Restrictions and Computational Methods for Nonabelian PDSs

Seth Nelson

William & Mary

Joint work with Dr. Eric Swartz

Introduction

Today, we will cover:

- Ott's work, and our extension of his work, on nonabelian PDSs.

Introduction

Today, we will cover:

- Ott's work, and our extension of his work, on nonabelian PDSs.
  - This is the 'theoretical' portion of the paper.

Introduction

Today, we will cover:

- Ott's work, and our extension of his work, on nonabelian PDSs.
  - This is the 'theoretical' portion of the paper.

- Our own direct methods to construct PDSs.

Introduction

Today, we will cover:

- Ott's work, and our extension of his work, on nonabelian PDSs.
  - This is the 'theoretical' portion of the paper.
- Our own direct methods to construct PDSs.
  - That is, for a group G and PDS D in G, we compute $|h^G \cap D|$ for every h.

Representation Theory Overview

- Definition: Let G be a finite group. A representation of G is a homomorphism $\mathfrak{F} : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$.

Representation Theory Overview

- Definition: Let G be a finite group. A representation of G is a homomorphism $\mathfrak{F} : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$.
- Definition: For a representation $\mathfrak{F} : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$, we call n the degree of $\mathfrak{F}$.

Representation Theory Overview

- Definition: Let G be a finite group. A representation of G is a homomorphism $\mathfrak{F} : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$.
- Definition: For a representation $\mathfrak{F} : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$, we call n the degree of $\mathfrak{F}$.
- Remark: Take a representation $\mathfrak{F} : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$. Then, G acts on $\mathbb{C}^n$ by $g \cdot v = \mathfrak{F}(g)v$.

Representation Theory Overview

- Definition: Let G be a finite group. A representation of G is a homomorphism $\mathfrak{F} : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$.
- Definition: For a representation $\mathfrak{F} : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$, we call n the degree of $\mathfrak{F}$.
- Remark: Take a representation $\mathfrak{F} : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$. Then, G acts on $\mathbb{C}^n$ by $g \cdot v = \mathfrak{F}(g)v$.
- Definition: We call $\mathfrak{F}$ an irreducible representation if the G-action induced by $\mathfrak{F}$ turns $\mathbb{C}^n$ into an irreducible $\mathbb{C}[G]$-module.

Character Theory Overview

- Definition: The function $\chi : G \longrightarrow \mathbb{C}$ given by $\chi(g) = \mathrm{Tr}(\mathfrak{F}(g))$ for all $g \in G$ is called the character afforded by $\mathfrak{F}$.

Character Theory Overview

- Definition: The function $\chi : G \longrightarrow \mathbb{C}$ given by $\chi(g) = \mathrm{Tr}(\mathfrak{F}(g))$ for all $g \in G$ is called the character afforded by $\mathfrak{F}$.

- Remark: If $\mathfrak{F}$ is a representation of degree n affording χ, then we say that χ has degree n. Also, $\chi(1) = n$.

Character Theory Overview

- Definition: The function $\chi : G \longrightarrow \mathbb{C}$ given by $\chi(g) = \mathrm{Tr}(\mathfrak{F}(g))$ for all $g \in G$ is called the character afforded by $\mathfrak{F}$.
- Remark: If $\mathfrak{F}$ is a representation of degree n affording χ, then we say that χ has degree n. Also, $\chi(1) = n$.
- Definition: We call χ irreducible if $\mathfrak{F}$ is irreducible.

Character Theory Overview

- Definition: The function $\chi : G \longrightarrow \mathbb{C}$ given by $\chi(g) = \mathrm{Tr}(\mathfrak{F}(g))$ for all $g \in G$ is called the character afforded by $\mathfrak{F}$.

- Remark: If $\mathfrak{F}$ is a representation of degree n affording χ, then we say that χ has degree n. Also, $\chi(1) = n$.

- Definition: We call χ irreducible if $\mathfrak{F}$ is irreducible.

- Lemma: We denote by $\mathrm{Irr}(G)$ the set of irreducible characters. This set is finite.

Character Theory Overview

- Definition: We call χ a linear character if χ is degree 1.

Character Theory Overview

- Definition: We call χ a linear character if χ is degree 1.

- Remark: Linear representations are also homomorphisms $G \longrightarrow \mathbb{C}$, for if $\mathfrak{F}$ affords a linear character ξ, then $\mathfrak{F}(g) = [\xi(g)]$.

Character Theory Overview

- Definition: We call χ a linear character if χ is degree 1.
- Remark: Linear representations are also homomorphisms $G \longrightarrow \mathbb{C}$, for if $\mathfrak{F}$ affords a linear character ξ, then $\mathfrak{F}(g) = [\xi(g)]$.
- There is always at least one linear character, called the principal character and denoted by 1_G, and given by $g \mapsto 1$ for all $g \in G$.

Character Theory Overview

- Definition: We call χ a linear character if χ is degree 1.
- Remark: Linear representations are also homomorphisms $G \longrightarrow \mathbb{C}$, for if $\mathfrak{F}$ affords a linear character ξ, then $\mathfrak{F}(g) = [\xi(g)]$.
- There is always at least one linear character, called the principal character and denoted by 1_G, and given by $g \mapsto 1$ for all $g \in G$.
- The set $\mathcal{L}$ of all linear characters forms a group under the multiplication $\xi\chi(g) = \xi(g)\chi(g)$.

Class Functions Overview

- Definition: We call $\phi : G \longrightarrow \mathbb{C}$ a class function if $\chi(h) = \chi(g^{-1}hg)$ for all $g \in G$.

Class Functions Overview

- Definition: We call $\phi : G \longrightarrow \mathbb{C}$ a class function if $\chi(h) = \chi(g^{-1}hg)$ for all $g \in G$.
- Theorem: The set of class functions are a vector space over $\mathbb{C}$, and this vector space is equipped with an inner product, denoted by $[\cdot, \cdot]$.

Class Functions Overview

- Definition: We call $\phi : G \longrightarrow \mathbb{C}$ a class function if $\chi(h) = \chi(g^{-1}hg)$ for all $g \in G$.
- Theorem: The set of class functions are a vector space over $\mathbb{C}$, and this vector space is equipped with an inner product, denoted by $[\cdot, \cdot]$.
- Lemma: All characters are class functions.

Class Functions Overview

- Definition: We call $\phi : G \longrightarrow \mathbb{C}$ a class function if $\chi(h) = \chi(g^{-1}hg)$ for all $g \in G$.
- Theorem: The set of class functions are a vector space over $\mathbb{C}$, and this vector space is equipped with an inner product, denoted by $[\cdot, \cdot]$.
- Lemma: All characters are class functions.
- Lemma: If ψ is a class function, then

$$\psi = \sum_{\chi \in \mathrm{Irr}(G)} [\psi, \chi]\chi.$$

Further Facts and Notation

- D is always a PDS, $\mathfrak{F}$ is always an irreducible representation, χ is always an irreducible character, and ξ is always a linear character.

Further Facts and Notation

- D is always a PDS, $\mathfrak{F}$ is always an irreducible representation, χ is always an irreducible character, and ξ is always a linear character.
- Lemma: If $\mathfrak{F}$ is an irreducible representation, then $\mathfrak{F}(D)$ has at most two eigenvalues, denoted by θ_1, θ_2.

Further Facts and Notation

- D is always a PDS, $\mathfrak{F}$ is always an irreducible representation, χ is always an irreducible character, and ξ is always a linear character.

- Lemma: If $\mathfrak{F}$ is an irreducible representation, then $\mathfrak{F}(D)$ has at most two eigenvalues, denoted by θ_1, θ_2.
  - One proves the above fact by observing that if D is a (v, k, λ, μ)-PDS, then $\mathfrak{F}(D)^2 = k(1) + \lambda D + \mu(G - D - 1)$.

Further Facts and Notation

- D is always a PDS, $\mathfrak{F}$ is always an irreducible representation, χ is always an irreducible character, and ξ is always a linear character.

- Lemma: If $\mathfrak{F}$ is an irreducible representation, then $\mathfrak{F}(D)$ has at most two eigenvalues, denoted by θ_1, θ_2.
  - One proves the above fact by observing that if D is a (v, k, λ, μ)-PDS, then $\mathfrak{F}(D)^2 = k(1) + \lambda D + \mu(G - D - 1)$.

- Lemma: Both θ_1, θ_2 are the non Perron eigenvalues of $\mathrm{Cay}(G, D)$.

Further Facts and Notation

- D is always a PDS, $\mathfrak{F}$ is always an irreducible representation, χ is always an irreducible character, and ξ is always a linear character.
- Lemma: If $\mathfrak{F}$ is an irreducible representation, then $\mathfrak{F}(D)$ has at most two eigenvalues, denoted by θ_1, θ_2.
  - One proves the above fact by observing that if D is a (v, k, λ, μ)-PDS, then $\mathfrak{F}(D)^2 = k(1) + \lambda D + \mu(G - D - 1)$.
- Lemma: Both θ_1, θ_2 are the non Perron eigenvalues of $\mathrm{Cay}(G, D)$.
- We define $\Delta = (\theta_1 - \theta_2)^2$. This is the discriminant of $\mathrm{Cay}(G, D)$.

Application to Partial Difference Sets

Literature

- The only known general restrictions for nonabelian PDSs is given by Swartz-Tauscheck in Restrictions on parameters of partial difference sets in nonabelian groups.

Literature

- The only known general restrictions for nonabelian PDSs is given by Swartz-Tauscheck in Restrictions on parameters of partial difference sets in nonabelian groups.
- Some progress on PDSs corresponding to particular cases, like Generalized Quadrangles (GQs).

Literature

- The only known general restrictions for nonabelian PDSs is given by Swartz-Tauscheck in Restrictions on parameters of partial difference sets in nonabelian groups.
- Some progress on PDSs corresponding to particular cases, like Generalized Quadrangles (GQs).
- For example, Swartz-Tauscheck's paper was inspired by Yoshiara's work, A generalized quadrangle with an automorphism group acting regularly on the points.

Literature

- Character theory is an especially powerful tool in analyzing abelian PDSs. In the nonabelian case, little is known.

Literature

- Character theory is an especially powerful tool in analyzing abelian PDSs. In the nonabelian case, little is known.

- Ott used techniques from character theory to solve a 30 year old conjecture of Ghinelli on nonabelian PDSs corresponding to GQs, in his paper On generalized quadrangles with a group of automorphisms acting regularly on the point set, difference sets with -1 as multiplier and a conjecture of Ghinelli.

Literature

- Character theory is an especially powerful tool in analyzing abelian PDSs. In the nonabelian case, little is known.
- Ott used techniques from character theory to solve a 30 year old conjecture of Ghinelli on nonabelian PDSs corresponding to GQs, in his paper On generalized quadrangles with a group of automorphisms acting regularly on the point set, difference sets with -1 as multiplier and a conjecture of Ghinelli.
- We extend Ott's results to the general case.

Generalizations of Ott's Results

- Let D be a (v, k, λ, μ)-PDS in a group G. Let H consist of all linear characters ξ of order coprime to Δ, and suppose H is nontrivial. Define N as $N = \bigcap_{\xi \in H} \ker \xi$. Then,

Generalizations of Ott's Results

- Let D be a (v, k, λ, μ)-PDS in a group G. Let H consist of all linear characters ξ of order coprime to Δ, and suppose H is nontrivial. Define N as $N = \bigcap_{\xi \in H} \ker \xi$. Then,
- Theorem: If $\xi \in H$, and χ is a nonprincipal irreducible character, then $\xi\chi(D) = \chi(D)$.

Generalizations of Ott's Results

- Let D be a (v, k, λ, μ)-PDS in a group G. Let H consist of all linear characters ξ of order coprime to Δ, and suppose H is nontrivial. Define N as $N = \bigcap_{\xi \in H} \ker \xi$. Then,
- Theorem: If $\xi \in H$, and χ is a nonprincipal irreducible character, then $\xi\chi(D) = \chi(D)$.
- Theorem: If $a \notin N$, $\xi \in H$, $\xi \neq 1_G$, then $|a^G \cap D||C_G(a)| = k - \xi(D)$.

Generalizations of Ott's Results

- Let D be a (v, k, λ, μ)-PDS in a group G. Let H consist of all linear characters ξ of order coprime to Δ, and suppose H is nontrivial. Define N as $N = \bigcap_{\xi \in H} \ker \xi$. Then,
- Theorem: If $\xi \in H$, and χ is a nonprincipal irreducible character, then $\xi\chi(D) = \chi(D)$.
- Theorem: If $a \notin N$, $\xi \in H$, $\xi \neq 1_G$, then $|a^G \cap D||C_G(a)| = k - \xi(D)$.
- Theorem: Let p be a prime dividing $|H|$ and $k - \theta_\alpha$, $(\alpha \in \{1, 2\})$. Let P be a Sylow p-subgroup of G. Let π_β be the product of primes powers q such that $q|v$ and $q|(k - \theta_\beta)$ $(\beta \neq \alpha)$ such that $q \nmid \sqrt{\Delta}$. Then, if G is solvable,

$$\pi_\beta \equiv 1 \pmod{p}.$$

The Φ Function

- Definition: We define $\Phi : G \longrightarrow \mathbb{C}$ by

$$\Phi(h) = |h^G \cap D||C_G(h)|.$$

The Φ Function

- Definition: We define $\Phi : G \longrightarrow \mathbb{C}$ by

$$\Phi(h) = |h^G \cap D||C_G(h)|.$$

- Remark: This function also has a combinatorial definition. Say that $\Gamma = \mathrm{Cay}(G, D)$, and that G acts on Γ in the natural way. Then, $\Phi(g)$ counts how many vertices v of Γ are adjacent to v^g. In the same way, if G acts regularly on an SRG Γ, then we get a Φ function.

The Φ Function

- Definition: We define $\Phi : G \longrightarrow \mathbb{C}$ by
$$\Phi(h) = |h^G \cap D||C_G(h)|.$$
- Remark: This function also has a combinatorial definition. Say that $\Gamma = \mathrm{Cay}(G, D)$, and that G acts on Γ in the natural way. Then, $\Phi(g)$ counts how many vertices v of Γ are adjacent to v^g. In the same way, if G acts regularly on an SRG Γ, then we get a Φ function.
- Ott first noticed that Φ is a class function, and he showed that
$$\Phi = \sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(D)}\chi.$$
By proving that $[\Phi, \chi] = \overline{\chi(D)}$.

The Φ Function

- Ott's theorems for PDSs come about via analysis of the function Φ.

The Φ Function

- Ott's theorems for PDSs come about via analysis of the function Φ.
- Theorem: If $\xi \in H$, $\chi \in \mathrm{Irr}(G)$, with $\chi \neq 1_G$, then $\xi\chi(D) = \chi(D)$.

The Φ Function

- Ott's theorems for PDSs come about via analysis of the function Φ.
- Theorem: If $\xi \in H$, $\chi \in \mathrm{Irr}(G)$, with $\chi \neq 1_G$, then $\xi\chi(D) = \chi(D)$.
- Recall H consists of all linear characters ξ of order coprime to Δ. Define N as $N = \bigcap_{\xi \in H} \ker \xi$.

The Φ Function

- Ott's theorems for PDSs come about via analysis of the function Φ.
- Theorem: If $\xi \in H$, $\chi \in \mathrm{Irr}(G)$, with $\chi \neq 1_G$, then $\xi\chi(D) = \chi(D)$.
- Recall H consists of all linear characters ξ of order coprime to Δ. Define N as $N = \bigcap_{\xi \in H} \ker \xi$.
- Theorem: Suppose H is nontrivial. If $a \notin N$ and $\xi \in H$ with $1_G \neq \xi$, then $\Phi(a) = |a^G \cap D||C_G(a)| = k - \xi(D)$.

The Φ Function

- Ott's theorems for PDSs come about via analysis of the function Φ.
- Theorem: If $\xi \in H$, $\chi \in \mathrm{Irr}(G)$, with $\chi \neq 1_G$, then $\xi\chi(D) = \chi(D)$.
- Recall H consists of all linear characters ξ of order coprime to Δ. Define N as $N = \bigcap_{\xi \in H} \ker \xi$.
- Theorem: Suppose H is nontrivial. If $a \notin N$ and $\xi \in H$ with $1_G \neq \xi$, then $\Phi(a) = |a^G \cap D||C_G(a)| = k - \xi(D)$.
- Main Idea: Use the previous theorem $\xi\chi(D) = \chi(D)$ since $\xi \in H$ and inspect both parts of

$$\Phi(a) = \sum_{\xi \in H} \overline{\xi(D)}\chi(a) + \sum_{\chi \notin H} \overline{\chi(D)}\chi(a).$$

Computational and Constructive Techniques

- Recall that if G acts regularly on an SRG, then we get a PDS.

Computational and Constructive Techniques

- Recall that if G acts regularly on an SRG, then we get a PDS.
- Recall also that if $\mathfrak{F}$ is an irreducible representation, then $\mathfrak{F}(D)$ has all its eigenvalues as θ_1, θ_2, which are the non Perron eigenvalues of $\mathrm{Cay}(G, D)$.

Computational and Constructive Techniques

- Recall that if G acts regularly on an SRG, then we get a PDS.
- Recall also that if $\mathfrak{F}$ is an irreducible representation, then $\mathfrak{F}(D)$ has all its eigenvalues as θ_1, θ_2, which are the non Perron eigenvalues of $\mathrm{Cay}(G, D)$.
- Finally, we also have that

$$\Phi = \sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(D)}\chi.$$

Computational and Constructive Techniques

- Recall that if G acts regularly on an SRG, then we get a PDS.
- Recall also that if $\mathfrak{F}$ is an irreducible representation, then $\mathfrak{F}(D)$ has all its eigenvalues as θ_1, θ_2, which are the non Perron eigenvalues of $\mathrm{Cay}(G, D)$.
- Finally, we also have that

$$\Phi = \sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(D)}\chi.$$

- Therefore, if there is no set $S \subseteq G$ such that $\overline{\chi(S)}$ is a sum of θ_1, θ_2, then G does not contain a PDS.

Computational and Constructive Techniques

- Main Idea: To search for a (v, k, λ, μ)-PDS in G, for the full set of irreducible characters $\chi_1, \ldots, \chi_n$, compute the values $\overline{\chi_i(S)}$ for every $S \subseteq G$, and check that

$$\overline{\chi_i(S)} = \overline{a\theta_1 + b\theta_2} = a\theta_1 + b\theta_2$$

where $a + b = \chi_i(1)$.

Computational and Constructive Techniques

- Main Idea: To search for a (v, k, λ, μ)-PDS in G, for the full set of irreducible characters $\chi_1, \ldots, \chi_n$, compute the values $\overline{\chi_i(S)}$ for every $S \subseteq G$, and check that

$$\overline{\chi_i(S)} = \overline{a\theta_1 + b\theta_2} = a\theta_1 + b\theta_2$$

where $a + b = \chi_i(1)$.

- Problem: There are too many possible sets S.

Computational and Constructive Techniques

- Main Idea: To search for a (v, k, λ, μ)-PDS in G, for the full set of irreducible characters $\chi_1, \ldots, \chi_n$, compute the values $\overline{\chi_i(S)}$ for every $S \subseteq G$, and check that

$$\overline{\chi_i(S)} = \overline{a\theta_1 + b\theta_2} = a\theta_1 + b\theta_2$$

where $a + b = \chi_i(1)$.

- Problem: There are too many possible sets S.

- Solution: Enforce modular constraints on S, and search subject to these constraints.

- Solution: Enforce modular constraints on S, and search subject to these constraints.

Computational and Constructive Techniques

- Solution: Enforce modular constraints on S, and search subject to these constraints.

- Since $\Delta = (\theta_1 - \theta_2)^2$, then $\theta_1 \equiv \theta_2 \pmod{\sqrt{\Delta}}$.

- Solution: Enforce modular constraints on S, and search subject to these constraints.

- Since $\Delta = (\theta_1 - \theta_2)^2$, then $\theta_1 \equiv \theta_2 \pmod{\sqrt{\Delta}}$.

- Therefore, if S is a valid PDS, then for $\chi \neq 1_G$, we get

$$\overline{\chi(S)} = \overline{a\theta_1 + b\theta_2} = a\theta_1 + b\theta_2 \equiv (a+b)\theta_1 \equiv \chi(1)\theta_1 \pmod{\sqrt{\Delta}}.$$

Computational and Constructive Techniques

- If S is a valid PDS, then $\overline{\chi(S)} \equiv \chi(1)\theta_1 \pmod{\sqrt{\Delta}}$ whenever $\chi \neq 1_G$.

Computational and Constructive Techniques

- If S is a valid PDS, then $\overline{\chi(S)} \equiv \chi(1)\theta_1 \pmod{\sqrt{\Delta}}$ whenever $\chi \neq 1_G$.
- Idea: Evaluate $\overline{\chi(S)}\chi(a)$ "mod" some prime power dividing $\sqrt{\Delta}$.

Computational and Constructive Techniques

- If S is a valid PDS, then $\overline{\chi(S)} \equiv \chi(1)\theta_1 \pmod{\sqrt{\Delta}}$ whenever $\chi \neq 1_G$.
- Idea: Evaluate $\overline{\chi(S)}\chi(a)$ "mod" some prime power dividing $\sqrt{\Delta}$.
- Remark: Although in general $\overline{\chi(S)}\chi(a)$ will not be an integer, we may use something known as a local ring, $\mathfrak{R}$, containing $\mathbb{Z}$, to evaluate $\overline{\chi(S)}\chi(a) \pmod{\mathfrak{p}^k}$.

Computational and Constructive Techniques

- If S is a valid PDS, then $\overline{\chi(S)} \equiv \chi(1)\theta_1 \pmod{\sqrt{\Delta}}$ whenever $\chi \neq 1_G$.
- Idea: Evaluate $\overline{\chi(S)}\chi(a)$ "mod" some prime power dividing $\sqrt{\Delta}$.
- Remark: Although in general $\overline{\chi(S)}\chi(a)$ will not be an integer, we may use something known as a local ring, $\mathfrak{R}$, containing $\mathbb{Z}$, to evaluate $\overline{\chi(S)}\chi(a) \pmod{\mathfrak{p}^k}$.
- Over this local ring, taking $x \in \mathbb{Z}$, then the residue $x \pmod{p^k}$ equals the residue of $x \pmod{\mathfrak{p}^k}$ if the ideal $\mathfrak{p}$ is properly chosen.

Computational and Constructive Techniques

- If S is a valid PDS, then $\overline{\chi(S)} \equiv \chi(1)\theta_1 \pmod{\sqrt{\Delta}}$ whenever $\chi \neq 1_G$.
- Idea: Evaluate $\overline{\chi(S)}\chi(a)$ "mod" some prime power dividing $\sqrt{\Delta}$.
- Remark: Although in general $\overline{\chi(S)}\chi(a)$ will not be an integer, we may use something known as a local ring, $\mathfrak{R}$, containing $\mathbb{Z}$, to evaluate $\overline{\chi(S)}\chi(a) \pmod{\mathfrak{p}^k}$.
- Over this local ring, taking $x \in \mathbb{Z}$, then the residue $x \pmod{p^k}$ equals the residue of $x \pmod{\mathfrak{p}^k}$ if the ideal $\mathfrak{p}$ is properly chosen.
- Therefore, $\overline{\chi(S)}\chi(a) \equiv \chi(1)\theta_1\chi(a) \pmod{\mathfrak{p}^k}$ whenever $\chi \neq 1_G$ like we wanted.

Computational and Constructive Techniques

- Take the function Φ so that $\Phi(a) = \sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(S)}\chi(a)$.

Computational and Constructive Techniques

- Take the function Φ so that $\Phi(a) = \sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(S)}\chi(a)$.
- If S is a PDS, then $\overline{\chi(S)}\chi(a) \equiv \chi(1)\theta_1\chi(a) \pmod{\mathfrak{p}^k}$ when $\chi \neq 1_G$, then it is not too challenging to show that

$$\sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(S)}\chi(a) = k - \theta_1 \pmod{\mathfrak{p}^k}$$

whenever $a \neq 1$, and otherwise

$$\sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(S)}\chi(1) = k + |G|(\theta_1 - 1) \pmod{\mathfrak{p}^k}$$

Computational and Constructive Techniques

- Take the function Φ so that $\Phi(a) = \sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(S)}\chi(a)$.
- If S is a PDS, then $\overline{\chi(S)}\chi(a) \equiv \chi(1)\theta_1\chi(a) \pmod{\mathfrak{p}^k}$ when $\chi \neq 1_G$, then it is not too challenging to show that

$$\sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(S)}\chi(a) = k - \theta_1 \pmod{\mathfrak{p}^k}$$

whenever $a \neq 1$, and otherwise

$$\sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(S)}\chi(1) = k + |G|(\theta_1 - 1) \pmod{\mathfrak{p}^k}$$

- Finally, $\Phi(a) \in \mathbb{Z}$, so $\Phi(a) = k - \theta_1 \pmod{p^k}$ and $\phi(1) = k + |G|(\theta_1 - 1) \pmod{p^k}$.

Computational and Constructive Techniques

- Thus, if S is a valid PDS, then $|a^G \cap S||C_G(a)| \equiv k - \theta_1 \pmod{p^k}$.

- Thus, if S is a valid PDS, then $|a^G \cap S||C_G(a)| \equiv k - \theta_1 \pmod{p^k}$.
- If p does not divide $|C_G(a)|$, then $|a^G \cap S| \equiv (k - \theta_1)|C_G(a)|^{-1} \pmod{p^k}$. This gives us the modular restriction on S we hoped for.

Computational and Constructive Techniques

- Thus, if S is a valid PDS, then $|a^G \cap S||C_G(a)| \equiv k - \theta_1 \pmod{p^k}$.

- If p does not divide $|C_G(a)|$, then $|a^G \cap S| \equiv (k - \theta_1)|C_G(a)|^{-1} \pmod{p^k}$. This gives us the modular restriction on S we hoped for.

- Now, let $h_1, \ldots, h_r$ be conjugacy class representatives of G.

Computational and Constructive Techniques

- Thus, if S is a valid PDS, then $|a^G \cap S||C_G(a)| \equiv k - \theta_1 \pmod{p^k}$.

- If p does not divide $|C_G(a)|$, then $|a^G \cap S| \equiv (k - \theta_1)|C_G(a)|^{-1} \pmod{p^k}$. This gives us the modular restriction on S we hoped for.

- Now, let $h_1, \ldots, h_r$ be conjugacy class representatives of G.

- To search for a PDS S, we restrict to searching for a set of integers $s_1, \ldots, s_r$ such that $\sum_{i=1}^r s_i = k$ and $s_i = (k - \theta_1)|C_G(a)|^{-1} \pmod{p^k}$ for each p dividing $\sqrt{\Delta}$ but not dividing $|C_G(a)|$.

Computational and Constructive Techniques

- This gives a set of constants $s_1, \ldots, s_r$ so that for any PDS D in G, $|h_i^G \cap D| = s_i$.

Computational and Constructive Techniques

- This gives a set of constants $s_1, \dots, s_r$ so that for any PDS D in G, $|h_i^G \cap D| = s_i$.

- We then modify Brady's Hill Climb algorithm to only search for PDSs satisfying this collection of constraints.

Computational and Constructive Techniques

- This gives a set of constants $s_1, \ldots, s_r$ so that for any PDS D in G, $|h_i^G \cap D| = s_i$.
- We then modify Brady's Hill Climb algorithm to only search for PDSs satisfying this collection of constraints.
- Combining these techniques with the theorems from Ott, we computed all intersections $|h^G \cap D|$ for every feasible $(v, k, \lambda\mu)$-PDS with v up to 506 (except for a small set of very specific v), and a further constrained set of PDSs for v up to 1300.

Applying the Results: PDSs We Ruled Out with $v \leq 506$

v	k	λ	μ
10	3	0	1
26	10	3	4
36	14	7	4
40	12	2	4
50	21	8	9
56	10	0	2
66	20	10	4
70	27	12	9
78	22	11	4
82	36	15	16
100	33	14	9
105	40	15	15
112	30	2	10
112	36	10	12

v	k	λ	μ
120	28	14	4
120	42	8	18
122	55	24	25
126	25	8	4
126	50	13	24
126	60	33	24
130	48	20	16
135	64	28	32
136	30	15	4
154	48	12	16
154	72	26	40
156	30	4	6
165	36	3	9
170	78	35	36

v	k	λ	μ
171	50	13	15
176	40	12	8
176	49	12	14
189	60	27	15
189	88	37	44
190	36	18	4
190	45	12	10
190	84	33	40
190	84	38	36
190	90	45	40
196	39	2	9
196	60	23	16
196	81	42	27
204	28	2	4

Applying the Results: PDSs We Ruled Out with $v \leq 506$

v	k	λ	μ
204	63	22	18
208	45	8	10
210	38	19	4
220	72	22	24
220	84	38	28
222	51	20	9
226	105	48	49
231	70	21	21
238	75	20	25
243	66	9	21
246	85	20	34
246	105	36	51
246	119	64	51
260	70	15	20

v	k	λ	μ
266	45	0	9
273	72	21	18
273	136	65	70
276	44	22	4
276	75	10	24
276	75	18	21
276	110	52	38
276	135	78	54
280	36	8	4
280	117	44	52
286	95	24	35
286	125	60	50
288	105	52	30
288	112	36	48

v	k	λ	μ
290	136	63	64
297	40	7	5
297	104	31	39
300	46	23	4
306	55	4	11
306	60	10	12
322	96	20	32
324	68	7	16
324	95	34	25
330	63	24	9
336	80	28	16
336	125	40	50
340	108	30	36
342	33	4	3

Applying the Results: PDSs We Ruled Out with $v \leq 506$

v	k	λ	μ
342	66	15	12
343	162	81	72
351	70	13	14
351	140	49	60
351	160	64	80
352	26	0	2
352	108	44	28
352	126	50	42
362	171	80	81
364	33	2	3
364	66	20	10
364	88	12	24
364	120	38	40
364	121	48	36

v	k	λ	μ
364	165	68	80
364	176	90	80
372	56	10	8
375	102	45	21
375	176	94	72
375	182	85	91
378	52	1	8
378	52	26	4
385	60	5	10
385	168	77	70
392	69	26	9
392	153	54	63
396	135	30	54
396	150	51	60

v	k	λ	μ
399	198	97	99
400	21	2	1
400	56	6	8
400	133	42	45
405	132	63	33
405	196	91	98
406	54	27	4
406	108	30	28
406	165	68	66
406	189	84	91
406	195	96	91
408	176	70	80
414	63	12	9
416	100	36	20

Applying the Results: PDSs We Ruled Out with $v \leq 506$

v	k	λ	μ	v	k	λ	μ	v	k	λ	μ
416	165	64	66	456	140	40	44	476	133	42	35
416	165	64	66	456	140	58	36	476	133	60	28
418	147	56	49	456	175	78	60	484	105	14	25
430	39	8	3	456	182	73	72	484	138	47	36
430	135	36	45	456	195	74	90	490	165	56	55
430	165	68	60	460	85	18	15	490	192	92	64
438	92	31	16	460	99	18	22	494	85	12	15
441	56	7	7	460	147	42	49	495	190	85	65
441	190	89	76	460	204	78	100	495	208	86	88
441	220	95	124	460	216	116	88	495	238	109	119
442	210	99	100	460	225	120	100	496	54	4	6
456	65	10	9	465	144	43	45	498	161	64	46
456	80	4	16	470	126	27	36	506	100	18	20
456	130	24	42	474	165	52	60				

Applying the Results: Class Intersection Sizes of a PDS (if it exists)

(v, k, λ, μ)	ID	Conjugacy Class Intersections
(21, 10, 3, 6)	1	[0, 3, 2, 3, 2]
(27, 10, 1, 5)	3	[0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
	4	[0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
(55, 18, 9, 4)	1	[0, 4, 1, 4, 1, 4, 4]
(57, 24, 11, 9)	1	[0, 9, 1, 9, 1, 1, 1, 1, 1]
(96, 35, 10, 14)	64	[0, 4, 14, 1, 1, 4, 4, 1, 2, 4]
	227	[0, 4, 14, 1, 1, 4, 4, 2, 1, 4]
(111, 44, 19, 16)	1	[0, 16, 1, 16, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]

Applying the Results: Class Intersection Sizes of a PDS (if it exists)

(v, k, λ, μ)	ID	Conjugacy Class Intersections
(125, 28, 3, 7)	3	[0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
	4	[0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
(125, 52, 15, 26)	3	[0, 2, 2, 1, 2, 2, 2, 1, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2]
	4	[0, 2, 2, 1, 2, 2, 2, 1, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2]

Applying the Results: Class Intersection Sizes of a PDS (if it exists)

(v, k, λ, μ)	ID	Conjugacy Class Intersections
(136, 30, 8, 6)	12	[0, 3, 3, 8, 2, 3, 3, 3, 3, 2]
(136, 60, 24, 28)	12	[0, 7, 10, 4, 4, 7, 7, 10, 7, 4]
(136, 63, 30, 28)	12	[0, 7, 7, 13, 4, 7, 7, 7, 7, 4]
(148, 63, 22, 30)	3	[0, 15, 15, 2, 15, 2, 2, 2, 2, 2, 2, 2, 2]
(148, 70, 36, 30)	3	[0, 15, 22, 2, 15, 2, 2, 2, 2, 2, 2, 2, 2]
(155, 42, 17, 9)	1	[0, 9, 1, 9, 9, 1, 9, 1, 1, 1, 1]

Applying the Results: Class Intersection Sizes of a PDS (if it exists)

(v, k, λ, μ)	ID	Conjugacy Class Intersections
(160, 54, 18, 18)	199	[0, 6, 6, 0, 0, 0, 6, 6, 6, 6, 6, 6, 6]
	199	[0, 6, 0, 6, 0, 0, 6, 6, 6, 6, 6, 6, 6]
	199	[0, 6, 0, 0, 6, 0, 6, 6, 6, 6, 6, 6, 6]
	234	[0, 6, 12, 3, 3, 0, 6, 6, 6, 12]
	234	[0, 6, 12, 3, 0, 3, 6, 6, 6, 12]
	234	[0, 6, 12, 0, 3, 3, 6, 6, 6, 12]
(171, 34, 17, 4)	3	[0, 4, 4, 1, 4, 4, 4, 1, 4, 4, 4]

Applying the Results: Class Intersection Sizes of a PDS (if it exists)

$\cdots$

Applying the Results: Infinite Families

- We used our PDS class intersections to construct some sporadic examples of PDSs and two PDS families.

Applying the Results: Infinite Families

- We used our PDS class intersections to construct some sporadic examples of PDSs and two PDS families.
- Both families arise from combinatorial constructions in adjacent mathematical fields, which have not been recognized as PDSs either at all, or until very recently.

Applying the Results: Infinite Families

- We used our PDS class intersections to construct some sporadic examples of PDSs and two PDS families.
- Both families arise from combinatorial constructions in adjacent mathematical fields, which have not been recognized as PDSs either at all, or until very recently.
- One family, a consequence of work by Clapham, was unknown until a paper by Ponomarenko and Ryabov in 2024.

Applying the Results: Infinite Families

- We used our PDS class intersections to construct some sporadic examples of PDSs and two PDS families.
- Both families arise from combinatorial constructions in adjacent mathematical fields, which have not been recognized as PDSs either at all, or until very recently.
- One family, a consequence of work by Clapham, was unknown until a paper by Ponomarenko and Ryabov in 2024.
- Theorem (Clapham): Let p be a prime such that $p^d > 9$ and $p^d \equiv 7 \pmod{12}$. Then, there exist

$$\left(p^d\left(\frac{p^d-1}{6}\right), 3\left(\frac{p^d-3}{2}\right), \frac{p^d+3}{2}, 9\right)$$

PDSs in the nonabelian group

$$C_{p^d} \rtimes C_{\frac{p^d-1}{6}} \leq (\mathrm{GF}(p^d), +) \rtimes (\mathrm{GF}(p^d)^\times, \cdot).$$

Applying the Results: Infinite Families

- Another family, a consequence from a paper by Wilson, appears to not have been recognized to this day.

Applying the Results: Infinite Families

- Another family, a consequence from a paper by Wilson, appears to not have been recognized to this day.
- Theorem (Wilson): Let p be a prime such that $p^d > (\frac{1}{2}k(k-1))^{k(k-1)}$. If $p^d \equiv k(k-1)+1 \pmod{2k(k-1)}$, then there exists a

$$\left(p^d\left(\frac{p^d-1}{k(k-1)}\right), \frac{k(p^d-k)}{k-1}, \frac{p^d-1}{k-1}+(k-1)^2-2, k^2\right)$$

PDS in the nonabelian group

$$C_{p^d} \rtimes C_{\frac{p^d-1}{k(k-1)}} \leq (\mathrm{GF}(p^d),+) \rtimes (\mathrm{GF}(p^d)^\times, \cdot).$$

Next Steps

Next Steps

- What can we use the following theorem to rule out in general?

Next Steps

- What can we use the following theorem to rule out in general?

- Theorem: Let p be a prime dividing $|H|$ and $k - \theta_\alpha$, $(\alpha \in \{1, 2\})$. Let P be a Sylow p-subgroup of G. Let π_β be the product of primes powers q such that $q|v$ and $q|(k - \theta_\beta)$ $(\beta \neq \alpha)$ such that $q \nmid \sqrt{\Delta}$. Then, if G is solvable,

$$\pi_\beta \equiv 1 \pmod{p}.$$

Next Steps

- To search for a PDS S, we restrict to searching for a set of integers $s_1, \ldots, s_r$ such that $\sum_{i=1}^{r} s_i = k$ and $s_i = (k - \theta_1)|C_G(a)|^{-1} \pmod{p^k}$ for each p dividing $\sqrt{\Delta}$ but not dividing $|C_G(a)|$.

Next Steps

- To search for a PDS S, we restrict to searching for a set of integers $s_1, \ldots, s_r$ such that $\sum_{i=1}^{r} s_i = k$ and $s_i = (k - \theta_1)|C_G(a)|^{-1} \pmod{p^k}$ for each p dividing $\sqrt{\Delta}$ but not dividing $|C_G(a)|$.

- Problem: It is especially hard searching in groups where for a prime p dividing $\sqrt{\Delta}$, we also expect p to divide $|C_G(a)|$. For these groups, we need some new methods.

Next Steps

- To search for a PDS S, we restrict to searching for a set of integers $s_1, \ldots, s_r$ such that $\sum_{i=1}^{r} s_i = k$ and $s_i = (k - \theta_1)|C_G(a)|^{-1} \pmod{p^k}$ for each p dividing $\sqrt{\Delta}$ but not dividing $|C_G(a)|$.
- Problem: It is especially hard searching in groups where for a prime p dividing $\sqrt{\Delta}$, we also expect p to divide $|C_G(a)|$. For these groups, we need some new methods.
- (Possible) Solution: We perform our search as if the s_i are independent, but in general they will not be independent of each other. Leverage their dependence to simplify the search.

Next Steps

- Remark: If we have a sum $\sum_{i=1}^{\ell} \overline{\chi_{k_i}(S)}\chi(a) \in \mathbb{Z}$, and it is possible to partition the k_i such that the two sets $\{\chi_{s_i}\}$ and $\{\chi_{r_i}\}$ take their values in coprime cyclotomic number rings, then $\sum_{i=1}^{\ell} \overline{\chi_{s_i}(S)}\chi(a)$ and $\sum_{i=1}^{\ell} \overline{\chi_{r_i}(S)}\chi(a)$ are in $\mathbb{Z}$.

Next Steps

- Remark: If we have a sum $\sum_{i=1}^{\ell} \overline{\chi_{k_i}(S)}\chi(a) \in \mathbb{Z}$, and it is possible to partition the k_i such that the two sets $\{\chi_{s_i}\}$ and $\{\chi_{r_i}\}$ take their values in coprime cyclotomic number rings, then $\sum_{i=1}^{\ell} \overline{\chi_{s_i}(S)}\chi(a)$ and $\sum_{i=1}^{\ell} \overline{\chi_{r_i}(S)}\chi(a)$ are in $\mathbb{Z}$.

- Choose "good" partitions $\{\chi_{a_i}\}, \{\chi_{b_i}\}, \ldots$ of the set $\chi_1, \ldots, \chi_n$. Find S such that $\sum_{i=1}^{\ell} \overline{\chi_{a_i}(S)}\chi(a)$, $\sum_{i=1}^{\ell} \overline{\chi_{b_i}(S)}\chi(a)$, ... are in $\mathbb{Z}$.

Thank you!