Boolean Functions Satisfying Higher Order Propagation Criteria

B. Preneel[1], René Govaerts and Joos Vandewalle

Katholieke Universiteit Leuven, Laboratorium ESAT,
Kardinaal Mercierlaan, 94, B–3001 Heverlee, Belgium.

Abstract

Boolean functions that satisfy higher order propagation criteria are studied. A complete characterization is given of the autocorrelation function and Walsh spectrum of second order functions. The number of second order functions satisfying $PC(k)$ is related to a problem in coding theory and can be computed explicitly for $k = 1, n-1$ and n. A new interpretation of the number of balanced second order functions is given and a class of functions showing interesting properties is discussed.

1 Definitions

1.1 Boolean functions

A Boolean function $f(\underline{x})$ is a function whose domain is the vector space $\mathbb{Z}_2^n$ of binary n-tuples $(x_1, x_2, \ldots, x_n)$ that takes the values 0 and 1. In some cases it will be more convenient to work with functions that take the values $\{-1, 1\}$. The functions $\hat{f}(\underline{x})$ is defined as $\hat{f}(\underline{x}) = 1-2\cdot f(\underline{x})$. The Hamming weight *hwt* of an element of $\mathbb{Z}_2^n$ is the number of components equal to 1.

A Boolean function is said to be linear if there exists a $\underline{w} \in \mathbb{Z}_2^n$ such that it can be written as $L_{\underline{w}}(\underline{x}) = \underline{x}\cdot\underline{w}$ or $\hat{L}_{\underline{w}}(\underline{x}) = (-1)^{\underline{x}\cdot\underline{w}}$. Here $\underline{x}\cdot\underline{w}$ denotes the dot product of $\underline{x}$ and $\underline{w}$, defined as $\underline{x}\cdot\underline{w} = x_1w_1 \oplus x_2w_2 \oplus \ldots \oplus x_nw_n$. The set of affine functions is the union of the set of the linear functions and their complement.

Definition 1 *Let $f(\underline{x})$ be any real-valued function with domain the vector space $\mathbb{Z}_2^n$. The* **Walsh transform** *of $f(\underline{x})$ is the real-valued function over the vector space $\mathbb{Z}_2^n$ defined as*

$$F(\underline{w}) = \sum_{\underline{x}} f(\underline{x}) \cdot (-1)^{\underline{x}\cdot\underline{w}},$$

where $\sum_{\underline{x}}$ denotes the sum over all 2^n elements of $\mathbb{Z}_2^n$.

The relationship between the Walsh transform of $f(\underline{x})$ and $\hat{f}(\underline{x})$ is given by [For88]

$$\hat{F}(\underline{w}) = -2F(\underline{w}) + 2^n\,\delta(\underline{w}) \quad \text{and} \quad F(\underline{w}) = -\frac{1}{2}\hat{F}(\underline{w}) + 2^{n-1}\,\delta(\underline{w}),$$

[1]NFWO aspirant navorser, sponsored by the National Fund for Scientific Research (Belgium).

Appeared in *Advances in Cryptology – EUROCRYPT 1991*, Lecture Notes in Computer Science 547, D. W. Davies (ed.), Springer-Verlag, pp. 141–152, 1991.

where $\delta(\underline{w})$ denotes the Kronecker delta ($\delta(\underline{0}) = 1, \delta(\underline{k}) = 0 \ \ \forall \underline{k} \neq \underline{0}$).

Definition 2 *The* **autocorrelation function** $\hat{r}(\underline{s})$ *is defined as*

$$\hat{r}(\underline{s}) = \sum_{\underline{x}} \hat{f}(\underline{x}) \cdot \hat{f}(\underline{x} \oplus \underline{s}).$$

Note that $\hat{r}(\underline{0})$ equals 2^n.

It can also be of interest to write a Boolean function as the sum of all products of the variables:

$$f(\underline{x}) = a_0 \oplus \bigoplus_{1 \leq i \leq n} a_i x_i \ \oplus \bigoplus_{1 \leq i < j \leq n} a_{ij} x_i x_j \ \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \cdots x_n.$$

This form is called the **algebraic normal form** of a Boolean function f and the corresponding transformation is called the algebraic normal transform.

Definition 3 *The* **non-linear order** *of a Boolean function (notation:* $\mathrm{ord}(f)$*) is defined as the degree of the highest order term in the algebraic normal form.*

The affine Boolean functions are the functions with non-linear order < 2.

1.2 Properties of Boolean Functions

A Boolean function is said to be **balanced** if its truth table contains as many 0 as 1 entries. It is easy to show that this is equivalent to $\hat{F}(\underline{0}) = 0$.

A Boolean function is said to be ***m*th order correlation immune** if $f(\underline{x})$ is statistically independent of any subset of m input variables [Sie84, XM88]. This can be shown to be equivalent to

$$\hat{F}(\underline{w}) = 0 \quad 1 \leq hwt(\underline{w}) \leq m,$$

and a necessary condition is $ord(f) \leq n - m$. If f is also balanced, this upper bound can be improved to $n - m - 1$, unless $m = n - 1$.

A Boolean function $f(\underline{x})$ satisfies the **propagation criterion of degree *k* (*PC*(*k*))** if $f(\underline{x})$ changes with a probability of one half whenever i ($1 \leq i \leq k$) bits of $\underline{x}$ are complemented [PVV90]:

$$\hat{r}(\underline{s}) = 0 \ \text{ for } \ 1 \leq hwt(\underline{s}) \leq k.$$

Note that the Strict Avalanche Criterion (SAC) is equivalent to $PC(1)$ and perfect non-linear is $PC(n)$.

A Boolean function $f(\underline{x})$ of n variables satisfies the **propagation criterion of degree *k* and order *m* (*PC*(*k*) of order *m*)** if any function obtained from $f(\underline{x})$ by keeping m input bits constant satisfies $PC(k)$.

The **propagation matrix N_n** for all Boolean functions of n variables is the $n \times n$ matrix: $N_n(k, m) = \#\{f \mid f \text{ satisfies } PC(k) \text{ of order } m\}/2^{n+1}$, with $k + m \leq n$. The division by 2^{n+1} implies that abstraction is made of linear and constant terms, that have no influence on propagation properties. The propagation matrix for all second order Boolean functions of three to seven bits is given in table 1. In this paper, we will explain most numbers in this table and, if possible, generalize certain properties for arbitrary n.

Appeared in *Advances in Cryptology – EUROCRYPT 1991*, Lecture Notes in Computer Science 547, D. W. Davies (ed.), Springer-Verlag, pp. 141–152, 1991.

k \ m	0	1	2
1	4	1	0
2	1	1	–
3	0	–	–

k \ m	0	1	2	3
1	41	10	1	0
2	28	1	1	–
3	28	0	–	–
4	28	–	–	–

k \ m	0	1	2	3	4
1	768	253	26	1	0
2	448	28	1	1	–
3	168	28	0	–	–
4	28	28	–	–	–
5	0	–	–	–	–

k \ m	0	1	2	3	4	5
1	27449	12068	1858	76	1	0
2	18788	3188	1	1	1	–
3	14308	421	1	0	–	–
4	13888	1	1	–	–	–
5	13888	0	–	–	–	–
6	13888	–	–	–	–	–

k \ m	0	1	2	3	4	5	6
1	1887284	1052793	236926	15796	232	1	0
2	1419852	237048	4901	1	1	1	–
3	889672	17668	841	1	0	–	–
4	402752	13888	1	1	–	–	–
5	111104	13888	0	–	–	–	–
6	13888	13888	–	–	–	–	–
7	0	–	–	–	–	–	–

Table 1: The matrices $N_3(k,m)$, $N_4(k,m)$, $N_5(k,m)$,$N_6(k,m)$ and $N_7(k,m)$ for second order functions.

2 Propagation characteristics of second order functions

Second order functions have been studied intensively to derive properties of the second order Reed-Muller codes. For the study of second order functions, it is useful to write the second order coefficients of the algebraic normal form in a binary symmetric matrix with zero diagonal: $[b_{ij}] = [a_{ij}]$, where $a_{ii} = 0$. This is called a **symplectic matrix**. The number of second order coefficients equals $\frac{n\cdot(n-1)}{2}$ and will be denoted with $\Delta(n)$. The second order functions can be reduced with an equivalence transform to a canonical form based on Dickson's theorem.

Theorem 1 (Dickson's theorem) *If B is a symplectic $n \times n$ matrix of rank $2h$, then there exists an invertible binary matrix R such that RBR^T has zeroes everywhere except on the two diagonals immediately above and below the main diagonal, and there has $1010\ldots100\ldots0$ with h ones.*
Every second order Boolean function can by an affine transformation of variables be reduced to $\bigoplus_{i=1}^{h} x_{2i-1}x_{2i} \oplus \epsilon$, with ϵ an affine function of x_{2h+1} through x_n.

The rank of the $2^{\Delta(n)}$ symplectic matrices is given by following theorem [MWS77]:

Lemma 1 *The number of symplectic $n \times n$ matrices over $\mathbb{Z}_2$ of rank $2h$ equals*

$$M(n,2h) = \begin{bmatrix} n \\ 2h \end{bmatrix} \cdot M(2h,2h).$$

Here $\begin{bmatrix} n \\ k \end{bmatrix}$ denotes the binary Gaussian binomial coefficient, defined for all non-negative integers k by

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = 1, \quad \begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + 2^k \begin{bmatrix} n-1 \\ k \end{bmatrix}$$

Appeared in *Advances in Cryptology – EUROCRYPT 1991*, Lecture Notes in Computer Science 547, D. W. Davies (ed.), Springer-Verlag, pp. 141–152, 1991.

and $M(2h, 2h) = (2^{2h-1} - 1)2^{2h-2} \cdots (2^3 - 1)2^2$.

In [MWS77] it is shown that in case n is even the functions of n bits satisfying $PC(n)$ (bent functions) are the functions for which the corresponding matrix B has full rank. The number of these functions is given by $M(n, n)$.

For n odd, the highest criterion that can be satisfied is $PC(n-1)$. The previous result can be extended for n odd.

Theorem 2 *Let f be a Boolean function of n variables, $n > 2$ and odd.*
Then f satisfies $PC(n-1)$ of order 0 and 1 iff f is obtained with following construction:

1. *Let f' be a function of $n-1$ variables satisfying $PC(n-1)$ with algebraic normal form coefficients equal to a'_{ij}.*
2. *Define $a_{ij} = a'_{ij}$ for $1 \leq i < j \leq n-1$ and*

$$a_{in} = \bigoplus_{j=0, j \neq i}^{n-1} a_{ij} \quad \text{for } 1 \leq i \leq n-1.$$

The number of functions satisfying $PC(n-1)$ of order 0 and 1 is given by $M(n-1, n-1)$.

Proof: The first part of the proof consists of showing that every function satisfying $PC(n-1)$ of order 0 satisfies $PC(n-1)$ of order 1. This part is a simple corollary of theorem 5 (cfr. infra). To characterize the functions satisfying $PC(n-1)$ of order 1, it is recalled that every function f^* obtained from f by fixing one input bit should satisfy $PC(n-1)$. This can be restated with the symplectic matrices B and B^* that correspond to f and f^* respectively: every matrix B^* obtained from B by deleting one column and the corresponding row should have full rank $n-1$. As the rank of a symplectic matrix is always even, this implies that B has necessarily rank $n-1$ and that any column (row) can be written as a linear combination of the other columns (rows). Any symplectic matrix B^* of rank $n-1$ can be extended in 2^{n-1} ways to a matrix B. However, if any matrix obtained from deleting one column and the corresponding row in B should have rank $n-1$, the only solution is that the added column (row) is the sum of all other columns (rows). This can be shown as follows: if a particular column and row are not selected in the sum, the deletion of this column and row from B will result in a singular matrix B^*, contradicting the requirement. ∎

Theorem 11 in [PVV90] states that a second order function satisfies $PC(1)$ or SAC if and only if every variable occurs at least once in the second order terms of the algebraic normal form. This makes it possible to compute the number of second order functions satisfying $PC(1)$.

Theorem 3 *The number of second order n-bit functions satisfying $PC(1)$ is given by*

$$N_n(1, 0) = \sum_{k=1}^{n-1} (-1)^{n-k-1} \binom{n-1}{k} 2^{\Delta(k)} (2^k - 1).$$

Proof: This follows from the observation that the second order functions satisfying $PC(1)$ correspond to the undirected simple graphs with n vertices with minimal degree equal to 1.

Appeared in *Advances in Cryptology – EUROCRYPT 1991*, Lecture Notes in Computer Science 547,
D. W. Davies (ed.), Springer-Verlag, pp. 141–152, 1991.

The degree of a vertex is equal to the number of edges incident to that vertex, and the minimal degree of a graph is the minimum of the set consisting of the degrees of the vertices. It is easily seen that the number of these graphs is given by following recursive equation (for $n > 1$):

$$N_n(1,0) = 2^{\Delta(n)} - 1 - \sum_{k=2}^{n-1} \binom{n}{k} N_k(1,0).$$

The theorem follows from the solution of this equation. ∎

3 Autocorrelation function properties

In [PVV90] it was shown that the non-linear order of functions satisfying $PC(1)$ is bounded by $n-1$. A well known result is that the non-linear order of functions satisfying $PC(n)$ (n even and > 2) is bounded by $n/2$, and for functions satisfying $PC(n-1)$ (n odd and > 2) the corresponding upper bound is $\lceil n/2 \rceil$.

An extension of this result for functions satisfying $PC(k)$ is non-trivial, because k depends on both the number of zeroes of the autocorrelation function as well as on the position of these zeroes. Hence $PC(k)$ is not invariant under affine transformations, where the non-linear order clearly is. The way to proceed is first to study a number that is invariant under affine transformations, namely the number of zeroes of the autocorrelation function (denoted by $N_{\hat{r}}$) and then to apply the results to $PC(k)$.

The upper bound on the non-linear order for functions satisfying $PC(1)$ can be improved as follows: even if the autocorrelation function has one zero, the function can not have maximal non-linear order.

Theorem 4 *Let f be a Boolean function of n variables with $n > 2$.*
If $N_{\hat{r}} > 0$ then $\mathrm{ord}(f) \leq n-1$.

Proof: It is sufficient to show that the Hamming weight of f is even. Let $\underline{s}$ be the value for which $\hat{r}(\underline{s}) = 0$ or $r(\underline{s}) = 2^{n-1}$. Then

$$\begin{aligned} hwt(f) &= \sum_{\underline{x}} f(\underline{x}) \mod 2 \\ &= \sum_{\underline{x}} f(\underline{x} \oplus \underline{s}) \mod 2 \\ &= \frac{1}{2} \sum_{\underline{x}} f(\underline{x}) \oplus f(\underline{x} \oplus \underline{s}) \mod 2 \\ &= \frac{1}{2} r(\underline{s}) \bmod 2 = 2^{n-2} \bmod 2. \end{aligned}$$

If $n > 2$, the theorem follows. ∎

A second result for second order functions is based on Dickson's theorem and Lemma 1.

Theorem 5 *The autocorrelation function of second order functions takes the values* 0 *and* $\pm 2^n$. *The number of zeroes is given by $N_{\hat{r}} = 2^n - 2^{n-2h}$ for $1 \leq h \leq \lfloor \frac{n}{2} \rfloor$.*

Appeared in *Advances in Cryptology – EUROCRYPT 1991*, Lecture Notes in Computer Science 547, D. W. Davies (ed.), Springer-Verlag, pp. 141–152, 1991.

The number of functions with this number of zeroes equals $M(n,2h)$. There are $\left[\begin{smallmatrix} n \\ 2h \end{smallmatrix}\right]$ possible patterns for these zeroes and to every pattern correspond exactly $M(2h,2h)$ functions. The coordinates where $\hat{r}(\underline{s}) \neq 0$ form a $n-2h$ dimensional subspace of $\mathbb{Z}_2^n$.

Proof: For the canonical second order function:

$$f(\underline{x}) = \bigoplus_{i=1}^{h} x_{2i-1}x_{2i},$$

the autocorrelation function can be written as follows:

$$r(\underline{s}) = \sum_{\underline{x}} \left(\bigoplus_{i=1}^{h} s_{2i-1}s_{2i} \ \oplus \ \bigoplus_{i=1}^{h} (x_{2i-1}s_i \oplus x_{2i}s_{2i-1}) \right).$$

Note that the affine function ϵ can be omitted because affine terms have no influence on the autocorrelation function. In case $r(\underline{s}) = 2^{n-1}$, corresponding to $\hat{r}(\underline{s}) = 0$, the first part of the sum has no influence on the result. It is easily seen that $r(\underline{s})$ will be equal to 2^{n-1} if there exists at least one $s_i \neq 0$, with $1 \leq i \leq 2h$. Hence the number of non-zeroes of $\hat{r}(\underline{s})$ equals 2^{n-2h}, corresponding to the vectors $\underline{s}$ with $s_i = 0$, for $1 \leq i \leq 2h$. It is clear that these vectors form a subspace of $\mathbb{Z}_2^n$ of dimension $n-2h$. The number of distinct subspaces of dimension $n-2h$ corresponds to the number of $[n, n-2h]$ codes and equals $\left[\begin{smallmatrix} n \\ 2h \end{smallmatrix}\right]$ [MWS77]. ∎

The last part of Theorem 5 makes it in principle possible to compute the number of second order functions satisfying $PC(k)$.

Corollary 1 *The number of second order functions of n variables satisfying $PC(k)$ is given by*

$$\sum_{h=1}^{\lfloor \frac{n}{2} \rfloor} L(n, n-2h, k) M(2h, 2h),$$

where $L(n,r,k)$ denotes the number of linear $[n,r,d]$ codes with minimum distance $d > k$.

Proof: This follows from the observation that a function will satisfy $PC(k)$ if the non-zeroes of r, that form a subspace of dimension $n-2h$, occur at positions with Hamming weight $> k$. This is equivalent to the statement that the non-zeroes should form a linear code with length n, dimension $n-2h$ and minimum distance $d > k$. ∎

Because of the Singleton bound ($d \leq n - r + 1$) [MWS77] the lower limit of this sum can be increased to $\lfloor \frac{k+1}{2} \rfloor$. However, the computation of $L(n,r,k)$ even for small values of n is a difficult problem. Even the maximal d for given n and r (notation $d_{max}(n,r)$) remains an open problem except for $r \leq 5$ and $d \leq 3$. In [HeSt73] a table of known bounds $d_{max}(n,r)$ is listed for $n \leq 127$. A small relevant part is reproduced in table 2. In case $n = 6$, $1 \leq h \leq 3$, the autocorrelation functions has 1, 4 or 16 non-zeroes and the number of corresponding functions is 13888 (bent functions), 18228 and 651. In case of 4 non-zeroes, $r = 2$ and from table 2 one finds $d_{max}(6,2) = 4$. Hence the bent functions are the only functions satisfying $PC(4)$, $PC(5)$ and $PC(6)$. The number of $[6,2,4]$, $[6,2,3]$, $[6,2,2]$ and $[6,2,1]$ codes is 15, 160, 305 and 171 respectively. With every code correspond 28 functions, resulting in 420, 4480,

Appeared in *Advances in Cryptology – EUROCRYPT 1991*, Lecture Notes in Computer Science 547, D. W. Davies (ed.), Springer-Verlag, pp. 141–152, 1991.

n \ r	1	2	3	4	5
4	4	2	2	1	5
5	5	3	2	2	1
6	6	4	3	2	2
7	7	4	4	3	3

Table 2: Upper bound on the minimum distance d for linear $[n, r, d]$ codes.

8540 and 4788 functions for every class. In case of 16 non-zeroes, every code corresponds to exactly one function. The number of $[6, 4, 2]$ and $[6, 4, 1]$ codes is given by 121 and 530. The number of 6-bit functions satisfying $PC(3)$ equals $13888 + 420 = 14308$, the number of functions satisfying $PC(2)$ equals $13888 + 420 + 4480 = 18788$, and the number of functions satisfying $PC(1)$ equals $18788 + 8540 + 121 = 27449$. This last result can also be obtained with theorem 3.

The number of $[n, 1, d]$ codes equals $\binom{n}{d}$ and hence for n odd the functions satisfying $PC(k)$ with $d_{max}(n, 3) \leq k \leq n - 1$ is given by

$$M(n-1, n-1) \sum_{i=k+1}^{n} \binom{n}{i},$$

for which no closed form exists.

4 Walsh transform and balancedness

It has been shown in [PVV90] that dyadic shifts in the Walsh spectrum modify only linear and constant terms and that the propagation characteristics remain unaffected. A corollary of this observation is that adding the right linear terms to a function with at least one zero in the Walsh spectrum will result in a balanced function with the same propagation properties. If the image of the other zeroes of the spectrum under the same transformation is the set of vectors with low Hamming weight, the corresponding function will also be correlation immune. This indicates that the number of zeroes of the Walsh spectrum is a relevant property.

The weight distribution of functions with *ord* ≤ 2 is known from the study of Reed-Muller codes [MWS77].

Theorem 6 *Let A_i be the number of functions with* ord ≤ 2 *and Hamming weight i. Then $A_i = 0$ unless $i = 2^{n-1}$ or $i = 2^{n-1} \pm 2^{n-1-h}$ for some h, $0 \leq h \leq \lfloor \frac{n}{2} \rfloor$. Also $A_0 = A_{2^n} = 1$ and*

$$A_{2^{n-1} \pm 2^{n-1-h}} = 2^{h(h+1)} \cdot \frac{(2^n - 1)(2^{n-1} - 1) \cdots (2^{n-2h+1} - 1)}{(2^{2h} - 1)(2^{2h-2} - 1) \cdots (2^2 - 1)} \quad \textit{for } 1 \leq h \leq \lfloor \frac{n}{2} \rfloor.$$

$A_{2^{n-1}}$ can be evaluated because all A_i sum to $2^{1+n+\Delta(n)}$.

Based on Dickson's theorem, the number of zeroes of the Walsh spectrum of a second order function can be calculated.

Appeared in *Advances in Cryptology – EUROCRYPT 1991*, Lecture Notes in Computer Science 547, D. W. Davies (ed.), Springer-Verlag, pp. 141–152, 1991.

Theorem 7 *The number of zeroes of the Walsh transform of a second order function is given by* $N_{\hat{F}} = 2^n - 2^{2h}$ *for* $1 \leq h \leq \lfloor \frac{n}{2} \rfloor$. *The number of functions with this number of zeroes equals* $M(n, 2h)$. *If* $\hat{F}(\underline{w}) \neq 0$, *then* $\mid \hat{F}(\underline{w}) \mid = 2^{n-h}$.

Proof: It will be shown that $\hat{F}(\underline{w})$, the Walsh transform of

$$f(\underline{x}) = \bigoplus_{i=1}^{h} x_{2i-1}x_{2i}$$

is equal in absolute value to 2^{n-h} for $w_i = 0$, $2h+1 \leq i \leq n$ and equal to zero elsewhere. The theorem then follows from the application of Dickson's theorem and from the observation that the addition of the affine term ϵ only causes a dyadic shift of the Walsh spectrum. The Walsh transform of f can be written as:

$$\hat{F}(\underline{w}) = \sum_{\underline{x}} (-1)^{\bigoplus_{i=1}^{h} x_{2i-1}x_{2i}} \cdot (-1)^{\bigoplus_{i=1}^{n} x_i w_i}.$$

Here we assume that $2h < n$. In case $h = 2n$, f is a bent function and the theorem is clearly true.

- In case $w_i = 0$, $2h+1 \leq i \leq n$, the expression for the Walsh transform reduces to

  $$\hat{F}(\underline{w}) = \sum_{\underline{x}} (-1)^{\bigoplus_{i=1}^{h} x_{2i-1}x_{2i}} \cdot (-1)^{\bigoplus_{i=1}^{2h} x_i w_i}.$$

  As the variables x_{2h+1} through x_n do not occur in this sum, it can be simplified to

  $$\hat{F}(\underline{w}) = 2^{n-2h} \cdot \sum_{\underline{x}'} (-1)^{\bigoplus_{i=1}^{h} x_{2i-1}x_{2i}} \cdot (-1)^{\bigoplus_{i=1}^{2h} x_i w_i},$$

  where $\underline{x}'$ denotes $[x_1 \ldots x_{2h}]$. By observing that the remaining sum corresponds to the Walsh transform of a bent function of $2h$ variables, it follows that its absolute value equals 2^h.

- In the other case, let U denote the set of indices $\{i_1, i_2, \ldots, i_k\}$ in the interval $[2h+1, n]$ for which $w_{i_j} = 1$. The Walsh transform can then be written as

  $$\hat{F}(\underline{w}) = \sum_{\underline{x}'} (-1)^{\bigoplus_{i=1}^{h} x_{2i-1}x_{2i}} \cdot (-1)^{\bigoplus_{i=1}^{2h} x_i w_i} \cdot \sum_{\underline{x}''} (-1)^{\bigoplus_{i_j \in U} x_{i_j}},$$

  where $\underline{x}'$ denotes $[x_1 \ldots x_{2h}]$ and $\underline{x}''$ denotes $[x_{2h} \ldots x_n]$. It is easily seen that the second sum vanishes, and hence $\hat{F}(\underline{w})$ equals zero.

■

From the proof it follows that the coordinates were $\hat{F}(\underline{w}) \neq 0$ will form a subspace of $\mathbb{Z}_2^n$ of dimension $2h$ if and only if the affine function ϵ is constant. If this condition is not satisfied, the non-zeroes will be a dyadic shift of a subspace.

Appeared in *Advances in Cryptology – EUROCRYPT 1991*, Lecture Notes in Computer Science 547, D. W. Davies (ed.), Springer-Verlag, pp. 141–152, 1991.

Theorem 7 results in a new interpretation of the number of balanced functions with $ord \leq 2$. There are $2(2^n - 1)$ balanced linear functions and every second order function with q zeroes in the Walsh spectrum corresponds to $2q$ balanced functions through addition of affine terms. Hence the total number of balanced functions with $ord \leq 2$ can also be written as

$$A_{2^{n-1}} = 2(2^n - 1) + 2\left(\sum_{h=1}^{\lfloor \frac{n}{2} \rfloor - 1} (2^n - 2^{2h}) M(n, 2h)\right).$$

For bent functions it is already known that the autocorrelation function has only one non-zero element and the Walsh spectrum has no zeroes. Following corollary, resulting from the combination of Theorem 5 and Theorem 7, gives the relation between the number of non-zeroes of the autocorrelation function and the Walsh spectrum for second order functions.

Corollary 2 *Let f be a Boolean function of n variables with* $\mathrm{ord}(f) \leq 2$. *Then*

$$(2^n - N_{\hat{r}}) \cdot (2^n - N_{\hat{F}}) = 2^n.$$

Note that if $ord(f) = n$, $N_{\hat{r}} = 0$ (theorem 4) and $N_{\hat{F}} = 0$ (because $hwt(f)$ is always odd) and this expression reaches its maximal value 2^{2n}. We conjecture that if $ord(f) > 2$, $(2^n - N_{\hat{r}}) \cdot (2^n - N_{\hat{F}}) \geq 2^n$, and equality holds only for functions satisfying $PC(n)$ or $PC(n-1)$.

5 A special class of functions

For $n = 5$ there exist 192 4th order functions satisfying $PC(2)$. The non-zeroes of the autocorrelation function have all absolute value 8. The zeroes of the autocorrelation function form the set of all 15 vectors with Hamming weight 1 or 2. An example of this class is

$$f_1(\underline{x}) = x_1x_2x_3x_4 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_4x_5 \oplus x_1x_3x_4x_5 \oplus x_2x_3x_4x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_3 \oplus x_2x_5 \oplus x_3x_4.$$

The value distribution of the Walsh spectrum (table 3) shows that this function is correlation immune of order 1. A related function f_2 can be defined as

$$f_2(\underline{x}) = f_1(\underline{x}) \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5.$$

The Walsh spectrum of f_2 is obtained by a dyadic shift over [11111] of the Walsh spectrum of f_1, resulting in a balanced function satisfying $PC(2)$ (table 3). Note that it is not possible to obtain from f_1 through an affine transformation of variables a function that is balanced and correlation immune of order 1, as this requires the vanishing of all coefficients of order 4 [XM88].

6 Summary

The distribution of the autocorrelation function and Walsh transform is invariant under affine transformations and can be computed for second order functions based on Dickson's theorem. In case of second order functions, a relation between the distribution of the autocorrelation function and the number of functions satisfying $PC(k)$ has been established and the study

Appeared in *Advances in Cryptology – EUROCRYPT 1991*, Lecture Notes in Computer Science 547,
D. W. Davies (ed.), Springer-Verlag, pp. 141–152, 1991.

$hwt(\underline{w})$	0	1	2	3	4	5
$\mid \hat{F}_1(\underline{w}) \mid$	12	0	4	8	4	0
$\mid \hat{F}_2(\underline{w}) \mid$	0	4	8	4	0	12

$hwt(\underline{s})$	0	1	2	3	4	5
$\hat{r}_1(\underline{s})$	32	0	0	8	8	-8
$\hat{r}_2(\underline{s})$	32	0	4	-8	8	8

Table 3: Value distribution of the Walsh spectrum and the autocorrelation function for the functions f_1 and f_2.

of the Walsh transform gives a new interpretation to the number of balanced second order functions. Finally a special class of functions of 5 bits combining interesting properties have been introduced. An interesting open problem is to generalize this class for arbitrary n.

References

[For88] R. Forré, "The strict avalanche criterion: spectral properties of Boolean functions and an extended definition", *Advances in Cryptology, Proc. Crypto 88*, Springer Verlag, 1990, p. 450–468.

[HeSt73] H.J. Helgert and R.D. Stinaff, "Minimum-Distance bounds for binary linear codes", *IEEE Trans. Inform. Theory*, Vol. IT-19, p. 344–356, May 1973.

[MWS77] F.J. MacWilliams and N.J.A. Sloane, *"The theory of error-correcting codes"*, North-Holland Publishing Company, Amsterdam, 1977.

[MS89] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions", *Advances in Cryptology, Proc. Eurocrypt 89*, Springer Verlag, 1990, pp. 549–562.

[PVV90] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts and J. Vandewalle, "Propagation Characteristics of Boolean Functions", *Advances in Cryptology, Proc. Eurocrypt 90, Lecture Notes in Computer Science 473*, Springer Verlag, 1991, pp. 161–173.

[Ruep90] R.A. Rueppel, "Stream Ciphers", in *Contemporary Cryptology: The Science of Information Integrity*, G. Simmons, ed., IEEE Press, to appear.

[Sie84] T. Siegenthaler, "Correlation immunity of non-linear combining functions for cryptographic applications", *IEEE Trans. Inform. Theory*, Vol. IT-30, p. 776–780, Oct. 1984.

[VV90] W. Van Leekwijck and L. Van Linden, *"Cryptographic properties of Boolean functions – in Dutch, Cryptografische eigenschappen van Booleaanse functies"*, ESAT Katholieke Universiteit Leuven, Thesis grad. eng., 1990.

[XM88] G.-Z. Xiao and J.L. Massey, "A spectral characterization of correlation-immune combining functions", *IEEE Trans. Inform. Theory*, Vol. IT-34, p. 569–571, May 1988.

Appeared in *Advances in Cryptology – EUROCRYPT 1991*, Lecture Notes in Computer Science 547, D. W. Davies (ed.), Springer-Verlag, pp. 141–152, 1991.