Partial difference sets in nonabelian groups

Eric Swartz
(joint with Jim Davis, John Polhill, Ken Smith)

William & Mary

November 1, 2023

Definition

The groups, graphs, etc., considered in this talk will be finite.

Definition

The groups, graphs, etc., considered in this talk will be finite.

Definition

A subset S of elements of a group G is a (v, k, λ, μ)-*partial difference set* (**PDS**)

Definition

The groups, graphs, etc., considered in this talk will be finite.

Definition

A subset S of elements of a group G is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,

Definition

The groups, graphs, etc., considered in this talk will be finite.

Definition

A subset S of elements of a group G is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,
- $|S| = k$,

Definition

The groups, graphs, etc., considered in this talk will be finite.

Definition

A subset S of elements of a group G is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,
- $|S| = k$,
- if $1 \neq g \in G$ and $g \in S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly λ different ways, and

Definition

The groups, graphs, etc., considered in this talk will be finite.

Definition

A subset S of elements of a group G is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,
- $|S| = k$,
- if $1 \neq g \in G$ and $g \in S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly λ different ways, and
- if $1 \neq g \in G$ and $g \notin S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly μ different ways.

Definition

The groups, graphs, etc., considered in this talk will be finite.

Definition

A subset S of elements of a group G is a (v, k, λ, μ)-*partial difference set* (**PDS**) if

- $|G| = v$,
- $|S| = k$,
- if $1 \neq g \in G$ and $g \in S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly λ different ways, and $a-b$
- if $1 \neq g \in G$ and $g \notin S$, then g can be written as the product ab^{-1}, where $a, b \in S$, exactly μ different ways. $a-b$

Why partial *difference* set? Originally interest was in abelian groups, and the operation was addition.

Small example

Example

- G: $\mathbb{Z}/13\mathbb{Z}$, operation $+$
- $S = \{1, 3, 4, 9, 10, 12\}$

Small example

Example

- G: $\mathbb{Z}/13\mathbb{Z}$, operation $+$
- $S = \{1, 3, 4, 9, 10, 12\}$

For elements in S:

- $1 = 4 - 3 = 10 - 9$
- $3 = 4 - 1 = 12 - 9$
- $4 = 3 - 12 = 1 - 10$
- $9 = 12 - 3 = 10 - 1$
- $10 = 1 - 4 = 9 - 12$
- $12 = 3 - 4 = 9 - 10$

Small example

Example

- G: $\mathbb{Z}/13\mathbb{Z}$, operation $+$
- $S = \{1, 3, 4, 9, 10, 12\}$

For nonidentity elements not in S:

- $2 = 3 - 1 = 12 - 10 = 1 - 12$
- $5 = 9 - 4 = 1 - 9 = 4 - 12$
- $6 = 9 - 3 = 10 - 4 = 3 - 10$
- $7 = 3 - 9 = 4 - 10 = 10 - 3$
- $8 = 4 - 9 = 9 - 1 = 12 - 4$
- $11 = 1 - 3 = 10 - 12 = 12 - 1$

Small example

Example

- G: $\mathbb{Z}/13\mathbb{Z}$, operation $+$
- $S = \{1, 3, 4, 9, 10, 12\}$

For nonidentity elements not in S:

- $2 = 3 - 1 = 12 - 10 = 1 - 12$
- $5 = 9 - 4 = 1 - 9 = 4 - 12$
- $6 = 9 - 3 = 10 - 4 = 3 - 10$
- $7 = 3 - 9 = 4 - 10 = 10 - 3$
- $8 = 4 - 9 = 9 - 1 = 12 - 4$
- $11 = 1 - 3 = 10 - 12 = 12 - 1$

S is a $(13, 6, 2, 3)$-PDS.

Small example, continued

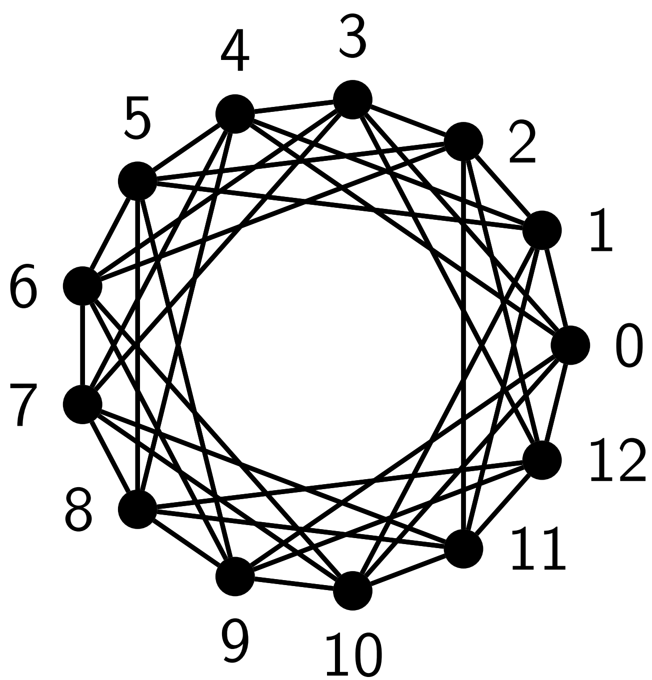
Example

- G: $\mathbb{Z}/13\mathbb{Z}$, operation $+$
- $S = \{1, 3, 4, 9, 10, 12\}$
- S is a $(13, 6, 2, 3)$-PDS with $0 \notin S$, $S = -S$
- $\mathrm{Cay}(G, S)$: undirected $(13, 6, 2, 3)$-strongly regular Cayley graph.

S: nonzero squares mod 13

$1 = 1^2$, $3 = 16 = 4^2$, $4 = 2^2$, $9 = 3^2$,

$10 = 36 = 6^2$, $12 = 25 = 5^2$



Paley's Theorem

In fact, the last example generalizes:

Theorem (Paley 1933)

- *q: odd prime power*
- $q \equiv 1 \pmod 4$
- *G: the additive group of a finite field* $\mathrm{GF}(q)$
- *S: set of all nonzero squares in* $\mathrm{GF}(q)$

Then, S is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS in G.

if q is prime

$\mathrm{GF}(q) = \mathbb{Z}/q\mathbb{Z}$

Equivalent concepts

Definition

A (v, k, λ, μ)-PDS is called *regular* if $1 \notin S$ and $S = S^{-1}$.

Equivalent concepts

Definition

A (v, k, λ, μ)-PDS is called *regular* if $1 \notin S$ and $S = S^{-1}$.

Proposition

G: finite group

S: regular (v, k, λ, μ)-PDS $\Leftrightarrow \mathrm{Cay}(G, S)$: (v, k, λ, μ)-SRG.

Equivalent concepts

Definition

A (v, k, λ, μ)-PDS is called *regular* if $1 \notin S$ and $S = S^{-1}$.

Proposition

G: finite group

S: regular (v, k, λ, μ)-PDS $\Leftrightarrow \mathrm{Cay}(G, S)$: (v, k, λ, μ)-SRG.

SO: regular (v, k, λ, μ)-PDS in $G \leftrightarrow G$ acts transitively, fixed-point-freely on vertices of (v, k, λ, μ)-SRG

What's known?

- Extensive knowledge for abelian groups (see Ma's survey (1994))
- Very few known for nonabelian groups!

What's known?

- Extensive knowledge for abelian groups (see Ma's survey (1994))
- Very few known for nonabelian groups!
- **Smith (1995):** regular $(4t^2, 2t^2 - t, t^2 - t, t^2 - t)$-PDSs in certain nonabelian groups
- **Kantor (1986), Ghinelli (2012):** regular $(q^3, q^2 + q - 2, q - 2, q + 2)$-PDS in Heisenberg group of order q^3 (q odd prime power)
- **S. (2015):** regular $(p^3, p^2 + p - 2, p - 2, p + 2)$-PDS S of extraspecial group of order p^3, exponent p^2 (p odd)
- **Feng, He, Chen (2020):** PDSs of exponent 4, 8, and 16 and of nilpotency class 2, 3, 4, and 6
- **Feng, Li (2021):** same graphs as Kantor/Ghinelli considered, but *many* groups!

Example: Set up

- $V = \mathbb{Z}/3\mathbb{Z}^4$, the 4-dimensional vector space over $\mathbb{Z}/3\mathbb{Z}$
- $|V| = 81$

Example: Set up

- $V = \mathbb{Z}/3\mathbb{Z}^4$, the 4-dimensional vector space over $\mathbb{Z}/3\mathbb{Z}$
- $|V| = 81$
- For $x = (x_1, x_2, x_3, x_4) \in V$, define

$$Q(x) = x_1x_2 + x_3x_4$$

Example: Set up

- $V = \mathbb{Z}/3\mathbb{Z}^4$, the 4-dimensional vector space over $\mathbb{Z}/3\mathbb{Z}$
- $|V| = 81$
- For $x = (x_1, x_2, x_3, x_4) \in V$, define

$$Q(x) = x_1x_2 + x_3x_4$$

For any $x, y \in V$, there are three options:

(1) $Q(x - y) = 0$

(2) $Q(x - y)$ is a nonzero square: $Q(x - y) = 1$

(3) $Q(x - y)$ is a nonsquare: $Q(x - y) = 2$

Three graphs

For each graph: vertices are $V = \mathbb{Z}/3\mathbb{Z}^4$

- Γ_0: $x \sim y \iff Q(x-y) = 0$
- Γ_0 is an $(81, 32, 13, 12)$-SRG

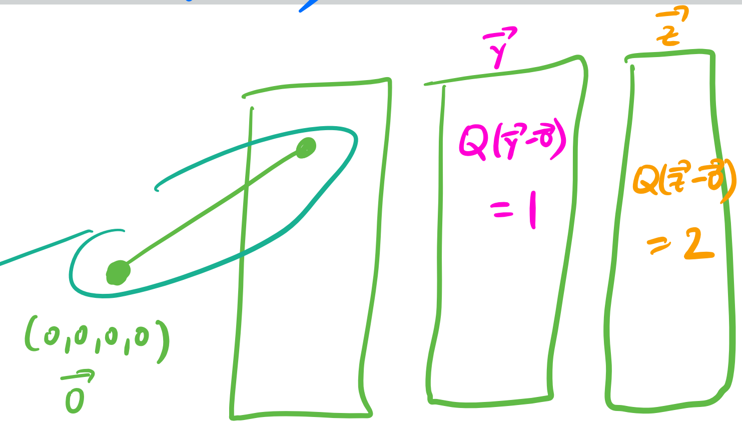
Three graphs

For each graph: vertices are $V = \mathbb{Z}/3\mathbb{Z}^4$

- Γ_0: $x \sim y \iff Q(x-y) = 0$
- Γ_0 is an $(81, 32, 13, 12)$-SRG

- Γ_1: $x \sim y \iff Q(x-y) = 1$ (nonzero square)
- Γ_1 is an $(81, 24, 9, 6)$-SRG

Three graphs (Affine Polar Graphs)



For each graph: vertices are $V = \mathbb{Z}/3\mathbb{Z}^4$

$\vec{x} \in$, then $Q(\vec{x}-0)=0$

$\vec{x}=(1,0,0,0)$

- Γ_0: $x \sim y \iff Q(x-y) = 0$
- Γ_0 is an $(81, 32, 13, 12)$-SRG

- Γ_1: $x \sim y \iff Q(x-y) = 1$ (nonzero square)
- Γ_1 is an $(81, 24, 9, 6)$-SRG

$\Gamma_1 \cong \Gamma_2$

- Γ_2: $x \sim y \iff Q(x-y) = 2$ (nonsquare)
- Γ_2 is an $(81, 24, 9, 6)$-SRG

Automorphisms

$g(x)$ $g(y)$

- **RECALL:** an automorphism g is a bijection of vertices such that $x^g \sim y^g \iff x \sim y$
- Here, this amounts to ensuring $Q(x^g - y^g) = Q(x - y)$

Automorphisms

- **RECALL:** an automorphism g is a bijection of vertices such that $x^g \sim y^g \iff x \sim y$
- Here, this amounts to ensuring $Q(x^g - y^g) = Q(x - y)$

- Translations!
- For $v \in V$, define T_v by $T_v : x \mapsto x + v$
- $Q(x^{T_v} - y^{T_v}) = Q((x + v) - (y + v)) = Q(x - y)$
- $T_V := \{T_v : v \in V\}$: transitive, fixed-point-free... $\underbrace{\text{but } \textit{very} \text{ abelian!}}$

$T_v T_u = T_{v+u} = T_u T_v$

Other automorphisms

- Matrices!
- Suppose $M \in \mathrm{GL}(4,3)$, $Q(vM) = Q(v)$.
- $Q(xM - yM) = Q((x-y)M) = Q(x-y)$
- Automorphism of each graph!

Other automorphisms

- Matrices!
- Suppose $M \in \mathrm{GL}(4,3)$, $Q(vM) = Q(v)$.
- $Q(xM - yM) = Q((x-y)M) = Q(x-y)$
- Automorphism of each graph!

what I translate by

- Combine the two: $M \in \mathrm{GL}(4,3)$, M preserves Q; $v \in V$
- $x^{[M,v]} := xM + v$
- $Q(x^{[M,v]} - y^{[M,v]}) = Q((xM+v) - (yM+v)) = Q(x-y)$
- $x^{[M,v]} \sim y^{[M,v]} \iff x \sim y$

$= Q((x-y)M)$

Other automorphisms

- Matrices!
- Suppose $M \in \mathrm{GL}(4,3)$, $Q(vM) = Q(v)$.
- $Q(xM - yM) = Q((x-y)M) = Q(x-y)$
- Automorphism of each graph!

- Combine the two: $M \in \mathrm{GL}(4,3)$, M preserves Q; $v \in V$
- $x^{[M,v]} := xM + v$
- $Q(x^{[M,v]} - y^{[M,v]}) = Q((xM+v) - (yM+v)) = Q(x-y)$
- $x^{[M,v]} \sim y^{[M,v]} \iff x \sim y$

- **Composition:** $[M_1, v_1][M_2, v_2] = [M_1 M_2, v_1 M_2 + v_2]$

$$\left(x^{[M_1, v_1]}\right)^{[M_2, v_2]} = (xM_1 + v_1)^{[M_2, v_2]} = xM_1M_2 + v_1M_2 + v_2 = x^{[M_1M_2,\, v_1M_2 + v_2]}$$

Example

- For $\alpha \in \mathbb{Z}/3\mathbb{Z}$, define

$$A_\alpha := \begin{pmatrix} 1 & 0 & 0 & \alpha \\ 0 & 1 & 0 & -\alpha \\ \alpha & -\alpha & 1 & \alpha^2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

- $x = (x_1, x_2, x_3, x_4)$
- $Q(x) = x_1x_2 + x_3x_4$

Example

- For $\alpha \in \mathbb{Z}/3\mathbb{Z}$, define

$$A_\alpha := \begin{pmatrix} 1 & 0 & 0 & \alpha \\ 0 & 1 & 0 & -\alpha \\ \alpha & -\alpha & 1 & \alpha^2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

- $x = (x_1, x_2, x_3, x_4)$
- $Q(x) = x_1x_2 + x_3x_4$
- $xA_\alpha = (x_1 + \alpha x_3, x_2 - \alpha x_3, x_3, \alpha x_1 - \alpha x_2 + \alpha^2 x_3 + x_4)$
-

$$\begin{aligned} Q(xA_\alpha) &= (x_1 + \alpha x_3)(x_2 - \alpha x_3) + x_3(\alpha x_1 - \alpha x_2 + \alpha^2 x_3 + x_4) \\ &= x_1x_2 - \alpha x_1x_3 + \alpha x_2x_3 - \alpha^2 x_3 \\ &\quad + \alpha x_1x_3 - \alpha x_2x_3 + \alpha^2 x_3 + x_3x_4 \\ &= x_1x_2 + x_3x_4 \\ &= Q(x) \end{aligned}$$

Example, cont.

- $A_0 = I$, $A_\alpha A_\beta = A_{\alpha+\beta}$
- $A_2 = A_1^2$, $A_0 = A_1^3$

Example, cont.

- $A_0 = I$, $A_\alpha A_\beta = A_{\alpha+\beta}$
- $A_2 = A_1^2$, $A_0 = A_1^3$

- Standard basis: e_1, e_2, e_3, e_4
- $v := e_1 + e_2 = (1,1,0,0)$
- $vA_1 = (1,1,0,0)\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & -1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = (1,1,0,0) = v$
- if $u \in \langle e_1 - e_2, e_3, e_4 \rangle = U$, then $uA_1 \in U$
- $\{A_0, A_1, A_2 = A_1^2\}$ stabilize decomposition $V = \langle v \rangle \oplus \langle e_1 - e_2, e_3, e_4 \rangle$

The group

- $T_U := \{[I, u] : u \in U = \langle e_1 - e_2, e_3, e_4 \rangle\}$

Translations by things in U

- $\mathcal{A} := \{[A_\alpha, \alpha v] : \alpha \in \mathbb{Z}/3\mathbb{Z}\}$, where $v = (1, 1, 0, 0)$
- $G := \langle T_U, \mathcal{A} \rangle$

The group

- $T_U := \{[I, u] : u \in U = \langle e_1 - e_2, e_3, e_4 \rangle\}$
- $\mathcal{A} := \{[A_\alpha, \alpha v] : \alpha \in \mathbb{Z}/3\mathbb{Z}\}$, where $v = (1, 1, 0, 0)$
- $G := \langle T_U, \mathcal{A} \rangle$

- $x^{[I, e_3][A_1, v]} = (x + e_3)^{[A_1, v]} = (x + e_3)A_1 + v =$
  $xA_1 + ((e_1 - e_2) + e_3 + e_4) + v$

The group

- $T_U := \{[I, u] : u \in U = \langle e_1 - e_2, e_3, e_4\rangle\}$
- $\mathcal{A} := \{[A_\alpha, \alpha v] : \alpha \in \mathbb{Z}/3\mathbb{Z}\}$, where $v = (1, 1, 0, 0)$
- $G := \langle T_U, \mathcal{A}\rangle$

- $x^{[I,e_3][A_1,v]} = (x + e_3)^{[A_1,v]} = (x + e_3)A_1 + v =$ $xA_1 + ((e_1 - e_2) + e_3 + e_4) + v$
- $x^{[A_1,v][I,e_3]} = (xA_1 + v)^{[I,e_3]} = xA_1 + e_3 + v$
- Nonabelian!

The group

- $T_U := \{[I, u] : u \in U = \langle e_1 - e_2, e_3, e_4 \rangle\}$
- $\mathcal{A} := \{[A_\alpha, \alpha v] : \alpha \in \mathbb{Z}/3\mathbb{Z}\}$, where $v = (1, 1, 0, 0)$
- $G := \langle T_U, \mathcal{A} \rangle$

- $x^{[I,e_3][A_1,v]} = (x + e_3)^{[A_1,v]} = (x + e_3)A_1 + v = xA_1 + ((e_1 - e_2) + e_3 + e_4) + v$
- $x^{[A_1,v][I,e_3]} = (xA_1 + v)^{[I,e_3]} = xA_1 + e_3 + v$
- Nonabelian!

- In fact, for $u \in \langle e_1 - e_2, e_3, e_4 \rangle$,

$$[I, u][A_\alpha, \cancel{\alpha} v] = [A_\alpha, \cancel{\alpha} v][I, uA_\alpha]$$

The group

- $T_U := \{[I, u] : u \in U = \langle e_1 - e_2, e_3, e_4 \rangle\}$
- $\mathcal{A} := \{[A_\alpha, \alpha v] : \alpha \in \mathbb{Z}/3\mathbb{Z}\}$, where $v = (1, 1, 0, 0)$
- $G := \langle T_U, \mathcal{A} \rangle$

- $x^{[I,e_3][A_1,v]} = (x + e_3)^{[A_1,v]} = (x + e_3)A_1 + v = xA_1 + ((e_1 - e_2) + e_3 + e_4) + v$
- $x^{[A_1,v][I,e_3]} = (xA_1 + v)^{[I,e_3]} = xA_1 + e_3 + v$
- Nonabelian!

- In fact, for $u \in \langle e_1 - e_2, e_3, e_4 \rangle$,

$$[I, u][A_\alpha, \alpha v] = [A_\alpha, \alpha v][I, uA_\alpha]$$

$$\underbrace{[A_\alpha, \alpha v]}_{3 \text{ choices}}\ \underbrace{[I, u]}_{|U| = 3^3 = 27}$$

- $|G| = 81$

The group, cont.

- $T_U := \{[I, u] : u \in U = \langle e_1 - e_2, e_3, e_4 \rangle\}$
- $\mathcal{A} := \{[A_\alpha, v] : \alpha \in \mathbb{Z}/3\mathbb{Z}\}$, where $v = (1, 1, 0, 0)$
- $G := \langle T_U, \mathcal{A} \rangle$

The group, cont.

- $T_U := \{[I, u] : u \in U = \langle e_1 - e_2, e_3, e_4 \rangle\}$
- $\mathcal{A} := \{[A_\alpha, v] : \alpha \in \mathbb{Z}/3\mathbb{Z}\}$, where $v = (1, 1, 0, 0)$
- $G := \langle T_U, \mathcal{A} \rangle$

$V = \langle v \rangle \oplus U$

- Let $x \in V$. $x = \alpha v + u$, $\alpha \in \mathbb{Z}/3\mathbb{Z}$. $u \in U$
- unique $[M, w] \in G$ with $w = x$:

$$[A_\alpha, \alpha v][I, u] = [A_\alpha, \alpha v + u] = [A_\alpha, x]$$

The group, cont.

- $T_U := \{[I, u] : u \in U = \langle e_1 - e_2, e_3, e_4 \rangle\}$
- $\mathcal{A} := \{[A_\alpha, v] : \alpha \in \mathbb{Z}/3\mathbb{Z}\}$, where $v = (1, 1, 0, 0)$
- $G := \langle T_U, \mathcal{A} \rangle$

- Let $x \in V$. $x = \alpha v + u$, $\alpha \in \mathbb{Z}/3\mathbb{Z}$. $u \in U$
- unique $[M, w] \in G$ with $w = x$:

$$[A_\alpha, \alpha v][I, u] = [A_\alpha, \alpha v + u] = [A_\alpha, x]$$

- $[A_\alpha, x]$ is the unique element of G such that $\vec{0}^{[A_\alpha, x]} = x$
- $|G| = |V| = 81$, G: transitive, fixed-point-free
- Each of Γ_0, Γ_1, Γ_2 can be expressed as a Cayley graph on G

Summary of some recent results

- First known examples of PDSs in nonabelian groups of order q^{2m}, where q is a power of an odd prime p and $m \geqslant 2$.
- The groups constructed can have exponent as small as p or as large as p^r in a group of order p^{2r}.

Summary of some recent results

- First known examples of PDSs in nonabelian groups of order q^{2m}, where q is a power of an odd prime p and $m \geqslant 2$.
- The groups constructed can have exponent as small as p or as large as p^r in a group of order p^{2r}.

- We construct what we believe are the first known Paley-type PDSs in nonabelian groups and what we believe are the first examples of Paley-Hadamard difference sets in nonabelian groups.
- **EXAMPLE:** $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4}) = (81, 40, 19, 20)$

Summary of some recent results

- First known examples of PDSs in nonabelian groups of order q^{2m}, where q is a power of an odd prime p and $m \geqslant 2$.
- The groups constructed can have exponent as small as p or as large as p^r in a group of order p^{2r}.

- We construct what we believe are the first known Paley-type PDSs in nonabelian groups and what we believe are the first examples of Paley-Hadamard difference sets in nonabelian groups.
- **EXAMPLE:** $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4}) = (81, 40, 19, 20)$

- Using analogues of "product theorems" for abelian groups, we obtain several examples of each

Recent results, cont.

Let q be a prime power and $r < q+1$ be an integer dividing $q+1$. There exists a genuinely nonabelian PDS with parameters

$$\begin{aligned} v &= q^3, \\ k &= (q-1)\left(\frac{(q+1)^2}{r} - q\right), \\ \lambda &= r\left(\frac{q+1}{r} - 1\right)^3 + r - 3, \\ \mu &= \left(\frac{q+1}{r} - 1\right)\left(\frac{(q+1)^2}{r} - q\right). \end{aligned}$$

Thank you!