# Skew Hadamard Difference Sets

Alexander Pott (with Cunsheng Ding and Qi Wang)

Otto-von-Guericke-University Magdeburg

December 06, 2013

# Difference set

Subset $D$ of a group $G$ such that every $g \in G$, $g \neq 0$, has the same number of difference representations $d - d'$ with $d, d' \in D$.

Example

$$\{1, 2, 4\} \subseteq \mathbb{Z}_7.$$

# Construction of difference sets

- Use trivial additive sub-structures, interprete multiplicatively.
- Use trivial multiplicative sub-structures, interprete additively.

# Construction of difference sets

- Use trivial additive sub-structures, interprete multiplicatively.
- Use trivial multiplicative sub-structures, interprete additively.

## Example

- $\mathrm{trace}(x) = 0$ in $\mathbb{F}_{2^n}^*$
- squares in $\mathbb{F}_q$

# How can we generalize trace$(x) = 0$?

- GORDON-MILLS-WELCH (1962): Modify trace

# How can we generalize $\text{trace}(x) = 0$?

- GORDON-MILLS-WELCH (1962): Modify trace

Breakthrough: MASCHIETTI (1998)

$$\{x \in \mathbb{F}_{2^n}^* \ : \ \text{trace}(x) = 0\} = \{y^2 + y \ : \ y \in \mathbb{F}_{2^n}^*, y \neq 1\}$$

Difference set is the image set of $y^2 + y$ in $\mathbb{F}_{2^n}^*$.

# How can we generalize $\mathrm{trace}(x) = 0$?

- GORDON-MILLS-WELCH (1962): Modify trace

Breakthrough: MASCHIETTI (1998)

$$\{x \in \mathbb{F}_{2^n}^* \ : \ \mathrm{trace}(x) = 0\} = \{y^2 + y \ : \ y \in \mathbb{F}_{2^n}^*, y \neq 1\}$$

Difference set is the image set of $y^2 + y$ in $\mathbb{F}_{2^n}^*$.

Generalize this description:

Use 2-to-1 mappings.

# Hyperovals

Maschietti used monomial hyperovals:

$$\left\{ \begin{pmatrix} 1 \\ x \\ x^d \end{pmatrix} \ : \ x \in \mathbb{F}_{2^n} \right\} \cup \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

is a hyperoval in $\mathrm{PG}(2, 2^n)$ if and only if $y^d + y$ is $2$-to-$1$.

# SIDELNIKOV

$$\{x^2 - 1 \ : \ x \in \mathbb{F}_q\} \ \subseteq \ \mathbb{F}_q^*$$

"almost" difference set in $\mathbb{F}_q^*$, yields sequences with optimal autocorrelation properties.

# Generalizing Squares I

Cyclotomy: Unions of cosets of multiplicative subgroup.

Tao Feng, Koji Momihara, Qing Xiang use small subgroups.

# Generalizing Squares II

Squares are image set of a 2-to-1 mapping $f : \mathbb{F}_q \to \mathbb{F}_q$!

But in the additive group.

# Generalizing Squares II

Squares are image set of a 2-to-1 mapping $f : \mathbb{F}_q \to \mathbb{F}_q$!

But in the additive group.

Consider the graph

$$G_f = \{(x, f(x)) \; : \; x \in \mathbb{F}_q\}$$

If $G_f$ has “nice” properties with respect to addition, then perhaps also the image set.

# Planar functions

$f : \mathbb{F}_q \to \mathbb{F}_q$ is planar if $f(x+a) - f(x)$ is a permutation for all $a \neq 0$.

Example

$f(x) = x^2$:

$$(x+a)^2 - x^2 = 2xa + a^2$$

is a permutation on $\mathbb{F}_q$ if $q$ odd.

Hence: Squares are image sets of a class of planar functions!

# Squares in $\mathbb{F}_q$ are nice

The set of squares are a difference set: $d - d' = x$ has $\frac{q-3}{4}$ solutions with $d, d' \in D$ for all $x$,

# Squares in $\mathbb{F}_q$ are nice

The set of squares are a difference set: $d - d' = x$ has $\frac{q-3}{4}$ solutions with $d, d' \in D$ for all $x$, and

$$D \cup (-D) \cup \{0\} = \mathbb{F}_q \qquad (*)$$

# Squares in $\mathbb{F}_q$ are nice

The set of squares are a difference set: $d - d' = x$ has $\frac{q-3}{4}$ solutions with $d, d' \in D$ for all $x$, and

$$D \cup (-D) \cup \{0\} = \mathbb{F}_q \qquad (*)$$

Example ($q = 7$)

$$\{1, 2, 4\} \cup \{3, 5, 6\} \cup \{0\} = \mathbb{F}_7$$

<u>skew</u> Hadamard difference sets

Hadamard difference set: without $(*)$.

# Are there others?

Brilliant idea due to DING and YUAN (2006):

Try other planar functions!

# Are there others?

Brilliant idea due to DING and YUAN (2006):

Try other planar functions!

Exactly one gives new example:

$$f(x) = x^{10} + x^6 - x^2$$

in $\mathbb{F}_{3^n}$ COULTER, MATTHEWS (1998).

# Are there others?

Brilliant idea due to DING and YUAN (2006):

Try other planar functions!

Exactly one gives new example:

$$f(x) = x^{10} + x^6 - x^2$$

in $\mathbb{F}_{3^n}$ COULTER, MATTHEWS (1998).

... still no theoretical proof that it is “new” in general

# ... rekindled interest in planar functions...

DING and YUAN also proved:

$$f(x) = x^{10} - x^6 - x^2$$

is planar and also gives skew Hadamard difference set.

# Another look at Ding-Yuan

composition of a permutation polynomial and $x^2$:

$$(x^5 \pm x^3 - x) \circ x^2$$

DICKSON of order $5$.

# Ding, Wang, Xiang (2007)

$q = 3^{2h+1}$, $\alpha = 3^{h+1}$, $u \in \mathbb{F}_q$

Use permutation polynomial

$$f(x) = x^{2\alpha+3} + (ux)^{\alpha} - u^2 x$$

(which is not planar):

# DING, WANG, XIANG (2007)

$q = 3^{2h+1}$, $\alpha = 3^{h+1}$, $u \in \mathbb{F}_q$

Use permutation polynomial

$$f(x) = x^{2\alpha+3} + (ux)^{\alpha} - u^2 x$$

(which is not planar):

Image set of

$$f \circ x^2$$

is skew Hadamard.

Inequivalence only in small cases proved.

# DING, P., WANG (2013)

$q = 3^m$, $m \not\equiv 0 \bmod 3$, $u \in \mathbb{F}_q$

Use DICKSON of order 7:

$$f(x) = x^7 - ux^5 - u^2x^3 - u^3x.$$

(which is not planar).

Inequivalence only in small cases proved.

# Proof I

Proof resembles Ding, Wang, Xiang.

Have to show $|\Psi(D)|^2 = \frac{3^m+1}{4}$ for additive characters $\Psi$.

Thanks to CHEN, SEHGAL, XIANG (1994), it is sufficient to show:

$$\Psi(D) \equiv \frac{3^{(m-1)/2} - 1}{2} \bmod 3^{(m-1)/2}.$$

# Proof II

Show

$$S_\beta = \sum_{z \in \mathbb{F}_q^*} \Psi_\beta(f(z))\chi(z) \equiv 0 \bmod 3^{(m-1)/2}$$

where $\chi$ is the quadratic character and

$$\Psi_\beta(z) = \zeta_3^{\mathrm{Trace}(\beta z)}.$$

This reduces to

$$\sum_{z \in \mathbb{F}_q^*} \zeta_3^{\mathrm{Trace}(z^7 + \eta z^5 + \gamma z)} \chi(z)$$

for some $\eta$ and $\gamma$.

# Proof III

$$\sum_{z \in \mathbb{F}_q^*} \zeta_3^{\mathrm{Trace}(z^7+\eta z^5+\gamma z)} \chi(z)$$

Use

$$\zeta_3^{\mathrm{Trace}(z)} = \frac{1}{q-1} \sum_{b=0}^{q-2} g(\omega^{-b}) \omega^b(z)$$

where

$$g(\omega^{-b})$$

is Gauss sum with respect to multiplicative character $\omega^{-b}$, where $\omega$ has order $q-1$.

# Proof IV

If $\gamma = 0$, we obtain

$$S_\beta = \pm \frac{1}{q-1} \sum_{b=0}^{q-2} g(\omega^{-b}) g(\omega^{-\frac{q-1}{2}+5^{-1}7b}) \times \text{root of unity}$$

Then use STICKELBERGER and combinatorial arguments.

Case $\gamma \neq 0$ is similar.

# ... use polynomials ...

- to construct more Hadamard difference sets;
- to construct Sidelnikov sequences $x^2 - 1$;
- to construct more skew Hadamard difference sets.

Problem: Show inequivalence!

# Muzychuk (2010)

Mikhail Muzychuk has another construction in $\mathbb{F}_{q^3}$ using orbits of vectors in $\mathbb{F}_q^3$ under the action of $\mathrm{GL}(3, q)$.

# MUZYCHUK (2010)

Mikhail Muzychuk has another construction in $\mathbb{F}_{q^3}$ using orbits of vectors in $\mathbb{F}_q^3$ under the action of $\mathrm{GL}(3, q)$.

He can show inequivalence.

# MUZYCHUK (2010)

Mikhail Muzychuk has another construction in $\mathbb{F}_{q^3}$ using orbits of vectors in $\mathbb{F}_q^3$ under the action of $\mathrm{GL}(3, q)$.

He can show inequivalence.

Inequivalence of some cyclotomic examples and squares has been shown by KOJI MOMIHARA.

# Inequivalence

Difference set corresponds to a design!

- triple intersection numbers;
- rank of incidence matrix;
- automorphism groups.

# Inequivalence

Difference set corresponds to a design!

- triple intersection numbers; MOMIHARA, computer
- rank of incidence matrix;
- automorphism groups.

# Inequivalence

Difference set corresponds to a design!

- triple intersection numbers; MOMIHARA, computer
- rank of incidence matrix; always the same for skew H.d.s
- automorphism groups.

# Inequivalence

Difference set corresponds to a design!

- triple intersection numbers; MOMIHARA, computer
- rank of incidence matrix; always the same for skew H.d.s
- automorphism groups. MUZYCHUK