On properties of a bent function secondary construction

Nikolay Kolomeec

Sobolev Institute of Mathematics, Novosibirsk, Russia

Novosibirsk State University, Novosibirsk, Russia

Laboratory of Cryptography JetBrains Research

Abstract

Properties of a secondary bent function construction, that inverts values of a given bent function on an affine subspace, are obtained. Some results regarding normal and weakly normal bent functions are generalized. Bent functions and their dual functions are considered in the construction context.

1 Preliminaries

Let us recall some definitions. *A bent function* is a Boolean function in even number of variables that is at the maximal possible Hamming distance from the set of all affine Boolean functions. Bent functions were introduced by O. Rothaus [1]. Additional information regarding them can be found in [2, 3]. Let $\langle x, y\rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$, where $x, y \in \mathbb{F}_2^n$. Let us denote by Ind_S the characteristic function of a set $S \subseteq \mathbb{F}_2^n$ and by $D_\alpha f(x) = f(x) \oplus f(x \oplus \alpha)$ *the derivative* of a Boolean function f *in the direction* α. For $x \in \mathbb{F}_2^n$ and $k \le n$, let us define

$$\begin{aligned} Proj_k(x) &= (x_1, \ldots, x_k), \\ Proj_k(S) &= \{Proj_k(x) \mid x \in S\}, \\ Elem_k(S) &= \{x \in \mathbb{F}_2^k \mid (x, \underbrace{0, \ldots, 0}_{n-k}) \in S\}. \end{aligned}$$

Hereinafter we suppose that n is even. By $\mathcal{B}_n$ we denote the set of all bent functions in n variables, by $\widetilde{f}$ *the dual* bent function of $f \in \mathcal{B}_n$.

In this work, we consider properties of a bent function construction

$$f \oplus Ind_U,$$

where $f \in \mathcal{B}_n$ is a given bent function and U is an affine subspace of an arbitrary dimension. Necessary and sufficient conditions for $f \oplus Ind_U$ to be a bent function were proven by C. Carlet [4].

Theorem 1.1 (C. Carlet, 1994) *Let $f \in \mathcal{B}_n$, $L \subseteq \mathbb{F}_2^n$ be a linear subspace and $a \in \mathbb{F}_2^n$. Then $f \oplus Ind_{a\oplus L}$ is a bent function if and only if any of the following equivalent conditions hold:*

- *$D_\alpha f$ is balanced on $a \oplus L$ for all $\alpha \in \mathbb{F}_2^n \setminus L$;*
- *$\widetilde{f}(x) \oplus \langle a, x\rangle$ is either constant or balanced on each coset of $L^\perp$.*

We will use the second condition. The next two sections describe properties of a dual bent function $\widetilde{f}$.

2 A balanced representation

Let us introduce the following notion.

Definition 2.1 *A Boolean function f in n variables has a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^n$ if f is either constant or balanced on each coset of L.*

Note that any function has a balanced representation by the 0-dimensional linear subspace ("either constant or balanced" case allows us to ignore its odd cardinality). The same situation holds for a 1-dimensional linear subspace.

First of all, there are some additional details regarding balanced representations of bent functions.

Theorem 2.2 *Let $f \in \mathcal{B}_n$ and L be a linear subspace, $\dim L \leq n/2$. Then*

- *f has a balanced representation by L if and only if f is constant on each of some $2^{n-2\dim L}$ distinct cosets of L;*
- *f can not be constant on more than $2^{n-2\dim L}$ distinct cosets of L.*

Note that the case $\dim L = n/2$ is especially interesting for bent functions. A large class of normal bent functions for this representation was introduced by H. Dobbertin [5].

3 A balanced representation of iterative constructed functions

Let us consider the simplest iterative construction of a bent function f_{+2} by $f \in \mathcal{B}_n$:

$$f_{+2}(x_1, \ldots, x_{n+2}) = f(x_1, \ldots, x_n) \oplus x_{n+1}x_{n+2}.$$

Recall that $f_{+2} \in \mathcal{B}_{n+2}$ if and only if $f \in \mathcal{B}_n$. Also, it holds

$$\widetilde{f_{+2}}(x_1, \ldots, x_{n+2}) = \widetilde{f}(x_1, \ldots, x_n) \oplus x_{n+1}x_{n+2}.$$

The question is the following: whether the balanced representations for f and f_{+2} are connected or not.

Proposition 3.1 *Let $f \in \mathcal{B}_n$ have a balanced representation by $L \subseteq \mathbb{F}_2^n$. Then the bent function f_{+2} has balanced representations by*

- *$L_0 = \{(x, 0, 0) \mid x \in L\}$, i. e. $\dim L_0 = \dim L$;*
- *$L_1 = \{(x, y, 0) \mid x \in L, y \in \mathbb{F}_2\}$, i. e. $\dim L_1 = \dim L + 1$.*

Moreover, there is a "feedback" from the f_{+2} to f.

Theorem 3.2 *Let $f \in \mathcal{B}_n$ and suppose that f_{+2} have a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^{n+2}$. Then there exists a linear subspace $L' \subseteq \mathbb{F}_2^n$ with*

$$\dim L - 1 \leq \dim L' \leq \dim L$$

such that f has a balanced representation by L'. Moreover, it holds

$$Elem_n(L) \subseteq L' \subseteq Proj_n(L).$$

In case $\dim L = n/2 + 1$ Theorem 3.2 can be easily transformed to "f is normal if and only if f_{+2} is normal" that was proven in [6]. I. e. it is a generalization of weakly normal and normal bent function properties.

4 Subspaces for iterative constructed functions

Using Theorem 1.1, the results of Section 3 can be generalized to the construction properties.

Proposition 4.1 *Let $f \in \mathcal{B}_n$ and $f \oplus Ind_U \in \mathcal{B}_n$, where U is an affine subspace of $\mathbb{F}_2^n$. Then for the bent function f_{+2} the following statements hold:*

- $f_{+2} \oplus Ind_{U_1} \in \mathcal{B}_{n+2}$, *where* $U_1 = \{(x, y, 0) \mid x \in U, y \in \mathbb{F}_2\}$, *i. e.* $\dim U_1 = \dim U + 1$;
- $f_{+2} \oplus Ind_{U_2} \in \mathcal{B}_{n+2}$, *where* $U_2 = \{(x, y, z) \mid x \in U, y, z \in \mathbb{F}_2\}$, *i. e.* $\dim U_2 = \dim U + 2$.

Theorem 4.2 *Let $f_{+2} \in \mathcal{B}_{n+2}$ and $f_{+2} \oplus Ind_{a \oplus L} \in \mathcal{B}_{n+2}$, where $L \subseteq \mathbb{F}_2^{n+2}$ is a linear subspace, $a \in \mathbb{F}_2^{n+2}$. Then there exists a linear subspace $L' \subseteq \mathbb{F}_2^n$ with*

$$\dim L - 2 \leq \dim L' \leq \dim L - 1$$

such that $f \oplus Ind_{Proj_n(a) \oplus L'} \in \mathcal{B}_n$. Moreover, it holds

$$Elem_n(L) \subseteq L' \subseteq Proj_n(L).$$

Similarly to Theorem 3.2, in case $\dim L = n/2 + 1$, Theorem 4.2 can be reformulated in terms of weakly normal bent function properties.

Trivial subspace dimensions for $f \in \mathcal{B}_n$ are n (just negation of the function) and $n - 1$ (addition of an affine function). We can naturally exclude these dimensions from the construction.

Computational experiments (see Section 5) show that for the non-weakly normal bent function $f_{10} \in \mathcal{B}_{10}$ found in [7] (Fact 14) the following fact holds.

Fact 4.3 *For any affine subspace $U \subseteq \mathbb{F}_2^{10}$, $\dim U \leq 8$, it holds that $f_{10} \oplus Ind_U \notin \mathcal{B}_{10}$.*

Corollary 4.4 *For any $n \geq 10$, there exists a bent function $f \in \mathcal{B}_n$ such that $f \oplus \mathrm{Ind}_U \notin \mathcal{B}_n$ for any affine subspace $U \subseteq \mathbb{F}_2^n$ of dimension at most $n/2 + 3$.*

5 Search subspaces

For a given $f \in \mathcal{B}_n$, the algorithm described in [6] can help to construct all affine subspaces $U \subseteq \mathbb{F}_2^n$ (of an arbitrary dimension) such that $f \oplus Ind_U \in \mathcal{B}_n$. Though it constructs affine subspaces such that f is affine on each of them, it "sorts" cosets for a convenient usage in a balanced representation.

The algorithm complexity can be calculated in the following way:

$$n \sum_{m=1}^{n/2} \left(|L_m(\widetilde{f})| + (2^m - 2)|L_m^0(\widetilde{f})| \right) + \mathcal{O}(n2^n),$$

where $L_m(f)$ ($L_m^0(f)$) is the set of an m-dimensional affine subspaces such that f is affine (constant) on them.

6 Count of the constructed functions

For $f \in \mathcal{B}_n$ and $0 \leq m \leq n$, we define

$$Constr_m(f) = \{f \oplus Ind_U \mid U \text{ is an } m\text{-dimensional affine subspace of } \mathbb{F}_2^n\} \cap \mathcal{B}_n.$$

Theorem 6.1 *Let $f \in \mathcal{B}_n$ and $f \oplus Ind_U \in \mathcal{B}_n$, where U is an affine subspace of $\mathbb{F}_2^n$ of dimension at most $n/2 + 1$. Then*

$$\mathrm{supp}\{\widetilde{f} \oplus \widetilde{(f \oplus Ind_U)}\}$$

is an affine subspace too.

Corollary 6.2 *$|Constr_m(f)| = |Constr_m(\widetilde{f})|$ for $m \le n/2+1$.*

Unlike $n/2$ and $n/2+1$ dimensions, for other cases we have

- $\mathrm{supp}\{\widetilde{f} \oplus \widetilde{(f \oplus Ind_U)}\}$ may not be an affine subspace;
- $|Constr_m(f)|$ and $|Constr_m(\widetilde{f})|$ may not be equal; such bent functions in 8 variables exist, for instance, in Maiorana–McFarland class [8].

Thus, for an arbitrary subspace dimensions, some construction properties differ from the case $m = n/2$.

It is well known that $|Constr_m(f)| = 0$ for $m < n/2$. The following theorem estimates cardinalities of all other $Constr_m(f)$.

Theorem 6.3 *For $f \in \mathcal{B}_n$ and $m \ge n/2$, it holds*

$$|Constr_m(f)| \le 2^{n-m} \prod_{i=1}^{n-m} \frac{2^{2m+2i-n}-1}{2^i-1}.$$

Moreover, for $m \le n-2$, the bound is reached if and only if f is quadratic.

This estimate generalizes the bound from [9] for the case $m = n/2$.

Acknowledgement

The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314–2019–0017) and supported by Russian Foundation for Basic Research (project no. 20–31–70043) and Laboratory of Cryptography JetBrains Research.

References

[1] O. Rothaus *On bent functions.* J. Combin. Theory. Ser. A, 20(3), 300–305, 1976.

[2] O. A. Logachev, A. A. Salnikov, V. V. Yashchenko *Boolean Functions in Coding Theory and Cryptography.* American Mathematical Society, 2012.

[3] N. Tokareva *Bent Functions, Results and Applications to Cryptography.* Acad. Press. Elsevier, 2015.

[4] C. Carlet *Two new classes of bent functions.* LNCS, 765, 77–101, 1994.

[5] H. Dobbertin *Construction of bent functions and balanced Boolean functions with high nonlinearity.* LNCS, 1008, 61–74, 1995.

[6] A. Canteaut, M. Daum, H. Dobbertin, G. Leander. *Finding nonnormal bent functions.* Discrete Appl. Math., 154(2), 202–218, 2006.

[7] G. Leander, G. McGuire *Construction of bent functions from near-bent functions.* J. Combin. Theory. Ser. A, 116(4), 960–970, 2009.

[8] R. L. McFarland *A family of difference sets in non-cyclic groups* J. Combin. Theory. Ser. A, 15, 1–10, 1973.

[9] N. Kolomeec *The graph of minimal distances of bent functions and its properties.* Designs, Codes and Cryptography, 85(3), 395–410, 2017.