Constructions of partial geometric difference sets

Oktay Olmez

Department of Mathematics
Ankara University

New Directions in Combinatorics
May 24, 2016
Singapore

Partial geometric designs

Partial geometric designs

- 1-**designs** :

$$NJ = rJ \quad \text{and} \quad JN = kJ$$

Partial geometric designs

- 1-**designs** :

$$NJ = rJ \text{ and } JN = kJ$$

- $2-(v,k,\lambda)$-**designs** :

$$NJ = rJ, \quad JN = kJ \text{ and } NN^t = (r-\lambda)I + \lambda J$$

Partial geometric designs

- 1-**designs** :

$$NJ = rJ \quad \text{and} \quad JN = kJ$$

- $2-(v, k, \lambda)$-**designs** :

$$NJ = rJ, \quad JN = kJ \quad \text{and} \quad NN^t = (r-\lambda)I + \lambda J$$

- **partial geometric designs** :

$$JN = kJ, \quad NJ = rJ \quad \text{and} \quad NN^tN = (\beta-\alpha)N + \alpha J$$

(**Bose et. al. 1978, Neumaier 1980**)

Partial geometric designs

- $s(x, B) :=$ the number of flags (y, C) such that $y \in B$ and $x \in C$:

$$s(x, B) = \begin{cases} \alpha & \text{if } x \notin B, \\ \beta & \text{if } x \in B, \end{cases} \qquad \forall (x, B) \in P \times \mathcal{B}.$$

Partial geometric designs

- $s(x, B) :=$ the number of flags (y, C) such that $y \in B$ and $x \in C$:

$$s(x, B) = \begin{cases} \alpha & \text{if } x \notin B, \\ \beta & \text{if } x \in B, \end{cases} \qquad \forall (x, B) \in P \times \mathcal{B}.$$

- $\lambda_{x,y} :=$ the number of blocks containing both the points x and y $(\lambda_{x,x} = r)$

$$s(x, B) = \sum_{y \in B} \lambda_{x,y}$$

Partial geometric designs

- $s(x, B)$:= the number of flags (y, C) such that $y \in B$ and $x \in C$:

$$s(x, B) = \begin{cases} \alpha & \text{if } x \notin B, \\ \beta & \text{if } x \in B, \end{cases} \qquad \forall (x, B) \in P \times \mathcal{B}.$$

- $\lambda_{x,y}$:= the number of blocks containing both the points x and y $(\lambda_{x,x} = r)$

$$s(x, B) = \sum_{y \in B} \lambda_{x,y}$$

- For a $2 - (v, k, \lambda)$-design

$$s(x, B) = \begin{cases} k\lambda & \text{if } x \notin B, \\ r + (k-1)\lambda & \text{if } x \in B, \end{cases} \qquad \forall (x, B) \in P \times \mathcal{B}.$$

Directed strongly regular graphs

Directed strongly regular graphs

- A directed strongly regular graph (dsrg) is a (0,1) matrix A with 0's on the diagonal such that the linear span of I, A and J is closed under matrix multiplication.

Directed strongly regular graphs

- A directed strongly regular graph (dsrg) is a (0,1) matrix A with 0's on the diagonal such that the linear span of I, A and J is closed under matrix multiplication.
- Integral parameters v, k, t, λ, μ of a dsrg is defined by:

$$AJ = JA = kJ, \qquad A^2 = tI + \lambda A + \mu(J - I - A).$$

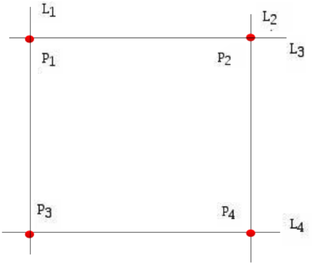
Directed strongly regular graphs

- A directed strongly regular graph (dsrg) is a (0,1) matrix A with 0's on the diagonal such that the linear span of I, A and J is closed under matrix multiplication.
- Integral parameters v, k, t, λ, μ of a dsrg is defined by:

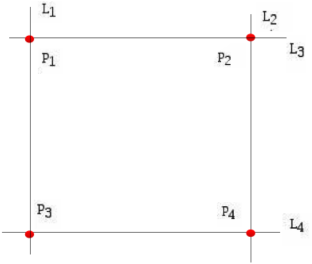
$$AJ = JA = kJ, \qquad A^2 = tI + \lambda A + \mu(J - I - A).$$

- The directed graph with as vertices the flags of this design and with adjacency $(x, B) \to (y, C)$ when the flags are distinct and x is in C is a dsrg with $t = \lambda + 1$. **Brouwer et. al. 2012**
- Similarly, the directed graph with as vertices the antiflags of this design, with the same adjacency, is a dsrg with $t = \mu$. **Brouwer et. al. 2012**

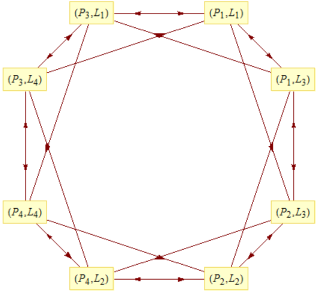
PGD to DSRG



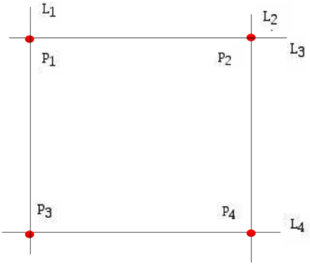
PGD to DSRG



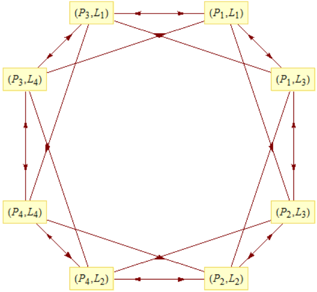
$$(v, k, t, \lambda, \mu) = (8, 3, 2, 1, 1)$$



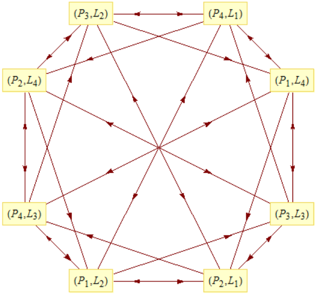
PGD to DSRG



$(v, k, t, \lambda, \mu) = (8, 3, 2, 1, 1)$



$(v, k, t, \lambda, \mu) = (8, 4, 3, 1, 3)$



Partial geometric difference sets

- Let S be a k-subset of a group G.
- $\zeta(g)$:= the number of ordered pairs $(s, t) \in S \times S$ such that $st^{-1} = g$.

Partial geometric difference sets

- Let S be a k-subset of a group G.
- $\zeta(g)$:= the number of ordered pairs $(s, t) \in S \times S$ such that $st^{-1} = g$.
- S is called a **partial geometric difference set** in G with parameters $(v, k; \alpha, \beta)$ if there exist constants α and β such that, for each $x \in G$,

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

$S = \{-1, i, j, k\}$ in $\mathbb{Q}_8$

Example

$$\zeta(i * -i) = 4$$

$$\zeta(i * -1) = 2$$

$$\zeta(i * -j) = 2$$

$$\zeta(i * -k) = 2$$

$$\beta = 4 + 2 + 2 + 2 = 10.$$

$$\zeta(1 * -1) = 0$$

$$\zeta(1 * -i) = 2$$

$$\zeta(1 * -j) = 2$$

$$\zeta(1 * -k) = 2$$

$$\alpha = 0 + 2 + 2 + 2 = 6.$$

	-1	i	j	k
-1	1	i	j	k
i	-i	1	-k	j
j	-j	k	1	-i
k	-k	-j	i	1
1	-1	- i	-j	-k
-i	i	-1	k	-j
-j	j	-k	-1	i
-k	k	j	-i	-1

Some results on partial geometric difference sets

- Development of a partial geometric difference set S is a partial geometric design whose full automorphism group has a subgroup isomorphic to G. **Olmez 2014**
- G acts transitively on the block set and the point set of the design $(G, Dev(S))$. **Olmez 2014**
- S is a partial geometric difference set with parameters $(v, k; \alpha, \beta)$ in G if and only if the equation

$$\mathcal{S}\mathcal{S}^{-1}\mathcal{S} = (\beta - \alpha)\mathcal{S} + \alpha\mathcal{G}$$

  holds in $\mathbb{Z}G$. **Olmez 2014**
- S is a partial geometric difference set in an abelian group 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. **Olmez 2014**

Construction A

- $s :=$ odd integer
- $C_m :=$ the class of elements of $\mathbb{Z}_2^s$ having exactly m ones as components.
- $S :=$ the set union of classes C_m with $m \equiv 0, 1 \mod 4$.
- $\chi(\mathcal{S}^2)$ is either 0 or 2^{s-1} for any non-principal character. **Olmez 2014**

Construction A

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

Construction B

- $D :=$ a Hadamard difference set in $\mathbb{Z}_2^s$.
- $S = (D, 0) \bigcup (\mathbb{Z}_2^s \setminus D, 1)$ a subset of $\mathbb{Z}_2^{s+1}$
- $\chi(\mathcal{S}^2)$ is either 0 or 2^s for any non-principal character of $\mathbb{Z}_2^{s+1}$.

Construction B

- $D :=$ a Hadamard difference set in $\mathbb{Z}_2^s$.
- $S = (D, 0) \bigcup (\mathbb{Z}_2^s \setminus D, 1)$ 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 $(32, 16; 120, 136)$

Boolean Functions

- For a Boolean function f, we can define a function $F := (-1)^f$ from $\mathbb{Z}_2^s$ to the set $\{-1, 1\}$. The Fourier transform of F is defined as follows:

$$\widehat{F}(x) = \sum_{y \in \mathbb{Z}_2^s} (-1)^{x \cdot y} F(y)$$

where $x \cdot y$ is the inner product of two vectors $x, y \in \mathbb{Z}_2^s$.

Bent Functions

- The nonlinearity N_f of f can be expressed as

$$N_f = 2^{s-1} - \frac{1}{2} \max\{|\widehat{F}(x)| : x \in \mathbb{Z}_2^s\}.$$

- A function f is called a **bent** function if $|\widehat{F}(x)| = 2^{s/2}$ for all $x \in \mathbb{Z}_2^s$. A bent function has an optimal nonlinearity.

Bent Functions

- The nonlinearity N_f of f can be expressed as

$$N_f = 2^{s-1} - \frac{1}{2}\max\{|\widehat{F}(x)| : x \in \mathbb{Z}_2^s\}.$$

- A function f is called a **bent** function if $|\widehat{F}(x)| = 2^{s/2}$ for all $x \in \mathbb{Z}_2^s$. A bent function has an optimal nonlinearity.
- Having a difference set with parameters

$$(2^s, 2^{s-1} \pm 2^{(s-2)/2}, 2^{s-2} \pm 2^{(s-2)/2})$$

  in $\mathbb{Z}_2^s$ is equivalent to having a bent function from $\mathbb{Z}_2^s$ to $\mathbb{Z}_2$. **Dillon 1974**

The link between Boolean functions and partial geometric difference sets

- Plateaued functions are introduced as Boolean functions from $\mathbb{Z}_2^s$ to $\mathbb{Z}_2$ which either are bent or have a Fourier spectrum with three values 0 and $\pm 2^t$ for some integer $t \geq \frac{s}{2}$. **Zheng and Zhang 1999**

The link between Boolean functions and partial geometric difference sets

- Plateaued functions are introduced as Boolean functions from $\mathbb{Z}_2^s$ to $\mathbb{Z}_2$ which either are bent or have a Fourier spectrum with three values 0 and $\pm 2^t$ for some integer $t \geq \frac{s}{2}$. **Zheng and Zhang 1999**
- Well-known examples are semibent, nearbent and partially-bent funtions. It is known that these functions provide some suitable candidates that can be used in cryptosystems.

The link between Boolean functions and partial geometric difference sets

- Plateaued functions are introduced as Boolean functions from $\mathbb{Z}_2^s$ to $\mathbb{Z}_2$ which either are bent or have a Fourier spectrum with three values 0 and $\pm 2^t$ for some integer $t \geq \frac{s}{2}$. **Zheng and Zhang 1999**
- Well-known examples are semibent, nearbent and partially-bent funtions. It is known that these functions provide some suitable candidates that can be used in cryptosystems.
- The existence of a partial geometric difference set in $\mathbb{Z}_2^s$ with parameters $(v = 2^s, k; \alpha, \beta)$ 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 $\{0, \pm 2^t\}$. **Olmez 2015**

Construction C

- $s :=$ odd integer
- Replace $\mathbb{Z}_2^s$ by $\mathbb{F}_{2^s}$ and the dot product $x \cdot y$ by the absolute trace function $Tr(xy)$.
- Gold function:

$$g(x) = x^{2^i+1} \quad gcd(i,s) = 1$$

- f(x)=Tr(g(x)) is a plateaued function with Fourier spectrum of $\{0, \pm 2^{\frac{s+1}{2}}\}$. **Gold 1968**

Construction C

- $s :=$ odd integer
- Replace $\mathbb{Z}_2^s$ by $\mathbb{F}_{2^s}$ and the dot product $x \cdot y$ by the absolute trace function $Tr(xy)$.
- Gold function:

$$g(x) = x^{2^i+1} \quad gcd(i, s) = 1$$

- f(x)=Tr(g(x)) is a plateaued function with Fourier spectrum of $\{0, \pm 2^{\frac{s+1}{2}}\}$. **Gold 1968**
- These functions yield partial geometric difference sets with parameters $(v = 2^s, k = 2^{s-1}; \alpha = 2^{2s-3} - 2^{s-2}, \beta = 2^{s-1} + 2^{2s-3} - 2^{s-2})$

p-arry bent functions

- $\zeta_p = e^{\frac{2i\pi}{p}}$.
- f := a function from the field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.
- The Walsh transform of f

$$W_f(\mu) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x)+Tr(\mu x)}, \quad \mu \in \mathbb{F}_{p^n}$$

p-arry bent functions

- $\zeta_p = e^{\frac{2i\pi}{p}}$.
- f := a function from the field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.
- The Walsh transform of f

$$W_f(\mu) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x)+Tr(\mu x)}, \quad \mu \in \mathbb{F}_{p^n}$$

- A function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is called a ***p*-ary bent** function if every Walsh coefficient has magnitude $p^{\frac{n}{2}}$.

p-arry bent functions

- $\zeta_p = e^{\frac{2i\pi}{p}}$.
- f := a function from the field $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.
- The Walsh transform of f

$$W_f(\mu) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x)+Tr(\mu x)}, \quad \mu \in \mathbb{F}_{p^n}$$

- 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 $\mathbb{F}_p$.
- The Walsh transform of f

$$W_f(\mu) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x)+Tr(\mu x)}, \quad \mu \in \mathbb{F}_{p^n}$$

- 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 $W_f(x) = \nu p^{n/2} \zeta_p^{f^*(x)}$.

- $$f(x) = Tr(\alpha x^2)$$

Weakly regular tenrary bent functions

- $f :=$ a bent function from the field $\mathbb{F}_{3^{2s}}$ to $\mathbb{F}_3$ satisfying $f(-x) = f(x)$ and $f(0) = 0$.
- $$D_i = \{x \in \mathbb{F}_{3^{2s}} : f(x) = i\}, \quad i = 0, 1, 2$$
- The sets $D_0 \setminus \{0\}$, D_1 and D_2 are all partial difference sets if and only if f is weakly regular. **Tan et. al. 2010**

Construction D

- $f :=$ a bent function from the field $\mathbb{F}_{3^{2s+1}}$ to $\mathbb{F}_3$ satisfying $f(-x) = f(x)$ and $f(0) = 0$.
- if f is weakly regular the sets D_0, D_1 and D_2 are all partial geometric difference sets. **Olmez 2016**

An example of construction D

An example of construction D

- $f(x) = Tr(\gamma P(x))$ 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 $f(x) = Tr(x^2)$.

An example of construction D

- $f(x) = Tr(\gamma P(x))$ 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

p-ary partially-bent functions

- The derivative of f in the direction of a is defined by

$$D_a f(x) = f(x+a) - f(x).$$

- A function f is called partially-bent if the derivative $D_a f$ is either balanced or constant for any a.

p-ary partially-bent functions

- The derivative of f in the direction of a is defined by

$$D_a f(x) = f(x+a) - f(x).$$

- A function f is called partially-bent if the derivative $D_a f$ is either balanced or constant for any a.
- $a \in \mathbb{F}_{p^n}$ is called a linear structure of f if $D_a f(x)$ is constant.
- $\Gamma_f :=$ the set of linear structures of f.

Construction E

- Let f be a partially bent function with s-dimensional linear subspace Γ_f and $f(0) = 0$.
- $S = \{(x, f(x)) : x \in \mathbb{F}_{p^n}\}$ is a partial geometric difference set in $G = \mathbb{F}_{p^n} \times \mathbb{F}_p$ with parameters $v = p^{n+1}$, $k = p^n$, $\alpha = (p^n - p^s)p^{n-1}$ and $\beta = (p^n - p^s)p^{n-1} + p^{n+s}$.

Construction E

- Let f be a partially bent function with s-dimensional linear subspace Γ_f and $f(0) = 0$.
- $S = \{(x, f(x)) : x \in \mathbb{F}_{p^n}\}$ is a partial geometric difference set in $G = \mathbb{F}_{p^n} \times \mathbb{F}_p$ with parameters $v = p^{n+1}$, $k = p^n$, $\alpha = (p^n - p^s)p^{n-1}$ and $\beta = (p^n - p^s)p^{n-1} + p^{n+s}$.

$A = \{(a, f(a)) : a \in \Gamma_f\}$ and $B = \{(a, y) : a \in \Gamma_f, y \in \mathbb{F}_p\}$.

1. $(x, y) \in G \setminus B$ can be represented in the form $s_1 - s_2$, $s_1, s_2 \in S$ in exactly p^{n-1} ways.
2. $(x, y) \in B \setminus A$ has no representation in the form $s_1 - s_2$, $s_1, s_2 \in S$.
3. $(x, y) \in A$ can be represented in the form $s_1 - s_2$, $s_1, s_2 \in S$ in exactly p^n ways.

THANK YOU FOR YOUR ATTENTION! ANY QUESTIONS?