Combinatorial t-designs from Special Functions

Chunming Tang
Joint work with Cunsheng Ding

Hong Kong University of Science and Technology
Hong Kong, China

Boolean Functions and their Applications
BFA 2019

Florence, Italy

June 18, 2019

Contents

Among functions, codes and combinatorial designs

Linear codes

- Let q be a power of a prime and let $\mathrm{GF}(q)$ be the finite field with q elements.
- Let $\mathrm{GF}(q)^n$ denote the vector space with dimension n over $\mathrm{GF}(q)$.
- The **weight** of $\mathbf{c} \in \mathrm{GF}(q)^n$ is the number of nonzero coordinates in $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$.
- An $[n, k, d]$ **linear code** $\mathcal{C}$ over $\mathrm{GF}(q)$ is a k-dimensional subspace of $\mathrm{GF}(q)^n$ with minimum (Hamming) distance d.
- The **dual** $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined by

$$\mathcal{C}^\perp = \{\mathbf{w} \in \mathrm{GF}(q)^n : \mathbf{w} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\},$$

  where $\mathbf{w} = (w_0, \ldots, w_{n-1})$, $\mathbf{c} = (c_0, \ldots, c_{n-1})$ and $\mathbf{w} \cdot \mathbf{c} = \sum_{i=0}^{n-1} w_i c_i$ is the **Euclidean inner product**.

Functions and polynomials

- A function f from $GF(q)$ to itself can be identified as a polynomial $\sum_{i=0}^{q-1} c_i x^i \in \mathrm{GF}(q)[x]$, where $c_i \in \mathrm{GF}(q)$.
- By a special function or polynomial over a finite field we mean a polynomial either of special form or with special property. For instance, monomials, permutation polynomials and APN functions are special functions. Special functions or polynomials have interesting applications to cryptography, coding theory and combinatorial designs. For instance, the Dickson polynomials $x^5 + ax^3 + a^2x$ over $\mathrm{GF}(3^m)$ led to a 70-year breakthrough in searching for new skew Hadamard difference sets.

t-designs

t-designs

A t-**design** with parameters t-(v, k, λ) is a pair $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ where $t \leq k$ and:

1. $\mathcal{P}$ is a v-element set of **points**;
2. $\mathcal{B}$ is a family of k-element subsets of $\mathcal{P}$ called **blocks**;
3. Every t-element subset of $\mathcal{P}$ is in exactly λ blocks.

- For convenience, $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ is also called a t-design if $\mathcal{B} = \emptyset$.
- A t-design is called **simple** if $\mathcal{B}$ does not contain repeated blocks. In this talk, we consider only simple t-designs.
- The parameters of a t-design are not independent, since they satisfy

$$\binom{v}{t}\lambda = \binom{k}{t}|\mathcal{B}|.$$

- A 2-design with an equal number of points and blocks is called a **symmetric design**.
- A t-$(v, k, 1)$ design is called a **Steiner system** denoted by $S(t, k, v)$.

t-designs from linear codes

t-designs from linear codes

Let $\mathcal{C}$ be a linear code over $\mathrm{GF}(q)$. Let $\mathcal{P}(\mathcal{C}) = \{0, 1, \ldots, \nu - 1\}$ be the set of the coordinate positions of $\mathcal{C}$, where ν is the length of $\mathcal{C}$. For a codeword $\mathbf{c} = (c_0, \ldots, c_{\nu-1})$ in $\mathcal{C}$, the **support** of $\mathbf{c}$ is defined by

$$\mathrm{Supp}(\mathbf{c}) = \{i : c_i \neq 0, i \in \mathcal{P}(\mathcal{C})\}.$$

Let $\mathcal{B}_w(\mathcal{C}) = \{\mathrm{Supp}(\mathbf{c}) : wt(\mathbf{c}) = w \text{ and } \mathbf{c} \in \mathcal{C}\}$. For some special $\mathcal{C}$, $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ is a t-design. If $(\mathcal{P}(\mathcal{C}), \mathcal{B}_w(\mathcal{C}))$ is a t-design for any $t \leq w \leq \nu$, we say that the code $\mathcal{C}$ **supports t-designs**.

Assmus-Mattson Theorem

The Assmus-Mattson theorem is a very famous theorem relating linear codes and combinatorial designs.

Theorem 1 (Assmus-Mattson)

Let $\mathcal{C}$ be a binary linear code of length ν over $\mathrm{GF}(q)$ with minimum weight d. Let $\mathcal{C}^\perp$ with minimum weight $d^\perp$ denote the dual code of $\mathcal{C}$. Let t $(1 \leq t < \min\{d, d^\perp\})$ be an integer such that there are at most $d^\perp - t$ weights of $\mathcal{C}$ in $\{t+1, t+2, \ldots, \nu - t\}$. Then $(\mathcal{P}(\mathcal{C}), \mathcal{B}_k(\mathcal{C}))$ and $(\mathcal{P}(\mathcal{C}^\perp), \mathcal{B}_k(\mathcal{C}^\perp))$ are t-designs for all $k \in \{t+1, t+2, \ldots, \nu\}$.

- If one would like to employ the Assmus-Mattson Theorem for the construction of t-designs, one has to settle the weight distribution of linear code and the minimum distance of its dual at the same time.

Linear codes from t-designs

Linear codes from t-designs

Let $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ be a t-design and $\mathcal{P} = \{p_1, \ldots, p_\nu\}$. For any block $B \in \mathcal{B}$, the **characteristic vector** of B is defined by the vector $\mathbf{c}_B = (c_1, \ldots, c_\nu) \in \{0, 1\}^\nu$, where

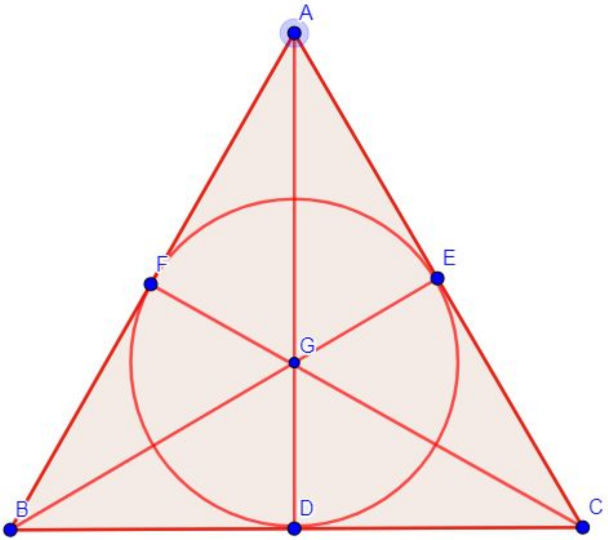
$$c_i = \begin{cases} 1, & \text{if } p_i \in B, \\ 0, & \text{if } p_i \notin B. \end{cases}$$

For a prime p, a **linear code** $\mathcal{C}_p(\mathbb{D})$ over the prime field $\mathrm{GF}(p)$ from the design $\mathbb{D}$ is spanned by the characteristic vectors of the blocks of $\mathbb{D}$, which is the subspace $\mathrm{Span}\{\mathbf{c}_B : B \in \mathcal{B}\}$ of the vector space $\mathrm{GF}(p)^\nu$.

A t-design $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ induces a linear code $\mathcal{C}_p(\mathbb{D})$ over GF(p) for any prime p. Linear codes $\mathcal{C}_p(\mathbb{D})$ from designs $\mathbb{D}$ have been studied and documented in the literature [Assmus, Key, 1992].

E. F. Assmus Jr., J. D. Key. Designs and Their Codes, Cambridge University Press, Cambridge, 1992.

Fano plane



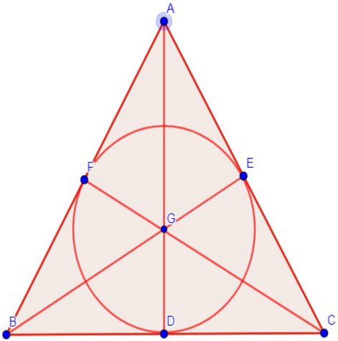
Finite projective plane

- The Fano plane is the projective plane arising from the finite field $\mathrm{GF}(2)$. It is the smallest projective plane, with only seven points and seven lines.
- In the figure above, the seven points are shown as small blue points, and the seven lines are shown as six line segments and a circle.
- We can give a description of the seven points and the seven lines using homogeneous coordinates.

Finite projective plane

- $A = (1:0:0)$, $B = (0:1:0)$, $C = (0:0:1)$, $D = (0:1:1)$, $E = (1:0:1)$, $F = (1:1:0)$, $G = (1:1:1)$.
- $\mathcal{B} \Longleftrightarrow$ Lines:

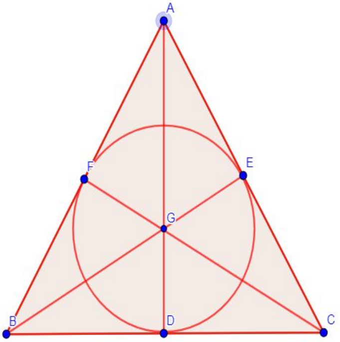
$$\{B, D, C\} \leftrightarrow x = 0$$
$$\{C, E, A\} \leftrightarrow y = 0$$
$$\{A, F, B\} \leftrightarrow z = 0$$
$$\{A, G, D\} \leftrightarrow y + z = 0$$
$$\{B, G, E\} \leftrightarrow z + x = 0$$
$$\{C, G, F\} \leftrightarrow x + y = 0$$
$$\{D, E, F\} \leftrightarrow x + y + z = 0$$



2-$(7,3,1)$ – *designs*

- $\mathcal{P} = \{A, B, C, D, E, F, G\}$.
- $\mathcal{B}$:

$$\{B, D, C\}$$
$$\{C, E, A\}$$
$$\{A, F, B\}$$
$$\{A, G, D\}$$
$$\{B, G, E\}$$
$$\{C, G, F\}$$
$$\{D, E, F\}$$

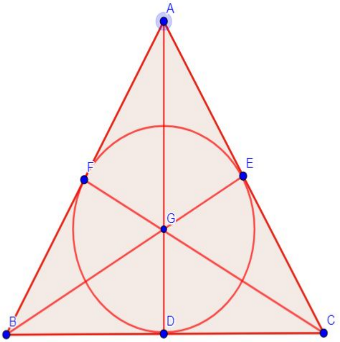


$[7,4,3]$ linear code from Fano plane

Blocks and codewords of weight 3

- $\mathcal{B} \Longleftrightarrow$ Codewords:

$$\{B,D,C\} \leftrightarrow (0,1,1,1,0,0,0)$$
$$\{C,E,A\} \leftrightarrow (1,0,1,0,1,0,0)$$
$$\{A,F,B\} \leftrightarrow (1,1,0,0,0,1,0)$$
$$\{A,G,D\} \leftrightarrow (1,0,0,1,0,0,1)$$
$$\{B,G,E\} \leftrightarrow (0,1,0,0,1,0,1)$$
$$\{C,G,F\} \leftrightarrow (0,0,1,0,0,1,1)$$
$$\{D,E,F\} \leftrightarrow (0,0,0,1,1,1,0)$$



The linear code $\mathcal{C}$ over $\mathrm{GF}(2)$ from the design of the Fano plane is a $[7,4,3]$ linear code.

2-designs from the $[7,4,3]$ linear codes

2-$(7,3,1)$ design

$$\{B,D,C\} \leftrightarrow (0,1,1,1,0,0,0)$$
$$\{C,E,A\} \leftrightarrow (1,0,1,0,1,0,0)$$
$$\{A,F,B\} \leftrightarrow (1,1,0,0,0,1,0)$$
$$\{A,G,D\} \leftrightarrow (1,0,0,1,0,0,1)$$
$$\{B,G,E\} \leftrightarrow (0,1,0,0,1,0,1)$$
$$\{C,G,F\} \leftrightarrow (0,0,1,0,0,1,1)$$
$$\{D,E,F\} \leftrightarrow (0,0,0,1,1,1,0)$$

2-$(7,4,2)$ design

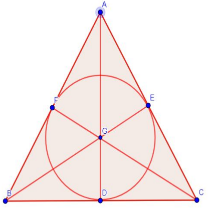
$$\{A,E,F,G\} \leftrightarrow (1,0,0,0,1,1,1)$$
$$\{B,D,F,G\} \leftrightarrow (0,1,0,1,0,1,1)$$
$$\{C,D,E,G\} \leftrightarrow (0,0,1,1,1,0,1)$$
$$\{B,C,E,F\} \leftrightarrow (0,1,1,0,1,1,0)$$
$$\{A,C,D,F\} \leftrightarrow (1,0,1,1,0,1,0)$$
$$\{A,B,D,E\} \leftrightarrow (1,1,0,1,1,0,0)$$
$$\{A,B,C,G\} \leftrightarrow (1,1,1,0,0,0,1)$$

The $[7,4,3]$ linear code $\mathcal{C}$ holds a 2-$(7,3,1)$ design and a 2-$(7,4,2)$ design. These two designs are complementary.

Affine functions and Fano plane

- $A=(1,0,0)$, $B=(0,1,0)$, $C=(0,0,1)$, $D=(0,1,1)$, $E=(1,0,1)$, $F=(1,1,0)$, $G=(1,1,1)$.
- $\mathcal{B} \Longleftrightarrow$ Codewords $\Longleftrightarrow$ Affine functions:

$$\{B,D,C\} \leftrightarrow (0,1,1,1,0,0,0) \leftrightarrow x+1$$
$$\{C,E,A\} \leftrightarrow (1,0,1,0,1,0,0) \leftrightarrow y+1$$
$$\{A,F,B\} \leftrightarrow (1,1,0,0,0,1,0) \leftrightarrow z+1$$
$$\{A,G,D\} \leftrightarrow (1,0,0,1,0,0,1) \leftrightarrow y+z+1$$
$$\{B,G,E\} \leftrightarrow (0,1,0,0,1,0,1) \leftrightarrow z+x+1$$
$$\{C,G,F\} \leftrightarrow (0,0,1,0,0,1,1) \leftrightarrow x+y+1$$
$$\{D,E,F\} \leftrightarrow (0,0,0,1,1,1,0) \leftrightarrow x+y+z+1$$

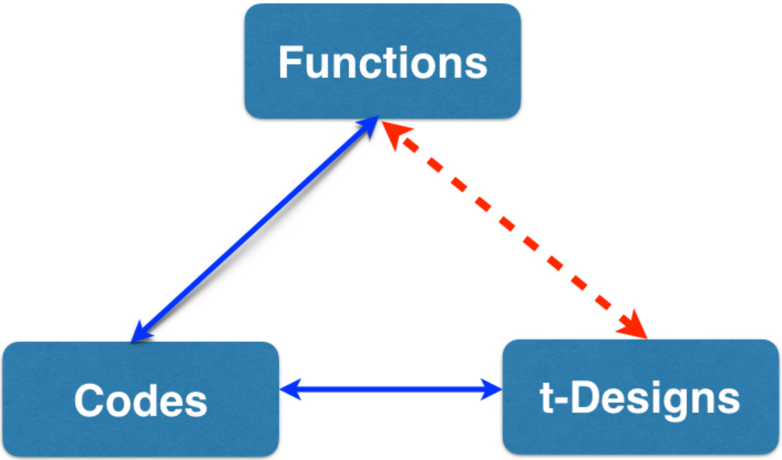


Every characteristic vector of a block of the design from Fano plane can be identified as the truth table of affine function $ax+by+cz+1$ at the non-zero points of $\mathrm{GF}(2)^3$, where (a,b,c) is a non-zero vector in $\mathrm{GF}(2)^3$. The linear code from this design is just the punctured code from the first order Reed-Muller code over $\mathrm{GF}(2)^3$.

Functions, codes and t-designs

- A lot of good codes are constructed from functions. In turn, many special functions can be characterized by coding theory.
- Linear codes and t-designs are companions. On one hand, the characteristic vectors of the blocks of a t-design generates a linear code. On the other hand, the supports of codewords of a fixed Hamming weight in a code may form a t-design under certain conditions.
- Our main goal is to establish a more direct link between functions and combinatorial designs. The main bridge is the group action.

A triangle relation



Combinatorial designs from group actions

Group action

Group action

If G is a group and $\mathcal{P}$ is a set, then a (left) **group action** ρ of G on $\mathcal{P}$ is a function

$$\begin{aligned} \rho: \; & G \times \mathcal{P} \to \mathcal{P} \\ & (g,x) \mapsto \rho(g,x) \end{aligned}$$

that satisfies the following two axioms (where we denote $\rho(g,x)$ as $g \cdot x$):

1. **Identity:** $1 \cdot x = x$ for all x in $\mathcal{P}$.
2. **Compatibility:** $(gh) \cdot x = g \cdot (h \cdot x)$ for all g, h in G and all x in $\mathcal{P}$.

- G is said to be t-**transitive** on $\mathcal{P}$, if for any two ordered t-subsets of $\mathcal{P}$, there is a $g \in G$ such that g sends the former to the latter.
- G is said to be t-**homogeneous** on $\mathcal{P}$, if for any two t-subsets of $\mathcal{P}$, there is a $g \in G$ such that g sends the former to the latter.

General affine group

General affine group $\mathrm{GA}_1(q)$

The **general affine group** $\mathrm{GA}_1(q)$ of **degree one** consists of all the following permutations of the finite field $\mathrm{GF}(q)$:

$$\pi_{a,b}(x) = ax + b,$$

where $(a,b) \in \mathrm{GF}(q)^* \times \mathrm{GF}(q)$. It is a group under the function composition operation, and is interesting, as it is 2-transitive on $\mathrm{GF}(q)$ and has a small group size.

t-designs via t-homogeneous groups

Orbit of k-subsets

Let B be a k-subset of $\mathcal{P}$ and $g(B) = \{g \cdot x : x \in B\}$, where $g \in G$. The **orbit** of B under the action of G is $G(B) = \{g(B) : g \in G\}$, and the **stabilizer** of B under the action of G is $G_B = \{g \in G : g(B) = B\}$. The incidence structure $\mathbb{S}(B) := (\mathcal{P}, G(B))$ may be a t-(ν, k, λ) design for some λ, where $\mathcal{P}$ is the point set, B is called a base block, and the incidence relation is the set membership. In this case, we say that the base block B **supports** a t-design and $(\mathcal{P}, G(B))$ is called the **orbit design** of B.

Theorem

Let G be t-homogeneous on $\mathcal{P}$ and let $B \subseteq \mathcal{P}$ be any k-element subset with $t < k < \nu = |\mathcal{P}|$, then the incidence structure $(\mathcal{P}, G(B))$ is a t-(ν, k, λ) design, where $\lambda = \frac{|G|}{|G_B|\binom{k}{t}}$.

2-designs from 1-transitive groups

Difference set

A (v, k, λ) **difference set** is a subset D of size k of a group G of order v such that every nonidentity element of G can be expressed as a product $d_1 d_2^{-1}$ of elements of D in exactly λ ways. A difference set D is said to be **cyclic**, **abelian**, **non-abelian**, etc., if the group G has the corresponding property.

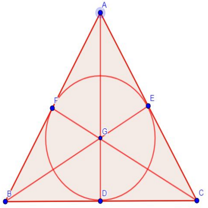
2-designs from 1-transitive group

Let $\mathcal{P} = G$ and let D be a k-subset of $\mathcal{P}$. Then $(\mathcal{P}, G(D))$ is always a 1-design. If D is a (v, k, λ) difference set, $(\mathcal{P}, G(D))$ is a 2-(v, k, λ) design, called the **development** of D. The group G acts as an automorphism group of the design. It is transitive on both points and blocks.

Fano plane and $(7,3,1)$-difference set in $\mathbb{Z}_7$

- $A=6$, $B=1$, $C=4$, $D=2$, $E=3$, $F=5$, $G=0$.
- $\mathcal{B} \Longleftrightarrow$ Translates of $\{1,2,4\}$:

$$
\begin{aligned}
\{B,D,C\} &\leftrightarrow \{1,2,4\} = 0+\{1,2,4\}\\
\{C,E,A\} &\leftrightarrow \{4,3,6\} = 2+\{1,2,4\}\\
\{A,F,B\} &\leftrightarrow \{6,5,1\} = 4+\{1,2,4\}\\
\{A,G,D\} &\leftrightarrow \{6,0,2\} = 5+\{1,2,4\}\\
\{B,G,E\} &\leftrightarrow \{1,0,3\} = 6+\{1,2,4\}\\
\{C,G,F\} &\leftrightarrow \{4,0,5\} = 3+\{1,2,4\}\\
\{D,E,F\} &\leftrightarrow \{2,3,5\} = 1+\{1,2,4\}
\end{aligned}
$$

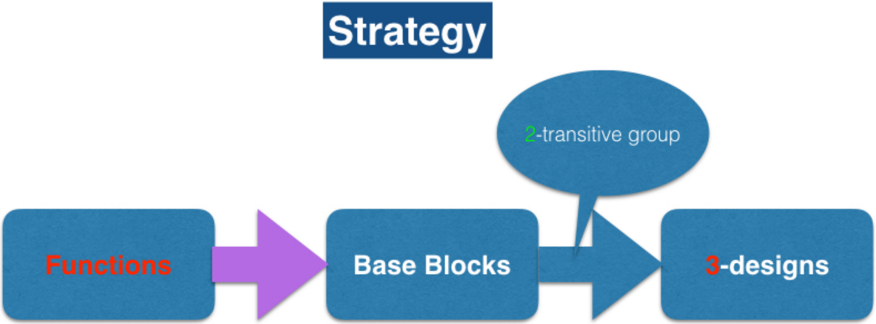


3-designs from 2–transitive group $\mathrm{GA}_1(q)$

3-designs from 2-transitive group $\mathrm{GA}_1(q)$

Motivation

Let $\mathcal{P} = \mathrm{GF}(q)$ and $G = \mathrm{GA}_1(q)$, which is 2-transitive. Then the incidence structure $(\mathrm{GF}(q), \mathrm{GA}_1(q)(B))$ is always a 2-design. Our main motivation is to study how to choose a base block $B \subseteq \mathrm{GF}(q)$ properly such that $(\mathrm{GF}(q), \mathrm{GA}_1(q)(B))$ is a 3-design.



Characteristic functions of base blocks

Walsh transform

For any Boolean function f from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2)$, the **Walsh transform** of f at $\mu \in \mathrm{GF}(2^n)$ is defined as

$$\hat{f}(\mu) = \sum_{x \in \mathrm{GF}(2^n)} (-1)^{f(x)+\mathrm{Tr}(\mu x)},$$

where $\mathrm{Tr}(\cdot)$ is the absolute trace function from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2)$. All the values $\hat{f}(\mu)$ are also called the **Walsh coefficients** of f. The Boolean function f is said to be **semi-bent** if $\{\hat{f}(\mu) : \mu \in \mathrm{GF}(2^n)\} = \{0, \pm 2^{\frac{n+1}{2}}\}$.

Characteristic functions of base blocks

Let B be a subset of $\mathrm{GF}(q)$. Then, the **characteristic function** $f_B(x)$ of B is given by

$$f_B(x) = \begin{cases} 1, & x \in B, \\ 0, & \text{otherwise.} \end{cases}$$

A characterization of base blocks supporting 3-designs

- Let E be any subset of $\mathrm{GF}(q)$ and $a, b, c \in \mathrm{GF}(q)$, then define

$$N_E(a,b,c) = |\{ax + by + cz = 0 : x, y, z \in E\}|.$$

Theorem 2

Let B be a k-subset of $\mathrm{GF}(q)$ with $k \geq 3$ and $\mathcal{B} = \mathrm{GA}_1(q)(B)$. Then, the following are equivalent:

1. $(\mathrm{GF}(q), \mathcal{B})$ *is a 3-design.*
2. $\sum_{x,y \in \mathrm{GF}(q)} (-1)^{f_B(x)+f_B(y)+f_B(ux+(1+u)y)}$ *is independent of u, where $u \in \mathrm{GF}(q) \setminus \mathrm{GF}(2)$.*
3. $\sum_{\alpha \in \mathrm{GF}(q)} \hat{f}_B(\alpha)\hat{f}_B(u\alpha)\hat{f}_B((1+u)\alpha)$ *is independent of u, where $u \in \mathrm{GF}(q) \setminus \mathrm{GF}(2)$.*
4. $N_B(u, 1+u, 1)$ *is independent of u, where $u \in \mathrm{GF}(q) \setminus \mathrm{GF}(2)$.*

More efficient characterization

If $\hat{f}_B(\mu)$ is the composition of a power function μ^d and the Walsh transformation $\hat{f}_E$ of a simpler function f_E, we have the following more practical and efficient characterization of the base block B supporting 3-design.

Theorem 3

Let B be a k-subset of $\mathrm{GF}(q)$ with $k \geq 3$ and $\mathcal{B} = \mathrm{GA}_1(q)(B)$. Let E be a subset of $\mathrm{GF}(q)$ such that $\hat{f}_B(\mu) = \hat{f}_E(\mu^d)$ for any $\mu \in \mathrm{GF}(q)$, where $\gcd(d, q-1) = 1$. Then, the following are equivalent:

1. $(\mathrm{GF}(q), \mathcal{B})$ *is a 3-design.*
2. $\sum_{x,y \in \mathrm{GF}(q)} (-1)^{f_E(x)+f_E(y)+f_E(u^d x+(1+u)^d y)}$ *is independent of u, where $u \in \mathrm{GF}(q) \setminus \mathrm{GF}(2)$.*
3. $\sum_{\alpha \in \mathrm{GF}(q)} \hat{f}_E(\alpha)\hat{f}_E(u^d\alpha)\hat{f}_E((1+u)^d\alpha)$ *is independent of u, where $u \in \mathrm{GF}(q) \setminus \mathrm{GF}(2)$.*
4. $N_E(u^d, (1+u)^d, 1)$ *is independent of u, where $u \in \mathrm{GF}(q) \setminus \mathrm{GF}(2)$.*

A characterization of 3-designs by solutions of some equation

In the case $f_E(x) = \mathrm{Tr}(x^t)$, we have the following characterization of the base block B supporting 3-design by solutions of some equation.

Theorem 4

Let B be a k-subset of $\mathrm{GF}(q)$ with $k \geq 3$ and $\mathcal{B} = \mathrm{GA}_1(q)(B)$. Suppose that $\hat{f}_B(\mu) = \sum_{x\in\mathrm{GF}(q)}(-1)^{\mathrm{Tr}(x^t+\mu^d x)}$ for any $\mu \in \mathrm{GF}(q)$, where $\gcd(td, q-1) = 1$. Then, $(\mathrm{GF}(q), \mathcal{B})$ is a 3-design, if and only if,

$$\left|\{x \in \mathrm{GF}(q) : \left(u^d x + (1+u)^d\right)^t + x^t + 1 = 0\}\right|$$

is independent of u, where $u \in \mathrm{GF}(q) \setminus \mathrm{GF}(2)$.

The stabilizer of the base block

The following theorem gives a sufficient condition for the stabilizer of the base blocks under the action of the general affine group to be trivial, which is used to determine parameters of designs derived from some special base blocks.

Theorem 5

Let B, E be two subsets of $\mathrm{GF}(q)$ such that f_E is a semi-bent function from $\mathrm{GF}(q)$ to $\mathrm{GF}(2)$. Suppose that $\hat{f}_B(\mu) = \hat{f}_E(\mu^d)$ for any $\mu \in \mathrm{GF}(q)$ and $\mathrm{Supp}(\hat{f}_E) \neq b \cdot \mathrm{Supp}(\hat{f}_E)$ for any $b \in \mathrm{GF}(q) \setminus \mathrm{GF}(2)$, where $\gcd(d, q-1) = 1$. Then

$$\mathrm{GA}_1(q)_B = \{x\}.$$

Hence, $|\mathrm{GA}_1(q)(B)| = q(q-1)$.

3-designs from APN functions

APN and AB functions

APN function

A function F from $\mathrm{GF}(q)$ to itself is called **almost perfect nonlinear** (**APN**), if $F(x+a)+f(x)=b$ has at most two solutions in $\mathrm{GF}(q)$ for every pair $(a,b) \in \mathrm{GF}(q)^* \times \mathrm{GF}(q)$.

AB function

F is said to be **almost bent** (**AB**) if $\mathcal{W}_F(a,b) = 0$, or $\pm 2^{\frac{n+1}{2}}$ for every pair (a,b) with $a \neq 0$, where

$$\mathcal{W}_F(a,b) = \sum_{x \in \mathrm{GF}(q)} (-1)^{\mathrm{Tr}(aF(x)+bx)}.$$

Every AB function is an APN function. The converse is not true in general (counter-examples: inverse function, Dobbertin function).

Known APN power functions x^s

1. $s = 2^i + 1$ with $\gcd(i, n) = 1$ (**Gold functions**);
2. $s = 2^{2i} - 2^i + 1$ with $\gcd(i, n) = 1$ (**Kasami functions**);
3. $s = 2^{\frac{n-1}{2}} + 3$ with n odd (**Welch functions**);
4. $s = 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} - 1$ with $n \equiv 1 \pmod 4$,
   $s = 2^{\frac{n-1}{2}} + 2^{\frac{3n-1}{4}} - 1$ with $n \equiv 3 \pmod 4$ (**Niho functions**);
5. $s = 2^n - 2$ with n odd (**inverse functions**);
6. $s = 2^{\frac{4n}{5}} + 2^{\frac{3n}{5}} + 2^{\frac{2n}{5}} + 2^{\frac{n}{5}} - 1$ with $n \equiv 0 \pmod 5$ (**Dobbertin functions**).

Known AB power functions

When n is odd, Gold functions, Kassami functions, Welch functions and Niho functions over $\mathrm{GF}(2^n)$ are AB functions.

Codes from AB functions

Codes from functions

For any function F from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2^m)$, we define the following linear code

$$\mathcal{C}_F = \{\left(\mathrm{Tr}_{2^m/2}(aF(x)+bx)+h\right)_{x\in\mathrm{GF}(2^m)} : a, b \in \mathrm{GF}(2^m), h \in \mathrm{GF}(2)\}. \quad (1)$$

Theorem 6 (Codes from AB functions)

Let $m \geq 5$ and let F be an AB function. The code $\mathcal{C}_F$ of (1) has parameters $[2^m, 2m+1, 2^{m-1}-2^{(m-1)/2}]$ and weight enumerator

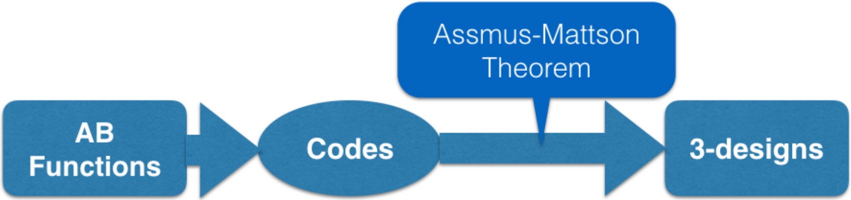
$$A(z) = 1 + uz^{2^{m-1}-2^{(m-1)/2}} + vz^{2^{m-1}} + uz^{2^{m-1}+2^{(m-1)/2}} + z^{2^m}, \quad (2)$$

where

$$u = 2^{2m-1} - 2^{m-1} \text{ and } v = 2^{2m} + 2^m - 2.$$

The dual code $\mathcal{C}_F^{\perp}$ has parameters $[2^m, 2^m-m-1, 6]$.

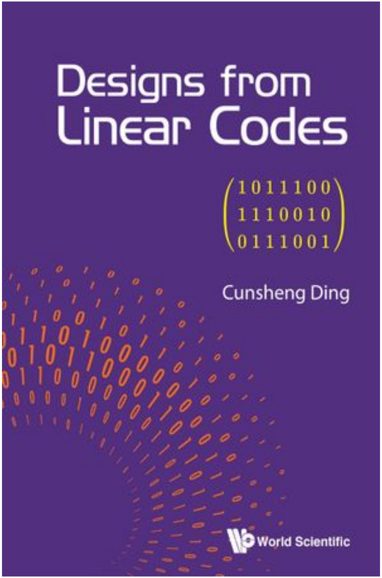
3-designs from the codes associated with AB functions



Cunsheng, Ding

Designs from linear codes

World Scientific, 2018



The first construction of 3-designs from Kassami APN functions by group actions

3-designs from Kassami APN functions

Let $\gcd(2, n) = 1$ and $\gcd(i, n) = 1$. Thus $\frac{1}{3}$ and $\frac{1}{2^i+1}$ exist. Define

$$B = \mathrm{GF}(q) \setminus \left\{ ((x+1)^s + x^s + 1)^{\frac{1}{2^i+1}} : x \in \mathrm{GF}(q) \right\},$$

where $s = 2^{2i} - 2^i + 1$. In this case, we also denote the base block B by $KA_{n,i}$.
We shall study the incidence structure

$$\mathbb{KA}_{n,i} = (\mathrm{GF}(2^n), \mathrm{GA}_1(2^n)(KA_{n,i})).$$

Remarks

In fact, if no exponent $\frac{1}{2^i+1}$ appears, the resulting block also supports 3-design. However, in this case, we do not know how to prove the corresponding result.

The Walsh transform of the characteristic function of $KA_{n,i}$

Lemma 7

Let n be an odd integer and i be a positive integer with $\gcd(i,n)=1$. Let $B=KA_{n,i}$. Then for all $\mu \in \mathrm{GF}(q)$ we have

$$\hat{f}_B(\mu) = \hat{f}_E\left(\mu^{\frac{2^i+1}{3}}\right) = \sum_{x\in\mathrm{GF}(q)} (-1)^{\mathrm{Tr}\left(x^3+\mu^{\frac{2^i+1}{3}}x\right)},$$

where $E=\{x\in\mathrm{GF}(q) : \mathrm{Tr}(x^3)=1\}$.

J. F. Dillon, H. Dobbertin. New cyclic difference sets with Singer parameters. Finite Fields and Their Applications, 10(3): 342-389, 2004.

The equation associated with $KA_{n,i}$

Lemma 8

Let $\sigma_1, \sigma_2, \sigma_3 \in \mathrm{GF}(2^n)$ such that $\sigma_1^2 \neq \sigma_2$ and $\sigma_3 \neq \sigma_1\sigma_2$. Then the cubic equation $x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 = 0$ has a unique solution $x \in \mathrm{GF}(2^n)$, if and only if

$$\mathrm{Tr}\left(\frac{(\sigma_2 + \sigma_1^2)^3}{(\sigma_3 + \sigma_1\sigma_2)^2} + 1\right) = 1.$$

Lemma 9

Let n be an odd integer and i be a positive integer with $\gcd(i,n) = 1$. Then the cubic equation

$$\left(u^d x + (1+u)^d\right)^3 + x^3 + 1 = 0$$

has a unique solution $x \in \mathrm{GF}(2^n)$, where $d \equiv \frac{2^i+1}{3} \pmod{2^n - 1}$ and $u \in \mathrm{GF}(2^n) \setminus \mathrm{GF}(2)$.

3-design $\mathbb{KA}_{n,i} = (\mathrm{GF}(q), \mathrm{GA}_1(q)(KA_{n,i}))$

Theorem 10

Let n be an odd integer and i be a positive integer with $\gcd(i,n) = 1$. Let $B = KA_{n,i}$. Then the incidence structure $\mathbb{KA}_{n,i} = (\mathrm{GF}(q), \mathrm{GA}_1(q)(B))$ is a 3-$\left(q, \frac{q}{2}, \frac{q(q-4)}{8}\right)$ design.

It is observed that $\mathbb{KA}_{n,i}$ and $\mathbb{KA}_{n,n-i}$ are isomorphic. Thus, we only need to consider the 3-design $\mathbb{KA}_{n,n-i}$, where $1 \leq i \leq \frac{n-1}{2}$ and $\gcd(i,n) = 1$.

C. Tang. Infinite families of 3-designs from APN functions. arXiv:1904.04071, 2019.

Another construction of 3-designs from APN functions

3-designs from APN functions

Let x^s be an APN function over $\mathrm{GF}(q)$ with $\gcd(s, q-1) = 1$. Define the base block B_s as

$$B_s = \{(x+1)^s + x^s : x \in \mathrm{GF}(q)\}. \quad (3)$$

Since x^s is APN, the function $(x+1)^s + x^s$ is 2-to-1. Thus, $|B_s| = \frac{q}{2}$. In this case, we also denote the base block B_s by $AP_{n,s}$. We shall study the incidence structure

$$\mathbb{AP}_{n,s} = (\mathrm{GF}(2^n), \mathrm{GA}_1(2^n)(AP_{n,s})).$$

When $s = 2^i + 1$, we have the following theorem on 3-designs $\mathbb{AP}_{n,s}$.

Theorem 11

Let $n \geq 4$ and $s = 2^i + 1$, where $n/\gcd(i, n)$ is odd. Then the incidence structure $\mathbb{AP}_{n,s} = (\mathrm{GF}(q), \mathrm{GA}_1(q)(AP_{n,s}))$ is a 3-$(q, q/2, (q-4)/4)$.

The case for special Kasami APN functions

Proposition 12

Let $n = 3i \pm 1$ *and* $s = 2^{2i} - 2^i + 1$, *where* i *is an even positive integer. Then,*

$$\hat{f}_{B_s}(\mu) = \hat{f}_E(\mu^d) = \sum_{x \in \mathrm{GF}(q)} (-1)^{\mathrm{Tr}\left(x^{2^i+1} + \mu^d x\right)},$$

where $E = \{\mu : \mathrm{Tr}(x^{2^i+1}) = 1\}$ *and* $d \equiv \frac{1}{s} \pmod{2^n - 1}$.

Proposition 13

Let $n = 3i \pm 1$ *and* $s = 2^{2i} - 2^i + 1$, *where* i *is an even positive integer. Let* $d \equiv \frac{1}{s} \pmod{2^n - 1}$. *Then, the incidence structure* $\mathbb{AP}_{n,s}$ *is a* 3*-design, if and only if,*

$$\left| \left\{ x \in \mathrm{GF}(2^n) : \left(u^d x + (1+u)^d\right)^{2^i+1} + x^{2^i+1} + 1 = 0 \right\} \right|$$

is independent of u, *where* $u \in \mathrm{GF}(q) \setminus \mathrm{GF}(2)$.

Equations associated with special Kasami APN functions

Conjecture 1

Let $n = 3i \pm 1$ and $s = 2^{2i} - 2^i + 1$, where i is an even positive integer. Let $u \in \mathrm{GF}(q) \setminus \mathrm{GF}(2)$. Then, the equation

$$\left(u^d x + (1+u)^d\right)^{2^i+1} + x^{2^i+1} + 1 = 0$$

has a unique solution $x \in \mathrm{GF}(2^n)$, where $d \equiv \frac{1}{s} \pmod{2^n - 1}$.

Conjecture 1 was confirmed by Magma for $n \in \{5, 7, 11, 13\}$. If Conjecture 1 is true, the base block $B_s \subseteq \mathrm{GF}(2^n)$ supports a 3-design, where $n = 6i \pm 1$ and $s = 2^{4i} - 2^{2i} + 1$. The equation $\left(u^d x + (1+u)^d\right)^{2^i+1} + x^{2^i+1} + 1 = 0$ may be reduced to $P_a(x) = x^{2^i+1} + x + a = 0$, which has been considered in many papers.

A. W. Bluher. On $x^{q+1} + ax + b$. Finite Fields and Their Applications, 10(3), 285305, 2004.

T. Helleseth, A. Kholosha. On the equation $x^{2^l+1} + x + a = 0$ over $\mathrm{GF}(2^k)$. Finite Fields and Their Applications, 14(1):159-176, 2008.

K. K. Kim, S. Mesnager. Solving $x^{2^k+1} + x + a = 0$ in $\mathbb{F}_{2^n}$ with $\gcd(n,k) = 1$. arXiv:1903.07481, 2019.

The uniqueness of the solution of the equation

- Although the equation $\left(u^d x + (1+u)^d\right)^{2^i+1} + x^{2^i+1} + 1 = 0$ can be reduced to the equation $x^{2^i+1} + x + a = 0$, the expression of a on u is extremely complicated.
- To solve Conjecture 1, one may need the following results.

Theorem 14

For any $a \in \mathrm{GF}(2^n)^*$ and a positive integer i with $n = 3i-1$, the polynomial $P_a(x) = x^{2^i+1} + x + a$ has either none, one, or three zeros in $\mathrm{GF}(2^n)$. Further, $P_a(x)$ has exactly one zero in $\mathrm{GF}(2^n)$ if and only if $\mathrm{Tr}\left(R_{n,\frac{1}{3}}(a^{-1}) + 1\right) = 1$, where $R_{n,\frac{1}{3}}(x) = x^{2^{2i}+2^i+1} + x^{2^{2i}+2^i-1} + x^{2^{2i}-2^i+1} + x^{2^i+1} + x$.

Therefore, the discriminating conditions for the unique solution of such equations are also complicated. The complexity of these two aspects makes it difficult to prove that the original equation has a unique solution.

More conjectured 3-designs from APN functions

Conjecture 2 (3-designs from Kassami functions)

Let $n \geq 5$ be odd. Let $s = 2^{2i} - 2^i + 1$ with $\gcd(3i, n) = 1$. Then the incidence structure $\mathbb{AP}_{n,s} = (\mathrm{GF}(q), \mathrm{GA}_1(q)(AP_{n,s}))$ is a 3-$\left(q, \frac{q}{2}, \frac{q(q-4)}{8}\right)$ design.

Conjecture 3 (3-designs from Welch functions)

Let $n \geq 5$ be odd and $s = 2^{\frac{n-1}{2}} + 3$. Then the incidence structure $\mathbb{AP}_{n,s} = (\mathrm{GF}(q), \mathrm{GA}_1(q)(AP_{n,s}))$ is a 3-$\left(q, \frac{q}{2}, \frac{q(q-4)}{8}\right)$ design.

Conjecture 4 (3-designs from Niho functions)

Let $n \geq 5$ be odd. Then the incidence structure $\mathbb{AP}_{n,s} = (\mathrm{GF}(q), \mathrm{GA}_1(q)(AP_{n,s}))$ is a 3-$\left(q, \frac{q}{2}, \frac{q(q-4)}{8}\right)$ design, where

- $s = 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} - 1$ *with* $n \equiv 1 \pmod 4$;
- $s = 2^{\frac{n-1}{2}} + 2^{\frac{3n-1}{4}} - 1$ *with* $n \equiv 3 \pmod 4$.

3-designs from APN functions

- We present two general constructions of 3-designs from APN functions over finite fields. The first construction has produced infinite families of 3-designs from Kassami APN functions over $\mathrm{GF}(2^n)$.
- Because the Walsh transformations of the character functions of the base blocks in the second construction are very complex and irregular, it seems difficult to study these conjectured 3-designs by Walsh transformations. We may need other techniques to prove these conjectured 3-designs.

3-designs from o-polynomials

Arcs in the projective plane $\mathrm{PG}(2, \mathrm{GF}(q))$

Definition

An **arc** in $\mathrm{PG}(2, \mathrm{GF}(q))$ is a set of at least three points in $\mathrm{PG}(2, \mathrm{GF}(q))$ such that no three of them are collinear.

Example

The set of points of $\mathrm{PG}(2, \mathrm{GF}(q))$

$$\mathcal{A} = \{(t^2 : t : 1) : t \in \mathrm{GF}(q)\} \cup \{(1 : 0 : 0)\}$$

is an arc with $q+1$ points in $\mathrm{PG}(2, \mathrm{GF}(q))$.

Ovals in $\mathrm{PG}(2, \mathrm{GF}(q))$

Theorem 15

If $\mathcal{A}$ is an arc of $\mathrm{PG}(2, \mathrm{GF}(q))$, then

$$|\mathcal{A}| \leq \begin{cases} q+1 & \text{if } q \text{ is odd,} \\ q+2 & \text{if } q \text{ is even.} \end{cases}$$

Definition

An **oval** O in $\mathrm{PG}(2, \mathrm{GF}(q))$ is a set of $q+1$ points such that no three of them are collinear, i.e., an arc with $q+1$ points.

Example

Let $q \geq 4$. Then

$$O = \{(t^2 : t : 1) : t \in \mathrm{GF}(q)\} \cup \{(1 : 0 : 0)\}$$

is an oval in $\mathrm{PG}(2, \mathrm{GF}(q))$.

Conics in $\mathrm{PG}(2, \mathrm{GF}(q))$

Definition

A *conic* in $\mathrm{PG}(2, \mathrm{GF}(q))$ is a set of points of $\mathrm{PG}(2, \mathrm{GF}(q))$ that are zeros of a nondegenerate homogeneous quadratic form $f(x, y, z)$ in three variables.

Example

Let $\mathcal{P}$ be the point set of $\mathrm{PG}(2, \mathrm{GF}(q))$, and let $f(x, y, z) = y^2 - xz$. Then the set

$$\mathcal{C} = \{(x : y : z) \in \mathcal{P} : y^2 = xz\} = \{(t^2 : t : 1) : t \in \mathrm{GF}(q)\} \cup \{(1 : 0 : 0)\}$$

is a conic in $\mathrm{PG}(2, \mathrm{GF}(q))$.

Conics and Ovals in $\mathrm{PG}(2, \mathrm{GF}(q))$

Theorem 16

A conic is an oval in $\mathrm{PG}(2, \mathrm{GF}(q))$.

Theorem 17 (Segre)

An oval in $\mathrm{PG}(2, \mathrm{GF}(q))$ *is a conic if* q *is odd.*

Comment

For q odd, ovals and conics in $\mathrm{PG}(2, \mathrm{GF}(q))$ are the same.

Hyperovals in $\mathrm{PG}(2,\mathrm{GF}(q))$

Definition

A **hyperoval** $\mathcal{H}$ in $\mathrm{PG}(2,\mathrm{GF}(q))$ is a set of $q+2$ points such that no three of them are collinear, i.e., an arc with $q+2$ points.

Example

Let $q=2^m$ with $m \geq 2$. Then

$$\mathcal{H} = \{(t^2 : t : 1) : t \in \mathrm{GF}(q)\} \cup \{(1:0:0) \cup (0:1:0)\}$$

is a hyperoval in $\mathrm{PG}(2,\mathrm{GF}(q))$.

Theorem

Hyperovals in $\mathrm{PG}(2,\mathrm{GF}(q))$ do not exist for odd q.

Hyperovals in $\mathrm{PG}(2,\mathrm{GF}(q))$ and $[q+2,3,q]$ codes

Conclusion

Hyperovals in $\mathrm{PG}(2,\mathrm{GF}(q))$ and $[q+2,3,q]$ MDS codes over $\mathrm{GF}(q)$ are the **same**.

Theorem 18

The weight enumerator of a $[q+2,3,q]$ MDS code over $\mathrm{GF}(q)$ is

$$1+\frac{(q+2)(q^2-1)}{2}z^q+\frac{q(q-1)^2}{2}z^{q+2}.$$

Remarks

- Every line in $\mathrm{PG}(2,\mathrm{GF}(q))$ meets a hyperoval either in 0 point, or 2 points.
- The weight enumerator says that a hyperoval has $(q+2)(q+1)/2$ secants, and $q(q-1)/2$ external lines.
- Orthogonal arrays, 2-class association schemes.

Hyperovals in $\mathrm{PG}(2, \mathrm{GF}(q))$

Remarks: Let $q = 2^m$

- Hyperovals can be constructed from the o-polynomials on $\mathrm{GF}(q)$.
- Hyperovals can be employed to construct 2-$((q-1)q/2, q/2, 1)$ designs.
- Hyperovals can be employed to construct 2-$(q^2-1, \frac{1}{2}q^2-1, \frac{1}{4}q^2-1)$ symmetric designs (Hadamard designs), which can be extended into 3-$(q^2, \frac{1}{2}q^2, \frac{1}{4}q^2-1)$ designs.

Hyperovals and polynomials

The next theorem shows that all hyperovals in $\mathrm{PG}(2, \mathrm{GF}(q))$ can be constructed with a special type of permutation polynomials of $\mathrm{GF}(q)$.

Theorem 19 (Segre)

Let $m \geq 2$. Any hyperoval in $\mathrm{PG}(2, \mathrm{GF}(q))$ can be written in the form

$$\mathcal{H}(f) = \{(f(c) : c : 1) : c \in \mathrm{GF}(q)\} \cup \{(1 : 0 : 0)\} \cup \{(0 : 1 : 0)\},$$

where $f \in \mathrm{GF}(q)[x]$ such that

1. *f is a permutation polynomial of $\mathrm{GF}(q)$ with $\deg(f) < q$ and $f(0) = 0$, $f(1) = 1$;*
2. *for each $a \in \mathrm{GF}(q)$, $g_a(x) = (f(x+a) + f(a))x^{q-2}$ is also a permutation polynomial of $\mathrm{GF}(q)$.*

Conversely, every such set $\mathcal{H}(f)$ is a hyperoval.

O-polynomials

O-polynomial

Polynomials satisfying the two conditions of Theorem 19 are called **o-polynomials**, i.e., oval-polynomials. For example, $f(x) = x^2$ is an o-polynomial over $\mathrm{GF}(q)$ for all $m \geq 2$.

Theorem 20 (Carlet and Msenager)

A polynomial F from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2^n)$ with $F(0) = 0$ is an o-polynomial if and only if $F_u := F(x) + ux$ is 2-to-1 for every $u \in \mathrm{GF}(2^n)^*$.

Carlet and Mesnager discovered a relation between Niho bent functions and o-polynomials.

C. Carlet and S. Mesnager. On Dillons class H of bent functions, Niho bent functions and O-polynomials. In Journal of Combinatorial Theory, Series A, Vol 118, no. 8, p. 2392-2410, 2011.

O-monomials

Two o-polynomials f and g are said to be equivalent if the two hyperovals $\mathcal{H}(f)$ and $\mathcal{H}(g)$ are equivalent. The o-monomials in the following theorem are equivalent.

Theorem 21

Let x^e be an o-polynomial over $\mathrm{GF}(q)$. Then every polynomial in

$$\left\{x^{\frac{1}{e}}, x^{1-e}, x^{\frac{1}{1-e}}, x^{\frac{e}{e-1}}, x^{\frac{e-1}{e}}\right\}$$

is also an o-polynomial, where $1/e$ denotes the multiplicative inverse of e modulo $q-1$.

Maschietti used o-monomials to construct new important difference sets.

Known o-monomials

1. $\mathrm{Trans}_{n,i}(x) = x^{2^i}$, $\gcd(i, n) = 1$.
2. $\mathrm{Segre}_n(x) = x^6$, n odd.
3. $\mathrm{Glynni}_n(x) = x^{3\times 2^{(n+1)/2}+4}$, n odd.
4. $\mathrm{Glynnii}_n(x) = \begin{cases} x^{2^{(n+1)/2}+2^{(3n+1)/4}} & \text{if } n \equiv 1 \pmod 4, \\ x^{2^{(n+1)/2}+2^{(n+1)/4}} & \text{if } n \equiv 3 \pmod 4. \end{cases}$

3-designs from o-monomials

Incidence structures from o-monomials

Let $q = 2^n$ and let x^s be an o-monomial over $\mathrm{GF}(q)$. Let $\mathbb{OV}_{n,s}$ be the incidence structure $(\mathrm{GF}(2^n), \mathrm{GA}_1(q)(OV_{n,s}))$, where

$$OV_{n,s} = \{x^s + x : x \in \mathrm{GF}(2^n)\}.$$

Theorem 22

Let $f(x) = x^s$ be an o-monomial over $\mathrm{GF}(q)$. Then $\mathbb{OV}_{n,s}$ is a 3-design with parameters $(q, q/2, q(q-4)/8\mu)$, where $\mu = \left|\mathrm{GA}_1(q)_{OV_{n,s}}\right|$.

Remarks

To obtain the parameters of the 3-design from the o-monomial x^s, we only need to determine the stabilizer of the base block $OV_{n,s}$. Usually, the stabilizer is trivial.

The proof of $\mathbb{OV}_{n,s}$ being 3-designs

The proof mainly uses the following geometric facts of o-polynomials:

Hyperoval

Suppose that f is an o-polynomial. Let x_1, x_2 and x_3 be three pairwise distinct elements in $\mathrm{GF}(q)$. Then $(f(x_1) : x_1 : 1)$, $(f(x_2) : x_2 : 1)$, and $(f(x_3) : x_3 : 1)$ are three points in the hyperoval $\mathcal{H}(f)$ defined by the o-polynomial $f(x)$, and thus are linearly independent over $\mathrm{GF}(q)$. That means the linear code $\mathcal{C} = \{(af(x) + bx + c)_{x \in \mathrm{GF}(q)} : a, b, c \in \mathrm{GF}(q)\}$ is a MDS code.

C. Ding, C. Tang. Combinatorial t-designs from special polynomials, arXiv: 1903.07375, 2019.

Parameters of the 3-designs from o-monomials

Conjecture 5

Let $q = 2^n$ and let x^s be an o-monomial over $\mathrm{GF}(q)$, where s is not a power of 2. Then

$$\mathrm{GA}_1(q)_{OV_{n,s}} = \{x\}.$$

Consequently, the design $\mathbb{OV}_{n,s}$ has parameters 3-$(q, q/2, q(q-4)/8)$.

Theorem 23

The incidence structure $\mathbb{OV}_{n,s}$ is a 3-$(q, q/2, q(q-4)/8)$ design if $f(x) = \mathrm{Segre}_n(x)$ or $f(x) = \mathrm{Glynnii}_n(x)$.

More generally, let x^s be an o-monomial with $s = 2^i + 2^j$. Then the incidence structure $\mathbb{OV}_{n,s}$ is a 3-$(q, q/2, q(q-4)/8)$ design.

The isomorphy of 3-designs from o-polynomials

We point out that two equivalent o-polynomials may give two non-isomorphic designs. For example, the two o-monomials x^2 and x^{q-2} are equivalent, but $\mathbb{OV}_{n,2}$ and $\mathbb{OV}_{n,q-2}$ are not isomorphic, as $\mathbb{OV}_{n,2}$ is a 3-$(q, q/2, (q-4)/4)$ design and $\mathbb{OV}_{n,q-2}$ is a 3-$(q, q/2, q(q-4)/8)$ design. Hence, the equivalence of o-polynomials is different from the isomorphy of designs $\mathbb{OV}_{n,s}$ from o-polynomials.

The comparison of different constructions

The comparison of different constructions

- In general, it is extremely difficult to analyze the equivalence of t-designs theoretically. We have given an isomorphic classification for the following set of 3-designs from o-polynomials and APN functions for the case $n = 5$ via Magma: $\mathbb{KA}_{5,1}, \mathbb{KA}_{5,2}, \mathbb{AP}_{5,5}, \mathbb{AP}_{5,7}, \mathbb{AP}_{5,13}, \mathbb{OV}_{5,6}, \mathbb{OV}_{5,26}, \mathbb{OV}_{5,28}, \mathbb{OV}_{5,4}, \mathbb{OV}_{5,24}, \mathbb{OV}_{5,8}$. These 3-designs are divided into seven distinct equivalence classes: $\{\mathbb{KA}_{5,1}\}$, $\{\mathbb{KA}_{5,2}\}$, $\{\mathbb{AP}_{5,7}\}$, $\{\mathbb{OV}_{5,24}\}$, $\{\mathbb{OV}_{5,28}\}$, $\{\mathbb{AP}_{5,5},\ \mathbb{OV}_{5,4},\ \mathbb{OV}_{5,8}\}$, $\{\mathbb{AP}_{5,13},\ \mathbb{OV}_{5,6},\ \mathbb{OV}_{5,26}\}$.
- Based on the above discussion, we next propose some conjectures, which have been confirmed by Magma for $n \in \{5, 7\}$.

Conjectures on these 3-designs

Conjecture 6

Let $n \geq 5$ be odd and $i \in \left\{i : 1 \leq i \leq \frac{n-1}{2}, \gcd(i,n) = 1\right\}$. Let $\phi(n)$ denote the Euler's totient function. Then the $\frac{\phi(n)}{2}$ 3-designs $\mathbb{KA}_{n,i}$ are pairwise non-isomorphic. Further, they are not equivalent to any designs $\mathbb{AP}_{n,s}$ from APN power functions, and are slso not equivalent to any designs $\mathbb{OV}_{n,s}$ from o-monomials.

Conjecture 7

Let $n \geq 5$ be odd and $i \in \left\{i : 1 \leq i \leq \frac{n-1}{2}, \gcd(i,n) = 1\right\}$. Then the $\frac{\phi(n)}{2}$ binary linear codes $\mathcal{C}_2(\mathbb{KA}_{n,i})$ are pairwise non-equivalence.

Codes from these 3-designs

- The codes $\mathcal{C}_2(\mathbb{KA}_{5,1})$, $\mathcal{C}_2(\mathbb{KA}_{5,2})$ and $\mathcal{C}_2(\mathbb{KA}_{7,1})$ have parameters $[32, 11, 12]$, $[32, 21, 6]$ and $[128, 15, 56]$, respectively. These codes are optimal. The binary code $\mathcal{C}_2(\mathbb{KA}_{7,2})$ is a self-dual linear code with parameters $[128, 64, 16]$. The examples of codes above demonstrate that it is worthwhile to study 3-designs $\mathbb{KA}_{n,i}$ and their codes $\mathcal{C}_2(\mathbb{KA}_{n,i})$, as these designs may yield optimal linear codes or self-dual binary codes.
- The parameters of the codes from these 3-designs are very flexible. It will also be challenging and interesting to study these codes.

Concluding remarks

Concluding remarks

- Using group actions, infinite families of 3-designs are constructed by employing APN functions and o-polynomials. Some 3-designs give rise to self-dual binary codes or linear codes with optimal or best parameters known. Thus, it is worthwhile to study 3-designs from functions and codes associated with these designs.

Concluding remarks

- Using group actions, infinite families of 3-designs are constructed by employing APN functions and o-polynomials. Some 3-designs give rise to self-dual binary codes or linear codes with optimal or best parameters known. Thus, it is worthwhile to study 3-designs from functions and codes associated with these designs.
- Special functions and polynomials are very useful in the construction of codes and combinatorial structures.

Concluding remarks

- Using group actions, infinite families of 3-designs are constructed by employing APN functions and o-polynomials. Some 3-designs give rise to self-dual binary codes or linear codes with optimal or best parameters known. Thus, it is worthwhile to study 3-designs from functions and codes associated with these designs.
- Special functions and polynomials are very useful in the construction of codes and combinatorial structures.
- Functions, coding theory, combinatorics and finite geometry are very much related. It would be very interesting to investigate their interplay.

Thank you for your attention!!