A. Marchenko

ON COMMUNICATION COMPLEXITY OF BENT FUNCTIONS FROM MAIORANA–MCFARLAND CLASS

Kazan (Volga Region) Federal University,
Institute of Computational Mathematics and Information Technologies, Department of Theoretical Cybernetics,
Kremlevskaya 35, Kazan, 420008, Russia

E-mail address: Anton.Marchenko@kpfu.ru

Abstract. In this article we study two party Communication Complexity of Boolean bent functions from Maiorana–McFarland class. In particular, we describe connections between Maiorana–McFarland construction of bent functions and operations on matrix form of Boolean functions and show that bent functions of $2n$ variables from Maiorana–McFarland class have deterministic communication complexity equal $n+1$. Finally, we show that not all bent functions have high communication complexity lower bound by giving the example of such function.

1. Introduction

1.1. **Bent functions.** Boolean functions play an important role in the construction of secure cryptographic primitives. Some special properties of Boolean functions can guarantee the resistance of the cryptosystems to the known attacks. One of this properties is bentness or extremely high nonlinearity. It can guarantee resistance to linear and differential attacks. Moreover, bent functions can serve as the basis to the other important classes of cryptographic Boolean functions, for example resilient functions that are high nonlinear and correlation immune.

Let $f : V_n \to \mathbb{F}_2$ be a Boolean function, where $\mathbb{F}_2$ is a finite field of 2 elements and V_n is an n-dimensional vector space over $\mathbb{F}_2$.

Nonlinearity is one of the main criteria for cryptographic Boolean function assessment.

2010 Mathematical Subject Classification. 46L51, 46L53, 46E30, 46H05.

Key words and phrases. bent functions, Maiorana–McFarland construction, communication complexity, log rank technique.

Any Boolean function has a unique algebraic normal form representation (Zhegalkin polynom or ANF):

$$f : V_n \to \mathbb{F}_2 = \sum_{I \subseteq \{1,\dots,n\}} a_I \prod_{i \in I} x_i (\text{mod } 2).$$

Affine Boolean functions are sums of linear functions and constants, thus they have algebraic degree of its algebraic normal form at most 1.

The Hamming weight $w_H(f)$ of Boolean function $f : V_n \to \mathbb{F}_2^n$ is the cardinality of its support $\{v \in V_n | \ f(v) = 1\}$.

The Hamming distance $d_H(f, g)$ between two Boolean functions is the Hamming weight of their difference $f + g$ taken modulo 2.

The nonlinearity of Boolean function f is the minimum distance from f to all affine functions. The highest possible value of nonlinearity of Boolean functions of n variables is $2^{n-1} - 2^{n/2-1}$. The class of Boolean functions, that are extremely high nonlinear, are called *bent* [1].

A comprehensive survey of bent functions is given by Tokareva in [2].

1.2. **Two-party Communication Complexity.** Communication complexity analyses the amount of communication bits needed to be exchanged by participants of a communication process in order to compute the value of some Boolean function. Yao [3] defined a two-party model with only two communicating parties Alice and Bob that need to evaluate a function $f(u, v)$ where Alice knows the first argument u and Bob knows the second argument v. Such model ignores all computational aspects except the amount of exchanged communication bits. Despite of model's simplicity different applications to many other fields such as VLSI, OBDD, finite automata, Turing machines and others were found.

Let us abbreviate classical (deterministic) two-party communication complexity as DCC.

2. Communication Complexity of bent functions from Maiorana–McFarland class

2.1. **Construction.** Maiorana–McFarland construction[4] is very important for specification of bent functions.

Construction describes Boolean bent functions of the form

$$f(u, v) = \sigma(u) \cdot v + g(v),$$

where $\sigma : V_n \to V_n$ is a permutation and $g : V_n \to \mathbb{F}_2$.

From the communicational point of view it is assumed that vectors are of the same size, vector u is given to Alice and v is given to Bob and both sides want to compute the value of function $f(u, v)$.

The set of all Boolean bent functions obtained by this construction forms Maiorana–McFarland class MM.

Let us denote bent functions of the form $f : V_n \oplus V_n \to \mathbb{F}_2$ from Maiorana–McFarland class as MM_n.

2.2. **Communication complexity of inner product.** In this paper we consider rank lower bound technique for estimating lower bounds of communication complexity and its application to Maiorana–McFarland's bent functions. Rank lower bound technique was proposed by Mehlhorn and Schmidt [5].

Their main theorem is:

Theorem 1. *Any function $f : X \oplus Y \to \mathbb{F}_2$ has $DCC \geq \log(2 * rank_{\mathbb{F}}(M_f) - 1)$ over any field $\mathbb{F}$.*

Considering the following fact the $rank_{\mathbb{R}}(M_f)$ is the highest rank value for M_f and, therefore, is the best possible lower bound for $DCC(f)$ that can be obtained by applying rank lower bound technique.

Claim 1. *Given an arbitrary matrix $M_{m\times n}$ with entries from $\mathbb{F}_2$ inequality $rank_{\mathbb{R}}(M) \geq rank_{\mathbb{F}}(M)$ holds true for any field $\mathbb{F}$*

Rank lower bound technique gives the exact value of $DCC(IP)$.

Theorem 2. *Inner product function $IP_n : V_n \oplus V_n \to \mathbb{F}_2$, $IP(u, v) = u \cdot v = \sum u_i v_i$ has deterministic two-party communicational complexity equal $n + 1$*

Let us define $\widetilde{IP}_n(u, v) = (-1)^{u\cdot v}$. Then we get $M_{\widetilde{IP}_1} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $M_{\widetilde{IP}_n} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n}$ by induction.

$M_{\widetilde{IP}_n}$ is a Hadamard matrix of Sylvester type and has a full rank. On the other hand $M_{\widetilde{IP}_n} = 2M_{IP_n} - J$, where J is matrix of all-ones.

From the simple algebraic fact presented below follows that $rank_{\mathbb{R}}(M_{\widetilde{IP}_n}) \geq rank_{\mathbb{R}}(M_{\widetilde{IP}_n}) - 1$.

Claim 2. *For an arbitrary matrices $A_{n\times m}$ and $B_{n\times m}$ inequalities*
$rank_{\mathbb{F}}(A + B) \geq \max[rank_{\mathbb{F}}(A), rank_{\mathbb{F}}(B)]$ and
$rank_{\mathbb{F}}(A + B) \leq rank_{\mathbb{F}}(A) + rank_{\mathbb{F}}(B)$ hold true for any field $\mathbb{F}$.

Thus, by theorem 1 $DCC(IP_n) \geq n + 1$, which is the maximal possible value. So, $DCC(IP_n) = n + 1$.

2.3. **Communication Complexity of the entire construction.** Rank lower bound technique gives the exact value of deterministic communication complexity for all Maiorana–McFarland's bent functions.

Theorem 3. *All bent functions $f \in MM_n$ have $DCC(f) = DCC(IP_n) = n + 1$.*

Let us recall Maiorana–McFarland construction $f(u, v) = \sigma(u) \cdot v + g(v)$. At the base of Maiorana–McFarland construction inner product function lies. The construction also contains two operations:

- $\sigma : V_n \to V_n$ – permutation[1] of Boolean vector inside inner product;
- addition of Boolean function $g : V_n \to \mathbb{F}_2$ applied to a Boolean vector.

These operations can be considered as operations on matrices:

- As all $u \in V_n$ correspond to rows and all $v \in V_n$ correspond to columns of the matrix form of a Boolean function $f : V_n \oplus V_n \to \mathbb{F}_2$, the permutation $\sigma(u)$ is equivalent to permutation of rows in the matrix M_{IP_n};
- Addition of $g(v)$ is equivalent to addition of a rank 1 matrix, where each row is a vector of values of a function $g(v)$.

A permutation of rows is an elementary operation on matrices and thus, leaves the rank of matrix unchanged. By claim 2 the addition of a rank 1 matrix can not reduce the rank of initial matrix, so it can be concluded that communication complexity of all Maiorana–McFarland bent functions are equal to communication complexity of inner product function.

□

3. Reasoning about bent functions

3.1. **Not all bent functions have high communication complexity.** Although all functions $f : V_n \oplus V_n \to \mathbb{F}_2$ from Maiorana–McFarland class have the highest possible DCC value, bent functions that have small DCC value also exist.

To prove this fact we need to consider one simple example of bent function that is a result of some special transformation applied to the inner product function. The resulting transformed function is still bent, but it's DCC value is small.

3.2. **Transformations leaving bent property invariant.** It is known [1] that there are transformations leaving bent property of bent functions invariant.

Theorem 4. *A bent function is invariant* [1]*:*

- *under affine transformation of variables such that $f : V_k \to \mathbb{F}_2$ is bent if an only if $f \circ \theta$ is also bent, where $\theta(x) = Ax + b$, $A \in GL(2, k)$, $b \in V_k$. Here $GL(2, k)$ is the general linear group of $k \times k$ matrices over $\mathbb{F}_2$;*
- *by adding an affine function, that $f : V_k \to \mathbb{F}_2$ is bent if and only if $\gamma(x) = c \cdot x + d$, where $c \in V_k$, $d \in \mathbb{F}_2$.*

  So that if $f : V_n \to \mathbb{F}_2$ is a bent function, then the function $g = f \circ \theta + \gamma$ is also bent.

[1] It is known [1] that the construction produces bent functions if and only if σ is a permutation

3.3. **Construction of bent function with small communication complexity lower bound.** Consider the following transformation of Boolean function.

Let Alt denote a permutation $Alt : V_{2n} \to V_{2n}$ of the form

$$\begin{pmatrix} u_1 & u_2 & u_3 & ... & v_{n-2} & v_{n-1} & v_n \\ u_1 & v_1 & u_2 & ... & v_{n-1} & u_n & v_n \end{pmatrix},$$

where after permutation of vector $(u_1, u_2, ..., u_n, v_1, v_2, ..., v_n)$ each u_i is followed by v_i.

This permutation is obviously a special case of affine transformation of variables.

After applying this permutation to the inner product function $IP(u_1, u_2, ..., u_n, v_1, v_2, ..., v_n)$ of two vectors of even length n, the function transforms into a modulo 2 sum of two inner products $IP_{left}(u_1, v_1, ..., u_{n/2}, v_{n/2})$ and $IP_{right}(u_{n/2+1}, v_{n/2+1}, ..., u_n, v_n)$.

Note that from communication complexity point of view Alice knows the values of IP_{left} variables and Bob knows the values of IP_{right} variables.

Therefore, to compute the value of the whole function Alice can compute inner product of her variables, send result to Bob and Bob, in his turn, can compute inner product of his variables, modulo 2 add his result to Alice's and send her the value of the entire function. So, communication complexity in this case is bounded above by 2.

Communication complexity lower bound of transformed inner product IP_{Alt} is equal to $\log(2rank(M_{IP_{Alt}})-1)$, where $M_{IP_{Alt}} = M_{IP_{rows}} + M_{IP_{cols}}$ is modulo 2 sum of two matrices of rank 1. In these rank 1 matrices the values of inner product are written in rows and columns respectively. So, it is easy to see that this matrix has rank 2 and IP_{Alt} has $DCC \geq 2$. Taking into account this lower bound and the above protocol we can conclude that IP_{Alt}'s DCC value is exactly 2.

4. Conclusion

Using matrix lower bound technique for estimating lower bounds of communication complexity we show that all bent functions from Maiorana–McFarland class have the highest possible value of deterministic two-party communication complexity. However, not all bent functions have high communication complexity. By applying affine transformation of variables to the inner product function of two vectors of even length we can transform it into a function with constant value of communication complexity.

References

[1] O. S. Rothaus, *On bent functions*, Journal of Combinatorial Theory, Series A **20** (3), 300–305 (1976).

[2] N. N. Tokareva, *Bent functions: results and applications. A survey*, Prikl. Diskr. Mat. **1** (1), 15-37 (2009).

[3] A. C. Yao. *Some complexity questions related to distributive computing (preliminary report).* Proceedings of the 11th Annual ACM Symposium on Theory of Computing (STOC '79), 209–213 (1979).

[4] R. L. McFarland. *A family of difference sets in non-cyclic groups.* Journal of Combinatorial Theory, Series A **15** (1), 1–10 (1973).

[5] K. Mehlhorn, E. M. Schmidt. *Las vegas is better than determinism in VLSI and distributed computing.* Proceedings of the 14th Annual ACM Symposium on the Theory of Computing, ACM, 330–337 (1982).