Constructions of bent functions and their number

Vladimir N. Potapov

Novosibirsk State University, Russia

Colloquia at Institute of Applied Mathematics, October 18, 2022

Boolean functions

$\mathbb{F}_2 = \{0, 1\}$. $\mathbb{F}_2^n$ is the n-dimensional Boolean hypercube.
$\langle \mathbb{F}_2^n, \oplus \rangle$ is an n-dimensional vector space over $\mathbb{F}_2$.
$f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Boolean function on n variables.

$\ell : \mathbb{F}_2^n \to \mathbb{F}_2$ is a linear function if
$\ell(x) = \langle u, x \rangle = u_1 x_1 \oplus u_2 x_1 \oplus \cdots \oplus u_n x_n$, $u \in \mathbb{F}_2^n$.

The Walsh–Hadamard transform of f is

$$W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle u, x \rangle \oplus f(x)}.$$

$\{W_f(u) | u \in \mathbb{F}_2^n\}$ is the Walsh spectrum of f.

$(-1)^f : \mathbb{F}_2^n \to \mathbb{R}$
$V = \{G : \mathbb{F}_2^n \to \mathbb{R}\}$ is a 2^n-dimensional vector space over $\mathbb{R}$.
$\{(-1)^{\langle u, x \rangle} : u \in \mathbb{F}_2^n\}$ is an orthogonal basis in V.

Boolean bent functions

The Parseval identity $\sum_{u \in \mathbb{F}_2^n} |W_f(u)|^2 = 2^{2n}$.

Definition

A Boolean function f on n variables is said to be a bent function if the Walsh spectrum of f consists of $\pm 2^{n/2}$.

Bent functions exist if and only if n is even.

S. Mesnager, *Bent Functions: Fundamentals and Results*. Springer, 2016.

Nonlinearity

The Hamming distance $d_H(f, g)$ between two functions f and g is the number of arguments on which they differ.

Denote by A_n the set of affine functions $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. The distance between a function f and a set of functions A is the minimum distance between f and any function $g \in A$.

The nonlinearity $nl(f)$ is the distance between f and A_n.

The nonlinearity of a Boolean function f is connected to its Walsh spectrum

$$nl(f) = 2^{n-1} - 2^{-1} \max_{u \in \mathbb{F}_2^n} |W_f(u)|. \quad (1)$$

Nonlinearity

$$nl(f) = 2^{n-1} - 2^{-1} \max_{u \in \mathbb{F}_2^n} |W_f(u)|. \quad (1)$$

Proof. Let $g(x) = \langle u, x \rangle$.
$W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle u,x \rangle \oplus f(x)} =$
$= |\{x \in \mathbb{F}_2^n : f(x) = g(x)\}| - |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}| =$
$= 2^n - 2|\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}| = 2^n - 2d_H(f, g)$.
Then $d_H(f, g) = 2^{n-1} - 2^{-1} W_f(u)$.

Let $g(x) = \langle u, x \rangle \oplus 1$.
$W_f(u) = 2^n - 2|\{x \in \mathbb{F}_2^n : f(x) \neq g(x) \oplus 1\}| =$
$= 2^n - 2(2^n - |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}|) = -2^n + 2d_H(f, g)$.
Then $d_H(f, g) = 2^{n-1} - 2^{-1}(-W_f(u))$.

Nonlinearity and bent functions

$$nl(f) = 2^{n-1} - 2^{-1} \max_{u \in \mathbb{F}_2^n} |W_f(u)|. \quad (1)$$

Theorem

A Boolean function f on even variables has maximal nonlinearity iff it is a bent function.

Proof. By the Parseval identity, $\max_{u \in \mathbb{F}_2^n} |W_f(u)| \geq 2^{n/2}$ for every f.

Then
$nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.
($\Rightarrow$) If $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, then $|W_f(u)| \leq 2^{n/2}$ for every u. By the Parseval identity $|W_f(u)| = 2^{n/2}$ for every u.
($\Leftarrow$) If f is a bent function, then $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ by (1).

Ternary case

A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called a p-ary bent function if and only if $|W_f(y)|$ does not depend on $y \in \mathbb{F}_p^n$.

Theorem

1) For every $f : \mathbb{F}_3^n \to \mathbb{F}_3$ it holds $nl(f) \leq 2 \cdot 3^{n-1} - 3^{\frac{n}{2}-1}$;
2) $nl(f) = 2 \cdot 3^{n-1} - 3^{\frac{n}{2}-1}$ if and only if f is a ternary bent function, n is even and $W_f(y) = -3^{n/2} e^{2\pi ai/3}$, $a \in \mathbb{F}_3$, for each $y \in \mathbb{F}_3^n$.

Potapov, V.N. On q-ary bent and plateaued functions // Des. Codes Cryptogr. 2020

Maiorana–McFarland construction

Let ψ be a Boolean function on n variables and let π be a permutation of $\mathbb{F}_2^n$.

Maiorana–McFarland family of bent functions (1973):

$$f_{\psi,\pi}(x,y) = f(x_1,\ldots,x_n,y_1,\ldots,y_n) = \psi(x) \oplus \langle \pi(x), y \rangle.$$

Proposition

$f_{\psi,\pi}$ is a bent function.

Proof.

$$W_f(u,v) = \sum_{x\in\mathbb{F}_2^n} \sum_{y\in\mathbb{F}_2^n} (-1)^{\langle u,x\rangle \oplus \langle v,y\rangle \oplus f(x,y)} =$$

$$= \sum_{x\in\mathbb{F}_2^n} (-1)^{\langle u,x\rangle \oplus \psi(x)} \left(\sum_{y\in\mathbb{F}_2^n} (-1)^{\langle v\oplus\pi(x),y\rangle} \right) =$$

$$2^n \sum_{x:\pi(x)=v} (-1)^{\langle u,x\rangle \oplus \psi(x)}.$$

Example

Let $q : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ be a quadratic function

$$q(x, y) = \langle x, y \rangle = x_1 y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n.$$

π is identity permutation, $\psi = 0$.

$q(x_1, x_2, y_1, y_2) = x_1 y_1 \oplus x_2 y_2$, $nl(q) = 6$.

Constructions

Definition

A collection $\mathcal{S} = \{S_1, \ldots, S_M\}$ of k-dimensional linear spaces $S_i \subseteq \mathbb{F}_2^n$, is called a partial k-spread if each $x \in \mathbb{F}_2^n \setminus \{\overline{0}\}$ belongs to no more than one S_i.

A partial spread is a spread if the union of all its elements equals $\mathbb{F}_2^n$.

Dillon's $\mathcal{PS}^-$ family of bent functions (1975):
Let $\mathcal{S}$ be a partial n-spread in $\mathbb{F}_2^{2n}$ of size $M = 2^{n-1}$.
Let $f_\mathcal{S}$ be a characteristic function of $\bigcup_{i=1}^{M} S_i \setminus \{\overline{0}\}$.

Proposition

$f_\mathcal{S}$ is a bent function.

$S^\perp = \{u : \langle u, x \rangle = 0, \forall x \in S\}$. Note that if $S_i \cap S_j = \overline{0}$ then $S_i^\perp \cap S_j^\perp = \overline{0}$ for all n-dimensional subspaces S_i and S_j of $\mathbb{F}_2^{2n}$.

Constructions

Proof.
$(-1)^{f_S} = \mathbf{1} + 2M\mathbf{1}_{\overline{0}} - 2\sum_i \mathbf{1}_{S_i}$.

$$W_{f_S}(u) = \sum_{x\in\mathbb{F}_2^{2n}} (-1)^{\langle u,x\rangle}(\mathbf{1} + 2M\mathbf{1}_{\overline{0}} - 2\sum_i \mathbf{1}_{S_i})(x).$$

$$\sum_{x\in\mathbb{F}_2^{2n}} \mathbf{1}_S(x)(-1)^{\langle u,x\rangle} = \sum_{x\in S}(-1)^{\langle u,x\rangle} = \begin{cases} 2^n, \text{ if} & u \in S^\perp; \\ 0, \text{ if} & u \notin S^\perp. \end{cases}$$

$$\sum_{x\in\mathbb{F}_2^{2n}} (-1)^{\langle u,x\rangle}(\mathbf{1} + 2M\mathbf{1}_{\overline{0}}) = 2^{2n}\mathbf{1}_{\overline{0}} + 2M\mathbf{1}.$$

$$W_{f_S}(u) = \begin{cases} 2^{2n} + 2M - 2M2^n = 2^n, \text{ if} & u = \overline{0}; \\ 2M - 2^{n+1} = -2^n, \text{ if} & u \in \bigcup_i S_i^\perp; \\ 2M = 2^n, \text{ if} & u \notin \bigcup_i S_i^\perp. \end{cases}$$

Constructions

Definition

Boolean function f is called a plateaued function iff $|W_f(u)| \in \{0, \mu\}$ for each $u \in \mathbb{F}_2^n$.

The support of the Walsh spectrum is the set $\{u : W_f(u) \neq 0\}$.
Let $\{C_a\}_{a\in\mathbb{F}_2^{n_1}}$, $C_a \subseteq \mathbb{F}_2^{n_2}$ be an ordered partition of $\mathbb{F}_2^{n_2}$ into affine subspaces of dimensions $n_2 - n_1$ (OPAS).
Let $\mathcal{F} = \{f_a\}_{a\in\mathbb{F}_2^{n_1}}$ be a family of plateaued functions such that the support of the Walsh spectrum of f_a is exactly C_a.

Constructions

Agievich (2008), Çeşmelioğlu and Meidl (2013), Baksova and Tarannikov (2020)

Construction (K)

Define a Boolean function f on n variables as a Boolean sum

$$f_{\mathcal{F}}(x, y) = \bigoplus_{a \in \mathbb{F}_2^{n_1}} f_a(y) x^a,$$

where $x \in \mathbb{F}_2^{n_1}, y \in \mathbb{F}_2^{n_2}$, $a \in \mathbb{F}_2$, $x^a = x_1^{a_1} \cdots x_{n_1}^{a_{n_1}}$, $x_i^1 = x_i$ and $x_i^0 = x_i \oplus 1$

here $n = n_1 + n_2$, $n_2 \geq n_1$, n and $n_2 - n_1$ are even, $\{C_a\}_{a \in \mathbb{F}_2^{n_1}}$ is OPAS, $f_a \in \mathcal{F}$.

Proposition

$f_{\mathcal{F}}$ is a bent function.

How many bent functions exist?

Class of bent f.	Asymptotics of $\log_2$ of cardinality
MM family	$\log_2 \lvert\mathcal{M}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1 + o(1))$
completed MM family	$\log_2 \lvert\mathcal{M}^{\#}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1 + o(1))$
$\mathcal{C}$ class	$\log_2 \lvert\mathcal{C}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1 + o(1))$
$\mathcal{D}$ class	$\log_2 \lvert\mathcal{D}(n)\rvert = \frac{n}{2} \cdot 2^{n/2}(1 + o(1))$
Agievich class	$\log_2 A(n) = \frac{n}{2} \cdot 2^{n/2}(1 + o(1))$
special subclass of $\mathcal{PS}$	$\log_2 \lvert\mathcal{PS}_{ap}(n)\rvert = 2^{n/2}(1 + o(1))$
$\mathcal{P}$artial $\mathcal{S}$pread family	$\log_2 \lvert\mathcal{PS}(n)\rvert \leq \frac{n^2}{8} \cdot 2^{n/2}(1 + o(1))$
Construction (K)	$\log_2 \lvert K(n,1)\rvert = \frac{3n}{4} \cdot 2^{n/2}(1 + o(1))$

Theorem (P., Taranenko, Tarannikov, 2022)

The logarithm of the number of bent function on n variables is not less than $\frac{3n}{4} \cdot 2^{n/2}(1 + o(1))$.

The number of bent functions constructed by (K)

Let b_m be the number of bent functions on m variables. Let $n_1 = n/2 - k$, $n_2 = n/2 + k$, where $k \in \mathbb{N}$, $k \geq 1$.

$$K(n,k) = (b_{2k})^{2^{n_1}} \cdot \widetilde{N}_{n_2}^{2k},$$

where $\widetilde{N}_{n_2}^{2k}$ is the number of OPAS.

Proposition

$$\log_2 \widetilde{N}_{n_2}^{2k} \leq \frac{(2k+1)n}{2^{k+1}} \cdot 2^{n/2} + o(n2^{n/2}).$$

Corollary

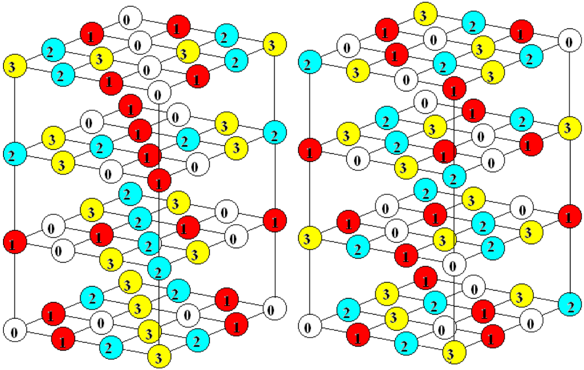
$$\log_2 K(n,k) \leq \frac{(2k+1)n}{2^{k+1}} \cdot 2^{n/2} + o(n2^{n/2}).$$

This number is maximal when $k = 1$.

The number of bent functions constructed by (K)

Definition

A transversal in a latin hypercube Q of order n is a collection of n entries hitting each hyperplane and each symbol exactly once.



The number of bent functions constructed by (K)

Let Q_m be the 3-dimensional latin hypercube of order 2^m such that

$$q_{\alpha_1,\alpha_2,\alpha_3} = \alpha_4 \Leftrightarrow \alpha_1 \oplus \cdots \oplus \alpha_4 = \overline{0}.$$

Q_m is the Cayley table of a 3-ary iterated group Z_2^m. Let T_m be the number of transversals in Q_m.

Theorem (Eberhard, 2017+)

$$T_m = (1 + o(1))\frac{2^m!^3}{2^{m(2^m-1)}}.$$

The number of bent functions constructed by (K)

Proposition (P., Taranenko, Tarannikov, 2022)

The number N_m of unordered partitions of $\mathbb{F}_2^m$ into 2-dimensional affine subspaces is not less than T_{m-2}:

$$\log_2 N_m \geq \log_2 T_{m-2} \geq \frac{m}{2} \cdot 2^m + c_1 \cdot 2^m + o(2^m).$$

Let $\widetilde{N}_m^i$ be the number of ordered partitions of $\mathbb{F}_2^m$ into i-dimensional affine subspaces. Then

$$\widetilde{N}_m^i = 2^{m-i}! \cdot N_m^i.$$

$k = 1$, $i = 2$, $m = n$.

Corollary

$\log_2 |K(n,1)| = \frac{3n}{4} \cdot 2^{n/2}(1 + o(1)).$

Upper bounds on the number of bent functions

Proposition

Since the algebraic degree of bent functions is bounded by $n/2$, we have

$$\log_2 b_n \leq \frac{1}{2} \cdot 2^n + \frac{1}{2}\binom{n}{n/2}.$$

Carlet, Klapper (2002) and Agievich (2020) slightly improved the upper bounds, but asymptotically $\log_2 b_n$ remained the same.

Theorem (P., 2021)

$$\log_2 b_n \leq \frac{3}{8} \cdot 2^n + o(2^n).$$

Connections between bent functions and other structures

Proposition

Let f be a Boolean bent function. Then $\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)}(-1)^{f(x \oplus a)} = 0$ for each $a \in \mathbb{F}_2^n \setminus \{\overline{0}\}$.

Define matrix H of size $2^n \times 2^n$ by equation $H_{xy} = (-1)^{f(x \oplus y)}$.

Proposition

H is the Hadamard matrix.

Connections between bent functions and other structures

Definition

Let G be a finite abelian group of order v. A subset D of G of cardinality k is called (v, k, λ)-difference set in G if every element $g \in G$, different from the identity, can be written as $d_1 - d_2$, $d_1, d_2 \in D$, in exactly λ different ways.

For every $f : \mathbb{F}_2^n \to \mathbb{F}_2$ define $D_f = \{x \in \mathbb{F}_2^n : f(x) = 1\}$.

Theorem (Dillon)

f is a bent function iff D_f is a $(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1})$-difference set in $\mathbb{F}_2^n$.

Connections between bent functions and other structures

Definition

A coloring f of a graph $G = (V, E)$ is called perfect if the collections of vertices adjacent to the vertices of the same color have identical color composition.

For every color i and all $x, y \in V(G)$

$$f(x) = f(y) \Rightarrow |f^{-1}(i) \in S(x)| = |f^{-1}(i) \in S(y)|,$$

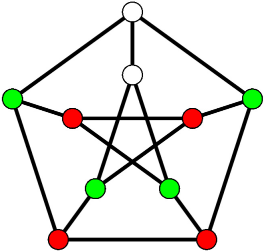
where $S(x)$ is the set of vertices adjacent to x.

The set $\{f^{-1}(i)\}_{i \in I}$ is called equitable partition of graph G.

The matrix $P = (p_{ij})$ whose entry p_{ij} equals the number of vertices of color j adjacent to some vertex of color i is called the parameter matrix of the perfect coloring.

Connections between bent functions and other structures

Perfect coloring of the Petersen graph.



$$P = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

Connections between bent functions and other structures

Grassmann graphs are a special class of graphs defined from systems of subspaces. The vertices of the Grassmann graph $J_q(n,k)$ are the k-dimensional subspaces of an n-dimensional vector space over a finite field of order q; two vertices are adjacent when their intersection is $(k-1)$-dimensional.

Theorem (Avgustinovich, P., 2020)

f is a bent function of weight $2^{n-1}+2^{n/2-1}$ iff it is a perfect coloring of the graph $J_2(n,2)$ with parameter matrix

$$\begin{pmatrix} 3(2^{n-3}-2^{(n/2)-2}-1) & 3\cdot 2^{n-2}-3 & 3(2^{n-3}+2^{(n/2)-2}) & 0 \\ 2^{n-2}-2^{(n/2)-1} & 5\cdot 2^{n-3}-2^{(n/2)-2}-5 & 2^{n-1}+2^{(n/2)-1} & 2^{n-3}+2^{(n/2)-2}-1 \\ 2^{n-3}-2^{(n/2)-2} & 2^{n-1}-2^{(n/2)-1}-1 & 5\cdot 2^{n-3}+2^{(n/2)-2}-3 & 2^{n-2}+2^{(n/2)-1}-2 \\ 0 & 3(2^{n-3}-2^{(n/2)-2}) & 3\cdot 2^{n-2} & 3(2^{n-3}+2^{(n/2)-2}-2) \end{pmatrix}$$