Annales Univ. Sci. Budapest., Sect. Comp. 21 (2004) 165-175

ON HIGHLY NONLINEAR FUNCTIONS

I. Licskó (Budapest, Hungary)

1. Introduction

Highly nonlinear functions play an important role in designing secure stream ciphers. The success of linear cryptanalysis has extended the significance of the functions to the design and analysis of block ciphers. The construction of this class of functions is important in practice. This importance is the basis of our work.

2. Notations

The mapping $f : \{0,1\}^n \to \{0,1\}$ is called *Boolean-function*.

A Boolean-function is often substituted by the Boolean-function-*generated* sequence of $\{-1,1\}$ value-set of 2^n elements, defined by

$$\overline{f}(x) = (-1)^{f(x)}$$

or

$$\overline{f}(x) = 1 - 2f(x).$$

The weight of function $f(x)$ means the number of 1's in its truth table: $w(f) = \sum_{x \in \{0,1\}^n} f(x)$.

The function $f(x)$ is called balanced if the number of 1's and the number of 0's in its truth table are equal, that is $f(x) = 1$ takes exactly as many places as $f(x) = 0$ does. In that case $\sum_{x \in \{0,1\}^n} \overline{f}(x) = 0$, and $w(f) = 2^{n-1}$ marks the weight of a balanced $f(x)$ function.

Ordinary *operations* can be interpreted among the vectors of Boolean-space:

If $a, b \in \{0,1\}^n$, $a = (a_0, a_1, \ldots, a_{n-1})$, $b = (b_0, b_1, \ldots, b_{n-1})$, then the *addition* taken by components can be specified by $a \oplus b = (a_0 \oplus b_0, a_1 \oplus \oplus b_1, \ldots, a_{n-1} \oplus b_{n-1})$ and the *scalar product* can be described with the formula $ab = \bigoplus_{i=0}^{n-1} a_i b_i$. In these cases multiplication and addition are to be understood in GF(2).

The function $f : \{0,1\}^n \to \{0,1\}$ is termed as *affine* if

$$f(x_0, x_1, \ldots, x_{n-1}) = a_0 x_0 \oplus a_1 x_1 \oplus \ldots \oplus a_{n-1} x_{n-1} \oplus c,$$

$a_i, c \in \{0,1\}$ and if $c = 0$ the functions are referred to as *linear*.

In this article $(\overline{f}(x) l_i)$ denotes the scalar product of two $\{-1,1\}$ sequences generated by the function $f(x)$ and the linear function $a_i x$.

The function f satisfies the *propagation criterion* regarding an element $a \in \in \{0,1\}^n, a \neq 0$, if the function $f(x) \oplus f(x \oplus a)$ is balanced.

The distance between functions $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^n \to \to \{0,1\}$ is

$$d(f,g) = w(f \oplus g) = \sum_{x \in \{0,1\}^n} (f(x) \oplus g(x)).$$

The correlation of two functions is specified as $c(f,g) = \sum_{x \in \{0,1\}^n} \overline{f}(x)\overline{g}(x) = = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus g(x)}$, and $c(f,g) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus g(x)} = 2^n - 2d(f,g)$.

The *autocorrelational* function of f is $r_f(a)$, and

$$r_f(a) = \sum_{x \in \{0,1\}^n} \overline{f}(x)\overline{f}(x+a).$$

The *Walsh-transformed* version of $f : \{0,1\}^n \to \{0,1\}$ in the position $a \in \in \{0,1\}^n = (a_0, a_1, \ldots, a_{n-1})$

$$F(a) = \sum_{x \in \{0,1\}^n} f(x)(-1)^{ax},$$

while the *Walsh-transformed* version of $\overline{f} : \{0,1\}^n \to \{-1,1\}$ *generated* by f is specified as

$$\overline{F}(a) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus xa}.$$

A vector specified as $a \in \{0,1\}^n$ is termed as the *linear structure* of function f, if the function $f(x) \oplus f(x \oplus a)$ is constant, that is

$$\sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus f(x \oplus a)} = \pm 2^n.$$

A function specified as $f : \{0,1\}^n \to \{0,1\}$ is termed to be *bent*, if it is true for all $a \in \{0,1\}^n$ that the Walsh-transformed version of the generated function is constant, and

$$\overline{F}(a) = \left| \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus xa} \right| = 2^{\frac{n}{2}}.$$

The *non-linearity* of a function specified as $f : \{0,1\}^n \to \{0,1\}$ means the distance of f from the affine functions and is specified as

$$N_f = 2^{n-1} - \frac{1}{2} \max_{i=0,1,\ldots,2^n-1} \left(\left| \overline{f}(x) l_i \right| \right).$$

The least value of non-linearity is 0, it is the non-linearity of affine functions. The maximum of non-linearity value is generated if $|\overline{f}(x) l_i|$ is constant and its value is $2^{\frac{n}{2}}$. The maximum non-linearity values can be realized by bent functions, whose non-linearity is $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$. Such functions are interpreted in spaces of even dimensions only, since the value of $2^{\frac{n}{2}}$ must be an integer number. Despite their favourable non-linearity characteristics they are not preferred for cryptographic applications because these functions are never balanced and are not correlation-immune.

It is practical therefore to find other functions, which are in all probable ways maximally non-linear, balanced or at least can easily be rearranged to be such.

Taking the above aspects into consideration, the authors of [8] sought functions, whose non-linearity was great, nearing maximum and could easily be made balanced. It is characteristic for bent functions that, except for the vector $(0, 0, \ldots, 0)$, they satisfy the propagation criterion for all elements of the Boolean-space. The paper [8] is focussed on determining the influence exerted over the non-linearity of the function by specific characteristics of vectors, regarding which the function does not satisfy the propagation criterion.

Bent functions can be generated in a very simple process, [4] provides a standard solution for the event if we intend to generate the function with the aid of Boolean-polynom. [6] provides a process for the formation of bent

functions through the concatenation of $\{-1, 1\}$ sequences generated by linear functions.

3. Construction of function with the superposition process

An analysis of the results with highly non-linear Boolean-functions of odd dimension provided in [8] offers the following considerations.

Let n be even and $f : \{0,1\}^n \to \{0,1\}$ a bent function. Let $g_i : \{0,1\}^{n+1} \to \{0,1\}$, $i = 0, 1, \ldots, n-1$, be the ith projection, that is $g_i(x_0, x_1, \ldots, x_n) = x_i$. In that case the function specified as $f(g_0, g_1, \ldots, g_{n-1})$ is interpreted in the $n+1$ dimensional space. The value of the function is independent from the x_n co-ordinate. Let us consider the function h for which the truth table is produced by copying the truth table of function f twice in succession so, that for the first $x_n = 0$, then $x_n = 1$ there appear. The function $h : \{0,1\}^{n+1} \to \{0,1\}$ generated in the process satisfies

$$h(x_0, x_1, \ldots, x_n) = f(g_0, g_1, \ldots, g_{n-1}) = f(x_0, x_1, \ldots, x_{n-1}).$$

Since the function f is bent,

$$\overline{F}(a) = \left| \sum_{x \in \{0,1\}} (-1)^{f(x) \oplus xa} \right| = 2^{\frac{n}{2}}$$

is met for every $a \in \{0,1\}^n$.

Let us see, how h and $\overline{h} : \{0,1\}^{n+1} \to \{-1,1\}$ are generated by its behaviour. Let $a = (a_0, a_1, \ldots, a_{n-1}) \in \{0,1\}^n$ and $b = (a_0, a_1, \ldots, a_{n-1}, x_n) \in \in \{0,1\}^{n+1}$,

$$\overline{H}(b) = \sum_{y \in \{0,1\}^{n+1}} (-1)^{h(y) \oplus yb} =$$

$$= \sum_{x \in \{0,1\}^n, x_n = 0} (-1)^{f(x) \oplus ax \oplus x_n b_n} + \sum_{x \in \{0,1\}^n, x_n = 1} (-1)^{f(x) \oplus ax \oplus x_n b_n}$$

and

$$\overline{H}(b) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus ax} + \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus ax \oplus b_n}.$$

This offers the conclusion that

$$\overline{H}(b) = \begin{cases} 0, & \text{if} \quad b_n = 1, \\ \\ 2 \cdot 2^{\frac{n}{2}}, & \text{if} \quad b_n = 0. \end{cases}$$

This function satisfies the conditions of Corollary 15 in [8], therefore the non-linearity of function h is

$$N_h = 2^{n+1-1} - 2^{\frac{1}{2}(n+1-1)}.$$

The disadvantage of the above construction lies in the need of a further step to make the function balanced.

A balanced function $h(x_0, x_1, \ldots, x_n)$ can be constructed on the basis of the $f(x_0, x_1, \ldots, x_{n-1})$ function in a very simple process

$$h(x_0, x_1, \ldots, x_n) = f(x_0, x_1, \ldots, x_{n-1}) \oplus x_n,$$

which means that in the truth-table of h we copied the truth-table of the negated f function after the truth-table of the f function so, that $x_n = 0$ is written in the rows of f and $x_n = 1$ in the rows of $\neg f$. Since negation will not influence the bent property and propagation criterion, the functions providing the previously introduced characteristics are also balanced. Example 2 provided in [8] is consistent with this statement.

The foregoing can also be expressed in general terms for the construction of highly non-linear Boolean-function of odd dimension.

Proposition 1. *Let*

$f : \{0,1\}^2 \to \{0,1\}$ *and* $f(x, y) = x \oplus y$,

$g_1 : \{0,1\}^n \to \{0,1\}$ $g_1(x_0, x_1, \ldots, x_{n-1})$ *be a bent function, where* n *is even,*

$g_2 : \{0,1\}^m \to \{0,1\}$ $g_2(y_0, y_1, \ldots, y_{m-1})$ *be a balanced function, where* m *is odd.*

The non-linearity of the function

$$f(g_1(x_0, x_1, \ldots, x_{n-1}),\ g_2(y_0, y_1, \ldots, y_{m-1})) = g_1(x) \oplus g_2(y),$$

$x \in \{0,1\}^n,\ y \in \{0,1\}^m$ *is* $N_f = 2^{n+m-1} - 2^{\frac{1}{2}(n+m-1)}$.

Proof. The result of the above construction is a function of odd dimension. It is evidently balanced, since due to the balanced nature of function g_2 the truth table of function g_1 is used exactly as many times as its negated version

is, which automatically provides the balancedness of f. Let us see which are the vectors for which the function f will not satisfy the propagation criterion.

If $f(g_1(x_0, x_1, \ldots, x_{n-1}),\ g_2(y_0, y_1, \ldots, y_{m-1})) = g_1(x_0, x_1, \ldots, x_{n-1}) \oplus \oplus g_2(y_0, y_1, \ldots, y_{m-1})$, f is already interpreted in $\{0,1\}^{n+m}$ and

$$f(x_0, x_1, \ldots, x_{n-1}, y_0, y_1, \ldots, y_{m-1}) = \\ = g_1(x_0, x_1, \ldots, x_{n-1}) \oplus g_2(y_0, y_1, \ldots, y_{m-1}).$$

If we take that $x = (x_0, x_1, \ldots, x_{n-1}) \in \{0,1\}^n$ and $y = (y_0, y_1, \ldots, y_{m-1}) \in \{0,1\}^m$, the result will be

$$f(x_0, x_1, \ldots, x_{n-1}, y_0, y_1, \ldots, y_{m-1}) = g_1(x) \oplus g_2(y).$$

Let $a \in \{0,1\}^{n+m},\ a = (a_{x_0}, a_{x_1}, \ldots, a_{x_{n-1}},\ a_{y_0}, a_{y_1}, \ldots, a_{y_{m-1}})$, let us denote as $a_x = (a_{x_0}, a_{x_1}, \ldots, a_{x_{n-1}})$ and $a_y = (a_{y_0}, a_{y_1}, \ldots, a_{y_{m-1}})$, in which case

$$f(a) = f(a_x, a_y) = f(g_1(a_x), g_2(a_y)) = g_1(a_x) \oplus g_2(a_y).$$

The formula $z \in \{0,1\}^{n+m},\ z = (x_0, x_1, \ldots, x_{n-1},\ y_0, y_1, \ldots, y_{m-1})$ gives

$$f(z \oplus a) =$$

$$f(x_0, x_1, \ldots, x_{n-1},\ y_0, y_1, \ldots, y_{m-1} \oplus a_{x_0}, a_{x_1}, \ldots, a_{x_{n-1}},\ a_{y_0}, a_{y_1}, \ldots, a_{y_{m-1}}) = \\ = g_1(x \oplus a_x) \oplus g_2(y \oplus a_y).$$

The satisfaction of propagation criterion means that function $f(z) \oplus f(z \oplus a)$ is balanced. Let us see, which are the vectors for which

$$\sum_{z \in \{0,1\}^{n+m}} (-1)^{f(z) \oplus f(z \oplus a)} = 0$$

is not fulfilled.

Due to the previous considerations,

$$\sum_{z \in \{0,1\}^{n+m}} (-1)^{f(z) \oplus f(z \oplus a)} = \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^m} (-1)^{g_1(x) \oplus g_2(y) \oplus g_1(x + a_x) \oplus g_2(y + a_y)}.$$

The order of summation may be changed, the constant values of the sum can be taken out with the following output

$$\sum_{z \in \{0,1\}^{n+m}} (-1)^{f(z) \oplus f(z \oplus a)} = \sum_y (-1)^{g_2(y) \oplus g_2(y \oplus a_y)} \left(\sum_x (-1)^{g_1(x) \oplus g_1(x \oplus a_x)} \right).$$

Since the function g_1 is bent, it satisfies the propagation criterion except for the vector $a_x = (0, 0, \ldots, 0)$, it means that the sum rendered to x is zero for all except $a_x = (0, 0, \ldots, 0)$. In the position $a_x = (0, 0, \ldots, 0)$ it produces the value 2^n. By using the terminology in Corollary 11 of [8], the elements of set $\Re$ are not more than the vectors of $\{0,1\}^m$, concatenated with point $(0, 0, \ldots, 0) \in \{0,1\}^n$, which, on the other hand, satisfies the conditions of Corollary 11 in [8]. So the nonlinearity value of function f will be

$$N_f = 2^{n+m-1} - 2^{\frac{1}{2}(n+m-1)}.$$

Examples in [8] and in this study can be termed with the following data:

1. If $g_2(x_0) \equiv 0$, then $f(g_1, g_2) : \{0,1\}^{n+1} \to \{0,1\}$ and we come back to the function mentioned first, that is the copy of the bent truth table.

2. If $m = 1$ and $g_2(x_0) = x_0$ then $f(g_1, g_2) : \{0,1\}^{n+1} \to \{0,1\}$ where we are getting the copy of the negated of the bent truth table, and so we obtain the second example in [8].

3. If $m = 5$ and $g_2 = (1 \oplus x_0)(l \oplus x_1)x_2 \oplus (1 \oplus x_0)x_1x_3 \oplus x_0(1 \oplus x_1)(x_2 \oplus x_3) \oplus \oplus x_0x_1(x_3 \oplus x_4)$ then we arrive at Example 1 in [8].

Example 3 in [8] is motivated by Lemma 2 of [6]. To make the proof easier we can change this lemma by using a constructive point of view.

Proposition 2. *Let* $m \leq n$, $g_i : \{0,1\}^m \to \{0,1\}$ $i = 0, 1, \ldots, 2^m - -1$, *where for* $x \in \{0,1\}^m$

$$g_i(x) = \begin{cases} 1 & \text{if } x = i, \\ 0 & \text{otherwise,} \end{cases}$$

$f_{\alpha_i} : \{0,1\}^n \to \{0,1\}$, $\alpha_i \in \{0,1\}^n$ $\alpha_i = 0, 1, \ldots, 2^m - 1$ *be a linear function, whose coefficients produce the binary form of integer number* α_i, *that is* $f_{\alpha_i} = = \alpha_i y$ *for all* $y \in \{0,1\}^n$, *and* $\alpha_i = 1, \ldots, 2^m$ *can be taken in order to keep the balancedness.*

In this case, $f : \{0,1\}^{n+m} \to \{0,1\}$, *which is created from* f_{α_i} *and* g_i *on the basis of Lemma 2 of [6] in the following manner*

$$f = \bigoplus_{i=0}^{2^m-1} g_i f_{\alpha_i}.$$

It is a function whose non-linearity value is $N_f = 2^{n+m-1} - 2^{\frac{1}{2}(m+n)}$ *if* $m = n$ *and* $N_f = 2^{n+m-1} - 2^{\frac{1}{2}(m+n-1)}$ *if* $m + n$ *is odd.*

Proof. Let $x \in \{0,1\}^m$, $x = (x_0, x_1, \ldots, x_{m-1})$, $y \in \{0,1\}^n$, $y = (y_0, y_1, \ldots, y_{n-1}), z \in \{0,1\}^{m+n}$, $z = (x_0, x_1, \ldots, x_{m-1}, y_0, y_1, \ldots, y_{n-1}) = (x, y)$ and $a \in \{0,1\}^{m+n} = (a_{x_0}, \ldots, a_{x_{m-1}}, a_{y_0}, \ldots, a_{y_{n-1}}) = (a_x, a_y)$.

Let $\alpha_x \in \{0,1\}^n$ be the vector of the coefficients of linear function with value $x = i$.

The function generated by f will be $\overline{f}(z) = (-1)^{\bigoplus_{i=0}^{2^m-1} f_{\alpha_i}(y) g_i(x)}$.

We check for $a \in \{0,1\}^{n+m}$ vectors, for which the function f fails to satisfy the propagation criterion. The satisfaction of the propagation crietion means, that $\sum_{z \in \{0,1\}^{n+m}} (-1)^{f(z) \oplus f(z \oplus a)} = 0$.

$$\sum_{z \in \{0,1\}^{n+m}} (-1)^{f(z) \oplus f(z \oplus a)} = \sum_{x \in \{0,1\}^m,\ y \in \{0,1\}^n} (-1)^{f(x,y) \oplus f((x,y) \oplus (a_x, a_y))} =$$

$$= \sum_{x=0}^{2^m-1} \left(\sum_{y=0}^{2^n-1} (-1)^{f(x,y) \oplus f((x,y) \oplus (a_x, a_y))} \right) =$$

$$= \sum_{x=0}^{2^m-1} \left(\sum_{y=0}^{2^n-1} (-1)^{\bigoplus_{i=0}^{2^m-1} g_i(x) f_{\alpha_i}(y) \oplus \bigoplus_{i=0}^{2^m-1} g_i(x \oplus a_x) f_{a_i}(y \oplus a_y)} \right) =$$

$$= \sum_x \sum_y (-1)^{f_{a_x}(y)} (-1)^{f_{\alpha_x \oplus a_x}(y \oplus a_y)} =$$

$$= \sum_x \sum_y (-1)^{a,y} (-1)^{\alpha_{x \oplus a_x} y \oplus \alpha_{x \oplus a_x} a_y}.$$

Factoring out the constant elements of the sum the following expression is received

$$\sum_{z \in \{0,1\}^{n+m}} (-1)^{f(z) \oplus f(z \oplus a)} = \sum_x (-1)^{\alpha_{x \oplus a_x} a_y} \sum_y (-1)^{(\alpha_x \oplus \alpha_{x \oplus a_x}) y},$$

$$\sum_y (-1)^{(\alpha_x \oplus \alpha_{x \oplus a_x}) y} = \begin{cases} 2^n & \text{if } (\alpha_x \oplus \alpha_{x \oplus a_x}) = 0, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\sum_x (-1)^{\alpha_{x \oplus a_x} a_y} = \begin{cases} 2^m & \text{if } a_y = 0, \\ 0 & \text{otherwise.} \end{cases}$$

So the vectors for which function f fails to satisfy propagation criterion are as follows.

1. In the case of $m = n$ the $(0, \ldots, 0)$ vector and the resulted function f is bent.

2. In the case of $m = n-1$ the $z \in \{0,1\}^{2n-1}$ vectors, for which either $a_x = (0, \ldots, 0)$ and $a_y = (0, \ldots, 0)$ or $a_x = (0, \ldots, 0)$ and $a_y = (1, 0, \ldots, 0)$ is true. These vectors, however, satisfy the conditions of Corollary 11 in [8], so the proposition is proved.

3. In the case of $m < n - 1$ the propagation criterion will not be satisfied in all cases when $a_x = (0, \ldots, 0)$ and $a_y = (y_0, \ldots, y_{n-m-1}, 0, \ldots, 0)$, and there exist exactly 2^{n-m} such points. In fact, if $m + n$ is odd the resulted function satisfies the conditions of Corollary 11 in [8] so its nonlinearity is as high as possible.

Note that the case $m = n - 1$ corresponds to Example 3 of [8].

4. Summary

The two propositions provide the general conception of some examples known from literature, by the use of superposition. Superposition, as a principle of construction may answer the question whether the functions preferred in cryptographic applications can or cannot be classified under one or more clones of the Boolean-functions.

Bibliography

[1] **Adams C.M. and Tavares S.E.,** Generating and counting binary bent sequences, *IEEE Transactions on Information Theory,* **IT-36** (5) (1990), 1170-1173.

[2] **Beauchamp K.G.,** *Walsh functions and their applications,* Academic Press, London-New York-San Francisco, 1975.

[3] **Pásztor-Varga K.,** Boole függvények Boole algebrájának strukturális tulajdonságait felhasználó Boole függvény optimizációs módszer, *Alk. Mat. Lapok,* **13** (1987-88), 69-76.

[4] **Rothaus O.S.,** On "bent" functions, *J. of Combinatorial Theory,* Ser. A, **20** (1976), 300-305.

[5] **Siegenthaler T.,** Correlation-immunity of nonlinear combining functions for cryptographic applications, *IEEE Transactions on Information Theory,* **IT-30** (5) (1984), 776-779.

[6] **Seberry J., Zhang X.M. and Zheng Y.,** Nonlinearity and propagation characteristics of balanced Boolean functions, *Information and Computation,* **119** (1) (1995),1-13.

[7] **Vajda I., Buttyán L. és Szekeres B.,** *Az algoritmikus adatvédelem módszerei,* Technical University of Budapest (non-published manuscript)

[8] **Zhang X.M. and Zheng Y.,** New lower bounds on nonlinearity and class of highly nonlinear functions, *Information Security and Privacy, Second Australian Conference, Sidney, Australia, July 1997,* Lecture Notes in Computer Science **1270**, Springer, 1997, 147-158.

Appendix

The 3 examples in [8].

Example 1.

Let $g(x_1, x_2, x_3, x_4, x_5) = (1 \oplus x_1)(1 \oplus x_2)x_3 \oplus (1 \oplus x_1)x_2x_4 \oplus x_1(1 \oplus x_2)(x_3 \oplus \oplus x_4) \oplus x_1x_2(x_4 \oplus x_5)$ and $f(u, v) = g(v) \oplus h(u)$, where $v \in V_5$ and h is a bent function on V_{n-5}. The set $\Re$ associated with f is composed of five vectors: $(0, \ldots, 0)$, $(0, 0, 0, 1, 0, \ldots, 0)$, $(0, 0, 1, 0, 0, \ldots, 0)$, $(0, 1, 0, 1, 0, \ldots, 0)$ and $(0, 1, 1, 0, 0, \ldots, 0)$. Let W be the set of the following four vectors: $(0, \ldots, 0)$, $(0, 0, 1, 1, 0, \ldots, 0)$, $(0, 1, 0, 0, 0, \ldots, 0)$ and $(0, 1, 1, 1, 0, \ldots, 0)$. It is easy to verify that W is a 2-dimensional subspace and $\Re - \{0\} \subset (0, 0, 0, 1, 0, \ldots, 0) \oplus W$. Hence $\Re$ is covered by $(0, 0, 0, 1, 0, \ldots, 0) \oplus W$ and by Corollary 14 the Walsh-transform of its generated function takes the value of 0 or $\pm 2^{\frac{n+1}{2}}$ and the nonlinearity of f takes the value $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

Example 2.

Consider $f(x) = cx_1 \oplus g(x_2, \ldots, x_n)$, where $x = (x_1, \ldots, x_n)$, $c \in GF(2)$, and g is a bent function on V_{n-1}. $\Re = \{(0, \ldots, 0), (1, 0, \ldots, 0)\}$. Obviously f satisfies the conditions mentioned in Corollary 11. By Corollary 14 the Walsh-transform of its generated function takes on the value on 0 or $\pm 2^{\frac{n+1}{2}}$, so the nonlinearity of $f(x)$ is $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$.

Example 3.

Let e_i be the i-th row of H_k. Hence $e_0, e_1, \ldots, e_{2^k-1}$ are the sequences of all the 2^k linear functions on V_k. Note that the length of each linear sequence e_i is 2^k. Thus one can see that the concatenation of any 2^{k-1} different linear sequences of length $2k$ is the sequence of a function on V_{2k-1} and the Walsh-transform of its generated function takes on the value of 0 or $\pm 2^{\frac{n+1}{2}}$. The nonlinearity of the constructed function takes the value $N_f = 2^{2k-1-1} - 2^{\frac{1}{2}(2k-1-1)}$.

(Received March 4, 2002)

I. Licskó
Budapesti Gazdasági Főiskola
Kereskedelmi, Vendéglátóipari és Idegenforgalmi Kar
Informatikai Intézet
H-1054 Budapest, V.
Alkotmány u. 9-11.
licsko@mail.edu.kvif.hu