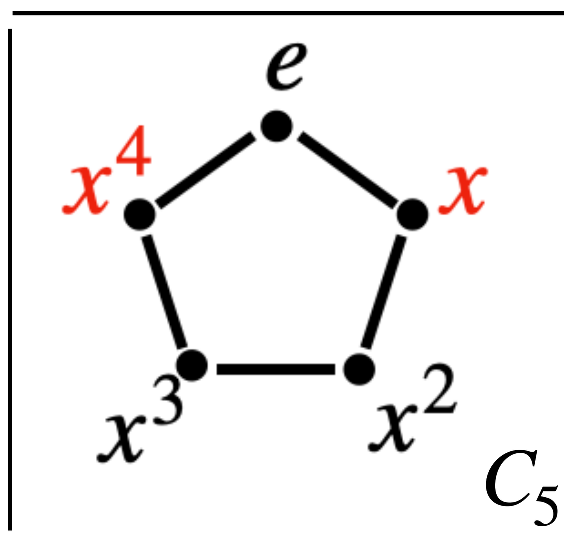
Needles in the Haystack: Finding Nonabelian Partial Difference Sets (PDSs) with Computer Search

Andrew Brady, Carnegie Mellon University
acbrady@andrew.cmu.edu

What is a partial difference set (PDS)?

A regular $(n = |G|, k = |D|, \lambda, \mu)$ PDS is a subset $D \subseteq G$ such that $D^2 = ke + \lambda D + \mu(G - D - e)$



Example PDS

$(n, k, \lambda, \mu) = (5,2,0,1)$

$D = x + x^4 \in \mathbb{Z}[C_5]$

$D^2 = (x + x^4)(x + x^4) = 2e + x^2 + x^3$

Negative Latin Square Type

Parameters of form $(n^2, r(n+1), -n + r^2 + 3r, r^2 + r)$

Why Find PDSs?

1. Connections to:
    1. projective 2-weight codes
    2. strongly regular graphs
    3. rank 3 association schemes
2. Testbed for search techniques

What was already known?

- Abelian groups: many constructions known
- Nonabelian groups: comparatively less, though recent work has begun to address gap
- Negative Latin Square Type Nonabelian: very little known
- Challenge: Search space is enormous

Why Nonabelian Groups?

- (Informally) Most PDSs in nonabelian groups [PDSS24]
- Some PDSs (called genuinely nonabelian) are only in nonabelian groups

Method 1: Reducing Search Space with Characters

$\phi : G \to N$, N abelian

$\chi : N \to \mathbb{C}$: character

D is PDS $\Longrightarrow$

$\chi(\phi(D)) \in \text{Spectrum}(D)$

For (64,18,2,6) PDSs:

$N = C_2^3 = \{x^i y^j z^k \mid x^2 = y^2 = z^2 = 1\}$

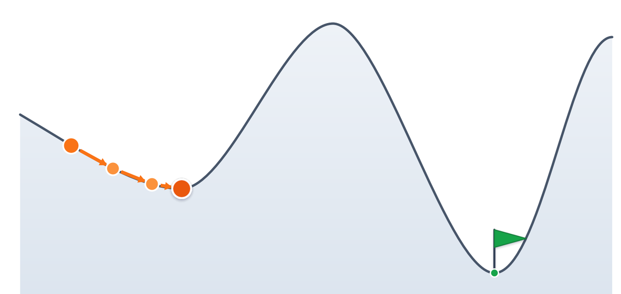
$\text{Spectrum}(D) = \{-6, 2, 18\}$

Number of elements in cosets $(1, x, y, z, xy, xz, yz, xyz)$ is either $(4,2,2,2,2,2,2,2)$, $(4,2,0,2,2,4,2,2)$, etc. Then check all exhaustively.

Results: (64,18,2,6) Search

- Motivation: (64,18,2,6) is negative Latin square type
- Effect of search space reduction $\approx 10^{15} \to 10^{10}$ candidate sets/group
- Main execution time was 3.5 hours on a desktop (code in Java). Preprocessing done in GAP [GAP21].
- Searched exhaustively among groups with C_2^3 normal subgroups (except C_2^6) (212/267 groups of order 64)
- Found precisely <u>48 nonabelian groups</u> with (64,18,2,6) PDSs
- For comparison, <u>only 3 abelian groups</u> with (64,18,2,6) PDSs

Method 2: Hill Climbing Local Search



$\text{Error}(D) = \|D^2 - ke - \lambda D - \mu(G - D - e)\|_2^2$

- Plan: run many instances of hill climb, hope one finds a PDS (ie random restart).
- No additional group-theoretic knowledge used.
- Benefit: Fast
- Drawback: Local search cannot show nonexistence

Results: Local Search

- Local search ran among all possible parameter sets where $n \leq 215$, finding many previously known PDSs, including all found with Method 1
- Found **(147,66,25,33)** and **(144,52,16,20)** PDSs. These
    1. **Proved existence of strongly regular graphs (SRGs) with these parameters**
    2. Are genuinely nonabelian
- (144,52,16,20) is also negative Latin square type
- Brouwer then applied switching on the (147,66,25,33) SRG to get a (148,77,36,44) SRG, which also was previously unknown [Bro24]

	Group	Trials	Time (s)	# PDSs found
(144,52,16,20)	$C_3 \times (C_4^2 \rtimes C_3)$	100K	88.79	3
(147,66,25,33)	$C_7^2 \rtimes C_3$	10K	13.77	78

Runtime Benchmark. 72-core machine. C++ code, shared-memory parallelism with Parlay [BAD20].

Open Questions: PDSs

- Some of the (64,18,2,6) PDSs found were decomposable into three (16,6,2) difference sets (i.e., a linking system). Can we use that structure to generate an infinite family?
- Why are some PDSs easier to find than others (as seen in table)?
- Why does local search work at all? Search space is enormous (10^{40})

Future Directions

- Takeaway: Low-resource computational search is surprisingly effective
- Future work: Low-resource computer search for other interesting combinatorial objects
- If low-resource methods achieved results, how far could high-resource methods (LLMs; SAT solving) go?

Acknowledgements

Thank you to Dr. Jim Davis for proposing and advising this project, paper editing, and mentorship. Thank you to Drs. Ken Smith and John Polhill for mentorship and helpful discussions. This work as supported by a University of Richmond undergraduate summer research fellowship.

References

[BAD20] G. Blelloch, D. Anderson, and L. Dhulipala. Parlaylib - a toolkit for parallel algorithms on shared-memory multicore machines. In Proceedings of the 32nd ACM Symposium on Parallelism in Algorithms and Architectures, SPAA '20, page 507–509, New York, NY, USA, 2020. Association for Computing Machinery.
[Bra22] A. C. Brady. Negative latin square type partial difference sets in nonabelian groups of order 64. Finite Fields and their Applications, 81:102044, 2022.
[Bra25] Andrew Brady. New strongly regular graphs found via local search for partial difference sets. The Electronic Journal of Combinatorics, 32(1), Feb. 2025.
[Bro24] A.E. Brouwer. Strongly regular graphs with parameters (148,77,36,44). https://www.win.tue.nl/~aeb/preprints/srg148.pdf, 2024.
[PDSS24] J. Polhill, J. A. Davis, K. W. Smith, and E. Swartz. Genuinely nonabelian partial difference sets. Journal of Combinatorial Designs, 32(7):351–370, 2024.