto de una (co)álgebra a un DG-módulo, según una contracción $c : (f, g, \phi)$. De modo que si $\phi(f * f) = 0$ (resp., $(f \otimes f)\Delta\phi = 0$), entonces $* = f(g * g)$ (resp., $\Delta = (f \otimes f)\Delta g$) constituye un (co)producto en el DG-módulo, respecto del cual es g (resp., f) un morfismo de (co)álgebras.

No obstante, aunque $(f_{\mathbb{Z}_n} \otimes f_{\mathbb{Z}_n})\Delta\phi_{\mathbb{Z}_n} \neq 0$ en nuestro caso, el coproducto $\Delta_{E\otimes\Gamma}$ de $E \otimes \Gamma$ sigue siendo el "heredado" por la contracción, de modo que

Lema 2.6.5 *[70]* $\Delta_{E\otimes\Gamma} = (f_{\mathbb{Z}_n} \otimes f_{\mathbb{Z}_n})\Delta g_{\mathbb{Z}_n}$.

Más aún, $\bar{B}(\mathbb{Z}[\mathbb{Z}_n])$ induce una A_∞-estructura de coálgebra sobre $E \otimes \Gamma$ (según el ardid tensorial), de manera que $\Delta_2 = \Delta_{E\otimes\Gamma}$ es asociativo, a pesar de que Δ_3 y los restantes Δ_i, $i > 2$, son todos distintos de cero. El motivo es que

$$(1 \otimes \Delta_2)\Delta_2 - (\Delta_2 \otimes 1)\Delta_2 = (d \otimes 1 \otimes 1 + 1 \otimes d \otimes 1 + 1 \otimes 1 \otimes d)\Delta_3 + \Delta_3 d = 0.$$

Lema 2.6.6 *La A_∞ estructura de coálgebra que induce $\bar{B}(\mathbb{Z}[\mathbb{Z}_n])$ sobre $E \otimes \Gamma$ viene dada por los morfismos Δ_i detallados en el Teorema 2.6.1,*

$$\Delta_i = (-1)^{\frac{(i-1)(i-2)}{2}} f_{\mathbb{Z}_n}^{\otimes i} \left[\sum_{k_2=1}^{2} \sum_{k_3=1}^{k_2+1} \cdots \sum_{k_{i-1}=1}^{k_{i-2}+1} \prod_{j=2}^{i-1} (-1)^{k_j} (1^{\otimes k_j - 1} \otimes \Delta\phi_{\mathbb{Z}_n} \otimes 1^{\otimes j-k_j}) \right] \Delta g_{\mathbb{Z}_n}.$$

Más aún, la fórmula para los Δ_i se reduce a un sólo sumando, a saber

$$\Delta_i = f_{\mathbb{Z}_n}^{\otimes i}(1^{\otimes i-2} \otimes \Delta\phi_{\mathbb{Z}_n}) \cdots (1 \otimes \Delta\phi_{\mathbb{Z}_n})\Delta g_{\mathbb{Z}_n}.$$

2.6.4 Estructuras en modelos (co)homológicos de extensiones centrales

Consideremos una extensión central $A_f \rtimes G$, con A abeliano finito y G producto iterado de extensiones centrales y productos semidirectos de grupos abelianos finitos;

y un modelo homológico suyo, según (2.17),

$$c_{A_f \rtimes G} : \{\bar{B}(\mathbb{Z}[A_f \rtimes G]), hA \tilde{\otimes} hG, f, g, \phi\},$$

donde hA y hG, como módulos graduados (que no DG-módulos), coinciden con productos del tipo $\bigotimes_{i=1}^{t}(E(u_i)\tilde{\otimes}\Gamma(w_i))$.

La contracción (2.17) resultaba de la composición

$$\bar{B}(\mathbb{Z}[A_f \rtimes G]) \overset{\varphi_1}{\Rightarrow} C_*(\bar{W}(A_f \rtimes G)) \overset{\varphi_2}{\Rightarrow} C_*(\bar{W}(A) \times_\tau \bar{W}(G)) \overset{EZ^{\tau}_{\bar{W}(A),\bar{W}(G)}}{\Rightarrow}$$

$$\overset{EZ_{\bar{W}(A),\bar{W}(G)}}{\Rightarrow} C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G)) \overset{C_t\cap}{\Rightarrow} hA \tilde{\otimes} hG$$

Nos podemos preguntar cómo varían las estructuras de (co)álgebra a lo largo de estas contracciones.

Desde el momento en que $A_f \rtimes G$ no es abeliano, el objeto $\bar{B}(\mathbb{Z}[A_f \rtimes G])$ es sólo una DGA-coálgebra, puesto que el producto shuffle no está definido en este caso.

Nota 2.6.7 *En general, $C_*(\bar{W}(A) \times_\tau \bar{W}(G))$ no tiene estructura de CDGA-álgebra.*

Según se recoge en [4], un producto cartesiano torcido principal $G \times_\tau G'$ tiene estructura de grupo simplicial con la ley de grupo usual si y sólo si τ es homomorfismo de grupos, $\tau(g'h') = \tau(g')\tau(h')$.

En nuestro caso, $\tau : \bar{W}(G) \to \bar{W}(A)$ actúa trivialmente en grado 1 ($\tau[g_0] = 0$) y para $n > 1$ viene dada por

$$\tau[g_{n-1}, \ldots, g_0] = [-f(g_{n-2}, g_{n-1}), -f(g_{n-3}, g_{n-2}g_{n-1}) + f(g_{n-3}, g_{n-2}), \ldots,$$

$$-f(g_0, g_1 \cdots g_{n-1}) + f(g_0, g_1 \cdots g_{n-2})].$$

De un lado, se tiene que

$$\tau([g_{n-1}, \ldots, g_0] \cdot [h_{n-1}, \ldots, h_0]) = [-f(g_{n-2}h_{n-2}, g_{n-1}h_{n-1}),$$

$$-f(g_{n-3}h_{n-3}, g_{n-2}h_{n-2}g_{n-1}h_{n-1}) + +f(g_{n-3}h_{n-3}, g_{n-2}h_{n-2}), \ldots,$$

$$, \ldots, -f(g_0h_0, g_1h_1 \cdots g_{n-1}h_{n-1}) + f(g_0h_0, g_1h_1 \cdots g_{n-2}h_{n-2})].$$

De otro,

$$\tau([g_{n-1},\dots,g_0])\cdot\tau([h_{n-1},\dots,h_0]) = [-f(g_{n-2},g_{n-1}) - f(h_{n-2},h_{n-1}),$$

$$-f(g_{n-3},g_{n-2}g_{n-1}) + f(g_{n-3},g_{n-2}) - f(h_{n-3},h_{n-2}h_{n-1}) + f(h_{n-3},h_{n-2}),\dots,$$

$$-f(g_0,g_1\cdots g_{n-1}) + f(g_0,g_1\cdots g_{n-2}) - f(h_0,h_1\cdots h_{n-1}) + f(h_0,h_1\cdots h_{n-2})].$$

Tomando por ejemplo las primeras entradas en estas dos expresiones, se tiene que, en general,

$$-f(g_{n-2}h_{n-2},g_{n-1}h_{n-1}) \neq -f(g_{n-2},g_{n-1}) - f(h_{n-2},h_{n-1}).$$

Baste tomar $h_{n-2} = g_{n-2}^{-1}$ y $h_{n-1} = 1$, de donde

$$-f(g_{n-2}h_{n-2},g_{n-1}h_{n-1}) = 0 \neq -f(g_{n-2},g_{n-1}),$$

en general. Con lo que, efectivamente, $C_*(\bar{W}(A)\times_\tau \bar{W}(G))$ no tiene estructura de CDGA-álgebra, en general.

En el siguiente paso, salvo isocontracción, nos encontramos con un producto tensorial torcido principal, de la CDGA-álgebra $\bar{B}(\mathbb{Z}[A])$ y la CDGA-coálgebra $\bar{B}(\mathbb{Z}[G])$, según la cocadena t.

Nota 2.6.8 *$\bar{B}(\mathbb{Z}[A])\otimes_t \bar{B}(\mathbb{Z}[G])$ no tiene estructura de DGA-álgebra con el producto heredado de los factores.*

En efecto, puesto que en general, G no será conmutativo, de donde $\bar{B}(\mathbb{Z}[G])$ no será DGA-álgebra y no tendrá sentido plantearse un producto heredado en $\bar{B}(\mathbb{Z}[A])\otimes \bar{B}(\mathbb{Z}[G])$, menos aún en el producto tensorial torcido ulterior.

Aún en el caso de que G fuera conmutativo y $\bar{B}(\mathbb{Z}[G])$ admitiera a $\star$ como producto, $\bar{B}(\mathbb{Z}[A])\otimes_t \bar{B}(\mathbb{Z}[G])$ tampoco sería una DGA-álgebra con el producto μ heredado.

La explicación la encontramos en que la perturbación $t\cap$ de la diferencial usual de $\bar{B}(\mathbb{Z}[A])\otimes \bar{B}(\mathbb{Z}[G])$ no conforma una derivación con respecto μ: vamos a probar que, en general,

$$\mu(1\otimes t\cap + t\cap\otimes 1) \neq t\cap\mu.$$

Una fórmula para t en grados 2 y 3 viene dada por $t([g_1, g_0]) = [-f(g_0, g_1)]$ y

$$t([g_2, g_1, g_0]) = [-f(g_1, g_2), -f(g_0, g_1 g_2)] + [-f(g_0, g_1), -f(g_0, g_1 g_2) + f(g_0, g_1)] -$$
$$-[-f(g_1, g_2), -f(g_0, g_1)] + [-f(g_0, g_1), -f(g_1, g_2)].$$

Así, se tiene que

$$\mu(1 \otimes t\cap + t\cap \otimes 1)(1 \otimes [k,k]) \otimes (1 \otimes [k]) = [-f(k,k)] \otimes [k],$$

mientras que

$$t\cap \mu(1 \otimes [k,k]) \otimes (1 \otimes [k]) = t\cap (1 \otimes [k,k,k]) =$$
$$= [-f(k,k)] \otimes [k] + [-f(k,k), -f(k,kk)] \otimes 1 + [-f(k,k), -f(k,kk) + f(k,k)] \otimes 1;$$

de donde

$$\mu(1 \otimes t\cap + t\cap \otimes 1)(1 \otimes [k,k]) \otimes (1 \otimes [k]) \neq t\cap \mu(1 \otimes [k,k]) \otimes (1 \otimes [k]).$$

Por último, llegamos al DG-módulo $hA\tilde{\otimes}hG$, que como módulo graduado es producto de álgebras exteriores y polinomiales divididas, lo que sugiere la posibilidad de que tenga estructura de álgebra. Nada más lejos de la realidad.

Nota 2.6.9 *El DG-módulo $hA\tilde{\otimes}hG$ no posee estructura de álgebra con los productos naturales de las álgebras en que factoriza.*

En efecto, la diferencial $d_{t\cap}$ que se obtiene en $hA \otimes hG$ al perturbar la contracción correspondiente según el dato de perturbación $t\cap$ no constituye una derivación, en general.

Consideremos el caso de los grupos $\mathbb{Z}_{2tf} \rtimes \mathbb{Z}_2$, con $f(-1,-1) = \lceil \frac{t}{2} \rceil + 1$, que ya trabajáramos como ejemplos de extensiones centrales. Un modelo homológico para los mismos, según el Teorema 2.3.5, es del tipo $(E(u_1) \otimes \Gamma(w_1) \otimes E(u_2) \otimes \Gamma(w_2), d)$. En particular, para $t = 3$, se tiene que, de un lado, $d(u_2 \otimes \gamma_1(w_2)) = -\gamma_1(w_1) + 3u_1 \otimes u_2$; mientras que, de otro, $d(u_2) = 0$ y $d(\gamma_1(w_2)) = 3u_1 + 2u_2$, de donde

$$-u_2 * d(\gamma_1(w_2)) + d(u_2) * \gamma_1(w_2) = 3u_1 \otimes u_2 \neq -\gamma_1(w_1) + 3u_1 \otimes u_2 = d(u_2 \otimes \gamma_1(w_2)).$$

Atendamos ahora a las A_∞-estructuras que subyacen en las contracciones anteriores.

Teorema 2.6.10 *El modelo $hA\bar{\otimes}hG$ posee la estructura de A_∞-coálgebra, naturalmente heredada de $\bar{B}(\mathbb{Z}[A_f \rtimes G])$.*

Demostración.

Desglosamos la demostración del teorema en tres procesos de perturbación.

1. Consideremos primero la contracción

$$T^a(s^{-1}(C_*(\bar{W}(A_f \rtimes G)))) \Rightarrow T^a(s^{-1}(C_*(\bar{W}(A) \times_\tau \bar{W}(G))))$$

que induce el isomorfismo simplicial φ_2 de (2.12). El perturbar por la diferencial simplicial d_s de la construcción cobar de $\mathbb{Z}[A_f \rtimes G]$ produce la isocontracción

$$\bar{\Omega}(C_*(\bar{W}(A_f \rtimes G))) \Rightarrow \bar{\Omega}(C_*(\bar{W}(A) \times_\tau \bar{W}(G))),$$

dado que la diferencial perturbada $\delta = T(\varphi_2)d_sT(\varphi_2^{-1})$ coincide con la diferencial simplicial de la construcción cobar de $C_*(\bar{W}(A) \times_\tau \bar{W}(G))$. Más concretamente,

$$\begin{aligned}
&\delta([\{(a^0_{r_0-1},\dots,a^0_0),(g^0_{r_0-1},\dots,g^0_0)\}|\cdots|\{(a^n_{r_n-1},\dots,a^n_0),(g^n_{r_n-1},\dots,g^n_0)\}]) = \\
&\quad = \sum_{k=0}^{n-1}\sum_{j=1}^{r_k-1}(-1)^{r_0+\cdots+r_{k-1}-k-j}[\{(a^0_{r_0-1},\dots,a^0_0),(g^0_{r_0-1},\dots,g^0_0)\}|\cdots \\
&\qquad \cdots|\{(a^k_{r_k-1},\dots,a^k_j),(g^k_{r_k-1},\dots,g^k_j)\}| \\
&|\{(a^k_{j-1}-f(g^k_{j-1},g^k_j\cdots g^k_{r_k-1}),a^k_{j-2}-f(g^k_{j-2},g^k_{j-1}\cdots g^k_{r_k-1})+f(g^k_{j-2},g^k_{j-1}),\cdots \\
&\qquad \dots,a^k_0-f(g^k_0,g^k_1\cdots g^k_{r_k-1})+f(g^k_0,g^k_1\cdots g^k_{j-1})),(g^k_{j-1},\dots,g^k_0)\}|\cdots| \\
&\qquad\qquad |\{(a^n_{r_n-1},\dots,a^n_0),(g^n_{r_n-1},\dots,g^n_0)\}].
\end{aligned}$$

2. Sea ahora la contracción

$$T^a(s^{-1}(C_*(\bar{W}(A) \times_\tau \bar{W}(G)))) \Rightarrow T^a(s^{-1}(C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G)))).$$

Veamos que el proceso de perturbación generado por la diferencial δ anterior es convergente, esto es, que la composición $T(SHI_\tau)\delta$ es puntualmente nilpotente.

De un lado, la aplicación δ separa una de las entradas del módulo tensorial en dos partes, la segunda de al menos dimensión simplicial dos.

De otro, SHI_τ intercala al menos un elemento neutro (1) en la componente de $\bar{W}(G)$ correspondiente, aunque para que su actuación no sea nula no todos sus antecesores pueden ser asimismo 1 en dicha componente. Además, la composición $EML_\tau AW_\tau$ no disminuye el número de 1 en la componente $\bar{W}(G)$.

Teniendo en cuenta estos dos hechos, la iteración de la composición $T(SHI_\tau)\delta$ acabará anulándose.

3. En el siguiente paso, tratamos de perturbar la contracción

$$T^a(s^{-1}(C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G)))) \Rightarrow (T^a(s^{-1}(hA \otimes hG)), d \otimes 1^* + \cdots + 1^* \otimes d)$$

tomando como dato de partida la diferencial d_δ,

$$d_\delta = T(AW_\tau)\delta \sum_{i\geq 0}((-1)^i T(SHI_\tau)\delta)^i T(EML_\tau).$$

Este proceso para, dada la nilpotencia puntual de la composición

$$T(\sum_{i\geq 0}(-1)^i((1 \otimes \phi_G + \phi_A \otimes g_G f_G)t\cap)^i(1 \otimes \phi_G + \phi_A \otimes g_G f_G))d_\delta.$$

Agrupando los pasos 1, 2 y 3 podemos concluir que existe una contracción

$$\bar{\Omega}(\mathbb{Z}[A_f \rtimes G]) \Rightarrow \tilde{\Omega}(hA\tilde{\otimes}hG, d),$$

de modo que se obtiene una estructura de A_∞-coálgebra sobre $hA\tilde{\otimes}hG$.

■

Aunque hemos demostrado la existencia de una estructura algebraica sobre $hA\tilde{\otimes}hG$, podemos ser aún más ambiciosos. Nos consta que $\bar{B}(\mathbb{Z}[A]) \otimes_t \bar{B}(\mathbb{Z}[G])$ es un producto tensorial torcido principal. ¿Acaso tiene una estructura análoga el modelo $hA\tilde{\otimes}hG$? La respuesta es positiva, en el ámbito de las A_∞-estructuras.

Teorema 2.6.11 *Sea A una DG-álgebra, C una DG-coálgebra y $A \otimes_t C$ un producto tensorial torcido principal. Sean $c_A : \{A, A', f_A, g_A, \phi_A\}$ y $c_C : \{C, M, f_C, g_C, \phi_C\}$ sendas contracciones a una DG-álgebra A' y un DG-módulo M, respectivamente; de modo que f_A es morfismo de DG-álgebras, $f_A t \phi_C = 0$ y c' induce sobre M una A_∞-estructura de coálgebra. Entonces, $A' \otimes_{f_A t g_C} M$ conforma un A_∞ producto tensorial torcido. Más aún, existe una contracción de $A \otimes_t C$ en $A' \otimes_{f_A t g_C} M$.*

Demostración.

De un lado, por ser f_A un morfismo de DG-álgebras, el objeto $A' \otimes_{f_A t} C$ adquiere la estructura de producto tensorial torcido principal. Más aún, de la demostración del Teorema 2.6.2 en [1] se sigue la existencia de una contracción $A \otimes_t C \Rightarrow A' \otimes_{f_A t} C$, si necesidad de que la composición $\phi_A t$ sea nula.

Por otra parte, dado que $f_A t \phi_C = 0$, el Teorema 2.6.1 garantiza que $A' \otimes_{f_A t g_C} M$ es un A_∞-producto tensorial torcido, que admite una contracción en la forma $A \otimes_t C \Rightarrow A' \otimes_{f_A t g_C} M$.

■

Teorema 2.6.12 *El DG-módulo $hA\tilde{\otimes}hG$ posee la estructura de A_∞-producto tensorial torcido, según el producto de la CDGA-álgebra hA y la A_∞-estructura de coálgebra sobre hG naturalmente heredada de $\bar{B}(\mathbb{Z}[G])$.*

Demostración.

Vamos a probar que en las circunstancias del enunciado se verifican las hipótesis del Teorema 2.6.11.

A partir de la contracción (2.17) que da el modelo homológico de una extensión central, consideremos el último eslabón de la cadena

$$c_{A_f \rtimes G} : \{\bar{B}(\mathbb{Z}[A]) \otimes_t \bar{B}(\mathbb{Z}[G]), hA\tilde{\otimes}hG, f_{t\cap}, g_{t\cap}, \phi_{t\cap}\},$$

donde

$$f_{t\cap} = (f_A \otimes f_G) \sum_{i\geq 0} (-1)^i (t \cap (1 \otimes \phi_G + \phi_A \otimes g_G f_G))^i$$

$$g_{t\cap} = \sum_{i\geq 0} (-1)^i ((1 \otimes \phi_G + \phi_A \otimes g_G f_G) t\cap)^i (g_A \otimes g_G)$$

$$\phi_{t\cap} = \sum_{i\geq 0} (-1)^i ((1 \otimes \phi_G + \phi_A \otimes g_G f_G) t\cap)^i (1 \otimes \phi_G + \phi_A \otimes g_G f_G).$$

Dado que A es un grupo conmutativo, la contracción $\bar{B}(\mathbb{Z}[A]) \Rightarrow hA$ es casi-completa desde el punto de vista de álgebras; en particular, f_A es un morfismo de DG-álgebras.

Por otra parte, $\bar{B}(\mathbb{Z}[G]) \Rightarrow hG$ induce una A_∞-estructura de coálgebra sobre hG, toda vez que G es producto iterado de extensiones centrales y productos semidirectos de grupos abelianos finitos (basta combinar los Teoremas 2.6.10 y 2.6.15).

Finalmente, $f_A t\phi_G = 0$, según la definición de estos morfismos, en función de los morfismos elementales que dan los modelos homológicos de grupos extensiones centrales, productos semidirectos y grupos finitos tratados al comienzo del presente capítulo.

Luego, según el Teorema 2.6.11, $hA\tilde{\otimes}hG$ posee la estructura de A_∞-producto tensorial torcido, según el producto de la CDGA-álgebra hA y la A_∞-estructura de coálgebra sobre hG naturalmente heredada de $\bar{B}(\mathbb{Z}[G])$

■

En particular, este resultado extiende el que se recoge en el Teorema 6.2.12 de [4], que aserta que el modelo homológico de grupos del tipo $A_f \rtimes \mathbb{Z}^n$, con A abeliano finitamente generado, tiene estructura de producto tensorial torcido principal.

Abordemos ahora el caso de productos semidirectos, considerablemente más complejo.

2.6.5 Estructuras en modelos (co)homológicos de productos semidirectos

Consideremos un producto semidirecto $A \ltimes_\chi G$, con A producto iterado de extensiones centrales y productos semidirectos de grupos abelianos finitos y G abeliano finito; y un modelo homológico suyo, según (2.22),

$$c_{A\ltimes_\chi G} : \{\bar{B}(\mathbb{Z}[A\ltimes_\chi G]), hA\tilde{\otimes}hG, f, g, \phi\},$$

donde hA y hG, como módulos graduados (que no DG-módulos), coinciden con productos del tipo $\oplus_{i=1}^{t}(E(u_i)\tilde{\otimes}\Gamma(w_i))$.

La contracción (2.22) resultaba de la composición

$$\bar{B}(\mathbb{Z}[A\ltimes_\chi G]) \overset{\varphi_1}{\Rightarrow} C_*(\bar{W}(A\ltimes_\chi G)) \overset{\varphi_2}{\Rightarrow} C_*(\bar{W}(A) \times_\tau \bar{W}(G)) \overset{EZ^\tau_{\bar{W}(A),\bar{W}(G)}}{\Rightarrow}$$

$$\overset{EZ_{\bar{W}(A),\bar{W}(G)}}{\Rightarrow} C_*(\bar{W}(A)) \otimes_t C_*(\bar{W}(G)) \overset{C_{t\cap}}{\Rightarrow} hA \tilde{\otimes} hG$$

Al igual que hiciéramos en el caso de extensiones centrales, nos preguntamos cómo varían las estructuras de (co)álgebra a lo largo de estas contracciones.

Desde el momento en que $A \ltimes_\chi G$ no es abeliano, el objeto $\bar{B}(\mathbb{Z}[A \ltimes_\chi G])$ es sólo una DGA-coálgebra, puesto que el producto shuffle no está definido en este caso.

En el siguiente paso, salvo isocontracción, nos encontramos con un producto tensorial torcido no principal, del DGA-módulo $\bar{B}(\mathbb{Z}[A])$ y la CDGA-coálgebra $\bar{B}(\mathbb{Z}[G])$, según la cocadena t y el grupo estructural G.

Nota 2.6.13 $\bar{B}(\mathbb{Z}[A]) \otimes_t \bar{B}(\mathbb{Z}[G])$ *no tiene estructura de DGA-álgebra con el producto heredado de los factores.*

Esto es, porque en general, A no será conmutativo, de donde $\bar{B}(\mathbb{Z}[A])$ no será DGA-álgebra y no tendrá sentido plantearse un producto heredado en $\bar{B}(\mathbb{Z}[A]) \otimes \bar{B}(\mathbb{Z}[G])$, menos aún en el producto tensorial torcido ulterior.

Aún en el caso de que A fuera conmutativo y $\bar{B}(\mathbb{Z}[A])$ admitiera a $\star$ como producto, $\bar{B}(\mathbb{Z}[A]) \otimes_t \bar{B}(\mathbb{Z}[G])$ tampoco sería una DGA-álgebra con el producto μ heredado.

La explicación la encontramos en que la perturbación $t\cap$ de la diferencial usual de $\bar{B}(\mathbb{Z}[A]) \otimes \bar{B}(\mathbb{Z}[G])$ no conforma una derivación con respecto μ: vamos a probar que, en general,

$$\mu(1 \otimes t\cap + t\cap \otimes 1) \neq t\cap \mu.$$

Una fórmula explícita para t viene dada por

$$t[g_{n-1}, \ldots, g_0] = \begin{cases} g_0 - e_0, & \text{si } n = 1; \\ 0, & \text{si } n \geq 2. \end{cases}$$

De donde $t\cap$ actúa en la forma

$$t\cap([a_{m-1}, \ldots, a_0] \otimes [g_{n-1}, \ldots, g_0]) =$$

$$(-1)^m([g_{n-1}a_{m-1}, \ldots, g_{n-1}a_0] - [a_{m-1}, \ldots, a_0]) \otimes [g_{n-2}, \ldots, g_0].$$

Así, se tiene que

$$\mu(1 \otimes t\cap + t\cap \otimes 1)([a] \otimes [g]) \otimes (1 \otimes [h]) = ([a] - [ga]) \otimes [h],$$

mientras que

$$t \cap \mu([a] \otimes [g]) \otimes (1 \otimes [h]) = t \cap ([a] \otimes ([g,h] - [h,g])) =$$

$$= ([a] - [ga]) \otimes [h] - ([a] - [ha]) \otimes [g];$$

de donde

$$\mu(1 \otimes t \cap + t \cap \otimes 1)([a] \otimes [g]) \otimes (1 \otimes [h]) \neq t \cap \mu([a] \otimes [g]) \otimes (1 \otimes [h]).$$

Por último, llegamos al DG-módulo $hA \tilde{\otimes} hG$, que como módulo graduado es producto de álgebras exteriores y polinomiales divididas, lo que sugiere la posibilidad de que tenga estructura de álgebra. Nada más lejos de la realidad.

Nota 2.6.14 *El DG-módulo $hA \tilde{\otimes} hG$ no posee estructura de álgebra con los productos naturales de las álgebras en que factoriza.*

En efecto, la diferencial $d_{t\cap}$ que se obtiene en $hA \otimes hG$ al perturbar la contracción correspondiente según el dato de perturbación $t\cap$ no constituye una derivación, en general.

Consideremos los grupos diédricos $D_{4t} = \mathbb{Z}_{2t} \ltimes_\chi \mathbb{Z}_2$, con $\chi(-1,b) = -b$, que ya tratáramos en la sección de computación y ejemplos dedicada a productos semidirectos; y cuyo modelo homológico es de la forma $(E(u_1) \otimes \Gamma(w_1) \otimes E(u_2)\Gamma(w_2), d)$.

Se tiene que $d(u_1 \otimes u_2) = -2u_1$, mientras que $d(u_1) = 0$ y $d(u_2) = 0$, de modo que

$$d(u_1) * u_2 - u_1 * d(u_2) = 0 \neq -2u_1 = d(u_1 \otimes u_2).$$

Atendamos ahora a las A_∞-estructuras que subyacen en las contracciones anteriores.

Por un lado, se tiene un resultado análogo al descrito para extensiones centrales, que ya se recogiera en [1] en su versión para resoluciones.

Teorema 2.6.15 *[1] La construcción $\bar{B}(\mathbb{Z}[A \ltimes_\chi G])$ induce una A_∞-estructura de coálgebra sobre $hA \tilde{\otimes} hG$.*

Tratemos ahora de ir más allá, según el camino que iniciáramos en el Teorema 2.6.12 para extensiones centrales. En cualquier caso, hemos de tener presente una diferencia fundamental entre ambos casos: si bien para extensiones centrales aparecía un producto tensorial torcido principal, ahora se trata de uno no principal. Eso quiere decir que no se pueden aplicar los teoremas 2.6.1, 2.6.2 y 2.6.11 tal cual.

En realidad, el problema que nos planteamos es el siguiente: estudiar las condiciones bajo las cuales dado un producto tensorial torcido no principal $M \otimes_t C$ y sendas contracciones $M \Rightarrow N$ y $C \Rightarrow C'$ se puede construir $M \otimes_t C \Rightarrow N \otimes_{\bar{t}} C'$.

El siguiente resultado constituye el primer paso hacia la solución.

Teorema 2.6.16 *Sea $M \otimes_t C$ el producto tensorial torcido no principal según una cocadena de torsión $t : C \to A$ y una acción $\mu : M \otimes A \to M$. Consideremos una contracción $c(f, g, \phi) : C \Rightarrow C'$ que induzca sobre C' una estructura de A_∞-coálgebra, y que adicionalmente verifique que $t\phi = 0$ y que $(1 \otimes \phi)t\cap$ es puntualmente nilpotente. Entonces, existe una contracción*

$$M \otimes_t C \Rightarrow M \otimes_{\bar{t}} C',$$

donde $\bar{t} = tg$ es una A_∞-cocadena de torsión y $M \otimes_{\bar{t}} C'$ un A_∞-producto tensorial torcido no principal.

Demostración.

Dado que $(1 \otimes \phi)t\cap$ es puntualmente nilpotente, la perturbación de la contracción

$$M \otimes C \Rightarrow M \otimes C'$$

que se obtiene de c tensorizando por M, según el dato de perturbación $t\cap$; converge para dar la contracción

$$M \otimes_t C \Rightarrow (M \otimes C', 1 \otimes d_{C'} + d_M \otimes 1 + d_{t\cap}),$$

con

$$d_{t\cap} = (1 \otimes f) \sum_{n \geq 0} (-1)^n [(\mu \otimes 1)(1 \otimes t \otimes 1)(1 \otimes \Delta_C)(1 \otimes \phi)]^n (\mu \otimes 1)(1 \otimes t \otimes 1)(1 \otimes \Delta_C g).$$

Por otra parte, como c induce una estructura de A_∞-coálgebra sobre C', por construcción ha de ser $\bar{t} = tg$ una A_∞-cocadena de torsión (según el ardid tensorial desarrollado en [48]).

Así, basta probar que bajo la condición de que $t\phi = 0$, entonces la diferencial $1 \otimes d_C + d_M \otimes 1 + d_{t\cap}$ coincide con la diferencial $d_{\bar{t}}$ que induce $\bar{t}$ en el A_∞-producto tensorial $M \otimes_{\bar{t}} C'$, con

$$d_{\bar{t}} = d_M \otimes 1 + \sum_{i=1}^{\infty} (\mu^{(i)} \otimes 1)(1 \otimes \bar{t}^{i-1} \otimes 1)(1 \otimes \Delta_i),$$

para $\mu^{(1)} = 1$, $\mu^{(2)} = \mu$, $\mu^{(3)} = \mu(1 \otimes *_A)$, y en general $\mu^{(i)} = \mu(1 \otimes *_A^{(i-1)})$; siendo por otra parte $\Delta_1 = \pi_1 \Delta$ y $\Delta_i : C' \to C' \overset{i}{\otimes} \cdots \otimes C'$, $i \geq 2$, la proyección canónica $-\pi_i \Delta$, con Δ el morfismo que determina la estructura de A_∞-coálgebra de C' según la contracción c:

$$d_{\tilde{\Omega}} = (-s^{-1} d_{C'} s)^{[\,]} + d_{\partial_{alg}} = -(T(s^{-1})\Delta s)^{[\,]},$$

$$d_{\partial_{alg}} = T(s^{-1} f s)\partial_{alg}(\sum_{i \geq 0} (-1)^i (T(s^{-1}\phi s)\partial_{alg})^i) T(s^{-1} g s)$$

y

$$\partial_{alg}|_{|\ |_s = n} = \sum_{k=1}^{n} 1^{k-1} \otimes (s^{-1} \otimes s^{-1}) \Delta_C s \otimes 1^{n-k}.$$

El resto de la demostración es una reproducción de la que se da en [1] para el Teorema 2.6.1, con la salvedad de que en este caso los morfismos $\mu^{(i)}$ no representan la manera de multiplicar i elementos de A, sino como se vio antes el resultado de la acción del producto de $i-1$ elementos de A sobre uno de M, $\mu^{(i)} = \mu(1 \otimes *_A^{(i-1)})$.

■

Ahora, hay que estudiar cómo se puede heredar una acción de un álgebra sobre un módulo mediante una contracción.

Sea M un DG-módulo a izquierda de una DG-álgebra A según una aplicación $*_M$ y $c : \{M, N, f, g, \phi\}$ una contracción. En estas circunstancias, el morfismo $*_N$ candidato a constituir una acción de A sobre N viene dado por $m *_N a = f(g(m) *_M a)$.

Lema 2.6.17 *El morfismo $*_N$ establece una acción de A sobre N si y sólo si*

$$f((d\phi + \phi d)(g(m) *_M a) *_M b) = 0, \qquad \forall\, a, b \in A.$$

Demostración.

A tenor de que gf y 1 son homótopos, según la relación $1 - gf = d\phi + \phi d$, es fácil deducir que la ecuación que mide la asociatividad de $*_N$,

$$f(gf(g(m) *_M a) *_M b) = f(g(m) *_M ab),$$

equivale a la condición del enunciado.

■

En estas circunstancias, podemos enunciar el siguiente resultado.

Teorema 2.6.18 *Sea $M \otimes_t C$ el producto tensorial torcido según una cocadena de torsión $t : C \to A$ y consideremos sendas contracciones $c : \{M, N, f_M, g_M, \phi_M\}$ y $c' : \{C, C', f, g, \phi\}$, de modo que c induzca sobre N una estructura de A-módulo a izquierda y c' induzca sobre C' una estructura de A_∞-coálgebra. Adicionalmente, supongamos que $t\phi = 0$ y que $(1 \otimes \phi)t\cap$ es puntualmente nilpotente. Entonces, existe una contracción*

$$M \otimes_t C \Rightarrow N \otimes_{\bar{t}} C',$$

donde $\bar{t} = tg$ es una A_∞-cocadena de torsión y $N \otimes_{\bar{t}} C'$ un A_∞-producto tensorial torcido no principal sobre la DG-álgebra A.

Demostración.

Se desprende de la combinación del Teorema 2.6.16 y el Lema 2.6.17.

■

Así, hemos traducido los resultados referentes a productos tensoriales torcidos principales al ámbito de productos tensoriales torcidos no principales.

Lamentablemente, las condiciones que envuelven la contracción (2.22) que da el modelo homológico de un producto semidirecto,

$$c_{A \ltimes_\chi G} : \{\bar{B}(\mathbb{Z}[A \ltimes_\chi G]), hA \otimes hG, f, g, \phi\},$$

no son las apropiadas del Teorema 2.6.18 anterior.

En efecto, la cadena de contracciones en que factoriza la anterior es

$$\bar{B}(\mathbb{Z}[A\ltimes_\chi G]) \overset{\varphi_1}{\Rightarrow} C_*(\bar{W}(A\ltimes_\chi G)) \overset{\varphi_2}{\Rightarrow} C_*(\bar{W}(A)\times_\tau \bar{W}(G)) \overset{EZ^\tau_{\bar{W}(A),\bar{W}(G)}}{\Rightarrow}$$

$$\overset{EZ_{\bar{W}(A),\bar{W}(G)}}{\Rightarrow} C_*(\bar{W}(A))\otimes_t C_*(\bar{W}(G)) \overset{C_{t\cap}}{\Rightarrow} hA\tilde{\otimes}hG.$$

Si atendemos al último eslabón, $C_{t\cap}(f,g,\phi) : C_*(\bar{W}(A))\otimes_t C_*(\bar{W}(G)) \Rightarrow hA\tilde{\otimes}hG$, resulta que $C_*(\bar{W}(A))\otimes_t C_*(\bar{W}(G))$ constituye un producto tensorial torcido no principal sobre $C_*(G)$, con acción dada por $[a_n,\ldots,a_0]*g = [ga_n,\ldots,ga_0]$.

Desafortunadamente, esta acción $*$ no se hereda a hA mediante la contracción $c_A(f_A,g_A,\phi_A) : C_*(\bar{W}(A)) \Rightarrow hA$, puesto que, en general, la condición necesaria del Lema 2.6.17 no se cumple.

Tomemos el caso de un grupo diédrico: sea $A\ltimes_\chi G = D_{12} = \mathbb{Z}_6\ltimes_\chi\mathbb{Z}_2$, y tomemos $m = \gamma(w) \in hA = E(u)\otimes\Gamma(w)$ y $a = b = -1 \in \mathbb{Z}_2$.

Se tiene que $f_A(g_A(m)*a) = f_A(\sum_{i=1}^{5}[1|i]*(-1)) = 5\gamma(w)$, por lo que, de un lado, es $f_A(g_A(f_A(g_A(m)*a))*b) = 25\gamma(w)$.

Sin embargo, de otro, $f_A(g_A(m)*ab) = f_A(g_A(m)) = m = \gamma(w)$.

Por tanto, habría que recurrir a una aproximación diferente a la hora de detectar estructuras algebraicas más ricas en el modelo homológico de un producto semidirecto.

Capítulo 3.

Matrices cocíclicas y aplicaciones

Capítulo 3.

Matrices cocíclicas y aplicaciones

3.1 Generalidades

En el capítulo preliminar de esta memoria, iniciábamos el estudio de la *Teoría del desarrollo cocíclico de diseños*, lo que nos llevaba de forma natural a la construcción de *matrices cocíclicas de Hadamard.* Rescatando los resultados fundamentales que se exponían en dichas secciones y apoyándonos en la información obtenida en el capítulo anterior, ahora nos planteamos analizar la existencia de matrices cocíclicas de Hadamard sobre determinados grupos finitos.

Para ello, en primer lugar tendremos que abordar el problema de la determinación de los generadores de 2-cobordes y 2-cociclos representativos para un grupo dado G.

Sea $(C,+)$ un grupo aditivo abeliano finito y $(G,\bullet)$ un grupo multiplicativo (no necesariamente abeliano) finito de v elementos, ordenados de la siguiente forma $G = \{a_1 = 1, a_2, \ldots, a_v\}$. Tal como se recoge en el capítulo primero, una matriz cocíclica M sobre G consiste, salvo equivalencia Hadamard, en una matriz $M = (f(a,b))$ desarrollada sobre un 2-cociclo $f : G \times G \to C$.

Denotemos por $B(G)$ al subgrupo de 2-cobordes, formado por las funciones del tipo

$$f(a,b) = \alpha(a)\alpha(b)\alpha(ab)^{-1}, \quad a,b \in G,$$

para una aplicación de conjuntos $\alpha : G \to C$ prefijada.

El grupo $Z(G)$ de todos los 2-cociclos consiste en la suma $B(G) \oplus H^2(G;C)$.

A la hora de buscar matrices de Hadamard, Horadam, de Launey y Flannery

evitan calcular una base explícita para $B(G)$, y consideran una matriz genérica $M = (g(ab))$ desarrollada sobre G; dado que esta matriz es equivalente Hadamard, con la sola negación de filas y columnas (sin intercambiar filas ni columnas), a la matriz cocíclica $(g(a)g(b)g(ab))$. No obstante, esta elección tiene un reflejo negativo en el coste computacional de la evaluación del carácter Hadamard de la matriz en cuestión, como destacaremos más adelante.

Obtener un sistema de generadores de $H^2(G;C)$ no resulta tan sencillo, en general.

Horadam y de Launey plantean la cuestión a través de la descomposición que provee el *Teorema de Coeficientes Universales* [59] de $H^2(G;C)$,

$$H^2(G;C) \cong \mathrm{Ext}_{\mathbb{Z}}(G/[G,G],C) \oplus \mathrm{Hom}(H_2(G),C),$$

lo cual da lugar a matrices de tamaño desproporcionado para órdenes no demasiado elevados del grupo G. Nosotros nos serviremos de los modelos (co)homológicos determinados en el capítulo previo, de modo que el tamaño de las matrices a utilizar permanece constante, independientemente del orden del grupo G considerado. Una tercera alternativa surge del trabajo de Flannery, quien calcula el $H_2(G)$ a partir de la fórmula de Hopf, e identifica $H^2(G;C)$ como suma de las imágenes de sendos morfismos de *inflación* y *transgresión*; las cuales constituyen copias isomorfas de $\mathrm{Ext}(G/[G,G],C)$ y $\mathrm{Hom}(H_2(G),C)$, respectivamente.

Como ya se viera en el primer capítulo, Horadam y de Launey sientan en [24, 25, 26] la base de la teoría cocíclica de diseños, sobre la cual fundamentan sus esfuerzos a la hora de buscar matrices cocíclicas de Hadamard. Uno de los resultados más destacables de estos trabajos es el que permite reducir la búsqueda de matrices cocíclicas de Hadamard a la localización de matrices cocíclicas puras normalizadas de Hadamard, mediante ciertas transformaciones propias de la equivalencia Hadamard de matrices.

Por otra parte, en [25, 26] se muestra la factorización de cualquier matriz cocíclica pura normalizada como producto Hadamard de tres matrices básicas: una asociada a los cociclos *principales* (esto es, 2-cobordes), otra *simétrica* (que proviene del factor $\mathrm{Ext}(G/[G,G],C)$) y una tercera *conmutadora* (que proviene del factor $\mathrm{Hom}(H_2(G),C)$).

En lugar de calcular una matriz generadora de los 2-cobordes, Horadam utiliza una matriz genérica desarrollada sobre G; la cual, al ser equivalente Hadamard por la sola

negación, sin realizar permutas, de filas y columnas, no afecta al estudio del carácter Hadamard de su producto con las matrices simétrica y conmutadora correspondientes. La principal ventaja en esta manera de trabajar es que las matrices cocíclicas quedan determinadas por bloques de una forma muy elegante. Como contrapartida, presenta el inconveniente de que al utilizar la matriz desarrollada sobre G como representante de la parte de los 2-cobordes, la matriz que se obtiene al hacer el producto Hadamard de las tres matrices, ya no es cocíclica, por lo que no es aplicable el test de Hadamard "económico" que propusieran Horadam y de Launey (que consiste en que la suma de los elementos de cualquier fila sea nula, a excepción de la primera, que es toda de unos por tratarse de una matriz normalizada). De modo que para verificar si las matrices así obtenidas son de Hadamard hay que comprobar necesariamente si cualesquiera dos filas (o columnas) son, en efecto, perpendiculares. Lo cual aumenta considerablemente la complejidad del proceso de localización de matrices cocíclicas de Hadamard.

Nuestro trabajo progresa sobre el desarrollado por Horadam y de Launey, con el objetivo primordial de rebajar el coste de construcción de la parte conmutadora, sin sacrificar la posibilidad de utilizar el test de Hadamard económico.

Así, por una parte, nosotros calculamos para cada grupo concreto una base de 2-cobordes, de modo que trabajamos con la forma de los mismos directamente. Esto permite, además, obtener condiciones necesarias para que un conjunto de generadores pueda dar lugar a una matriz de Hadamard, cotas superior e inferior sobre el número de generadores a utilizar, etc. Otra ventaja a destacar en nuestra forma de trabajo es que, al no dejar de utilizar en todo momento matrices cocíclicas, podemos seguir aplicando el test de Hadamard de orden cuadrático que propusieran Horadam y de Launey.

Respecto al estudio de la parte conmutadora, un paso fundamental es la determinación de la homología en grado 2 de G. Tal y como comentábamos en el capítulo segundo, el algoritmo de Veblen permite el cálculo de la homología en grado 2 de un grupo (o lo que es lo mismo, de la construcción bar asociada a dicho grupo) a través de las matrices D_3 y D_2 que provienen de las diferenciales de grados 3 y 2, ∂_3, ∂_2. Obsérvese que si el grupo G es de orden v, la matriz D_3 será de orden $v^3 \times v^2$. Por tanto, en el caso de grupos con un elevado número de elementos, el cálculo de esta matriz puede volverse computacionalmente inabarcable.

Nosotros proponemos una alternativa con el fin de simplificar el problema. Así, reducimos el estudio de la homología del grupo G, al estudio de un *modelo homológico*. Es decir, pasamos a estudiar la homología de otro grupo con un número menor de generadores en cada grado, pero con igual homología, en función de *contracciones*. Como veremos en algunos casos concretos, este procedimiento permite reducir considerablemente el orden de las matrices implicadas. En contrapartida, a la hora de construir explícitamente los generadores de la parte conmutadora, el hecho de calcular la homología en grado 2 del modelo homológico hG, en lugar de calcular directamente la homología de $\bar{B}(\mathbb{Z}[G])$, hace necesario un ulterior proceso de *levantamiento* de la información homológica obtenida, a través de la composición del isomorfismo (1.2)

$$\begin{aligned} \phi : Z(G) = B(G) \oplus H^2(G;C) &\rightarrow \mathrm{Hom}(\bar{B}_2(\mathbb{Z}[G])/\mathrm{Im}\,\partial_3, C) \\ h &\rightarrow \phi(h), \end{aligned}$$

$$\phi(h)(\sum_{a,b)\in G\times G} \lambda_{a,b}[a,b]) = \sum_{(a,b)\in G\times G} \lambda_{a,b} h((a,b));$$

y la proyección f,

$$f : \bar{B}(\mathbb{Z}[G]) \longrightarrow hG,$$

de la contracción que da el modelo homológico.

En general este proceso puede resultar complejo, pero veremos distintas familias de grupos en las que prevalecerá la bondad de este último procedimiento.

3.1.1 Aproximación de Horadam y de Launey

Sea $(C,+)$ un grupo aditivo abeliano finito y $(G,\bullet)$ un grupo multiplicativo (no necesariamente abeliano) finito de v elementos, ordenados de la siguiente forma $G = \{a_1 = 1, a_2, \ldots, a_v\}$.

Para la determinación del grupo $Z(G)$ de los 2-cociclos sobre C, Horadam y de Launey recurrieron, como es preceptivo, al *Teorema de Coeficientes Universales* [59], de modo que

$$Z(G)/B(G) \cong H^2(G;C) \cong \mathrm{Ext}_{\mathbb{Z}}(H_1(G), C) \oplus \mathrm{Hom}(H_2(G), C),$$

donde $B(G)$ conforman los 2-cobordes, $H_1(G) = G/[G,G]$ es el abelianizado de G (asimismo finito por serlo G) y $H_2(G)$ es el segundo grupo de homología de G.

El cálculo de grupos $\mathrm{Ext}_{\mathbb{Z}}(F,H)$ para grupos abelianos F y H, con F finito y H finitamente generado se realiza así: teniendo en cuenta que el funtor Ext es biaditivo, si las descomposiciones primarias de F y H son respectivamente $F = \bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{t_i}}$ y $H = \mathbb{Z}^k \oplus (\bigoplus_{j=1}^{m} \mathbb{Z}_{q_j^{s_j}})$, con cada p_i y q_j primos, entonces

$$\mathrm{Ext}_{\mathbb{Z}}(F,H) \cong \bigoplus_{i=1}^{n}(\mathrm{Ext}_{\mathbb{Z}}(\mathbb{Z}_{p_i^{t_i}}, \mathbb{Z}^k) \oplus (\bigoplus_{j=1}^{m} \mathrm{Ext}_{\mathbb{Z}}(\mathbb{Z}_{p_i^{t_i}}, \mathbb{Z}_{q_j^{s_j}}))) \cong$$

$$\cong \bigoplus_{i=1}^{n}(\mathbb{Z}_{p_i^{t_i}}^{k} \oplus (\bigoplus_{j=1}^{m} \mathbb{Z}_{mcd(p_i^{t_i}, q_j^{s_j})})).$$

El cálculo del término $\mathrm{Hom}(H_2(G), C)$, sin embargo, no es tan inmediato.

En la cuarta sección del capítulo primero recogimos un isomorfismo (1.2) entre el grupo $Z(G)$ de 2-cociclos y el conjunto de homomorfismos de $U(G) = \bar{B}_2(\mathbb{Z}[G])/\mathrm{Im}\,\partial_3$ en C, de manera que

$$\begin{aligned} \phi : Z(G) = B(G) \oplus H^2(G;C) &\to \mathrm{Hom}(U(G), C) \\ h &\to \phi(h), \end{aligned}$$

$$\phi(h)(\sum_{a,b)\in G\times G} \lambda_{a,b}[a,b]) = \sum_{(a,b)\in G\times G} \lambda_{a,b} h((a,b));$$

que está bien definido por ser h un 2-cociclo.

En [24] se relaciona $H_2(G)$ con $U(G)$, de manera que $H_2(G) \subset U(G)$. Es más, se prueba que, si denotamos por $S(G) = U(G)/H_2(G)$, es $S(G) \cong \mathbb{Z}^v$. De donde la parte de torsión de $U(G)$ viene dada por $H_2(G)$, siendo entonces

$$\mathrm{Hom}(U(G), C) \cong \mathrm{Hom}(S(G), C) \oplus \mathrm{Hom}(H_2(G), C).$$

Por otra parte, teniendo en cuenta el teorema de coeficientes universales, la fórmula anterior y que los 2-cobordes se anulan sobre $H_2(G)$, podemos deducir que los 2-cociclos representativos simétricos $\mathrm{Hom}(S(G), C)$ corresponden a

$$C^v \cong \mathrm{Hom}(B(G), C) \oplus \mathrm{Ext}_{\mathbb{Z}}(G/[G,G], C).$$

Además, tenemos que

$$\mathrm{Hom}(S(G),C)/\mathrm{Hom}(B(G),C) \cong \mathrm{Ext}_{\mathbb{Z}}(G/[G,G],C) \cong$$

$$\cong \mathrm{Hom}(S(G/[G,G]),C)/\mathrm{Hom}(B(G/[G,G]),C). \tag{3.1}$$

Como consecuencia, cualquier 2-cociclo f sobre $G/[G,G]$ admite una elevación en la forma $f^+ = f \circ (p \times p)$ como 2-cociclo sobre G, siendo $p : G \to G/[G,G]$ el homomorfismo que da la proyección de paso al cociente.

En [25] se observa que los 2-cociclos simétricos en efecto dan lugar a matrices simétricas (de aquí el calificativo de simétricos), puesto que cualquier $f \in \mathrm{Hom}(S(G/[G,G],C)$ satisface la relación de simetría $f(x,y) = f(y,x)$, para cualesquiera $x, y \in G/[G,G]$; de donde los 2-cociclos elevados deben verificar, por extensión, que $f^+(a,b) = f^+(b,a)$ para cualesquiera $a, b \in G$.

Además, según (3.1), si se elevan dos 2-cociclos de $\mathrm{Hom}(S(G/[G,G],C)$ pertenecientes a distintas clases de equivalencia cocíclica, se obtienen sendos 2-cociclos de $\mathrm{Hom}(S(G,C))$, también correspondientes a clases de equivalencia distintas. Así, cualquier 2-cociclo simétrico de $\mathrm{Hom}(S(G),C)$ puede descomponerse en la forma $f = f_S^+ \cdot f_B$, donde $f_B \in \mathrm{Hom}(B(G),C)$ es un 2-coborde. Esta descomposición es única salvo elevación de 2-coborde $h_B \in \mathrm{Hom}(B(G/[G,G]),C)$, de modo que $f = (f_S^+ \cdot h_B^+) \cdot (f_B \cdot (h_B^+)^{-1})$.

Teniendo en cuenta la aditividad del funtor $\mathrm{Hom}(-,C)$, si partimos de una descomposición primaria de $G/[G,G] = \oplus_{i=1}^n \mathbb{Z}_{p_i^{t_i}}$, entonces tenemos el isomorfismo

$$\mathrm{Hom}(S(G),C)/\mathrm{Hom}(B(G),C) \cong \oplus_{i=1}^n \mathrm{Hom}(S(\mathbb{Z}_{p_i^{t_i}}),C)/\mathrm{Hom}(B(\mathbb{Z}_{p_i^{t_i}}),C) \cong$$

$$\cong \oplus_{i=1}^n \mathrm{Ext}_{\mathbb{Z}}(\mathbb{Z}_{p_i^{t_i}},C),$$

de modo que todo $f \in \mathrm{Hom}(S(G),C)$ admite una descomposición en la forma $f = (\prod_{i=1}^n f_{S_i})^+ \cdot f_B$, con $f_{S_i} \in \mathrm{Hom}(S(\mathbb{Z}_{p_i^{t_i}}),C)$ y $f_B \in \mathrm{Hom}(B(G),C)$. Tal descomposición es única salvo representante de la clase $[f_B]$ en $\mathrm{Hom}(B(G),C)/\mathrm{Hom}(B(G/[G,G]),C)$.

Así, el cálculo de los generadores de los 2-cociclos simétricos representativos puede reducirse, según las descomposiciones primarias de $G/[G,G]$ y de C, al cálculo de los generadores de $\mathrm{Ext}_{\mathbb{Z}}(\mathbb{Z}_m,\mathbb{Z}_r)$, con $m > 1$ y $r \in \mathbb{Z}^+\backslash\{1\}$, conviniendo que $\mathbb{Z}_0 = \mathbb{Z}$. Para la búsqueda de estos generadores, Horadam y de Launey se basaron en la relación que ellos mismos probaron en [24] entre las clases de equivalencia de los 2-cociclos sobre grupos cíclicos y las funciones de desarrollo ω-cíclicas.

Si se consideran las presentaciones $< x : \ x^r = 1 > \cong \mathbb{Z}_r$ (recuérdese que convenimos $\mathbb{Z}_0 \cong \mathbb{Z}$) y $< a : \ a^m = 1 > \cong \mathbb{Z}_m$, se puede definir la función $w : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}$ dada por $w(a^i, a^j) = x^{\lfloor (i+j)/m \rfloor}$, con $0 \leq i, j \leq m-1$. Se tiene que $w^l \in \mathrm{Hom}(S(\mathbb{Z}_m), \mathbb{Z})$, y $w^l \sim w^k$ si y sólo si $l \equiv k(mod\ m)$. De hecho, todo 2-cociclo $f \in \mathrm{Hom}(S(\mathbb{Z}_m), \mathbb{Z})$ es cocíclicamente equivalente a alguna potencia de w.

Una representación matricial de w es

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & \cdots & 1 & x \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & \cdots & x & x \\ 1 & x & \cdots & x & x \end{pmatrix}$$

Del mismo modo, se puede definir la función $w : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_r$ dada por $w(a^i, a^j) = x^{(r/mcd(r,m))\lfloor (i+j)/m \rfloor}$, con $0 \leq i, j \leq m-1$. Una vez más se tiene que, $w^l \in \mathrm{Hom}(S(\mathbb{Z}_m), \mathbb{Z}_r)$, y $w^l \sim w^k$ si y sólo si $l \equiv k(mod\ mcd(r,m))$. Es más, todo 2-cociclo $f \in \mathrm{Hom}(S(\mathbb{Z}_m), \mathbb{Z}_r)$ es cocíclicamente equivalente a alguna potencia de w.

Si llamamos $g = mcd(r, m)$, w es en este caso

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & \cdots & 1 & x^{r/g} \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & \cdots & x^{r/g} & x^{r/g} \\ 1 & x^{r/g} & \cdots & x^{r/g} & x^{r/g} \end{pmatrix}$$

En definitiva, si una descomposición primaria de $G/[G,G]$ es $\oplus_{i=1}^{n} \mathbb{Z}_{p_i^{t_i}}$, existe una ordenación de los elementos de G de modo que un sistema de generadores para los 2-cociclos simétricos representativos es

$$MD_s(G) = J_{|[G,G]|} \otimes MD(p_1^{t_1}) \otimes \cdots \otimes MD(p_n^{t_n}),$$

donde $J_{|[G,G]|}$ es la matriz de orden $|[G,G]|$ con la unidad en todas sus entradas,

$MD(p_i^{t_i})$ es la matriz cuadrada de orden $p_i^{t_i}$ dada por

$$MD(p_1^{t_1}) = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & \cdots & 1 & A \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & \cdots & A & A \\ 1 & A & \cdots & A & A \end{pmatrix}, \qquad A^{p_i^{t_i}} = 1,$$

y $\otimes$ representa el producto de Kronecker.

Ahora, fijado un grupo de coeficientes C, el cálculo del sistema de generadores de los 2-cociclos simétricos representativos consiste, salvo equivalencia cocíclica, en tomar $\mathrm{Hom}(MD_s(G), C)$. Gracias a la aditividad del funtor $\mathrm{Hom}(MD_s(G), -)$, el proceso se puede desglosar según una descomposición primaria de C (nótese que $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_r) = \mathbb{Z}_g$, con $g = mcd(m, r)$, y viene generado por $f(a) = x^{r/g}$; por lo que $\mathrm{Hom}(MD_s(G), \mathbb{Z}_r)$ consiste en los generadores w descritos previamente).

Hemos de hacer hincapié en que la forma de las matrices descritas previamente depende de la ordenación inicial de los elementos de G. En general, fijada una ordenación y una presentación del grupo G, hay que determinar la clase $[g]$ en $G/[G,G] \cong \oplus_{i=1}^{n} \mathbb{Z}_{p_i}^{t_i}$ de cada elemento $g \in G$, y en función de ésta traducir cuál sería la entrada correspondiente en la matriz generadora asociada en cuestión. Incidiremos con más detalle sobre este asunto posteriormente.

La determinación de un sistema de generadores de la parte conmutadora, $\mathrm{Hom}(H_2(G), C)$, es el proceso de mayor complejidad en el cálculo de los generadores de 2-cociclos.

Tal como describiéramos en el capítulo segundo, un sistema de generadores de $H_2(G)$ se puede determinar aplicando el algoritmo de Veblen a la diferencial de $\bar{B}_3(\mathbb{Z}[G])$, que consiste en una matriz de tamaño $v^3 \times v^2$. Una vez obtenidos los generadores de $\bar{B}_2(\mathbb{Z}[G])$ con información homológica relevante (no trivial) en $H_2(G)$, basta ver cuáles de ellos se mantienen como generadores en $\mathrm{Hom}(H_2(G), C)$. Lamentablemente, si el orden v del grupo G es suficientemente elevado, el coste computacional del algoritmo de Veblen sobre la matriz $v^3 \times v^2$ se hace insostenible. Necesitamos una alternativa más viable.

3.1.2 Aproximación de Flannery

Aunque también consideró los 2-cobordes en la forma de matrices desarrolladas sobre el grupo dado, Flannery atacó en [40, 41, 42, 43] el problema de la búsqueda de los 2-cociclos representativos desde una perspectiva diferente, a partir de los morfismos siguientes.

Sea G un grupo finito, U un G-módulo, y N un subgrupo normal de G. Denotemos por U^N al G-submódulo dado por un conjunto de N elementos fijos de U. Para cada n-cociclo $f \in Z^n(G/N, U^n)$, se define el homomorfismo *inflación*, $\inf f \in Z^n(G, U)$, de manera que

$$(\inf f)(g_1, \ldots, g_n) = f(g_1 N, \ldots, g_n N).$$

La inflación en el segundo grupo de Homología puede describirse en términos de matrices cocíclicas. Tomando $f \in Z^2(G/N, U^N)$, ordenando los elementos de N en la forma $x_1 = 1, x_2, \ldots, x_s$ y eligiendo un conjunto $g_1 = 1, g_2, \ldots, g_r$ representativo para las clases de G/N; las matrices cocíclicas asociadas a $\inf f$ y f, denotadas por $M_{\inf f}$ y M_f, tienen sus filas y columnas indexadas en la forma $1, g_2, \ldots, g_r, x_2, \ldots, g_r x_2, x_s, \ldots, g_r x_s$ y $N, g_2 N, \ldots, g_r N$, respectivamente. Obviamente se tiene que

$$M_{\inf f} = M_f \otimes J_s,$$

donde $\otimes$ denota el producto de Kronecker de matrices y J_s es la matriz $s \times s$ toda de unos.

De aquí en adelante, vamos a suponer que N es un subgrupo central de G y que G actúa trivialmente sobre U. En estas circunstancias, se puede definir el homomorfismo *transgresión* τ,

$$\tau : \mathrm{Hom}(N, U) \to H^2(G/N, U),$$

de la siguiente manera.

Dado que $1 \to N \xrightarrow{i} G \xrightarrow{p} G/N \to 1$ es una extensión central[1] de N por G/N, se puede asociar una función σ_T a cada conjunto T de representantes de las clases del conúcleo de $G/i(N)$,

$$\sigma_T : G/N \to G,$$

[1]Se trata de una extensión central puesto que $i(N)$ está en el centro de G.

de modo que $p \circ \sigma_T = 1_G/N$ y $\sigma_T(1) = 1$. Entonces, el elemento $t_g t_h (t_{gh})^{-1}$, para $t_g, t_h \in T$, está en la imagen de N por i en G. Así, se obtiene un 2-cociclo f_T asociado a T tal que

$$f_T(g,h) = i^{-1}(t_g t_h (t_{gh})^{-1}) \; g, h \in G/N.$$

Esto no es más que una dirección de la conocida relación existente entre 2-cociclos y extensiones centrales: en [64], por ejemplo, se puede ver que cualquier 2-cociclo está asociado a una extensión central y viceversa. Detallaremos esta relación más adelante.

En estas circunstancias, se puede definir $\tau(\phi) = [\phi \circ f_T]$.

Otro homomorfismo que es necesario introducir en este punto es la *restricción*, res : $H^n(G,U) \to H^n(H,U)$, inducido por la restricción a N del dominio de definición de los n-cociclos.

Los tres homomorfismos definidos previamente están relacionados entre sí, mediante la siguiente sucesión exacta

$$0 \to \mathrm{Hom}(G/N,U) \overset{\inf}{\to} \mathrm{Hom}(G,U) \overset{\mathrm{res}}{\to} \mathrm{Hom}(N,U) \overset{\tau}{\to}$$

$$\overset{\tau}{\to} h^2(G/N,U) \overset{\inf}{\to} H^2(G,U)$$

Consideremos a partir de ahora el caso en que U está finitamente generado y $N = [G,G]$. En estas circunstancias, teniendo en cuenta el *Teorema de los Coeficientes Universales* [59],

$$H^2(G,U) \cong \mathrm{Ext}(G/[G,G]),U) \oplus \mathrm{Hom}(H_2(G),U),$$

queda definida una inmersión de $\mathrm{Ext}(G/[G,G])$ en $H^2(G,U)$, que resulta de la restricción a $\mathrm{Ext}(G/[G,G],U)$ del homomorfismo inflación sobre $H^2(G/[G,G],U)$.

Por otra parte, existe una inmersión de $\mathrm{Hom}(H_2(G);U)$ en $H^2(G,U)$. Teniendo en cuenta la fórmula de Hopf para $H_2(G)$, para cualquier presentación F/R de G, donde F es un grupo libre de generadores y R aporta las relaciones, se tiene que

$$R/[R,F] = R \cap [F,F]/[R,F] \oplus S/[R,F];$$

donde el primer sumando corresponde a la parte de torsión $(R \cap [F,F])/[R,F] \cong H_2(G)$ y el segundo sumando es el llamado *complemento de Schur*, el cual no es en general único (depende de la elección de S).

Así, se tiene

$$1 \to R/S \xrightarrow{i} F/S \xrightarrow{\pi} F/R \to 1,$$

donde i es la inclusión y π es la proyección natural. A partir de esta extensión central de $R/S \cong H_2(G)$ por $F/R \cong G$, queda caracterizado el homomorfismo transgresión correspondiente

$$\tau_s : \mathrm{Hom}(R/S, U) \to H^2(F/R, U).$$

En [41] se prueba que tanto la inflación como la transgresión son homomorfismos inyectivos y que sus imágenes se complementan, de modo que

$$\mathrm{Im}\,(\mathrm{inf}) \oplus \mathrm{Im}\,\tau_s \cong H^2(G, U)$$

da una factorización de los 2-cociclos representativos, a partir de la cual se puede determinar un sistema de generadores.

La dificultad en esta aproximación reside precisamente en hallar un complemento de Schur de una presentación F/R de G sobre la que construir τ_s.

3.1.3 Nuestra aproximación: Método de la reducción homológica

Las dos vertientes que hemos descrito hasta ahora para determinar una base de 2-cociclos de G presentan ciertos problemas, a saber:

- La forma en la que tanto el tándem Horadam-de Launey como el propio Flannery codifican los 2-cobordes $B(G)$, en virtud de una matriz genérica $MD_p = (g(a \cdot b))$ desarrollada sobre el grupo G considerado, impide aplicar el test de Hadamard cuadrático al producto $MD_p(G) \bullet MD_s(G) \bullet MD_c(G)$ de las partes principal, simétrica y conmutadora, respectivamente; puesto que $MD_p(G)$ no es, en general, una matriz cocíclica (la negación arbitraria de filas y/o columnas no es una operación interna de 2-cociclos, en general).
- El tamaño de la matriz conmutadora con que trabajan Horadam y de Launey, $v^3 \times v^2$, depende del orden v del grupo G, por lo que el procedimiento en cuestión sólo es válido para grupos relativamente "pequeños".

- En ambos casos, los procedimientos considerados no admiten una extensión fluida para el cálculo de n-cociclos, con $n > 2$.

Nosotros hemos diseñado una nueva aproximación, que trata de solventar los inconvenientes señalados.

El trabajo progresa sobre el desarrollado por Horadam y de Launey, con el objetivo primordial de rebajar el coste de construcción de la parte conmutadora, sin sacrificar la posibilidad de utilizar el test de Hadamard económico.

A grandes trazos, la idea consiste en determinar un modelo homológico hG para G, y proyectar la información (co)homológica desde hG hasta G.

Todo esto nos permitirá encontrar en algunos casos concretos, además, sendas cotas superior e inferior sobre el número de generadores a utilizar y ciertas condiciones necesarias para que un conjunto de generadores pueda dar lugar a una matriz de Hadamard. Sin olvidar que, al utilizar en todo momento matrices cocíclicas, podremos seguir aplicando el test de Hadamard cuadrático.

Para generar una base de los 2-cobordes, procedemos según dicta el álgebra lineal clásico.

Proposición 3.1.1 *Una base para los 2-cobordes se obtiene mediante una reducción por filas en $\mathbb{Z}$ de una matriz $v \times v^2$, donde la fila i está asociada a la función característica $\alpha_i : G \to \mathbb{Z}$ que lleva $\alpha_i(a_j) = \delta_{ij}$, con δ la función de Kronecker.*

A continuación describimos una rutina en *Mathematica* que determina una base de 2-cociclos, que guardamos en `base2cociclos`. El orden del grupo se almacena en la variable `orden`.

```
base2cociclos={};
Print["Calculando un sistema de generadores de 2-cobordes."];
orden=Apply[Times,card];
cobordes=Table[Apply[Join,Table[Table[Mod[KroneckerDelta[i,k]+
     KroneckerDelta[i,j]+KroneckerDelta[i,prodarbol[k,j]],2],
{j,orden}],{k,orden}]],{i,2,orden}];
Module[{m,n,i,j,filas}, m=cobordes; gen={}; i=0; While[i<orden-1,
```

```
      n=Select[Range[i+1,orden-1],m[[#1]]=!=Table[0,{k,orden^2}]&,1];
      If[n=={}, i=orden-1, gen=Join[gen,n]; i=n[[1]];
        j=Position[m[[i]],1,1,1];
        filas=Select[Range[i+1,orden-1],m[[#1,j[[1,1]]]]==1&];
        Do[
m=ReplacePart[m,Mod[sumlist[m[[filas[[k]]]],m[[i]]],2],filas[[k]]],
{k, Length[filas]}]]; ]];
Do[base2cociclos=Append[base2cociclos,Partition[Replace[Replace[
      cobordes[[gen[[i]]]],1->-1,1],0->1,1],orden]];
      Print["El 2-coborde ",gen[[i]]+1," es generador:"];
Print[base2cociclos[[i]]//MatrixForm],{i, Length[gen]}];
```

En lo que concierne a las partes simétrica y conmutadora, naturalmente, al utilizar un modelo homológico hG, el cálculo de $G/[G,G] \cong H_1(G) \cong H_1(hG)$ y $H_2(G) \cong H_2(hG)$ se simplifica, en mayor o menor medida dependiendo del caso.

No obstante, a la hora de construir explícitamente los generadores de las partes simétrica y conmutadora, el hecho de calcular las homologías en grados 1 y 2 a partir de hG, en lugar de trabajar directamente la homología de $\bar{B}(\mathbb{Z}[G])$, hace necesario un proceso de *levantamiento* o *proyección* de la información homológica obtenida, a través de la proyección f,

$$f : \bar{B}(\mathbb{Z}[G]) \longrightarrow hG,$$

de la contracción que da el modelo homológico.

Más concretamente, sabemos que si $\oplus_{i=1}^{n} \mathbb{Z}_{p_i{}^{t_i}}$ es una descomposición primaria de $G/[G,G]$, existe una ordenación de los elementos de G de modo que un sistema de generadores para los 2-cociclos simétricos representativos es

$$MD_s(G) = J_{|[G,G]|} \otimes MD(p_1^{t_1}) \otimes \cdots \otimes MD(p_n^{t_n}),$$

donde $J_{|[G,G]|}$ es la matriz de orden $|[G,G]|$ con la unidad en todas sus entradas, $MD(p_i^{t_i})$ es la matriz cuadrada de orden $p_i^{t_i}$ dada por

$$MD(p_1^{t_1}) = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & \cdots & 1 & A \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 1 & \cdots & A & A \\ 1 & A & \cdots & A & A \end{pmatrix}, \qquad A^{p_i^{t_i}} = 1,$$

y $\otimes$ representa el producto de Kronecker. Posteriormente, para cada factor $\mathbb{Z}_b$ en que se descomponga el grupo C dado, habría que determinar la matriz generadora correspondiente al término $\mathrm{Hom}(MD(p_i^{t_i}), \mathbb{Z}_b)$. Nosotros nos centraremos en el caso $C = \mathbb{Z}_2 \simeq \mathbb{F}_2$, que da origen a las matrices cocíclicas binarias, y por consiguiente a las matrices de Hadamard usuales. Otra elección de C conduciría a matrices de Hadamard *generalizadas* [64], que se escapan de los objetivos del presente trabajo.

De esta forma, hay tantos generadores en la parte simétrica como factores $\mathbb{Z}_{2^{t_i}}$ aparecen en la descomposición primaria de $G/[G,G]$, todos ellos de la forma $MD(2^{t_i})$ con $A^2 = 1$, para cierta ordenación de los elementos de G. Todos estos generadores proceden de funciones $w_i : \mathbb{Z}_{2^{t_i}} \times \mathbb{Z}_{2^{t_i}} \to \mathbb{F}_2$ con $w(j,k) = (-1)^{\lfloor \frac{j+k}{2^{t_i}} \rfloor}$.

El problema estriba ahora en que la ordenación $G = \{1, a_2, \ldots, a_v\}$ fijada de antemano, en general, no coincidirá con la que corresponde a la elegante codificación que acabamos de describir. Hemos de proveer un procedimiento que traduzca una en función de la otra.

Denotemos por $d : hG \to hG$ la diferencial del DG-módulo hG, y sean $\mathcal{B}_1$ y $\mathcal{B}_2$ las bases de hG en grados 1 y 2, respectivamente.

La forma en la que nosotros determinamos $G/[G,G]$ es calculando $H_1(hG)$ mediante el algoritmo de Veblen, que describiéramos al comienzo del capítulo 2. Dado que G es un grupo finito, $H_1(G) \cong H_1(hG)$ sólo consta de parte de torsión, de modo que el algoritmo de Veblen se reduce a trabajar con la matriz $M_2(d)$ proveniente de d_2.

En particular, si $\mathcal{B}_2 = \{\mathbf{e_1}, \ldots, \mathbf{e_n}\}$ y $\mathcal{B}_1 = \{\mathbf{u_1}, \ldots, \mathbf{u_m}\}$, la forma normal de Smith de

$$M_2(d) = \begin{pmatrix} d(\mathbf{e_1}) \\ \vdots \\ d(\mathbf{e_n}) \end{pmatrix}_{n \times m}$$

será una matriz diagonal

$$D_2 = \left(\begin{array}{ccc|c} b_1 & & & \\ & \ddots & & 0 \\ & & b_l & \\ \hline & 0 & & 0 \end{array}\right)_{n \times m}$$

donde $G/[G,G] \cong H_1(G) \cong H_1(hG) \cong \mathbb{Z}_{b_1} \oplus \cdots \oplus \mathbb{Z}_{b_l}$, que de ningún modo será la descomposición primaria de $G/[G,G]$, puesto que $1 \leq b_1|b_2|\cdots|b_l$.

Más aún, existen matrices de paso P y Q de modo que $D_2 = P \cdot M_2(d) \cdot Q$,

$$\begin{array}{ccc} \mathcal{B}_2 & \xrightarrow{M_2(d)} & \mathcal{B}_1 \\ P\uparrow & \# & \downarrow Q \\ \bar{\mathcal{B}}_2 & \xrightarrow{D_2} & \bar{\mathcal{B}}_1 \end{array}$$

Para construir las matrices generadoras simétricas procedemos según los pasos siguientes:

1. Seleccionamos las columnas j de D_2 que contienen una entrada par en la posición diagonal, que son precisamente las que corresponden a factores $\mathbb{Z}_{b_j}$ de $H_1(hG)$ que aportan términos del tipo $\mathbb{Z}_{2^t}$ en la descomposición primaria del abelianizado de G. Así, habrá tantos generadores como columnas de esta forma.

2. Para cada una de tales columnas, sea la j-ésima por ejemplo, seleccionamos las filas i que corresponden a entradas (i,j) de Q no nulas módulo b_j. Dado que Q es la matriz del cambio de base de $\mathcal{B}_1$ a $\bar{\mathcal{B}}_1$, esta operación determina qué elementos de $\mathcal{B}_1$ tienen la j-ésima coordenada no nula en $H_1(hG)$ respecto de la base de paso al cociente naturalmente asociada a $\bar{\mathcal{B}}_1$. En definitiva, qué elementos de $\mathcal{B}_1$ se reflejan en el factor $\mathbb{Z}_{b_j}$ de $G/[G,G]$.

3. La matriz simétrica $M_j = (f_j(g,h))$ que corresponde al generador f_j de dicha columna j se ha de construir *levantando* la función $w_j : \mathbb{Z}_{b_j} \times \mathbb{Z}_{b_j} \to \mathbb{F}_2$ a todo $G \times G$, con $w_j(k,l) = (-1)^{\lfloor \frac{k+l}{b_j} \rfloor}$. Dados $g, h \in G$, basta tomar $f_j(g,h) = w_j([g]_j, [h]_j)$, donde $[g]_j$ es la j-ésima coordenada de la clase de g en $G/[G,G]$ según la base de paso al cociente naturalmente asociada a $\bar{\mathcal{B}}_1$. Explícitamente, $f_j(g,h)$ queda determinado en función de la proyección $f : \bar{B}_1(\mathbb{Z}[G]) \to hG$, puesto que $[g]_j$ es la j-ésima coordenada de $f(g)$ respecto de la base $\bar{\mathcal{B}}_1$; esto es, la j-ésima coordenada del vector $f(g) \cdot Q$, en tanto en cuanto la proyección f está definida entre la base usual de $\bar{B}_2(\mathbb{Z}[G])$ y $\mathcal{B}_1$.

Gráficamente,

$$\begin{array}{ccc} \bar{B}_1(\mathbb{Z}[G]) & \xrightarrow{f} & \mathcal{B}_1 \\ & & \downarrow Q \\ & & \bar{\mathcal{B}}_1 \end{array}$$

Proposición 3.1.2 *Los morfismos f_j anteriores definen una base para 2-cociclos de inflación.*

A la hora de determinar un sistema de generadores que provenga de la parte conmutadora hay que seguir un procedimiento análogo, a la luz del isomorfismo (1.2)

$$\begin{aligned} \phi : Z(G) = B(G) \oplus H^2(G;C) &\to \mathrm{Hom}(\bar{B}_2(\mathbb{Z}[G])/\mathrm{Im}\,\partial_3, C) \\ h &\to \phi(h), \end{aligned}$$

$$\phi(h)(\sum_{a,b)\in G\times G} \lambda_{a,b}[a,b]) = \sum_{(a,b)\in G\times G} \lambda_{a,b} h((a,b));$$

que permite identificar $h((a,b))$ con $\phi(h)([a,b])$.

Sea ahora $\mathcal{B}_3$ la base de hG en grado 3. Dado que G es un grupo finito, nuevamente $H_2(G) \cong H_2(hG)$ sólo consta de parte de torsión, de modo que el algoritmo de Veblen se reduce a trabajar con la matriz $M_3(d)$ proveniente de d_3.

En particular, si $\mathcal{B}_2 = \{\mathbf{e_1}, \ldots, \mathbf{e_n}\}$ y $\mathcal{B}_3 = \{\mathbf{v_1}, \ldots, \mathbf{v_s}\}$, la forma normal de Smith de

$$M_3(d) = \begin{pmatrix} d(\mathbf{v_1}) \\ \vdots \\ d(\mathbf{v_s}) \end{pmatrix}_{s\times n}$$

será una matriz diagonal

$$D_3 = \left(\begin{array}{ccc|c} b_1 & & & \\ & \ddots & & 0 \\ & & b_l & \\ \hline & 0 & & 0 \end{array}\right)_{s\times n}$$

donde $H_2(G) \cong H_2(hG) \cong \mathbb{Z}_{b_1} \oplus \cdots \oplus \mathbb{Z}_{b_l}$, con $1 \leq b_1 | b_2 | \cdots | b_l$; con matrices de paso P y Q asociadas, de modo que $D_3 = P \cdot M_3(d) \cdot Q$,

$$\begin{array}{ccc} \mathcal{B}_3 & \xrightarrow{M_3(d)} & \mathcal{B}_2 \\ P\uparrow & \# & \downarrow Q \\ \bar{\mathcal{B}}_3 & \xrightarrow{D_3} & \bar{\mathcal{B}}_2 \end{array}$$

Para construir las matrices generadoras provenientes de la parte conmutadora, $\mathrm{Hom}(H_2(G), \mathbb{Z}_2)$, procedemos según los pasos siguientes:

1. Seleccionamos las columnas j de D_3 que contienen una entrada b_j par en la posición diagonal; dado que $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_2) \cong \mathbb{Z}_{mcd(n,2)}$, luego sólo son relevantes precisamente los factores $\mathbb{Z}_{b_i}$ con b_i par. Así, habrá tantos generadores como columnas de esta forma.

2. Para cada una de tales columnas, sea la j-ésima por ejemplo, seleccionamos las filas i que corresponden a entradas (i, j) de Q impares. Dado que Q es la matriz del cambio de base de $\mathcal{B}_2$ a $\bar{\mathcal{B}}_2$, esta operación determina qué elementos de $\mathcal{B}_2$ tienen la j-ésima coordenada no nula en $H_2(hG)$ respecto de la base de paso al cociente naturalmente asociada a $\bar{\mathcal{B}}_2$. En definitiva, qué elementos de $\mathcal{B}_2$ se reflejan en el factor $\mathbb{Z}_{b_j}$ de $H_2(hG) \cong H_2(G)$.

3. La matriz conmutadora $M_j = (f_j(g,h))$ que corresponde al generador f_j de dicha columna j queda caracterizada, a tenor del isomorfismo ϕ de (1.2), *proyectando* los elementos $(g,h) \in G \times G$ sobre la base $\bar{\mathcal{B}}_2$ de hG mediante la composición de la proyección f y el cambio de base Q. De este modo, dados $g, h \in G$, es $f_j(g,h) = f([g,h]) \cdot Q$.

Gráficamente,

$$\begin{array}{ccc} \bar{B}_2(\mathbb{Z}[G]) & \xrightarrow{f} & \mathcal{B}_2 \\ & & \downarrow Q \\ & & \bar{\mathcal{B}}_2 \end{array}$$

Proposición 3.1.3 *Los morfismos f_j anteriores definen una base para 2-cociclos de transgresión.*

Concretamos este procedimiento en forma de algoritmo.

Algoritmo 3.1.4 (método de reducción homológica)

ENTRADA: *grupo con modelo homológico* $\{G, hG, f, g, \phi\}$.

P1 Construir una base para 2-cobordes según Proposición 3.1.1

P2 Construir una base para 2-cociclos de inflación según Proposición 3.1.2

P3 Construir una base para 2-cociclos de transgresión según Proposición 3.1.3

P4 Generar todos los 2-cociclos normalizados sobre G

P5 Aplicar el test de Hadamard cuadrático a cada 2-cociclo

SALIDA: *matrices cocíclicas de Hadamard sobre G.*

Comentemos una implementación de este algoritmo en *Mathematica.*

Primero determinamos el `abelianizado` del grupo y su `homologia` en grado 2, adaptando el algoritmo de Veblen a nuestras circunstancias. La diferencial del modelo se denota como `difarbol` y el número de $\mathbb{Z}_n$ en que factoriza el grupo como `numgru`, por coherencia con las notaciones seguidas en el capítulo anterior.

```
b2=Binomial[numgru+1,2];
b1=numgru;
A=Table[Table[0, {i,b1}], {j,b2}];
primbase=basemod[i,numgru];
Module[{k,k1,k2}, Do[ k={-1}+difarbol[primbase[[i]]];
      k2=Table[coef[k[[k1]]], {k1,2,Length[k]}];
      Do[
A=ReplacePart[A,k2[[j,1]],{i,conversion[1,numgru][k2[[j,2]]]}],
{j, Length[k2]}], {i, b2}]; ];
SetAttributes[Plus,Listable]; SetAttributes[Times,Listable];
fnsa1=ExtendedSmithForm[A];
ClearAttributes[Plus,Listable]; ClearAttributes[Times,Listable];
```

```
abelianizado=Select[Table[fnsa1[[1,ji,ji]], {ji, b1}],#1>0&];
Print["El abelianizado es Z_",Select[abelianizado,#1>1&]];
b1=b2; b2=Binomial[2+numgru,3];
A=Table[Table[0, {i,b1}], {j,b2}];
segbase=basemod[3,numgru];
Module[{k,k1,k2}, Do[ k={-1}+difarbol[segbase[[i]]];
      k2=Table[coef[k[[k1]]], {k1,2,Length[k]}];
      Do[
A=ReplacePart[A,k2[[j,1]],{i,conversion[2,numgru][k2[[j,2]]]}],
{j, Length[k2]}], {i, b2}]; ];
SetAttributes[Plus,Listable]; SetAttributes[Times,Listable];
fnsa2=ExtendedSmithForm[A];
ClearAttributes[Plus,Listable]; ClearAttributes[Times,Listable];
homologia=Select[Table[fnsa2[[1,ji,ji]], {ji, b1}],#1>0&];
Print["La homología en grado 2 es Z_",Select[homologia,#1>1&]];
```

Para calcular un sistema de generadores de 2-cociclos simétricos representativos, procedemos de la siguiente manera.

```
Module[{col,k,matriz,mi,mj,m2,n},
      k=Select[Range[Length[abelianizado]],EvenQ[abelianizado[[#1]]]&];
      Do[col=Select[Range[numgru],Mod[fnsa1[[2,2,#1,k[[m1]]]],
        abelianizado[[k[[m1]]]]]=!=0&];
      matriz={Table[1,{i, orden}]};
      m2=2F̂actorInteger[abelianizado[[k[[m1]]]]][[1,2]];
      Do[matriz=Append[matriz,{1}];
        Do[mi=farbol[{i}]; mj=farbol[{j}];
         n=Mod[Apply[Plus,Table[fnsa1[[2,2,col[[m3]],k[[m1]]]]*
          coeficiente[mi,Insert[Table[0,{per,numgru-1}],1,col[[m3]]]],
         {m3, Length[col]}]],m2]+Mod[Apply[Plus,Table[
          fnsa1[[2,2,col[[m3]],k[[m1]]]]*coeficiente[mj,
         Insert[Table[0,{per,numgru-1}],1,col[[m3]]]],
        {m3,Length[col]}]],m2];
        matriz[[i]]=Append[matriz[[i]],(-1)F̂loor[n/m2]],{j,2,orden}],
        {i,2,orden}]; base2cociclos=Append[base2cociclos,matriz];
Print[matriz//MatrixForm], {m1,Length[k]}]];
```

Por último calculamos un sistema de generadores de la parte conmutadora.

```
Module[{col,k,matriz,m,m2},
      k=Select[Range[Length[homologia]],EvenQ[homologia[[#1]]]&];
      Do[col=Select[Range[b1],OddQ[fnsa2[[2,2,#1,k[[m1]]]]]&];
        matriz={Table[1, {i, orden}]};
         Do[matriz=Append[matriz,{1}]; Do[m=farbol[{i,j}];
          m2=Mod[Apply[Plus,Table[coeficiente[m,
          primbase[[col[[m3]]]]], {m3, Length[col]}]], 2];
      matriz[[i]]=Append[matriz[[i]],(-1)m̂2],{j,2,orden}],{i,2,orden}];
      base2cociclos=Append[base2cociclos,matriz];
Print[matriz//MatrixForm], {m1, Length[k]}]];
```

Una vez que tenemos una base de los 2-cociclos, pasamos a construirlos todos, en una lista que llamamos `lista2cociclos`. Utilizamos sendas funciones auxiliares `combinar1` y `combinar2`.

```
combinar2[l_]:=Table[Append[l,i],{i,Last[l]+1,Length[base2cociclos]}];
combinar1[l_]:=Flatten[Map[combinar2,l],1];
lista2cociclos=Flatten[Rest[NestList[combinar1,Table[{i},
      {i,Length[base2cociclos]}],Length[base2cociclos]- 1]],1];
```

Ahora ya podemos aplicar el test de Hadamard cuadrático, `testhadamard`. El comando `prodhadamard` realiza el producto hadamard de dos matrices.

```
testhadamard[L_]:=Catch[Do[If[Apply[Plus,L[[i]]]=!= 0,
      Throw[False]], {i,2,Length[L]}]; Throw[True]];
prodhadamard[a_,b_]:=Table[Table[a[[i, j]]*b[[i, j]],
      {j, Length[a[[1]]]}], {i, Length[a[[1]]]}];
Print["Buscando matrices de Hadamard..."];
had={}; Do[If[testhadamard[base2cociclos[[i]]],
      Print["El generador ",i," es de Hadamard:"];
      had = Append[had, base2cociclos[[i]]], {i,
Length[base2cociclos]}];       Module[{m}, Do[
        m=Fold[prodhadamard,base2cociclos[[lista2cociclos[[i,1]]]],
          Table[base2cociclos[[lista2cociclos[[i,j]]]],
      {j,2,Length[lista2cociclos[[i]]]}]];
```

```
      If[testhadamard[m], Print["El 2-cociclo generado por el producto
        hadamard de los generadores ",lista2cociclos[[i]],
        " es de Hadamard"]; had=Append[had,m]]
,{i, Length[lista2cociclos]}]]; Print["Hay ",Length[had],
      " matrices de hadamard provenientes de 2-cociclos
normalizados."];
```

3.2 Búsqueda de matrices cocíclicas de Hadamard

A diferencia del método de construcción que describiéramos en la Sección 1.2.1, basado en el estudio de matrices desarrolladas sobre un grupo, las matrices cocíclicas de Hadamard pueden tener un orden $4t$ cualquiera (no necesariamente un cuadrado perfecto). Más aún, actualmente se conjetura que de este modo se puede obtener matrices de Hadamard en cualquier orden múltiplo de 4.

Al final del capítulo primero describimos ciertas obstrucciones para el carácter Hadamard de 2-cociclos en grupos dados, de las cuales nos serviremos posteriormente de forma puntual para determinar matrices cocíclicas de Hadamard.

Estas obstrucciones vienen a decir que un grupo de Hadamard que escinda sobre su subgrupo central distinguido ha de tener orden $2m^2$, y que los 2-subgrupos de Sylow de grupos de Hadamard de orden $2^k m$, con $k \geq 3$ y m impar, no pueden ser ni cíclicos ni diédricos.

Dado que el resultado de hacer el producto Kronecker de una matriz de Hadamard de orden 2 por una matriz de Hadamard de orden $4t$ facilita una matriz de Hadamard de orden $8t$, si se pretende encontrar matrices de Hadamard en todos los órdenes múltiplos de 4 bastará con hallar dichas matrices para órdenes $4t$ con t impar. En lo que sigue, a no ser que se especifique lo contrario, t será impar.

Flannery en [42] estudia la existencia de matrices cocíclicas de Hadamard desarrolladas sobre ciertos grupos: el grupo cíclico de orden $4t$, $\mathbb{Z}_{4t} \overset{t \text{ impar}}{\cong} \mathbb{Z}_4 \times \mathbb{Z}_t$; el grupo dicíclico $Q_{4t} \cong \mathbb{Z}_4 \ltimes \mathbb{Z}_t$; el grupo producto directo $\mathbb{Z}_t \times \mathbb{Z}_2^2$; y el grupo diédrico $D_{4t} \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_{2t}$.

Veamos, de forma resumida, los resultados que obtiene en su estudio de matrices

cocíclicas de Hadarmard sobre estos grupos.

Comencemos exponiendo los resultados que obtiene para los grupos $\mathbb{Z}_4 \times \mathbb{Z}_t$. Una presentación de estos grupos es $< a, b : a^t = b^4 = [a, b] = 1 >$.

Tomemos la ordenación $G = \{1, b, b^2, a, ba, b^2a, b^3a, \ldots, a^{t-1}, ba^{t-1}, b^2a^{t-1}, b^3a^{t-1}\}$.

Dado que $H^2(\mathbb{Z}_t, Z_2) = 0$ (recuérdese que t es impar), se tiene que $H^2(G, \mathbb{Z}_2) \cong H^2(G/ < a >, \mathbb{Z}_2) = \mathbb{Z}_2$, cuyo único generador es simétrico y viene dado (gracias a la ordenación elegida) como la matriz S producto de Kronecker de la matriz reversa negacíclica de orden 4 por la matriz toda de unos de orden t.

Como una matriz genérica procedente de los 2-cobordes $B^2(G, \mathbb{Z}_2)$ es equivalente Hadamard (exclusivamente por negaciones de filas o columnas, sin realizar permutaciones) a una matriz desarrollada sobre G, resulta que una matriz representando un 2-coborde genérico es, salvo negación de filas y/o columnas, del tipo

$$B = \begin{pmatrix} X_1 & X_2 & \cdots & X_t \\ X_2 & X_3 & \cdots & X_1 \\ \vdots & \vdots & & \vdots \\ X_t & X_1 & \cdots & X_{t-1} \end{pmatrix},$$

con cada X_j matriz reversa circular de orden 4; de modo que las matrices cocíclicas sobre G son equivalentes Hadamard a las del tipo $S^i \cdot B^j$ para $i, j \in \{0, 1\}$.

Se puede probar que ninguna matriz del tipo $S \cdot B^j$ es Hadamard, para $j = 0, 1$, de modo que las matrices cocíclicas de Hadamard se han de buscar entre las matrices B que provienen de 2-cobordes, que sólo pueden existir para órdenes cuadrados perfectos $4t = 4n^2$.

Más aún, estas matrices 2-cobordes son equivalentes Hadamard a matrices reversas circulares, y se conjetura que una matriz de este forma sólo puede ser de Hadamard para $t = 1$. Esto hace desaconsejable tratar de seguir buscando matrices cocíclicas de Hadamard sobre este grupo.

Consideremos ahora el grupo dicíclico $Q_{4t} =< a, b : a^{2t}, b^2 = a^t, b^{-1}ab = a^{-1} >$.

Para valores de t impar, Flannery prueba que toda matriz cocíclica de Hadamard sobre G está necesariamente asociada a un 2-coborde. De modo que caemos en la

misma problemática que en el caso anterior, puesto que sólo pueden existir matrices cocíclicas de Hadamard desarrolladas sobre estos grupos para órdenes cuadrados perfectos.

De hecho, Horadam en [63] comenta que se han llevado a cabo trabajos experimentales tanto con el grupo cíclico, $\mathbb{Z}_{4t}$, como con el dicíclico, Q_{4t}; sin obtener en caso alguno matrices cocíclicas de Hadamard para t impar.

El grupo producto directo $\mathbb{Z}_t \times \mathbb{Z}_2^2$ como base para encontrar matrices cocíclicas de Hadamard, ha sido ampliamente estudiado por Baliga y Horadam como se refleja en [7].

Una presentación de este grupo es:

$$< x : x^t > \times < u, v : u^2, v^2, [u, v] >, \tag{3.2}$$

siendo x, v y u los generadores de $\mathbb{Z}_t^{\bullet}$, $\mathbb{F}_2$ y $\mathbb{F}_2$, respectivamente.

Tal y como comentábamos anteriormente, Horadam divide los 2-cociclos puros normalizados en un producto Hadamard de una matriz procedente de los 2-cobordes, otra simétrica y una tercera desarrollada sobre un 2-cociclo conmutador. Baliga y Horadam en el artículo citado describen cómo son las matrices correspondientes a la parte simétrica y conmutadora.

La matriz simétrica, como se indicaba en [24], es de la forma:

$$S = 1_t \otimes \begin{pmatrix} 1 & 1 \\ 1 & B \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & A \end{pmatrix} = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & A & 1 & A \\ 1 & 1 & B & B \\ 1 & A & B & AB \end{pmatrix}; \; A, B = \pm 1. \tag{3.3}$$

Por otra parte, la matriz asociada a la parte conmutadora es de la forma:

$$C = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & K & 1 & K \\ 1 & K & 1 & K \end{pmatrix}; \; K = \pm 1. \tag{3.4}$$

Por último, la matriz asociada a los 2-cobordes la encuentran normalizando una matriz arbitraria desarrollada sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$. Aunque, en realidad, en lugar de trabajar con dicha matriz, consideran una matriz Hadamard equivalente desarrollada

sobre el grupo. Esta matriz es una matriz de $t \times t$ bloques circular hacia atrás, cuya fila superior está constituida por bloques 4×4 desarrollados cada uno de ellos sobre $\mathbb{Z}_2^2$ (podríamos denotar la primera fila del bloque i-ésimo por a_i, b_i, c_i, d_i).

Con todo esto, cualquier matriz cocíclica pura normalizada sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$ es Hadamard equivalente a una matriz de $t \times t$ bloques circular hacia atrás, en la que un bloque cualquiera de su primera fila será de la forma:

$$\begin{pmatrix} a_i & b_i & c_i & d_i \\ b_i & Ac_i & d_i & Aa_i \\ c_i & Kd_i & Ba_i & BKb_i \\ d_i & AKa_i & Bb_i & ABKc_i \end{pmatrix}; \ 1 \leq i \leq t.$$

Algunos resultados obtenidos por Baliga y Horadam a partir del conocimiento de las matrices cocíclicas asociadas a $\mathbb{Z}_t \times \mathbb{Z}_2^2$ son los siguientes.

En primer lugar, se tiene que si la matriz cocíclica desarrollada sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$ es simétrica ($K = 1$) y, además, $A = B = 1$, dicha matriz es Hadamard equivalente a una matriz desarrollada sobre un grupo, pudiendo dar lugar a una matriz de Hadamard sólo si se trata de una matriz de orden $4t$, con t un cuadrado perfecto. Por consiguiente, estas matrices con $A = B = K = 1$ no parecen una buena opción para efectuar la búsqueda de matrices cocíclicas de Hadamard.

Es más, demuestran que no existen matrices cocíclicas de Hadamard simétricas sobre este grupo para $t \equiv 3(\text{mod } 4)$, llegando a conjeturar, incluso, que no existen matrices cocíclicas de Hadamard simétricas sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$ para $t > 1$ impar. Luego, ciertamente, las matrices cocíclicas simétricas desarrolladas sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$, no son las más apropiadas para tratar de encontrar matrices cocíclicas de Hadamard.

A su vez, Baliga y Horadam demuestran que las matrices de Williamson son Hadamard equivalentes a matrices cocíclicas de Hadamard sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$, en las que $A = B = K = -1$. Hemos de aclarar que se obtienen más matrices cocíclicas de Hadamard sobre este grupo que matrices de Hadamard del tipo de Williamson.

Más aún, Horadam y Baliga demuestran que una matriz cocíclica de la forma $(A, B, -1)$ sólo puede dar lugar a una matriz de Hadamard si $A = B = -1$. Por tanto, parece que la búsqueda de matrices cocíclicas de Hadamard sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$ se ha de centrar en el prometedor caso en que $(A, B, K) = (-1, -1, -1)$.

Como veremos a continuación, el grupo diédrico, D_{4t} también parece propicio a la hora de buscar matrices cocíclicas de Hadamard. Este grupo ha sido estudiado ampliamente por Flannery en este sentido en [41, 42].

Una presentación de este grupo viene dada por $\mathbb{Z}_2 \ {}_\chi\ltimes \mathbb{Z}_{2t} =< a, b : a^{2t} = b^2 = (ab)^2 = 1 >$.

Flannery encuentra la forma que han de tener las matrices simétrica y conmutadora asociadas a este grupo. Tomando la ordenación

$$\{1, a, a^2, \ldots, a^{2t-1}, b, ab, a^b, \ldots, a^{2t-1}b\}$$

de los elementos de D_{4t}, la matriz simétrica es de la forma:

$$S = 1_t \otimes \begin{pmatrix} 1 & 1 \\ 1 & B \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & A \end{pmatrix} = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & A & 1 & A \\ 1 & 1 & B & B \\ 1 & A & B & AB \end{pmatrix} ; \ A, B = \pm 1. \qquad (3.5)$$

La matriz asociada a la parte conmutadora es de la forma:

$$C = \left(\begin{array}{c|ccc|c|ccc|c} + & + & \cdots & + & + & + & \cdots & + & + \\ \hline + & + & \cdots & K & + & + & \cdots & K & + \\ \vdots & & / & \vdots & & & / & \vdots & \vdots \\ + & K & \cdots & K & + & K & \cdots & K & + \\ \hline + & K & \cdots & K & + & K & \cdots & K & + \\ \vdots & & \ddots & \vdots & & & \ddots & \vdots & \vdots \\ + & + & \cdots & K & + & + & \cdots & K & + \\ \hline + & + & \cdots & + & + & + & \cdots & + & + \end{array}\right)_{4t \times 4t} ; \ K = \pm 1. \qquad (3.6)$$

Por último, la matriz asociada a los 2-cobordes la toma como una matriz desarrollada sobre este grupo, dando lugar a una matriz de la forma:

$$\begin{pmatrix} M & N \\ NC_{2t} & NC_{2t} \end{pmatrix},$$

donde M y N son matrices circulares reversas de orden $2t \times 2t$ y C_{2t} es la matriz circular reversa de orden $2t \times 2t$ cuya primera fila es $(\ 1 \ \ 0 \ \ 0 \ \cdots \ 0 \ )$.

El primer resultado destacable que obtiene Flannery en nuestro contexto es que para t impar, no se pueden obtener matrices cocíclicas de Hadamard en los casos en los que $(A, B, K) = (1, 1, -1)$, $(A, B, K) = (-1, -1, -1)$ ó $(A, B, K) = (-1, 1, -1)$.

En el caso en que $(A, B, K) = (1, -1, -1)$ existe una matriz de Hadamard desarrollada sobre D_{4t} si y sólo si existen M y N de orden $2t \times 2t$, cada una de ellas obtenidas como el producto Hadamard de una matriz circular reversa por una matriz negacíclica reversa, tales que:

$$M^2 + N^2 = 4tI_{2t}.$$

Es más, Flannery consigue reducir esta condición considerablemente, llegando a demostrar que si $\overrightarrow{m}_i$ y $\overrightarrow{n}_i$ son las filas i-ésimas de M y N respectivamente, entonces $M^2 + N^2 = 4tI_{2t}$ si y sólo si $\overrightarrow{m}_1 \overrightarrow{m}_i^T = -\overrightarrow{n}_1 \overrightarrow{n}_i^T$ para todo i, $2 \leq i \leq t$. A su vez, esto se puede simplificar, de manera que para encontrar una matriz de Hadamard a partir de un 2-cociclo tal que $(A, B, K) = (1, -1, -1)$, basta encontrar un par de $2t$-tuplas $\overrightarrow{m}$ y $\overrightarrow{n}$ con entradas ± 1 tales que $\overrightarrow{m}(\overrightarrow{m}P^iW_i) = -\overrightarrow{n}(\overrightarrow{n}P^iW_i)$ para $1 \leq i \leq t-1$, siendo W_i una matriz diagonal de orden $2t \times 2t$ cuya diagonal principal es

$$\overbrace{1\,1\,\cdots 1}^{2t-1}\ -1\ \cdots\ -1$$

y P una matriz circular hacia adelante cuya primera fila es

$$0\,0\,\cdots\,0\,1;$$

de modo que al multiplicar un vector fila $(a_1\ a_2\ \cdots\ a_{2t})$ por la matriz P^i, se obtiene un vector igual al primero, pero cuyos elementos están rotados a la izquierda i posiciones, $(a_{i+1}\ a_{i+2}\ \cdots\ a_{2t}\ a_1\ \cdots\ a_i)$.

La importancia de este resultado estriba en que gracias a él, comprobar si una matriz asociada a un 2-cociclo de la forma $(A, B, K) = (1, -1, -1)$ es de Hadamard se reduce a estudiar sus $t-1$ primeras filas. Pero, además, esta reducción adquiere más relevancia en el momento en que Flannery constata que existe una mayor densidad de matrices de Hadamard desarrolladas sobre D_{4t} precisamente en el caso $(A, B, K) = (1, -1, -1)$. Luego, según estos resultados parece que interesa buscar matrices cocíclicas de Hadamard a partir de matrices cocíclicas en las que $(A, B, K) = (1, -1, -1)$, puesto que por una parte es donde se puede encontrar más matrices de Hadamard y por otra parte, la búsqueda es mucho más rápida. De hecho, como $\overrightarrow{m}$ y $\overrightarrow{n}$ son $2t$-tuplas, el espacio de búsqueda de cada uno de estos vectores

contiene 2^{2t} vectores. En realidad, se puede reducir a 2^{2t-1}, puesto que si $\overrightarrow{m}$ y $\overrightarrow{n}$ son vectores que verifican la condición exigida, $-\overrightarrow{m}$ y $-\overrightarrow{n}$, también la verifican; de modo que se puede tomar que ambos comienzan con la entrada 1. Así, el espacio de búsqueda de la primera fila de una matriz cocíclica de Hadamard proveniente de un 2-cociclo tal que $(A, B, K) = (1, -1, -1)$ es de tamaño $2^{2t-1} \cdot 2^{2t-1} = 2^{4t-2}$.

Mediante este procedimiento, Flannery es capaz de encontrar matrices cocíclicas de Hadamard sobre D_{4t}, con $(A, B, K) = (1, -1, -1)$, hasta $t = 11$.

A la vista de estos resultados, parece que tanto el grupo $\mathbb{Z}_2^2 \times \mathbb{Z}_t$ como D_{4t} presentan buenas maneras a la hora de encontrar matrices cocíclicas de Hadamard. Esto lo corrobora Horadam en [63], donde muestra una tabla en la que compara el número de matrices cocíclicas de Hadamard para los grupos cíclicos Z_{4t}, dicíclicos Q_{4t}, el producto directo $\mathbb{Z}_t \times \mathbb{Z}_2^2$ y los grupos diédricos D_{4t}:

t	$\mathbb{Z}_{4t}$	Q_{4t}	$\mathbb{Z}_t \times \mathbb{Z}_2^2$	D_{4t}
1	2	2	6	6
2	0	0	168	32
3	0		24	72
4	0			768
5	0		120	2380

(3.7)

Para contrastar cuán beneficioso puede ser el método de reducción homológica que propusimos al comienzo del capítulo, vamos a trabajar estas dos familias de grupos desde nuestra particular perspectiva, con la esperanza de obtener más información acerca de la existencia de matrices cocíclicas de Hadamard sobre ellos.

3.3 Matrices cocíclicas de Hadamard por el método de la reducción homológica

3.3.1 Matrices cocíclicas de Hadamard sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$

Acabamos de ver que el producto directo $\mathbb{Z}_t \times \mathbb{Z}_2^2$, es un grupo potencialmente interesante a la hora de buscar matrices de Hadamard, por varios motivos:

1. Estos grupos, a priori, pueden dar lugar a matrices de Hadamard en cualquier

orden múltiplo de 4, pues no existe ninguna restricción conocida al respecto.

2. La factorización en 2-cobordes, parte simétrica y conmutadora es bien conocida para grupos abelianos como éste.

3. Las matrices de Hadamard del tipo de Williamson son Hadamard equivalentes a matrices cocíclicas de Hadamard desarrolladas sobre este grupo.

En esta sección vamos a estudiar la posibilidad de obtener matrices cocíclicas de Hadamard sobre el grupo $\mathbb{Z}_t \times \mathbb{Z}_2^2$. Para ello vamos a utilizar el método de reducción homológica y las implementaciones en *Mathematica* que hemos presentado a lo largo de la memoria. De hecho, nuestra forma de trabajo se puede dividir en dos fases:

1. Una primera, en la que se obtienen resultados experimentales con la ayuda del ordenador; en base a los cuales posteriormente se establecen conjeturas.

2. Una segunda, en la que se trata de formalizar las conjeturas previamente elaboradas en resultados teóricos contrastados.

En primer lugar, estudiaremos cómo son las matrices correspondientes a los generadores de los 2-cociclos asociados a este grupo para, a partir de ellas, buscar una base de los mismos. Con esta base se podrían generar todas las matrices cocíclicas y, utilizando el test de Hadamard cuadrático, determinar las matrices de Hadamard que se pueden obtener para una dimensión dada.

Al igual que hiciese Horadam, consideramos los 2-cociclos puros normalizados como el producto Hadamard de una matriz procedente de los 2-cobordes, otra simétrica y una tercera desarrollada sobre un 2-cociclo conmutador.

Por otra parte, siguiendo las mismas pautas que Horadam y Baliga en [7], nos centramos en el estudio de los valores impares de t; para los cuales obtenemos las mismas matrices de las partes simétrica (ver (3.3)) y conmutadora (ver (3.4)), que denotamos por β_1, β_2 y γ, respectivamente:

$$\beta_1 = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \qquad \beta_2 = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

$$\gamma = 1_t \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix}$$

El método de reducción homológica exige que determinemos, adicionalmente, una base para las matrices que provienen de los 2-cobordes normalizados. Como demostraremos más adelante, para un valor de t genérico (impar) se obtiene que dicha base viene dada por $4t-3$ matrices α_i. Experimentalmente, obtenemos que estas matrices α_i, con $2 \leq i \leq 4t-2$, están constituidas por unos y menos unos; de manera que los menos unos están dispuestos en todas las posiciones $(-,i)$ e $(i,-)$ (exceptuando las posiciones $(i,1)$, (i,i) y $(1,i)$), y también en los bloques que a continuación se marcan mediante una x:

$$\text{Para} \begin{cases} i = 2 \\ i = 3 \\ i = 4 \end{cases} \quad \left(\begin{array}{c|c|c|c|c|c} x & & & \cdots & & \\ \hline & & & \cdots & & x \\ \hline & & & \cdots & x & \\ \hline & & & / & & \\ \hline & & x & \cdots & & \\ \hline & x & & \cdots & & \end{array}\right) \tag{3.8}$$

$$\text{Para} \begin{cases} i = 5 \\ i = 6 \\ i = 7 \\ i = 8 \end{cases} \quad \left(\begin{array}{c|c|c|c|c|c} & x & & \cdots & & \\ \hline x & & & \cdots & & \\ \hline & & & \cdots & & x \\ \hline & & & \cdots & x & \\ \hline & & & / & & \\ \hline & & x & \cdots & & \end{array}\right) \tag{3.9}$$

$$\text{Para} \begin{cases} i = 4(t-2)+1 \\ i = 4(t-2)+2 \\ i = 4(t-2)+3 \\ i = 4(t-1) \end{cases} \quad \left(\begin{array}{c|c|c|c|c|c} & & & \cdots & x & \\ \hline & & & / & & \\ \hline & & x & \cdots & & \\ \hline & x & & \cdots & & \\ \hline x & & & \cdots & & \\ \hline & & & \cdots & & x \end{array}\right) \tag{3.10}$$

$$\text{Para } \begin{cases} i &= 4(t-1)+1 \\ i &= 4(t-1)+2 \end{cases} \quad \left(\begin{array}{|c|c|c|c|c|c|} \hline & & & \cdots & & x \\ \hline & & & \cdots & x & \\ \hline & & & / & & \\ \hline & & x & \cdots & & \\ \hline & x & & \cdots & & \\ \hline x & & & \cdots & & \\ \hline \end{array}\right) \tag{3.11}$$

Por otra parte, para un mismo 2-coborde los bloques x marcados en estas matrices son iguales entre sí, aunque el tipo de bloque x depende del 2-coborde en cuestión. De hecho, los bloques que nos podemos encontrar son los siguientes (con la salvedad ya comentada de que en el 2-coborde α_i los bloques que contienen a la fila y/o columna i-ésima tienen dichas líneas formadas sólo por menos unos, exceptuando las posiciones 1 e i, que son unos):

$$\text{Para } i \equiv 2 \pmod 4 : \quad \left(\begin{array}{|c|c|c|c|} \hline & - & & \\ \hline - & & & \\ \hline & & & - \\ \hline & & - & \\ \hline \end{array}\right) \tag{3.12}$$

$$\text{Para } i \equiv 3 \pmod 4 : \quad \left(\begin{array}{|c|c|c|c|} \hline & & - & \\ \hline & & & - \\ \hline - & & & \\ \hline & - & & \\ \hline \end{array}\right) \tag{3.13}$$

$$\text{Para } i \equiv 0 \pmod 4 : \quad \left(\begin{array}{|c|c|c|c|} \hline & & & - \\ \hline & & - & \\ \hline & - & & \\ \hline - & & & \\ \hline \end{array}\right) \tag{3.14}$$

$$\text{Para } i \equiv 1 \pmod 4 : \quad \left(\begin{array}{|c|c|c|c|} \hline - & & & \\ \hline & - & & \\ \hline & & - & \\ \hline & & & - \\ \hline \end{array}\right) \tag{3.15}$$

Analíticamente se puede comprobar que las matrices asociadas a los 2-cobordes son de la forma indicada anteriormente. Para ello vamos a trabajar, en lugar de con los elementos del grupo $\mathbb{Z}_t \times \mathbb{Z}_2^2$ según la presentación (3.2), con una representación de los elementos mediante ternas,

$$\mathbb{Z}_t \times \mathbb{Z}_2^2 = \{(0,0,0),(0,1,0),(0,0,1),(0,1,1),(1,0,0),(1,1,0),(1,0,1),(1,1,1),\ldots,$$
$$(t-1,0,0),(t-1,1,0),(t-1,0,1),(t-1,1,1)\}$$

Recordemos que los 2-cobordes vienen dados por:

$$[\alpha_{a,b,c}]((a_0,b_0,c_0),(a_1,b_1,c_1)) =$$
$$= \alpha_{a,b,c}(a_0,b_0,c_0)\cdot\alpha_{a,b,c}(a_1,b_1,c_1)\cdot\alpha_{a,b,c}^{-1}((a_0,b_0,c_0)(a_1,b_1,c_1)),$$

siendo

$$\alpha_{a,b,c}(a_j,b_j,c_j) = \begin{cases} 1 & \text{si} \quad (a_j,b_j,c_j) \neq (a,b,c) \\ -1 & \text{si} \quad (a_j,b_j,c_j) = (a,b,c) \end{cases}$$

Teniendo en cuenta que en $\mathbb{F}_2$ el inverso de un elemento es él mismo y que la ley del grupo $\mathbb{Z}_t \times \mathbb{Z}_2^2$ es la natural, componente a componente,

$$(a_0,b_0,c_0)(a_1,b_1,c_1) = (a_0+a_1, b_0+b_1, c_0+c_1);$$

se puede decir que

$$[\alpha_{a,b,c}]((a_0,b_0,c_0),(a_1,b_1,c_1)) =$$
$$= \alpha_{a,b,c}(a_0,b_0,c_0)\cdot\alpha_{a,b,c}(a_1,b_1,c_1)\cdot\alpha_{a,b,c}(a_0+a_1,b_0+b_1,c_0+c_1).$$

Si consideramos un 2-coborde distinto del primero (que será el único no normalizado), esto es, si $\alpha_{(a,b,c)} \neq \alpha_{(0,0,0)}$, analicemos cómo serán las distintas filas de la matriz asociada a dicho 2-coborde:

1. Si $(a_0,b_0,c_0) = (0,0,0)$, es decir, si nos remitimos a la primera fila de la matriz asociada al 2-coborde (a,b,c). En este caso se tiene que las entradas correspondientes a cada una de las columnas son

$$[\alpha_{(a,b,c)}]((0,0,0),(a_1,b_1,c_1)) = \alpha_{(a,b,c)}(0,0,0)\alpha_{(a,b,c)}(a_1,b_1,c_1)\alpha_{(a,b,c)}(a_1,b_1,c_1) =$$
$$= 1\cdot\alpha_{(a,b,c)}^2(a_1,b_1,c_1) = 1.$$

Por tanto, en la primera fila del 2-coborde todas las entradas son $+1$.

2. Si consideramos la fila $(a_0, b_0, c_0) = (a, b, c)$, esto es, la fila i-ésima del 2-coborde i-ésimo, como $\alpha_{(a,b,c)}(a, b, c) = -1$, se tiene que

$$[\alpha_{(a,b,c)}]((a, b, c), (a_1, b_1, c_1)) = -\alpha_{(a,b,c)}(a_1, b_1, c_1)\alpha_{(a,b,c)}(a + a_1, b + b_1, c + c_1).$$

El factor $\alpha_{(a,b,c)}(a_1, b_1, c_1)$ será -1 siempre que $(a_1, b_1, c_1) = (a, b, c)$. En este caso

$$\alpha_{(a,b,c)}(a + a_1, b + b_1, c + c_1) = \alpha_{(a,b,c)}(a + a, b + b, c + c) = 1,$$

pues para que fuese -1 tendía que ser $a = b = c = 0$, lo cual es una contradicción, ya que estamos suponiendo que el 2-coborde considerado es distinto del primero, $(0, 0, 0)$. Es decir, en la fila i-ésima del 2-coborde i-ésimo, la posición (i, i) le corresponde una entrada positiva.

Por otra parte, el factor $\alpha_{(a,b,c)}(a + a_1, b + b_1, c + c_1)$ será igual a -1 si y sólo si $a + a_1 = a$, $b + b_1 = b$ y $c + c_1 = c$, lo cual sólo ocurre si $a_1 = b_1 = c_1 = 0$. En este caso, $\alpha_{(a,b,c)}(0, 0, 0) = 1$, pues $(a, b, c) \neq (0, 0, 0)$.

Por tanto, el 2-coborde (a, b, c), en la entrada $((0, 0, 0), (a, b, c))$ tiene otro 1, esto es, la matriz correspondiente al 2-coborde i-ésimo tiene otra entrada positiva en la posición $(i, 1)$. Cualquier otra entrada de la fila (a, b, c) de la matriz correspondiente al 2-coborde (a, b, c) será negativa, puesto que los dos factores $\alpha_{(a,b,c)}(a_1, b_1, c_1)$ y $\alpha_{(a,b,c)}(a + a_1, b + b_1, c + c_1)$ son positivos.

Como conclusión, se tiene que la fila i-ésima de la matriz asociada al i-ésimo 2-coborde tiene todas sus entradas negativas, salvo en las posiciones $(i, 1)$ y (i, i), que son positivas.

3. Para cualquier otra fila (a_0, b_0, c_0), con $(a_0, b_0, c_0) \neq (0, 0, 0)$y $(a_0, b_0, c_0) \neq (a, b, c)$, se tiene que

$$[\alpha_{(a,b,c)}]((a_0, b_0, c_0), (a_1, b_1, c_1)) =$$

$$= \alpha_{(a,b,c)}(a_0, b_0, c_0)\alpha_{(a,b,c)}(a_1, b_1, c_1)\alpha_{(a,b,c)}(a_0 + a_1, b_0 + b_1, c_1),$$

El primer factor, $\alpha_{(a,b,c)}(a_0, b_0c_0)$, por ser $(a, b, c) \neq (a_0, b_0, c_0)$ es siempre igual a 1.

El segundo factor, $\alpha_{(a,b,c)}(a_1, b_1, c_1)$, valdrá -1 siempre que $a_1 = a$, $b_1 = b$ y $c_1 = c$. Cuando esto ocurre el tercer factor vale 1, puesto que $(a_0, b_0, c_0) \neq (0, 0, 0)$. Es decir, la columna i-ésima del 2-coborde i-ésimo tiene todas sus entradas negativas, en cualquier fila distinta de la primera y (la i-ésima).

Si estudiamos cuándo es -1 el tercer factor, llegamos a la conclusión que esto ocurre si y sólo si

$$\begin{cases} a_0 + a_1 &= a \\ b_1 + b_0 &= b \\ c_0 + c_1 &= c \end{cases} \tag{3.16}$$

Como $(a_0, b_0, c_0) \neq (0,0,0)$, entonces $(a_1, b_1, c_1) \neq (a, b, c)$. Del mismo modo, como $(a_0, b_0, c_0) \neq (a, b, c)$, entonces $(a_1, b_1, c_1) \neq (0,0,0)$. Así, en las posiciones indicadas habrá un -1, puesto que $\alpha_{(a,b,c)}(a_0, b_0, c_0) = 1$ y $\alpha_{(a,b,c)}(a_1, b_1 c_1) = 1$.

Al resolver el sistema (3.16) se tiene que:

2-coborde (a,b,c)	fila (a_0,b_0,c_0)	columna (a_1,b_1,c_1)
$(a,0,0)$	(a_0,b_0,c_0)	$([a-a_0]_t, [b_0]_2, [c_0]_2)$ con $\begin{cases} a_0 \neq a \\ a \neq 0 \end{cases}$
$(a,1,0)$	(a_0,b_0,c_0)	$([a-a_0]_t, [1+b_0]_2, [c_0]_2)$
$(a,0,1)$	(a_0,b_0,c_0)	$([a-a_0]_t, [b_0]_2, [1+c_0]_2)$
$(a,1,1)$	(a_0,b_0,c_0)	$([a-a_0]_t, [1+b_0]_2, [1+c_0]_2)$

donde $[a]_n$ denota la clase de a módulo n.

Como conclusión de todo este análisis se tiene que el 2-coborde i-ésimo tiene en cada fila, distintas de la primera y de la i-ésima, dos entradas iguales a -1 y el resto de entradas son iguales a 1.

Nos queda por analizar el primer 2-coborde:

$$[\alpha_{(0,0,0)}]((a_0,b_0,c_0),(a_1,b_1,c_1)) =$$

$$= \alpha_{(0,0,0)}(a_0,b_0,c_0)\alpha_{(0,0,0)}(a_1,b_1,c_1)\alpha_{(0,0,0)}(a_0+a_1, b_0+b_1, c_0+c_1),$$

Si estudiamos cómo son las entradas correspondientes a la primera fila y a la primera columna de la matriz de este 2-coborde se lo siguiente:

- La primera fila corresponde a $(a_0, b_0, c_0) = (0,0,0)$.

$$[\alpha_{(0,0,0)}]((0,0,0),(a_1,b_1,c_1)) = -\alpha^2_{(0,0,0)}(a_1,b_1,c_1) = -1,$$

por tanto, sus entradas serán todas negativas.

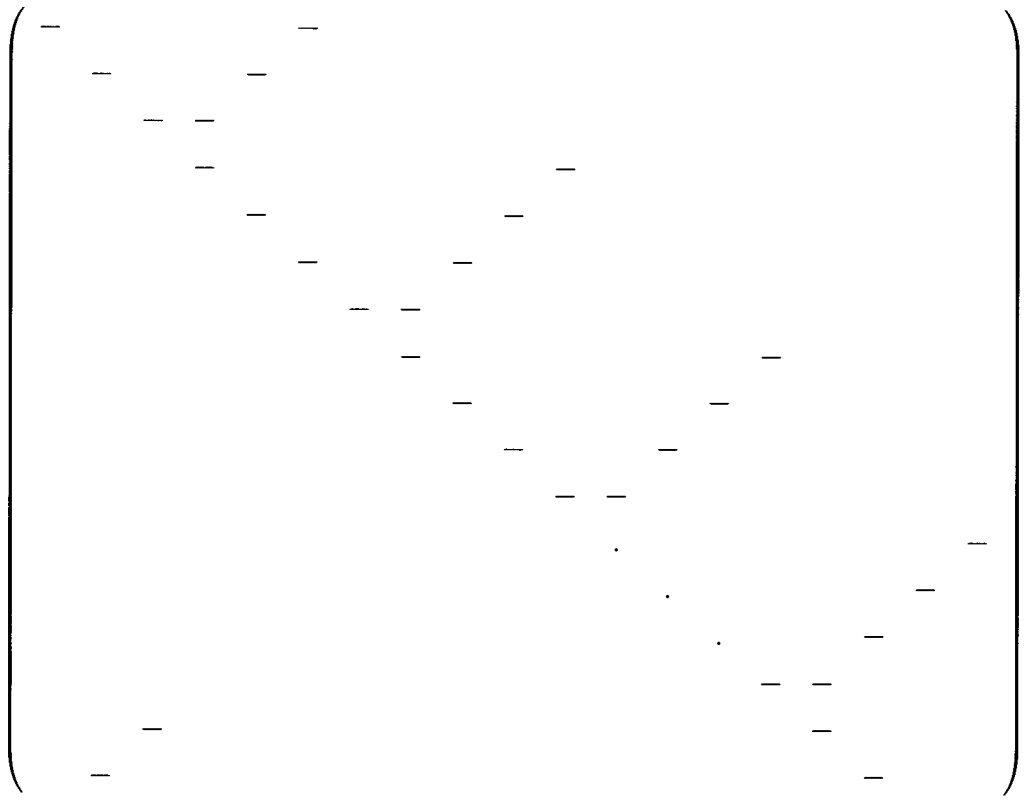
- La primera columna es la correspondiente a $(a_1, b_1, c_1) = (0, 0, 0)$, siendo todas sus entradas también negativas, por un razonamiento análogo:

$$[\alpha_{(0,0,0)}]((a_0, b_0, c_0), (0, 0, 0)) = -\alpha^2_{(0,0,0)}(a_0, b_0, c_0) = -1.$$

Luego, el 2-coborde $[\alpha_{(0,0,0)}]$ es el único no normalizado (no tiene todas las entradas de la primera fila y columna positivas). Nosotros sólo estamos interesados en los 2-cobordes normalizados, por lo que podemos prescindir de éste.

Base de los 2-cobordes

Experimentalmente se puede ver que para cualquier valor de t una base de los 2-cobordes viene dada por $\{\alpha_2, \ldots, \alpha_{4t-2}\}$, como adelantásemos en la sección anterior. Para demostrar este resultado vamos a construir una matriz $(4t-3) \times 4t$, de manera que la fila i-ésima venga dada por las entradas del 2-coborde i-ésimo (con $2 \leq i \leq 4t-2$). Si nos fijamos en las $4t-1$ últimas columnas, se tiene la submatriz de orden $(4t-3) \times (4t-1)$:



Podemos comprobar mediante inducción que esta matriz es de rango máximo.

1. Para $t = 3$, si a la fila $4t-4$ de la submatriz anterior le restamos las filas 3 y 4, $F_{4t-4} - (F_3 + F_4)$, el -1 que inicialmente estaba en la posición $(4t-4, 3)$, pasa a la posición $(4t-4, 11)$ de la siguiente forma:

$$(4t-4, 3) \to (4t-4, 4) \to (4t-4, 11) = (4t-4, 4t-1).$$

Del mismo modo, si a la fila $4t-3$ de la submatriz anterior le restamos las filas 2 y 5, $F_{4t-3} - (F_2 + F_5)$, el -1 que aparece en la posición $(4t-3, 2)$, lo llevamos a la posición $(4t-3, 10)$ de la siguiente forma:

$$(4t-3, 2) \to (4t-3, 5) \to (4t-3, 10) = (4t-3, 4t-2).$$

Así, la matriz anterior se transforma en una matriz con diagonal principal de menos unos, y por debajo de la misma no aparece ninguno:

$$\begin{pmatrix} - & & & & - & & & & & & & \\ & - & & - & & & & & & & & \\ & & - & - & & & & & & & & \\ & & & - & & & & & & & - & \\ & & & & - & & & & - & & & \\ & & & & & - & & - & & & & \\ & & & & & & - & - & & & & \\ & & & & & & & - & & & - & \\ & & & & & & & & - & - & & \end{pmatrix}_{(4t-3)\times(4t-1)}$$

Por tanto, el rango de la matriz cuyas filas son las componentes de las matrices asociadas a los 2-cobordes $\alpha_2, \ldots, \alpha_{4t-2}$ es máximo, igual a $4t-3$.

2. Para $t = 5$ se tiene de forma análoga que la matriz correspondiente es de rango máximo puesto que, si se hacen las siguientes transformaciones elementales:

   (a) $F_{4t-4} - (F_3 + F_4 + F_{11} + F_{12})$, el -1 que inicialmente estaba en la posición $(4t-4, 3)$, pasa a la posición $(4t-4, 19)$ de la siguiente forma:

$$(4t-4, 3) \to (4t-4, 4) \to (4t-4, 11) \to (4t-4, 12) \to (4t-4, 19) =$$

$$= (4t-4, 4t-1).$$

(b) $F_{4t-3} - (F_2 + F_5 + F_{10} + F_{13})$, el -1 que aparece en la posición $(4t-3, 2)$, lo llevamos a la posición $(4t-3, 18)$ de la siguiente forma:

$$(4t-3,2) \to (4t-3,5) \to (4t-3,10) \to (4t-3,13) \to (4t-3,18) =$$
$$= (4t-3, 4t-2).$$

3. Supongamos que este razonamiento es cierto para $t \leq k$, con k impar. Es decir, si se hacen las siguientes transformaciones elementales:

(a) $F_{4k-4} - (\sum_{r=0}^{\lfloor k/2 \rfloor - 1} F_{3+8r} + F_{4+8r})$, el -1 que inicialmente está en la posición $(4k-4, 3)$, pasa a la posición $(4k-4, 4k-1) = (4t-4, 4t-1)$.

(b) $F_{4k-3} - (\sum_{r=0}^{\lfloor k/2 \rfloor - 1} F_{2+8r} + F_{3+8r})$, el -1 que aparece en la posición $(4k-3, 2)$, lo llevamos a la posición $(4k-3, 4k-2) = (4t-3, 4t-2)$

4. Veamos que sigue siendo cierto para $t = k+2$.

(a) Por hipótesis de inducción se tiene que haciendo

$$F_{4(k+2)-4} - (\sum_{r=0}^{\lfloor k/2 \rfloor - 1} F_{3+8r} + F_{4+8r}),$$

el -1 de la posición $(4(k+2)-4, 3)$, pasa a la posición $(4(k+2)-4, 4k-1)$. Si además, a la fila $F_{4(k+2)-4}$ le restamos las filas F_{3+8r} y F_{4+8r}, con $r = \lfloor k/2 \rfloor$, el -1 de la posición $(4(k+2)-4, 4k-1)$ se movería de la siguiente forma:

$$(4(k+2)-4, 4k-1) \to (4(k+2)-4, 4k-1+7) \to (4(k+2)-4, 4k-1+7+1) =$$
$$= (4t-4, 4t-1).$$

(b) Por otra parte, se tiene por hipótesis de inducción que haciendo

$$F_{4(k+2)-3} - (\sum_{r=0}^{\lfloor k/2 \rfloor - 1} F_{2+8r} + F_{3+8r}),$$

el -1 de la posición $(4(k+2)-3, 2)$, pasa a la posición $(4(k+2)-3, 4k-2)$. Si además, a la fila $F_{4(k+2)-2}$ le restamos las filas F_{2+8r} y F_{3+8r}, con $r = \lfloor k/2 \rfloor$, el -1 de la posición $(4(k+2)-2, 4k-2)$ se movería de la siguiente forma:

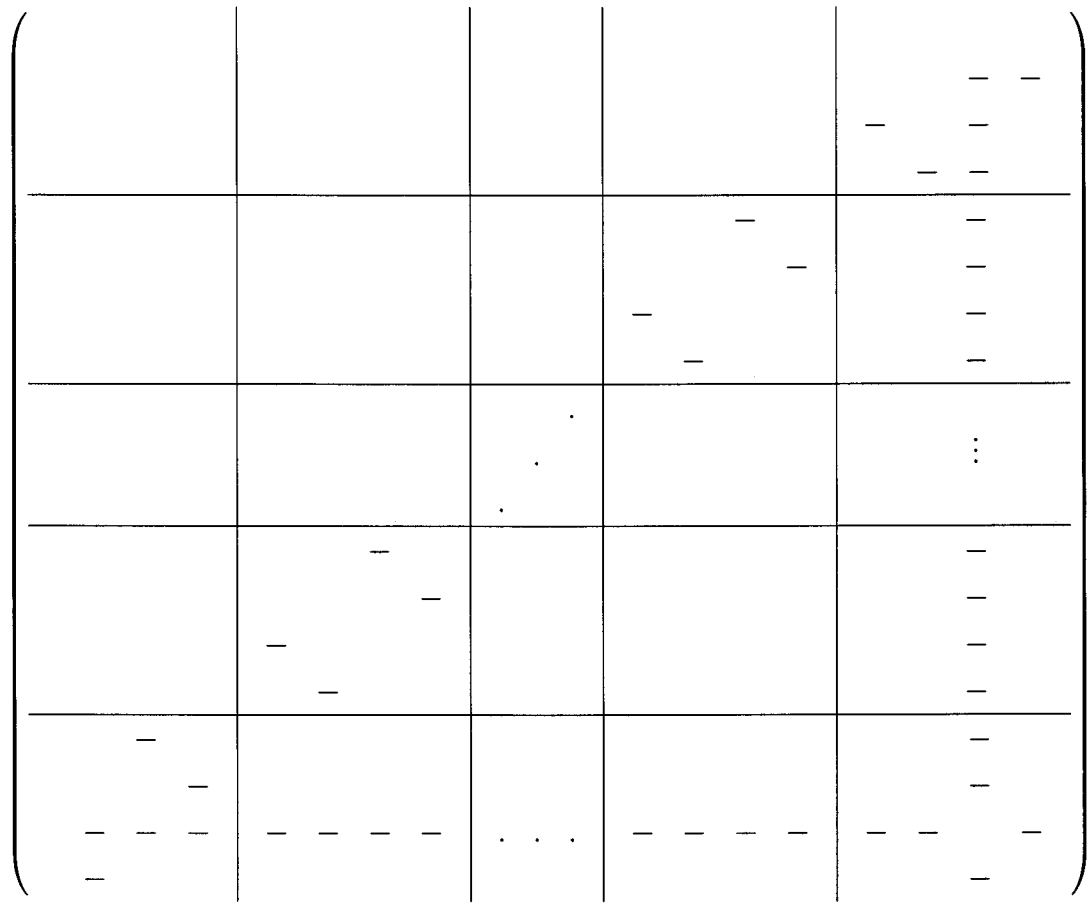
$$(4(k+2)-3, 4k-2) \to (4(k+2)-3, 4k-2+3) \to (4(k+2)-2, 4k-2+3+5) =$$
$$= (4t-2, 4t-2).$$

Por tanto, podemos concluir que, efectivamente, con la sucesión de transformaciones elementales indicada se obtiene una matriz cuya diagonal principal es toda de menos unos y por debajo de dicha diagonal no hay ninguno. Por lo que la matriz considerada es de rango máximo, igual a $4t-3$.

De este modo se tiene que las matrices asociadas a los 2-cobordes $\alpha_2, \ldots, \alpha_{4t-2}$ son linealmente independientes.

Es más, se puede probar que las matrices asociadas a los 2-cobordes $\alpha_2, \ldots, \alpha_{4t-2}$ forman un sistema generador de 2-cobordes normalizados. Para ello, basta comprobar que las matrices asociadas a los 2-cobordes α_{4t-1} y α_{4t} son combinación lineal de las anteriores.

Considerando la forma que tienen las matrices asociadas a los 2-cobordes, se tiene que las entradas negativas del 2-coborde α_{4t-1} están dispuestas del siguiente modo:



Es decir, podemos considerar la matriz asociada al 2-coborde $4t-1$ como una matriz por bloques 4×4, de la siguiente forma:

$$\left(\begin{array}{c|c|c|c|c|c|c} & & & & & & I \\ \hline & & & & & II & VI \\ \hline & & & & II & & VI \\ \hline & & & / & & & \vdots \\ \hline & & II & & & & VI \\ \hline & II & & & & & VI \\ \hline III & IV & IV & IV & IV & IV & V \end{array}\right) \tag{3.17}$$

Es fácil comprobar que para $t = 3$ el 2-coborde $\alpha_{4t-1} = \alpha_{11}$ se puede obtener a partir del producto Hadamard siguiente:

$$\alpha_{11} = \alpha_2\alpha_3\alpha_6\alpha_7\alpha_{10}.$$

Del mismo modo, para $t = 5$ el 2-coborde $\alpha_{4t-1} = \alpha_{19}$ se puede obtener a partir de:

$$\alpha_{19} = \alpha_2\alpha_3\alpha_6\alpha_7\alpha_{10}\alpha_{11}\alpha_{14}\alpha_{15}\alpha_{18}$$

Si tratamos de generalizar estos resultados, se tendría que:

$$\alpha_{4t-1} = (\prod_{r=0}^{t-2} \alpha_{2+4r}\alpha_{3+4r})\alpha_{4t-2}.$$

Veamos que esta generalización es adecuada.

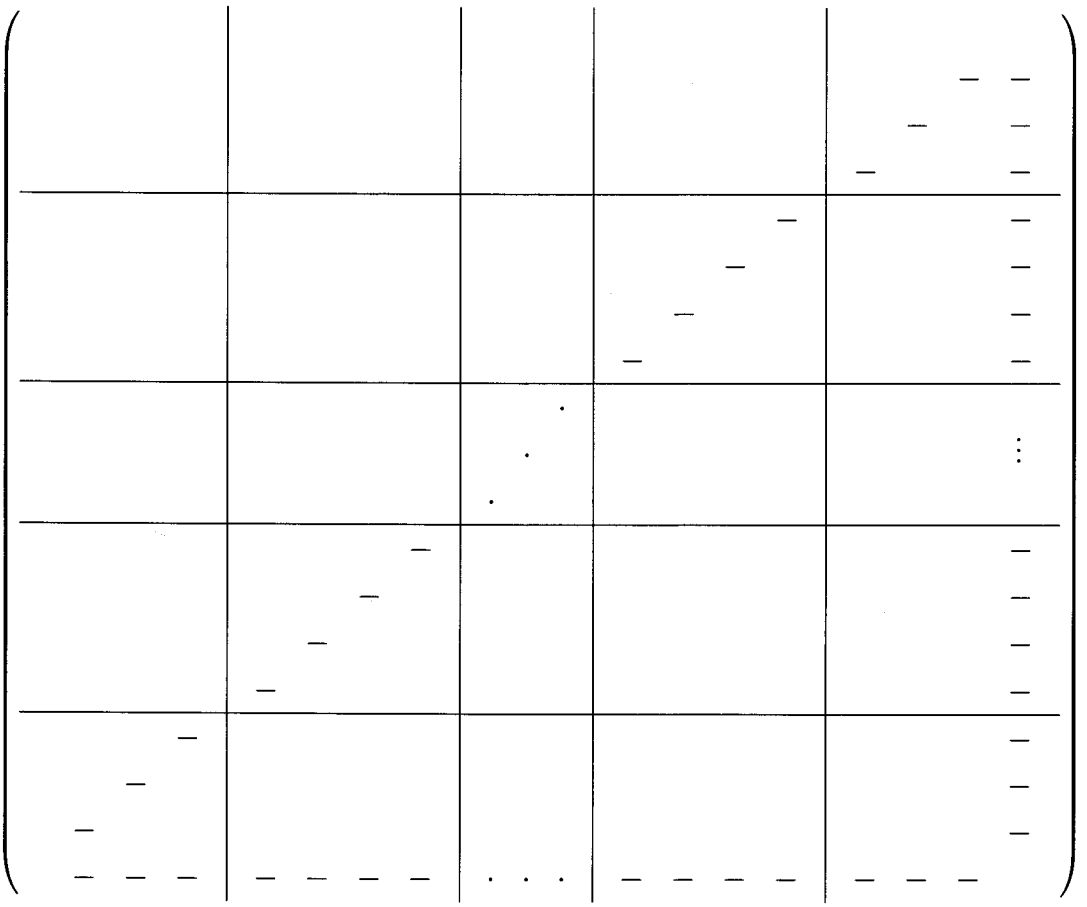
Para cualquier valor de r, comprendido entre 0 y $t-2$, al multiplicar los 2-cobordes α_{2+4r} y α_{3+4r} estamos multiplicando determinados bloques de la matriz por bloques de la forma (3.12) y (3.13), respectivamente. De hecho, considerando que los 2-cobordes α_i son de la forma indicada en (3.8-3.11), al recorrer todos los posibles valores de r para un t dado, todos los bloques salvo los de la diagonal secundaria se ven afectados de igual modo. Además, las filas y columnas $2+4r$ y $3+4r$ quedan multiplicadas por -1, salvo en la primera posición y en las posiciones $(2+4r, 2+4r)$ y $(3+4r, 3+4r)$ respectivamente. Esto hace que en la matriz resultante aparezcan los bloques que no contienen entradas negativas indicados en (3.17). En la última fila y la última columna de bloques la única diferencia (exceptuando a los de la diagonal secundaria)

es que sólo se ve multiplicada por menos uno la fila/columna $4t-2$, como consecuencia de la multiplicación por el 2-coborde α_{4t-2}. Esto da lugar a los bloques IV, V y VI de la matriz (3.17).

Las entradas negativas de los bloques de la diagonal secundaria se obtienen como consecuencia de la actuación del 2-coborde $4t-2$, que en cada uno de dichos bloques introduce las entradas negativas correspondientes a los bloques de la forma (3.12). En los bloques situados en los extremos de esta diagonal, el 2-coborde $4t-2$ además actúa multiplicando la fila y columna $4t-2$ por -1, salvo en la posición primera y en la $(4t-2, 4t-2)$. En el resto de los bloques de dicha diagonal se produce la negación de las filas y columnas $2+4r$ y $3+4r$, con $0 \leq r \leq t-2$ como consecuencia de la actuación del resto de los 2-cobordes. Esto da lugar a los bloques I, II y III de la matriz (3.17).

Luego, efectivamente, el 2-coborde $4t-1$ se puede obtener mediante la combinación lineal dada anteriormente. Hagamos un estudio análogo para comprobar que el 2-coborde $4t$ también es combinación lineal de $\alpha_2, \ldots, \alpha_{4t-2}$.

Teniendo en cuenta (3.11) y (3.15), las entradas negativas del 2-coborde α_{4t} están dispuestas del siguiente modo:



Es decir, podemos considerar la matriz asociada al 2-coborde $4t$ como una matriz por bloques 4×4, de la siguiente forma:

$$\left(\begin{array}{c|c|c|c|c|c|c} & & & & & & I \\ \hline & & & & & II & VI \\ \hline & & & & II & & VI \\ \hline & & & / & & & \vdots \\ \hline & & II & & & & VI \\ \hline & II & & & & & VI \\ \hline III & IV & IV & IV & IV & IV & V \end{array}\right) \tag{3.18}$$

Se puede comprobar fácilmente que para $t = 3$ el 2-coborde $\alpha_{4t} = \alpha_{12}$ se obtener a partir del producto Hadamard siguiente:

$$\alpha_{12} = \alpha_2\alpha_4\alpha_6\alpha_8\alpha_{10}.$$

Del mismo modo, para $t = 5$ el 2-coborde $\alpha_{4t} = \alpha_{20}$ se puede obtener a partir de:

$$\alpha_{20} = \alpha_2\alpha_4\alpha_6\alpha_8\alpha_{10}\alpha_{12}\alpha_{14}\alpha_{16}\alpha_{18}$$

Si tratamos de generalizar estos resultados, se tendría que:

$$\alpha_{4t} = (\prod_{r=0}^{t-2} \alpha_{2+4r}\alpha_{4(1+r)})\alpha_{4t-2}.$$

Veamos que esta generalización es correcta.

Considerando que los 2-cobordes α_i son de la forma dada en (3.8-3.11), al multiplicar los 2-cobordes α_{2+4r} y $\alpha_{4(1+r)}$ para todos los posibles valores de r, comprendidos entre 0 y $t-2$, para un t dado, todos los bloques, salvo los de la diagonal secundaria, se ven afectados del siguiente modo: estamos multiplicando determinados bloques de la matriz por bloques de la forma (3.12) y (3.14) respectivamente. Además, las filas y columnas $2+4r$ y $4(1+r)$ quedan multiplicadas por -1, salvo en la primera posición y en las posiciones $(2+4r, 2+4r)$ y $(4(1+r), 4(1+r))$ respectivamente. Esto hace que en la matriz resultante de dicho producto aparezcan los bloques que no contienen entradas negativas indicados en (3.18). En la última fila y la última columna de bloques la única diferencia (exceptuando a los de la diagonal secundaria) es que sólo se ve multiplicada por menos uno la fila/columna $4t-2$, como consecuencia de la multiplicación por el 2-coborde α_{4t-2}. Esto da lugar a los bloques IV, V y VI de la matriz (3.18).

Las entradas negativas de los bloques de la diagonal secundaria se obtienen como consecuencia de la actuación del 2-coborde $4t-2$, que en cada uno de dichos bloques introduce las entradas negativas correspondientes a los bloques de la forma (3.12). En los bloques situados en los extremos de esta diagonal, el 2-coborde $4t-2$ además actúa multiplicando la fila y columna $4t-2$ por -1, salvo en la posición primera y en la $(4t-2, 4t-2)$; en el resto de los bloques de dicha diagonal se produce la negación de las filas y columnas $2+4r$ y $4(1+r)$, con $0 \leq r \leq t-2$, como consecuencia de la actuación del resto de los 2-cobordes. Esto da lugar a los bloques I, II y III de la matriz (3.18).

Luego, efectivamente, el 2-coborde $4t$ se puede obtener mediante la combinación lineal dada anteriormente. Y, por consiguiente, los 2-cobordes $\alpha_2, \ldots, \alpha_{4t-2}$ forman un sistema generador.

Proposición 3.3.1 *Los 2-cobordes* $\alpha_2, \ldots, \alpha_{4t-2}$ *constituyen una base de los 2-cobordes normalizados de* $\mathbb{Z}_t \times \mathbb{Z}_2^2$.

Como consecuencia, podemos dar una base de los 2-cociclos normalizados.

Corolario 3.3.2 *Una base de los 2-cociclos normalizados de* $\mathbb{Z}_t \times \mathbb{Z}_2^2$ *viene dada por el conjunto* $\{\alpha_2, \ldots, \alpha_{4t-2}, \beta_1, \beta_2, \gamma\}$.

Así, cualquier matriz normalizada asociada a un 2-cociclo sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$ se puede escribir como el producto Hadamard siguiente:

$$\prod_{i=2}^{4t-2} \alpha_i^{r_i} \beta_1^{b_1} \beta_2^{b_2} \gamma^r, \tag{3.19}$$

para $r_i, b_j, r \in \{0, 1\}$.

Matrices cocíclicas de Hadamard

Una vez que conocemos una base de 2-cociclos normalizados de $\mathbb{Z}_t \times \mathbb{Z}_2^2$, la búsqueda de matrices cocíclicas de Hadamard sobre dicho grupo se reduce a encontrar de entre todas las matrices cocíclicas normalizadas que se pueden generar a partir de la base dada mediante el producto Hadamard de los generadores, las matrices que verifican el test de Hadamard cuadrático. Es decir, se trata de encontrar aquellas matrices cocíclicas normalizadas cuyas filas están constituidas por tantas entradas positivas como negativas, exceptuando la primera fila, ya que por tratarse de matrices normalizadas, sólo consta de entradas positivas.

Definición 3.3.3 La fila k-ésima, con $2 \leq k \leq 4t$, de una matriz cocíclica normalizada *está en posición Hadamard* si tiene tantas entradas positivas como negativas.

Nos será de utilidad analizar cuándo una matriz cocíclica normalizada dada tiene alguna de sus filas en posición Hadamard, ya que esto permitirá extraer información acerca de cómo han de combinarse las matrices de la base de 2-cociclos que conocemos para obtener matrices cocíclicas de Hadamard.

Si consideramos los generadores de los 2-cociclos según la ordenación anterior

$$\alpha_2, \cdots, \alpha_{4t-2}, \beta_1, \beta_2, \gamma,$$

podemos introducir el concepto de configuración.

Definición 3.3.4 Una *configuración* es una lista binaria de longitud $4t$, tal que, si la entrada i-ésima de la lista es un 1, el generador i-ésimo interviene en la generación de la matriz cocíclica normalizada asociada a dicha configuración.

Es decir, podemos identificar cada matriz cocíclica normalizada por una lista de $4t$ entradas de la forma $(r_2, \ldots, r_{4t-2}, b_1, b_2, r)$, en lugar de por el producto dado en (3.19), de manera que si en una posición aparece un cero, el 2-cociclo correspondiente de la base no interviene en la generación de la matriz cocíclica resultante; mientras que si aparece un 1 en una posición, el generador correspondiente sí interviene. Es decir, los 2-cociclos correspondientes a las posiciones en las que aparece un 1 se multiplican entre sí, mediante el producto Hadamard, para dar lugar a una matriz cocíclica normalizada nueva, combinación lineal de los generadores de la base.

Cuando buscamos de forma experimental, con ayuda del ordenador, las matrices cocíclicas de Hadamard para los primeros valores de t (impar), se puede observar que todas las matrices de Hadamard así obtenidas resultan del producto de unas ciertas matrices de la base de 2-cobordes por $\beta_1\beta_2\gamma$. De hecho, Horadam y Baliga, en su artículo conjunto, demuestran que para algunos valores de t es imposible encontrar matrices cocíclicas de Hadamard sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$ que no sean de este tipo. Es más, conjeturan que no existen matrices cocíclicas de Hadamard fuera de la clase de cohomología que determina $\beta_1\beta_2\gamma$.

Es por esto, que nuestra búsqueda de matrices cocíclicas de Hadamard sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$ se puede reducir a aplicar el test de Hadamard a matrices cocíclicas obtenidas a partir del producto $\beta_1\beta_2\gamma$ por matrices asociadas a los 2-cobordes.

La matriz $\beta_1\beta_2\gamma$ es una matriz constituida por $t \times t$ bloques de orden 4×4 cada uno:

$$\beta_1\beta_2\gamma = \begin{pmatrix} A & A & \cdots & A \\ A & A & \cdots & A \\ \vdots & \vdots & & \vdots \\ A & A & \cdots & A \end{pmatrix}$$

donde cada bloque A es de la forma:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix}$$

Queda claro que la matriz cocíclica $\beta_1\beta_2\gamma$ no es de Hadamard, puesto que las filas que ocupan las posiciones 1 (mod 4) están formadas sólo por unos y sabemos por el test de Hadamard reducido que una matriz cocíclica es de Hadamard si y sólo si todas sus filas, salvo la primera, tiene tantos unos como menos unos. Por tanto, para que se trate de una matriz de Hadamard, habrá que añadir $2t$ menos unos en dichas filas y que el resto de filas mantengan el número de unos y menos unos.

En lugar de trabajar con las matrices de los 2-cobordes normalizados, utilizaremos unas matrices asociadas a estas: los 2-cobordes generalizados.

Definición 3.3.5 El *2-coborde generalizado* i-ésimo se define como la matriz del 2-coborde normalizado i-ésimo con la fila i-ésima multiplicada por menos uno.

Por tanto, el 2-coborde generalizado i-ésimo es exactamente igual que el 2-coborde i-ésimo, salvo que la fila i-ésima es toda de unos excepto en las posiciones $(1,i),(i,i)$, en las que se encuentran sendas entradas negativas. Estos 2-cobordes generalizados no son realmente 2-cobordes, sin embargo, la búsqueda de matrices de Hadamard a partir de estas nuevas matrices es completamente análoga, ya que el test de Hadamard cuadrático seguirá siendo válido. Esto es así porque al generar distintas matrices como producto Hadamard de los 2-cobordes generalizados y los 2-cociclos β_1, β_2, γ, la única diferencia que se origina con respecto a la utilización de los 2-cobordes propios asociados, es que algunas filas quedarán multiplicadas por -1; de modo que la matriz que se obtiene a partir de 2-cobordes propios es de Hadamard si y sólo si la que se obtiene con los 2-cobordes generalizados también, como consecuencia de que multiplicar filas por -1 son transformaciones que preservan equivalencia Hadamard.

Por tanto, a partir de ahora y por comodidad utilizaremos los 2-cobordes generalizados, en lugar de los 2-cobordes propios, y denotaremos $\bar{\alpha}_i$ al 2-coborde generalizado i-ésimo, asociado a α_i.

Veamos a continuación algunos resultados que hemos encontrado a raíz del estudio de la base de los 2-cociclos generalizados y que permitirán extraer conclusiones acerca de cómo ha de ser una configuración para que dé lugar a una matriz cocíclica de Hadamard. Para ello nos centraremos principalmente en cómo se modifican las filas de unos de la matriz producto de $\beta_1\beta_2\gamma$ (filas 1 (mod 4)) cuando actúan distintos 2-cobordes, ya que aunque son las más sencillas de estudiar, de hecho aportan información interesante al respecto.

Antes de esto, introducimos algunos conceptos de los que haremos uso en repetidas ocasiones a lo largo de este capítulo.

Definición 3.3.6 Dos 2-cobordes generalizados *están relacionados*, respecto de una fila, cuando tienen alguna entrada negativa en la misma posición dentro de esa fila. La relación será simple cuando sólo tengan en común una entrada negativa; será doble, cuando tengan en común dos entradas negativas en la fila considerada. En este caso las filas consideradas de ambos 2-cobordes generalizados son idénticas, puesto que cada fila tiene dos entradas negativas.

Definición 3.3.7 Dados dos 2-cobordes generalizados $\bar{\alpha}_i$, $\bar{\alpha}_j$ diremos que *son del mismo tipo* cuando $i \equiv j \pmod 4$, es decir, cuando tiene sus entradas negativas en las mismas posiciones dentro de cada bloque, aunque estos bloques estén distribuidos de distinta forma dentro de la matriz.

En caso contrario se dirá que los 2-cobordes generalizados *son de distinto tipo.*

Proposición 3.3.8 *Dos 2-cobordes generalizados del mismo tipo están relacionados simplemente en dos filas o doblemente en una fila; es decir, dos 2-cobordes generalizados del mismo tipo se cancelan mutuamente una entrada negativa en dos filas determinadas (distintas según la pareja de 2-cobordes que se considere) o se cancelan mutuamente dos entradas negativas en una misma fila.*

Demostración.

Consideremos dos 2-cobordes generalizados del mismo tipo, $\bar{\alpha}_i, \bar{\alpha}_j$.

Cada uno de estos 2-cobordes, además de la columna i-ésima (resp. j-ésima) de entrada negativas, salvo en la primera posición, tiene otra entrada negativa en cada fila distinta de la primera y en cada columna distribuidas según los bloques dados en (3.8-3.15).

Los bloques en los que se encuentran las entradas negativas de sendos 2-cobordes están situados en distintas posiciones por tratarse de 2-cobordes congruentes módulo 4, como se vio en (3.8-3.11). Por tanto, las entradas negativas de los bloques de ambas matrices no pueden coincidir.

Como el 2-coborde $\bar{\alpha}_i$ ($i \equiv j \pmod 4$) posee toda la columna i-ésima de entradas negativas, salvo en la posición $(1, i)$, mientras que el 2-coborde $\bar{\alpha}_j$ posee una entrada negativa en cada fila/columna, situada en uno de los bloques indicados anteriormente; necesariamente ha de coincidir en alguna fila un -1 de la columna i-ésima de $\bar{\alpha}_i$, con un -1 del 2-coborde $\bar{\alpha}_j$.

De forma análoga ocurre si consideramos la fila j-ésima de $\bar{\alpha}_j$ y las entradas negativas de $\bar{\alpha}_i$.

Por tanto, en dichas filas ambos 2-cobordes generalizados están relacionados.

■

Si nos centramos en el estudio de las filas 1 (*mod* 4) que son las que en la matriz $\beta_1\beta_2\gamma$ están constituidas exclusivamente por entradas positivas, obtenemos el siguiente resultado.

Proposición 3.3.9 *Una pareja de 2-cobordes generalizados del mismo tipo $\bar{\alpha}_i, \bar{\alpha}_j$ están relacionados simplemente en las filas $(i - j + 1)$ $(mod\ 4t)$.*

Demostración.

Si nos fijamos en las entradas negativas del 2-coborde $\bar{\alpha}_i$ distribuidas según (3.8-3.15), se tiene que en las filas 1 (*mod* 4) se encuentran en las posiciones:

$$(i, 1), (5, i - 4\ (mod\ 4t)), (9, i - 8\ (mod\ 4t)), \ldots, (4t - 3, i - (4(t - 1)\ (mod\ 4t));$$

es decir, que están en las posiciones $(4(r-1)+1, i-4(r-1)\ (mod\ 4t))$, con $1 \leq r \leq t-1$.

Según veíamos anteriormente sólo pueden coincidir entradas negativas de un 2-coborde generalizado situadas en los bloques (3.12-3.15) con las entradas negativas de la columna negada de otro 2-coborde generalizado. Por tanto, las entradas negativas indicadas del 2-coborde $\bar{\alpha}_i$ sólo podrán coincidir con las de la columna j-ésima de $\bar{\alpha}_j$.

Para que coincidan las entradas negativas de ambos en la fila $(4(r-1)+1$, con $1 \leq r \leq t-1$, se ha de cumplir lo siguiente:

$$i - 4(r-1) \ (mod\ 4t) = j \ \Leftrightarrow \ r - 1 = \frac{i-j}{4} \ (mod\ 4t).$$

Es decir, coinciden en las filas:

$$4(r-1)+1 = (i-j+1) \ (mod\ 4t);$$

que, en realidad, son dos filas distintas: la $(i-j+1)$ $(mod\ 4t)$ y la $(j-i+1)$ $(mod\ 4t)$; puesto que la ecuación $(i-j+1 = j-i+1)$ $(mod\ 4t)$ sólo tiene como soluciones $i = j$ ó $i = j+2t$, pero ninguna de ellas es admisible, pues por una parte estamos considerando 2-cobordes distintos, por lo que $i \neq j$; y, por otra parte, estamos considerando en todo momento que t es impar y, además, i, j deben ser congruentes módulo 4 (por ser del mismo tipo), por lo que i necesariamente ha de ser distinto de $j + 2t$.

■

Proposición 3.3.10 *Dos 2-cobordes generalizados de distinto tipo, no están relacionados en las filas $k \equiv 1$ $(mod\ 4t)$.*

Demostración.

Dados dos 2-cobordes generalizados de distinto tipo, $\bar{\alpha}_i, \bar{\alpha}_j$, los bloques de entradas negativas de ambos 2-cobordes pueden estar situados en las mismas posiciones o no. En el supuesto de que los bloques tengan la misma disposición, las entradas negativas dentro de cada uno de ellos ocupan distintas posiciones (por tratarse de 2-cobordes de distinto tipo), por lo que dichas entradas negativas no pueden cancelarse entre sí. En el caso en que los bloques de entradas negativas estén situados en distintos sitios para ambos 2-cobordes, es obvio que tampoco pueden anularse (esto es un resultado genérico que ocurre en todas las filas, no sólo en las $k \equiv 1(\ mod\ 4t)$).

En particular, en las filas $k \equiv 1$ $(mod\ 4t)$, el 2-coborde $\bar{\alpha}_i$ tiene una entrada negativa en la posición s, con $i \equiv s$ $(mod\ 4t)$, mientras que el 2-coborde $\bar{\alpha}_j$ tiene la columna

j-ésima negada (salvo en la primera posición). Por ser $\bar{\alpha}_i$ y $\bar{\alpha}_j$ de distinto tipo, i y j no son congruentes modulo 4, resultando que $j \not\equiv s \ (mod\ 4t)$. Análogamente ocurre al considerar la columna i-ésima del 2-coborde $\bar{\alpha}_i$ y las entradas negativas del 2-coborde $\bar{\alpha}_j$. De donde se concluye la tesis de este resultado.

■

Corolario 3.3.11 *Los 2-cobordes generalizados de distinto tipo suman dos entradas negativa en cada fila de unos de la matriz $\beta_1\beta_2\gamma$.*

Corolario 3.3.12 *Dos 2-cobordes generalizados de distinto tipo, a lo más pueden estar relacionados simplemente en alguna fila, es decir, no pueden estar relacionados doblemente en ninguna fila.*

Demostración.

Como veíamos en la demostración de (3.3.10) las entradas negativas de dichos 2-cobordes generalizados distribuidas en los bloques no pueden coincidir en ninguna fila, por lo que a lo más puede coincidir la entrada negativa situada en un bloque de uno de los 2-cobordes con la entrada negativa de la columna negada del otro 2-coborde en algunas filas.

■

Corolario 3.3.13 *En una misma fila se cancelan tantas entradas negativas como parejas de 2-cobordes congruentes módulo 4 hay que disten lo mismo.*

Si denotamos por m_i al número de 2-cobordes del tipo i, con $0 \leq i \leq 3$, podemos encontrar una relación entre el número de 2-cobordes de cada tipo que puede tener una configuración para dar lugar a una matriz de Hadamard, para un t dado.

Proposición 3.3.14 *Una configuración en la que intervienen, además de las matrices $\beta_1\beta_2\gamma$, m_i 2-cobordes generalizados del tipo i, con $0 \leq i \leq 3$, es necesario que verifique la siguiente relación para generar una matriz de Hadamard de orden $4t$:*

$$2(m_0 + m_1 + m_2 + m_3)t - \sum_{i=0}^{3} m_i - \sum_{i=0}^{3} m_i^2 = 2t(t-1).$$

Demostración.

En la matriz $\beta_1\beta_2\gamma$ hay $t-1$ filas de unos. Para tener una matriz de Hadamard, en cada fila debe haber $2t$ entradas negativas. Por tanto, el número de entradas negativas en todas estas filas será $2t(t-1)$.

Por otra parte, si multiplicamos la matriz $\beta_1\beta_2\gamma$ por m_i 2-cobordes generalizados de cada tipo (con $0 \leq i \leq 3$), para calcular el número de entradas negativas en todas estas filas habrá que tener en cuenta:

1. Cada 2-coborde introduce un menos uno en cada fila como consecuencia de las entradas negativas dispuestas en los bloques y como estamos considerando las $t-1$ filas de unos, el resultado es que se añaden en estas filas un total de $(m_0+m_1+m_2+m_3)(t-1)$ entradas negativas.

2. Si actúan m_i 2-cobordes generalizados del tipo i, se habrán negado m_i columnas en la matriz producto, de manera que donde aparecía una entrada negativa ahora hay una positiva y viceversa. Como cada 2-coborde del tipo m_i proporciona un bloque que posee una entrada negativa en una de las columnas que se van a negar (y nunca se solapan entre sí), inicialmente había m_i entradas negativas en cada una de estas m_i columnas. Al negar las columnas, como hay t filas de unos inicialmente, quedan $t-m_i$ entradas negativas en dichas filas en cada una de las m_i columnas. Por tanto, habrá $(t-m_i)m_i$ entradas negativas en las t filas como consecuencia de las columnas negadas por la actuación de los 2-cobordes generalizados del tipo m_i. Esto ocurre para todo i, con $0 \leq i \leq 3$.

   En este razonamiento ha de tenerse en cuenta que la fila negada por la actuación de un 2-coborde del tipo m_i no puede anular ninguna entrada negativa que proceda de un 2-coborde de otro tipo.

Con todo esto, el número total de entradas negativas en estas t filas, será:

$$(m_0+m_1+m_2+m_3)(t-1)+(t-m_0)m_0+(t-m_1)m_1+(t-m_2)m_2+(t-m_3)m_3 =$$

$$= 2(m_0+m_1+m_2+m_3)t-\sum_{i=0}^{3} m_i-\sum_{i=0}^{3} m_i^2,$$

Igualando con el resultado anterior, se tiene:

$$2(m_0 + m_1 + m_2 + m_3)t - \sum_{i=0}^{3} m_i - \sum_{i=0}^{3} m_i^2 = 2t(t-1).$$

■

Proposición 3.3.15 *En una configuración, el número máximo de 2-cobordes del mismo tipo que disten*[2] *distinto puede ser a lo sumo*

$$m = \frac{1 \pm \sqrt{1 + 4(t-1)}}{2}$$

.

Demostración.

$$2(\frac{m(m-1)}{2}) \leq t - 1 \Rightarrow m^2 - m - t + 1 = 0 \Rightarrow$$

$$\Rightarrow m = \frac{1 \pm \sqrt{1 + 4(t-1)}}{2}.$$

■

Proposición 3.3.16 *Las 4 primeras filas de la matriz obtenida como producto de la matriz $\beta_1\beta_2\gamma$ por algún 2-coborde siempre están en posición Hadamard.*

Esto es porque siempre que actúa un 2-coborde generalizado multiplica cada una estas filas por -1 en dos posiciones, una cuya entrada es positiva y otra cuya entrada es negativa, por lo que sigue teniendo el mismo número de unos que de menos unos. Exceptuando, como siempre, la primera fila, cuyas entradas son todas positivas.

Otro resultado realmente interesante por la simplificación que supone en la búsqueda de matrices cocíclicas de Hadamard sobre estos grupos es el siguiente.

[2]Consideramos que la distancia entre dos 2-cobordes es la distancia de sus posiciones en la representación de la configuración en la que intervienen.

Teorema 3.3.17 *En una configuración en la que intervengan β_1, β_2 y γ el número de generadores que se ha de utilizar para obtener una matriz cocíclica de Hadamard oscilará entre un mínimo de $t+3$ y un máximo de $3t+2$ si $t \geq 5$. Para $t = 3$, el máximo es $4t = 12$.*

Demostración.

Comencemos demostrando que el número mínimo de generadores necesario para obtener una matriz cocíclica de Hadamard en una configuración en la que intervienen β_1, β_2 y γ es $t+3$.

Tal y como sabemos la matriz obtenida como el producto Hadamard de β_1, β_2 y γ tiene sus filas $k \equiv 1 \pmod 4$ de unos. Para transformar esta matriz en una matriz cocíclica de Hadamard será necesario multiplicar por determinadas matrices de la base de 2-cobordes generalizados de manera que todas las filas lleguen a tener $2t$ entradas negativas. En el supuesto más favorable en que ningún par de 2-cobordes generalizados utilizados estén relacionados entre sí en las filas $k \equiv 1 \pmod 4$, cada 2-coborde generalizado aportaría 2 entradas negativas, por lo que se necesitarían t generadores $\bar{\alpha}_i$ para que dichas filas estuviesen en posición Hadamard. Si de esta forma las restantes filas han mantenido el número de entradas positivas y negativas iguales, se tendría una matriz de Hadamard. Por tanto, el número mínimo de generadores en una configuración de este tipo es $t+3$: t generadores correspondientes a 2-cobordes y los tres restantes correspondientes a la parte simétrica y conmutadora.

Veamos ahora que el número máximo de generadores en una configuración en la que intervienen β_1, β_2 y γ para obtener una matriz cocíclica de Hadamard es $4t$ si $t = 3$ ó $3t+2$ si $t \geq 5$.

En primer lugar, comprobemos si es posible conseguir una matriz de Hadamard a partir de una configuración en la que aparecen todos los 2-cobordes generalizados de la base.

Según comentábamos más arriba, si intervienen sólo β_1, β_2 y γ, en las filas $k \equiv 1 \pmod 4$ todas las entradas son positivas. Si además, intervienen $\bar{\alpha}_2, \ldots, \bar{\alpha}_{4t-2}$, analicemos cómo se vería afectada una de estas filas. Para ello y simplemente por fijar ideas, analicemos qué ocurriría con la fila 5 (en el resto de filas $1 \pmod 4$ el comportamiento es análogo).

1. Teniendo en cuenta la forma que tienen los 2-cobordes generalizados, añaden en dicha fila $4t-3$ entradas negativas correspondientes a las posiciones indicadas según (3.8)-(3.15):

−	−	−	−	−	−	−	−	−	−	−	−	⋯	−	−	+	+	+	−	−	−

2. Como el 2-coborde $\bar{\alpha}_i$ introduce una entrada negativa en la posición i de cualquier fila (salvo la primera [3]) y teniendo en cuenta que estamos utilizando todos los 2-cobordes $\bar{\alpha}_i$, con $2 \leq i \leq 4t-2$, se estarían introduciendo las siguientes entradas negativas:

+	−	−	−	−	−	−	−	−	−	−	−	⋯	−	−	−	−	−	−	+	+

De manera que, teniendo en cuenta los -1 que se introducen de un modo u otro, las entradas negativas en esta fila quedarían en las posiciones:

−	+	+	+	+	+	+	+	+	+	+	+	⋯	+	+	−	−	−	+	−	−

Es decir, independientemente del valor de t, en cualquier fila 1 (mod 4) (salvo la primera) de una matriz obtenida como producto de todos los generadores de la base, existen 6 entradas negativas. Como consecuencia, en general, una matriz cocíclica de esta forma no será de Hadamard. De hecho, sólo podría serlo para $t=3$, pues en cualquier otro caso tendríamos que esta matriz no tiene el mismo número de entradas positivas y negativas en todas sus filas, pues, al menos en las filas 1 (mod 4) no ocurre así.

Es más, para $t=5$ tendríamos que dejar de lado al menos 2 generadores para tener el mismo número de entradas positivas que negativas en estas filas, pues en este caso cada fila 1 (mod 4) tiene 20 entradas y si actúan todos los demás generadores, 6 de ellas son negativas y el resto positivas. Para que esta filas estén en posición Hadamard se necesitan 4 entradas negativas más. Por cada generador que eliminemos, como mucho tendremos dos entradas negativas más. Luego, necesitamos eliminar 2 generadores como mínimo para tener una matriz cocíclica de Hadamard. Esto es, para $t=5$ el número máximo de generadores que intervienen en una configuración puede ser $4t-2=3t+3$.

[3] Estamos considerando que en la fila i-ésima las entradas negativas están sólo en las posiciones primera e i-ésima, pues consideramos la fila multiplicada por -1

Análogamente, para un t dado cada fila tiene $4t$ entradas, como partimos de que actúan todos los generadores, en principio se tienen sólo 6 entradas negativas, hasta $2t$, faltan $2t-6$, luego, habría que prescindir de $t-3$ generadores, por lo que podríamos tener una matriz cocíclica de Hadamard con una configuración en la que interviniesen a lo más $4t-(t-3)=3t+3$ generadores.

Por otra parte, si hacemos un estudio similar al anterior para todas las filas $1 \pmod 4$ (salvo la primera) de una matriz de orden t, se tiene:

- La fila F_5:

$-$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$\cdots$	$+$	$+$	$-$	$-$	$-$	$+$	$-$	$-$

$\vdots$

- La fila $F_{4(t-2)+1}$:

$-$	$+$	$+$	$+$	$+$	$+$	$-$	$-$	$-$	$+$	$+$	$+$	$\cdots$	$+$	$+$	$+$	$+$	$+$	$+$	$-$	$-$

- La fila $F_{4(t-1)+1}$:

$-$	$+$	$-$	$-$	$-$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$\cdots$	$+$	$+$	$+$	$+$	$+$	$+$	$-$	$-$

Podemos ver que si pretendemos prescindir de $(t-3)$ 2-cociclos generalizados para buscar una matriz cocíclica de Hadamard, deberíamos elegir los 2-cobordes generalizados a eliminar de manera que al quitar cada uno de ellos se sustituyesen dos entradas positivas por dos negativas en cada una de las filas. Para que esto ocurra, la única posibilidad es que los 2-cobordes eliminados sean elegidos de entre los siguientes: $\{\bar{\alpha}_2, \bar{\alpha}_6, \ldots, \bar{\alpha}_{4t-2}\}$. Ya que cada uno de estos 2-cobordes generalizados introducirían 2 entradas negativas donde inicialmente había entradas positivas en todas las filas consideradas. Sin embargo, todos estos 2-cobordes generalizados están relacionados simplemente en alguna de las filas consideradas (esto se puede comprobar viendo la forma de los 2-cobordes (3.8)-(3.11) y (3.12)). Por tanto, será necesario eliminar un 2-coborde más en la configuración, quedando que si $t \geq 5$, el número máximo de generadores será $3t+2$.

■

Como el número de configuraciones en las que intervienen n generadores además de β_1, β_2 y γ es $\binom{4t-3}{n}$ y teniendo en cuenta las cotas obtenidas para el número de generadores que intervienen en una configuración de este tipo, se puede reducir el número de matrices cocíclicas que hay que comprobar si son o no de Hadamard. Para un t dado ($t \geq 5$) se pasa de tener que estudiar $2^{4t-3} - 1$ configuraciones a tener que verifircar si son de Hadamard las configuraciones siguientes:

$$\binom{4t-3}{t} + \binom{4t-3}{t+1} + \cdots + \binom{4t-3}{3t-1}.$$

Teniendo en cuenta todos los resultados anteriormente descritos hemos podido calcular matrices cocíclicas de Hadamard para distintos valores de t. En la siguiente tabla damos algunas de las matrices cocíclicas de Hadamard obtenidas como el producto de los elementos de la base de 2-cociclos para algunos valores de t impar:

t	producto de generadores
3	$\alpha_4\alpha_8\alpha_9\alpha_{10}\beta_1\beta_2\gamma$
5	$\alpha_3\alpha_8\alpha_{12}\alpha_{15}\alpha_{17}\alpha_{18}\beta_1\beta_2\gamma$
7	$\alpha_3\alpha_8\alpha_9\alpha_{11}\alpha_{12}\alpha_{13}\alpha_{15}\alpha_{16}\alpha_{20}\alpha_{23}\alpha_{25}\alpha_{26}\beta_1\beta_2\gamma$
9	$\alpha_3\alpha_8\alpha_9\alpha_{11}\alpha_{12}\alpha_{14}\alpha_{15}\alpha_{16}\alpha_{18}\alpha_{19}\alpha_{20}\alpha_{21}\alpha_{23}\alpha_{24}\alpha_{28}\alpha_{31}\alpha_{33}\alpha_{34}\beta_1\beta_2\gamma$
11	$\alpha_2\alpha_3\alpha_4\alpha_5\alpha_7\alpha_8\alpha_9\alpha_{10}\alpha_{11}\alpha_{14}\alpha_{17}\alpha_{18}\alpha_{20}\alpha_{21}\alpha_{22}\alpha_{24}\alpha_{26}\alpha_{29}\alpha_{30}\alpha_{31}\alpha_{33}$ $\alpha_{35}\alpha_{36}\alpha_{38}\alpha_{39}\alpha_{40}\alpha_{41}\alpha_{44}\beta_1\beta_2\gamma$
13	$\alpha_2\alpha_3\alpha_4\alpha_5\alpha_7\alpha_8\alpha_{11}\alpha_{13}\alpha_{14}\alpha_{16}\alpha_{20}\alpha_{22}\alpha_{26}\alpha_{32}\alpha_{33}\alpha_{34}\alpha_{36}\alpha_{39}\alpha_{41}\alpha_{43}\alpha_{44}$ $\alpha_{46}\alpha_{47}\alpha_{48}\alpha_{50}\alpha_{54}\beta_1\beta_2\gamma$

3.3.2 Matrices cocíclicas de Hadamard sobre D_{4t}

Tal y como comentásemos en secciones anteriores, el diédrico es un grupo con un potencial prometedor a la hora de buscar matrices cocíclicas de Hadamard. Por una parte, porque no existe ninguna restricción conocida para que estos grupos puedan llegar a generar matrices de Hadamard en cualquier orden múltiplo de 4; de hecho, Horadam en [63] hace alusión a la cantidad de matrices cocíclicas de Hadamard que se pueden obtener con estos grupos para valores de t no muy elevados, en comparación

con los grupos $\mathbb{Z}_t \times \mathbb{Z}_2^2$. Por otra parte, el diédrico ha sido muy estudiado, por lo que su factorización en 2-cobordes, parte simétrica y conmutadora es bien conocida.

La búsqueda de matrices cocíclicas de Hadamard sobre

$$D_{4t} = \mathbb{Z}_{2t} \ltimes_{\chi} \mathbb{Z}_2 \quad (t \geq 1),$$

la vamos a enfocar del mismo modo que hicimos en el caso anterior con el grupo $\mathbb{Z}_t \times \mathbb{Z}_2^2$; nos basaremos en los resultados experimentales obtenidos a partir de la implementación presentada en el capítulo anterior, para emitir hipótesis y conjeturas que trataremos de consolidar en resultados teóricos.

Estudiaremos cómo son las matrices correspondientes a los generadores de los 2-cociclos asociados al grupo diédrico y daremos una base de los mismos. Con esta base se puede generar todas las matrices cocíclicas y, mediante el test de Hadamard cuadrático, determinar las matrices de Hadamard que se pueden generar en una dimensión dada.

El estudio de las matrices de Hadamard así obtenidas permite deducir algunas características que debe verificar una configuración para obtener una matriz de Hadamard.

Comencemos estudiando cómo son las matrices asociadas a los 2-cociclos. Esto nos permitirá dar una base de los tres tipos de 2-cociclos: 2-cobordes, simétricos (inflación) y asociados a la parte conmutadora (transgresión). Experimentalmente obtenemos que una representación matricial de cada uno de ellos viene dada por:

- Respecto a los 2-cociclos simétricos, en el caso que nos atañe, siempre se obtienen únicamente dos generadores. Las matrices asociadas a ellos y que denotaremos por β_1 y β_2, son de la forma:

$$\beta_1 = I_{2t} \otimes \begin{pmatrix} + & + \\ + & - \end{pmatrix} = \left(\begin{array}{cc|c|cc} + & + & & + & + \\ + & - & \cdots & + & - \\ \hline \multicolumn{2}{c|}{\vdots} & & \multicolumn{2}{c}{\vdots} \\ \hline + & + & & + & + \\ + & - & \cdots & + & - \end{array}\right)_{4t \times 4t}$$

$$\beta_2 = \begin{pmatrix} + & + \\ + & - \end{pmatrix} \otimes I_{2t} = \left(\begin{array}{ccc|ccc} + & \overset{2t}{\cdots} & + & + & \overset{2t}{\cdots} & + \\ 2t\,\vdots & & \vdots & \vdots & & \vdots \\ + & \cdots & + & + & \cdots & + \\ \hline + & \cdots & + & - & \cdots & - \\ 2t\,\vdots & & \vdots & \vdots & & \vdots \\ + & \cdots & + & - & \cdots & - \end{array}\right)$$

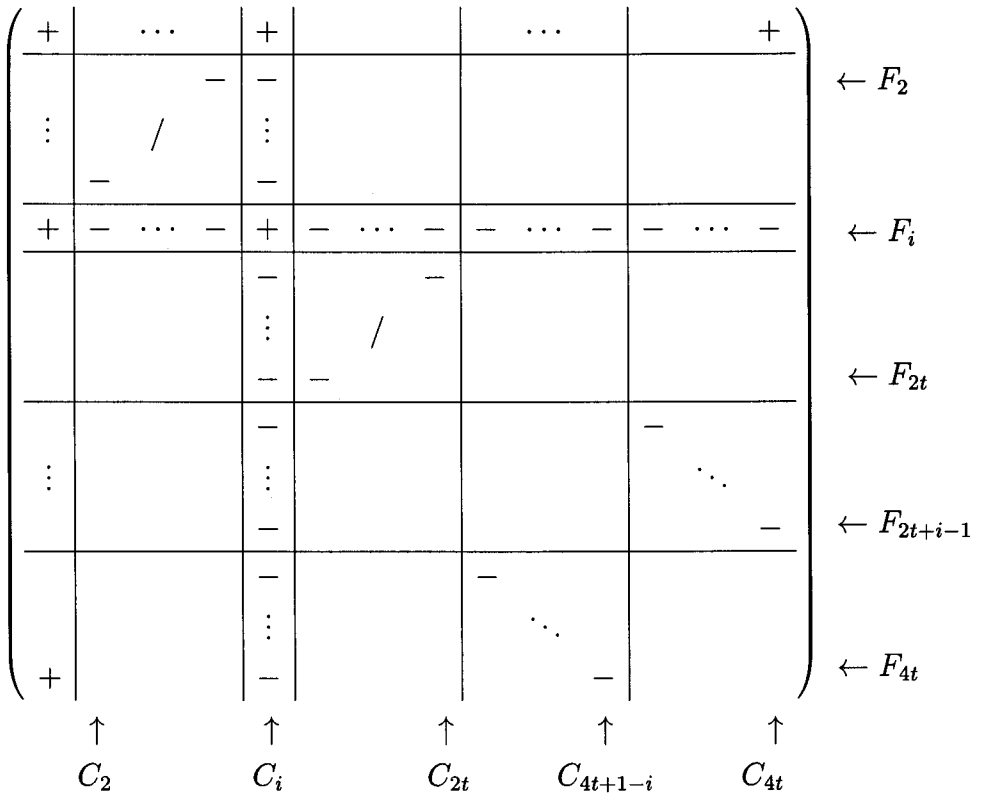
Como se puede observar, estas son las matrices (3.5) de Flannery.

- En cuanto a la parte conmutadora, da lugar a un único generador en cualquier dimensión, cuya representación matricial, que denotaremos por γ, es de la forma:

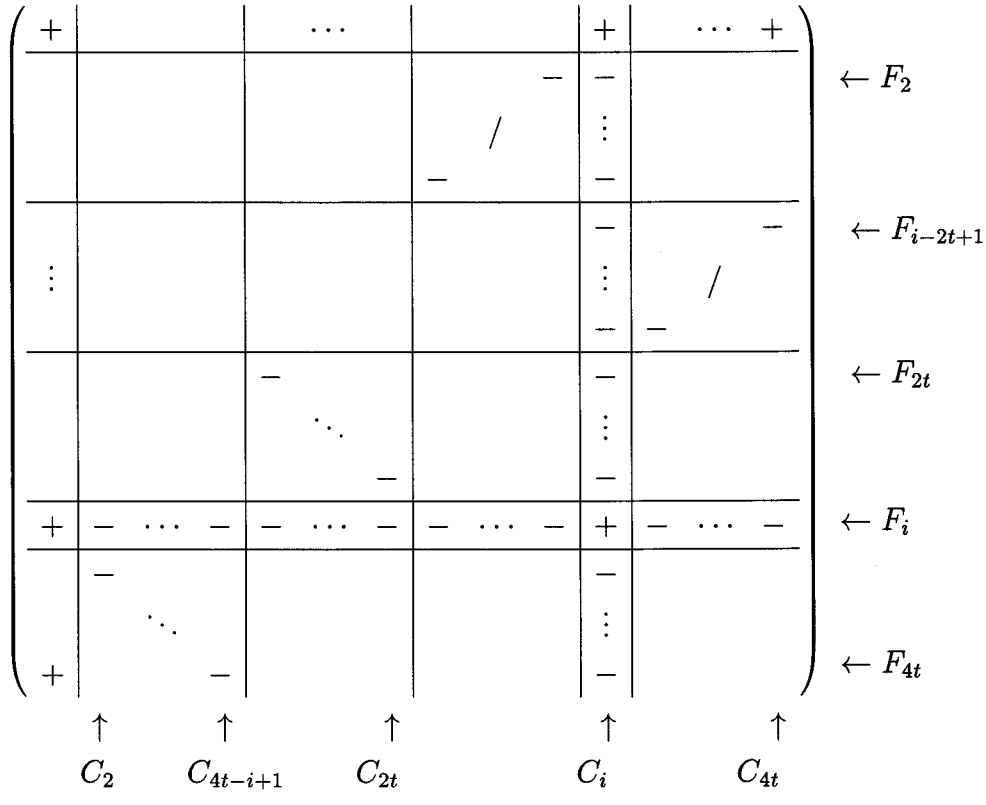
$$\gamma = \left(\begin{array}{c|ccc|c|ccc|c} + & + & \cdots & + & + & + & \cdots & + & + \\ \hline + & + & \cdots & - & + & + & \cdots & - & + \\ \vdots & & / & \vdots & & & / & \vdots & \vdots \\ + & - & \cdots & - & + & - & \cdots & - & + \\ \hline + & - & \cdots & - & + & - & \cdots & - & + \\ \vdots & & \ddots & \vdots & & & \ddots & \vdots & \vdots \\ + & + & \cdots & - & + & + & \cdots & - & + \\ \hline + & + & \cdots & + & + & + & \cdots & + & + \end{array}\right)$$

Esta matriz es la misma que la dada por Flannery en (3.6).

- Al igual que en el caso anterior, buscamos una base de las matrices asociadas a los 2-cobordes. Como demostraremos más adelante, para un valor de t genérico (impar) se obtiene que dicha base viene dada por $4t - 3$ matrices α_i. Experimentalmente obtenemos que estas matrices α_i, para $2 \leq i \leq 2t$, son de la forma:



Para $2t+1 \leq i \leq 4t-2$ se tiene la matriz



De modo que cada matriz correspondiente a un 2-coborde tiene en cada fila y columna dos entradas -1 y el resto son $+1$, salvo en las líneas i-ésimas, que tiene dos $+1$ y el resto son -1.

Así, las posiciones de las entradas negativas para el 2-coborde α_i quedan:

- En la fila k, con $2 \leq k \leq 2t$:
  - Para $2 \leq i \leq k-1$ las posiciones son $(k,i),(k,2t+i-k+1)$.
  - Para $i = k$ las posiciones son $(k,j)\ \forall j \neq 1,k$.
  - Para $k+1 \leq i \leq 2t$ las posiciones son $(k,i),(k,i-k+1)$.
  - Para $2t+1 \leq i \leq 2t+k-1$ las posiciones son $(k,i),(k,2t+i-k+1)$.
  - Para $2t+k \leq i \leq 4t-2$ las posiciones son $(k,i),(k,i-k+1)$.
- En la fila k, con $2t+1 \leq k \leq 4t$.
  - Para $2 \leq i \leq k-2t$ las posiciones son $(k,i),(k,k-i+1)$.
  - Para $k-2t+1 \leq i \leq 2t$ las posiciones son $(k,i),(k,2t-i+k+1)$.
  - Para $2t+1 \leq i \leq k-1$ las posiciones son $(k,i),(k,k-i+1)$.
  - Para $i = k$ las posiciones son $(k,j)\ \forall j \neq 1,k$.
  - Para $k+1 \leq i \leq 4t-2$ las posiciones son $(k,i),(k,2t-i+k+1)$.

Analíticamente se puede comprobar que las matrices asociadas a los 2-cobordes son de la forma indicada anteriormente. Para ello es necesario recordar que los 2-cobordes vienen dados por:

$$[\alpha_i]_{(a,b)} = \alpha_i(a) \cdot \alpha_i(b) \cdot \alpha_i^{-1}(ab),$$

siendo

$$\alpha_i(a) = \begin{cases} 1 & \text{si} \quad i \neq a \\ -1 & \text{si} \quad i = a \end{cases}$$

Teniendo en cuenta que en $\mathbb{F}_2$ el inverso de un elemento es él mismo, se puede decir que

$$[\alpha_i]_{(a,b)} = \alpha_i(a) \cdot \alpha_i(b) \cdot \alpha_i(ab).$$

Podemos tomar, por ejemplo, la siguiente ordenación de los elementos:

$$\mathbb{Z}_{2t} \ltimes \mathbb{Z}_2 = D_{4t} = \{(0,0),(1,0),\cdots,(2t-1,0),(0,1),(1,1),\cdots,(2t-1,1)\}.$$

Es necesario recordar que la acción correspondiente al producto semidirecto, χ, actúa del siguiente modo

$$(a,g)(a',g') = (a + (-1)^g \times a', g + g'),$$

donde, $g = 0, 1$.

Al actuar el 2-coborde $[\alpha_{(a,b)}]$ sobre el par $((a_0,g_0),(a_1,g_1))$ se tiene que

$$[\alpha_{(a,g)}]((a_0,g_0),(a_1,g_1)) = \alpha_{(a,g)}(a_0,g_0)\alpha_{(a,g)}(a_1,g_1)\alpha_{(a,g)}(a_0 + (-1)^{g_0}a_1, g_0 + g_1).$$

Si consideramos un 2-coborde distinto del primero, esto es, si $\alpha_{(a,g)} \neq \alpha_{(0,0)}$, analicemos cómo serán las distintas filas de la matriz asociada a dicho 2-coborde:

1. Si $(a_0,g_0) = (0,0)$, es decir, si nos remitimos a la primera fila de la matriz asociada al 2-coborde (a,g). En este caso se tiene que las entradas correspondientes a cada una de las columnas son

   $$[\alpha_{(a,g)}]((0,0),(a_1,g_1)) = \alpha_{(a,g)}(0,0)\alpha_{(a,g)}(a_1,g_1)\alpha_{(a,g)}(a_1,g_1) = 1 \cdot \alpha^2_{(a,g)}(a_1,g_1) = 1.$$

   Por tanto, en la primera fila del 2-coborde todas las entradas son $+1$.

2. Si consideramos la fila $(a_0,g_0) = (a,g)$, como $\alpha_{(a,g)}(a,g) = -1$, se tiene que

   $$[\alpha_{(a,g)}]((a,g),(a_1,g_1)) = -\alpha_{(a,g)}(a_1,g_1)\alpha_{(a,g)}(a + (-1)^g a_1, g + g_1).$$

   El factor $\alpha_{(a,g)}(a_1,g_1)$ será -1 siempre que $a_1 = a$ y $g_1 = g$. Cuando esto ocurre, el segundo factor queda

   $$\alpha_{(a,g)}(a + (-1)^g a_1, g + g_1) = \alpha_{(a,g)}(a + (-1)^g a, g + g),$$

   siendo -1 sólo si se verifica

   $$\begin{cases} g + g = g & \Rightarrow \quad g = 0 \\ a + (-1)^g a = a & \Rightarrow \quad a = 0. \end{cases}$$

   Sin embargo, esto es una contradicción, puesto que estábamos suponiendo que el 2-coborde considerado era distinto del $(0,0)$. Por tanto, si $\alpha_{(a,g)}(a_1,g_1) = -1$, entonces, necesariamente

   $$\alpha_{(a,g)}(a + (-1)^g a_1, g + g_1) = 1.$$

Luego, en este caso se tiene que

$$[\alpha_{(a,g)}]((a,g),(a,g)) = (-1)(-1)(+1) = 1,$$

es decir, en la matriz correspondiente al 2-coborde i-ésimo, la entrada (i,i) es positiva.

Por otra parte, el factor $\alpha_{(a,g)}(a+(-1)^g a_1, g+g_1)$ será -1 si

$$\left.\begin{array}{l} a = a+(-1)^g a_1 \\ g = g+g_1 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} g_1 = 0 \\ a_1 = 0 \end{array}\right.$$

En ese caso, como estamos suponiendo que $(a,g) \neq (0,0)$, resulta que

$$[\alpha_{(a,g)}]((a,g),(0,0)) = \alpha_{(a,g)}(a,g)\alpha_{(a,g)}(0,0)\alpha_{(a,g)}(a,g) = -1\cdot 1\cdot(-1) = 1.$$

Por tanto, el 2-coborde (a,g), en la entrada $((0,0),(a,g))$ tiene otro 1, esto es, la matriz correspondiente al 2-coborde i-ésimo tiene otra entrada positiva en la posición $(i,1)$. Cualquier otra entrada de la fila (a,g) de la matriz correspondiente al 2-coborde (a,g) será negativa, puesto que los dos factores $\alpha_{(a,g)}(a_1,g_1)$ y $\alpha_{(a,g)}(a+(-1)^g a_1, g+g_1)$ son positivos.

Como conclusión, se tiene que la fila i-ésima de la matriz asociada al i-ésimo 2-coborde tiene todas sus entradas negativas, salvo en las posiciones $(i,1)$ y (i,i), que son positivas.

3. Para cualquier otra fila (a_0,g_0), con $(a_0,g_0) \neq (0,0)$y $(a_0,g_0) \neq (a,g)$, se tiene

$$[\alpha_{(a,g)}]((a_0,g_0),(a_1,g_1)) = \alpha_{(a,g)}(a_0,g_0)\alpha_{(a,g)}(a_1,g_1)\alpha_{(a,g)}(a_0+(-1)^{g_0}a_1, g_0+g_1).$$

El primer factor, $\alpha_{(a,g)}(a_0,g_0)$, por ser $(a,g) \neq (a_0,g_0)$ es siempre igual a 1.

El segundo factor, $\alpha_{(a,g)}(a_1,g_1)$, valdrá -1 siempre que $a_1 = a$ y $g_1 = g$. Cuando esto ocurre el tercer factor vale 1, puesto que $(a_0,g_0) \neq (0,0)$. Es decir, para el 2-coborde i-ésimo, en la columna i-ésima todas las entradas son -1, salvo la primera y la i-ésima.

Si estudiamos cuándo es -1 el tercer factor, llegamos a la conclusión que esto ocurre si

$$\left\{\begin{array}{lcl} g_1+g_0 & = & g \\ a_0+(-1)^{g_0}a_1 & = & a \end{array}\right.$$

Al resolver este sistema se tiene que:

- Si $g_1 = g$ (y $a_1 \neq a$). En este caso g_0 ha de ser 0 (por tanto, $a_0 \neq 0$) y, además, $a_0 + a_1 = a$ (con $a_1 \neq a$). Las soluciones de este sistema, por tanto, son

2-coborde (a,g)	fila (a_0,g_0)	columna (a_1,g_1)	
$(a,0)$	$(a_0,0)$	$(a-a_0,0)$	con $a_0 \neq a$
$(a,1)$	$(a_0,0)$	$(a-a_0,1)$	

- Si $g_1 \neq g$. Las soluciones del sistema son

2-coborde (a,g)	fila (a_0,g_0)	columna (a_1,g_1)	
$(a,0)$	$(a_0,1)$	$(a-a_0,0)$	
$(a,1)$	$(a_0,1)$	$(a-a_0,1)$	con $a_0 \neq a$

En cualquiera de estos casos se ha de considerar que $a_0 \neq 0$ y tener en cuenta que $(a,g) \neq (0,0)$.

La conclusión que se obtiene de este análisis es que el 2-coborde i-ésimo tiene en cada fila, distintas de la primera y de la i-ésima, dos entradas iguales a -1 y el resto de entradas son iguales a 1.

El 2-coborde que aún no hemos analizado es el primero

$$[\alpha_{(0,0)}]((a_0,g_0),(a_1,g_1)) = \alpha_{(0,0)}(a_0,g_0)\alpha_{(0,0)}(a_1,g_1)\alpha_{(0,0)}(a_0+(-1)^{g_0}a_1, g_0+g_1),$$

Si estudiamos cómo son las entradas correspondientes a la primera fila y a la primera columna de la matriz de este 2-coborde se tiene que

- La primera fila corresponde a $(a_0,g_0) = (0,0)$, por tanto, sus entradas serán todas negativas:
$$-\alpha_{(0,0)}(a_1,g_1)\alpha_{(0,0)}(a_1,g_1) = -1$$
- La primera columna es la correspondiente a $(a_1,g_1) = (0,0)$, siendo todas sus entradas también negativas:
$$-\alpha_{(0,0)}(a_0,g_0)\alpha_{(0,0)}(a_0,g_0) = -1$$

Luego, el 2-coborde $[\alpha_{(0,0)}]$ es el único no normalizado (no tiene todas las entradas de la primera fila y columna positivas). Nosotros sólo estamos interesados en los 2-cobordes normalizados, por lo que podemos prescindir de éste.

Base de los 2-cobordes

Experimentalmente se puede ver que para cualquier valor de t una base de los 2-cobordes viene dada por $\{\alpha_2, \ldots, \alpha_{4t-2}\}$. Para demostrar este resultado vamos a construir una matriz $(4t-3) \times 4t$, de manera que la fila i-ésima venga dada por las entradas del 2-coborde i-ésimo (con $2 \leq i \leq 4t-2$). Atendiendo a las primeras $4t-1$ componentes relevantes de cada una de las filas de esta matriz, es decir, a las primeras $4t-1$ componentes relevantes de cada una de las matrices asociadas a los 2-cobordes $\alpha_2, \cdots, \alpha_{4t-2}$ (por tratarse de matrices normalizadas, estas componentes corresponden a la segunda fila de cada una de las matrices, salvo la primera entrada), se puede comprobar fácilmente que las filas de la submatriz así obtenida son linealmente independientes:

$$\begin{pmatrix} - & - & & & & & & \\ & - & - & & & & & \\ & & \ddots & \ddots & & & & \\ & & & - & & & - & \\ & & & & \ddots & \ddots & & \\ & & & & & & - & - \end{pmatrix},$$

de donde se deduce que los 2-cobordes $\alpha_2, \cdots, \alpha_{4t-2}$ son linealmente independientes.

Por otra parte, se puede comprobar que los 2-cobordes α_{4t} y α_{4t-1} se pueden generar como combinación de los demás de la siguiente forma:

$$\alpha_{4t} = \alpha_2\alpha_4 \cdots \alpha_{4t-2}$$

$$\alpha_{4t-1} = \alpha_2\alpha_4 \cdots \alpha_{2t}\alpha_{2t+1} \times \alpha_{4t-3}$$

Proposición 3.3.18 *Una base de los 2-cobordes normalizados sobre D_{4t} viene dada por $\alpha_2, \cdots, \alpha_{4t-2}$.*

Corolario 3.3.19 *Una base de los 2-cociclos normalizados sobre D_{4t} viene dada por $\alpha_2, \cdots, \alpha_{4t-2}\beta_1, \beta_2, \gamma$.*

De este modo, cualquier matriz normalizada asociada a un 2-cociclo sobre D_{4t} se puede escribir como el producto Hadamard siguiente:

$$\prod_{i=2}^{4t-2} \alpha_i^{r_i} \beta_1^{b_1} \beta_2^{b_2} \gamma^r, \tag{3.20}$$

para $r_i, b_j, r \in \{0,1\}$, aunque generalmente, en lugar de representar una 2-cociclo como este producto, utilizaremos el concepto de configuración de la Definición 3.3.4.

Matrices cocíclicas de Hadamard

A partir de la base que acabamos de presentar de matrices cocíclicas normalizadas para el diédrico, la búsqueda de una matriz cocíclica de Hadamard se puede realizar, como siempre, generando todas las matrices cocíclicas normalizadas mediante el producto Hadamard de dichos generadores y aplicando el test de Hadamard a cada una de ellas para verificar si las matrices así construidas son de Hadamard.

En el caso del diédrico, sin embargo, el problema se puede reducir considerablemente como veremos a continuación.

Para ello, trataremos de analizar, en primer lugar, cuándo la fila k-ésima, con $2 \leq k \leq 4t$, de una matriz cocíclica normalizada está en posición Hadamard; esto es, tiene $2t$ entradas iguales a 1 y otras tantas entradas negativas.

Al igual que hacíamos cuando trabajábamos con el producto directo $\mathbb{Z}_t \times \mathbb{Z}_2^2$, utilizaremos por comodidad y sin pérdida de información los 2-cobordes generalizados, $\bar{\alpha}_i$; es decir, las matrices asociadas a los 2-cobordes, pero multiplicando su fila i-ésima por -1, con el fin de que todas las filas tengan exactamente 2 entradas negativas.

Teniendo en cuenta las posiciones de las entradas negativas en la fila k-ésima de un 2-coborde generalizado, podemos analizar las relaciones entre cualesquiera dos de ellos.

- Si la fila k a la que nos referimos es tal que $2 \leq k \leq 2t$:
  - Para $2 \leq i \leq k-1$ los 2-cobordes $\bar{\alpha}_i$ y $\bar{\alpha}_{2t+i-k+1}$ están simplemente relacionados.

En el caso particular en que $k = t+1$ las posiciones de las dos entradas negativas correspondientes a $\bar{\alpha}_i$ y $\bar{\alpha}_{t+i}$ coinciden, por lo que están doblemente relacionados.

- Para $k+1 \leq i \leq 2t$ los 2-cobordes $\bar{\alpha}_i$ y $\bar{\alpha}_{i-k+1}$ están simplemente relacionados.

  Si $k = t+1$ los 2-cobordes $\bar{\alpha}_i$ y $\bar{\alpha}_{t+i}$ están doblemente relacionados.

- Para $2t+1 \leq i \leq 2t+k-3$ los 2-cobordes $\bar{\alpha}_i$ y $\bar{\alpha}_{2t+i-k+1}$ están simplemente relacionados.

  En este caso, quedan libres, es decir, no están relacionados con ningún otro $\bar{\alpha}_i$ los generadores:

  * $\bar{\alpha}_{2t+k-1}$, que tiene los -1 en las posiciones $(k, 2t+k-1)$ y $(k, 4t)$.
  * $\bar{\alpha}_{2t+k-2}$, que tiene los -1 en las posiciones $(k, 2t+k-2)$ y $(k, 4t-1)$.
  * $\bar{\alpha}_k$, que tiene los -1 en todas las posiciones (k, j), con $j \neq 1, k$.

- Para $2t+k \leq i \leq 4t-2$ los 2-cobordes $\bar{\alpha}_i$ y $\bar{\alpha}_{i-k+1}$ están simplemente relacionados.

- Si la fila k a la que nos referimos es tal que $2t+1 \leq k \leq 4t$:

  - Para $2 \leq i \leq k-2t$ los 2-cobordes $\bar{\alpha}_i$ y $\bar{\alpha}_{k+1-i}$ están doblemente relacionados.

  - Para $k-2t+1 \leq i \leq 2t$ los 2-cobordes $\bar{\alpha}_i$ y $\bar{\alpha}_{2t+k+1-i}$ están doblemente relacionados.

  - Los generadores $\bar{\alpha}_k$, $\bar{\alpha}_{k-2t+1}$ y $\bar{\alpha}_{k-2t+2}$ no están relacionados con ningún otro.

Proposición 3.3.20 *Si se dispone la base de 2-cobordes generalizados en la forma*

$$< -, \bar{\alpha}_2, \cdots, \bar{\alpha}_{k-1}, \bar{\alpha}_k, \bar{\alpha}_{k+1}, \cdots, \bar{\alpha}_{2t} >$$

$$< \bar{\alpha}_{2t+1}, \cdots, \bar{\alpha}_{4t-2}, -, - >$$

los 2-cobordes generalizados están relacionados cíclicamente, de manera que cada $\bar{\alpha}_i$ está relacionado con el 2-coborde generalizado que dista $k-1$ de él de forma cíclica a izquierda.

Definición 3.3.21 Denominaremos *componente n-conexa* a todo subconjunto de una configuración que aporta 2 entradas negativas en una determinada fila.

La denominación de componente n-conexa procede del hecho de que una componente $(k-1)$-conexa está constituida por una serie de $\bar{\alpha}_i$ que distan $k-1$ cíclicamente. Cada componente $(k-1)$-conexa aporta 2 entradas negativas, siempre y cuando dicha componente no sea cerrada, en cuyo caso se cancelan todos los -1 que aportarían, de manera que no añaden ningún -1 a en la fila k correspondiente. Cuando hablemos de componente n-conexa nos referiremos, salvo que se especifique lo contrario, a una componente n-conexa no cerrada.

En este punto podemos introducir un concepto íntimamente relacionado con la noción de *relación* entre dos 2-cobordes.

Definición 3.3.22 Diremos que en una fila se produce una *intersección*, cuando uno o más generadores de los que intervienen en la configuración correspondiente tienen un -1 en la misma posición. Por la forma que tienen los generadores, las intersecciones pueden ser dobles, cuando dos generadores tienen un -1 en la misma posición, o triples, cuando son tres los generadores que coinciden con un -1 en la misma posición.

Con todo esto, dada la fila k-ésima ($2 \leq k \leq 4t$) de una matriz de orden $4t$, denotemos por c al número de componentes $(k-1)$-conexas no cíclicas de generadores de 2-cobordes generalizados, r al número de -1 que realmente aportan los generadores β_1, β_2 y γ e i al número de intersecciones dobles no triples.

Teorema 3.3.23 *La fila k está en posición Hadamard si y sólo si se verifica la condición*

$$2c + r - 2i = 2t.$$

Configuraciones en las que intervienen β_2 y γ, pero no β_1

Si observamos detenidamente las matrices cocíclicas de Hadamard obtenidas experimentalmente a partir del producto Hadamard de los elementos de la base de 2-cociclos, se tiene que la gran mayoría de ellas corresponde a una configuración en la que inter-

vienen los generadores β_2 y γ, pero no β_1, como se muestra en la tabla siguiente:

t	número de config.	con β_1	con β_2 y γ, sin β_1
2	32	8	16
3	72	0	72
4	768	64	512

Para $t = 2$ el 50% de las configuraciones contienen a β_2 y γ, pero no a β_1. Para $t = 3$ se tiene que todas las configuraciones hacen uso de β_2 y γ, pero ninguna de β_1. Para $t = 4$ la razón entre las configuraciones que utilizan β_2 y γ, pero no β_1 es del 66.67%. Este comportamiento se mantiene para valores elevados de t.

Este resultado experimental coincide con la apreciación hecha por Flannery en [42], donde apuntaba una mayor densidad de matrices cocíclicas de Hadamard entre las configuraciones que utilizan β_2 y γ, pero no β_1.

Como consecuencia de todo esto, pare razonable centrarnos en el estudio de estas configuraciones. A continuación trataremos de encontrar resultados que nos permitan saber a priori si una configuración dada puede dar lugar a una matriz cocíclica de Hadamard, y por otro lado reducir en lo posible la búsqueda estas matrices.

El primer resultado que tenemos nos permite reducir la aplicación del test de Hadamard a menos filas en estas configuraciones.

Proposición 3.3.24 *En una configuración en la que intervienen β_2 y γ, pero no β_1, las filas k-ésimas, con $2t + 1 \leq k \leq 4t$ están siempre en posición Hadamard.*

Demostración.

Al multiplicar las matrices asociadas a β_2 y γ, se obtiene una matriz que contiene una banda en diagonal con $2t$ entradas negativas consecutivas en cada fila, empezando en la columna 2 de la fila $2t - 1$ y en la columna $2t - 1$ de la fila $4t$, y el resto valores positivos. Luego, en cada una de estas filas se tienen ya $2t$ entradas positivas y otras tantas entradas negativas.

$$\beta_2\gamma = \left(\begin{array}{ccccccc|ccccccc}
+ & \cdots & \cdots & \cdots & \cdots & \cdots & + & + & \cdots & \cdots & \cdots & \cdots & \cdots & + \\
+ & \cdots & \cdots & \cdots & \cdots & + & - & + & \cdots & \cdots & \cdots & \cdots & + & - \\
+ & \cdots & \cdots & \cdots & + & - & - & + & \cdots & \cdots & \cdots & + & - & - \\
\vdots & & & / & & & & \vdots & & & / & & & \vdots \\
+ & \cdots & + & - & \cdots & \cdots & - & + & \cdots & + & - & \cdots & \cdots & - \\
+ & + & - & \cdots & \cdots & \cdots & - & + & + & - & \cdots & \cdots & \cdots & - \\
+ & - & \cdots & \cdots & \cdots & \cdots & - & + & - & \cdots & \cdots & \cdots & \cdots & - \\
\hline
+ & - & \cdots & \cdots & \cdots & \cdots & \cdots & - & + & \cdots & \cdots & \cdots & \cdots & + \\
+ & + & - & \cdots & \cdots & \cdots & \cdots & \cdots & - & + & \cdots & \cdots & \cdots & + \\
+ & \cdots & + & - & \cdots & \cdots & \cdots & \cdots & \cdots & - & + & \cdots & \cdots & + \\
+ & & & \ddots & & & & & & & & \ddots & & + \\
+ & \cdots & \cdots & \cdots & + & - & \cdots & \cdots & \cdots & \cdots & \cdots & - & + & + \\
+ & \cdots & \cdots & \cdots & \cdots & + & - & \cdots & \cdots & \cdots & \cdots & \cdots & - & + \\
+ & \cdots & \cdots & \cdots & \cdots & \cdots & + & - & \cdots & \cdots & \cdots & \cdots & \cdots & -
\end{array}\right)$$

Por otra parte, analicemos qué ocurre cuando actúe cualquier $\bar{\alpha}_i$ (o cualquier componente $(k-1)$-conexa) en una fila k $(2t+1 \leq k \leq 4t)$.

Teniendo en cuenta el análisis anterior acerca de las relaciones entre dos 2-cobordes generalizados para una fila k $(2t+1 \leq k \leq 4t)$, se deduce que si consideramos las listas

$$< -, \bar{\alpha}_2, \cdots, \bar{\alpha}_{k-2t} | \bar{\alpha}_{2t+1}, \cdots, \bar{\alpha}_{k-1}, \bar{\alpha}_k >$$

$$< \bar{\alpha}_{k-2t+1}, \bar{\alpha}_{k-2t+2}, \bar{\alpha}_{k-2t+3}, \cdots, \bar{\alpha}_{2t} | \bar{\alpha}_{k+1}, \cdots, \bar{\alpha}_{4t-2}, -, - >,$$

en cada una de ellas, los $\bar{\alpha}_i$ están relacionados con sus simétricos respecto de la barra, " | ", de manera que las dos entradas negativas que aportan en la fila k son las mismas.

Así, si sobre la configuración en la que actúan β_2 y γ interviene un $\bar{\alpha}_i$ dado, en cualquier fila k $(2t+1 \leq k \leq 4t)$ se tendrá que una de las dos entradas negativas de que consta coincidirá con una entrada positiva en la matriz obtenida mediante el producto Hadamard de β_2 y γ y la otra entrada negativa de $\bar{\alpha}_i$ en dicha fila estará en el lugar de otra entrada negativa de la matriz producto de β_2 y γ. De modo que la fila en cuestión mantendrá el mismo número de entradas positivas y negativas y, por tanto, seguirá estando en posición Hadamard.

■

Podemos ir más allá.

Proposición 3.3.25 *En una configuración en la intervienen β_2 y γ, pero no β_1, la fila $t+1$ siempre está en posición Hadamard.*

Demostración.

El generador γ tiene en dicha fila $2t$ entradas negativas que van desde la columna $t+1$ a la $2t$ y de la $3t+1$ a la $4t$ (es decir, está en posición Hadamard). Además, el generador β_2 tiene todas sus entradas positivas en esta fila, por lo que es indiferente su actuación. Si se analiza la posición en que se encuentran las entradas negativas para cada uno de los $\bar{\alpha}_i$ en esta fila, se observa que los 2-cobordes están relacionados de manera que si se ordenan de la siguiente forma:

$$< -, \bar{\alpha}_2, \cdots, \bar{\alpha}_t | \bar{\alpha}_{2t}, \cdots, \bar{\alpha}_{t+2}, \bar{\alpha}_{t+1} >$$

$$< \bar{\alpha}_{2t+1}, \cdots, \bar{\alpha}_{3t-2}, \bar{\alpha}_{3t-1} | -, -, \bar{\alpha}_{4t-2}, \cdots, \bar{\alpha}_{3t+1} >,$$

entonces, los 2-cobordes genéricos simétricos respecto de la barra tienen sus dos entradas negativas de la fila $t+1$ en las mismas posiciones. Además la matriz asociada a γ tiene una entrada positiva en la posición de una de las entradas negativas de cada uno de los 2-cobordes genéricos y otra entrada negativa en la posición de la otra entrada negativa de los 2-cobordes genéricos para la fila considerada. Por tanto, cada uno de los 2-cobordes $\bar{\alpha}_i$ mantiene el mismo número de entradas negativas que tenía γ. Por tanto, la fila $t+1$ está en posición Hadamard para cualquier configuración.

■

Proposición 3.3.26 *En una configuración en la que intervienen β_2 y γ, pero no β_1, la fila F_i $(2 \leq i \leq t)$ está en posición Hadamard si y sólo si la fila $2t+2-i$ está en posición Hadamard.*

Demostración.

La fila $2t+2-i$ tiene las mismas entradas negativas que la fila i-ésima, pero desplazadas $k-1$ columnas cíclicamente a la izquierda. Por tanto, si una de estas filas tiene $2t$ entradas negativas, la otra tendrá el mismo número.

Además, si se rota $i-1$ posiciones a la izquierda la fila $2t+2-i$ de la matriz γ y se multiplica dicha fila por -1, se obtiene la fila i-ésima de γ (para $2 \leq i \leq t$).

En la fila i el 2-coborde generalizado $\bar{\alpha}_n$ tiene entradas negativas en las columnas n-ésima y $(n-(i-1))$-ésima. En la fila $2t+2-i$ las entradas negativas se encuentran sobre las columnas n-ésima y $(n+(i-1))$-ésima. Por lo que, rotando $i-1$ posiciones a la izquierda la fila $2t+2-i$, ésta fila coincide con la fila i.

■

Combinando las proposiciones anteriores, podemos concluir el siguiente resultado, crucial para reducir el gasto computacional en la evaluación del test de Hadamard a configuraciones que usen β_2 y γ, pero no β_1.

Teorema 3.3.27 *Una matriz cocíclica obtenida a partir de una configuración en la que intervienen β_2 y γ, pero no interviene β_1, es de Hadamard si y sólo si las t primeras filas están en posición Hadamard.*

Esto supone una gran simplificación a la hora de buscar matrices de Hadamard entre las matrices cocíclicas desarrolladas sobre D_{4t}, puesto que el problema se reduce de tener que estudiar las $4t$ filas de cada matriz a estudiar sólo las t primeras (en realidad la primera fila también está siempre en posición Hadamard, por tratarse de matrices normalizadas). Además, recuérdese que la condición que deben cumplir las t primeras filas para que se trate de una matriz de Hadamard es muy sencilla, gracias al hecho de que estamos trabajando con 2-cociclos en todo momento; simplemente se ha de cumplir que la suma de los elementos de cada una de estas filas sea 0.

A continuación vamos a obtener una cota para el número de generadores que pueden intervenir en una configuración para que ésta de lugar a una matriz de Hadamard.

Un resultado auxiliar es el siguiente.

Lema 3.3.28 *La relación entre el número de componentes conexas, c, las interacciones dobles (no triples) entre 2-cobordes generalizados, i, y el número t que indica la dimensión de la matriz para que una fila k esté en posición Hadamard, se puede simplificar en el caso de estudiar las t primeras filas, de modo que*

$$c_k + k - 1 - i_k = t, \qquad 2 \leq k \leq t \tag{3.21}$$

Teorema 3.3.29 *En una configuración en la que intervengan β_2 y γ, pero no β_1, el número de generadores que se han de utilizar para obtener una matriz cocíclica de Hadamard oscilará entre un mínimo de $t+1$ y un máximo de $3t$.*

Demostración.

Si particularizamos la relación (3.21) para la segunda fila, se deduce que se necesitan t componentes 1-conexas en la lista

$$< \bar{\alpha}_2, \cdots, \bar{\alpha}_{2t}, \gamma, \bar{\alpha}_{2t+1}, \cdots, \bar{\alpha}_{4t-2} > .$$

Luego, el número mínimo de generadores que deben intervenir en una configuración del tipo considerado para que dé origen a una matriz de Hadamard es $t+1$, pues β_2 también interviene.

Por otra parte, el número máximo de generadores que intervienen en una configuración de las que estamos considerando es $3t$, puesto que para tener t componentes conexas es necesario prescindir, al menos, de $t-1$ generadores de entre los α_i y γ y también estamos excluyendo el β_1.

■

Nota 3.3.30 *En todo momento estamos considerando configuraciones en las que intervienen γ y β_2 y no interviene β_1. Si consideramos otra configuración cualquiera distinta de estas, entonces el número mínimo de generadores sería t y el número máximo de generadores $3t+1$.*

Estos resultados son positivos, en el sentido de que permiten reducir la búsqueda de matrices cocíclicas de Hadamard sobre el diédrico en el caso configuraciones en las que intervienen γ y β_2, pero no β_1. Según el trabajo de Flannery, [42], como ya comentásemos con anterioridad, la búsqueda de matrices cocíclicas de Hadamard sobre este grupo en configuraciones de este tipo se reducía a encontrar dos vectores $\overrightarrow{m}$ y $\overrightarrow{n}$ de $2t$ componentes cada uno de modo que la dimensión del espacio en que había que buscar dichos vectores era 2^{2t-1} para cada uno de ellos, quedando, por tanto, que las matrices cocíclicas de Hadamard sobre D_{4t} debían buscarse de entre 2^{4t-2} posibilidades.

Con la acotación que aquí damos del número de generadores que deben intervenir en una configuración del tipo indicado para dar lugar a una matriz cocíclica de Hadamard sobre el diédrico, el número de posibles matrices cocíclicas entre las que hay que busca las de Hadamard se reduce a:

$$\binom{4t-3}{t+1}+\binom{4t-3}{t+2}+\cdots+\binom{4t-3}{3t}.$$

Si comparamos ambas posibilidades, se puede ver que asintóticamente estas cotas reducen a la mitad el número de matrices cocíclicas asociadas a configuraciones en las que intervienen β_1, β_2 y γ que pueden ser de Hadamard.

Por otra parte, si se analiza cómo se generan las matrices cocíclicas de Hadamard obtenidas para distintos valores de t a partir de los elementos de la base de 2-cociclos, se puede observar una mayor densidad de estas matrices cuando se utilizan alrededor de $2t$ generadores y disminuye a medida que el número de generadores se aleja de este valor central. Un ejemplo de esto lo podemos ver en la siguiente tabla, en la que se muestra para distintos valores de t el número de matrices cocíclicas de Hadamard que se obtienen cuando se utilizan n generadores en la configuración de dichas matrices:

$t\backslash n$	3	4	5	6	7	8	9	10	11	12
2	12	8	8	4						
3		6	12	18	18	12	6			
4			20	52	276	128	100	84	84	24

(3.22)

Este comportamiento se sigue observando para valores de t superiores.

Algoritmo genético

La implementación que hemos realizado sólo nos permite encontrar matrices cocíclicas de Hadamard para valores pequeños de t: hay que tener en cuenta que una vez construida la base, lo cual no requiere mucho tiempo, se determinan **todas las matrices cocíclicas**, proceso que conlleva un elevado coste en tiempo y en memoria, y resulta impracticable para $t \geq 6$.

Aún cuando se tratara de aplicar el test de Hadamard al unísono que se van creando todas las matrices cocíclicas (rutina que también hemos implementado), es tal la cantidad de matrices cocíclicas que no son de Hadamard con respecto las que sí lo son, que nuevamente el ordenador es incapaz de ofrecer ni siquiera una matriz ortogonal para $t \geq 6$ en un tiempo "prudencial" (hablamos incluso de que transcurridos unos días la máquina ofrece un mensaje en el que avisa que sus recursos han sido desbordados). Quizás esta rutina sería apropiada en caso de utilizar ordenadores conectados en paralelo, disponibilidad que no hemos tenido en nuestro caso.

Como alternativa, pensamos en hacer uso de *algoritmos genéticos* para buscar estas matrices para valores de t elevados. Como bien es sabido, los algoritmos genéticos son procedimientos de adaptación que permiten la búsqueda de soluciones a problemas que pueden plantearse como procesos que siguen pautas similares a las de la evolución biológica, basada en los principios de evolución darwinianos de reproducción y supervivencia de los individuos que mejor se adaptan a su hábitat. El caso del diédrico se ajusta convenientemente a esta situación, aunque igualmente se podría haber tratado de aplicar en cualquier otro ejemplo.

Para elaborar un algoritmo genético en este sentido, tendremos que adaptar algunas definiciones "clásicas" relacionadas con estos algoritmos a nuestro contexto.

En primer lugar, un *individuo*, x_i^t, va a ser para nosotros una matriz cocíclica normalizada.

Tal y como hemos introducido en secciones anteriores, cada individuo está identificado con una *configuración*, de modo que todo individuo tiene asociada una lista binaria de longitud fija $4t$ (para cada valor de t), tal que cada coordenada de la lista hace referencia a un generador de la base de 2-cociclos en el orden siguiente:

$$(\alpha_1, \ldots, \alpha_{4t-2}, \beta_1, \beta_2, \gamma);$$

de forma que, si la entrada i-ésima de la lista es un 1, el generador i-ésimo interviene en la generación de la matriz cocíclica resultante y si en una posición aparece un cero, indicará que el 2-cociclo correspondiente no interviene. Así, podríamos decir que la configuración que representa a un individuo es su conjunto de *cromosomas*, de modo que cada individuo viene unívocamente determinado por sus $4t$ cromosomas: los $4t-3$ primeros, correspondientes a los 2-cobordes de la base, y los tres últimos que indican respectivamente si en la configuración intervienen los 2-cociclos simétricos y el conmutador.

Para empezar se ha de partir de una población de individuos, que inicialmente se genera de forma aleatoria y en cada iteración dicha población da lugar a una *nueva generación.* La nueva población estará formada por los individuos mejor *adaptados* de entre los individuos de la generación anterior, así como de individuos que resulten de la reproducción de individuos de la generación anterior mediante *cruce* o *mutación.* El cruce consiste en la recombinación de los cromosomas de dos individuos, a los que podríamos llamar padres, para dar lugar a un par de hijos. La mutación es la alteración de alguno de los cromosomas de un individuo, es decir, la modificación de algún 0 ó 1 de la configuración asociada al individuo padre.

Como consecuencia de la existencia de los operadores genéticos de cruce y mutación, a cada individuo se le asocia respectivamente una *probabilidad de cruce*, P_c, y una *probabilidad de mutación*, P_m. La primera es la probabilidad de aplicar el operador de cruce a una pareja de individuos y la segunda es la probabilidad de aplicar el operador de mutación sobre la cadena de cromosomas de un individuo.

Este proceso hace necesario definir una *función de adaptación*, $f(x_i^t)$, que indique el grado de adaptación de cada individuo. La función de adaptación hace una evaluación de los individuos, la cual permite llevar a cabo un *proceso de selección* que dará lugar a la nueva generación de individuos.

Los algoritmos genéticos tienen garantizada la convergencia, desde que Holland lo probara en 1975 [62]. No obstante, no hay constancia del número de generaciones necesarias para alcanzar un individuo óptimo (en nuestro caso, una matriz cocíclica de Hadamard). De hecho, la *condición de parada* que adoptaremos en nuestro algoritmo consistirá en alcanzar el valor máximo de la función de adaptación, es decir, el algoritmo parará cuando se haya obtenido una matriz de Hadamard.

Una vez que se han introducido los conceptos fundamentales y se ha dado la idea de en qué consiste un algoritmo genético, analicemos cómo funciona el nuestro.

Para aligerar el proceso de construcción de matrices cocíclicas a partir de los generadores, en vez de trabajar directamente con matrices $4t \times 4t$ y su producto hadamard punto a punto, guardamos las posiciones en las que éstas presentan un -1. De este modo, el producto hadamard de una lista `l` de matrices, `prodbis[l]`, se traduce en unir las listas correspondientes de posiciones, y seleccionar de entre éstas aquellas que aparezcan un número impar de veces. Este ardid se traduce en

una ostensible reducción en el tiempo que requiere hacer el producto Hadamard de matrices, lo que redunda en un funcionamiento más rápido del algoritmo genético, que consume menos tiempo al construir los individuos de la población en cada generación.

```
t=Input["Introduzca el valor de t deseado para el diédrico D_4t:  "];
matrizdeunos[n_]:=Table[Table[1,{j, n}],{i, n}];
Print["Creando generadores..."];
(* Construcción de los 4t-3 generadores 2-cobordes.  *)
base={ }; m=matrizdeunos[4*t];
Do[base=Append[base,Join[Delete[Table[{i,j},{j,4*t}],{{1},{i}}],
      Table[{j,i}, {j,2,i-1}],
      Table[{j,i}, {j,i+1,4*t}],
      Table[{i+1-j,j}, {j,2,i-1}],
      Table[{2*t+i+1-j,j}, {j,i+1,2*t}],
      Table[{j+i-1,j}, {j,2*t+1,4*t+1-i}],
      Table[{j-2*t+i-1,j}, {j,4*t+2-i,4*t}]]],
{i,2,2*t}];
Do[base=Append[base,Join[Delete[Table[{i,j},{j,4*t}],{{1},{i}}],
      Table[{j,i}, {j,2,i-1}],
      Table[{j,i}, {j,i+1,4*t}],
      Table[{j,i}, {j,2,i-1}],
      Table[{j,i}, {j,i+1,4*t}],
      Table[{j,i}, {j,2,i-1}],
      Table[{j,i}, {j,i+1,4*t}],
      Table[{i+j-1,j}, {j,2,4*t-i+1}],
      Table[{i-2*t+j-1,j}, {j,4*t-i+2,2*t}],
      Table[{i+1-j,j}, {j,2*t+1,i-1}],
      Table[{2*t+i+1-j,j}, {j,i+1,4*t}]]],
{i,2*t+1,4*t-2}];
(* Construcción de los 2 generadores de inflación.  *)
(* Primer generador de inflación *)
base=Append[base,Flatten[Table[Table[{i,j},
      {j,2,4*t,2}],{i,2,4*t,2}],1]];
(* Segundo generador de inflación *)
base=Append[base,Flatten[Table[Table[{i,j},
     {j,2*t+1,4*t}],{i,2*t+1,4*t}],1]];
```

```
(* Construcción del generador de transgresión.  *)
base=Append[base,Flatten[Join[Table[
      Join[Table[{i,j},{j,2*t+2-i,2*t}],
      Table[{i,j}, {j,4*t+2-i,4*t}]], {i,2,2*t}],
      Table[Join[Table[{i,j}, {j,i-2*t+1,2*t}],
      Table[{i,j}, {j,i+1,4*t}]], {i,2*t+1,4*t-1}]],1]];
prodbis[l_]:=Apply[Union,Select[Split[Sort[
      Apply[Join,l]]],OddQ[Length[#1]]&]];
```

Como se discutía con anterioridad, existe claramente una mayor densidad de matrices cocíclicas de Hadamard sobre D_{4t} entre las matrices o individuos que contienen en su configuración a γ y β_2, pero no a β_1. Por tanto vamos a trabajar con individuos que cumplan este requisito, pudiéndose distinguir a los individuos sólo por los 2-cobordes que intervengan en su configuración. Esto hace que la longitud de la cadena binaria que define a cada individuo sea de longitud $4t-3$.

Por otra parte, sabemos que la primera fila de la matriz asociada a cualquier individuo está siempre en posición Hadamard, por ser toda de unos; y que, para las configuraciones indicadas, para que una matriz cocíclica sobre D_{4t} sea de Hadamard basta con que sus t primeras filas estén en posición Hadamard. Así, la función adaptación, `adaptacion1`, medirá, en realidad, cuántas de las $t-1$ primeras filas (sin contar la primera) están en posición Hadamard.

```
tfilas[l_]:=l[[Select[Range[Length[l]],l[[#1,1]]<=t&]]];
base=Map[tfilas, base];
adaptacion[p_]:=Map[adaptacion1,p];
adaptacion1[l_]:=Module[{k,n}, k=Flatten[Position[l,1],1];
      Length[Select[Split[Transpose[prodbis[Join[
        Table[base[[k[[i]]]], {i,Length[k]}],
{base[[4*t-1]],base[[4*t]]}]]][[1]]], Length[#1]==2*t&]]];
```

Vamos a partir de una población inicial de $4t$ individuos, que se crea de forma aleatoria a partir de una base de 2-cobordes.

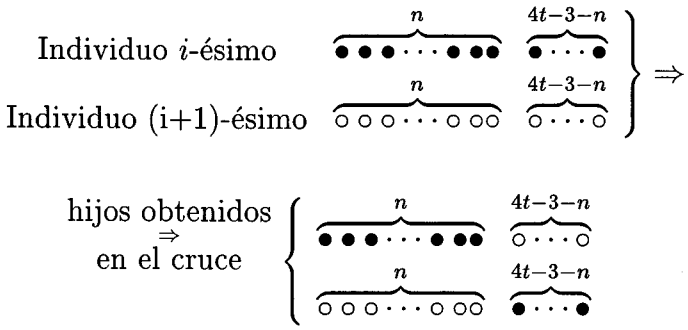
```
pob={ };
Do[pob=Append[pob,Table[Random[Integer],{j,4*t-3}]],{i,4*t}];
```

Esta población va a ir evolucionando generación tras generación, hasta que se

obtenga que la adaptación de un individuo es $t-1$, instante en que el algoritmo finaliza por haberse encontrado una matriz de Hadamard. El cambio generacional se produce de la siguiente forma:

1. En primer lugar, se mide cuál es la adaptación de cada individuo. Si alguno de ellos tiene adaptación $t-1$, el algoritmo finaliza, pues esto significa que ya se tiene una matriz cocíclica de Hadamard. En caso contrario, pasamos al siguiente punto.

2. En segundo lugar, se producen los cruces entre individuos. Para ello se hace uso de la función `cruces` que reordena aleatoriamente los $4t$ individuos de partida para después agrupar los $2t$ primeros individuos de dos en dos y aplicar a cada una de estas parejas de individuos la función `cruces1`. Esta nueva función determina de forma aleatoria en qué punto, n, de la configuración de cada pareja se va a producir el cruce, de forma que:




```
RandomPermutation[n_Integer?Positive]:=Block[{t},
      t=Array[{Random[],#}&,n]; t=Sort[t];
      Map[#[[2]]&,t]];
cruces[p_]:=Module[{k,l,n}, n=2*Floor[Length[p]/2];
      l=RandomPermutation[n]; k={}; Do[
        k=Join[k,cruces1[p[[l[[2*i-1]]]],p[[l[[2*i]]]]],
{i, n/2}]; k];
cruces1[k_,l_]:=Module[{m,n}, n=Random[Integer,{1,4*t-4}];
      {Join[Take[k,n],Take[l,-(4*t-3- n)]],
        Join[Take[l, n],Take[k,-(4*t-3-n)]]}];
```

3. En tercer lugar, se realiza la mutación de un carácter de la configuración de un porcentaje pequeño de la población. Asumimos que la probabilidad de mutación es del 1%. Para ello, se asocia aleatoriamente un valor entre 1 y 100

a cada individuo, considerando que aquellos individuos que tengan asociado el valor 1 sufrirán mutación. La función `mutación1` se encarga de elegir de forma aleatoria una posición de la cadena binaria de cromosomas de un individuo con probabilidad 1 de mutación y cambia el carácter situado en dicha posición.

```
mutacion[p_]:=Module[{n,k},
      k=Table[Random[Integer,{1,100}], {i,Length[p]}];
      n=Select[Range[Length[p]],k[[#1]]<=10&]; k={};
      Do[k=Append[k,mutacion1[p[[n[[i]]]]]], {i,Length[n]}];
k];
mutacion1[l_]:=Module[{n,k}, n=Random[Integer,{1,4*t-3}];
      k=l; ReplacePart[k,1-l[[n]],n]];
```

4. Por último, de entre todos los individuos (padres, hijos y mutantes) nos quedaremos con los mejor adaptados. Para ello habrá que hacer el siguiente barrido:

   - Se cuentan los individuos que tienen adaptación $t-1$ y en el caso de que haya alguno, finaliza el algoritmo. En caso contrario se pasa al siguiente punto.
   - Se cuentan los individuos con adaptación $t-2$, si son menos de $4t$, se suman los que tiene adaptación $t-3$ y así sucesivamente hasta conseguir una población con $4t$ individuos. Esta es la nueva generación de individuos.

```
pob={}; iter=0;
Do[pob=Append[pob,Table[Random[Integer], {j,4*t-3}]], {i,4*t}];
mathad=adaptacion[pob]; pos=Flatten[Position[mathad,t-1],1];
While[Length[pos]==0, iter=iter+1;
      Print["Buscando en la generación ",iter];
      descen=mutacion[pob];
      pob=Join[pob,descen];
      mathad=Join[mathad,adaptacion[descen]];
      descen=Union[cruces[pob]];
      pob=Join[pob,descen];
      mathad=Join[mathad,adaptacion[descen]];
      Print["Cruces y mutaciones realizados"];
      ind=1; pob2={}; numero=0; mathad2={};
      While[numero<4*t,
```

```
        natalidad=Flatten[Position[mathad,t-ind],1];
        Print["A falta de ",ind-1," filas para ser hadamard"];
        config=Union[Table[pob[[natalidad[[i]]]],
          {i, Length[natalidad]}]];
        pob2=Join[pob2,config];
        mathad2=Join[mathad2,Table[t-ind, {i,Length[config]}]];
        numero=numero+Length[config];
        Print[Length[config]," configuraciones"];
      ind=ind+1];
      Print["Selección natural realizada"];
      pob=pob2; mathad=mathad2;
      If[ind=3, , mathad=Take[mathad2,4*t];
        auxiliar=Table[Random[Integer,
          {numero-Length[config]+1,numero+1-i}],
        {i,numero-4*t}];
        Do[pob=Delete[pob,auxiliar[[i]]], {i, Length[auxiliar]}]
      ];
      Do[pob=Append[pob,Table[Random[Integer],
        {j,4*t-3}]], {i,t}];
      mathad=Join[mathad,adaptacion[Take[pob,-t]]];
      pos=Flatten[Position[mathad,t-1],1]
];
Print["Se han generado las siguientes matrices de Hadamard en ",
      iter," generaciones..."];
Do[Print[pob[[pos[[i]]]]], {i,Length[pos]}];
```

Es conveniente realizar varias observaciones, que se han tenido en cuenta para la elaboración del algoritmo:

1. Una vez que se ha utilizado el programa para obtener matrices de Hadamard para una dimensión $4t$ dada, para obtener matrices de Hadamard de dimensión $4(t+1)$ se parte de una población construida a partir de la última generación obtenida en el caso de dimensión $4t$. Es necesario tener en cuenta que en dimensión $4t$ hay 4 generadores menos que en dimensión $4(t+1)$, por lo que para tener la población inicial en $4(t+1)$ hay que añadir en las configuraciones de los individuos de la última generación del caso $4t$ 4 caracteres. Se puede

observar que para los primeros valores t existe una gran densidad de matrices de Hadamard obtenidas a partir de configuraciones en las que intervienen los generadores correspondientes a los 2-cobordes t, $t+1$, $3t$ y $3t+1$. Es por esto que los 4 caracteres que hay que introducir para obtener una población en el caso de $4(t+1)$ a partir del caso $4t$ serán unos en las posiciones $t+1$, $t+2$, $3(t+1)$ y $3(t+1)+1$.

```
anadir[l_]:=Module[{k,k2}, k2={t,t+1,3*t,3*t+1};
      k=l; Do[k=Insert[k,Random[Integer],k2[[i]]], {i,4}];
k];
pob2=Map[anadir,pob];
```

2. En un principio el número de individuos en una generación dada no se consideraba fijo, de modo que cuando una generación daba paso a la siguiente, esta última estaba formada por las matrices con mejor función de adaptación, pudiendo tener tantos individuos como fuese necesario. Evidentemente, este procedimiento no era operativo, pues para valores de t no excesivamente grandes la población aumentaba sobremanera generación tras generación, haciendo que el proceso se ralentizase. Como consecuencia se modificó el programa convenientemente para que todas las generaciones mantuviesen el mismo número de individuos, $4t$. La elección de la población de una generación posterior se realiza tomando en primer lugar los individuos cuya función de adaptación es mayor. Si con esos individuos la población no llega a $4t$ individuos, se completa con el nivel siguiente de adaptación y así sucesivamente. Si al completar la población con los individuos de un nivel se superan los $4t$ individuos, lo que se hace es elegir los individuos que formarán parte de la nueva generación de forma aleatoria de entre los individuos del último nivel de adaptación considerado. El que esta elección se realice de forma aleatoria es fundamental para que, el el caso de que la población sea formada por individuos de un sólo nivel de adaptación, en la siguiente generación no nos quedemos con los mismos individuos si no se ha mejorado la adaptación de los individuos, puesto que en caso contrario, siempre estaría formada la población por los mismos individuos (los primeros).

3. Cuando la población está exclusivamente formada por individuos a los que sólo les falta una fila para constituir matrices de Hadamard, es decir, individuos con función de adaptación $t-2$, se permite que la población crezca indefinidamente con el fin de tener más individuos y que no se estanque la población. Al permitir esto, se observa que la población no crece excesivamente en las sucesivas

iteraciones y, sin embargo, da más juego para obtener con menos iteraciones matrices de Hadamard.

4. Inicialmente no se tenía en cuenta que al pasar de una generación a otra, podían generarse individuos idénticos (con igual configuración), así que para evitar esto se introdujo una pequeña modificación en el programa que permitiese eliminar los individuos repetidos.

5. A medida que t va tomando valores más elevados, se requieren más iteraciones para localizar matrices de Hadamard. Una alternativa que consideramos fue aumentar el número de mutaciones, de forma que pasamos de considerar que la probabilidad de mutación era del 1%, al 10%. La diferencia no parece significativa.

6. Observando las configuraciones que dan lugar a matrices de Hadamard para valores de t relativamente pequeños, comprobamos que hay mayor densidad de matrices de Hadamard en las configuraciones que utilizan alrededor de $2t$ generadores de 2-cobordes, según vimos en (3.22). Como consecuencia el programa se modificó para que buscase las matrices de Hadamard a partir de una población en la que los individuos tuviesen en su configuración $2t-1$, $2t$ o $2t+1$ unos. Aunque en las distintas generaciones se añadían algunos individuos cuyas configuraciones eran completamente aleatorias, para no viciar demasiado la población. Tampoco fue significativa esta modificación.

Con ayuda de este algoritmo genético se han obtenido matrices cocíclicas de Hadamard para distintos valores de t. En la siguiente tabla se muestran algunos de estos resultados, indicando cuántas generaciones (iteraciones) se han necesitado para encontrar una matriz de Hadamard y cómo se puede obtener dicha matriz como producto los elementos de la base de 2-cociclos.

Como se puede observar el número de iteraciones no está completamente relacionado con el orden de la matriz que se está buscando. En algunas ocasiones se encuentra una matriz de Hadamard en muy pocas iteraciones, como ha ocurrido en el caso de $t = 9$, pero en otras ocasiones para valores menores, o incluso para el mismo valor de t, se ha tardado mucho más en encontrar una matriz de Hadamard (comparar los resultados para $11 \leq t \leq 13$).

t	generaciones	producto de generadores
6	0	$\alpha_2\alpha_3\alpha_5\alpha_6\alpha_7\alpha_8\alpha_{10}\alpha_{11}\alpha_{12}\alpha_{15}\alpha_{17}\alpha_{18}\alpha_{19}\alpha_{21}\beta_2\gamma$
7	4	$\alpha_5\alpha_6\alpha_9\alpha_{11}\alpha_{14}\alpha_{15}\alpha_{16}\alpha_{17}\alpha_{19}\alpha_{21}\alpha_{24}\alpha_{25}\beta_2\gamma$
8	3	$\alpha_4\alpha_6\alpha_8\alpha_9\alpha_{12}\alpha_{14}\alpha_{19}\alpha_{26}\alpha_{27}\beta_2\gamma$
9	7	$\alpha_2\alpha_7\alpha_8\alpha_{10}\alpha_{12}\alpha_{16}\alpha_{19}\alpha_{20}\alpha_{23}\alpha_{24}\alpha_{26}\alpha_{27}\alpha_{28}\alpha_{33}\beta_2\gamma$
10	78	$\alpha_3\alpha_4\alpha_6\alpha_7\alpha_8\alpha_9\alpha_{11}\alpha_{12}\alpha_{13}\alpha_{15}\alpha_{19}\alpha_{20}\alpha_{22}\alpha_{26}\alpha_{27}\alpha_{29}\alpha_{32}\alpha_{37}\beta_2\gamma$
11	471	$\alpha_2\alpha_3\alpha_4\alpha_5\alpha_9\alpha_{10}\alpha_{11}\alpha_{12}\alpha_{14}\alpha_{15}\alpha_{16}\alpha_{17}\alpha_{19}\alpha_{20}\alpha_{21}\alpha_{25}\alpha_{27}\alpha_{29}\alpha_{30}$ $\alpha_{31}\alpha_{32}\alpha_{33}\alpha_{35}\alpha_{38}\alpha_{41}\alpha_{42}\beta_2\gamma$
12	279	$\alpha_6\alpha_7\alpha_9\alpha_{10}\alpha_{11}\alpha_{13}\alpha_{14}\alpha_{16}\alpha_{19}\alpha_{20}\alpha_{21}\alpha_{22}\alpha_{24}\alpha_{25}\alpha_{30}\alpha_{31}\alpha_{33}\alpha_{37}$ $\alpha_{39}\alpha_{41}\alpha_{42}\alpha_{46}\beta_2\gamma$
13	970	$\alpha_3\alpha_8\alpha_9\alpha_{11}\alpha_{15}\alpha_{17}\alpha_{18}\alpha_{20}\alpha_{22}\alpha_{23}\alpha_{28}\alpha_{29}\alpha_{30}\alpha_{31}\alpha_{32}\alpha_{38}\alpha_{42}\alpha_{46}$ $\alpha_{47}\alpha_{49}\beta_2\gamma$

3.3.3 Matrices cocíclicas de Hadamard sobre otros grupos

En las secciones anteriores hemos estudiado a fondo los ejemplos de la búsqueda de matrices cocíclicas de Hadamard a partir del cálculo de una base de matrices cocíclicas sobre D_{4t} y $\mathbb{Z}_t \times \mathbb{Z}_2^2$ mediante el método de la reducción homológica. A continuación veremos que este método y la implementación que se ha realizado en relación al mismo se puede utilizar para otros grupos. A modo de ejemplo, expondremos algunos resultados experimentales obtenidos en el caso de trabajar con una extensión central o con un producto iterado de una extensión central por un producto semidirecto. En un futuro podría hacerse un estudio más exhaustivo de estos ejemplos, del tipo de los realizados con D_{4t} y $\mathbb{Z}_t \times \mathbb{Z}_2^2$.

Como ejemplo de extensión central hemos tomado la definida del siguiente modo:

$$\mathbb{Z}_{2tf_1} \rtimes \mathbb{Z}_2$$

siendo $f_1 : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_{2t}$ el 2-cociclo dado por:

$$f_1(g_i, g_j) = \begin{cases} \lceil \frac{t}{2} \rceil + 1 & \text{si} \quad g_i = g_j = -1 \\ 0 & \text{e.o.c.} \end{cases}$$

Como ejemplo de producto iterado de una extensión central por un producto

semidirecto hemos escogido el siguiente :

$$(\mathbb{Z}_t \ {}_{\bar{f}}\rtimes \mathbb{Z}_2)\ltimes_{\bar{\chi}}\mathbb{Z}_2,$$

siendo $f_2 : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_t$ el 2-cociclo dado por

$$f_2(g_i, g_j) = \begin{cases} \lceil \frac{t}{2} \rceil + 1 & \text{si} \quad g_i = g_j = -1 \\ 0 & \text{e.o.c.} \end{cases}$$

y χ la acción

$$\chi(a, b) = \begin{cases} -b & \text{si} \quad a = -1 \\ b & \text{si} \quad a = 1 \end{cases}$$

El número de matrices cocíclicas de Hadamard para estos ejemplos y para los primeros valores de t son los dados en la siguiente tabla:

t	$\mathbb{Z}_t \times \mathbb{Z}_2^2$	D_{4t}	$\mathbb{Z}_{2tf_1} \rtimes \mathbb{Z}_2$	$(\mathbb{Z}_{tf_2} \rtimes \mathbb{Z}_2)\ltimes_{\chi}\mathbb{Z}_2$
1	6	6	**6**	**6**
2	168	32	**16**	**168**
3	24	72	**12**	**72**
4	**696**	768	**0**	**272**
5	120	2380	**150**	**800**

Si comparamos los resultados de las dos primeras columnas con la tabla (3.7) podemos comprobar que reobtenemos los mismos resultados. Además, hemos completado la tabla con los datos que aparecen en negrita.

En este momento, quizá merece la pena hacer un alto para comentar algunas cuestiones respecto a los ejemplos considerados de extensiones centrales y productos iterados.

En el caso de la extensión central, al igual que en las otras ocasiones, en primer lugar hemos calculado una base de 2-cociclos, encontrando que para todo t la dimensión de esta base es $4t$. De estos elementos se tiene que uno de ellos corresponde a la parte conmutadora, mientras que parece existir una "anomalía" en el número de elementos asociados a la parte simétrica y a los 2-cobordes, pues es distinto según el valor de t que se considere. Si t es 1 (mod 4) ó 2 (mod 4), la base consta de $4t - 3$ generadores asociados a 2-cobordes y 2 generadores correspondientes a la parte simétrica; si t es 3 (mod 4) ó 0 (mod 4), la base consta de $4t - 2$ generadores asociados a 2-cobordes

y un único generador correspondiente a la parte simétrica. Esta anomalía permite suponer que el estudio en profundidad de este ejemplo pueda ser complejo.

Aunque por una parte sea patente esta dificultad y, por otra, se haya encontrado que para $t = 4$ no existen matrices de Hadamard en este ejemplo, podría ser interesante su estudio puesto que para valores mayores de t sí hemos encontrado matrices cocíclicas de Hadamard. De hecho, para $t = 5$ se tienen 150 matrices de Hadamard. No obstante, también se podría probar con otras extensiones centrales.

Respecto al producto iterado que hemos estudiado como ejemplo proporciona grandes expectativas dado el número de matrices cocíclicas de Hadamard que genera para los primeros valores de t, por lo que también sería conveniente hacer un estudio pormenorizado de las matrices de Hadamard así obtenidas para intentar deducir pautas de cómo combinar los generadores de la base de 2-cociclos para generar matrices de Hadamard. Sirva como adelanto al futuro estudio que se puede hacer de la generación de matrices cocíclicas de Hadamard a partir de este grupo, la siguiente tabla en la que se refleja el número de 2-cobordes, 2-cociclos simétricos y 2-cociclos correspondientes a la parte conmutadora para los primeros valores de t:

t	$2-$ cobordes	parte simétrica	parte conmutadora
1	1	2	1
2	4	3	3
3	9	2	1
4	13	2	1
5	17	2	0

Como puede comprobase a raíz de los datos de esta tabla, el número de generadores linealmente independientes no mantiene una relación tan clara con el valor de t como en los otros ejemplos estudiados. A su vez, el número de generadores correspondientes a 2-cobordes, parte simétrica y conmutadora también difiere para cada valor de t. Esto puede hacer más complicado el estudio de la generación de matrices de Hadamard a partir de este grupo, aunque como dijéramos antes, parece un grupo con una densidad de matrices cocíclicas de Hadamard elevada (al menos para valores de t pequeños).

Al igual que decíamos en el caso anterior, también podría ser productivo estudiar la generación de matrices cocíclicas de Hadamard para otros grupos de este tipo, procedentes de productos iterados.

3.4 Aplicaciones

Vamos a cerrar la memoria generando códigos correctores asociados a matrices cocíclicas de Hadamard, según los métodos generales descritos en [66, 67, 6, 128]. Llamemos A_n a la matriz que se obtiene al sustituir en una matriz de Hadamard normalizada H_n de orden $n \times n$ los 1 por 0 y los -1 por 1. Entonces:

- Como las filas de H_n son ortogonales 2 a 2, cualquier par de filas distintas en A_n deben coincidir en $\frac{n}{2}$ posiciones y diferir en otras tantas; de modo que si se elimina la primera columna de A_n las filas de la matriz resultante conforman un código $\mathcal{A}_n$ de n palabras de longitud $(n-1)$ y distancia mínima $\frac{n}{2}$.
- Si a $\mathcal{A}_n$ se añaden los complementarios de las propias palabras de $\mathcal{A}_n$, se obtiene el código $\mathcal{B}_n$ que consiste en $2n$ palabras de longitud $(n-1)$ y distancia mínima $\frac{n}{2}-1$.
- Si a H_n se le añaden los complementarios de sus filas, se obtiene el código $\mathcal{C}_n$ que consiste en $2n$ palabras de longitud n y distancia mínima $\frac{n}{2}$.
- El código $\mathcal{D}_n$ consiste en el código lineal de matriz generadora $(I_n|A_n)$, de 2^n palabras de longitud $2n$ y distancia mínima $\frac{n}{2}+1$.
- Otra versión del código anterior es $\mathcal{E}_n$, cuya matriz generadora es de la forma $\left(\begin{array}{c|c|c|c} \mathbf{1^T} & I_{n-1} & \mathbf{0^T} & A_{n-1} \\ 0 & \mathbf{0} & 1 & \mathbf{1} \end{array}\right)$, con A_{n-1} la matriz que se obtiene al eliminar la primera fila y la primera columna de A_n.

Estos códigos pueden ser o no lineales y/o cíclicos. Por ejemplo, los códigos que resultan de una matriz de Hadamard H_n del tipo de Sylvester (producto de Kronecker de H_2 por sí mismo $\frac{n}{2}$ veces) son siempre lineales; mientras que los códigos que resultan de una matriz de Hadamard del tipo de Paley, para $n > 8$, nunca son lineales [128], aunque $\mathcal{A}_n$ y $\mathcal{B}_n$ son cíclicos en este caso, y siempre puede tomarse su extensión lineal.

En concreto, consideremos la matriz de Paley $H_{12} = \begin{pmatrix} 1 & 1 \\ 1^T & Q_{11} - I_{11} \end{pmatrix}$, dada por

$$\left(\begin{array}{c|cccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - \\ 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 \\ 1 & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - \\ 1 & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - \\ 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 & 1 \\ 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 & 1 \\ 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - \\ 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 \\ 1 & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - \end{array}\right)$$

Se tiene que $\mathcal{A}_{12}$ es un código cíclico no lineal, de 12 palabras de longitud 11 y distancia mínima 6; $\mathcal{B}_{12}$ es asimismo cíclico no lineal de 24 palabras de longitud 11 y distancia mínima 5; $\mathcal{C}_{12}$ es un código no cíclico de 24 palabras de longitud 12 y distancia mínima 6; y $\mathcal{E}_{12}$ es el código de Golay G_{24}, código lineal de dimensión 12 con palabras de longitud 24 y distancia mínima 8.

En [7, 66, 67] se demuestra que buena parte de los códigos más conocidos y tradicionalmente más utilizados son en verdad códigos que provienen de matrices cocíclicas de Hadamard:

1. La función $f : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{F}_2$ dada por $f(\mathbf{u}, \mathbf{v}) = (-\mathbf{1})^{\mathbf{u}\cdot\mathbf{v}}$ define un 2-cociclo *ortogonal* sobre $\mathbb{Z}_2^n$, de modo que la matriz cocíclica asociada $M(f(\mathbf{u}, \mathbf{v}))$ es la matriz de Hadamard de Sylvester de orden 2^n,

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \overset{n}{\cdots} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

   En particular, de este modo se obtienen los códigos de Reed-Muller de primer orden.

2. Las matrices de Williamson, del tipo

$$\begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}, \quad \text{con } A, B, C, D \text{ circulares simétricas,}$$

son equivalentes Hadamard a matrices cocíclicas sobre $\mathbb{Z}_2^2 \times \mathbb{Z}_t$ [7].

3. Las matrices de Paley H_{4t} del tipo I $(4t - 1 = p^k)$ son cocíclicas sobre D_{4t} [74]. En particular, para $t = 3$ se obtiene el código de Golay extendido G_{24}.

4. Las matrices de Paley H_{4t} del tipo II $(4t = 2p^k + 2)$ son del tipo de Williamson [121], y por tanto cocíclicas sobre $\mathbb{Z}_2^2 \times \mathbb{Z}_t$ [7].

De este modo, es posible plantearse el construir un código corrector con determinadas propiedades, trabajando códigos cocíclicos sobre grupos finitos elegidos. En este sentido, se puede tratar de generar códigos cocíclicos que sean alternativas reales para los códigos Reed-Solomon de los sistemas de audio-CD y de transmisiones espaciales actuales.

En cuanto a las aplicaciones finales de los códigos, nos gustaría destacar que no sólo sirven para mantener un sistema de comunicación "estable" a través de los ruidos del canal; sino que también pueden ser utilizados para establecer sistemas de criptografía de clave pública, como el que diseñara McEliece en [88].

Este método utiliza como clave privada un par de matrices binarias (S, P), con S invertible de orden $k \times k$ y P matriz de permutación de orden $n \times n$. La clave pública consiste en una matriz $\bar{G} = S \cdot G \cdot P$, donde G es una matriz generadora de un código lineal C_G de dimensión k, de palabras de longitud n y corrector de t errores.

A la hora de codificar un mensaje binario, primero se organiza en palabras de longitud k. Cada palabra m se encripta en la forma $c = m \cdot \bar{G} + z$, donde z es un vector aleatorio de peso a lo sumo t.

Para descifrar la palabra c, basta formar

$$\bar{c} = c \cdot P^{-1} = m \cdot S \cdot G + z \cdot P^{-1}.$$

Como C_G es corrector de t errores y $z \cdot P^{-1}$ pesa a lo sumo t, $\bar{c}$ determina unívocamente la palabra $m \cdot S$, a partir de la cual es inmediato recuperar la palabra m original multiplicando a derecha por S^{-1}.

Dependiendo del propósito, se podría tomar un código C_G u otro, por ejemplo atendiendo a la rapidez del algoritmo de decodificación asociado.

Si tomamos la matriz H cocíclica de Hadamard sobre $(\mathbb{Z}_{5f_2} \rtimes \mathbb{Z}_2) \ltimes_\chi \mathbb{Z}_2$ asociada al producto de los 2-cobordes $\alpha_2\alpha_3\alpha_4\alpha_5\alpha_6\alpha_9\alpha_{17}$ y el 2-cociclo $I_{10} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$,

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & - & 1 & - & 1 & 1 & 1 & - & 1 & 1 & - & 1 & - & - & - & 1 & - & - & - & 1 \\
1 & - & - & 1 & 1 & 1 & - & 1 & 1 & - & 1 & 1 & - & - & 1 & - & 1 & - & - & - \\
1 & 1 & - & - & 1 & - & - & - & 1 & 1 & - & 1 & - & 1 & - & - & 1 & 1 & 1 & - \\
1 & - & 1 & 1 & - & 1 & - & - & 1 & - & - & - & 1 & - & - & - & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & - & - & - & - & 1 & 1 & - & 1 & - & - & 1 & - & 1 & 1 & - & - & 1 \\
1 & - & - & 1 & - & - & - & - & - & 1 & - & 1 & 1 & 1 & 1 & 1 & 1 & - & - & 1 \\
1 & 1 & 1 & - & 1 & - & - & - & - & - & 1 & 1 & 1 & - & 1 & - & - & - & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & 1 & 1 & 1 & - & 1 & - & - \\
1 & - & - & 1 & 1 & - & 1 & - & 1 & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - \\
1 & - & 1 & 1 & - & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & 1 & 1 & - \\
1 & 1 & - & - & - & 1 & - & 1 & 1 & 1 & - & - & 1 & - & 1 & 1 & - & - & 1 & - \\
1 & - & - & - & 1 & - & 1 & 1 & - & - & - & - & - & - & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & - & 1 & - & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & - & 1 & - & 1 \\
1 & - & 1 & - & - & - & 1 & 1 & 1 & - & - & 1 & 1 & 1 & 1 & - & - & 1 & - & - \\
1 & 1 & - & 1 & - & 1 & 1 & 1 & - & - & - & 1 & - & 1 & - & - & - & - & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - & - & - & 1 & - & - & - \\
1 & - & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & 1 & - & 1 & - \\
1 & - & - & - & 1 & 1 & - & 1 & - & 1 & 1 & - & 1 & 1 & - & - & - & 1 & - & 1 \\
1 & 1 & - & - & - & 1 & 1 & - & - & - & 1 & 1 & 1 & - & - & 1 & 1 & 1 & - & -
\end{pmatrix}$$

el código lineal binario generado por $G = (I|H)$ consta de $2^{20} = 1048576$ palabras de longitud 40 y distancia mínima 11.

Utilizando esta matriz, en cada cadena de 40 bits se podría introducir hasta 5 errores; esto es, se podría modificar hasta un 12'5% del contenido de cada palabra.

3.5 Conclusiones y problemas abiertos

Después de todo lo expuesto a lo largo de las distintas secciones de este capítulo, nos atreveríamos a decir que el método de la reducción homológica parece acertado para la búsqueda de matrices cocíclicas de Hadamard.

Por una parte, reduce la complejidad del cálculo de los 2-cociclos de un grupo G y, por tanto, de las matrices cocíclicas asociadas, al simplificar el cálculo de la homología de G estudiando la correspondiente de modelos homológicos con menos generadores.

Por otra parte, el hecho de trabajar con una base de 2-cobordes permite determinar, de forma mucho más económica, si una matriz obtenida a partir de la combinación (producto Hadamard) de los 2-cociclos de la base es de Hadamard; puesto que al estar considerando en todo instante matrices cocíclicas, es aplicable el test de Hadamard cuadrático ideado por Horadam y de Launey.

Además, hemos comprobado que esta forma de trabajar concede otras ventajas, como la de extraer más información acerca de cómo han de combinarse los elementos de la base de 2-cobordes para generar matrices cocíclicas de Hadamard. Algunos de estos resultados son realmente interesantes, puesto que permiten reducir el tamaño del espacio de búsqueda de estas matrices, por ejemplo al acotar el número de generadores que pueden intervenir en una configuración.

Al aplicar el método al caso de los grupos $\mathbb{Z}_t \times \mathbb{Z}_2^2$ y D_{4t} hemos recuperado incluso muchos de los resultados y conclusiones establecidos por Horadam y Baliga en [7] y por Flannery en [42], respectivamente.

Adicionalmente ha permitido generar el número total de matrices cocíclicas sobre $\mathbb{Z}_t \times \mathbb{Z}_2^2$ para $t = 4$, dato que a nuestro parecer se desconocía hasta ahora; desde luego, al menos hasta el momento en que apareció el artículo [63].

Esto nos ha permitido verificar la utilidad y bondad del método. Pero también hemos querido mostrar que es aplicable a otros grupos, como son los productos iterados de extensiones centrales por productos semidirectos de grupos abelianos finitos.

También queda claro que a partir de matrices cocíclicas se obtienen infinitas matrices de Hadamard. De hecho, nosotros conjeturamos que a partir del diédrico se

pueden encontrar matrices cocíclicas de Hadamard para cualquier orden $4t$. Sin embargo, es arriesgado pensar esto, pues aunque hemos encontrado que para los primeros valores de t el número de matrices de Hadamard crece ostensiblemente al aumentar t, por otra parte, también hemos observado que en ejemplos realizados con otros grupos, no había un comportamiento regular en el número de matrices cocíclicas de Hadamard para los sucesivos valores de t.

Quizá con el estudio en profundidad de estos u otros grupos podamos algún día arrojar más luz sobre esta problemática y, si no intentar demostrar la conjetura de Hadamard, sí al menos tratar de encontrar matrices de Hadamard en dimensiones en las que se desconozcan. Aunque se antoja una difícil tarea.

De cualquier modo, nuestro método se puede complementar con otros, como el que se recoge en [6] acerca de la restauración de imágenes digitales asociadas a espectros de matrices cocíclicas de Hadamard sobre un grupo G dado; el cual permite encontrar una alta densidad de matrices cocíclicas de Hadamard, partiendo de un conjunto inicial mínimo de matrices cocíclicas de Hadamard previamente conocidas, que nuestro método puede proveer.

También ha de ser un deber el estudiar cómo se traducen al contexto de la Teoría de Perturbación Homológica morfismos clásicos en la (co)homología de grupos, tales como la inflación, la transgresión y la conjugación, por citar algunos; lo cual podría redundar en una mejora de nuestro método.

Otra cuestión sobre la que no hemos trabajado hasta ahora, pero que pretendemos abordar en un futuro próximo, es el estudio de diseños n-dimensionales. Más concretamente, nos gustaría relacionar diseños n-dimensionales con n-(co)homología, a ser posible en una línea similar en la que 2-diseños y 2-cociclos lo están.

En la década de 1970, Shlichta en [112, 113] se preocupaba de la existencia de matrices n-dimensionales binarias con ciertas propiedades de ortogonalidad. Él ya apuntaba que estos diseños pueden dar lugar a códigos de seguridad y a la construcción de códigos correctores de errores. Esto dio lugar al estudio de diseños n-dimensionales por parte de muchos autores, entre ellos Hammer y Seberry [56], de Launey y Horadam [25]. Estos dos últimos, en su artículo conjunto, relacionan los diseños n-dimensionales propios, ya descritos en la Sección 1.3.2, con las denominadas matrices de Hadamard n-dimensionales. Se entiende por *matriz de Hadamard n-dimensional* de orden v, para

$n \geq 2$, toda matriz binaria $A(i_1, i_2, \ldots, i_n)$ con $1 \leq i_k \leq v, 1 \leq k \leq n$, donde cada submatriz obtenida al fijar todos los índices, excepto 2, es una matriz de Hadamard.

Tanto Hammer y Seberry en el artículo previamente citado, como de Launey en [23] y Horadam junto con Lin en [65], describen diversas técnicas para obtener matrices de Hadamard n-dimensionales a partir de matrices de Hadamard 2-dimensionales. Los tres últimos autores apuntan cómo a partir de matrices cocíclicas de Hadamard y matrices de Hadamard desarrolladas sobre un grupo se pueden construir matrices de Hadamard n-dimensionales.

Teniendo en cuenta por una parte la relación entre matrices (cocíclicas) de Hadamard 2-dimensionales y matrices de Hadamard n-dimensionales, por otra la conexión establecida entre diseños 2-dimensionales con n-diseños, así como la relación entre homología en grados 2 y 3 con las matrices cocíclicas de Hadamard; nos preguntamos si sería posible relacionar los n-diseños, así como las matrices de Hadamard n-dimensionales con n-(co)homología.

Si la respuesta fuese afirmativa, el método de la reducción homológica automáticamente cobraría un protagonismo principal, en tanto en cuanto los métodos sugeridos por Horadam, de Launey y Flannery no son extrapolables al caso de n-cohomología con $n > 2$.

Más aún, dado que al incrementar la dimensión n los cálculos (co)homológicos disparan su complejidad, el estudio de las estructuras subyacentes en los modelos (co)homológicos sería de gran utilidad; por su hipotético beneficio en la reducción del proceso de cálculo. Hemos de reconocer que en esta memoria estábamos interesados en el cálculo (co)homológico en dimensiones 2 y 3, en las que las mejoras computacionales que propicia el estudio de las estructuras es prácticamente inapreciable.

Si bien es cierto que a lo largo de la memoria hemos estudiado la (co)homología de los grupos con los que más tarde hemos buscado matrices de Hadamard, a la hora de la verdad, hemos optado por tratar la búsqueda de estas matrices sólo a partir de la homología. Esta decisión tuvo que tomarse por cuestiones meramente prácticas, ya que un trabajo como el aquí presentado ha de tener unas limitaciones espacio-temporales. Aunque momentáneamente hayamos descartado la búsqueda de matrices de Hadamard a partir de la cohomología de grupos, sería conveniente hacer este estudio paralelo próximamente, para determinar cuál de los dos caminos ofrece

más ventajas.

Otro tema relacionado con los estudios aquí desarrollados es la búsqueda de matrices de Hadamard generalizadas. La definición de estas matrices dada originalmente por Butson [16] y Drake [28], es la siguiente: una matriz M de orden $v \times v$ con entradas en un grupo W finito y multiplicativo de orden w, donde w divide a v, es una *matriz generalizada de Hadamard* $GH(w, \frac{v}{w})$ sobre W si, para cualesquiera $i \neq k$ y $i, k \in \{1, \ldots, v\}$, la lista de los cocientes $m_{ij}m_{kj}^{-1}$, $1 \leq j \leq v$, contiene a cada elemento de W exactamente $\frac{v}{w}$ veces. Se dice que $GH(w, \frac{v}{w})$ es normalizada si la primera fila y la primera columna sólo están formadas por el elemento identidad de W. Un tratamiento similar al realizado en esta memoria para el cálculo de matrices de Hadamard podría ser igualmente interesante para la búsqueda de matrices de Hadamard generalizadas, por su aplicación a la construcción de códigos correctores de errores.

Referencias

[1] Álvarez V.: *Complejos reducidos de resoluciones y perturbación homológica*, Tesis Doctoral (2001).

[2] Álvarez V., Armario J.A., Frau M.D. y Real P.: *An algorithm for computing cocyclic matrices developed over some semidirect products*, Proceedings AAECC'14, Eds. A. Betten, A. Kohnert, R. Lave, A. Wassermann, Springer Lecture Notes in Computational Science, Springer–Verlag, Heidelberg (2001).

[3] Álvarez V., Armario J.A. y Real P.: *On the homology of semi-direct products of groups*, Colloquium on Topology, Gyula, Hungary (1998).

[4] Armario J.A.: *Estructuras multiplicativas y homología de fibrados*, Tesis doctoral (1999).

[5] Assmus E.F. y Key J.D.: *Designs and their codes*, Cambridge University Press, **103** (1992).

[6] Baliga A. y Chua J.: *Self-dual codes using image restoration techniques*, Proceedings AAECC'14, Eds. A. Betten, A. Kohnert, R. Lave, A. Wassermann, Springer Lecture Notes in Computational Science, Springer–Verlag, Heidelberg (2001).

[7] Baliga A. y Horadam K.J.: *Cocyclic Hadamard matrices over* $\mathbb{Z}_t \times \mathbb{Z}_2^2$, Australas. J. Combin., **11**, pp. 123–134 (1995).

[8] Barrat M.G., Gugenheim V.K.A.M. y Moore J.C.: *On semisimplicial fibre bundles*, Am. J. Math., **81**, pp. 639–657 (1959).

[9] Baues H.J. y Lemaire J.M.: *Minimal models in homotopy theory*, Math. Ann., **225**, pp. 219–225 (1977).

[10] Beth T., Jungnickel D. y Lenz H.: *Design theory*, Vol. 1, 2^{nd} edition, Cambridge University Press (1999).

[11] Bose R.C. y Shrikhande S.S.: *A note on a result in the theory of code construction*, Inform. and Control, **2**, pp. 183–194 (1959).

[12] Bosma W., Cannon J. y Playoust C.: *The* MAGMA *algebra system I*, The user language computational algebra and number theory, London (1993). J. Symb. Computation, **24**, (**3-4**), pp. 235–265 (1997).

[13] Brown E.H.: *Twisted tensor products I*, Annals of Math., **69** pp. 223–246 (1959).

[14] Brown R.: *The twisted Eilenberg-Zilber theorem*, Celebrazioni Archimedae del Secolo XX, Simposio di Topologia, pp. 34–37 (1967).

[15] Brown K.S.: *Cohomology of groups*, Graduate Texts in Math., **87**, Springer-Verlag, New York (1982).

[16] Butson A. T.: *Generalised Hadamard matrices*, roc. Amer. Math. Soc. **13**, pp. 864–898 (1962).

[17] Cameron P.J.: *Combinatorics: topics, techniques, algorithms*, Cambridge University Press (1994).

[18] Cannon P.J. y Playoust C.: *MAGMA: a new computer algebra system*, Euromath Bull., **2** (**1**), pp. 113–144 (1996).

[19] Cartan H. y Eilenberg S.: *Homological Algebra*, Princeton University Press, Princeton (1956).

[20] C.H.A.T.A. Group: *Computing small 1-homological models for CDGAs*, Proceedings of CASC'00, Samarcanda, Uzbekistan, Eds. V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov, Springer-Verlag, pp. 87–100 (2000).

[21] Cooper J. y Wallis J.: *A construction for Hadamard arrays*, Bull. Austral. Math. Soc., **7**, pp. 269–277 (1972).

[22] Decker C.J.: *The integral homology algebra of an Eilenberg-Mac Lane space*, Ph. d. thesis, University of Chicago (1974).

[23] de Launey W.: *On the construction of n-dimensional designs from 2-dimensional designs*, Australas. J. Combin., **1**, pp. 67–81 (1990).

[24] de Launey W. y Horadam K.J.: *Cocyclic development of designs*, J. Algebraic Combin., **2** (3), pp. 267–290 (1993). *Erratum*: J. Algebraic Combin., (1), pp. 129 (1994).

[25] de Launey W. y Horadam K.J.: *A weak difference set construction for higher dimensional designs*, Designs, Codes and Cryptography, **3**, pp. 75–87 (1993).

[26] de Launey W. y Horadam K.J.: *Generation of cocyclic Hadamard matrices*, chap. 20 in Computational Algebra and Number Theory, eds. W. Bosma and van der Poorten, Mathematics and its Applications 325, Kluwer Academic, pp. 279–290 (1995).

[27] Dousson X., Rubio J. y Sergeraert F.: *Kenzo Program*, http://www-fourier.ujf-grenoble.fr/~sergerar/Kenzo/

[28] Drake D.A.: *Partial λ-geometries and generalised Hadamard matrices*, Canad. J. Math., **31**, pp. 617–627 (1979).

[29] Eckmann B.: *Der Cohomologie-Ring einer beliebigen Gruppe*, Comment. Math. Helv., **18**, pp. 232–282 (1946).

[30] Eilenberg S.: *Singular homology theory*, Ann. of Math, **45**, pp. 407–447 (1944).

[31] Eilenberg S. y Mac Lane S.: *Relations between homology and homotopy groups*, Proc. NAS USA, **29**, pp. 155–158 (1943).

[32] Eilenberg S. y Mac Lane S.: *Relations between homology and homotopy groups of spaces*, Ann. of Math., **46**, pp. 480–509 (1945).

[33] Eilenberg S. y Mac Lane S.: *General theory of natural equivalences*, Trans. AMS, **58**, pp. 231–294 (1945).

[34] Eilenberg S. y Mac Lane S.: *On the groups $H(\pi, n)$, I*, Annals of Math. **58**, pp. 55-106 (1953).

[35] Eilenberg S. y Mac Lane S.: *On the groups $H(\pi, n)$ II*, Annals of Math. **66**, pp. 49–139 (1954).

[36] Eilenberg S. y Moore J.C.: *Limits and spectral sequences*, Top., **1**, pp. 1–24 (1962).

[37] Eilenberg S. y Moore J.C.: *Homology and fibrations I. Coalgebras, cotensor product and its derived functors*, Comm. Math. Helv., **40**, pp. 199–236 (1966).

[38] Eilenberg S. y Zilber J.A.: *On products of complexes*, Am. J. Math. **75**, pp. 200–204 (1953).

[39] Elias P.: *Coding for noisy channels*, IRE Convention Record **4**, pp. 46–47 (1955).

[40] Flannery D.L.: *Transgression and the calculation of cocyclic matrices*, Australas. J. Combin., **11**, pp. 67–78 (1995).

[41] Flannery D.L.: *Calculation of cocyclic matrices*, J. Pure Appl. Algebra 112 (2), pp. 181–190 (1996).

[42] Flannery D.L.: *Cocyclic Hadamard matrices and Hadamard groups are equivalent*, J. Algebra **192**, pp. 749–779 (1997).

[43] Flannery D.L. y O'Brien E.A.: *Computing 2-cocycles for central extensions and relative difference sets*, Comm. Algebra, **28 (4)**, pp. 1939–1955 (2000).

[44] González–Díaz R. y Real P.: *A combinatorial method for computing Steenrod squares*, J. of Pure Appl. Alg. (1999).

[45] Grabmeier J. y Lambe L.A.: *Computing Resolutions Over Finite p-Groups*, Proceedings ALCOMA'99, Eds. A. Betten, A. Kohnert, R. Lave, A. Wassermann, Springer Lecture Notes in Computational Science and Engineering, Springer-Verlag, Heidelberg (2000).

[46] Gugenheim V.K.A.M.: *On Chen's iterated integrals*, Illinois J. Math., pp. 703–715 (1977).

[47] Gugenheim V.K.A.M. y Lambe L.A.: *Perturbation theory in Differential Homological Algebra, I*, Illinois J. Math. **33**, pp. 556–582 (1989).

[48] Gugenheim V.K.A.M., Lambe L.A. y Stasheff J.D.: *Perturbation theory in Differential Homological Algebra II*, Illinois J. Math. **35** (**3**), pp. 357–373 (1991).

[49] Gugenheim V.K.A.M. y May P.J.: *On the theory and application of differential torsion products*, Memo. Amer. Math. Soc., **142** (1974).

[50] Gugenheim V.K.A.M. y Moore J.C.: *Acyclic models and fibre spaces*, Trans. AMS, **85**, pp. 265–306 (1957).

[51] Gugenheim V.K.A.M. y Stasheff J.D.: *On perturbations and A_∞ structures*, Bull. Soc. Math. de Belg. **38**, pp. 237–246 (1986).

[52] Hadamard J.: *Résolution d'une question relative aux déterminants*, Bull. Sci. Math. **17** (parte 1), pp. 240–246 (1893).

[53] Halperin S.: *Finiteness in minimal models*, Trans. Amer. Math. Soc., **230**, pp. 173–199 (1977).

[54] Halperin S.: *Rational fibrations, minimal models, and fibirngs of homogeneous spaces*, Trans. Amer. Math. Soc., **244**, pp. 199–224 (1978).

[55] Halperin S.: *Lectures on minimal models*, Mémoire de la Société Mathématique de France (N.S.), **9/10** (1983).

[56] Hammer J. y Seberry D.R.:*Higher dimensional orthogonal desings and Hadamard matrices II*, Congr. Numer., 27 pp. 23-29 (1979).

[57] Hamsher R.M.: *Eilenberg-Mac Lane algebras and their computation. An invariant description of $H(\Pi, 1)$*, Ph. d. thesis, University of Chicago (1973).

[58] Hedayat A. y Wallis W.D.: *Hadamard matrices and their applications*, The Annals of Statistics **6**, (**6**), pp. 1184–1238 (1978).

[59] Hilton P.J. y Stammbach U.: *A Course in Homological Algebra*, Graduate Texts in Math. 4, Springer-Verlag, New York, (1971).

[60] Hochschild G. y Serre J.P.: *Cohomology of group extensions*, TAMS **74**, pp. 110–134 (1953).

[61] Hoffman D.G., Leonard D.A., Linder C.C., Phelps K.T., Rodger C.A. y Wall J.R.: *Coding Theory. The Essentials*, Marcel Dekker (1992).

[62] Holland J.*Adaptation in Natural and Artificial Systems*, University of Michigan Press (1975).

[63] Horadam K.J.: *Progress in cocyclic matrices*, Congressus Numerantium **118**, pp 161-171 (1996).

[64] Horadam K.J.: *An introduction to cocyclic generalised Hadamard matrices*, Royal Melbourne Institute of Technology, Research Report No.11 (1999).

[65] Horadam K.J. y Lin C.:*Construction of proper higher dimensional Hadamard matrices from perfect binary arrays*, JCMCC, **28**, pp. 237-248 (1998).

[66] Horadam K.J. y Perera A.A.I.: *Codes from cocycles*, Lecture Notes in Computer Science, Springer–Verlag, Berlin–Heidelberg–New York, **1255**, pp. 151–163 (1997).

[67] Horadam K.J. y Udaya P.: *Cocyclic Hadamard codes*, IEEE Trans. Inform. Theory **46** (4), pp. 1545–1550 (2000).

[68] Huebschmann J.: *Perturbation theory and free resolutions for nilpotent groups of class 2*, J. Alg. **126**, pp. 348–399 (1989).

[69] Huebschmann J.: *Cohomology of nilpotent groups of class 2*, J. Alg. **126**, pp. 400–450 (1989).

[70] Huebschmann J.: *Cohomology of finitely generated abelian groups*, L'Enseignement Mathématique **t. 37** pp. 61–71 (1991).

[71] Huebschmann J.: *Cohomology of metacyclic groups*, Transactions of the American Mathematical Society **328**, **1**, pp. 1–72 (1991).

[72] Huesbschmann J. y Kadeishvili T.: *Small models for chain algebras*, Math. Z. **207**, pp. 245–280 (1991).

[73] Hurewicz W.: *Beiträge zur Topologie der deformationen*, Proc. Akad. Amsterdam, **38**, pp. 112–119, 521–538 (1935); **39**, pp. 117–125, 215–224 (1936).

[74] Ito N.: *On Hadamard groups*, J. Algebra **168**, pp. 981–987 (1994).

[75] Jiménez M.J.: *A_∞-estructuras y perturbación homológica*, Tesis Doctoral. Universidad de Sevilla (2003).

[76] Kadeishvily T.V.: *On the homology theory of fibre spaces*, Uspekhi Mat. Nauk., **35** (**3**), pp. 183–188 (1980).

[77] Lambe L.A.: *Algorithms for the homology of nilpotent groups*, Conf. on applications of computers to Geom. and Top., Lecture Notes in Pure and Applied Math. **114**, Marcel Dekker Inc., N.Y. (1989).

[78] Lambe L.A.: *Resolutions via homological perturbation*, J. Symbolic Comp. **12**, pp. 71–87 (1991).

[79] Lambe L.A.: *Homological perturbation theory, Hochschild homology and formal groups*, Proc. Conference on Deformation Theory and Quantization with Applications to Physics, Amherst, MA, June 1990, Cont. Math. **134**, A.M.S, pp. 183–218 (1992).

[80] Lambe L.A.: *Resolutions which split off of the bar construction*, J. Pure Appl. Alg. **84**, pp. 311–329 (1993).

[81] Lambe L.A.: *Next generation computer algebra systems AXIOM and the scraptchpad concept: applications to research in algebra*, Collection "Analysis, algebra and computers in mathematical research, Lulea, pp. 201–222 (1992). Lect. Notes in Pure and Appl. Math., Dekker, **156** (1994).

[82] Lambe L.A.: *An algorithm for calculating cocycles*, Preprint, Department of Mathematics and Centre for Innovative Computation, University of Wales, Bangor (1997).

[83] Lambe L.A. y Stasheff J.D.: *Applications of perturbation theory to iterated fibrations*, Manuscripta Math. **58**, pp. 367–376 (1987).

[84] Leray J.: *L'anneau d'une representation*, C.R. Acad. Paris, **222**, pp. 1366–1368 (1946).

[85] Levenshtein V.I.: *Aplication of the Hadamard matrices to a problem in coding*, Problems of Cybernetics, **5**, pp. 166–184 (1964).

[86] Lyndon R.: *The cohomology theory of group extensions*, Duke Math. J., **15**, pp. 271–292 (1948).

[87] Mac Lane S.: *Homology*, Classics in Mathematics, Springer-Verlag, Berlin (1995). Reimpresión de la edición de 1975.

[88] MacEliece R.J.: *A public-key cryptosystem based on algebraic coding theory*, DSN Progress Report 42-4 (1978).

[89] MacWilliams F.J. y Sloane N.J.A.: *The theory of error-correcting codes*, North Holland, New York (1977).

[90] May J.P.: *The cohomology of restricted Lie algebras and of Hopf algebras*, J. Alg., **3**, pp. 123–146 (1966).

[91] May J.P.: *Simplicial objects in Algebraic Topology*, Van Nostrand, Princenton (1967). Chicago Lectures in Mathematics, The University of Chicago Press, Chicago and London (1992).

[92] Paley R.E.A.C.: *On orthogonal matrices*, J. Math. and Physics, **12**, pp. 311–320 (1933).

[93] Plotkin M.: *Binary codes with soecified minimum distances*, IEEE Trans. Information Theory, **6**, pp. 445–450 (1960).

[94] Pretzel O.: *Error-Correcting Codes and Finite Fields*, Oxford (1992).

[95] Prouté A.: *Algébres differentielles fortement homotopiquement associatives*, Thèse de Mathematiques, Université Paris VII (1984).

[96] Quillen D.: *Homotopical Algebra*, Lecure Notes in Mathematics, Springer, **43** (1967).

[97] Quillen D.: *Rational homotopy theory*, Ann. of Math., **90**, pp. 205–295 (1969).

[98] Real P.: *Homological Perturbation Theory and Associativity*, Homology, Homotopy and Applications, **2**, **5**, pp. 51–88 (2000).

[99] Rubio J.: *Homologie Effective des espace de lacets itérés: un logiciel*, Tesis Doctoral. Universidad Joseph Fourier, Grenoble, Francia (1991).

[100] Rubio J.: *Integrating functional programming and symbolic computation*, Mathematics and computers in simulation, **44**, pp. 505-511 (1997).

[101] Rubio J. y Sergeraert F.: *Homologie effective et suites spectrales d'Eilenberg-Moore*, C.R. Acad. Sc. Paris, **306**, pp. 723–726 (1988).

[102] Scarpis U.: *Sui determinants di valore massime*, Rend. R. Inst. Lombardo Sci. e Lett (2), **31**, pp. 1441–1446 (1898).

[103] Schörnert M. et al.: *Groups, Algorithms and Programming*, Technical report, LDFM, Aachen (1995).

[104] Shlichta P.J.: *Tree and four-dimensional Hadamard matrices*, Bull. Amer. Phys. Soc, ser.1, **16**, pp. 825–826 (1971).

[105] Shlichta P.J.:*Higer dimensional Hadamard matrices*, IEEE Trans. Inform. Theory, **IT-25**, pp. 566–572 (1979).

[106] Sergeraert F.: *Homologie effective I,II*, C.R. Acad. Sc. Paris, **304** (**11** y **12**), pp. 279–281 y 319–321 (1987).

[107] Sergeraert F.: *The computability problem in Algebraic Topology*, Advances in Math., **1104**, pp. 1–29 (1994).

[108] Serre J.P.: *Cohomologies des extensions de groupes*, C.R. Acad. Sci. Paris, **226**, pp. 303-305 (1948).

[109] Serre J.P.: *Homologie singulière des espaces fibrés*, Ann. of Math., **54**, pp. 425–505 (1951).

[110] Shannon C.E.: *A mathematical theory of communication*, Bell Syst. Tech. J. **27**, pp. 379–423 (1948).

[111] Shih W.: *Homologie des espaces fibrés*, Inst. Hautes Etudes Sci. **13**, pp. 293–312 (1962).

[112] Shlichta P.J.: *Three and four-dimensional Hadamard matrices*, Bull. Amer. Phys. Soc., ser. 11, **16**, pp. 825–826 (1971).

[113] Shlichta P.J.: *Higher dimensional Hadamard matrices*, IEEE Trans. Inform. Theory, IT-**25**, pp. 566–572 (1979).

[114] Stasheff J.D.: *Homotopy associativity of a H-space I,II*, Trans. Amer. Math. Soc. **108**, pp. 275–292 y 293–312 (1963).

[115] Stasheff J.D.: *H-spaces from a homotopy point of view*, Lecture Notes in Math. **161**, Springer, N.Y. (1970).

[116] Stewart I.: *De aquí al infinito: las Matemáticas de hoy*, Ed. Crítica Grijalbo Mondadori (1998).

[117] Sullivan D.: *Differential forms and the topology of manifolds*, Proc. Inter. Conf. on Manifolds and Related Topics in Topology, Tokyo, Uni. Tokyo Press (1973).

[118] Sullivan D.: *Cartan–de Rham homotopy theory*, Astérisque, **32–33**), pp. 227–254 (1976).

[119] Sullivan D.: *Infinitesimal computations in topology*, Publ. I.H.E.S., **47**, pp. 269–331 (1977).

[120] Sylvester J.J: *Thougths on inverse orthogonal matrices, simultaneous sign-successions, and tesselated pavements in two oe more colors, with applications to Newton's rule, ornamental tile-work, and the theory of numbers*, Phil. Mag. (4), **34**, pp. 461–475 (1867).

[121] Turyn R.J.: *An infinite class of Williamson matrices*, J. Combin. Theory Ser. A **12**, pp. 319–321 (1972).

[122] Turyn R.J.: *Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression and surface wave encoding*, J. Combinatorial Theory (A), **16**, pp. 313–333 (1974).

[123] Veblen O.: *Analisis situs*, A.M.S. Publications, **5** (1931).

[124] Wallis J.: *Hadamard matrices of order* $28m$, $36m$ *and* $44m$, J. Combinatorial Theory (A), **15**, pp. 323–328 (1973).

[125] Wallis W.D.: *Combinatorial designs*, Marcel Dekker, New York (1988).

[126] Weibel C.A.: *An introduction to homological algebra*, Cambridge studies in advanced mathematics, Cambridge University Press, **38** (1994).

[127] Welsh D.: *Codes and Cryptography*, Oxford Science Publications, Oxford University Press (1988).

[128] Wicker S.B.: *Error control systems for digital communication and storage*, Prentice Hall Inc., New Jersey (1995).

[129] Williamson J.: *Hadamard's determinant theorem and the sum of four squares*, Duke Math. J., **11**, pp. 65–81 (1944).