Image sets with regularity of differences

Robert Coulter

Department of Mathematical Sciences
University of Delaware
Newark, DE 19716 USA
coulter@udel.edu

This is joint work with Patrick Cesarz.

June 2018

Sometimes it pays to be stupid

Sometimes it pays to be stupid

Tor Helleseth, June 13th, 2018

Research motto

Iteration #1: Sometimes it pays to be naive

Research motto

Iteration #2: Sometimes it pays to be naive and stupid

Notational framework

Let G be a group of order v written additively, but not necessarily abelian.
We use 0 to denote the identity in G.
For any $S \subseteq G$, we adopt the following conventions:

- $S^\star$ for the non-zero elements of S.
- $-S$ for the set of all inverses of elements of S.
- If $S \cap -S = \varnothing$, then we say S is *skew*.
- By a "difference in S" we mean $s - t$ where $s, t \in S$.

Sets with regularity of difference?

Definition

Let S, D be two subsets of our group G, and set $|D| = k$, $|S| = s$.

Sets with regularity of difference?

Definition

Let S, D be two subsets of our group G, and set $|D| = k$, $|S| = s$.

- If there exist non-negative integers λ and μ such that every element of $S^\star$ can be written in precisely λ ways as a difference in D while every element of $G^\star \setminus S$ can be written in precisely μ ways as a difference in D, then D is a (v, s, k, λ, μ) *generalised difference set (GDS) related to* S.

Sets with regularity of difference?

Definition

Let S, D be two subsets of our group G, and set $|D| = k$, $|S| = s$.

- If there exist non-negative integers λ and μ such that every element of $S^\star$ can be written in precisely λ ways as a difference in D while every element of $G^\star \setminus S$ can be written in precisely μ ways as a difference in D, then D is a (v, s, k, λ, μ) *generalised difference set (GDS) related to* S.
- If $S = D$, then D is a (v, k, λ, μ) *partial difference set (PDS)*.
- If $S = D$ and $\lambda = \mu$, then D is a (v, k, λ) *difference set (DS)*.

Sets with regularity of difference?

Definition

Let S, D be two subsets of our group G, and set $|D| = k$, $|S| = s$.

- If there exist non-negative integers λ and μ such that every element of $S^\star$ can be written in precisely λ ways as a difference in D while every element of $G^\star \setminus S$ can be written in precisely μ ways as a difference in D, then D is a (v, s, k, λ, μ) *generalised difference set (GDS) related to* S.
- If $S = D$, then D is a (v, k, λ, μ) *partial difference set (PDS)*.
- If $S = D$ and $\lambda = \mu$, then D is a (v, k, λ) *difference set (DS)*.

One point to note immediately about these objects is that if D is any of these objects, then so is the complement $G \setminus D$.

Examples DS and PDS

There are some easy and some not-so-easy examples. It is possible for a multiplicative subgroup of a finite field to form a DS or PDS in the additive group of a finite field.

Examples DS and PDS

There are some easy and some not-so-easy examples. It is possible for a multiplicative subgroup of a finite field to form a DS or PDS in the additive group of a finite field.

- Take the non-zero elements of any subfield of a finite field and you will obtain a PDS.

Examples DS and PDS

There are some easy and some not-so-easy examples. It is possible for a multiplicative subgroup of a finite field to form a DS or PDS in the additive group of a finite field.

- Take the non-zero elements of any subfield of a finite field and you will obtain a PDS. (That was the easy example...)
- Perhaps the most famous examples are those of Paley (1933): let D be the set of all non-zero squares in $\mathbb{F}_q$, q odd.
  - If $q \equiv 1 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS in the additive group of $\mathbb{F}_q$.
  - If $q \equiv 3 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$-DS in the additive group of $\mathbb{F}_q$. In this case, D is necessarily skew.

Examples DS and PDS

There are some easy and some not-so-easy examples. It is possible for a multiplicative subgroup of a finite field to form a DS or PDS in the additive group of a finite field.

- Take the non-zero elements of any subfield of a finite field and you will obtain a PDS. (That was the easy example...)
- Perhaps the most famous examples are those of Paley (1933): let D be the set of all non-zero squares in $\mathbb{F}_q$, q odd.
  - If $q \equiv 1 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS in the additive group of $\mathbb{F}_q$.
  - If $q \equiv 3 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$-DS in the additive group of $\mathbb{F}_q$. In this case, D is necessarily skew.
- There are other such examples, though they are somewhat rare. Lehmer (1953) showed that if D is the set of all non-zero 4th powers in $\mathbb{F}_p$ with p a prime of the form $1 + 4t^2$, t odd, then D is a DS in the additive group of $\mathbb{F}_p$.

Another definition

Definition

A polynomial $f \in \mathbb{F}_q[X]$ is *r-to-1* over $\mathbb{F}_q$ if every non-zero $y \in f(\mathbb{F}_q)$ has precisely r pre-images.

Note that this definition is only concerned about non-zero images.
I don't care about how many roots the polynomial has, only about the regularity on its non-zero images.

More examples

Theorem (Qiu, Wang, Weng, Xiang, 2007)
Let $f \in \mathbb{F}_q[X]$ be a 2-to-1 planar polynomial over $\mathbb{F}_q$ and set $D = f(\mathbb{F}_q) \setminus \{0\}$.

- If $q \equiv 1 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS in the additive group of $\mathbb{F}_q$.
- If $q \equiv 3 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$-DS in the additive group of $\mathbb{F}_q$. In this case, D is necessarily skew.

More examples

Theorem (Qiu, Wang, Weng, Xiang, 2007)
Let $f \in \mathbb{F}_q[X]$ be a 2-to-1 planar polynomial over $\mathbb{F}_q$ and set $D = f(\mathbb{F}_q) \setminus \{0\}$.

- If $q \equiv 1 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS in the additive group of $\mathbb{F}_q$.
- If $q \equiv 3 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$-DS in the additive group of $\mathbb{F}_q$. In this case, D is necessarily skew.

Yes, this should look familiar!
The examples of Paley do fit this criteria: it is easy to prove X^2 is a 2-to-1 planar polynomial over any finite field of odd order.

There are many more examples...

There are many more examples...

Most of us are familiar with bent functions in characteristic 2 being those boolean functions whose supports are non-trivial difference sets in elementary abelian 2-groups – we get $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$-DS in such cases.

And there are many other constructions – perhaps the most spectacular result is that of Muzychuk, who constructed exponentially many inequivalent skew Hadamard difference sets in elementary abelian groups of order q^3.

An initial query on the planar result

Theorem (Qiu, Wang, Weng, Xiang, 2007)
Let $f \in \mathbb{F}_q[X]$ be a 2-to-1 planar polynomial over $\mathbb{F}_q$ and set $D = f(\mathbb{F}_q) \setminus \{0\}$.

- If $q \equiv 1 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS in the additive group of $\mathbb{F}_q$.
- If $q \equiv 3 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$-DS in the additive group of $\mathbb{F}_q$. In this case, D is necessarily skew.

An initial query on the planar result

Theorem (Qiu, Wang, Weng, Xiang, 2007)
Let $f \in \mathbb{F}_q[X]$ be a 2-to-1 planar polynomial over $\mathbb{F}_q$ and set $D = f(\mathbb{F}_q) \setminus \{0\}$.

- If $q \equiv 1 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS in the additive group of $\mathbb{F}_q$.
- If $q \equiv 3 \bmod 4$, then D is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$-DS in the additive group of $\mathbb{F}_q$. In this case, D is necessarily skew.

Question: How close is this relationship between 2-to-1 planar polynomials and image sets of polynomials being DS or PDS?

Initial query and answer

Question: How close is this relationship between 2-to-1 planar polynomials and image sets of polynomials being DS or PDS?

Initial query and answer

Question: How close is this relationship between 2-to-1 planar polynomials and image sets of polynomials being DS or PDS?
Perhaps not that close?

Initial query and answer

Question: How close is this relationship between 2-to-1 planar polynomials and image sets of polynomials being DS or PDS?

Even for monomials we can see an immediate difference.

A necessary condition for X^n to be planar over $\mathbb{F}_q$ is $\gcd(n, q-1) = 2$, but this is not sufficient.
But to generate the Paley PDS/DS examples, $\gcd(n, q-1) = 2$ is a necessary and sufficient condition.

Potential idea?

The relationship between Paley's examples and those of planar functions might not be quite as close as one might like, but the planar examples and those examples coming from a subgroup of a multiplicative group of the finite field do have one common point:

Potential idea?

The relationship between Paley's examples and those of planar functions might not be quite as close as one might like, but the planar examples and those examples coming from a subgroup of a multiplicative group of the finite field do have one common point:

The condition on planar polynomials to construct DS/PDS is that they be 2-to-1, and we then take D to be the non-zero images of the polynomial.

A subgroup of order d in the multiplicative group of $\mathbb{F}_q$ can be written as the set of non-zero images of the polynomial X^k where $q-1=kd$, and what is more, X^k is a k-to-1 polynomial. Again the non-zero images of the monomial are the potential DS/PDS.

Bent functions?

Even the DS coming from bent functions are not too far removed from being described by the image set of a polynomial.

In the single variable representation of a bent function, if you have a polynomial $f \in \mathbb{F}_{2^{2n}}[X]$ for which $Tr(f(x)) = 1$ whenever $f(x) \neq 0$ and $Tr(f(x))$ is a bent function, then the non-zero images of f are precisely those elements of the support of the bent function, i.e. they are the DS.

There is no mention of regularity of images here, but that is not to say that bent function examples wouldn't occur this way.

Basic questions

Basic questions

1. Given a finite field $\mathbb{F}_q$, is there a general form for a polynomial that has t zeros and is r-to-1?

Basic questions

1. Given a finite field $\mathbb{F}_q$, is there a general form for a polynomial that has t zeros and is r-to-1?
2. For such polynomials, when, if ever, is $D = f(\mathbb{F}_q) \setminus \{0\}$ a DS/PDS/GDS? That is, when does the image set of a r-to-1 polynomial exhibit a regularity of differences?

Basic questions

1. Given a finite field $\mathbb{F}_q$, is there a general form for a polynomial that has t zeros and is r-to-1?
2. For such polynomials, when, if ever, is $D = f(\mathbb{F}_q) \setminus \{0\}$ a DS/PDS/GDS? That is, when does the image set of a r-to-1 polynomial exhibit a regularity of differences?
3. More generally, do those polynomials which exhibit a regularity of images often produce image sets that exhibit a regularity of differences?
   Here, by a regularity of images I mean something potentially looser than a r-to-1 polynomial, say a polynomial that has some certain number of zeros, and is r-to-1 on some part of its image set, and s-to-1 on the remainder of its image set – can such f produce image sets which exhibit a regularity of differences?

Basic answers – #1

1. Given a finite field $\mathbb{F}_q$, is there a general form for a polynomial that has t zeros and is r-to-1?

Basic answers – #1

1. Given a finite field $\mathbb{F}_q$, is there a general form for a polynomial that has t zeros and is r-to-1?

The general form of such an $f \in \mathbb{F}_q[X]$ is going to be

$$f(x) = z(X)\, c(X),$$

where $z(X)$ is a degree t polynomial that splits completely over $\mathbb{F}_q$, while $c(X)$ is, in a sense, the controlling polynomial that forces f to be r-to-1.

An obvious first point is that the way in which $c(X)$ controls the images occurring is dependent on the set of roots of $z(X)$.

Basic answers – #1

1. Given a finite field $\mathbb{F}_q$, is there a general form for a polynomial that has t zeros and is r-to-1?

Basic answers – #1

1. Given a finite field $\mathbb{F}_q$, is there a general form for a polynomial that has t zeros and is r-to-1?

We have not investigated this much further.

One initial idea, and one we will use later, is to confine the roots of f to be zero and a subgroup of the multiplicative group, so that

$$z(X) = X^t - X,$$

with $(t-1)|(q-1)$.

Basic answers – #2

2. Can the image set of a r-to-1 polynomial exhibit a regularity of differences?

Basic answers – #2

2. Can the image set of a r-to-1 polynomial exhibit a regularity of differences?

The obvious answer is yes – since the basis of the idea comes from observing certain objects do.

But if we are to make some real progress here, we need to first formulate a simplistic answer to our previous question, and for this reason we chose to either make $z(X) = X$ (only to deal with monomials) or $X^t - X$.

Basic answers – #2; Monomial case

2. Can the image set of a r-to-1 polynomial exhibit a regularity of differences?

Basic answers – #2; Monomial case

2. Can the image set of a r-to-1 polynomial exhibit a regularity of differences?

First let us revisit the monomial case.

We have $f(X) = X^n = X\,X^{n-1}$.

This has been well studied for DS and PDS, with Paley and Lehmer the key early results.

But even here, in the simplest possible object, there is no classification result.

Basic answers – #2; Monomial case

2. Can the image set of a r-to-1 polynomial exhibit a regularity of differences?

First let us revisit the monomial case.

We have $f(X) = X^n = X\,X^{n-1}$.

This has been well studied for DS and PDS, with Paley and Lehmer the key early results.

But even here, in the simplest possible object, there is no classification result.

You can view this as an advance warning that we're probably approaching a difficult problem, and that maybe we can't expect to get a nice working theory to come out of this.

Basic answers – #2; Binomial case

2. Can the image set of a r-to-1 polynomial exhibit a regularity of differences?

Basic answers – #2; Binomial case

2. Can the image set of a r-to-1 polynomial exhibit a regularity of differences?

Next simplest form is the binomial case.

With $f(X) = z(X)c(X)$, and $z(X) = X^t - X$, we set $d = t - 1$ and write

$$f(X) = X^i(X^d - 1), \text{ with } i \geq 1.$$

Basic answers – #2; Binomial case

2. Can the image set of a r-to-1 polynomial exhibit a regularity of differences?

Next simplest form is the binomial case.

With $f(X) = z(X)c(X)$, and $z(X) = X^t - X$, we set $d = t - 1$ and write

$$f(X) = X^i(X^d - 1), \text{ with } i \geq 1.$$

And what now? The only thing for it is to compute and see if there is anything potentially going on here in general.

What we find is, perhaps a little surprisingly, they occur in reasonable numbers.

Some results – $q = 16$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[16,10,6]	1	$\{2, 6, 8, 12\}$	DS	1-to-1 on 8 images, 3-to-1 on rest
	5	$\{1, 3, 4, 6, 7, 9\}$	DS	1-to-1 on non-zero images
[16,12,8,12]	3	{2,4,5,7,8,10}	PDS	$\mathbb{F}_q \setminus \mathbb{F}_4$
[16,9,4,6]	1	{4,10}	PDS	2-to-1 on 6 images, 1-to-1 on rest
[16,5,11,6,8]	1	{3,11}	GDS	
[16,6,7,4,2]	1	7	GDS	

Some results – $q = 16$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[16,10,6]	1	$\{2, 6, 8, 12\}$	DS	1-to-1 on 8 images, 3-to-1 on rest
	5	$\{1, 3, 4, 6, 7, 9\}$	DS	1-to-1 on non-zero images
[16,12,8,12]	3	{2,4,5,7,8,10}	PDS	$\mathbb{F}_q \setminus \mathbb{F}_4$
[16,9,4,6]	1	{4,10}	PDS	2-to-1 on 6 images, 1-to-1 on rest
[16,5,11,6,8]	1	{3,11}	GDS	
[16,6,7,4,2]	1	7	GDS	

Note that these immediately answer Question #3 also – we have polynomials showing a "dual-regularity" on their image sets producing a DS and a PDS.

Some results – $q = 64$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[64,36,20]	9	$\pm\{1, 4, 8, 11, 22, 25\}$ mod 54	DS	1-to-1 and 3-to-1
[64,56,48,56]	7	32 in [2..54]	PDS	$\mathbb{F}_q \setminus \mathbb{F}_8$
[64,42,26,30]	21	$\gcd(i, 63) = 1$	PDS	$[64,21,8,6]^c$
[64,35,18,20]	1	$\{8, 54\}$	PDS	2-to-1 and 1-to-1
[64,27,10,12]	9	$\pm\{2, 10, 16, 17, 23\}$ mod 54	PDS	2-to-1
[64,21,8,6]	7	$\pm\{4, 13, 16, 22, 25, 31\}$ mod 65	PDS	$[64,42,26,30]^c$ 3-to-1 and 2-to-1
[64,14,6,2]	21	$3k$ with $k \not\equiv 1$ mod 3	PDS	3-to-1
[64,21,42,30,26]	3	$\pm\{2, 16, 23\}$ mod 60	GDS	
[64,18,18,2,6]	9	$\pm\{12, 21\}$ mod 54	GDS	

Some results – $q = 256$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[256,240,224,240]	15	many	PDS	$\mathbb{F}_q \setminus \mathbb{F}_{16}$
[256,204,164,156]	51	many	PDS	$[256,51,2,12]^c$
[256,170,114,110]	5	many	PDS	
	85	many	PDS	$[256,85,24,30]^c$
[256,135,70,72]	1	$\{16,238\}$	PDS	
[256,119,54,56]	17	30 in range $2 \leq i \leq 236$	PDS	
[256,85,24,30]	85		PDS	$[256,170,114,110]^c$
[256,68,12,20]	51	26, all of form $3k$	PDS	
[256,51,2,12]	51	many	PDS	$[256,204,164,156]^c$
[256,119,239,222,224]	1	15,239	GDS	
[256,82,238,220,222]	17	30 in range $2 \leq i \leq 236$	GDS	
[256,75,180,132,124]	3	$\pm\{40, 112, 125\}$ mod 252	GDS	
	3	55,197	GDS	
[256,27,48,16,8]	15	$\pm\{20, 50\}$ mod 240	GDS	
	15	$\pm\{40, 115\}$ mod 240	GDS	

Some results – $q = 256$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[256,240,224,240]	15	many	PDS	$\mathbb{F}_q \setminus \mathbb{F}_{16}$
[256,204,164,156]	51	many	PDS	$[256,51,2,12]^c$
[256,170,114,110]	5	many	PDS	
	85	many	PDS	$[256,85,24,30]^c$
[256,135,70,72]	1	$\{16,238\}$	PDS	
[256,119,54,56]	17	30 in range $2 \leq i \leq 236$	PDS	
[256,85,24,30]	85		PDS	$[256,170,114,110]^c$
[256,68,12,20]	51	26, all of form $3k$	PDS	
[256,51,2,12]	51	many	PDS	$[256,204,164,156]^c$
[256,119,239,222,224]	1	15,239	GDS	
[256,82,238,220,222]	17	30 in range $2 \leq i \leq 236$	GDS	
[256,75,180,132,124]	3	$\pm\{40, 112, 125\}$ mod 252	GDS	
	3	55,197	GDS	
[256,27,48,16,8]	15	$\pm\{20, 50\}$ mod 240	GDS	
	15	$\pm\{40, 115\}$ mod 240	GDS	

The two [256,170,114,110] PDS are inequivalent.

This is not just a characteristic two thing

This is not just a characteristic two thing – sorry!

Some results – $q = 3^5 = 243$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[243,121,60]	11	$22k + 12,\ 0 \leq k \leq 9$	DS	D_1
	11	$22k + 21,\ 0 \leq k \leq 9$	DS	$-D_1$
	121	$\gcd(i, 11) = 1$	DS	$\pm D_2 \neq D_1$
[243,220,199,220]	22	many	PDS	
[243,110,37,60]	22	many	PDS	
[243,110,176,125,130]	11	$22k + 2,\ 0 \leq k \leq 10$	GDS	D_3
	11	$22k + 2,\ 0 \leq k \leq 10$	GDS	$D_4 \neq \pm D_3$
[243,110,66,9,25]	22	$22k + 10,\ 0 \leq k \leq 9$	GDS	D_5
	22	$22k + 12,\ 0 \leq k \leq 9$	GDS	$-D_5$

Some results – $q = 3^5 = 243$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[243,121,60]	11	$22k + 12,\ 0 \leq k \leq 9$	DS	D_1
	11	$22k + 21,\ 0 \leq k \leq 9$	DS	$-D_1$
	121	$\gcd(i, 11) = 1$	DS	$\pm D_2 \neq D_1$
[243,220,199,220]	22	many	PDS	
[243,110,37,60]	22	many	PDS	
[243,110,176,125,130]	11	$22k + 2,\ 0 \leq k \leq 10$	GDS	D_3
	11	$22k + 2,\ 0 \leq k \leq 10$	GDS	$D_4 \neq \pm D_3$
[243,110,66,9,25]	22	$22k + 10,\ 0 \leq k \leq 9$	GDS	D_5
	22	$22k + 12,\ 0 \leq k \leq 9$	GDS	$-D_5$

We have equivalent DS and inequivalent DS from this construction.

Some results – $q = 3^5 = 243$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[243,121,60]	11	$22k + 12,\ 0 \leq k \leq 9$	DS	D_1
	11	$22k + 21,\ 0 \leq k \leq 9$	DS	$-D_1$
	121	$\gcd(i, 11) = 1$	DS	$\pm D_2 \neq D_1$
[243,220,199,220]	22	many	PDS	
[243,110,37,60]	22	many	PDS	
[243,110,176,125,130]	11	$22k + 2,\ 0 \leq k \leq 10$	GDS	D_3
	11	$22k + 2,\ 0 \leq k \leq 10$	GDS	$D_4 \neq \pm D_3$
[243,110,66,9,25]	22	$22k + 10,\ 0 \leq k \leq 9$	GDS	D_5
	22	$22k + 12,\ 0 \leq k \leq 9$	GDS	$-D_5$

We have equivalent DS and inequivalent DS from this construction.

This [243,110,37,60] PDS is known, but to my knowledge it is still not known to be part of an infinite family.

Some results – $q = 3^5 = 243$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[243,121,60]	11	$22k + 12,\ 0 \leq k \leq 9$	DS	D_1
	11	$22k + 21,\ 0 \leq k \leq 9$	DS	$-D_1$
	121	$\gcd(i, 11) = 1$	DS	$\pm D_2 \neq D_1$
[243,220,199,220]	22	many	PDS	
[243,110,37,60]	22	many	PDS	
[243,110,176,125,130]	11	$22k + 2,\ 0 \leq k \leq 10$	GDS	D_3
	11	$22k + 2,\ 0 \leq k \leq 10$	GDS	$D_4 \neq \pm D_3$
[243,110,66,9,25]	22	$22k + 10,\ 0 \leq k \leq 9$	GDS	D_5
	22	$22k + 12,\ 0 \leq k \leq 9$	GDS	$-D_5$

We have equivalent DS and inequivalent DS from this construction.

This [243,110,37,60] PDS is known, but to my knowledge it is still not known to be part of an infinite family.

An open parameter for strongly regular graphs is (or was) [243,66,9,21], so this is remarkably close. We, and others, have since proved that it cannot exist in abelian groups, so we can't hope to manipulate this GDS into a PDS of this type.

Some results – $q = 3^6 = 729$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[729,676,625,650]	52	odd & more	PDS	
[729,624,531,552]	104	odd & more	PDS	$[729,104,31,12]^c$
[729,364,181,182]	26	$4k+3,\ k \geq 0$+more	PDS	
	182	$4k+1,\ k \geq 0$+more	PDS	
	364	as for $d = 26$	PDS	
[729,312,135,132]	104	$4k+2$ & more	PDS	
[729,182,55,42]	26	$4k+1$ & more	PDS	
	52	$4k+2$ & more	PDS	
	182	$4k+3$ & more	PDS	
	364	$4k+2$ & more	PDS	
[729,156,45,30]	104	$8k+4$ & more	PDS	
[729,104,31,12]	26	$14k+8$+more	PDS	$[729,624,531,552]^c$
	52	$14k+9$+more	PDS	$[729,624,531,552]^c$
	104		PDS	$[729,624,531,552]^c$
[729,52,25,2]	26	$28k+15$ & more	PDS	
	52	$28k+16$ & more	PDS	
	104	$28k+18$ & more	PDS	
	182	$28k+21$ & more	PDS	
	364	$14k+7$ & more	PDS	
[729,546,364,181,183]	91	$\gcd(8k+2, 91) = 1$	GDS	
	91	$\gcd(8k+3, 91) = 1$	GDS	
[729,702,351,162,351]	26		GDS	
	26		GDS	

Nor is this a small characteristic thing

Some results – $q = 47^2 = 2209$ with $f(X) = X^i(X^d - 1)$

Parameters	d	i	Type	Comments
[2209,1104,551,552]	46,138,1104	many	PDS	two equivalent examples
[2209,1012,465,462]	184	many	PDS	
[2209,920,387,380]	368	many	PDS	
[2209,828,317,306]	552	many	PDS	
[2209,736,255,240]	many	many	PDS	and complements of
[2209,644,201,182]	276	many	PDS	
[2209,552,155,132]	many	many	PDS	and complements of
[2209,460,117,90]	368	many	PDS	
[2209,368,87,56]	many	many	PDS	and complements of
[2209,276,65,30]	many	many	PDS	and complements of
[2209,184,51,12]	many	many	PDS	and complements of
[2209,138,47,6]	many	many	PDS	
[2209,92,45,2]	many	many	PDS	and complements of

With so much data. . . what to do?!

With so much data. . . what to do?!

Our general strategy from here has been to

- Sift through the data and try to identify some infinite families.
- Look to prove any such families theoretically.
- Categorise them against known examples.
- Develop, as much as possible, a general framework which encapsulates the approaches used in establishing any infinite families.

With so much data. . . what to do?!

Our general strategy from here has been to

- Sift through the data and try to identify some infinite families.
- Look to prove any such families theoretically.
- Categorise them against known examples.
- Develop, as much as possible, a general framework which encapsulates the approaches used in establishing any infinite families.

Ideally, we want new infinite families, but at this early stage we're more concerned with showing that the approach can produce infinite families; i.e. that the construction method can actually work.

Established infinite families using this approach

We have so far theoretically established the following infinite families.

Established infinite families using this approach

We have so far theoretically established the following infinite families.

1. Fix $q = 2^n$.
   Set $f(X) = X^2(X^{q-1} - 1) \in \mathbb{F}_{q^2}[X]$.
   f is 2-to-1 and $f(\mathbb{F}_{q^2})^\star$ is a
   $[q^2, \frac{1}{2}(q+1)(q-2), \frac{1}{4}(q+2)(q-1), \frac{1}{4}q(q-2)]$-PDS.

Established infinite families using this approach

We have so far theoretically established the following infinite families.

1. Fix $q = 2^n$.
   Set $f(X) = X^2(X^{q-1} - 1) \in \mathbb{F}_{q^2}[X]$.
   f is 2-to-1 and $f(\mathbb{F}_{q^2})^\star$ is a
   $[q^2, \frac{1}{2}(q+1)(q-2), \frac{1}{4}(q+2)(q-1), \frac{1}{4}q(q-2)]$-PDS.
2. Fix $q = 2^n$ and Tr be the trace mapping from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$.
   Set $f(X) = X(X^q - 1) \in \mathbb{F}_{q^2}[X]$.
   f is 1-to-1 on those images $a \in \mathbb{F}_{q^2}$ for which $Tr(a) = 1$ and 2-to-1 on all other images, and $f(\mathbb{F}_{q^2})^\star$ is a
   $[q^2, \frac{1}{2}(q-1)(q+2), \frac{1}{4}(q-2)(q+1), \frac{1}{4}q(q+2)]$-PDS.

Established infinite families using this approach

We have so far theoretically established the following infinite families.

1. Fix $q = 2^n$.
   Set $f(X) = X^2(X^{q-1} - 1) \in \mathbb{F}_{q^2}[X]$.
   f is 2-to-1 and $f(\mathbb{F}_{q^2})^\star$ is a
   $[q^2, \frac{1}{2}(q+1)(q-2), \frac{1}{4}(q+2)(q-1), \frac{1}{4}q(q-2)]$-PDS.
2. Fix $q = 2^n$ and Tr be the trace mapping from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$.
   Set $f(X) = X(X^q - 1) \in \mathbb{F}_{q^2}[X]$.
   f is 1-to-1 on those images $a \in \mathbb{F}_{q^2}$ for which $Tr(a) = 1$ and 2-to-1 on all other images, and $f(\mathbb{F}_{q^2})^\star$ is a
   $[q^2, \frac{1}{2}(q-1)(q+2), \frac{1}{4}(q-2)(q+1), \frac{1}{4}q(q+2)]$-PDS.
3. Fix q to be any prime power and let $\alpha\beta = q + 1$.
   Set $f(X) = X^\alpha(1 - \alpha\sum_{i=0}^{\beta-1} X^{i\alpha(q-1)}) \in \mathbb{F}_{q^2}[X]$.
   f is α-to-1 and $f(\mathbb{F}_{q^2})^\star$ is a
   $[q^2, (q-1)(\beta-1), q - 3(\beta-1) + (\beta-1)^2, (\beta-1)(\beta-2)]$-PDS.

Comparison against known example

All of the three families established fall into known general examples.

Classes I and II are the complements of Maiorana-McFarland bent functions – this can be shown directly with a little bit of work.

Class III turns out to be connected to orthogonal arrays – details are still to be typed up in full.

Comparison against known example

All of the three families established fall into known general examples.

Classes I and II are the complements of Maiorana-McFarland bent functions – this can be shown directly with a little bit of work.

Class III turns out to be connected to orthogonal arrays – details are still to be typed up in full.

I want to highlight that the methods we've used to establish these are roughly uniform and rely on the regularity of our polynomials to reduce the character theory approach we use.

Initial steps

Proving any of our classes falls into two basic steps.

Initial steps

Proving any of our classes falls into two basic steps.

1. Applying a general theory for counting images of differences using character theory and Gauss sums that uses the regularity of the polynomial.

Initial steps

Proving any of our classes falls into two basic steps.

1. Applying a general theory for counting images of differences using character theory and Gauss sums that uses the regularity of the polynomial.
2. Specialising to the specific polynomial in question. Here you rely on the form of the polynomial, the type of images it produces, and its regularity.

This second step has so far been fairly intensive and as it is case specific, we don't really envisage being able to make this part into a general theory.

Outline of the general theory component

One fact so far hidden in our approach is that we are only looking to construct cyclotomic PDS, which are those that are the union of cosets of some subgroup C of $\mathbb{F}_q^\star$. We rely on this quite a bit in the theory I'm about to outline.

Outline of the general theory component

The main technique we use in order to determine if D is a PDS is to evaluate a particular character sum.

For any $y \in \mathbb{F}_q^\star$, set

$$\lambda_y = |\{(d_1, d_2) : d_1, d_2 \in D \wedge d_1 - d_2 = y\}|.$$

Clearly we wish to count λ_y, for if D is a PDS, then λ_y will only be dependent on whether or not $y \in D$.

Outline of the general theory component

Let q be a power of the prime p and let χ be the canonical additive character on $\mathbb{F}_q$ – that is $\chi(x) = \omega^{Tr(x)}$, where ω is a primitive pth root of unity and Tr is the trace mapping from $\mathbb{F}_q$ into $\mathbb{F}_p$.

Classical character theory techniques give us the following formula for λ_y:

$$\lambda_y = \frac{1}{q} \sum_{t \in \mathbb{F}_q} \chi(ty) \, |\chi(tD)|^2$$

Outline of the general theory component

$$\lambda_y = \frac{1}{q} \sum_{t \in \mathbb{F}_q} \chi(ty) \, |\chi(tD)|^2$$

Now let $C = \langle g^\alpha \rangle$, $\alpha | (q-1)$, a subgroup of the multiplicative group $\mathbb{F}_q^\star = \langle g \rangle$ and let D be a union of cosets of C – so $D = \cup_{a \in I} aC$ for some $I \subset \mathbb{F}_q$.

Setting $X_i = \chi(g^i C)$ and $Y_i = \chi(g^i D)$ (note these are still character sums!) we can rewrite this equation (after some work!) to

$$q\lambda_y - k^2 = \sum_{i=0}^{\alpha-1} |Y_i|^2 X_{m+i},$$

where $|D| = k$ and where $y \in g^m C$.

Outline of the general theory component

So, with $X_i = \chi(g^i C)$ and $Y_i = \chi(g^i D)$, and with $|D| = k$ and $y \in g^m C$, we have

$$q\lambda_y - k^2 = \sum_{i=0}^{\alpha-1} |Y_i|^2 X_{m+i}.$$

Note that the formula is only dependent on which coset of C the element y lies in, and this greatly reduces the calculations necessary for testing if D is a PDS.

However, we still need to calculate X_i and Y_i, and it is in computing these that different classes require drastically different methods.

Also, at this point, we've not seen anything about the regularity of the polynomial (or indeed any polynomial!) being utilised.

The impact of the polynomial's regularity

Say our potential PDS D is also the non-zero image set of a polynomial $f \in \mathbb{F}_q[X]$ which has z zeros and is r-to-1.

Then we have $k = |D| = (q - z)/r$.

Setting $S_t(f) = \sum_{x \in \mathbb{F}_q} \chi(tf(x))$, we have the identity

$$\chi(tD) = \frac{1}{r}\left(S_t(f) - z\right).$$

Thus, calculating all of the Y_i in our equation on λ_y is directly related to calculating absolute values of Weil sums related to our polynomial f.

This impact is fairly significant, as now much of our problem is reduced to calculating these Weil sums for (presumably!) nicely behaving polynomials.

From the general framework to specifics

At this stage, individual cases take different paths.

How the polynomial behaves, its shape, any additional structure about its image set, all of these and more can impact the remaining parts of the proof.

The essential tasks are to compute the partial sums X_i and Y_i, and also to understand the interaction of the Y_i term with X_{m+i} term for elements in the $g^m C$ coset – it is not enough to be able to evaluate each of X_i and Y_i separately; we need to know how they evaluate together.

From the general framework to specifics

At this stage, individual cases take different paths.

How the polynomial behaves, its shape, any additional structure about its image set, all of these and more can impact the remaining parts of the proof.

The essential tasks are to compute the partial sums X_i and Y_i, and also to understand the interaction of the Y_i term with X_{m+i} term for elements in the $g^m C$ coset – it is not enough to be able to evaluate each of X_i and Y_i separately; we need to know how they evaluate together.

Patrick likes to describe the completion of these remaining difficulties as "a matter of using linear functionals and double-counting arguments".

From the general framework to specifics

At this stage, individual cases take different paths.

How the polynomial behaves, its shape, any additional structure about its image set, all of these and more can impact the remaining parts of the proof.

The essential tasks are to compute the partial sums X_i and Y_i, and also to understand the interaction of the Y_i term with X_{m+i} term for elements in the $g^m C$ coset – it is not enough to be able to evaluate each of X_i and Y_i separately; we need to know how they evaluate together.

Patrick likes to describe the completion of these remaining difficulties as "a matter of using linear functionals and double-counting arguments".

I'm just going to say that "it is easy to see" and let you fill in the gaps.

Future work

Future work – short version

Lots to do!

Future work

The search data is just the tip of the iceberg, and already we have enormous numbers of examples.

In the smaller orders, we can categorise (with some guess work) many of the DS and PDS we're finding against known examples.

However, as we get into slightly larger orders, or larger degree extensions, the number of examples explodes and then things become much less clear.

Additionally, we have situations where we get inequivalent DS with the same parameters. We have not yet tackled these cases theoretically.

Future work

All of the computational data we have so far is only for binomials.

We have not yet even begun to look at more general forms of polynomial.

To reasonably extend the search, however, we would need to have a much better understanding of how to construct r-to-1 polynomials with z roots.

I think this is probably hard.

Future work

Most of our efforts so far have been directed at establishing infinite classes of PDS as a "proof of concept" type thing.

However, we also have what we believe is an infinite class of new GDS, but we're still trying to complete a proof for them.

Indeed, the data we have so far contains many examples of GDS, and most of them I suspect to be new.

With all of the computational side of this its clear that presently we have way too many questions and way too few answers.

Future work

There is also the not-so-small matter of finding a better general theory.

I think it is fairly clear that there is no hope of having an all-encompassing theory here, but I still hope that there is at least some main theory that will cover some reasonably large set of examples of DS/PDS/GDS.

Additionally, the classification of the monomial examples remains, and this is a problem dating back at least 60 years now.

There are a lot more problems I could list here
but I think that's enough for today.

There are a lot more problems I could list here
but I think that's enough for today.

You probably do too!

Thanks for listening.