On Minimal Distance between q-ary Plateaued Functions

Vladimir N. Potapov

Sobolev Institute of Mathematics, Novosibirsk, Russia

XVI International Symposium "Problems of Redundancy in Information and Control Systems", Moscow, October 21 – 26, 2019

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 $f : G \to \mathbb{C}\setminus\{0\}$ is called a character of G if it is a group 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 $V(G)$.

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 of characters.

Definitions

Suppose that q is prime number and $G = F_q^n$ is the n-dimensional vector space over Galois field F_q. Then $\phi_z(x) = \xi^{\langle x,z\rangle}$, where $\xi = e^{2\pi i/q}$ and $\langle x, y\rangle = x_1 y_1 + \cdots + x_n y_n \mod q$ for each $z \in Z_q^n$.

Define the Walsh–Hadamard transform of a function $f : F_q^n \to F_q$ by the formula $W_f = \widehat{\xi^f}$, i.e.

$$W_f(z) = \frac{1}{q^{n/2}} \sum_{x \in F_q^n} \xi^{f(x)+\langle x,z\rangle}.$$

Definitions

A function $f : F_q^n \to F_q$ is called a q-ary bent function if and only if $|W_f(z)| = 1$ for each $z \in F_q^n$ and it is called a q-ary plateaued function if and only if $|W_f(z)| \in \{0, \mu\}$ for each $y \in F_q^n$.

From Parseval identity $(g, g) = \|g\|^2 = \|\widehat{g}\|^2$
we obtain that
$q^n = \sum_x |\xi^{f(x)}|^2 = \sum_y |W_f(y)|^2 = \mu^2 |\mathrm{supp}(W_f)|$.
Since q is prime we have that $|W_f(y)|^2$ takes q^{n-s} times the value $\mu^2 = q^s$. Such q-ary plateaued function f is called s-plateaued.
Since q is a prime number we have $W_f(y) = \pm q^{s/2} \xi^a$ or $W_f(y) = 0$, where $a \in F_q$. Any 0-plateaued function is a bent function.

Main results

The Hamming distance between two functions f and g is the cardinality of the support $\{x \in Dom(f) : f(x) - g(x) \neq 0\}$ of their difference.

Theorem 1

The Hamming distance between two binary s-plateaued functions is not less than $2^{\frac{s+n-2}{2}}$;
the Hamming distance between two ternary s-plateaued functions is not less than $3^{\frac{s+n-1}{2}}$.

These bounds are tight.

Main results

Proposition

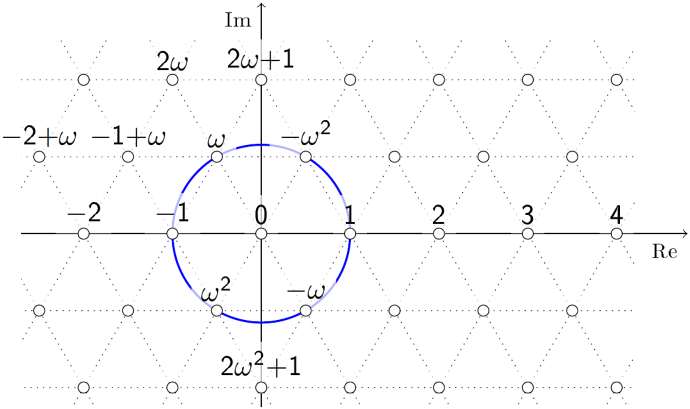
1) For $n = d + s$, $d > 4$, $s > \log d$, there exist pairs of 2-ary s-plateaued functions at distance $2^{\frac{s+n-2}{2}}$.
2) For $n = d + s$, $d > 0$, $s > \log d$, there exist pairs of 3-ary s-plateaued functions at distance $3^{\frac{s+n-1}{2}}$.

Functions $R(x_1, x_2, x_3, x_4) = (x_1 + x_2)(x_3 + x_4) + x_1 + x_3$ and $R'(x_1, x_2, x_3, x_4) = (x_1 + x_4)(x_3 + x_2) + x_1 + x_3$ are 2-plateaued functions over F_2 at distance $4 = 2^{\frac{s+n-2}{2}}$. Functions $T(x) = x^2$ and $T'(x) = x + 2x^2$ are 0-plateaued functions over F_3 at distance $1 = 3^{\frac{s+n-1}{2}}$.

Eisenstein integers

Case $q = 3$. If $f : F_3^n \to F_3$ then $\sum_{x \in F_3^n} \xi^{f(x)+\langle x,z\rangle} = 3^{n/2} W_f(z)$ are Eisenstein integers.

$$a + b\omega, \quad a, b \in \mathbb{Z}, \quad \omega := \frac{-1 + i\sqrt{3}}{2}$$



Proof Theorem 1

uncertainty principle

Let G be a finite abelian group. For every $f \in V(G)$ the following inequality is true:

$$|\mathrm{supp}(f)| \cdot |\mathrm{supp}(\widehat{f})| \geq |G|.$$

Let $f, g : F_3^n \to F_3$ be s-plateaued functions. Then
$|\xi^{f(x)} - \xi^{g(x)}| = \sqrt{3}$ if $f(x) \neq g(x)$ and
$|W_f(y) - W_g(y)| = 3^{s/2}|\xi^a \pm \xi^b|$, $a, b \in F_3$, or
$|W_f(y) - W_g(y)| = 3^{s/2}|\xi^a - 0|$ if $W_f(y) \neq W_g(y)$. In both cases
$|W_f(y) - W_g(y)| \geq 3^{s/2}$.

$$3|\mathrm{supp}(f-g)| = \|\xi^f - \xi^g\|^2 = \|W_f - W_g\|^2 \geq 3^s|\mathrm{supp}(W_f - W_g)|$$

$$3^{1-s}|\mathrm{supp}(f-g)|^2 \geq |\mathrm{supp}(f-g)||\mathrm{supp}(W_f - W_g)| \geq 3^n$$

Main results

Theorem 2

1) If an s-plateaued function $f : F_q^n \to F_q$ is an affine function on an affine subspace Γ, then $\dim\Gamma \leq \frac{s+n}{2}$.
2) If an s-plateaued function $f : F_q^n \to F_q$ is an affine function on an $\frac{s+n}{2}$-dimensional affine subspace, then there exist $q-1$ s-plateaued functions that differ from f only on this subspace.

Lemma

If Γ is a linear subspace in F_q^n and the subspace $\Gamma^\perp$ is the dual of Γ then it holds

$$\sum_{y\in\Gamma} \widehat{f}(y) = q^{\dim(\Gamma)-n/2} \sum_{x\in\Gamma^\perp} f(x).$$

Extremal property of plateaued functions

The nonlinearity of a function f on F_q^n is expressed via its Walsh–Hadamard coefficients by the formula
$nl(f) = q^{n-1} - q^{\frac{n}{2}-1} \max_{u \in F_q^n} |W_f(u)|.$

The correlation immunity of a balanced ($W_f(\bar{0}) = 0$) function f on F_q^n is expressed via its Walsh–Hadamard coefficients by the formula
$cor(f) = \min_{u \in F_q^n, W_f(u) \neq 0} wt(u) - 1,$
where $wt(u)$ is the Hamming weight of a vector u.

Theorem (Tarannikov 2000)

Let f be a balanced Boolean function on F_2^n, $cor(f) \leq n-2$. Then $nl(f) \leq 2^{n-1} - 2^{cor(f)+1}$. If $nl(f) = 2^{n-1} - 2^{cor(f)+1}$ then f is a plateaued function.