правила в общем случае достаточно громоздко. Для частично определенных данных можно дать более простое прямое доказательство, используя приведенные выше явные представления.

Количество информации $\mathcal{I}(X,Y)$ в X о Y находится из соотношения $\mathcal{I}(X,Y) = \mathcal{H}(Y) - \mathcal{H}(Y|X)$ и для частично определенных данных выразимо в явном виде. Рассмотрим пример. Пусть выход полностью определенного источника X, порождающего символы 0 и 1 с вероятностями p_0 и p_1, подается на вход канала, где символы стираются (заменяются на $*$) с вероятностью ε. Требуется вычислить информацию $\mathcal{I}(Y,X)$ в выходе Y канала о его входе X и информацию $\mathcal{I}(X,Y)$ во входе X о выходе Y. Используя приведенные выше формулы, получаем

$$\mathcal{I}(Y,X) = H(p_0,p_1) - p_0H(\varepsilon p_1, 1-\varepsilon p_1) - p_1H(\varepsilon p_0, 1-\varepsilon p_0),$$
$$\mathcal{I}(X,Y) = (1-\varepsilon)H(p_0,p_1),$$

где $H(x_0,x_1) = -x_0\log x_0 - x_1\log x_1$.

ЛИТЕРАТУРА

1. *Шоломов Л. А.* Сжатие частично определенной информации // Нелинейная динамика и управление. М.: Физматлит, 2004. Вып. 4. С. 385–399.
2. *Шоломов Л. А.* Правило сложения энтропий для недоопределенных данных // Материалы XVII Межгосударственной школы-семинара «Синтез и сложность управляющих систем». Новосибирск: ИМ СО РАН, 2008. С. 193–196.

УДК 519.7

ON QUATERNARY AND BINARY BENT FUNCTIONS[1]

P. Solé, N. N. Tokareva

In this paper direct links between Boolean bent functions (Rothaus, [1], 1976), generalized Boolean bent functions (Schmidt, [2], 2006) and quaternary bent functions (Kumar, Scholtz, Welch, [3], 1985) are explored. We also study Gray images of bent functions and notions of generalized nonlinearity for Boolean functions.

Let n, q be integers, $q \geqslant 2$. We consider the following mappings:

1) $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ — **Boolean function** in n variables. Its *sign function* is $F := (-1)^f$. The *Walsh Hadamard transform* (WHT) of f is $\widehat{F}(x) := \sum_{y\in\mathbb{Z}_2^n}(-1)^{f(y)+x.y} = \sum_{y\in\mathbb{Z}_2^n} F_y(-1)^{x.y}$. Here $x.y$ is a usual inner product of vectors. A Boolean function f is said to be *bent*, iff $|\widehat{F}(x)| = 2^{n/2}$ for all $x \in \mathbb{Z}_2^n$. It is *near bent* iff $\widehat{F}(x) \in \{0, \pm 2^{(n+1)/2}\}$. Note that Boolean bent (resp. near bent) functions exist only if the number of variables, n, is even (resp. odd).

2) $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ — **generalized Boolean function** in n variables. Its *sign function* is $F := \omega^f$, with ω a primitive complex root of unity of order q, i. e. $\omega = e^{2\pi i/q}$. When $q = 4$, we write $\omega = i$. Its WHT is given as $\widehat{F}(x) := \sum_{y\in\mathbb{Z}_2^n}\omega^{f(y)}(-1)^{x.y} = \sum_{y\in\mathbb{Z}_2^n} F_y(-1)^{x.y}$. As above, a generalized Boolean function f is *bent*, iff $|\widehat{F}(x)| = 2^{n/2}$ for all $x \in \mathbb{Z}_2^n$. In comparison to the previous case it not follows that n should be even if f is bent. Such functions for $q = 4$ were studied in [2]. Here we consider $q = 4$ only.

[1] The first author was partially supported by ANR grant NUGET. The second author was supported by the Russian Science Support Foundation and by the Russian Foundation for Basic Research (grants 07-01-00248, 08-01-00671, 09-01-00528).

3) $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ — q-**ary function** in n variables. Its *sign function* is given by $F := \omega^f$ as in the previous case. Its WHT is defined by $\widehat{F}(x) := \sum_{y\in\mathbb{Z}_q^n} \omega^{f(y)+x.y} = \sum_{y\in\mathbb{Z}_q^n} F_y\omega^{x\cdot y}$. Note that the matrix of this transform is no longer a Sylvester type Hadamard matrix as in the previous case, but a generalized (complex) Hadamard matrix. A q-ary function f is called *bent*, iff $|\widehat{F}(x)| = q^{n/2}$ for all $x \in \mathbb{Z}_q^n$. Notice that again it not follows from the definition that q-ary bent functions do not exist if n is odd. Kumar, Scholtz and Welch [3] have studied q-ary bent functions in 1985. They proved that such functions exist for any even n and $q \neq 2(\mathrm{mod}\, 4)$. Later Ambrosimov described all quadratic q-ary bent functions over an arbitrary finite field and Agievich proposed an approach to describe regular q-ary bent functions in terms of bent rectangles. If $q = 4$ we call f a **quaternary function**. Here we study such functions only.

Let $f : \mathbb{Z}_2^{2n} \to \mathbb{Z}_4$ be any generalized Boolean function. Represent it as $f(x, y) = = a(x, y) + 2b(x, y)$, for any $x, y \in \mathbb{Z}_2^n$, where $a, b : \mathbb{Z}_2^{2n} \to \mathbb{Z}_2$ are Boolean functions.

Theorem 1. The following statements are equivalent:
(i) the generalized Boolean function f is bent in $2n$ variables;
(ii) the Boolean functions of $2n$ variables b and $a + b$ are both bent.

Define a quaternary function $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ as $g(x + 2y) = f(x, y)$.

We say that two Boolean functions c and d in $2n$ variables are *bent correlated* (with respect to dividing variables into two halves) if for any $x, y \in \mathbb{Z}_2^n$, the conditions hold

1) $\widehat{C}^2(x, y) + \widehat{C}^2(x + y, y) + \widehat{D}^2(x, y) + \widehat{D}^2(x + y, y) = 4^{n+1}$;

2) $\widehat{C}(x, y) = \widehat{D}(x + y, y) = \pm 2^n \Longleftrightarrow \widehat{C}(x + y, y) = \widehat{D}(x, y) = \pm 2^n$.

It is easy to construct examples of such functions.

Theorem 2. The following statements are equivalent:
(i) the quaternary function g is bent in n variables;
(ii) the Boolean functions b and $a + b$ are bent correlated.

Now let f be a generalized Boolean function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_4$. The *Gray map* $\varphi(f)$ of f is the Boolean function in variables (z, w) with $z \in \mathbb{Z}_2^n$ and $w \in \mathbb{Z}_2$ defined as $a(z)w + b(z)$. Using results from [2] we prove

Proposition 3. If f is bent then $\varphi(f)$ is either bent (n odd) or near bent (n even).

Proposition 4. Let n be odd. If $\varphi(f)$ is a Boolean bent function in $n + 1$ variables then f is a generalized Boolean bent function in n variables.

It is well-known that bent binary Boolean functions are characterized by their distance to the first order Reed Muller code. This fact can be generalized to their quaternary analogues. Here we present it for a generalized Boolean bent functions.

Define, for $0 \leqslant r \leqslant m$ the quaternary code $ZRM(r, m) = \varphi^{-1}(RM(r, m+1))$. This code is spanned by vectors of values for functions of degree at most $r - 1$ together with twice functions of degree at most r, see [4]. Let f be a generalized Boolean function in n variables. We introduce the **nonlinearity** $N(f)$ of f as $N(f) := 2^{n-1} - 1/2 \cdot \max_{u\in\mathbb{Z}_2^n, v\in\mathbb{Z}_2} \Re(i^{-v}\widehat{F}(u))$.

Proposition 5. $N(f) = d_L(f, ZRM(1, n)) = d_H(\Phi(f), RM(1, n+1)) \leqslant 2^n - 2^{(n-1)/2}$.

Here d_L and d_H are respectively Lee and Hamming metrics.

Now propositions 3 and 4 can be reformulated like this.

Proposition 6. Let n be odd. A function f is bent $\Longleftrightarrow N(f) = 2^n - 2^{(n-1)/2}$.

Proposition 7. Let n be even. If a function f is bent then $N(f) = 2^n - 2^{n/2}$.

Actually, it is not clear what is the maximum possible value of $N(f)$ if n is even. To know it one should find the value of covering radius of the code $RM(1, n+1)$ when $n+1$ is odd. But it is a hard old problem without analogy to the easy case of even $n+1$.

Authors wish to thank Sihem Mesnager for helpful discussions.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory, Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Schmidt K-U.* Quaternary Constant-Amplitude Codes for Multicode CDMA // Available at `http://arxiv.org/abs/cs.IT/0611162`.
3. *Kumar P. V., Scholtz R. A., Welch L. R.* Generalized bent functions and their properties // J. Combin. Theory, Ser. A. V. 40. 1985. P. 90—107.
4. *Hammons R., Kumar V., Calderbank A. R., et al.* Kerdock, Preparata, Goethals and others are linear over $\mathbb{Z}_4$ // IEEE Trans. of Inform. Theory. 1994. V. 40. P. 301–319.