On Minimal Distance between q-ary Bent Functions

Vladimir N. Potapov

Sobolev Institute of Mathematics

Problems of Redundancy in Information and Control Systems

Saint–Petersburg, Russia in 26–29 September 2016

Definitions

Let G be a finite abelian group. Consider a vector space $V(G)$ consisting of functions $f : G \to \mathbb{C}$ with inner product

$$(f, g) = \sum_{x \in G} f(x)\overline{g(x)}.$$

A function $f : G \to \mathbb{C}\backslash\{0\}$ is called a character of G if it is a homomorphism from G to $\mathbb{C}$, i.e. $\phi(x + y) = \phi(x)\phi(y)$ for each $x, y \in G$.
The set of characters of an abelian group is an orthogonal basis of $V(G)$. If $G = Z_q^n$ then $\phi_z(x) = \xi^{\langle x,z \rangle}$, where $\xi = e^{2\pi i/q}$ and $\langle x, y \rangle = x_1y_1 + \cdots + x_ny_n \bmod q$ for each $z \in Z_q^n$.

Define the Fourier transform of a $f \in V(G)$ by the formula $\widehat{f}(z) = (f, \phi_z)/|G|^{1/2}$,
$\widehat{f}(z)$ is the coefficients of the expansion of f in the basis.

Definitions

A function $f : Z_q^n \to Z_q$ is called a q-ary bent function iff $\widehat{\xi^f} \cdot \overline{\widehat{\xi^f}} = I$, where I is equal to 1 everywhere.

Define the convolution of $f \in V(G)$ and $g \in V(G)$ by equation $f * g(z) = \sum_{x \in G} f(x)g(z-x)$. It is well known that $\widehat{f * g} = |G|^{1/2}\widehat{f} \cdot \widehat{g}$.

The definition of bent function is equivalent to the equation $\xi^f * \overline{\xi^f} = |G|\chi^{\{0\}}$. Then the matrix $B = (b_{z,y})$, where $b_{z,y} = \xi^{f(z+y)}$, is a generalized Hadamard matrix.

There χ^S is the characteristic function of the set S.

Definitions

A bent function b is called regular iff there exists a function $b' : Z_q^n \to Z_q$ such that $\xi^{b'} = \widehat{\xi^b}$. Then b' is a bent function as well. If q is a prime power and n is even, then each bent function is regular.

If q is a prime power and n is even, then each bent function is regular.
We assume below that p is a prime number and n is even.

Results

The Hamming distance between two functions f and g is the cardinality of the support $\{x \in G \mid f(x) \neq g(x)\}$ of their difference.

Proposition 1

The Hamming distance between two bent function on Z_p^n is not less than $p^{n/2}$. If it is equal to $p^{n/2}$, then the difference between these functions is equal to $c\chi^{\Gamma}$, where $c \in Z_p$ and Γ is an $n/2$-dimensional affine subspace.

Results

Proposition 2

If a bent function $b : Z_p^n \to Z_p$ is an affine function on an affine subspace Γ, then $\dim\Gamma \leq n/2$.

Proposition 3

If a bent function $b : Z_p^n \to Z_p$ is an affine function on an $n/2$-dimensional affine subspace, then there exist $p-1$ bent function which differ from b only on this subspace.

Results

Consider quadratic form

$$Q_0(v_1, \ldots, v_d, u_1, \ldots u_d) = v_1 u_1 + \cdots + v_d u_d.$$

It is well known that Q_0 is a bent function from Maiorana–McFarland class.

Proposition 4

If p is a prime number and $p > 2$, then there are $p^d(p^{d-1}+1)\cdots(p+1)(p-1)$ p-ary bent functions at the distance p^d from Q_0.

In the binary case the analogous statement was proved in [1] and [2].

1. C. Carlet, "Two new classes of bent functions", *Advances in Cryptology - EUROCRYPT'93*, Lecture Notes in Comput. Sci., no. 765, Berlin: Springer-Verlag, 1994.
2. N.A. Kolomeets, "Enumeration of the bent functions of least deviation from a quadratic bent function", *J. Appl. Ind. Math.*,2012.

In [3] was established that this bound for the number of bent functions at the minimal distance is reached only for quadratic bent functions. It is natural to assume that this property of p-ary quadratic bent functions is true for any prime $p > 2$.

3.N.A. Kolomeec, "An upper bound for the number of bent functions at the distance 2^k from an arbitrary bent function in $2k$ variables", *Prikl. Diskr. Mat.*, 2014.