mathematics

MDPI

Article

Boolean Functions and Permanents of Sylvester Hadamard Matrices

José Andrés Armario

Departamento de Matemática Aplicada I, Universidad de Sevilla, Avda. Reina Mercedes s/n,
41012 Sevilla, Spain; armario@us.es

Abstract: One of the fastest known general techniques for computing permanents is Ryser's formula. On this note, we show that this formula over Sylvester Hadamard matrices of order 2^m, H_m, can be carried out by enumerating m-variable Boolean functions with an arbitrary Walsh spectrum. As a consequence, the quotient $per(H_m)/2^{2^m}$ might be a measure of the "density" of m-variable Boolean functions with high nonlinearity.

Keywords: permanent; Sylvester Hadamard matrices; Ryser's formula; Boolean functions; Walsh spectrum; high nonlinearity

MSC: 15A15; 05B20; 06E30; 65T50

1. Introduction

The theory of Boolean functions is a fascinating area of research in discrete mathematics with applications to cryptography and coding theory. Claude Shannon's properties of confusion and diffusion are fundamental concepts for achieving security in cryptosystems. The notion of diffusion is related to the degree to which the influence of a single input plaintext bit is spread throughout the resulting ciphertext, and the notion of confusion is related to the complexity of the relationship between the secret key and ciphertext. Boolean functions with high nonlinearity can be used to provide confusion in block encryption algorithms [1,2]. Nonlinearity is the minimum number of bits which must change in the truth table of a Boolean function to become an affine function. The Walsh transform is the most important mathematical tool for the analysis of cryptographic properties of Boolean functions. The understanding of the Walsh transform of a Boolean function uniquely determines the function; therefore, working fully with the Walsh transform is possible.

Here we study a connection between the Walsh spectrum of m-variable Boolean functions and Ryser's formula of the permanent for Sylvester Hadamard matrices of order 2^m.

In 1812, Cauchy and Binet independently introduced the notion of the permanent as a matrix function.

Definition 1. *Let N be the set $\{1,\dots,n\}$, $(n \in \mathbf{Z}^+)$. The symmetric group S_n is the group of all $n!$ permutations of N. The permanent of an $n \times n$ matrix $A = [a_{ij}]$ is defined by*

$$per\,(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

At first glance, it seems to be a straightforward version of the determinant, but this is a misleading impression. For instance, the determinant of an arbitrary matrix can be evaluated efficiently using Gaussian elimination; however, the computation of the permanent is much more complicated. Valiant [3] proved that it belongs to the class of ♯P-complete problems, which basically means that there is almost no possibility of

check for updates

Citation: Armario, J.A. Boolean Functions and Permanents of Sylvester Hadamard matrices. *Mathematics* **2021**, *9*, 177. https://doi.org/10.3390/math9020177

Received: 27 November 2020
Accepted: 15 January 2021
Published: 17 January 2021

finding a polynomial time deterministic algorithm for computing the permanent in general. Precisely, the central problem studied in arithmetic complexity theory is the permanent versus determinant problem, which is considered the arithmetic analogue of the NP vs. P problem (see [4]).

There are wide applications of the permanent of certain matrices, such as 0,1 and/or sparse matrices with special structures. Especially in combinatorial counting and graph theory [5]. For instance, if G is a balanced (the two parts have equal size) bipartite graph and M_G is its adjacency matrix, the per (M_G) counts perfect matchings in G. Nevertheless, as far as we know, there is not any clear combinatorial interpretation of the permanent of Hadamard matrices. Here we give some ideas towards an interpretation of the permanent of the Sylvester Hadamard matrices in terms of Boolean functions with high nonlinearity.

Notation. Throughout the article, we make use of $-$ for -1 and 1 for $+1$. We write H_m for a Sylvester Hadamard matrix of order 2^m. The cardinality of a set S is denoted $\sharp S$. We use I_n for the identity matrix of order n and M^T for the transpose of M. The Galois field with two elements is denoted by $GF(2)$ and the m-dimensional vector space over $GF(2)$, equipped with the canonical basis by $GF(2)^m$. $\langle g_i, g_j \rangle$ means the usual inner product for $g_i, g_j \in GF(2)^n$.

2. Preliminaries

Basic concepts and results on Hadamard matrices and Boolean functions will be reviewed. We refer the reader to [6] for more details about Hadamard matrices and see [7] and the references therein for some of the theories of Boolean functions.

2.1. Hadamard Matrices

A *Hadamard matrix* H of order n is an $n \times n$ matrix with entries ± 1 and $HH^T = nI$. If a Hadmard matrix has its first row and column all 1*s* are said to be normalized. A Hadamard matrix can always be normalized by multiplying rows and columns by -1 . It is well-known that n can only be either 2 or a multiple of 4 and it is conjectured that Hadamard matrices exist for every $n \equiv 0 \mod 4$ (see [6]).

It was observed by Sylvester in 1867 that, if H is a Hadamard matrix of order n, then

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

is a Hadamard matrix of order $2n$. Matrices of this configuration are called *Sylvester Hadamard* and are defined for all powers of 2. The Sylvester Hadamard matrix of order 2 is given as

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}.$$

Sylvester Hadamard matrices of order 2^k, denoted by H_k, can be formed by $\overbrace{H_1 \times \cdots \times H_1}^{k-copies}$ the Kronecker product of k copies of H_1. These matrices have many interesting properties (see [8]), for instance $H_m = [(-1)^{\langle g_i, g_j \rangle}]_{g_i, g_j \in GF(2)^m}$.

Two Hadamard matrices H and H' are said to be *equivalent* when one can be acquired from the other by a series of row and/or column interchanges and row and/or column negations. The question of classifying Hadamard matrices of order $n \geq 36$ remains unanswered and only partial results are known.

We recollect that Hadamard proved that $n^{n/2}$ is an upper bound for the absolute value of the determinant of an $n \times n$ matrix with entries from the unic disc, and this bound is attainable by matrices with entries ± 1 if and only if they are Hadamard. However, the permanent of a Hadamard matrix has hardly been worked on, and it is considered a very difficult problem. From what we know, the permanents for all Hadamard matrices of orders smaller or equal to 28 were calculated in [9], but for orders greater than 28 the permanent remains unknown in general. The permanent of the Sylvester Hadamard matrix of order 32 is 6829323892021002240 ([10]).

2.2. Boolean Functions

A *Boolean function* is a mapping

$$f\colon GF(2)^m \to GF(2).$$

We denote by $\mathbf{B}_m$ the set of all m-variable Boolean functions. Since there are 2^m possible inputs of length m, $\sharp\mathbf{B}_m = 2^{2^m}$.

Example 1. *$f(x) = \langle x, g\rangle + c$ where $g \in GF(2)^m$ and $c \in GF(2)$ represent a Boolean function, the so-called* affine function. *In particular, if $c = 0$ then $f(x)$ is called a linear function. We denoted by $\mathbf{A}_m$ the set of m-variable affine functions and $\sharp\mathbf{A}_m = 2^{m+1}$.*

A Boolean function can be displayed in several ways. One prospect is to simply list all values in a fixed order. To this end we denote g_i as the binary representation of the integer $i-1$ with m bits. For instance, $g_1 = (0,0,\ldots,0)$ and $g_2 = (0,\ldots,0,1)$, hence this list $g_1, g_2, \ldots, g_{2^m}$ contains all the elements of $GF(2)^m$. The vector

$$[f(g_1), f(g_2), \ldots, f(g_{2^m})]$$

is called the *truth table* (TT) of a Boolean function f. The *support* of f is the set $S_f = \{g \in GF(2)^m\colon f(g) = 1\}$, and the *weight* of f, $wt(f)$, is the cardinality of the support, i.e., $wt(f) = \sharp S_f$.

The *Hamming distance* between two Boolean functions f and h on $GF(2^m)$ is defined as $wt(f+h)$. The *nonlinearity* of f and denoted by N_f is the minimum distance between f and the set of all affine functions. This concept has several applications in cryptography and coding theory. For instance, nonlinearity can be utilized as a measure of the strength of cryptosystems (see [11]). The Walsh-Hadamard transform is the main tool to study the nonlinearity of Boolean functions, which is defined for an m-variable Boolean function f, such as

$$W_f(g) = \sum_{x \in GF(2)^m} (-1)^{f(x)+\langle x, g\rangle}, \qquad g \in GF(2)^m.$$

The vector $[W_f(g_1), W_f(g_2), \ldots, W_f(g_{2^n})]$ is called the *Walsh spectrum* (WS) of a Boolean function f. Each component $W_f(g)$ of WS is called a *Walsh coefficient*. Its magnitude is the correlation between f and the corresponding linear function $l_g(x) = \langle x, g\rangle$ for $g, x \in GF(2)^m$.

Now, we recall some results involving the Sylvester Hadamard matrix and the WS of a Boolean function.

Proposition 1. *Assuming that f is an m-variable Boolean function and $H_m = [h_{i,j}]$ is the Sylvester Hadamard matrix of order 2^m. The following identities hold,*

1. *$[F(g_1), F(g_2), \ldots, F(g_{2^m})]\, H_m = [W_f(g_1), W_f(g_2), \ldots, W_f(g_{2^m})]$, where $F(g) = (-1)^{f(g)}$.*
2. *$\displaystyle\sum_{i \in S_f} h_{i,k} = 2^{m-1}\delta_{g_1}^{g_k} - \frac{1}{2} W_f(g_k), \quad k = 1, \ldots, 2^m$ where $\delta_{g_1}^{g_k}$ is Kronecker's symbol.*

Proof. The first identity follows from the fact that $H_m = [(-1)^{\langle g_i, g_j \rangle}]^m_{g_i, g_j \in GF(2)}$. For the second, we have to take into account the following facts:

- $W_f(g_k) = \sum_{i \in \bar{S}_f} h_{i,k} - \sum_{i \in S_f} h_{i,k}$ where $\bar{S}_f = \{1, 2, \ldots, 2^m\} \setminus S_f$.
- $\sum_{i=1}^{2^m} h_{i,k} = \begin{cases} 2^m & k = 0 \\ 0 & 0 < k \le 2^m \end{cases}$

□

3. Ryser's Formula for H_m and the Walsh Spectrum of Boolean Functions

H.J. Ryser found the following alternative method to evaluate the permanent of a matrix $A = [a_{ij}]$ of order n,

$$\mathrm{per}\,(A) = (-1)^n \sum_{r=1}^{n} (-1)^r \sum_{\alpha \in Q_{r,n}} \prod_{j=1}^{n} \sum_{i \in \alpha} a_{i,j}, \tag{1}$$

where $Q_{r,n}$ denotes the set of all strictly increasing sequences of r integers taken from the set $\{1, 2, \ldots, n\}$. This is one of the fastest known general algorithms for computing a permanent.By counting multiplications it has an efficiency of $O(2^n n)$ (see pp. 31–11 [12]).

Proposition 2. *Assuming that $H_m = [h_{i,j}]$ is the Sylvester Hadamard matrix of order 2^m, f an arbitary m-variable Boolean function and $\Phi(f) = \prod_{j=2}^{2^m} \sum_{i \in S_f} h_{i,j}$. Then,*

1. $\Phi(f) = -\, 2^{1-2^m} \prod_{j=2}^{2^m} W_f(g_j).$
2. $per\,(H_m) = \sum_{r=1}^{2^m} (-1)^r r \sum_{s_f \in Q_{r,2^m}} \Phi(f).$

Proof. The first identity follows from Proposition 1 and the second one is immediate. □

The following result studies some properties of the function Φ that we will use later.

Lemma 1. *1. Let f be an arbitrary $f \in \mathbf{B}_{m-1}$ and $h = [f|f]$ be the result of concatenating the TT of f to itself. Then $\Phi(h) = 0$.*
2. Let $l \in \mathbf{A}_{m-1}$, $f \in \mathbf{B}_{m-1}$ and $h = [f|l]$. If $\Phi(f) = 0$ then $\Phi(h) = 0$. For instance, $\Phi(h) = 0$ when $wt(f) = 2$ or 4.
3. Let $l(x) = \langle x, g_j \rangle + c \in \mathbf{A}_m$, $f \in \mathbf{B}_m$ and $h = l + f$. Then $\Phi(h) = \frac{(2^m - 2wt(f))}{W_f(g_j)} (-1)^c \Phi(f)$.

Proof. Identities 1 and 2 follow from

$$W_h(g_k) = \begin{cases} W_{f_1}(g_k) + W_{f_2}(g_k) & 1 \le k \le 2^{m-1} \\ W_{f_1}(g_k) - W_{f_2}(g_k) & 2^{m-1} + 1 \le k \le 2^m \end{cases}$$

for $h = [f_1|f_2]$ and $W_l(g_k)$ is null for some $k > 1$. For identity 3, we have to take into account that $W_h(g_k) = (-1)^c W_f(g_j + g_k)$. □

In the sequel, we will try to extract some consequences of the Proposition 2. Firstly, it may help in finding an interpretation of the permanent of H_m in terms of nonlinearity.

Since

$$W_f(g) = 2^m - 2\mathrm{wt}(f + l_g),$$

the nonlinearity of f is computed from the Walsh spectrum by

$$N_f = 2^{m-1} - \frac{1}{2} \max_{g \in GF(2)^m} |W_f(g)|.$$

If a maximum absolute value of W_f occurs at g_k, then either l_{g_k} is the best linear approximation of f (when $W_f(g_k) > 0$) or its complement, the affine function $1 + l_{g_k}$, is as good as, or better than, the best linear approximation (when $W_f(g_k) < 0$).

It is a simple corollary of Parseval's identity,

$$\sum_{i=1}^{2^m} W_f(g_i)^2 = 2^{2m},$$

that

$$\max_i |W_f(g_i)| \geq 2^{\frac{m}{2}}. \tag{2}$$

Therefore, for any Boolean function in m variables,

$$N_f \leq 2^{m-1} - 2^{\frac{m}{2}-1},$$

and this bound is achieved only when m is even and $|W_f(g_i)| = 2^{\frac{m}{2}}, \quad \forall i$. Hence,

$$\mathrm{wt}(f) = \frac{2^m - 2^{m/2}}{2} \text{ or } \frac{2^m + 2^{m/2}}{2}.$$

An m-variable Boolean function with m even and maximum nonlinearity is called *bent*. Furthermore, if f is bent then $|\Phi(f)| = 2^{m2^{m-2}}$. This is the maximum of $|\Phi|$ in $\mathbf{B}_m$ and $\Phi(f) < 0$.

The affine functions are the other extreme, with respect to the Walsh spectrum. There is only one non-null Walsh coefficient for an affine function, and its value is either 2^m, when it is linear, or -2^m otherwise. Therefore,

$$\Phi(l_{g_k} + c) = 0.$$

By Parseval's identity, if some of the Walsh coefficients are smaller than average in absolute value, especially if some are 0, then the others must be larger. Thus, if f is a Boolean function with a small N_f and $wt(f)$ even then it can be expected that $\Phi(f)$ will be null. For $wt(f)$ odd and after carrying out some computer searches up to $m = 5$, we found that Φ more often takes positive than negative values.

Although the formula for nonlinearity is sign free, the quotient $\frac{\mathrm{per}(H_m)}{\sharp\mathbf{B}_m}$ could provide some information of the "global" nonlinearity of the whole set m-variable Boolean functions. Especially, when $\frac{\mathrm{per}(H_m)}{\sharp\mathbf{B}_m} < \frac{\mathrm{per}(H_{m'})}{\sharp\mathbf{B}_{m'}}$ could indicate a better density of Boolean functions with high nonlinearity in $\mathbf{B}_m$ than in $\mathbf{B}_{m'}$. For $m = 2$ and 4, this is confirmed with the behaviour of the quotient between the number of bent functions in m variables between the number of Boolean functions (see [2], Chapter 7). Attending to our observation we also claim the following.

Conjecture 1. If m is even, then

$$2^{(m-2)2^{m-4}} \leq \mathrm{per}(H_m) \leq 2^{m2^{m-2}}$$

and if m is odd, then

$$2^{(m-1)2^{m-2}} \leq \mathrm{per}(H_m) \leq 2^{(m+1)2^{m-2}}.$$

Secondly, we will try to take advantage of computing the permanent of a Sylvester Hadamard matrix from partitioning $\mathbf{B}_m$ in classes under the affine equivalence relationship.

Definition 2 ([2])**.** *Two m-variable Boolean functions f and h are said to be affine equivalent if there exists an invertible matrix A with entries in $GF(2)$ and a constant $b \in GF(2)^m$ such that for all $x \in GF(2)^m$ it holds that*

$$f(x) = h(A(x) + b).$$

The following Lemma studies the Walsh spectra of affine equivalent Boolean functions f and h. As immediate consequence, we have $N_f = N_h$.

Lemma 2 ([13])**.** *Let f and h be two affine equivalent m-variable Boolean functions, $f(x) = h(A(x) + b)$, then*

$$W_f(g) = (-1)^{\langle b,(A^{-1})^T(g)\rangle} W_h((A^{-1})^T(g)).$$

Another important consequence is,

Proposition 3. *If f and h are affine equivalent m-variable Boolean functions then*

$$\Phi(f) = \Phi(h).$$

Proof. This follows from Proposition 2 and Lemma 2. Since $(A^{-1})^T(g)$ runs over all the elements of $GF(2) \setminus \{0\}$ when g runs over all the elements of $GF(2) \setminus \{0\}$ and the number of times that $\langle b, (A^{-1})^T(g)\rangle = 1 \mod 2$ is even for any fixed $b \in GF(2)$ when when g runs over all the elements of $GF(2) \setminus \{0\}$. This last statement is due to the fact that the number of elements of $GF(2)^m$ with concrete values in certain positions divides 2^m. □

Now, the formula for the permanent of H_m can be rewritten in terms of classes under the affine equivalence relation for the set of m-variable Boolean functions.

Proposition 4.

$$per(H_m) = \sum_{r=1}^{2^{m-1}-1} (-1)^r (2r - 2^m) \sum_{i=1}^{\sharp\Omega_{r,m}} \sharp[X_i^r]\Phi(f_{X_i^r}). \tag{3}$$

where $\Omega_{r,m}$ is the set of classes under the affine equivalence for the m-variable Boolean functions of weight r, $f_{X_i^r}$ is a representative of the class $X_i^r \in \Omega_{r,m}$, $r = wt(f_{X_i^r})$.

Proof. It is immediate from Proposition 2, Proposition 3 and the fact that $\sum_{i\in\alpha} h_{i,j} = -\sum_{i\in\bar{\alpha}} h_{i,j}, j \geq 2$; where $\alpha \cup \bar{\alpha} = \{1, 2, \ldots, 2^m\}$. □

Example 2. *Now we are going to compute per (H_3) using formula (3),*

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & - & 1 & 1 & - & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - \end{bmatrix}.$$

Taking into account that $\Phi(f) = 0$ for any 3-variable Boolean function with $wt(f)$ even. Then,

$$per\,(H_3) = \ (-1)^1(2-8) \sum_{i=1}^{\sharp\Omega_{1,3}} \sharp[X_i^1]\Phi(f_{X_i^1}) + (-1)^3(6-8) \sum_{i=1}^{\sharp\Omega_{3,3}} \sharp[X_i^3]\Phi(f_{X_i^3})$$

(Using Table 1, we get)

$$= \ 6 \times (8 \times 1) + 2 \times (56 \times 3) = 384.$$

Therefore, the problem of computing the permanent of a Sylvester Hadamard matrix of order 2^m can be carried out by enumerating m-variable Boolean functions with an arbitrary Walsh spectrum. This enumeration problem, although of interest in cryptography [14], requires a huge amount of computational resources. For instance, the number of bent functions (those Boolean functions with flat spectrum) so far has only been known for dimensions up to and including 8 (see [15]). Thus, Formula (3) only has a theoretical interest.

Finally, we give another formula for the permanent of H_m as a straightforward consequence of some results from [16,17]. Let $Sym(E)$ be the group of permutations on the set E and $\varepsilon(\sigma)$ be the parity $+1$ or -1 of σ for each $\sigma \in Sym(E)$. Then, $\Gamma(f)$ is defined as the set $\{\sigma \in Sym(GF(2)^m) \colon \forall a \in GF(2)^m,\ f(a + \sigma(a)) = 1\}$.

Now, taking into account the following facts:

1. Theorem 1 of [16] proves that the Walsh spectrum of f coincides with the spectrum of G_f, the Cayley graph associated to f, where the vertex set of G_f is equal to $GF(2)^m$, while the edge set E_f is defined as follows:

$$E_f = \{(g_i, g_j) \,|\, f(g_i + g_j) = 1\}.$$

   This connects the problem of analyzing the spectral coefficients of Boolean functions with the framework of spectral analysis of graphs. Let us denote by $w_f(g_i)$ the eigenvalues of the adjacency matrix of the Cayley graph associated to f.
2. Corollary 2 of [17] proves that the product $\prod_{i=1}^{2^m} w_f(g_i) = \sum_{\sigma\in\Gamma(f)} \varepsilon(\sigma)$.

Therefore, the formula for the permanent of H_m given in Proposition 2 can be rewritten as

$$\mathrm{per}\,(H_m) = \sum_{r=1}^{2^m} (-1)^{r+1} r \sum_{s_f \in Q_{r,2^m}} \frac{\sum_{\sigma\in\Gamma(f)} \varepsilon(\sigma)}{2^{2^m-1} w_f(g_1)}.$$

Table 1. Number of inequivalent m-variable Boolean functions of weight r under the affine equivalence for $m = 3$ and $r = 1, 3$.

r	# Inequivalent 3-Variable Boolean Functions	# Orbits
1	1	8
3	1	56

4. Conclusions

The paper demonstrates a connection between two different mathematical areas: Boolean functions and permanents. Firstly, Ryser's formula for computing the permanent of Sylvester Hadamard matrices has been rewritten in terms of the Walsh spectrum of m-variable functions. Although this formula does not represent a real shortcut for computing the permanent of H_m, it suggested the bounds given in Conjecture 1, since $|\prod_{j=2}^{2^m} W_f(g_j)| = 2^{m2^{m-2}}$ when f is bent. Secondly, we show that the quotient $per(H_m)/2^{2^m}$ provides information about the density of m-variable Boolean functions with high nonlinearity (i.e., Boolean functions with linearity close to the minimum). We have checked until $m = 5$ that $per(H_m)/2^{2^m}$ is a strictly increasing function and the quotient between the number of bent functions in m variables and the number Boolean functions (2^{2^m}) is a strictly decreasing function (up to $m = 8$) which means that density Boolean functions with high nonlinearity are worse when m increase. Finally, let us point out the following asymptotic result about the linearity of random Boolean functions due to Olejár and Stanek.

Theorem 1 ([18])**.** *There is a constant c, such that if m is big enough, then for almost every Boolean function in m variables*

$$N_f \geq 2^{m-1} - c\sqrt{m}2^{m/2}.$$

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The author thanks Kristeen Cheng for reading the manuscript. This work is partially supported by the Research Projects FQM-016 from Junta de Andalucí a.

Conflicts of Interest: The author declare no conflict of interest.

References

1. Guesmi, R.; Farah, M.A.B.; Kachouri, A.; Samet, M. Chaos-based designing of a highly nonlinear S-box using Boolean functions. In Proceedings of the 12th International Multi-Conference on Systems, Signals and Devices, SSD, Tunisia, Mahdia, 16–19 March 2015; Volume 2015, p. 7348106.
2. Tokareva, N. *Bent Functions: Results and Applications to Cryptography*; Elsevier Science: London, UK, 2015.
3. Valiant, L.G. The complexity of computing the permanent. *Theoret. Comput. Sci.* **1979**, *8*, 189–201. [CrossRef]
4. Aaronson, S. $P\overset{?}{=}NP$ *Chapter 3 in Open Problems in Mathematics*; Nash, J.F., Rassias, M.T., Eds.; Springer: Berlin/Heidelberg, Germany, 2016.
5. Minc, H. Permanents. In *Encyclopedia of Mathematics and its Applications 6*; Addison-Wesley: Reading, MA, USA, 1978.
6. Horadam, K.J. *Hadamard Matrices and Their Applications*; Princeton University Press: Princeton, NJ, USA, 2007.
7. Carlet, C. Boolean functions for cryptography and error correcting codes. In *Boolean Models and Methods in Mathematics, Computer Science and Engineering*; Crama, Y., Hammer, P.L., Eds.; Cambrige University Press: Cambridge, UK, 2010; pp. 257–397.
8. Mitrouli, M. Sylvester Hadamard matrices revisited. *Spec. Matrices* **2014**, *2*, 120–124. [CrossRef]
9. Wanless, I.M. Permanents of matrices of signed ones. *Linear Multilinear Algebra* **2005**, *52*, 57–63. [CrossRef]
10. Szöllósi, F. (Department of Mathematical Science, Shimane University, Matsue, Japan). Personal communication, 2014.
11. Carlet, C. On cryptographic complexity of Boolean functions. In *Proceedings of the Sixth Conference on Finite Fields with Applications to Coding Theory, Cryptrography, and Related Areas, Berlin, Germany*; Mullen, G.L., Stichtenoth, H., Tapia-Recillas, H., Eds.; Springer: Berlin, Germany, 2002; pp. 53–69.
12. Wanless, I.M. Permanents. In *Chapter 31 in Handbook of Linear Algebra*; Hogben, L., Ed.; Chapman & Hall/CRC: London, UK, 2007.
13. Preneel, B. Analysis and Design of Cryptographic Hash Functions. Ph.D. Thesis, Katholieke Universiteit Leuven, Leuven, Belgium, 1993.
14. Uyan, E.; Calik, C.; Doganaksoy, A. Counting Boolean functions with specified values in their Walsh spectrum. *J. Comput. Appl. Math.* **2014**, *259*, 522–528. [CrossRef]
15. Langevin, P.; Leander, G. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Des. Codes Cryptogr.* **2011**, *59*, 193–205. [CrossRef]
16. Bernasconi, A.; Codenotti, B. Spectral analysis of Boolean functions as a graph eigenvalue problem *IEEE Trans. Comput.* **1999**, *48*, 345–351.
17. Mitton, M. On the Walsh-Fourier analysis of Boolean functions. *J. Discret. Math. Scien. Cryptogr.* **2006**, *9*, 429–439. [CrossRef]
18. Olejár, D.; Stanek, M. On cryptographic properties of fandom Boolean functions. *J. Univers. Comput. Sci.* **1998**, *4*, 705–717.