Conceptos básicos sobre isocriptografía siguiendo el modelo MCIM

Falcón Ganfornina, R.M. * Núñez Valdés, J. †

Resumen

Una de las aplicaciones prácticas de la isoteoría de Santilli que ha surgido en los últimos años se refiere al campo de la criptografía. Generalizando la unidad utilizada en los criptogramas se originan una nueva clase de estos, denominada isocriptogramas. Se presentarán las nociones básicas necesarias para originar tales estructuras, mostrando algunos ejemplos al respecto. Se tratarán haciendo uso de los últimos modelos de construcción de isotopías, lo que permitirá estudiar la isocriptografía de Santilli como caso particular.

1 Introducción

En 1978, Santilli propuso una generalización de la teoría convencional de Lie haciendo uso de isotopías, dando lugar a la *isoteoría de Lie-Santilli* (véase [**3**]). Para ello consideró que la unidad básica I de toda estructura matemática puede sufrir dependencia en varios factores externos del sistema en el que nos encontremos (coordenadas, velocidad, tiempo, densidad, temperatura, etc.), dando lugar a una isounidad $\widehat{I} = \widehat{I}(x, \overset{\bullet}{x}, \overset{\bullet\bullet}{x}, ..., \mu, \tau, ...)$.

Esta dependencia puede englobar a su vez el carácter no asociativo o no lineal de ciertas aplicaciones físicas (en Dinámica de particulas o Mecánica Cuántica - véase [**6**]), que convencionalmente han hecho uso de la teoría de Lie, de carácter asociativo y lineal. No obstante, para que esta generalización sea coherente,

*Departamento de Geometría y Topología (Facultad de Matemáticas), Universidad de Sevilla, e-mail: rafalgan@us.es

†Departamento de Geometría y Topología (Facultad de Matemáticas), Universidad de Sevilla, e-mail: jnvaldes@us.es

Actas de las IV Jornadas de Matemática Discreta y Algorítmica. Cercedilla (Madrid), 2004, pp. 299 - 306.
ISBN: 84 - 86189 - 98 - 5.

Santilli junto a otros autores han realizado una construcción metódica que generaliza las estructuras matemáticas más importantes, dando lugar a las denominadas *isoestructuras matemáticas* (véanse **[4]**, **[5]**, **[7]**)).

Pese a que la línea de investigación preferente en isoteoría ha sido la relativa a sus aplicaciones prácticas en Física y Química, también se han ido tratando a su vez otros campos de estudio. En concreto, en el Apéndice 2C de la segunda edición del monográfico **[6]**, se introduce una nueva clase de criptogramas, cuya idea principal es utilizar isotopías de tipo I, para generalizar cualquier criptograma numérico existente basado en la unidad convencional $+1$ o bien $I = diag(+1, ..., +1)$ y en el producto usual asociativo $a \times b$, dando lugar de esta forma a una nueva estructura basada en una isounidad $\widehat{I}$ y en el isoproducto $a\widehat{\times}b = a \times T \times b$, donde $\widehat{I}$ puede ser cualquier número no nulo del conjunto de partida.

Posteriormente en 2002, Jiang ha mostrado en **[2]** algunos fundamentos básicos de lo que se conoce ya como *teoría isocriptográfica de Santilli*, tratando varios aspectos en isocriptografía de clave secreta y de clave pública, como cifrado en bloque, exponenciación o esquema RSA. Las ventajas que indica respecto a la criptografía convencional son las siguientes:

a) Incremento en la dificultad para resolver criptogramas, al disponer de una infinidad de unidades básicas a utilizar.

b) Capacidad de computerizar el cambio de unidad sin necesidad de alterar los criptogramas de partida.

c) Disminución de costes frente a aumento de seguridad, incluso en criptogramas simples.

Jiang se basa en el modelo de isotopía de 1978. Ahora bien, en 2001, se desarrolló un modelo de construcción más general que enfatiza las propiedades de las operaciones que intervienen en la generalización de las estructuras de partida. Se trata del modelo de construcción del isoproducto basado en la multiplicación (m.c.i.m.) dado en **[1]**.

Por todo esto parece recomendable la revisión del estudio de Jiang a partir del m.c.i.m., analizando la posible generalización de los resultados ya obtenidos sobre isocriptografía de Santilli.

2 Preliminares

Se denomina *isotopía* o *levantamiento isotópico* a toda correspondencia entre una estructura matemática fijada y otra del mismo tipo, esto es, tal que verifique sus mismas propiedades. Obsérvese que según esta definición, una isotopía puede no ser una aplicación. La nueva estructura obtenida se denomina *isoestructura*.

El modelo de isotopía de Santilli de 1978 se basa en la generalización de la unidad de partida: $I \to \widehat{I} = \widehat{I}(x, \overset{\bullet}{x}, \overset{\bullet\bullet}{x}, ..., \mu, \tau, ...)$. En particular, fijada una estructura matemática cualquiera E, dotada de un producto interno $\times$, se considera un conjunto $V \supseteq E$, dotado de una operación asociativa $*$ y tal que existen $I, \widehat{I}, T \in V$, donde $I \in E$ es la unidad de $*$ en V y $T = \widehat{I}^{-I}$. A V, T e $\widehat{I}$ se les conoce respectivamente como *conjunto general, elemento isotópico e isounidad* de la isotopía en cuestión. De esta forma, se definen los elementos de la isoestructura matemática $\overline{\widehat{E}}$ dotada del isoproducto $\overline{\widehat{\times}}$ de unidad $\widehat{I}$ como :

$$E \to \overline{\widehat{E}} : x \to \overline{\widehat{x}} = x * \widehat{I} \ , \qquad a \overline{\widehat{\times}} b = a * T * b, \text{ para todos } a, b \in \overline{\widehat{E}}.$$

El m.c.i.m. de 2001 generaliza la construcción anterior, haciendo uso de tantas isounidades y operaciones similares a $*$, como operaciones tenga la estructura de partida. De una manera esquemática, toda isotopía puede venir reflejada entonces a partir del siguiente diagrama:

$$\begin{array}{ccc}
\text{Nivel convencional} & \longrightarrow & \begin{array}{c}\text{Nivel general}\\ (V, *, \star, ...)\\ \cup\end{array}\\
(E, +, \times, ...) & & (E, *, \star, ...)\\
\downarrow & \sharp & \downarrow \mathbf{I}\\
\text{Nivel de Proyección} & \overset{\pi}{\longleftarrow} & \text{Nivel isotópico}\\
(\overline{\widehat{E}}, \overline{\widehat{+}}, \overline{\widehat{\times}}, ...) & & (\widehat{E}, \widehat{+}, \widehat{\times}, ...)
\end{array}$$

El m.c.i.m. impone que $(E, *, \star, ...)$ sea una estructura del mismo tipo que la inicial $(E, +, \times, ...)$, lo que permite en concreto determinar explícitamente los elementos del conjunto general asociado a la isotopía:

$$V = E \cup \overline{\widehat{E}} \cup \{T\} \cup E_T \text{ , donde } E_T = \left\{ a_T = a * T : a \in \overline{\widehat{E}} \right\}.$$

Además, notando por F el conjunto de factores externos de los que depende la isounidad $\widehat{I}$, salvo aquellos que dependen del factor coordenada $(x, \overset{\bullet}{x}, \overset{\bullet\bullet}{x}, ...)$, la operación $\overline{\widehat{\times}}$ se define como:

$$\left(a * \widehat{I}(a, F_a)\right) \overline{\widehat{\times}} \left(b * \widehat{I}(b, F_b)\right) = (a * b) * \widehat{I}\left(a * b, \Phi_{\times}(F_a, F_b)\right).$$

Donde la aplicación $\Phi_{\times} : F \times F \to F : (F_{\alpha}, F_{\beta}) \to \Phi_{\times}(F_{\alpha}, F_{\beta})$, debe estar prefijada de antemano.

3 Isocriptosistemas

Fijemos un criptosistema (M, C, K, E, D), donde los espacios indicados se refieren respectivamente a los espacios de mensajes, textos cifrados o criptogramas, claves, transformaciones de cifrado y tranformaciones de descifrado, correspondientes a tal criptosistema. Para simplificar nuestro estudio, consideraremos la equivalencia numérica asociada a M en la forma $\mathbb{Z}/\mathbb{Z}_n$ dotado de las operaciones $+$ y $\times$ usuales, en caso de estar asociado a un alfabeto de n letras.

Basamos M por tanto en el $\mathbb{Z}$-módulo $(\mathbb{Z}, +, \times)$, que está incluido a su vez en el cuerpo real $(\mathbb{R}, +, \times)$. De tal forma, que si realizamos un levantamiento isotópico del cuerpo señalado, mediante un cambio de unidad, este hecho afectará a su vez a la estructura de $\mathbb{Z}$ y por tanto a M.

Para simplificar, supondremos tal isotopía basada en un conjunto general $V \supseteq \mathbb{R}$, dotado de un par de leyes internas asociativas $\star$ y $*$, de elementos unidades respectivos $S, I \in \mathbb{Z}$ y tal que podemos elegir un elemento $T \in V$, con inversa $\widehat{I} = T^{-I} \in V$. Se define entonces el *isoespacio de mensajes* $\overline{\widehat{M}} = \left\{\widehat{M_i} = M_i * \widehat{I} : M_i \in M\right\} \subseteq V$, que estará dotado del isoproducto $\overline{\widehat{\times}}$, definido como $A \overline{\widehat{\times}} B = A * T * B$, para todos $A, B \in \overline{\widehat{M}}$.

Proposición 3.1. *El isoespacio de mensajes $\overline{\widehat{M}}$ es de hecho un espacio de criptogramas asociado a M.*

Demostración. Basta tener en cuenta que $*$ es asociativa y que $T = \widehat{I}^{-I}$. De esta forma tenemos la transformación de cifrado $E_{\widehat{I}} = \pi \circ \mathbf{I} : M \to \overline{\widehat{M}} : A \to \overline{\widehat{A}} = A * \widehat{I}$ y la transformación de descifrado $D_T : \overline{\widehat{M}} \to M : A \to A * T$.

La clave de cifrado vendría dada entonces por el par $(\widehat{I},*)$ y la de descifrado por el par $(T,*)$. $\square$

Hay que tener en cuenta que la aritmética del isoespacio de mensajes no es ya la usual. Veamos un ejemplo al respecto:

Ejemplo 3.2. Sea la equivalencia numérica de un alfabeto de 27 letras, $M = \mathbb{Z}/\mathbb{Z}_{27}$ y fijemos $T \in \mathbb{R}$ no nulo, siendo $\widehat{I} = T^{-1}$. Consideremos el levantamiento isotópico del cuerpo real $(\mathbb{R},+,\times)$ referente a los elementos de isotopía principales $*_{|_{\mathbb{R}}} \equiv \times$ e $\widehat{I}$ y secundarios $\star \equiv +$ y $\widehat{S} = 0$. Esto es, $(\widehat{\mathbb{R}},\widehat{+},\widehat{\times}) = (\mathbb{R},+,\widehat{\times})$, donde $a\widehat{\times}b = a \times T \times b$, para todos $a,b \in \mathbb{R}$.

La aritmética modular cambia entonces. En particular, $(\mathbb{Z},+,\widehat{\times})$ no tiene estructura de $\mathbb{Z}$-módulo y deberemos trabajar con $(\widehat{\mathbb{Z}},+,\widehat{\times})$, que tiene estructura de $\widehat{\mathbb{Z}}$-módulo.

Consideramos entonces $*$ definida de tal forma que para todo $a \in \mathbb{Z}$:
$(a+\mathbb{Z}_{27}) * \widehat{I} = \left(a * \widehat{I}\right) + \widehat{\mathbb{Z}}_{27*\widehat{I}}$.

En estas condiciones, el isoespacio de mensajes resulta $\widehat{M} = \widehat{\mathbb{Z}}/\widehat{\mathbb{Z}}_{27\widehat{I}}$, que consta de 27 elementos, pues fijados $a,b \in \mathbb{Z}$, se tiene que $a*\widehat{I}+\widehat{\mathbb{Z}}_{27\widehat{I}} = b*\widehat{I}+\widehat{\mathbb{Z}}_{27\widehat{I}}$ si y sólo si existe $k*\widehat{I} \in \widehat{\mathbb{Z}}$ tal que $a*\widehat{I} = b*\widehat{I}+(k*\widehat{I})\widehat{\times}(27\widehat{I})$. O equivalentemente, $(a-b)\widehat{I} = 27k\widehat{I}$.

Notaremos por $mod\ 27$ y $\widehat{mod}\ 27\widehat{I}$ a la congruencia usual en $\mathbb{Z}$ y la referente a $\widehat{Z}$, respectivamente. Diferenciaremos con ello ambos conceptos, resultando que el isoproducto $\widehat{\times}$ de unidad $\widehat{I}$, está definido para todos $a,b \in \mathbb{Z}$ como: $a * \widehat{I}(\widehat{mod}\ 27\widehat{I})\ \widehat{\times}\ b * \widehat{I}(\widehat{mod}\ 27\widehat{I}) = (a \times b) * \widehat{I}\ (\widehat{mod}\ 27\widehat{I})$. Además, se tiene que $a * \widehat{I} = b * \widehat{I}\ (\widehat{mod}\ 27\widehat{I})$ si y sólo si $a = b\ (mod\ 27)$.

Con lo anterior queda probado que $\widehat{M}$ puede considerarse como cifrado de M, habiendo cambiado para ello sólamente la unidad del espacio de partida. Obsérvese que en caso de no atender al producto $\widehat{\times}$, lo que se ha realizado es una transformación afín. No obstante, una de las ventajas que tiene la construcción de isocriptogramas es que la isounidad $\widehat{I}$ puede sufrir dependencia en factores

externos a la estructura matemática en sí. En particular, podemos imponer una dependencia en el factor tiempo. Así por ejemplo podemos considerar el isocuerpo asociado a $(\mathbb{R},+,\times)$ a partir de una isotopía asociada a $\widehat{S}=0, \star\equiv +, *_{|_{\mathbb{R}}}\equiv \times$ e $\widehat{I}=\widehat{I}(x,t)$. Lograremos de esta forma que el isoespacio de mensajes varíe en el tiempo, al igual que las claves correspondientes $(\widehat{I}(x,t),*)$ y $(T(x,t),*)$, lo que aumenta considerablemente la dificultad en resolver isocriptosistemas asociados a este tipo de isotopías, en caso de no poseer ninguna de tales claves. Veamos un ejemplo concreto:

Ejemplo 3.3. Supongamos que en el levantamiento isotópico del cuerpo real $(\mathbb{R},+,\times)$ utilizamos como isounidad a $\widehat{I}=\widehat{I}(x,t)=x^2+\frac{5t}{x}$, con el tiempo $t\in F=\mathbb{N}$, como factor externo. Supondremos además $*_{|_{\mathbb{R}}}\equiv\times$, $\star\equiv +$ y $\widehat{S}=0$. Será entonces $T=\widehat{I}^{-1}=T(x,t)=\frac{(x-5t)^{1/3}}{x}$.

Para evitar singularidades, consideraremos que el producto $\widehat{\overline{\times}}$ se define en tiempos paralelos, usando para ello la aplicación $\Phi_{\times}(t_0,t_0)=t_0$. Resulta entonces como estructura matemática la terna $(\widehat{\overline{\mathbb{R}}},\widehat{\overline{+}},\widehat{\overline{\times}})=(\mathbb{R},+,\widehat{\overline{\times}})$, donde fijado un instante t_0, se define el producto $a\,\widehat{\overline{\times}}\,b=(a-5t_0)^{1/3}\times b$, para todos $a,b\in\mathbb{R}$.

A la hora de obtener el isocriptograma asociado a esta isotopía, deberemos trabajar con la transformación de cifrado $E_{\widehat{I}}:x\to\widehat{\overline{x}}=x^3+5t$, donde $x\in M$ (el espacio de mensajes correspondiente) y t será tratado como el tiempo pasado a partir del instante inicial prefijado t_0 en el que se manda el mensaje , obteniéndose de esta manera un cifrado cuyo contenido varía en el tiempo. A través de un canal seguro, el receptor del mensaje debe obtener por tanto la clave $(\widehat{I},*)$. De esta forma, obtendrá como transformación de descifrado $D_T: x\to D_T(x)=(x-5t)^{1/3}$.

Otro aspecto a destacar en el uso de isocriptogramas es la utilización de una nueva aritmética en cada caso concreto, al cambiar la estructura del cuerpo base con el que se trabaja usualmente. Esto puede aprovecharse si al isoespacio de mensajes $\widehat{\overline{M}}$ se le aplica a su vez claves de K, que continuarían el proceso de cifrado del mensaje inicial, si bien atendiendo a la definición de $\widehat{\overline{\times}}$. Así por ejemplo podemos considerar:

a) **Cifrado en flujo:** En particular, cualquier cifrador por sustitución que se pueda usar en $\mathbb{Z}/\mathbb{Z}_{27}$ referente a $\times$, puede usarse también en $\widehat{\overline{\mathbb{Z}}}/\widehat{\overline{\mathbb{Z}}}_{27\widehat{I}}$ res-

pecto a $\overline{\widehat{\times}}$. Así, fijado $b \in \mathbb{Z}$ tal que $0 < b < 27$, tendremos respectivamente las transformaciones de cifrado y descifrado siguientes:

$$M_i \in M \to C_i = (M_i + b) * \widehat{I}\ (\overline{\widehat{mod}}\ 27\widehat{I})$$
$$C_i \in C \to M_i = (C_i - b * \widehat{I}) * T\ (mod\ 27)$$

b) **Cifrado en bloque:** Puede trabajarse en este caso con matrices no singulares como isounidad, $\widehat{I} \in \mathbf{M}_n(\mathbb{R})$, teniendo presente la variación que se producirá en la definición del producto usual entre matrices:

$$A\overline{\widehat{\times}}B = A*T*B,\ A^{-I} = \widehat{I}*A^{-1}*\widehat{I},\ A\overline{\widehat{\div}}B = A*B^{-1}*\widehat{I},\ \widehat{I}^n = \widehat{I},\ \widehat{I}*T = I$$

c) **Cifrado exponencial:** Téngase en cuenta que para este tipo de cifrado hace falta trabajar con el concepto de primo en el nuevo cuerpo base y por tanto debe estudiarse la divisibilidad atendiendo a $\overline{\widehat{\times}}$. Ahora bien, obsérvese que en $\overline{\widehat{\mathbb{Z}}}$, $\overline{\widehat{a}} = a * \widehat{I}$ divide a $\overline{\widehat{b}} = b * \widehat{I}$ si y sólo si existe $k \in \mathbb{Z}$, tal que $b * \widehat{I} = (k * a) * \widehat{I}$. En particular, en caso de que el levantamiento isotópico utilizado sea inyectivo, la divisibilidad (y con ello el concepto de ser primo) en $\overline{\widehat{\mathbb{Z}}}$ es equivalente a la de $\mathbb{Z}$.

Atendiendo a la clave privada $(\widehat{I}, *)$ del emisor, siendo $p * \widehat{I}$ primo en $\overline{\widehat{\mathbb{Z}}}$, las transformaciones de cifrado y descifrado exponencial vienen dadas por:

$$M_i \in M \to C_i = M_i^{\widehat{I}}\ (\overline{\widehat{mod}}\ p * \widehat{I})$$
$$C_i \in C \to M_i = C_i^{T}\ (\overline{\widehat{mod}}\ p * \widehat{I})$$

Indicar por último que el estudio de levantamientos isotópicos no inyectivos en los que se utilizan isounidades dependientes de factores externos, siendo F no vacío, resulta interesante a la hora de estudiar posibles generalizaciones de resultados referentes a aritmética modular. Así por ejemplo, el cifrado exponencial genérico de tipo RSA, se ve influido, pues en este caso se toma el producto de dos primos en $\overline{\widehat{\mathbb{Z}}}$, $\overline{\widehat{n}} = \overline{\widehat{p}}\overline{\widehat{\times}}\overline{\widehat{q}} = \overline{\widehat{p * q}}$. Es necesario por tanto analizar resultados como la función de Euler en $\overline{\widehat{\mathbb{Z}}}$ y las consecuencias que conlleva la utilización de la isounidad $\widehat{I}$ en este tipo de isotopías.

Agradecimientos

Los autores quieren expresar su agradecimiento al profesor Ruggero Maria Santilli por la útil ayuda aportada.

Referencias

[1] R. M. Falcón Ganfornina, J. N. Valdés, La isoteoría de Santilli, Mathematical Series, International Academic Press, America - Europe - Asia, ISBN 1-57485-055-5 (2001).

[2] C. X. Jiang, Foundations of Santilli's Isonumber Theory. With Applications to New Cryptograms, Fermat's Theorem and Goldbach's Conjecture, International Academic Press, America-Europe-Asia, ISBN 1-58485-056-3 (2002)

[3] R. M. Santilli, *On a possible Lie-admissible covering of the Galilei Relativity in Newtonian Mechanics for nonconservative and Galilei noninvariant systems*, Hadronic J. **1** (1978), 223-423. Addendum, ibid, **1** (1978), 1279-1342.

[4] R. M. Santilli, *Isotopic liftings of contemporary mathematical structures*, Hadronic Journal Suppl. **4** A (1988), 155-266.

[5] R. M. Santilli, *Isotopies of contemporary mathematical structures, I: Isotopies of fields, vector spaces, transformation theory, Lie algebras, analytic mechanics ans space-time symmetries*, Algebras, Groups and Geometries **8** (1991), 169-266.

[6] R. M. Santilli, Elements of Hadronic Mechanics, Vol. I, *Mathematical Foundations* Second Edition, Kiev, 1995.

[7] G. T. Tsagas and D. S. Sourlas, *Mathematical Foundations of the Lie-Santilli Theory*, Hadronic Press (1993).