On Alltop functions, p-ary Alltop functions and almost Hadamard matrices

Ferruh Özbudak
Sabanci University - Faculty of Engineering and Natural Sciences
(Joint work with Fuad Hamidli and Vladimir N. Potapov)

Hadamard 2025, 26-30, May 2025
Universidad de Sevilla
May 29, 2025

Definition

$\mathbb{F}_q$ is a finite field, where $q = p^n$, p is odd prime. $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$.

A function F is called an Alltop function over $\mathbb{F}_q$ if, for any $a \in \mathbb{F}_q^*$, the derivative

$$D_a F(x) = F(x + a) - F(x)$$

is a planar function. Equivalently, for any $a, b \in \mathbb{F}_q^*$, the expression

$$D_b D_a F(x) = F(x + a + b) - F(x + a) - F(x + b) + F(x)$$

is a permutation function. This definition forces $p > 3$. The typical Alltop function is x^3.

Definition

A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ has a unique representation (called the univariate algebraic normal form) as a univariate polynomial over $\mathbb{F}_{p^n}$ of degree at most $p^n - 1$. Hence we can assume that

$$F(x) = \sum_{i=0}^{p^n-1} c_i x^i,$$

where $c_i \in \mathbb{F}_{p^n}$ are uniquely determined by F.
Any integer $d \in \{0, \ldots, p^n - 1\}$ can be uniquely written in base p as $d = \sum_{j=0}^{n-1} b_j p^j$ with $b_j \in \{0, \ldots, p-1\}$. Defining $w_p(d) = \sum_{j=0}^{n-1} b_j$, the *algebraic degree* of a nonzero function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is defined and denoted as

$$d^o(F) = \max\{w_p(i) : i \in \{0, \ldots, p^n - 1\}, c_i \neq 0\},$$

where $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$ is the univariate representation of F. The algebraic degree of the zero function is 0 by convention.

Definition

Assume that p is a prime, $s \geq 1$ and $q = p^s$.
For $n \geq 2$, we say that $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is q-affine if its algebraic normal form is in the form $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$, with

$$x^i \in \{1, x, x^q, x^{q^2}, \ldots, x^{q^{n-1}}\} \text{ for each } c_i \neq 0.$$

For $n \geq 2$, we say that $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is (at most) q-quadratic if its algebraic normal form is in the form $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$, with

$$x^i \in \{1, x, x^q, x^{q^2}, \ldots, x^{q^{n-1}}\} \cup \{x^2, x^{1+q}, \ldots, x^{1+q^{n-2}}, x^{2q}, x^{q+q^2}, \ldots\} \text{ for each } c_i \neq 0.$$

Similarly we define (at most) q-cubic.

Definition

Any function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ has a representation of the form

$$f(x) = \mathrm{Tr}(F(x)),$$

where F is a map $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the trace map. Here F is not unique but algebraic degree of F is invariant, that we call the algebraic degree of f.

Definition

Let F and G be functions on $\mathbb{F}_{p^n}$. The functions F and G are called extended affine equivalent (EA-equivalent) if there exist an affine map $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and affine invertible maps $L_1, L_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that

$$G + \phi = L_1 \circ F \circ L_2$$

.

Definition

Let F and G be functions on $\mathbb{F}_{p^n}$. The functions F and G are said to be extended quadratic equivalent (EQA) if there exist a (at most) quadratic map $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and affine invertible maps $L_1, L_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that

$$G + \phi = L_1 \circ F \circ L_2$$

.

Remark

It is straightforward to see that the Alltop property is preserved under extended quadratic equivalency. In addition, for any homogeneous cubic functions F and G on $\mathbb{F}_{p^n}$, extended affine equivalency (EA) is the same as extended quadratic equivalency (EQA).

Theorem (Hall et al. 2013)

Let $p \geq 5$ be an odd prime, and n is an integer such that 3 does not divide $p^n + 1$. Then $f(x) = x^{p^n+2}$ is an Alltop polynomial on $\mathbb{F}_{p^{2n}}$.

Theorem (Hall et al. 2013)

Let $p \geq 5$ be an odd prime, and n is an integer such that 3 does not divide $p^n + 1$. Then the Alltop functions x^3 and x^{p^n+2} $\mathbb{F}_{p^{2n}}$ are not EA.

Cubic Alltop q-Monomials and q-Binomials over $\mathbb{F}_{q^2}$

Over the field $\mathbb{F}_{q^2}$, the set of all cubic q-monomials is as follows:

- $A_1)$ x^3
- $A_2)$ x^{q+2}
- $A_3)$ $x^{2q+1} = (x^{q+2})^q$
- $A_4)$ $x^{3q} = (x^3)^q$

The pairs $A_1)$ and $A_4)$, as well as $A_2)$ and $A_3)$, are equivalent under extended affine (EA) equivalence, as they are q-th powers of each other.

Cubic Alltop q-Monomials and q-Binomials over $\mathbb{F}_{q^2}$

Let $u \in \mathbb{F}_{q^2}^*$. The set of all cubic q-binomials over $\mathbb{F}_{q^2}$ takes the following forms:

- $B_1)$ $x^3 + ux^{2q+1}$
- $B_2)$ $x^3 + ux^{q+2}$
- $B_3)$ $x^3 + ux^{3q}$
- $B_4)$ $x^{q+2} + ux^{2q+1}$
- $B_5)$ $x^{q+2} + ux^{3q}$
- $B_6)$ $x^{2q+1} + ux^{3q}$

Pairs $B_1)$ and $B_5)$ are EA-equivalent, as are $B_2)$ and $B_6)$. After eliminating equivalent functions, we identify $B_1), B_2), B_3)$, and $B_4)$ as the only classes needed to be studied wlog upto EA over $\mathbb{F}_{q^2}$.

Cubic Alltop q-Monomials and q-Binomials over $\mathbb{F}_{q^2}$

- B_3) is easy. As $x^3 + ux^{3q} = (x + ux^q) \circ x^3$ and $x + ux^q$ is a permutation iff u is not a $q-1$ power: A function in B_3) is Alltop iff u is not a $q-1$ power in $\mathbb{F}_{q^2}^*$. Moreover they all are EA to x^3 if Alltop.

- B_4) is similar. As $x^{q+2} + ux^{2q+1} = (x + ux^q) \circ x^{q+2}$ and $x + ux^q$ is a permutation iff u is not a $q-1$ power: A function in $B4$) is Alltop iff u is not a $q-1$ power in $\mathbb{F}_{q^2}^*$. Moreover they all are EA to x^{q+2} if Alltop.

The class of $B1$) is quite interesting. Different from $B2$) and $B4$) above, there are u_1 and u_2 in this class, one is EA to x^3, while the other one EA to x^{q+2}. Moreover we classify all of them in the following.

Theorem

Let $p \geq 5$ be an odd prime, and n is an integer. Put $q = p^n$ and let $u \in \mathbb{F}_{q^2}^*$. Let $F_u(x) = x^3 + ux^{2q+1}$. We have the followings:

- F_u is EA to x^3 if and only if $\frac{u}{3} \in \{\theta^2 : \theta^{q+1} = -1\} \subseteq \mathbb{F}_{q^2}^*$.
- F_u is EA to x^{q+2} if and only if $u \in \{\theta^{q-1} : \theta^{q+1} = -1\} \subseteq \mathbb{F}_{q^2}^*$.

Cubic Alltop q-Monomials and q-Binomials over $\mathbb{F}_{q^3}$

Theorem

Except for x^3 and its equivalent class under EA, there are no Alltop cubic q-monomials in $\mathbb{F}_{q^3}$.

Based on our computations, except for $x^3 + cx^{3q}$ (which is Alltop if and only if c is not a $(q-1)$-st power, since $f(x) = (x + cx^q) \circ x^3$, the other cubic q-binomials are not Alltop when $q = 5$ and $q = 7$.

Definition p-ary Alltop

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ where p is an odd prime and $n \geq 1$ is an integer. Then f is called a p-ary bent function if $D_a f(x) = f(x + a) - f(x)$ is balanced for any $a \in \mathbb{F}_{p^n}^*$. We define f as a p-ary Alltop function if the difference function $D_a f(x) = f(x + a) - f(x)$ is p-ary bent for any $a \in \mathbb{F}_{p^n}^*$. In other words, for any $a, b \in \mathbb{F}_{p^n}^*$, the second-order difference function $D_b D_a f(x)$ is balanced.

Theorem

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be arbitrary function and let $f_\alpha : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a p-ary function defined as

$$f_\alpha(x) = \mathrm{Tr}(\alpha F(x))$$

for any $\alpha \in \mathbb{F}_{p^n}^*$, where Tr is the usual trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.
Then F is Alltop if and only if f_α is p-ary Alltop for any $\alpha \in \mathbb{F}_{p^n}^*$.

A Characterization p-ary Alltop

Let f denote a p-ary function mapping from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. The Walsh transform of f is defined as

$$W_f(\alpha) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(x) - \mathrm{Tr}(\alpha x)}.$$

Definition (Mesnager 2014)

Let f denote a p-ary function mapping from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. For any nonnegative integer i, the $2i$-th moment of the Walsh transform of f is defined as

$$S_i(f) = \sum_{\alpha \in \mathbb{F}_{p^n}} |W_f(\alpha)|^{2i},$$

with the convention that $S_0(f) = p^n$ when $i = 0$.

A Characterization p-ary Alltop

Observation

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be any p-ary function. Then f is a p-ary Alltop function if and only if

$$\sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{D_b D_a f(x)} = 0,$$

for all $a, b \in \mathbb{F}_{p^n}^*$, where ϵ_p represents a p-th root of unity.

Theorem

If $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is a p-ary Alltop, then

$$S_2(f) = p^{2n}(2p^n - 1).$$

A Nonexistence Result 3-ary Alltop

q is a power of 3.

Theorem

Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_3$ be an arbitrary function whose (geometric) q-ary degree is 3. Then f is never 3-ary Alltop.

An Existence Result 3-ary Alltop: An Infinite Family of New 3-ary Alltops

q is a power of 3.
Recall that there is no Alltop in characteristic 3. Hence there is no 3-ary Alltop as a component of an Alltop function.

Also the previous slide shows nonexistence 3-ary Alltop functions in the class of q-cubic functions $f : \mathbb{F}_{q^2} \to \mathbb{F}_3$.

The next theorem gives a new infinite class and also its full characterization.

Theorem

Let $f : \mathbb{F}_{q^3} \to \mathbb{F}_3$ be the infinite class of p-ary functions of q-ary degree is 3 given by $f(x) = \mathrm{Tr}_{q^3/3}(Ax^{q^2+q+1})$, where $A = \mathbb{F}^*_{q^3}$. Then f is 3-ary Alltop if and only if $\mathrm{Tr}_{q^3/q}(A) \neq 0$.

Further existence results p-ary Alltop

q is a power of p, $p > 3$.

Recall that many restrictions of p-ary bent functions disappear if $p > 2$.

Similarly, studying p-ary Alltop functions for $p > 3$ seems less restrictive.

This is useful, for example, to applications to Kerdock codes in the following slides.

A Connection Certain Hadamard Matrices

A Hadamard matrix is called p-ary Butson type matrix if it consists of elements ϵ^x, $x \in \mathbb{F}_p$. Here ϵ is a primitive p-th root of 1 in $\mathbb{C}$.

We only consider Butson type Hadamard matrices here.

Definition (Shlichta 1979)

A k-dimensional matrix $H(x_1, \ldots, x_k)$ of size $N \times \cdots \times N$ is called a proper Hadamard matrix if for any $i, j \in \{1, \ldots, k\}$ the matrix $\mathcal{H}_{a_1,\ldots,a_k}(y, z) = H(a_1, \ldots, y, \ldots, z, \ldots, a_k)$ is the Hadamard matrix for every fixed values $a_1, \ldots, a_m, \ldots a_k \in N$, where $m \neq i, j$.

Definition (Hammer and Seberry 1981)

A k-dimensional matrix $H(x_1, \ldots, x_k)$ of size $N \times \cdots \times N$ is called an almost Hadamard matrix if for any $i, j \in \{1, \ldots, k\}$ the matrix $\mathcal{H}_{a_1,\ldots,a_k}(y, z) = H(a_1, \ldots, y, \ldots, z, \ldots, a_k)$ is the Hadamard matrix or all 1s matrix for every fixed values $a_1, \ldots, a_m, \ldots a_k \in N$, where $m \neq i, j$.

A Connection Certain Hadamard Matrices

Define

$$H(x,y,z) = \epsilon^{f(x+y+z)-f(x+y)-f(y+z)-f(z+x)+f(x)+f(y)+f(z)},$$

where f is a p-ary function and $f(0) = 0$.

Theorem

f is a p-ary Alltop function if and only if H is a p-ary almost Butson type Hadamard matrix with only one non Hadamard submatrix in every direction.

Sketch of the proof

Let $z_1 \neq z_2$ and consider

$$\begin{aligned} & f(x+y+z_1) \\ & -f(x+y)-f(x+z_1)-f(y+z_1) \\ & f(x)+f(y)+f(z_1) \end{aligned}$$

$$\begin{aligned} & -f(x+y+z_2) \\ & +f(x+y)+f(x+z_2)+f(y+z_2) \\ & -f(x)-f(y)-f(z_2) \end{aligned}$$

If $y \neq 0$, then observe that this expression, upto a multiplication by a constant on the unit circle depending on y, is equal to

$$D_y D_{z_1-z_2} f(x+z_2).$$

An application Kerdock Codes

Definition

A set of bent functions $K \subseteq \{f : \mathbb{F}_{p^n} \to \mathbb{F}_p : f \text{ bent}\}$ is called a Kerdock set if for any $f_1, f_2 \in K$ with $f_1 \neq f_2$, the difference $f_1 - f_2$ is a bent function.

Theorem

If f is a p-ary Alltop function then $\mathcal{K}_f = \{D_a f : a \in \mathbb{F}_{p^n}^*\}$ is a Kerdock set.

An application Kerdock Codes

Consider a set

$$\mathcal{D}_K = \{K + \ell_{b,c} : b \in \mathbb{F}_p^n, c \in \mathbb{F}_p\},$$

where K is a Kerdock set and $\ell_{b,c}(x) = (x, b) + c$ is an affine function.

Theorem

$\mathcal{D}_K$ is a p-ary Kerdock codes with parameters $(p^n, p^{2n+1}, (p-1)(p^{n-1} - p^{\frac{n}{2}-1})$ for even n and $(p^n, p^{2n+1}, (p-1)p^{n-1} - p^{\frac{n-1}{2}})$ for odd n.

This theorem improves a result of van Ash and van Tilborg 2001.

A Natural Generalization: generalized Alltop functions of degree s

$\mathbb{F}_q$ is a finite field, where $q = p^n$, p is a prime. Let $s \geq 2$ be an integer. $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$.

A function f is called a generalized Alltop function of degree s over $\mathbb{F}_q$ if, for any $a_1, \ldots, a_s \in \mathbb{F}_q^*$, the derived map

$$D_{a_1} D_{a_1} \cdots D_{a_s} f(x)$$

is a permutation function on $\mathbb{F}_{p^n}$.

If $s = 2$, then they correspond to planar functions. The canonical example is x^2 for $p > 2$.

If $s = 3$, then they correspond to Alltop functions. The canonical example is x^3 for $p > 3$.

If $s = 5$, then the canonical example is x^5 for $p > 5$.

Note that s is not necessarily a prime. For example, if $s = 4$, then x^4 is generalized Alltop function of degree 4 if $p > 4$.

Another Natural Generalization: generalized p-ary Alltop functions of degree s

$\mathbb{F}_q$ is a finite field, where $q = p^n$, p is a prime. Let $s \geq 2$ be an integer. A p-ary function $f : \mathbb{F}_q \to \mathbb{F}_p$ is called a generalized p-ary Alltop function of degree s over $\mathbb{F}_q$ if, for any $a_1, \ldots, a_s \in \mathbb{F}_q^*$, the derived map

$$D_{a_1} D_{a_1} \cdots D_{a_s} f(x)$$

is a balanced function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.

If $s = 2$, then they correspond to p-ary bent functions.

If $s = 3$, then they correspond to p-ary Alltop functions.

We have the similar results for the generalized p-ary Alltop function of degree s in some cases. But the problem becomes harder as s increases in general.

It seems there are generic constructions of improper higher dimensional almost Hadamard matrices using generalized p-ary Alltop of functions of degree s.

Thank you very much for your attention.

Muchas gracias por su atención.