Annales Univ. Sci. Budapest., Sect. Comp. 25 (2005) 3-11

RELATION BETWEEN BENT FUNCTIONS AND HIGHLY NONLINEAR FUNCTIONS

I. Licskó (Budapest, Hungary)

Abstract. The highly nonlinear odd-dimensional Boolean-functions have many applications in the cryptographic practice, that is why the research of this class of functions and the construction of such functions has a great importance. This study focuses on some types of functions having special characteristics in the class of highly nonlinear odd-dimensional Boolean-functions. Upper bound can be given for the number of non-zero linear structures of such functions [2]. The relation between bent functions and highly nonlinear odd-dimensional functions is shown in this article.

1. Introduction

Different types of ciphers use Boolean functions. So, LFSR based stream ciphers use Boolean functions as a nonlinear combiner or a nonlinear filter, block ciphers use Boolean functions in substitution boxes and so on. Boolean functions used in ciphers must satisfy some specific conditions to resist different attacks. One of the most important properties of the Boolean functions desired for a LFSR based stream cipher is the nonlinearity. Other important properties are correlation immunity, high algebraic degree, balancedness and so on. For Boolean functions used in block ciphers the most important properties are nonlinearity and differential (or autocorrelation) characteristics (propagation degree, avalanche criterion, the absolute indicator and so on) based on the autocorrelation coefficients of Boolean functions.

2. Preliminaries

The mapping $f : \{0,1\}^n \to \{0,1\}$ is called a *Boolean-function*. Sometimes the mapping $\overline{f} : \{0,1\}^n \to \{-1,1\}$ is used instead of the Boolean-function. The relation between $\overline{f}$ and f can be described as follows

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

or

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

In the following we use the notation $\overline{f}(x)$ to denote the whole $\{-1,1\}$ sequence generated by $f(x)$, that means $\overline{f}(x)$ can be regarded as a vector having 2^n elements.

The elements of the set $\{0,1\}^n$ can be regarded as vectors. In this case $\{0,1\}^n$ is a vector space called Boolean-space. As the coordinates of these vectors are the numbers 0 and 1, the vector can be regarded as an integer written in binary form. We can refer to a vector by an integer and in this case the components of the vector show the binary representation of the integer. It is also possible to refer to a vector by an indexed name where the index is the integer corresponding to the vector.

The weight of a function $f(x)$ is 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 is equal, that is $\sum\limits_{x \in \{0,1\}^n} \overline{f}(x) = 0$, and the weight of a balanced function is $w(f) = 2^{n-1}$.

Ordinary *operations* are defined by components in GF(2). If $a, b \in \{0,1\}^n$, $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$, then $a \oplus b = (a_0 \oplus b_0,\ a_1 \oplus b_1, \ldots, a_{n-1} \oplus b_{n-1})$ is the *sum* and $ab = \bigoplus\limits_{i=0}^{n-1} a_i b_i$ is the *scalar product* of the two vectors.

If the Zhegalkin-polynomial of the Boolean-function $f(x_0, x_1, \ldots x_{n-1})$ is equal to

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

where $c, a_i \in \{0,1\}$ for $0 \leq i \leq n-1$, the function is called *affine*, and the function is *linear* in the special case if $c = 0$. A linear function can be regarded as the scalar product of the vector x of the variables and the constant $a \in \{0,1\}^n$. The function f satisfies the *propagation criterion* regarding an element $a \in \{0,1\}^n$, $a \neq 0$, if $f(x) \oplus f(x \oplus a)$ is balanced. The distance between the functions f and g is

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

while their correlation is defined as

$$c(f,g) = \sum_{x \in \{0,1\}^n} \overline{f}(x)\overline{g}(x) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus g(x)} = 2^n - 2d(f,g).$$

The *autocorrelation* function $r_f(a)$ of f is defined as

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

This expression is in principle the scalar product of the 2^n-dimensional vectors $\xi(0)$, $\xi(a)$, where $\xi(0)$ is given by $\overline{f}(x)$ and $\xi(a)$ is given by $\overline{f}(x+a)$.

A matrix $H = (h_{i,j})$, where $h_{ij} \in \{-1,1\}$ for $i,j = 0,1,\ldots,m-1$, is called Hadamard matrix if $HH^T = mI$. H^T means the transpose of H, and I is the identity matrix of order m. The 2^n-order Hadamard-matrix is denoted by H_n and it can be generated by the following recursive process:

$$H_0 = 1, \quad H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}, \quad n = 1,2,\ldots .$$

The rows of H_n are denoted by l_i, $i = 0,1,\ldots,2^n-1$. l_i can be regarded as a $\{-1,1\}$ sequence generated by the linear function ix. The $\{-1,1\}$ sequences of all linear functions in $\{0,1\}^n$ appear in the rows of H_n.

The *Walsh-transform* of the function f at $a = (a_0, a_1, \ldots, a_{n-1}) \in \{0,1\}^n$ is

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

while the *Walsh-transform* of $\overline{f}$ is defined as

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

The value $\overline{F}(a)$ is the correlation of function f with the linear functions ax and it can be written as the scalar product $(\overline{f}(x)l_a)$.

A Boolean-function f is called *bent function*, if for all $a \in \{0,1\}^n$ the correlation of f with the linear function ax has constant absolute-value

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

The Wiener-Khintchine theorem represents the relation between the Hadamard-matrix H_n, the auto-correlation function of f and its correlation with the linear functions

$$\left(\overline{f}(x)\overline{f}(x \oplus a_0), \ldots, \overline{f}(x)\overline{f}\left(x \oplus a_{2^n-1}\right)\right) H_n = \left(\left(\overline{f}(x)l_0\right)^2, \ldots, \left(\overline{f}(x)l_{2^n-1}\right)^2\right),$$

where l_i means the rows of H_n (see [8]).

The non-linearity of a function f, denoted by N_f, is the distance between f and the set of affine functions

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

The minimal value of the non-linearity is 0, which is the non-linearity of the affine functions. The maximum of the non-linearity is obtained if $\left|\overline{f}(x)l_i\right| = 2^{\frac{n}{2}}$ for every i and this maximal value can be realized by the bent functions, whose non-linearity $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$. Such functions exist only in a space of even dimensions. Despite their favourable characteristics with respect to the non-linearity they are not preferred for cryptographic applications because these functions are never balanced, correlation-immune, etc.

In the cryptographic practice highly nonlinear functions are preferred to bent functions. Highly nonlinear functions exist only in odd dimensional Boolean-space, their correlation with the linear functions takes only the values 0 and $\pm C$ and the number of linear functions having nonzero correlation with the given functions is 2^{n-1}. Among the highly nonlinear functions one can find pairs of functions characterized as follows. Considering a given linear function, its correlation with the members of such a pair never takes the same absolute value and this statement is true for all linear functions. This characteristic can be formalized as follows. Let n be an odd positive integer and $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ highly nonlinear functions that means their correlation with linear functions takes only the values 0 and $\pm C$ and the number of linear functions having non-zero correlation with the two functions is 2^{2m}, where

$2m = n - 1$. The set of linear functions having non-zero correlation with g_1 is disjoint from the set of linear functions having non-zero correlation with g_2 if and only if $(\overline{g}_1(x)l_i)^2 + (\overline{g}_2(x)l_i)^2 = 2^{2n-2m}$ for each $i = 0, 1, \ldots, 2^{n-1}$. The two sets of linear functions are disjoint when from $(\overline{g}_1(x)l_i)^2 = 0$ follows that $(\overline{g}_2(x)l_i)^2 \neq 0$, and conversely.

3. Relation between bent functions and highly nonlinear odd dimensional functions

It is possible to construct bent functions of a one-level higher dimension by the use of odd dimensional highly non-linear functions. Let us consider a pair of highly nonlinear functions g_1 and g_2 whose correlation with a given linear function never takes the same absolute value. The following algorithm can be applied. Copying the truth-table of g_2 after the truth-table of g_1 so that in the rows of g_1 $x_n = 0$ and in the rows of g_2 $x_n = 1$ is written respectively, the resulting truth-table is the truth-table of a bent function in a one-level higher dimension. This can be formulated by

$$f = (x_n \oplus l)g_1 \oplus x_n g_2.$$

In this way we can produce two bent functions from a pair of highly nonlinear functions. The conditions are given in

Theorem 1. *Let n be an odd positive integer, $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ Boolean-functions whose correlation with the linear-functions takes only the vales 0 and $\pm C$. The number of the linear functions having non-zero correlation with the given functions is 2^{2m} for both functions and $(\overline{g}_1(x)l_i)^2 + (\overline{g}_2(x)l_i)^2 = 2^{2n-2m}$ for each $i = 0, 1, \ldots, 2^{n-1}$. The functions $f_1, f_2 : \{0,1\}^{n+1} \to \{0,1\}$, in detail*

$$f_1(x_0, \ldots, x_{n-1}, x_n) = (x_n \oplus 1)g_1(x_0, \ldots, x_{n-1}) \oplus x_n g_2(x_0, \ldots, x_{n-1})$$

and

$$f_2(x_0, \ldots, x_{n-1}, x_n) = (x_n \oplus 1)g_2(x_0, \ldots, x_{n-1}) \oplus x_n g_1(x_0, \ldots, x_{n-1}),$$

constructed in this manner are $n+1$ dimensional Boolean-functions, and they are bent functions in the $n+1$ dimensional Boolean-space.

Proof. The function-values for both functions are

$$f_1(x_0, \ldots, x_{n-1}, x_n) = \begin{cases} g_1(x_0, \ldots, x_{n-1}) & \text{if } x_n = 0, \\ g_2(x_0, \ldots, x_{n-1}) & \text{if } x_n = 1 \end{cases}$$

and

$$f_2(x_0,\ldots,x_{n-1}x_n)=\begin{cases} g_2(x_0,\ldots,x_{n-1}) & \text{if } x_n=0,\\ g_1(x_0,\ldots,x_{n-1}) & \text{if } x_n=1.\end{cases}$$

Let us use the following notations

$$y\in\{0,1\}^{n+1},\ b\in\{0,1\}^{n+1},\ x\in\{0,1\}^n,\ a\in\{0,1\}^n,$$

$$y=(x_0,\ldots,x_{n-1},x_n),\ y=(x,x_n),\ b=(a_0,\ldots,a_{n-1},b_n),\ b=(a,b_n).$$

The correlation-value of f_1 with the linear function by is

$$(\overline{f}_1(y)l_k)=\sum_{y=0}^{2^{n+1}-1}(-1)^{f_1(y)\oplus by},$$

where $yb=ax+b_nx_n$ is the scalar product of y and b. This equation above can be split in two sums:

$$(\overline{f}_1(y)l_k)=\sum_{y=0}^{2^{n+1}-1}(-1)^{f_2(y)\oplus by}=\sum_{\substack{x=0\\x_n=0}}^{2^n-1}(-1)^{(x_n\oplus1)g_1(x)\oplus x_ng_2(x)\oplus ax\oplus b_nx_n}+$$
$$+\sum_{\substack{x=0\\x_n=1}}^{2^n-1}(-1)^{(x_n\oplus1)g_1(x)\oplus x_ng_2(x)\oplus ax\oplus b_nx_n}.$$

Upon having done the operations we get

$$(\overline{f}_1(y)l_k)=\pm2^{\frac{2n-2m}{2}}=\pm2^{\frac{n+1}{2}}$$

for any linear function. With f_2 we get the same result, so our proposition is proved.

Theorem 2. *If n is an even positive integer and $f:\{0,1\}^n\to\{0,1\}$ is a bent-function, then f can be written in the following form*

$$f(x_0,\ldots,x_{n-2},x_{n-1})=(x_n\oplus1)g_1(x_0,\ldots,x_{n-2})\oplus x_ng_2(x_0,\ldots,x_{n-2}),$$

so that $g_1,\ g_2:\{0,1\}^{n-1}\to\{0,1\}$ are highly nonlinear functions in the $n-1$ dimensional Boolean-space and they fulfill the condition $(\overline{g}_1(x)l_i)^2+(\overline{g}_2(x)l_i)^2=2^{2n-2m}$ for each $i=0,1,\ldots,2^{n-1}$, where l_i is the ith row of H_{n-1}.

Remark. This means that the truth-table of f can be cut into two parts so that one of them is the truth-table of the function g_2 and the other part is the truth-table of g_1 and both of them are highly nonlinear functions in a

one-level lower dimension. In the rows of g_1 a 0 and in the rows of g_2 a 1 is written in the column denoted by x_{n-1}, respectively.

Proof. Let us use the following notations:

$$(x_0,\ldots,x_{n-2},x_{n-1}) = x \in \{0,1\}^n,\ (x_0,\ldots,x_{n-2}) = y \in \{0,1\}^{n-1},$$

$$x = (y,x_{n-1}),\ (i_0,\ldots,i_{n-2},i_{n-1}) = i \in \{0,1\}^n,\ j \in \{0,1\}^{n-1},\ i = (j,i_{n-1}).$$

Because f is a bent-function, it is true for each i that

$$\sum_{x=0}^{2^n-1} (-1)^{f(x)\oplus ix} = \pm 2^{\frac{n}{2}}.$$

The sum on the left hand side can be decomposed in two sums and using the introduced notations we get

$$\sum_{\substack{x=0\\x_n=0}}^{2^{n-1}-1} (-1)^{f(x_0,\ldots,x_{n-2},0)\oplus(i_0,\ldots,i_{n-2},i_{n-1})(x_0,\ldots,x_{n-2},0)} +$$

$$+ \sum_{\substack{x=0\\x_n=1}}^{2^{n-1}-1} (-1)^{f(x_0,\ldots,x_{n-2},1)\oplus(i_0,\ldots,i_{n-2},i_{n-1})(x_0,\ldots,x_{n-2},1)} = \pm 2^{\frac{n}{2}}.$$

Upon having done the operations one can see that both of $f(x_0,\ldots,x_{n-2},0)$ and $f(x_0,\ldots,x_{n-2},l)$ are $n-1$-dimensional functions. Substituting $f(x_0,\ldots,x_{n-2},0)$ by $g_1(x_0,\ldots,x_{n-2})$ and $f(x_0,\ldots,x_{n-2},1)$ by $g_2(x_0,\ldots,x_{n-2})$ we get

$$\sum_{y=0}^{2^{n-1}-1} (-1)^{g_1(y)\oplus jy} + \sum_{y=0}^{2^{n-1}-1} (-1)^{g_2(y)\oplus jy} = \pm 2^{\frac{n}{2}},$$

or

$$\sum_{y=0}^{2^{n-1}-1} (-1)^{g_1(y)\oplus jy} - \sum_{y=0}^{2^{n-1}-1} (-1)^{g_2(y)\oplus jy} = \pm 2^{\frac{n}{2}},$$

depending on the value of i_{n-1}. After squaring the two equations and adding them together we get

$$(\overline{g}_1(y)l_j)^2 + (\overline{g}_2(y)l_j)^2 = 2^n$$

for each j. As g_1 and g_2 are $n-1$ dimensional functions and $2m = (n-1)-1$,

$$n = 2(n-1) - 2m,$$

that is the two functions fulfill the criterion of $(\overline{g}_1(x)l_i)^2+(\overline{g}_2(x)l_i)^2 = 2^{2n-2m}$, so they have the stated properties.

4. Summary

The results indicate that there is a relationship between bent functions and highly nonlinear functions. A pair of highly nonlinear functions defines two bent functions in a one-level higher dimension and the bent functions define a pair of highly nonlinear functions in a one-level lower dimension.

Acknowledgement. I should like to express my sincere thanks to Professor Dr. Tibor Nemetz and Associate Professor Mrs. Katalin Pásztor Varga Dr. for whose encouragement and valuable technical advices I am deeply grateful.

Bibliography

[1] **Licskó I.,** On highly nonlinear functions, *Annales Univ. Sci. Budapest. Sect. Comp.,* **21** (2002), 165-175.

[2] **Licskó I.,** Construction of highly nonlinear functions, *Annales Univ. Sci. Budapest. Sect. Comp.,* **23** (2004), 179-192.

[3] **Pásztor-Varga K.,** Boole függvények Boole algebrájának strukturális tulajdonságait felhasználó Boole függvény optimizációs módszer, *Alkalmazott Mat. Lapok,* **13** (1987-88), 69-76. (An optimizing method for Boolean functions applying the structural properties of the Boolean algebra of the Boolean functions, *Alkalmazott 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 Trans. 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. and Szekeres B.,** *Az algoritmikus adatvédelem módszerei (Methods of algorithmic data protection),* 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.

(Received March 18, 2002)

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