Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 16-19*

Note: On a Class of Boolean Functions [1]

Yuri Borissov youri@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
8 G. Bonchev str., 1113, Sofia, BULGARIA
Krassimir Manev manev@fmi.uni-sofia.bg
Faculty of Mathematics and Informatics, Sofia University
5 J. Bourchier blvd., 1164, Sofia, BULGARIA
and
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
8 G. Bonchev str., 1113, Sofia, BULGARIA

Abstract. In this note, we present an initial attempts to study a class of Boolean functions which might be useful in some coding-theoretical and cryptographic considerations. Some suggestions for future research are proposed.

1 Introduction

When studying Boolean functions (BFs) it is helpful to take into account the different types of equivalence relations among them. As a rule these relations keep invariant many of coding-theoretical and cryptographic properties of the functions, like the distributions of absolute Walsh and autocorrelation spectrum, as well as the properties derived by latter ones, as nonlinearity, balancedness (more generally coset weight distribution), dimension of the linear space, GAC indicators, distances to functions with non-zero linear structures [5], etc. Of course, these equivalence relations come from the action of corresponding groups of transformations on the set of variables. Usually, in this connection the role of some general groups is studied, e.g., the general affine (or the general linear) group $AGL(m,2)$ ($GL(m,2)$) (see, [2] and [3]), but sometimes much can be gained also when considering their subgroups (like the cyclic group C_m or the dihedral group D_m), and even only separate transformations (see, e.g., [7], [1] and [6]).

In this note, we present our initial efforts to investigate the properties of BFs under the action of one such transformation that takes function's variables in reverse order, and show that these properties are interesting from combinatorial and coding-theoretical point of view.

[1]This work is suported by the Found Scientific Research of Sofia University "St. Kliment Ohridski" by a Contract with the preliminary number 182/2009.

2 Some preliminaries

Let $x_1, x_2, \ldots, x_n$ be n Boolean variables. The function $f : \{0,1\}^n \to \{0,1\}$ is called ***Boolean function*** (BF) on n variables. We shall denote by $\mathcal{F}_n$ the set of BFs on n variables and by $\mathcal{F} = \bigcup \mathcal{F}_n, n = 1, 2, 3, \ldots$ the set of all BFs, respectively. If the vectors of $\{0,1\}^n$ are lexicographically ordered: ($\alpha_0 = \mathbf{0}, \alpha_1, \ldots, \alpha_{2^n-1} = \mathbf{1}$) then each Boolean function $f \in \mathcal{F}_n$ can be represented by the vector-column $\beta = (b_0, b_1, \ldots, b_{2^n-1})$ (also called truth-table of f), where $b_i = f(\alpha_i), i = 0, 1, \ldots, 2^n - 1$. Another useful representation of f is by its ***Zhegalkin polynomial*** [4] (also known as ***Algebraic Normal Form*** of f), $P_f(x_1, x_2, ..., x_n)$ that is a formulae over the set of BFs $Z = \{0, 1, xy, x \oplus y\}$ which gives the value of f for every assignment of $x_1, x_2, \ldots, x_n$. A Boolean function f possessing linear polynomial P_f is called ***linear***. We shall also, denote by L_n (and by L), the set of the linear BFs in $\mathcal{F}_n$ (the set of all linear BFs, respectively).

Definition 1 *Let $\alpha = (a_1, a_2, \ldots, \alpha_n) \in \{0,1\}^n$. Then $\widetilde{\alpha} = (a_n, a_{n-1}, \ldots, a_1)$ is called **reverse** to α. If $\alpha = \widetilde{\alpha}$ then we call α **self-reverse** (or **palindrome-vector**).*

Definition 2 *Let $f(x_1, x_2, \ldots, x_n) \in \mathcal{F}_n$. The Boolean function $\widetilde{f}(x_1, x_2, \ldots, x_n)$ defined by $\widetilde{f}(x_1, x_2, \ldots, x_n) = f(x_n, x_{n-1}, \ldots, x_1)$ is called **reverse** to f. If $f = \widetilde{f}$ then f is called **self-reverse**.*

We will denote by $\widetilde{S}$ the set of the self-reverse BFs, and by $\widetilde{S_n} = \widetilde{S} \bigcap \mathcal{F}_n$ and $\widetilde{SL_n} = \widetilde{S} \bigcap L_n = \widetilde{S_n} \bigcap L$, respectively.

3 Properties of $\widetilde{S_n}$ as a class of BFs

Traditional problems, when a class of Boolean functions is considered, are: to finding the cardinality of this class; to decide is it closed or complete by the superposition of functions, in what relation it is with the important closed classes of Boolean functions - T_0, T_1, S, M, L (see, [4] for notations and more details), etc.?

Herein, we formulate some results in the aforementioned directions.

Lemma 1 *For any $n \geq 1$ there are $2^{\lceil \frac{n}{2} \rceil}$ palindrome-vectors, as well as $2^{n-1} - 2^{\lceil \frac{n}{2} \rceil - 1}$ pairs of reverse to each other vectors.*

Proposition 1 $|\widetilde{S_n}| = 2^{2^{n-1} + 2^{\lceil \frac{n}{2} \rceil - 1}}$.

Proposition 2 *For each Boolean function f: $(\widetilde{\widetilde{f}}) = f$.*

Proposition 3 *If $f \in \mathcal{F}_m$ and $g_1, \ldots, g_m \in \widetilde{S_n}$ then $f(g_1, \ldots, g_m)$ belongs to $\widetilde{S_n}$.*

Proposition 4 *Each BF $f \in \mathcal{F}_n$ and its negation $\overline{f} = f \oplus 1$ belong both to $\widetilde{S_n}$ or to $\mathcal{F}_n - \widetilde{S_n}$.*

Let us give some examples of self-reverse BFs. Clearly, we have $\widetilde{S_1} \equiv \mathcal{F}_1$, i.e. all BFs of one variable are self-reverse. For $n = 2$, the property to be self-reverse BF, coincides with the commutativity of that function. So, the self-reverse Boolean functions of two variables are: $0, xy, x \oplus y, x \vee y, x|y, x \equiv y, x \uparrow y$ and 1. Since the set generating all Zhegalkin polynomials is a subset of $\widetilde{S_2}$ we have

Proposition 5 $[\widetilde{S_2}] = [\widetilde{S}] = \mathcal{F}$, *where* $[\mathbf{F}]$ *is the closure of the set* $\mathbf{F}$ *of BFs generated by the superposition of BFs.*

Finally, we would like to mention that the property of self-reverseability is not preserved when a dummy variable is appended. For example, if $f(x, y, z) = xy$, then $\widetilde{f} = f(z, y, x) = yz$ and $f \neq \widetilde{f}$.

4 Coding-theoretical properties of $\widetilde{S_n}$

In this section, we consider Boolean functions as vectors of 2^n-dimensional vector space over $GF(2)$. Since $0 \in \widetilde{S_n}$, and obviously if $f, g \in \widetilde{S_n}$ then $f \oplus g \in \widetilde{S_n}$ (a particular case of Proposition 3), we have the following:

Proposition 6 *For any $n \geq 1$, $\widetilde{S_n}$ is a binary $[2^n, 2^{n-1} + 2^{\lceil \frac{n}{2} \rceil - 1}, 1]$-code.*

By the same reasoning the linear functions in $\widetilde{S_n}$ form a linear sub-code of that code:

Proposition 7 *For any $n \geq 1$, $\widetilde{SL_n}$ is a binary $[2^n, \lceil \frac{n}{2} \rceil + 1, 2^{n-1}]$-code.*

Also, since the all-one vector $\mathbf{1}$ belongs to $\widetilde{S_n}$ the following proposition holds

Proposition 8 *For any $n \geq 1$, the dual code $\widetilde{S_n}^{\perp}$ is a binary $[2^n, 2^{n-1} - 2^{\lceil \frac{n}{2} \rceil - 1}, \geq 2]$-code.*

5 Conclusion

In this note, we present an initial efforts to investigate combinatorial and coding-theoretical properties of one special class of BFs. Our future goal will be to deeper and extend this study in several directions. For instance, we aim to investigate into more details the cryptographic properties of these functions, and, of course, to find useful applications of them.

References

[1] T.W. Cusick, P. Stănică, Fast evaluation, weights and nonlinearity of rotation-symmetric functions, *Discr. Math.* 258, 2002, 289-301.

[2] X. D. Hou, $AGL(m, 2)$ acting on $R(r, m)/R(s, m)$, *J. Algebra* 171, 1995, 921-938.

[3] X. D. Hou, $GL(m, 2)$ acting on $R(r, m)/R(r-1, m)$, *Discr. Math.* 149, 1996, 99-122.

[4] Kr. Manev, *Introduction to Dicrete Mathematics*, 4-th edition, KLMN, Sofia, 2005 (in Bulgarian).

[5] W. Meier, O. Staffelbach, Nonlinearity criteria for cryptographic functions, Proc. of EUROCRYPT'89, LNCS 434, 1989, Springer-Verlag, 549-562.

[6] S. Kavut, M.D. Yücel, Generalized rotation-symmetric and dihedral symmetric Boolean functions – 9 variable Boolean functions with nonlinearity 242, Proc. of AAECC-17, LNCS 4851, 2007, Springer-Verlag, 321-329.

[7] J. Pieprzyk, C. X. Qu, Fast hashing and rotation-symmetric functions, *J. Univ. Comput. Science* 5, 1999, 20-31.