Links Between Plateaued Functions and Partial Geometric Difference Sets

Oktay Olmez

Department of Mathematics
Ankara University

BFA 2019 (June 16-21, Florence, Italy)

Difference sets: Partial Geometric Difference Sets

- A k-subset D of an abelian group G is a (v, k, λ, n) **difference sets** (DS) if and only if every nonprincipal character χ satisfies $|\chi(D)| = \sqrt{n}$.
- A k-subset R of an abelian group G is an (m, u, k, λ) **semiregular relative difference set** (RDS) if and only if (i) every nonprincipal character χ that is nonprincipal on U satisfies $|\chi(R)| = \sqrt{k}$ and (ii) every nonprincipal character χ that is principal on U satisfies $|\chi(R)| = 0$.
- A k-subset S of an abelian group G is a **partial geometric difference set** in G with parameters $(v, k; \alpha, \beta)$ if and only if $|\chi(S)| = \sqrt{\beta - \alpha}$ or $\chi(S) = 0$ for every non-principal character χ of G.

Combinatorial Designs: Partial Geometric Difference Sets

Let G be a group of order v and let $S \subset G$ be a k-subset. For each $g \in G$, we define

$$\delta(g) := |\{(s,t) \in S \times S \colon g = st^{-1}\}|.$$

Let G be a group of order v. A k-subset S of G is called a partial geometric difference set (PGDS) in G with parameters $(v, k; \alpha, \beta)$ if there exist constants α and β such that, for each $x \in G$,

$$\sum_{y \in S} \delta(xy^{-1}) = \begin{cases} \alpha & \text{if } x \notin S, \\ \beta & \text{if } x \in S \end{cases}$$

If $D \subset G$ is a (v, k, λ)-DS, then D is a $(v, k; k\lambda, k + (k-1)\lambda)$-PGDS in G.

An infinite family of PGDS

- Let s be an integer and C_m be the class of elements of $\mathbb{Z}_2^s$ having exactly m ones as components.
- $S :=$ the set union of classes C_m with $m \equiv 2, 3 \mod 4$.
- if s is odd then $\chi(\mathcal{S})$ is either 0 or $2^{\frac{s-1}{2}}$ for any non-principal character. **Olmez 2014**
- If s is even S is a difference set. **Menon 1960**

Boolean functions from the support sets

$$f(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{otherwise} \end{cases}. \text{ where } S = \cup C_m \text{ and } m \equiv 2 \text{ or } 3 \mod 4$$

$f(x_0, x_1, x_2, x_3) =$
$x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3$
Fourier spectra $= \{\pm 2^2\}$
Bent function:
Fourier spectra $= \{\pm 2^{n/2}\}$

$f(x_0, x_1, x_2, x_3, x_4) =$
$x_0x_1 + x_0x_2 + x_0x_3 + x_0x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$
Fourier spectra $= \{0, \pm 2^3\}$
Plateaued function:
Fourier spectra $= \{0, \pm 2^t\}$ for some integer t

- **(D1974)Having a $(2^s, 2^{s-1} \pm 2^{(s-2)/2}, 2^{s-2} \pm 2^{(s-2)/2}) - DS$ in $\mathbb{Z}_2^s$ is equivalent to having a bent function from $\mathbb{Z}_2^s$ to $\mathbb{Z}_2$.**
  $2-(v,k,\lambda)$-designs:
  $NJ = rJ, \quad JN = kJ \;\; \text{and} \;\; NN^t = (r-\lambda)I + \lambda J$
- **(O2015)The existence of a $(v = 2^s, k; \alpha, \beta) - PGDS$ satisfying $\beta - \alpha = 2^{2t-2}$ for some integer t and $k \in \{2^{s-1}, 2^{s-1} \pm 2^{t-1}\}$ is equivalent to the existence of a plateaued function f with Fourier spectrum of $\{0, \pm 2^t\}$**
  Partial geometric designs:
  $JN = kJ, \quad NJ = rJ \;\; \text{and} \;\; NN^tN = (\beta-\alpha)N + \alpha J$

Another Example

- $D :=$ a Hadamard difference set in
- $S = (D, 0) \bigcup (\mathbb{Z}_2^s \setminus D, 1)$ a subset of $\mathbb{Z}_2^{s+1}$
- $\chi(\mathcal{S}^2)$ is either 0 or 2^s for any non-principal character of $\mathbb{Z}_2^{s+1}$.
- For instance $(16, 6, 2)$-Hadamard difference set yields a partial geometric difference set with parameters $(32, 16; 120, 136)$

$$S = \{(1,1,0,0,0),(1,0,1,0,0),(0,1,1,0,0),(1,1,1,0,0),$$

$$(1,0,0,1,0),(0,1,0,1,0),(1,1,0,1,0),(0,0,1,1,0),$$

$$(1,0,1,1,0),(0,1,1,1,0),(0,0,0,0,1),(1,0,0,0,1),$$

$$(0,1,0,0,1),(0,0,1,0,1),(0,0,0,1,1),(1,1,1,1,1)\}$$

$$f(x_0, x_1, x_2, x_3, x_4) = x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_4$$

Combinatorial designs

Suppose f is a plateaued function with $Spec = \{0, \pm 2^t\}$ for some integer t. Define $F = (-1)^f$ and a matrix $M_f = (m_{x,y})$ where $m_{x,y} = F(x+y)$. Then,

$$(M_f^3)_{x,y} = ((F * F) * F)(x+y).$$

Let $A = (F * F) * F$. Then, the Fourier transform of A is $\widehat{A} = \widehat{F} \cdot \widehat{F} \cdot \widehat{F}$. Now by Fourier inversion

$$A(x+y) = 2^{2t} F(x+y).$$

Hence the equation $M_f^3 = 2^{2t} M_f$ holds.
Incidence matrix of PGD:

$$N = \frac{1}{2}(M_f + J)$$

p-arry bent functions

- $\zeta_p = e^{\frac{2i\pi}{p}}$.
- $f :=$ a function from the field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.
- A function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is called a p-**ary bent** function if every Walsh coefficient has magnitude $p^{\frac{n}{2}}$.
- $$R = \{(x, f(x)) : x \in \mathbb{F}_{p^n}\}$$

  is a (p^n, p, p^n, p^{n-1})-relative difference set in $H = \mathbb{F}_{p^n} \times \mathbb{F}_p$

p-arry bent functions

- $\zeta_p = e^{\frac{2i\pi}{p}}$.
- $f :=$ a function from the field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.
- A function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is called a p-**ary bent** function if every Walsh coefficient has magnitude $p^{\frac{n}{2}}$.
- $$R = \{(x, f(x)) : x \in \mathbb{F}_{p^n}\}$$

  is a (p^n, p, p^n, p^{n-1})-relative difference set in $H = \mathbb{F}_{p^n} \times \mathbb{F}_p$
- Any non-principal character χ of the additive group of $\mathbb{F}_{p^n} \times \mathbb{F}_p$ satisfies $|\chi(R)|^2 = p^n$ or 0. This observation reveals that the relative difference set R is indeed a partial geometric difference set.

Weakly regular bent functions

- weakly regular bent function:= if there exists some function

$$f^* : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$$

  such that $W_f(x) = \nu p^{n/2} \zeta_p^{f^*(x)}$.
- Let f be a bent function from the field $\mathbb{F}_{3^{2s}}$ to $\mathbb{F}_3$ satisfying $f(-x) = f(x)$ and $f(0) = 0$ and

$$D_i = \{x \in \mathbb{F}_{3^{2s}} : f(x) = i\}, \quad i = 0, 1, 2$$

  The sets $D_0 \setminus \{0\}$, D_1 and D_2 are all partial difference sets if and only if f is weakly regular. **Pot et. al. 2010**
- if f is weakly regular bent function from $\mathbb{F}_{3^{2s+1}}$ to $\mathbb{F}_3$ then the sets D_0, D_1 and D_2 are all partial geometric difference sets. **Olmez 2017**

An example from planar functions

- $f(x) = Tr(\gamma P(x))$ from a planar function P and $\gamma \neq 0$.(all mappings $x \mapsto P(x+a) - P(x)$ are bijective for all $a \neq 0$)
- Let $s = 1$ and $f(x) = Tr(x^2)$.

Sets	v	k	α	β
D_0	27	9	24	33
D_1	27	6	6	15
D_2	27	12	60	69
$D_1 \cup D_2$	27	18	210	219
$D_0 \cup D_1$	27	21	336	345
$D_0 \cup D_1$	27	15	120	129

Vectorial functions

- Let F be a vectorial function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. For every $b \in \mathbb{F}_{p^m}^*$, the component function F_b of F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is defined as $F_b(x) = Tr_m(bF(x))$.
- A vectorial function is called *vectorial plateaued* if all its nonzero component functions are plateaued. If the nonzero component functions of a vectorial plateaued function are s-plateaued for the same $0 \leq s \leq n$ then F is called as *s-plateaued*
- The set $G_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}$ is called the graph of F.
- **Çeşmelioğlu and O. 2018** A vectorial function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is s-plateaued if and only if its graph is a $(p^{n+m}, p^n; p^{2n-m} - p^{n+s-m}, p^{n+s} + p^{2n-m} - p^{n+s-m}) - PGDS$.

Vectorial functions: 3-valued autocorrelations

- Let $F(x) = x^d$ be a vectorial function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ with $gcd(d, p^n - 1) = 1$. If the cross-correlation of the p-ary m-sequences that differ by decimation d takes three values, namely $-1, -1 + p^{\frac{n+s}{2}}$ and $-1 - p^{\frac{n+s}{2}}$, then F is a vectorial s-plateaued function. **Çeşmelioğlu and O. 2018**
- Let $n \geq 3$ be an integer and $d = \frac{3^{2k}+1}{2}$ with $\gcd(n, k) = s$ and n/s is odd. For $i = 0, 1, 2$ the sets $D_i = \{x : F(x) = Tr_n(x^d) = i\}$ are $(3^n, 3^{n-1}, 3^{2n-3} - 3^{n-2}, 3^{n-1} + 3^{2n-3} - 3^{n-2})$ partial geometric difference sets in the additive group of $\mathbb{F}_{3^n}$. **Çeşmelioğlu and O. 2018**

Difference Criteria I

$$\delta((x,y)) = |\{((s_1,t_1),(s_2,t_2)) \in G_F \times G_F : \\ x = s_1 - s_2, y = t_1 - t_2 = F(s_1) - F(s_2)\}| \\ = |\{s_2 \in \mathbb{F}_{p^n} : y = F(s_2 + x) - F(s_2)\}|$$

So the criteria for PGDS is given by

$$\sum_{a \in \mathbb{F}_{p^n}} \delta((x-a, y-F(a))) = \begin{cases} \alpha & \text{if } y \neq F(x), \\ \beta & \text{if } y = F(x) \end{cases}$$

and hence

$$\sum_{a \in \mathbb{F}_{p^n}} |\{s \in \mathbb{F}_{p^n} : y = F(s+x-a) - F(s) + F(a)\}| = \begin{cases} \alpha & \text{if } y \neq F(x), \\ \beta & \text{if } y = F(x) \end{cases}$$

Example: Perfect nonlinear

A p-ary function is called perfect nonlinear if

$$|\{s \in \mathbb{F}_{p^n} \colon y = f(s+x) - f(s)\}| = p^{n-1}$$

for all $x \in \mathbb{F}_{p^n}^*$ **Graph of f is a PGDS.**

$$\begin{aligned}
&\sum_{a \in \mathbb{F}_{p^n}} |\{s \in \mathbb{F}_{p^n} \colon y = f(s+x-a) - f(s) + f(a)\}| \\
&\quad = |\{s \in \mathbb{F}_{p^n} \colon y = f(x)\}| \\
&\quad + \sum_{a \in \mathbb{F}_{p^n}, a \neq x} |\{s \in \mathbb{F}_{p^n} \colon y - f(a) = f(s+x-a) - f(s)\}| \\
&\quad = \begin{cases} (p^n - 1)p^{n-1} & \text{if } y \neq f(x), \\ (p^n - 1)p^{n-1} + p^n & \text{if } y = f(x) \end{cases}
\end{aligned}$$

Difference Criteria II

Replace y in the expression

$$y = F(s + x - a) - F(s) + F(a)$$

by $F(x) - c$ for $c \in \mathbb{F}_{p^n}$. Then

$$\begin{aligned}
&\sum_{a \in \mathbb{F}_{p^n}} |\{s \in \mathbb{F}_{p^n} : y = F(s + x - a) - F(s) + F(a)\}| \\
=&|\{(t, a) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} : D_t F(a) - D_t F(x) = c\}| \\
=&N_F(c, x)
\end{aligned}$$

Difference Criteria II

Let F be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Then the set G_F is a PGDS with parameters $(p^{n+m}, p^n; \alpha, \beta)$ if and only if

$$N_F(c, x) = \begin{cases} \alpha, & c \neq 0 \\ \beta, & c = 0 \end{cases}$$

for all $x \in \mathbb{F}_{p^n}$ and some constants α and β.

p-arry s-plateaued functions

- $M = (m_{x,y})$ be a $p^n \times p^n$ matrix where $m_{x,y} = \zeta_p^{f(x+y)}$. Then, f is an s-plateaued function if and only if

$$MM^*M = p^{n+s}M \tag{1}$$

  where M^* is the adjoint of the matrix M. **Ç. and O. 2018**
- A $q^n \times q^n$ Butson-Hadamard matrix M also satisfies

$$MM^*M = q^nM.$$

  Our result implies that M can be associated with $0-$plateaued function.
- **Mesnager et al 2015** f is an s-plateaued function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ if and only if the expression $\sum_{a,b\in\mathbb{F}_{p^n}} \zeta_p^{D_aD_bf(u)}$ does not depend on $u \in \mathbb{F}_{p^n}$. This constant expression equals to p^{n+s}.

Partially bent relative difference sets

Let $G = H \times N$, A be a subgroup of G such that $A \cap N = \{(0,0)\}$, and $B = A \bigoplus N$. Suppose that $|H| = m, |N| = n, |A| = l$. We call a k-subset R of G an (m,n,l,k,λ)-partially bent relative difference set if R_1, R_2, R_3 hold:

R_1 $(x,y) \in G \setminus B$ can be represented in the form $r_1 - r_2$, $r_1, r_2 \in R$ in exactly λ ways, where we put $\lambda = p^{n-1}$.

R_2 $(x,y) \in B \setminus A$ has no representation in the form $r_1 - r_2$, $r_1, r_2 \in R$.

R_3 $(x,y) \in A$ can be represented in the form $r_1 - r_2$, $r_1, r_2 \in R$ in exactly $|R| = k$ ways. **Ç. M. and T. 2014**

Partially bent relative difference sets

- Let f be partially bent with $f(0) = 0$, and Γ be its linear space (dimension s). We consider the sets $A = \{(a, f(a)) : a \in \Gamma\}$ and $B = \{(a, y) : a \in \Gamma, y \in \mathbb{F}_p\}$.
- **Then the graph of s-partially bent functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is a $(p^n, p, p^s, p^n, p^{n-1})$-partially bent relative difference set.**
- Let f be an s-plateaued function with $f(0) = 0$ and linear structure Λ of dimension m. Then the incidence matrix A of the design associated with the partial geometric difference set G_f can be written as a Kronecker product of $1 \times p^m$ all-ones matrix j and an incidence matrix N of a partial geometric design. **Ç. and O. 2018**

THANK YOU
FOR
YOUR
ATTENTION!
ANY QUESTIONS?