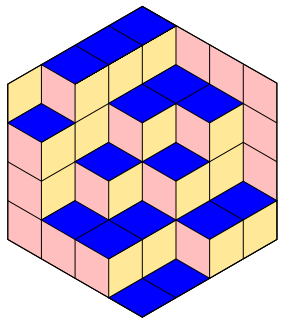


ALGEBRAIC COMBINATORICS

James A. Davis, John Polhill, Ken Smith & Eric Swartz

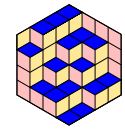
Nonabelian partial difference sets constructed using abelian techniques

Volume 8, issue 2 (2025), p. 399-419.

https://doi.org/10.5802/alco.416

Algebraic Combinatorics is published by The Combinatorics Consortium and is a member of the Centre Mersenne for Open Scientific Publishing
www.tccpublishing.org www.centre-mersenne.org
e-ISSN: 2589-5486

Algebraic Combinatorics
Volume 8, issue 2 (2025), p. 399–419
https://doi.org/10.5802/alco.416



Nonabelian partial difference sets constructed using abelian techniques

James A. Davis, John Polhill, Ken Smith & Eric Swartz

Abstract A (v, k, λ, μ)-partial difference set (PDS) is a subset D of a group G such that $|G| = v$, $|D| = k$, and every nonidentity element x of G can be written in either λ or μ different ways as a product gh^{-1}, depending on whether or not x is in D. Assuming the identity is not in D and D is inverse-closed, the corresponding Cayley graph $\mathrm{Cay}(G, D)$ will be strongly regular. Partial difference sets have been the subject of significant study, especially in abelian groups, but relatively little is known about PDSs in nonabelian groups. While many techniques useful for abelian groups fail to translate to a nonabelian setting, the purpose of this paper is to show that examples and constructions using abelian groups can be modified to generate several examples in nonabelian groups. In particular, in this paper we use such techniques to construct the 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}. Furthermore, 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, and, using analogues of product theorems for abelian groups, we obtain several examples of each. We conclude the paper with several possible future research directions.

1. Introduction

This work focuses on the algebraic structure known as a partial difference set (PDS). A (v, k, λ, μ)-PDS is a subset D of a group G such that $|G| = v$; $|D| = k$; every nonidentity element of D can be written as $d_1 d_2^{-1}$, where $d_1, d_2 \in D$, in λ different ways; and every nonidentity element of $G - D$ can be written as $d_1 d_2^{-1}$, where $d_1, d_2 \in D$, in μ different ways. These sets have received much attention due to their correspondences with strongly regular graphs, codes, bent functions, and association schemes.

Over the past few decades, numerous constructions of PDSs have been given in many *abelian* groups (for example, [6, 10, 15, 18, 19, 22, 25]). The methods nearly always include the use of characters, no doubt because they provide a relatively simple proof. Recent work has shed light on the fact that PDSs can be constructed in nonabelian groups as well, see for instance [3, 8, 9, 26, 30, 31]. We believe that nonabelian groups will provide many interesting examples of PDSs, even though relatively few examples are known in this setting (see [26, Sections 4–5] for a recent survey).

In a previous paper [26], the authors investigated PDSs in nonabelian groups for which there are no abelian PDSs with those parameters. In this situation, both the

Manuscript received 11th October 2023, revised 25th July 2024 and 16th December 2024, accepted 7th January 2025.

Keywords. partial difference set, difference set.

parameters and the PDS itself are called *genuinely nonabelian*. On the other end of the spectrum, there are examples of PDSs in nonabelian groups that are not genuinely nonabelian, such as in [9]; that is, given a (v, k, λ, μ)-PDS in an abelian group, there also exists a (v, k, λ, μ)-PDS in a nonabelian group. While one of the main themes of [26] is that many tools from the abelian setting simply do not apply to nonabelian groups, the purpose of this paper is to show that several constructions and existence results in abelian groups have direct analogues in nonabelian groups. In fact, in several instances, both the abelian group and the nonabelian group act on the same underlying combinatorial object (in this case, the same strongly regular graph).

The main results of this paper can be summarized as follows.

(1) Let q be a power of an odd prime p and $m \geqslant 2$. Then, there exist nonisomorphic, nonabelian groups of order q^{2m} and exponent p whose nonidentity elements can be partitioned into PDSs (Theorem 3.4, Remark 3.7, Theorem 3.9, Remark 3.10, Theorem 3.11).

(2) Let q be a power of an odd prime p. There exists a nonabelian group of order q^4 and exponent p that can be partitioned into $q+3$ PDSs, the union of any of which is also a PDS (Theorem 3.14). In particular, this group contains a Paley-type PDS (Corollary 3.15).

(3) Let $t \geqslant 2$ and p be an odd prime. The group
$$\widehat{G_t} := \left\langle x, y : x^{p^t} = y^{p^t} = 1, yxy^{-1} = x^{(p-1)p^{t-1}+1} \right\rangle \cong \mathbb{Z}_{p^t} \rtimes_{(p-1)p^{t-1}+1} \mathbb{Z}_{p^t}$$
can be partitioned into $2p$ PDSs in such a way that the union of any of them is also a PDS. In particular, there is a Paley-type PDS in $\widehat{G_t}$ (Theorem 4.6).

(4) If two groups G and G' of order v possess Paley-type PDSs, then the group $G \times G'$ also contains a Paley-type PDS (Theorem 5.1). Combined with the results of (2) and (3), this provides infinitely many more examples of Paley-type PDSs in nonabelian groups.

(5) If a group G of order v contains a Paley-type PDS and the group G' of order $v \pm 2$ contains a skew Hadamard difference set (DS), then the product group $G \times G'$ contains a Paley–Hadamard DS in the Stanton–Sprott (Twin prime power) family (Theorem 5.3). Combined with the results of (2) and (3), this provides more examples of Paley–Hadamard difference sets in nonabelian groups.

(6) In many cases, the group ring calculations needed to prove a product theorem in the abelian case (that is, the existence of PDSs in abelian groups G and G' imply the existence of a PDS in $G \times G'$) do not depend on whether or not the groups are abelian, meaning that they will automatically translate to the nonabelian setting (Lemma 6.1, Theorem 6.2).

To the best of our knowledge, the PDSs constructed in this paper are the first infinite families of PDSs in nonabelian groups of order q^d, where q is an odd prime power and d is not a multiple of 3. (Partial difference sets have been constructed in nonabelian groups of order q^3, where q is an odd prime power, in [30] and [26].) Moreover, in this paper 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 DSs in nonabelian groups.

This paper is organized as follows. Section 2 contains preliminary material related to PDSs, association schemes, and quadratic forms. In Section 3, we will use geometric techniques to construct families of PDSs in certain nonabelian groups or order q^{2m} and exponent p, where p is an odd prime and q is a power of p. In Section 4, we will use group ring equations from the abelian world to obtain PDSs in groups of the form $G = \mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{p^r}$ that have a large center, $Z(G) = pG \cong \mathbb{Z}_{p^{r-1}} \times \mathbb{Z}_{p^{r-1}}$.

Section 5 highlights new constructions of Paley-type PDSs and how they can be used to construct new difference sets using the twin prime power construction. In Section 6, we show that group ring equations will be forced to hold for various product constructions previously shown to work for abelian groups by characters. In this case, since the input group ring relations for the product are identical for the abelian case as for the nonabelian case we can avoid messy group ring equations. The product will take as input the nonabelian PDSs from Sections 3 and 4 and will generate new PDSs in many nonabelian groups. We conclude in Section 7 with some remarks and a considerable list of open problems.

2. Preliminaries

2.1. Partial difference sets. Let G be a finite group of order v with a subset D of order k. Suppose further that the differences $d_1{d_2}^{-1}$ for $d_1, d_2 \in D, d_1 \neq d_2$, represent each nonidentity element of G precisely λ times. Then, D is a (v, k, λ)-*difference set* (DS) in G.

Now suppose that G is a finite group of order v with a subset D of order k. Suppose further that the differences $d_1{d_2}^{-1}$ for $d_1, d_2 \in D, d_1 \neq d_2$, represent each nonidentity element of D exactly λ times and the nonidentity element of $G - D$ exactly μ times. Then, D is called a (v, k, λ, μ)-*partial difference set* (PDS) in G. The survey article of Ma is an excellent resource for these sets [17]. Typically, a proper PDS D for which $\lambda \neq \mu$ will have the two properties that the identity element from G is not in D and that $x \in D$ implies $x^{-1} \in D$, and such a PDS is called *regular*. A PDS having parameters $(n^2, r(n-1), n+r^2-3r, r^2-r)$ for some natural number r is called a *Latin square type PDS*. Similarly, a PDS having parameters $(n^2, r(n+1), -n+r^2+3r, r^2+r)$ is called a *negative Latin square type PDS*. Assuming the PDS is regular, the Cayley graph for a (v, k, λ, μ)-PDS will always be a *strongly regular graph* with the same parameters; that is, the corresponding Cayley graph has v vertices, every vertex has k neighbors, adjacent vertices have λ common neighbors, and nonadjacent vertices have μ common neighbors.

The earliest examples of PDSs date back to Paley [21], though his work long predates the systematic study of PDSs. Paley showed that the nonzero squares in $\mathbb{F}_q$ will be a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS in the additive group when q is a prime power and $q \equiv 1 \pmod 4$. We will call these *Paley partial difference sets*, and more generally $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$-PDSs will be *Paley-type partial difference sets*. This family of PDSs has received much attention in abelian groups. Davis was the first to construct Paley-type PDSs in groups that are not elementary abelian [6], work that was subsequently generalized in [16] and [27]. Polhill found examples where v was not a prime power in [24].

Paley [21] showed in the case when q is a prime power and $q \equiv 3 \pmod 4$ that the set of nonzero squares will instead be a $(q, \frac{q-1}{2}, \frac{q-3}{4})$-difference set, now called a *Paley–Hadamard difference set*. Stanton and Sprott found new examples of Paley–Hadamard difference sets [29] which are known as *Twin prime power difference sets* in the additive group of $\mathbb{F}_q \times \mathbb{F}_{q+2}$, when q and $q+2$ are both prime powers.

Partial difference sets are often studied within the context of the particular group ring $\mathbb{Z}[G]$, whether the group G is abelian or not. For a subset D of a group G, we abuse notation slightly and write $D := \sum_{d \in D} d$ and $D^{(-1)} := \sum_{d \in D} d^{-1}$. The following equation will then hold for a regular (v, k, λ, μ)-partial difference set D in the group G with identity 1_G:

$$DD^{(-1)} = DD = \lambda D + \mu(G - D - 1_G) + k1_G = (\lambda - \mu)D + \mu G + (k - \mu)1_G.$$

2.2. Association schemes. When studying PDSs, and in particular those with (negative) Latin square type parameters, one often has a partition of the nonidentity elements into multiple PDSs. As such, they form a multi-class association scheme, and so it will be helpful to consider these mathematical structures.

Let $\mathcal{X}$ be a finite set. An *association scheme* with d classes on $\mathcal{X}$ is a partition of $\mathcal{X} \times \mathcal{X}$ into sets R_0, $R_1, \ldots, R_d$ (relations, or associate classes) such that

(1) $R_0 = \{(x, x) : x \in \mathcal{X}\}$ (the diagonal relation);
(2) for each ℓ, $R_\ell^t = \{(y, x) : (x, y) \in R_\ell\} = R_{\ell'}$ for some ℓ';
(3) for all i, j, k in $\{0, 1, 2, \ldots, d\}$ there is an integer p_{ij}^k such that, for all $(x, y) \in R_k$,

$$|\{z \in \mathcal{X} : (x, z) \in R_i \text{ and } (z, y) \in R_j\}| = p_{ij}^k.$$

When $p_{ij}^k = p_{ji}^k$ for all k, i, j then the association scheme is called *commutative*. If $\ell = \ell'$ for all ℓ, then the association scheme is said to be *symmetric*; otherwise, it is *nonsymmetric*.

Each of the relations R_l can be interpreted as a directed graph with vertex set $\mathcal{X}$ and edge set R_l, $\Gamma_l = (\mathcal{X}, R_l)$ for all l. An association scheme can be viewed as a decomposition of the complete directed graph with vertex set $\mathcal{X}$ into directed graphs Γ_l with the property that for $i, j, k \in \{1, 2, \cdots d\}$ and for $xy \in E(\Gamma_k)$,

$$|\{z \in X : xz \in E(\Gamma_i) \text{ and } zy \in E(\Gamma_j)\}| = p_{ij}^k,$$

where $E(\Gamma_i)$ is edge set of graph Γ_i. The graphs Γ_i are called the *graphs* of the association scheme. Likewise, a symmetric association scheme can be viewed as a decomposition of the complete graph on vertex set $\mathcal{X}$ into undirected graphs. A strongly regular graph Γ corresponds to a symmetric association scheme with two classes, where $R_1 = \{(x, y) : xy \in E(\Gamma)\}$ and $R_2 = \{(x, y) : x \neq y \text{ and } (x, y) \notin R_1\}$.

For an association scheme, we can interpret the relations as adjacency matrices for the graphs, i.e. $\{0, 1\}$-matrices indexed by the vertex set V such that for the matrix A_i there is a 1 in position (x, y) exactly when $(x, y) \in R_i$. Then, we have:

(1) $A_0 = I$;
(2) $A_0 + A_1 + \cdots + A_d = J$, the matrix with all 1's;
(3) for each i there is some i' with ${A_i}^t = A_{i'}$;
(4) $A_i A_j = \Sigma_k {p_{ij}}^k A_k$.

This collection forms what is known as the *Bose–Mesner algebra*, and what is key for this article is that for a commutative association scheme it will necessarily follow that the Bose–Mesner algebra is commutative, so that the graph adjacency matrices satisfy $A_i A_j = A_j A_i$ for all i, j.

Given an association scheme, we can take unions of classes to produce graphs with larger edge sets, with such unions termed *fusions*. Fusions are not always association schemes in general, but when a particular association scheme has the property that any of its fusions also forms an association scheme we call the scheme *amorphic*. For an excellent introduction to amorphic association schemes, see [32].

It is not difficult to prove that d-class amorphic association schemes are symmetric when $d \geqslant 3$.

Lemma 2.1. *An amorphic association scheme with $d \geqslant 3$ classes is symmetric.*

Proof. Let $\{R_0, \ldots, R_t\}$ be an amorphic association scheme, $d > 2$, and suppose there exists i, $1 \leqslant i \leqslant d$, such that $R_i^t = R_j$, $j \neq i$. Without loss of generality, assume $R_1^t = R_2$. Consider the fusion $\{S_0, S_1, S_2\}$, where $S_0 = R_0$, $S_1 = R_1$, and $S_2 = \bigcup_{k \geqslant 2} R_k$. In this case, $S_1^t \neq S_0, S_1, S_2$, violating property (2) of association

schemes, a contradiction. Therefore, an amorphic association scheme with $d \geqslant 3$ classes is symmetric. □

Note that all association schemes with 2 classes are trivially amorphic. On the other hand, all association schemes we consider here are symmetric, since they correspond to edge-decompositions of the complete graph. Thus, for our purposes, all amorphic association schemes we consider are symmetric.

LEMMA 2.2. *Symmetric association schemes are commutative.*

Proof. Let $\{R_0, \ldots, R_d\}$ be a symmetric association scheme. We consider the associated adjacency matrices:

$$\sum_{k=0}^{d} p_{ji}^k A_k = A_j A_i = A_j^t A_i^t = (A_i A_j)^t = \left(\sum_{k=0}^{d} p_{ij}^k A_k \right)^t = \sum_{k=0}^{d} p_{ij}^k A_k^t = \sum_{k=0}^{d} p_{ij}^k A_k.$$

Since $\sum_{i=0}^{d} A_i = J$, this implies $p_{ji}^k = p_{ij}^k$ for all i, j, k, i.e. the association scheme is commutative. □

Thus, a symmetric association scheme is commutative, and hence any association scheme corresponding to a partition of the edges of a complete graph into strongly regular graphs is an amorphic, symmetric, and commutative association scheme.

Partial difference sets give rise to strongly regular Cayley graphs. When we partition the nonidentity elements of a group into partial difference sets, we also have a partition of the complete Cayley graph into strongly regular Cayley graphs.

Now we are ready to consider what will be an essential ingredient for many of the constructions in this article, a powerful result of van Dam:

THEOREM 2.3. [33, Theorem 3] *Let $\{\Gamma_1, \Gamma_2, \ldots, \Gamma_d\}$ be an edge-decomposition of the complete graph on a set X, where each Γ_i is strongly regular. If the Γ_i are all of Latin square type or all of negative Latin square type, then the decomposition is a d-class amorphic association scheme on X.*

We interpret the implications of this result into the context of PDSs to form the following, which we will use throughout the paper.

COROLLARY 2.4. *Suppose the nonidentity elements of a group G can be partitioned into a collection of PDSs all of Latin square type or all of negative Latin square type, $\{P_1, P_2, \ldots, P_n\}$. Then, a union of any number of these PDSs is also a PDS of that same type. Moreover, $P_i P_j = P_j P_i$ in the group ring $\mathbb{Z}[G]$.*

Proof. Such a collection of PDSs corresponds to a strongly regular Cayley graph decomposition of the complete graph on $|G|$ points, which will be amorphic by Theorem 2.3 and inherently symmetric, since the edges are undirected. As such, any fusion of the graph is a strongly regular graph of the same type as the PDSs P_i and therefore any union of PDSs $\bigcup_i P_i$ corresponds to another PDS of that type. By Lemma 2.2, the association scheme is commutative, and it follows that the graph adjacency matrices commute and therefore so do the group ring equations for the PDSs: i.e. $P_i P_j = P_j P_i$. □

We remark that such a partition of the nonidentity elements of a group G is called a *Cayley (association) scheme*. Cayley schemes are equivalent to *Schur rings* [14], and amorphic association schemes of (negative) Latin square type were previously used in [9] to construct examples of PDSs in nonabelian 2-groups.

2.3. Quadratic forms. Quadratic forms have been used for constructing PDSs of both Latin square type and negative Latin square type (see [17]). Let q be a power of a prime. We denote the field with q elements by $\mathbb{F}_q$. A *quadratic form* Q on a d-dimensional vector space $\mathbb{F}_q^d$ over $\mathbb{F}_q$ is a function $Q : \mathbb{F}_q^d \to \mathbb{F}_q$ such that:

(i) $Q(\alpha x) = \alpha^2 Q(x)$ for all $\alpha \in \mathbb{F}_q$ and all $x \in \mathbb{F}_q^d$, and
(ii) the function $\beta : \mathbb{F}_q^d \times \mathbb{F}_q^d \to \mathbb{F}_q$ given by $\beta(x, y) = Q(x + y) - Q(x) - Q(y)$ is $\mathbb{F}_q$-bilinear.

A quadratic form Q is said to be *nondegenerate* if $\beta(x, y) = 0$ for all $y \in \mathbb{F}_q^d$ implies $x = 0$. We have the following well-known result, which we state only for vector spaces of even dimension when q is odd. (For information about quadratic forms on $V = \mathbb{F}_q^n$, where n is odd and/or q is even, see [2, Theorem 3.28].)

Theorem 2.5. [2, Theorem 3.28] *Let Q be a nondegenerate quadratic form on $V = \mathbb{F}_q^{2m}$, where q is odd. There exists a basis for V such that exactly one of the following holds for all $x = (x_1, \ldots, x_{2m}) \in V$:*

(i) $Q(x) = x_1x_2 + x_3x_4 + \cdots + x_{2m-1}x_{2m}$, *or*
(ii) $Q(x) = x_1x_2 + x_3x_4 + \cdots + x_{2m-3}x_{2m-2} + x_{2m-1}^2 + bx_{2m}^2$, *where $-b$ is a nonsquare in $\mathbb{F}_q$.*

If (i) of Theorem 2.5 holds, then we say Q is *hyperbolic* and has type $\varepsilon = +1$ (often denoted simply with "+" when used as a superscript), and, if (ii) of Theorem 2.5 holds, then we say Q is *elliptic* and has type $\varepsilon = -1$ (often denoted simply with "−").

3. Nonabelian PDS families related to affine polar graphs

Let q be an odd prime power and $m \geqslant 2$. Let $V = \mathbb{F}_q^{2m}$ be equipped with a nondegenerate quadratic form Q of type $\varepsilon = \pm 1$. In particular, by Theorem 2.5, if $x = (x_1, \ldots, x_{2m}) \in V$, we will assume

$$Q(x) = x_1x_2 + x_3x_4 + \cdots + x_{2m-1}x_{2m}$$

if $\varepsilon = 1$, and we will assume

$$Q(x) = x_1x_2 + x_3x_4 + \cdots + x_{2m-3}x_{2m-2} + x_{2m-1}^2 + bx_{2m}^2,$$

where $-b$ is a nonsquare in $\mathbb{F}_q$, if $\varepsilon = -1$. Note that there is a nondegenerate symmetric bilinear form β associated with Q.

The graphs $\mathrm{VO}^\varepsilon(2m, q)$ are defined by taking the vectors in V to be vertices, with distinct vectors $u, v \in V$ adjacent if $Q(v - u) = 0$. As noted in [5, Section 3.3.1], $\mathrm{VO}^\varepsilon(2m, q)$ is a strongly regular graph with

$$\begin{aligned} v &= q^{2m}, \\ k &= (q^m - \varepsilon)(q^{m-1} + \varepsilon), \\ \lambda &= q(q^{m-1} - \varepsilon)(q^{m-2} + \varepsilon) + q - 2, \\ \mu &= q^{m-1}(q^{m-1} + \varepsilon). \end{aligned}$$

The graphs $\mathrm{VNO}^\varepsilon(2m, q)$ are defined by taking the vectors in V to be vertices, with distinct vectors $u, v \in V$ adjacent when $Q(u - v)$ is a nonzero square in $\mathbb{F}_q$. As

noted in [5, Section 3.3.2], the graph $\mathrm{VNO}^\varepsilon(2m,q)$ is a strongly regular graph with

$$\begin{aligned} v &= q^{2m}, \\ k &= \frac{1}{2}(q-1)(q^m-\varepsilon)q^{m-1}, \\ \lambda &= \frac{1}{4}q^{m-1}(q-1)(q^m-q^{m-1}-2\varepsilon)+\varepsilon q^{m-1}, \\ \mu &= \frac{1}{4}q^{m-1}(q-1)(q^m-q^{m-1}-2\varepsilon). \end{aligned}$$

Finally, we note that the complement to $\mathrm{VO}^\varepsilon(2m,q)\cup\mathrm{VNO}^\varepsilon(2m,q)$ in the complete graph on V will itself be a strongly regular graph isomorphic to $\mathrm{VNO}^\varepsilon(2m,q)$. To see this, note that this new graph has adjacency defined by $u\sim v$ when $Q(v-u)$ is a nonsquare in $\mathbb{F}_q$. If a is a nonsquare in $\mathbb{F}_q$, the map $\phi: v\mapsto av$ interchanges nonsquares with nonzero squares, and $Q(v^\phi-u^\phi)=Q(av-au)=a^2Q(v-u)$ is still a nonzero square if and only if $Q(v-u)$ is, meaning ϕ is an isomorphism between $\mathrm{VNO}^\varepsilon(2m,q)$ and this new complement graph, which we will denote by $\mathrm{VNO}_2^\varepsilon(2m,q)$. Therefore, the complete graph on V can be partitioned into $\mathrm{VO}^\varepsilon(2m,q)$, $\mathrm{VNO}^\varepsilon(2m,q)$, and $\mathrm{VNO}_2^\varepsilon(2m,q)$. We remark that when $\varepsilon=+1$ the graphs are of Latin square type, and when $\varepsilon=-1$ the graphs are of negative Latin square type. For an analysis of such graphs with q even, see [9].

3.1. Automorphisms of affine polar graphs. We represent the elements of the affine general linear group $\mathrm{AGL}(2m,q)$ in the form $[M,u]$, where $M\in\mathrm{GL}(2m,q)$ and $u\in V$, where for all (row vectors) $v\in V$,

$$v^{[M,u]} := vM+u,$$

and multiplication in $\mathrm{AGL}(2m,q)$ is defined by

$$[M_1,v_1][M_2,v_2]=[M_1M_2,v_1M_2+v_2].$$

The special orthogonal group $\mathrm{SO}^\varepsilon(2m,q)$ is the set of all determinant 1 matrices in $\mathrm{GL}(2m,q)$ preserving the bilinear form β (and quadratic form Q), and, given a subspace U of V, denote the subgroup of translations of V by vectors in U by T_U, i.e.

$$T_U := \{[I,u] : u\in U\},$$

where I is the $2m\times 2m$ identity matrix. Hence,

$$\mathrm{ASO}^\varepsilon(2m,q) := \{[M,v] : M\in\mathrm{SO}^\varepsilon(2m,q), v\in V\}\cong T_V\rtimes\mathrm{SO}^\varepsilon(2m,q),$$

where the semidirect product denotes the natural action of $\mathrm{SO}^\varepsilon(2m,q)$ on T_V and $M\in\mathrm{SO}^\varepsilon(2m,q)$ is identified naturally with $[M,0]\in\mathrm{AGL}(2m,q)$.

Lemma 3.1. *The group* $\mathrm{ASO}^\varepsilon(2m,q)$ *is a subgroup of automorphisms of each of* $\mathrm{VO}^\varepsilon(2m,q)$, $\mathrm{VNO}^\varepsilon(2m,q)$, *and* $\mathrm{VNO}_2^\varepsilon(2m,q)$.

Proof. Let $[M,w]\in\mathrm{ASO}^\varepsilon(2m,q)$ and $u,v\in V$. Then,

$$Q(v^{[M,w]}-u^{[M,w]})=Q((vM+w)-(uM+w))=Q((v-u)M)=Q(v-u),$$

and so $[M,w]$ preserves adjacency in all three graphs. □

We could have chosen $T_V\rtimes\mathrm{GO}^\varepsilon(2m,q)$, where $\mathrm{GO}^\varepsilon(2m,q)$ is the general orthogonal group, in Lemma 3.1; however, in the coming sections, we will be interested in p-elements of these groups, where q is a power of p, and thus it suffices to consider $\mathrm{ASO}^\varepsilon(2m,q)$.

Remark 3.2. Note that $T_V \subseteq \mathrm{ASO}^\varepsilon(2m,q)$ is an elementary abelian regular subgroup of automorphisms of each of $\mathrm{VO}^\varepsilon(2m,q)$, $\mathrm{VNO}^\varepsilon(2m,q)$, and $\mathrm{VNO}_2^\varepsilon(2m,q)$, and so the corresponding decomposition of the nonidentity elements of T_V into PDSs is an amorphic Cayley scheme. In the following subsections, we will find "twists" of the group T_V in $\mathrm{ASO}^\varepsilon(2m,q)$ – roughly speaking, replacing certain translations $[I,v]$ by elements of the form $[M,v]$, where $M \neq I$ – to provide new examples of PDSs in nonabelian groups. The constructions in this section produce isomorphic association schemes to the known amorphic Cayley scheme in T_V.

3.2. A family of PDSs in nonabelian groups of order q^{2m}. Fix $\varepsilon = \pm 1$. Let v be a nonsingular vector in V, i.e. $Q(v) \neq 0$, so $\langle v \rangle$ is a nonsingular subspace. The stabilizer of $\langle v \rangle$ in $\mathrm{SO}^\varepsilon(2m,q)$ contains an elementary abelian group H of order q; see, e.g. [4, Sections 2.2.1, 8.2], [13, Tables 3.5 E, F and Proposition 4.1.6], or [34, Section 3.7.4]. Note that $vM = v$ for all $M \in H$: we know that $0M = 0$, and that $vM = v$ follows from the Orbit-Stabilizer Theorem.

Since v is nonsingular, we have $V = \langle v \rangle \oplus v^\perp$, where

$$v^\perp := \{u \in V : \beta(u,v) = 0\};$$

to see this, note that the map $\beta(-,v) : V \to \mathbb{F}_q$ is a linear transformation with kernel $v^\perp$. Since $vM = v$ for all $M \in H$ and M preserves β, we have $v^\perp M = v^\perp$, i.e. $v^\perp$ is an H-invariant subspace.

Remark 3.3. Choosing a nonsingular vector v is not strictly necessary for this construction: as long as the elementary abelian group H stabilizes a decomposition $V = \langle v \rangle \oplus U$ for some complementary subspace U to $\langle v \rangle$, the construction will work.

Since H is an elementary abelian group of order q, H is naturally isomorphic to $(\mathbb{F}_q, +)$. For each $\alpha \in \mathbb{F}_q$, we will denote by A_α the corresponding element of H under this natural isomorphism. Define

$$\mathcal{A} := \{[A_\alpha, \alpha v] : \alpha \in \mathbb{F}_q\}.$$

Since v is fixed by right multiplication by elements of H, $\mathcal{A}$ is an elementary abelian group of order q that is itself naturally identified with $(\mathbb{F}_q, +)$.

Recall that $T_{v^\perp}$ is the set of elements of the form $[I,u]$ for $u \in v^\perp$. Then, for $u \in v^\perp$, we have

$$[A_\alpha, \alpha v]^{-1}[I,u][A_\alpha, \alpha v] = [A_\alpha^{-1}, -\alpha v][I,u][A_\alpha, \alpha v] = [I, uA_\alpha] \in T_{v^\perp},$$

so $\mathcal{A}$ normalizes $T_{v^\perp}$.

Define

$$G_1^\varepsilon := \langle T_{v^\perp}, \mathcal{A} \rangle = T_{v^\perp} \rtimes \mathcal{A}.$$

Theorem 3.4. *The group G_1^ε is a nonabelian group of order q^{2m} in which the nonidentity elements can be partitioned into $D_0 \cup D_1 \cup D_2$, where each D_i is a PDS,* $\mathrm{Cay}(G_1^\varepsilon, D_0) \cong \mathrm{VO}^\varepsilon(2m,q)$, *and* $\mathrm{Cay}(G_1^\varepsilon, D_1) \cong \mathrm{Cay}(G_1^\varepsilon, D_2) \cong \mathrm{VNO}^\varepsilon(2m,q)$.

Proof. First, we have $|G_1^\varepsilon| = q^{2m}$ since $G_1^\varepsilon = T_{v^\perp} \rtimes \mathcal{A}$, $|T_{v^\perp}| = |v^\perp| = q^{2m-1}$, and $|\mathcal{A}| = q$. Moreover, since H acts faithfully on V and fixes $\langle v \rangle$ pointwise, there exist $u \in v^\perp$ and $A \in H$ such that $uA \neq u$. Since $A \in H$, there is a unique $w \in \langle v \rangle$ such that $[A,w] \in \langle \mathcal{A} \rangle$. Thus,

$$[I,u][A,w] = [A, uA + w] \neq [A, u + w] = [A,w][I,u],$$

and hence G_1^ε is nonabelian.

Let $x \in V$. Then, we may write $x = w + u$, where $w \in \langle v \rangle$ and $u \in v^\perp$. There is a unique $A \in H$ such that $[A,w] \in \mathcal{A}$, and so $[A,x] = [A, w+u] = [A,w][I,u]$ is an

element of G_1^ε such that $0^{[A,x]} = x$, and hence G_1^ε is transitive on V. Since $|G_1^\varepsilon| = |V|$, in fact G_1^ε acts regularly on V.

Finally, since $A \in \mathrm{SO}^\varepsilon(2m, q)$ for all $[A, x] \in G_1^\varepsilon$, $G_1^\varepsilon \leqslant \mathrm{ASO}^\varepsilon(2m, q)$, and, by Lemma 3.1, G_1^ε is a subgroup of automorphisms of $\mathrm{VO}^\varepsilon(2m, q)$, $\mathrm{VNO}^\varepsilon(2m, q)$, and $\mathrm{VNO}_2^\varepsilon(2m, q)$. The result follows. □

Example 3.5. We can construct a concrete example for each ε, q, and m. When $\varepsilon = 1$, for $\alpha \in \mathbb{F}_q$ we define

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

and when $\varepsilon = -1$, for $\alpha \in \mathbb{F}_q$ we define

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

Then, we may choose

$$A_\alpha := \left(\begin{array}{c|c} I_{2m-4} & 0 \\ \hline 0 & C_\alpha \end{array}\right).$$

Let $\{e_i : 1 \leqslant i \leqslant 2m\}$ be the standard basis for V. Then, we may choose $v = e_1 + e_2$ if $\varepsilon = 1$ and $v = e_2$ if $\varepsilon = -1$.

Example 3.6. As another example, if $m > 2$, for $\alpha \in \mathbb{F}_q$, if

$$B_\alpha := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -\alpha & 0 \\ 0 & 0 & 1 & 0 \\ \alpha & 0 & 0 & 1 \end{pmatrix},$$

then we may choose

$$A_\alpha := \left(\begin{array}{c|c} B_\alpha & 0 \\ \hline 0 & I_{2m-4} \end{array}\right)$$

with $v = e_5 + e_6$ (regardless of the value of ε). Thus, when $m > 2$, we may actually assume $G_1^+ = G_1^-$.

Remark 3.7. Every element of G_1^ε can be expressed uniquely as $[A_\alpha, \alpha v + u]$, where $\alpha \in \mathbb{F}_q$ and $u \in v^\perp$. Since

$$[A_\alpha, \alpha v + u]^p = \left[A_\alpha^p, p\alpha v + u \sum_{i=0}^{p-1} A_\alpha^i\right] = \left[I, u(A_\alpha - I)^{p-1}\right],$$

the choices of A_α from Examples 3.5 and 3.6 show that, when $p > 3$ or $m > 2$, we can choose G_1^ε to have exponent p. That such groups can be chosen to have exponent 3 when $p = 3$ and $m = 2$ follows from direct inspection with GAP [11].

3.3. A second family of PDSs in nonabelian groups of order q^{2m}. The second family of PDSs requires a bit more care. We will assume for this construction that either $m > 2$ or, if $m = 2$, $\varepsilon = 1$. As in Example 3.6, for $\alpha \in \mathbb{F}_q$, if

$$B_\alpha := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -\alpha & 0 \\ 0 & 0 & 1 & 0 \\ \alpha & 0 & 0 & 1 \end{pmatrix},$$

we then define

$$A_\alpha := \left(\begin{array}{c|c} B_\alpha & 0 \\ \hline 0 & I_{2m-4} \end{array}\right).$$

(Again, we allow $m = 2$ as long as the quadratic form Q is hyperbolic.) In this case, $H := \{A_\alpha : \alpha \in \mathbb{F}_q\}$ is an elementary abelian group of order q preserving the form Q. Define

$$U := \langle e_1, e_4, e_5, e_6, \ldots, e_{2m} \rangle .$$

Direct calculation shows that U is an H-invariant subspace of V.

Define

$$\mathcal{B} := \langle [A_\alpha, \alpha e_2 + \beta e_3] : \alpha, \beta \in \mathbb{F}_q \rangle .$$

Lemma 3.8. *The group $\mathcal{B}$ is an elementary abelian group of order q^2. In particular, for each $w \in \langle e_2, e_3 \rangle$, there exists a unique element $[A, x] \in \mathcal{B}$ with $x = w$.*

Proof. Noting that H fixes e_3, a direct calculation shows that, for all $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$, we have

$$\begin{aligned}[A_\alpha, \alpha e_2 + \beta e_3][A_\gamma, \gamma e_2 + \delta e_3] &= [A_\gamma, \gamma e_2 + \delta e_3][A_\alpha, \alpha e_2 + \beta e_3] \\ &= [A_{\alpha+\gamma}, (\alpha + \gamma)e_2 + (\beta + \delta - \alpha\gamma)e_3].\end{aligned}$$

The result follows. □

Recalling that U is H-invariant, for any $u \in U$, we have

$$\begin{aligned}[A_\alpha, \alpha e_2 + \beta e_3]^{-1}[I, u][A_\alpha, \alpha e_2 + \beta e_3] &= [A_\alpha^{-1}, -\alpha e_2 - (\alpha^2 + \beta)e_3][I, u][A_\alpha, \alpha e_2 + \beta e_3] \\ &= [I, uA_\alpha] \in T_U,\end{aligned}$$

so $\mathcal{B}$ normalizes T_U.

Define

$$G_2 := \langle T_U, \mathcal{B} \rangle = T_U \rtimes \mathcal{B}.$$

Theorem 3.9. *Let $m > 2$ or, if $m = 2$, then $\varepsilon = 1$. The group G_2 is a nonabelian group of order q^{2m} in which the nonidentity elements can be partitioned into $D_0 \cup D_1 \cup D_2$, where each D_i is a PDS,* $\mathrm{Cay}(G_2, D_0) \cong \mathrm{VO}^\varepsilon(2m, q)$, *and* $\mathrm{Cay}(G_2, D_1) \cong \mathrm{Cay}(G_2, D_2) \cong \mathrm{VNO}^\varepsilon(2m, q)$.

Proof. The proof is largely the same as that of Theorem 3.4. First, we have $|G_2| = q^{2m}$ since $G_2 = T_U \rtimes \mathcal{B}$, $|T_U| = |U| = q^{2m-2}$, and $|\mathcal{B}| = q^2$. Moreover, not all vectors in U are fixed by H; for example, $e_4 A_1 = e_1 + e_4$, and so

$$[I, e_4][A_1, e_2] = [A_1, e_1 + e_2 + e_4] \neq [A_1, e_2 + e_4] = [A_1, e_2][I, e_4],$$

and hence G_2 is nonabelian.

Let $x \in V$. Then, we may write $x = w + u$, where $w \in \langle e_2, e_3 \rangle$ and $u \in U$. There is a unique $A \in H$ such that $[A, w] \in \mathcal{B}$, and so $[A, x] = [A, w + u] = [A, w][I, u]$ is an element of G_2 such that $0^{[A,x]} = x$, and hence G_2 is transitive on V. Since $|G_2| = |V|$, in fact G_2 acts regularly on V.

Finally, since $A \in \mathrm{SO}^\varepsilon(2m, q)$ for all $[A, x] \in G_2$, $G_2 \leqslant \mathrm{ASO}^\varepsilon(2m, q)$, and, by Lemma 3.1, G_2 is a subgroup of automorphisms of $\mathrm{VO}^\varepsilon(2m, q)$, $\mathrm{VNO}^\varepsilon(2m, q)$, and $\mathrm{VNO}_2^\varepsilon(2m, q)$. The result follows. □

Remark 3.10. A similar calculation to that done in Remark 3.7 shows that G_2 has exponent p.

Theorem 3.11. *Let $m > 2$ or, if $m = 2$, then $\varepsilon = +1$. The groups G_1^ε and G_2 are not isomorphic.*

Proof. If $m > 2$, we can choose H to be the same group in each case. If W is the subspace of points fixed by H, then

$$W = \langle e_1, e_3, e_5, \ldots, e_{2m} \rangle,$$

which has dimension $2m-2$. In each case, the central elements are of the form $[I, w]$, where $w \in W$. Since $v = e_5 + e_6 \in W$, $|Z(G_1^\varepsilon)| = q^{2m-3}$. On the other hand, $|Z(G_2)| = |W| = q^{2m-2}$, which proves the claim for $m > 2$

The proof is similar when $m = 2$ and $\varepsilon = 1$: when $A_\alpha = C_\alpha$ (as in Example 3.5), we see that the subspace of of points fixed by H is $W = \langle e_1 + e_2, e_4 \rangle$, and, since $v = e_1 + e_2$,

$$Z(G_1^+) = \{[I, \beta e_4] : \beta \in \mathbb{F}_q\}.$$

Thus, $|Z(G_1^+)| = q$. On the other hand,

$$Z(G_2) = \{[I, w] : w \in W\},$$

and so $|Z(G_2)| = q^2$, which proves the claim when $m = 2$ and $\varepsilon = 1$. □

3.4. A $(q+3)$-class amorphic association scheme in a group of order q^4. Let $V = GF(q)^4$, where q is an odd prime. Let $Q(x) = x_1x_2 + x_3x_4$, a hyperbolic form on V, and consider the group

$$G := G_2 = T_U \rtimes \mathcal{B}$$

defined in Subsection 3.3, and define

$$H := \{B_\alpha : \alpha \in \mathbb{F}_q\}.$$

As in Theorem 3.9, we take D_0 to be the elements $[C, x]$ in G where $Q(x) = 0$; D_1 to be the elements $[C, x]$ in G where $Q(x)$ is a nonzero square; and D_2 to be the elements $[C, x]$ in G where $Q(x)$ is a nonzero nonsquare. Since each vector x in V occurs exactly once as the second component of an element $[C, x] \in G$, we may identify the elements of G with the corresponding vector in the second component. In other words, we identify D_0 with the set V_0 of vectors x in V such that $Q(x) = 0$, D_1 with the set V_1 of vectors x in V such that $Q(x)$ is a nonzero square, and D_2 with the set V_2 of vectors x in V such that $Q(x)$ is a nonsquare.

Lemma 3.12. *The set V_0 can be partitioned into $q+1$ disjoint subsets of size q^2-1, where each subset is the set of nonzero vectors in a 2-dimensional subspace of V. Moreover, we can take each subset of the partition of V_0 to be H-invariant.*

Proof. To see that we have a H-invariant partition for V_0, we define $v_\infty := e_4 = (0, 0, 0, 1)$ and, for each $\alpha \in \mathbb{F}_q$, we define $v_\alpha := e_2 + \alpha e_4 = (0, 1, 0, \alpha)$. Since $Q(v_\alpha) = 0$, both $v_\alpha, v_\alpha B \in V_0$ for all $B \in H$. Moreover, if we define $u_\infty := e_1 = (1, 0, 0, 0)$, $u_\alpha := \alpha e_1 - e_3 = (\alpha, 0, -1, 0)$ for $\alpha \in \mathbb{F}_q$, and $U_\alpha := \langle v_\alpha, u_\alpha \rangle$, for each $\alpha \in \mathbb{F}_q \cup \{\infty\}$ and $\beta \in \mathbb{F}_q$, we have

$$v_\alpha B_\beta = v_\alpha + \beta u_\alpha \in U_\alpha.$$

Since $u_\alpha \in \langle e_1, e_3 \rangle$, $u_\alpha B_\beta = u_\alpha$ for each α, β, and thus each U_α is an H-invariant subspace. It is routine to check that the $q+1$ subspaces U_α, $\alpha \in \mathbb{F}_q \cup \{\infty\}$ are pairwise disjoint, and since $|V_0| = (q+1)(q^2-1)$, these subspaces form an H-invariant partition of V. □

Proposition 3.13. *Let $D \subset V$ be a H-invariant subset of V, and view $(V, +)$ as the elementary abelian group of order q^4. Then, G is isomorphic to a regular subgroup of* $\mathrm{Aut}(\mathrm{Cay}(V, D))$*; that is, if*

$$D' := \{[C, x] \in G : x \in D\},$$

then $\mathrm{Cay}(G, D') \cong \mathrm{Cay}(V, D)$.

Proof. Viewing V additively, we then can define the graph $\mathrm{Cay}(V, D)$, where vectors v and w are adjacent iff $v - w \in D$. For any $[C, x] \in G$, we have

$$v^{[C,x]} - w^{[C,x]} = (vC + x) - (wC + x) = (v - w)C,$$

and so $v - w \in D$ iff $v^{[C,x]} - w^{[C,x]} \in D$. Since G is transitive on V and preserves adjacency in $\mathrm{Cay}(V, D)$, the result follows. □

Recall the definitions of D_1 and D_2 in G from above. Let $\mathbb{F}_q \cup \{\infty\} = \{\alpha_3, \ldots, \alpha_{q+3}\}$, define

$$U_i := U_{\alpha_i}$$

as in the proof of Lemma 3.12, and define

$$D_i := \{[C, x] \in G : x \in U_i - \{0\}\}.$$

Theorem 3.14. *Each D_i, $1 \leqslant i \leqslant q + 3$, is a PDS of Latin square type in G. Consequently, $\{D_i : 1 \leqslant i \leqslant q + 3\}$ corresponds to a $(q + 3)$-class amorphic association scheme, and a union of any number of these PDSs is also a PDS of Latin square type in G.*

Proof. First, D_1 and D_2 are PDSs of Latin square type in G with $r = q(q - 1)/2$ by Theorem 3.9.

Since each U_i is a subspace of size q^2, each graph $\mathrm{Cay}(V, U_i - \{0\})$ is a union of disjoint complete subgraphs, i.e. each graph $\mathrm{Cay}(V, U_i - \{0\})$ is a $(q^4, q^2 - 1, q^2 - 2, 0)$-strongly regular graph of Latin square type. By Proposition 3.13, this means each D_i, $3 \leqslant i \leqslant q + 3$ is also a PDS of Latin square type. Finally, since $\{D_i : 3 \leqslant i \leqslant q + 3\}$ is a partition of D_0 and $\{D_0, D_1, D_2\}$ is a partition of G, $\{D_i : 1 \leqslant i \leqslant q + 3\}$ is a $(q + 3)$-class amorphic association scheme. The result follows from Corollary 2.4. □

Corollary 3.15. *The group G contains a Paley-type PDS.*

Proof. Define

$$D := D_1 \cup \bigcup_{i=3}^{(q+5)/2} D_i,$$

i.e. D is the union of D_1 and half of the D_i's, where $i \geqslant 3$. By Theorem 3.14, D is a PDS of Latin square type, and, since D contains the elements of D_1 and exactly half of the elements of D_0,

$$|D| = \frac{q(q-1)(q^2-1)}{2} + \frac{(q+1)(q^2-1)}{2} = \frac{q^4 - 1}{2}.$$

The result follows. □

4. Partial difference sets in semidirect products with a large center

Let p be a prime, and define $G := \left\langle x, y : x^{p^2} = y^{p^2} = 1, xy = yx \right\rangle \cong \mathbb{Z}_{p^2}^2$. The following sets were shown in [6] to be $(p^4, p(p^2 - 1), 2p^2 - 3p, p^2 - p)$-PDSs in G for $1 \leqslant i \leqslant p - 1$:

$$P_i = \left(\bigcup_{j=0}^{p-1} \left(\left\langle xy^{j+pi} \right\rangle - \left\langle x^p y^{pj} \right\rangle \right) \right) \cup \left(\left\langle x^{pi} y \right\rangle - \left\langle y^p \right\rangle \right).$$

The following subgroups with the identity removed are trivial $(p^2, p^2 - 1, p^2 - 2, 0)$-PDSs:

$$S_j = \left\langle xy^j \right\rangle - \{1\} \text{ for } 0 \leqslant j \leqslant p - 1, S_\infty = \langle y \rangle - \{1\}.$$

The P_i and S_j partition the nonidentity elements of G into Latin square type PDSs. The next theorem applies Theorem 2.3 to this collection.

THEOREM 4.1. *The collection* $\{P_1, P_2, \ldots, P_{p-1}, S_0, S_1, \ldots, S_{p-1}, S_\infty\}$ *is a* $2p$*-class amorphic association scheme on* G*.*

Combining Corollary 2.4 with Theorem 4.1 implies that

$$D := \left(\bigcup_{j=1}^{\frac{p-1}{2}} P_i\right) \cup \left(\bigcup_{j=0}^{\frac{p-1}{2}} S_j\right)$$

is a Paley-type $\left(p^4, \frac{p^4-1}{2}, \frac{p^4-5}{4}, \frac{p^4-1}{4}\right)$-PDS.

This construction was the first known PDS with Paley-type parameters in a group that was not elementary abelian; other abelian PDSs with these parameters have since appeared (see, for instance, [27]).

We now show that a similar construction will produce Paley-type PDSs in certain nonabelian groups, which along with the construction in the previous section (Corollary 3.15) are the first such constructions of Paley-type PDSs in nonabelian groups known to these authors. Consider the group

$$\widehat{G_2} := \left\langle x, y : x^{p^2} = y^{p^2} = 1, yxy^{-1} = x^{p^2-p+1} \right\rangle \cong \mathbb{Z}_{p^2} \rtimes_{p^2-p+1} \mathbb{Z}_{p^2}.$$

Define

$$\widehat{P_i} := \left(\bigcup_{j=0}^{p-1} \left(\left\langle xy^{j+pi}\right\rangle - \left\langle x^p y^{pj}\right\rangle\right)\right) \cup \left(\left\langle x^{pi}y\right\rangle - \left\langle y^p\right\rangle\right)$$

and $\widehat{S_j} := \left\langle xy^j\right\rangle - \{1\}$ for $0 \leqslant j \leqslant p-1$, $\widehat{S_\infty} := \langle y\rangle - \{1\}$, and finally

$$\widehat{D_2} := \left(\bigcup_{j=1}^{\frac{p-1}{2}} \widehat{P_i}\right) \cup \left(\bigcup_{k=0}^{\frac{p-1}{2}} \widehat{S_k}\right).$$

We note that the formal sets P_i and $\widehat{P_i}$ appear the same, but the element $(xy^{p+1})^2 = x^2y^{2p+2} \in P_1$ whereas $(xy^{p+1})^2 = x^{p^2+2}y^2 \in \widehat{P_1}$.

In order to demonstrate that $\widehat{P_i}$ is a PDS, we first prove two lemmas that we will use in the proof of the result.

LEMMA 4.2. *Let* $1 \leqslant i \leqslant (p-1)$*. For the group* $\widehat{G_2}$ *and the subset* $\widehat{P_i}$ *defined above, we have*

$$\sum_{j=0}^{p-1} \left((p^2-2p)\left\langle xy^{ip+j}\right\rangle + p\left\langle x^p y^{pj}\right\rangle\right) + (p^2-2p)\left\langle x^{ip}y\right\rangle + p\left\langle y^p\right\rangle$$

$$= (p^2-p)(p+1)1_{\widehat{G_2}} + (p^2-2p)\widehat{P_i} + (p^2-p)\left\langle x^p, y^p\right\rangle.$$

Proof. All of the elements of $\widehat{P_i}$ of order p^2 will appear (p^2-2p) times, and all of the elements of $\langle x^p, y^p\rangle$ will appear an additional p times. □

LEMMA 4.3. *For* $j, j' \in \{0, 1, \ldots, p-1\}$ *we have*

$$\sum_{j\neq j'} \left(\left\langle xy^{ip+j}\right\rangle - \left\langle x^p y^{pj}\right\rangle\right)\left(\left\langle xy^{ip+j'}\right\rangle - \left\langle x^p y^{pj'}\right\rangle\right)$$

$$+ \sum_{j=0}^{p-1} \left(\left\langle xy^{ip+j}\right\rangle - \left\langle x^p y^{pj}\right\rangle\right)\left(\left\langle x^{ip+j}y\right\rangle - \left\langle x^{pj}y^p\right\rangle\right) = (p^2-p)\widehat{G_2} - (p^2-p)\left\langle x^p, y^p\right\rangle.$$

Proof. A symmetry argument implies that all of the elements of order p^2 appear the same number of times in this sum, and the fact that these are different values of j, j' implies that we will not get any elements of order p. The result follows from a counting argument. □

Theorem 4.4. *Let p be a prime. The collection $\{\widehat{P_1}, \widehat{P_2}, \ldots, \widehat{P_{p-1}}, \widehat{S_0}, \widehat{S_1}, .., \widehat{S_{p-1}}, \widehat{S_\infty}\}$ is a $2p$-class amorphic association scheme on $\widehat{G_2}$ and the set $\widehat{D_2}$ is a Paley-type $\left(p^4, \frac{p^4-1}{2}, \frac{p^4-5}{4}, \frac{p^4-1}{4}\right)$-PDS in G_2.*

Proof. Since the $\widehat{S_i}$ are all subgroups, they are all (trivial) Latin square type PDSs, and Lemmas 4.2 and 4.3 imply the following.

$$\begin{aligned}
\widehat{P_i}^2 = & \sum_{j=0}^{p-1} \left(\left\langle xy^{ip+j}\right\rangle - \left\langle x^p y^{pj}\right\rangle\right)^2 + \left(\langle x^p y\rangle - \langle y^p\rangle\right)^2 \\
& + \sum_{j\neq j'} \left(\left\langle xy^{ip+j}\right\rangle - \left\langle x^p y^{pj}\right\rangle\right)\left(\left\langle xy^{ip+j'}\right\rangle - \left\langle x^p y^{pj'}\right\rangle\right) \\
& + \sum_{j=0}^{p-1} \left(\left\langle xy^{ip+j}\right\rangle - \left\langle x^p y^{pj}\right\rangle\right)\left(\left\langle x^{ip+j} y\right\rangle - \left\langle x^{pj} y^p\right\rangle\right) \\
= & (p^2-p)(p+1)1_{\widehat{G_2}} + (p^2-2p)\widehat{P_i} + (p^2-p)\left\langle x^p, y^p\right\rangle + (p^2-p)\widehat{G_2} - (p^2-p)\left\langle x^p, y^p\right\rangle \\
= & (p^3-p)1_{\widehat{G_2}} + (p^2-2p)\widehat{P_i} + (p^2-p)\widehat{G_2} \\
= & (p^3-p)1_{\widehat{G_2}} + (2p^2-3p)\widehat{P_i} + (p^2-p)(\widehat{G_2} - \widehat{P_i} - 1_{\widehat{G_2}})
\end{aligned}$$

Thus, the $\widehat{P_i}$ are all $(p^4, p^3-p, 2p^2-3p, p^2-p)$-PDSs in $\widehat{G_2}$ as claimed. Since these are all Latin square type PDSs, Corollary 2.4 implies that any union of these PDSs will be a PDS. In particular,

$$\widehat{D_2} = \left(\bigcup_{j=1}^{\frac{p-1}{2}} \widehat{P_i}\right) \cup \left(\bigcup_{k=0}^{\frac{p-1}{2}} \widehat{S_i}\right)$$

is a $\left(p^4, \frac{p^4-1}{2}, \frac{p^4-5}{4}, \frac{p^4-1}{4}\right)$-PDS as required. □

We now turn to a generalization of this construction. Let

$$G_t = \left\langle x, y : x^{p^t} = y^{p^t} = 1, xy = yx\right\rangle \cong \mathbb{Z}_{p^t} \times \mathbb{Z}_{p^t}.$$

Polhill [27] showed that the sets $P_{t,i}$ are Latin square type PDSs with parameters

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

in G_t for $1 \leqslant i \leqslant p-1$, where $P_{t,i}$ is defined to be

$$\bigcup_{r=1}^{t-1} \bigcup_{j=0}^{p^{r-1}-1} \left(\bigcup_{k=0}^{p-1} \left(\left\langle xy^{ip^r+pj+k}\right\rangle - \left\langle x^{p^{t-r}} y^{jp^{t+1-r}+kp^{t-r}}\right\rangle\right)\right) \cup \left(\left\langle x^{ip^r+jp} y\right\rangle - \left\langle x^{jp^{t-r+1}} y^{p^{t-r}}\right\rangle\right).$$

If we define $S_{t,j} := \left\langle xy^j\right\rangle - \{1_{G_t}\}, 0 \leqslant j \leqslant p-1$, and $S_{t,\infty} := \langle y\rangle - \{1_{G_t}\}$, then we get the following theorem, which is analogous to Theorem 4.1.

Theorem 4.5. *For $t \geqslant 2$, $\{P_{t,1}, P_{t,2}, \ldots, P_{t,p-1}, S_{t,0}, S_{t,1}, \ldots, S_{t,p-1}, S_{t,\infty}\}$ is a $2p$-class amorphic association scheme on G_t.*

The combination of Corollary 2.4 and Theorem 4.5 imply that

$$D_t := \left(\bigcup_{i=1}^{\frac{p-1}{2}} P_{t,i}\right) \cup \left(\bigcup_{j=0}^{\frac{p-1}{2}} S_{t,j}\right)$$

is a Paley-type $\left(p^{2t}, \frac{p^{2t}-1}{2}, \frac{p^{2t}-5}{4}, \frac{p^{2t}-1}{4}\right)$-PDS in G_t.

We now construct Paley-type PDSs in the nonabelian group

$$\widehat{G_t} := \left\langle x, y : x^{p^t} = y^{p^t} = 1, yxy^{-1} = x^{(p-1)p^{t-1}+1} \right\rangle \cong \mathbb{Z}_{p^t} \rtimes_{(p-1)p^{t-1}+1} \mathbb{Z}_{p^t}.$$

To do this, we define a collection of disjoint PDSs that partition the nonidentity elements of $\widehat{G_t}$ in an analogous fashion as those defined in G_t: first, we define $\widehat{P_{t,i}}$ to be

$$\bigcup_{r=1}^{t-1}\bigcup_{j=0}^{p^{r-1}-1}\left(\bigcup_{k=0}^{p-1}\left(\left\langle xy^{ip^r+pj+k}\right\rangle - \left\langle x^{p^{t-r}}y^{jp^{t+1-r}+kp^{t-r}}\right\rangle\right)\right) \cup \left(\left\langle x^{ip^r+jp}y\right\rangle - \left\langle x^{jp^{t-r+1}}y^{p^{t-r}}\right\rangle\right);$$

then we define

$$\widehat{S_{t,j}} := \left\langle xy^j \right\rangle - \{1_{\widehat{G_t}}\},$$
$$\widehat{S_{t,\infty}} := \langle y \rangle - \{1_{\widehat{G_t}}\}.$$

The main construction in this section is the following, and along with those examples in the previous section are the first examples of Paley-type PDSs in nonabelian groups known to the authors.

THEOREM 4.6. *For $t \geqslant 2$, $\{\widehat{P_{t,1}}, \widehat{P_{t,2}}, \ldots, \widehat{P_{t,p-1}}, \widehat{S_{t,0}}, \widehat{S_{t,1}}, \ldots, \widehat{S_{t,p-1}}, \widehat{S_{t,\infty}}\}$ is a $2p$-class amorphic association scheme on $\widehat{G_t}$. Therefore,*

$$\widehat{D_t} := \left(\bigcup_{i=1}^{\frac{p-1}{2}} \widehat{P_{t,i}}\right) \cup \left(\bigcup_{j=0}^{\frac{p-1}{2}} \widehat{S_{t,j}}\right)$$

is a Paley-type $\left(p^{2t}, \frac{p^{2t}-1}{2}, \frac{p^{2t}-5}{4}, \frac{p^{2t}-1}{4}\right)$-PDS in $\widehat{G_t}$.

The proof uses the same reasoning as the proof of Theorem 4.4 and is left for the reader.

REMARK 4.7. Computational evidence suggests that the amorphic association schemes produced by the constructions in this section are isomorphic to the amorphic association schemes listed in Theorems 4.1 and 4.5.

5. Paley-type PDSs and Paley–Hadamard DSs in nonabelian groups

In this section, we will use results from the previous sections to construct additional examples of nonabelian Paley-type PDSs as well as nonabelian Stanton–Sprott (Twin prime power) Paley–Hadamard DSs. Davis [6] used character theory to prove a product construction for abelian groups; we will show that the theorem remains true for nonabelian groups. The theorem will enable us to recursively build nonabelian PDSs with Paley-type parameters.

THEOREM 5.1. *Suppose that the groups G and G' of order v both possess PDSs of the Paley-type having parameters $\left(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4}\right)$, D and D' respectively. Then,the group $\mathcal{G} := G \times G'$ also contains a Paley-type PDS with parameters $\left(v^2, \frac{v^2-1}{2}, \frac{v^2-5}{4}.\frac{v^2-1}{4}\right)$.*

Proof. If D and D' are Paley-type PDSs in G and G', resp. then $D^c = G - 1_G - D$ and $D'^c = G' - 1_{G'} - D'$ are also Paley-type PDSs in G and G', respectively. The following group ring equations then hold in G and G' as a consequence of the sets D, D^c, D', D'^c being PDSs:

$$DD^c = D^cD = \frac{v-1}{4}G^*,$$
$$D'D'^c = D'^cD' = \frac{v-1}{4}G'^*,$$

where G^* and G'^* denote $G - 1_G$ and $G' - 1_{G'}$, respectively.

Our Paley-type PDS in $\mathcal{G} = G \times G'$ is given by $\mathcal{D} = D(1 + D') + D^c(1 + D'^c)$, as verified in the following group ring computation:

$$\begin{aligned}
\mathcal{D}^2 &= (D(1+D') + D^c(1+D'^c))^2 \\
&= D^2(1+D')^2 + 2DD^c(1+D')(1+D'^c) + (D')^2(1+D'^c)^2 \\
&= \left(\frac{v-5}{4}D + \frac{v-1}{4}D^c + \frac{v-1}{2}1_G\right)\left(\frac{v+3}{4}D' + \frac{v-1}{4}D'^c + \frac{v+1}{2}1_{G'}\right) \\
&\quad + \frac{v-1}{2}G^*\left(1 + \frac{v+3}{4}G'^*\right) \\
&\quad + \left(\frac{v-1}{4}D + \frac{v-5}{4}D^c + \frac{v-1}{2}1_G\right)\left(\frac{v-1}{4}D' + \frac{v+3}{4}D'^c + \frac{v+1}{2}1_{G'}\right) \\
&= \frac{v^2-1}{4}1_{\mathcal{G}} + \frac{v^2-5}{4}\mathcal{D} + \frac{v^2-1}{4}(\mathcal{G} - \mathcal{D}).
\end{aligned}$$

□

To illustrate the scope of Theorem 5.1, consider the groups $G = \mathbb{Z}_{25} \rtimes_{21} \mathbb{Z}_{25}$ and $G' = G_2 = \langle T_U, \mathcal{B}\rangle$ (with $q = 5$ and $m = 2$) from the discussion before Theorem 3.9. Both of these groups have $(625, 312, 155, 156)$-PDSs and hence $\mathcal{G} = G \times G'$ will have a $\left(5^8, \frac{5^8-1}{2}, \frac{5^8-5}{4}, \frac{5^8-1}{4}\right)$-PDS. We can continue to apply the theorem by first constructing a $\left(5^8, \frac{5^8-1}{2}, \frac{5^8-5}{4}, \frac{5^8-1}{4}\right)$-PDS in $\mathcal{G}' = \mathbb{Z}_{25}^2 \times \mathbb{Z}_5^4$ (both $\mathbb{Z}_{25}^2$ and $\mathbb{Z}_5^4$ have $(625, 312, 155, 156)$-PDSs, and Theorem 5.1 implies that their product will have a PDS), and we can then apply Theorem 5.1 to get a $\left(5^{16}, \frac{5^{16}-1}{2}, \frac{5^{16}-5}{4}, \frac{5^{16}-1}{4}\right)$-PDS in $\mathcal{G} \times \mathcal{G}'$. Repeated uses of the Theorem give constructions of Paley-type PDSs in groups of the form $G^{2^t}, G'^{2^t}, (\mathcal{G} \times \mathcal{G}')^{2^t}$, and $\mathcal{G}^{2^t}$. As long as the sizes of the groups are the same, we can repeatedly apply Theorem 5.1 to get Paley-type PDSs in larger groups. One general example of a family with a variety of exponents for the constituent groups is the following.

Corollary 5.2. *The group* $\mathbb{Z}_p^4 \times (\mathbb{Z}_{p^2} \rtimes_{p^2-p+1} \mathbb{Z}_{p^2}) \times (\mathbb{Z}_{p^4} \rtimes_{p^4-p^3+1} \mathbb{Z}_{p^4}) \times \cdots \times (\mathbb{Z}_{p^{2^t}} \rtimes_{p^{2^t}-p^{2^t-1}+1} \mathbb{Z}_{p^{2^t}})$ *has a Paley-type PDS for all* $t \geqslant 2$.

Paley-type PDSs can in turn be used to generate Paley–Hadamard DSs using the Stanton–Sprott construction [29]. As with the recursive construction for Paley-type PDSs, we show that the input groups need not be abelian. Since we now have constructions of nonabelian Paley-type PDSs, we will be able to construct new Paley–Hadamard DSs that are nonabelian. To our knowledge, these are the first nonabelian DSs with these parameters.

Theorem 5.3. *Suppose that the group* G *contains a Paley-type* $\left(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4}\right)$*-PDS and the group* G' *contains a skew Hadamard* $\left(v \pm 2, \frac{(v\pm2)-1}{2}, \frac{(v\pm2)-3}{4}\right)$*-DS.*

Then,the product group $G \times G'$ contains a Paley–Hadamard DS in the Stanton–Sprott (Twin prime power) family.

Proof. We will prove the case where $|G'| = v+2$, with the $v-2$ case being extremely similar. If D is a Paley-type $\left(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4}\right)$-PDS in G, then $D^c = G - 1_G - D$ is also a Paley-type PDS. We use the facts from the proof of Theorem 5.1 together with the similar equations for the skew-Hadamard DS D' in G' to get the following.

The set $\mathcal{D} := G + DD' + D^c D'^{(-1)} \subset G \times G'$ is a DS as verified below:

$$\begin{aligned}
\mathcal{D}\mathcal{D}^{(-1)} &= \left(G + DD' + D^c D'^{(-1)}\right)\left(G + DD' + D^c D'^{(-1)}\right)^{(-1)} \\
&= \left(G + DD' + D^c D'^{(-1)}\right)\left(G + DD'^{(-1)} + D^c D'\right) \\
&= G^2 + (GD)D'^{(-1)} + (GD^c)D' + (GD)D' + D^2(D'D'^{(-1)}) + (DD^c)D'^2 \\
&\quad + (GD')D'^{(-1)} + (DD^c)(D'^{(-1)})^2 + D^{c2}(D'^{(-1)}D) \\
&= vG(1_{G'}) + (v-1)G(D' + D'^{(-1)}) \\
&\quad + \left(\frac{v-1}{4}G^*\right)\left(\frac{v-3}{4} + \frac{v-1}{4}\right)G'^* \\
&\quad + \left(\frac{v-1}{4}G^*\right)\left(\left(\left(\frac{v-5}{4} + \frac{v-1}{4}\right)G^* + (v-1)1_G\right)\left(\frac{v+1}{2}1_{G'} + \frac{v-1}{4}G'^*\right)\right).
\end{aligned}$$

Combining terms leads to the equation

$$\mathcal{D}\mathcal{D}^{(-1)} = \frac{v^2+2v-3}{4}\mathcal{G}^* + \frac{v^2+2v-1}{2}1_{\mathcal{G}},$$

thus proving the result. □

Recall the group G_2 from Section 3, letting $q = 3$ and $m = 2$. As examples of Theorem 5.3, the nonabelian groups $G_2 \times \mathbb{Z}_{83}$ and $(\mathbb{Z}_9 \rtimes_7 \mathbb{Z}_9) \times \mathbb{Z}_{83}$ each have a $(6723, 3361, 1680)$-difference set; the nonabelian groups $(G_2)^2 \times \mathbb{Z}_{6563}$, $(\mathbb{Z}_9 \rtimes_7 \mathbb{Z}_9) \times G_2 \times \mathbb{Z}_{6563}$, $(\mathbb{Z}_9 \rtimes_7 \mathbb{Z}_9)^2 \times \mathbb{Z}_{6563}$, and $(\mathbb{Z}_{81} \rtimes_{55} \mathbb{Z}_{81}) \times \mathbb{Z}_{6563}$ have $(45724643, 22862321, 11431160)$-difference sets; and the nonabelian group $(\mathbb{Z}_{27} \rtimes_{19} \mathbb{Z}_{27}) \times \mathbb{Z}_{727}$ has a $(529983, 264991, 132495)$-difference set. A more general corollary is the following (although there will be many nonabelian groups containing a Paley–Hadamard difference set that are not contained in this result).

Corollary 5.4. *Let $r \geqslant 2$. If $q = p^{2^r} \pm 2$ is prime, then the nonabelian group*

$$(\mathbb{Z}_{p^{2^r}} \rtimes_{(p-1)p^{2^r-1}-1+1} \mathbb{Z}_{p^{2^r}}) \times \mathbb{Z}_q$$

has a $\left(qp^{2^r}, (qp^{2^r}-1)/2, (qp^{2^r}-3)/4\right)$-difference set.

6. Many product theorems allow nonabelian groups

In the previous section, we used group rings to prove that two results previously known in abelian groups also hold in nonabelian groups. In this section, we will show that in some cases we can avoid the quadratic group ring calculations entirely because the relations needed to simplify the calculations do not depend on whether the group is abelian or not.

Lemma 6.1. *Suppose the group G has a partition of the nonidentity elements into PDSs $P_1, P_2, \ldots, P_n$ all of the Latin square type or all of the negative Latin square type. If P_i and P_j have parameters $(v, k_i, \lambda_i, \mu_i)$ and $(v, k_j, \lambda_j, \mu_j)$ resp. with $i \neq j$, then $P_i \cup P_j$ will be a $(v, k_i + k_j, \lambda, \mu)$-PDS for some λ and μ, and*

$$P_iP_j = P_jP_i = (\lambda - \lambda_i - \mu_j)P_i + (\lambda - \lambda_j - \mu_i)P_j + (\mu - \mu_i - \mu_j)(G - 1 - P_i - P_j),$$

independent of whether the group G is abelian or not.

Proof. Let P_i be a $(v, k_i, \lambda_i, \mu_i)$-PDS. Then:

$$P_i{}^2 = (k_i - \mu_i)1_G + \lambda_i P_i + \mu_i(G - P_i).$$

Now suppose that P_i and P_j are part of the partition of G into Latin or negative Latin square type PDSs. Let P_i be a $(v, k_i, \lambda_i, \mu_i)$-PDS and P_j be a $(v, k_j, \lambda_j, \mu_j)$-PDS. The key to getting a relation for P_iP_j is the fact that the union of disjoint PDSs of Latin (alternatively negative Latin square type) will also be a PDS of the same type by Corollary 2.4. The same corollary ensures $P_iP_j = P_jP_i$.

Therefore, we can write two equations for $(P_i+P_j)^2$, the first of which is expanding and using the individual PDS parameters:

$$\begin{aligned}(P_i + P_j)^2 &= P_iP_j + P_jP_i + P_i{}^2 + P_j{}^2 \\ &= 2P_iP_j + (k_i - \mu_i)1_G + \lambda_i P_i + \mu_i(G - P_i) + (k_j - \mu_j) + \lambda_j P_j + \mu_j(G - P_j).\end{aligned}$$

Now we will use the fact that $P_i \cup P_j$ is a $(v, k_i + k_j, \lambda, \mu)$-PDS.

$$(P_i + P_j)^2 = (k_i + k_j - \mu)1_G + \lambda(P_i + P_j) + \mu(G - P_i - P_j).$$

Setting the equations equal and solving yields:

$$P_iP_j = (\lambda - \lambda_i - \mu_j)P_i + (\lambda - \mu_i - \lambda_j)P_j + (\mu - \mu_i - \mu_j)(G - 1 - P_i - P_j).$$

Hence, the relations for both $P_i{}^2$ and P_iP_j are determined by the parameters. Suppose that G has a partition of the nonidentity elements into PDSs $P_1, P_2, \ldots, P_n$ and G' has a partition of the nonidentity elements into PDSs $P'_1, P'_2, \ldots, P'_n$ where P_i and P'_i have the same parameters. Then, the relations for $P_i{}^2$ and $P'_i{}^2$ are the same for P_i relative to G as for P'_i relative to G' and furthermore the relations for P_iP_j and $P'_iP'_j$ are the same for P_i and P_j relative to G as for P'_i and P'_j relative to G'. The result follows. □

Theorem 6.2. *Suppose the group G has a partition $\mathcal{P} = \{1_G = P_0, P_1, P_2, \ldots, P_n\}$ where all the P_i are Latin square type PDSs or negative Latin square type PDSs and 1_G is the identity in G. Let G' be any other group, and suppose $D = \sum_{i=0}^n P_iA'_i$ is a PDS in $G \times G'$, where $A'_i \subseteq G'$. Suppose there is another group $\widehat{G}$ that has a partition of its nonidentity elements into PDSs $\{\widehat{P_1}, \widehat{P_2}, \ldots, \widehat{P_n}\}$ where P_i and $\widehat{P_i}$ have the same parameters for all i. Then, $\widehat{D} = \sum_{i=0}^n \hat{P}_iA'_i$ will be a PDS in $\hat{G} \times G'$ with the exact same parameters as D.*

Proof. Let D be a (v, k, λ, μ)-PDS in $G \times G'$ so that:

$$DD^{(-1)} = (k - \mu)1_{G\times G'} + \lambda D + \mu(G \times G' - D).$$

Consider $\widehat{D}\widehat{D}^{(-1)}$. Each term in the expansion will have one of the following forms:

1. $(1_{\widehat{G}}x')(1_{\widehat{G}}y') = 1_{\widehat{G}}x'y'$ where $x', y' \in G'$. In our calculation of $DD^{(-1)}$ we have the corresponding term $(1_Gx')(1_Gy') = 1_Gx'y'$.
2. $(1_{\widehat{G}}x')(\widehat{P}_iy') = \widehat{P}_ix'y'$ where $x', y' \in G'$. In our calculation of $DD^{(-1)}$ we have the corresponding term $(1_Gx')(P_iy') = P_ix'y'$.
3. $(\widehat{P}_ix')(\widehat{P}_iy') = \widehat{P}_i{}^2x'y' = ((k_i-\mu_i)1_{\widehat{G}}+\lambda_i\widehat{P}_i+\mu_i(\widehat{G}-\widehat{P}_i))x'y'$ where $x', y' \in G'$, In our calculation of $DD^{(-1)}$ we have the corresponding term $(P_ix')(P_iy') = P_i{}^2x'y' = (k_i - \mu_i)1_G + \lambda_iP_i + \mu_i(G - P_i)x'y'$, where both P_i and $\widehat{P}_i$ are $(v, k_i, \lambda_i, \mu_i)$-PDSs.
4. $(\widehat{P}_ix')(\widehat{P_j}y') = \widehat{P}_i\widehat{P_j}(x', y')$ where $x', y' \in G'$. In our calculation of $DD^{(-1)}$ we have the corresponding term $(P_ix')(P_jy') = (P_iP_j)(x'y')$. By the preceding lemma, we know that $P_iP_m = aP_i + bP_j + c(G - 1_G - P_i - P_j)$ means that $\widehat{P}_i\widehat{P_m} = a\widehat{P}_i + b\widehat{P_j} + c(G - 1_{\widehat{G}} - \widehat{P}_i - \widehat{P_j})$ and vice versa, since the quadratic group ring equations relating the P_i are determined by the parameters.

Therefore, when we expand $\widehat{D}\widehat{D}^{(-1)}$ we will the exact same count of terms for $\widehat{P}_i x'$ and $1_{\widehat{G}} x'$ for any $x' \in G'$ as we would respectively for $P_i x'$ and $1_G x'$ when calculating $DD^{(-1)}$. It follows that:

$$\widehat{D}\widehat{D}^{(-1)} = (k-\mu)1_{\widehat{G}\times G'} + \lambda\widehat{D} + \mu(\widehat{G}\times G' - \widehat{D}).$$

□

All of the product constructions in [7, 22, 23, 25, 26] satisfy the hypotheses of Theorem 6.2 and hence can be used to construct nonabelian PDSs.

We illustrate one use of Theorem 6.2 by considering the case $v = 729$. In [22], product constructions were given showing that there exists a partition of the nonidentity elements of the groups ${\mathbb{Z}_3}^2 \times {\mathbb{Z}_3}^4$ and ${\mathbb{Z}_3}^2 \times \mathbb{Z}_9 \times \mathbb{Z}_9$ into three PDSs of cardinalities $260, 234$, and 234 respectively or $224, 252$, and 252 respectively. Now we can use the examples from Sections 3 (G_1^+, G_1^-, G_2) and 4 ($\mathbb{Z}_9 \rtimes_7 \mathbb{Z}_9$) in conjunction with Theorem 6.2 to add the following groups as having both of these PDS partitions: ${\mathbb{Z}_3}^2 \times G_1^+$, ${\mathbb{Z}_3}^2 \times G_1^-$, ${\mathbb{Z}_3}^2 \times G_2$, and ${\mathbb{Z}_3}^2 \times \mathbb{Z}_9 \rtimes_7 \mathbb{Z}_9$.

Moreover, by [25, p. 1645], we also have a partition of $\mathbb{Z}_{27} \times \mathbb{Z}_{27}$ into three PDSs of cardinalities $260, 234$, and 234, respectively. In fact, direct calculation in GAP [11] shows that $\mathbb{Z}_{27} \rtimes_{19} \mathbb{Z}_{27}$ also has such a partition into three PDSs of cardinalities 260, 234, and 234, respectively. (The PDSs in $\mathbb{Z}_{27} \rtimes_{19} \mathbb{Z}_{27}$ are obtained from those in $\mathbb{Z}_{27} \times \mathbb{Z}_{27}$ analogously as when moving from G_t to $\widehat{G_t}$ in Section 4.)

7. Possible next steps

While we have constructed PDSs in several nonabelian groups, we believe there is much more to be uncovered. We list some open questions.

(1) All the constructions in this paper are in p-groups. There have been some constructions of Latin and negative Latin square type PDSs in nonabelian non-p-groups, and in particular for $|G| = 100$ (see [12] and [28]), but aside from these and a few other small examples little is known. It seems likely that there will be some nonabelian groups with PDSs having the same parameters as those that exist in certain abelian groups, and perhaps (such as with $|G| = 100$ there might be some genuinely nonabelian parameters).

(2) We saw four distinct techniques in this paper that used abelian PDSs to obtain nonabelian PDSs: using quadratic forms and analyzing affine polar graphs, exploiting groups with a large center, calculating group ring equations in place of characters, and identifying that certain product constructions depend only on parameters. Abelian PDSs have been extensively studied, and there are many other techniques to explore from this previous work. One could consider additional ways to carry over the well-developed techniques from abelian groups to the less familiar nonabelian setting. Especially in light of [20], it seems likely that at least some techniques from character theory would fit this description.

(3) Theorem 6.2 from Section 6 could be applied to other results from abelian groups. In particular, there are likely to be many nonabelian PDSs in 2-groups. (For example, consider the results of [9] combined with product theorems such as Theorem 6.2.).

(4) In Section 6, the objective was to see that the technique of certain product constructions can carry over to nonabelian input groups with the appropriate partition. One starts to see that many nonabelian groups will have PDSs that are the same as the abelian case. One could begin to catalog all the groups that support (v, k, λ, μ)-PDSs for relatively small v.

(5) Since PDSs produce strongly regular Cayley graphs, one could also begin to catalog which groups have PDSs that correspond to the various nonisomorphic (v, k, λ, μ)-strongly regular graphs for small v.
(6) In recent work (see, e.g. [1]), amorphic association schemes have been constructed using *bent functions*. It would be interesting to know whether the amorphic schemes produced by Theorem 3.14 have connections to bent functions.

References

[1] Nurdagül Anbar, Tekgül Kalaycı, and Wilfried Meidl, *Amorphic association schemes from bent partitions*, Discrete Math. **347** (2024), no. 1, article no. 113658 (13 pages).
[2] Simeon Ball, *Finite geometry and combinatorial applications*, London Mathematical Society Student Texts, vol. 82, Cambridge University Press, Cambridge, 2015.
[3] Andrew C. Brady, *Negative Latin square type partial difference sets in nonabelian groups of order 64*, Finite Fields Appl. **81** (2022), article no. 102044 (11 pages).
[4] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Mathematical Society Lecture Note Series, vol. 407, Cambridge University Press, Cambridge, 2013, With a foreword by Martin Liebeck.
[5] Andries E. Brouwer and H. Van Maldeghem, *Strongly regular graphs*, Encyclopedia of Mathematics and its Applications, vol. 182, Cambridge University Press, Cambridge, 2022.
[6] James A. Davis, *Partial difference sets in p-groups*, Arch. Math. (Basel) **63** (1994), no. 2, 103–110.
[7] James A. Davis and Qing Xiang, *Negative Latin square type partial difference sets in nonelementary abelian 2-groups*, J. London Math. Soc. (2) **70** (2004), no. 1, 125–141.
[8] Stefaan De Winter, Ellen Kamischke, and Zeying Wang, *Automorphisms of strongly regular graphs with applications to partial difference sets*, Des. Codes Cryptogr. **79** (2016), no. 3, 471–485.
[9] Tao Feng, Zhiwen He, and Yu Qing Chen, *Partial difference sets and amorphic Cayley schemes in non-abelian 2-groups*, J. Combin. Des. **28** (2020), no. 4, 273–293.
[10] Tao Feng, Koji Momihara, and Qing Xiang, *Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes*, Combinatorica **35** (2015), no. 4, 413–434.
[11] The GAP Group, *Gap – Groups, Algorithms, and Programming, Version 4.14.0*, 2024, `https://www.gap-system.org`.
[12] L. K. Jørgensen and M. Klin, *Switching of edges in strongly regular graphs. I. A family of partial difference sets on 100 vertices*, Electron. J. Combin. **10** (2003), article no. 17 (31 pages).
[13] Peter Kleidman and Martin Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990.
[14] M. Kh. Klin, *The axiomatics of cellular rings*, in Investigations in the algebraic theory of combinatorial objects (Russian), Vsesoyuz. Nauchno-Issled. Inst. Sistem. Issled., Moscow, 1985, pp. 6–32.
[15] Ka Hin Leung and Siu Lun Ma, *Constructions of partial difference sets and relative difference sets on p-groups*, Bull. London Math. Soc. **22** (1990), no. 6, 533–539.
[16] Ka Hin Leung and Siu Lun Ma, *Partial difference sets with Paley parameters*, Bull. London Math. Soc. **27** (1995), no. 6, 553–564.
[17] S. L. Ma, *A survey of partial difference sets*, Des. Codes Cryptogr. **4** (1994), no. 3, 221–261.
[18] Martin E. Malandro and Ken W. Smith, *Partial difference sets in $C_{2^n} \times C_{2^n}$*, Discrete Math. **343** (2020), no. 4, article no. 111744 (22 pages).
[19] Koji Momihara and Qing Xiang, *Strongly regular Cayley graphs from partitions of subdifference sets of the Singer difference sets*, Finite Fields Appl. **50** (2018), 222–250.
[20] Udo Ott, *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*, European J. Combin. **110** (2023), article no. 103681 (10 pages).
[21] R. E. A. C. Paley, *On Orthogonal Matrices*, J. Math. Phys. **12** (1933), no. 1–4, 311–320.
[22] John Polhill, *New negative Latin square type partial difference sets in nonelementary abelian 2-groups and 3-groups*, Des. Codes Cryptogr. **46** (2008), no. 3, 365–377.
[23] John Polhill, *Negative Latin square type partial difference sets and amorphic association schemes with Galois rings*, J. Combin. Des. **17** (2009), no. 3, 266–282.

[24] John Polhill, *Paley type partial difference sets in non p-groups*, Des. Codes Cryptogr. **52** (2009), no. 2, 163–169.
[25] John Polhill, *A new family of partial difference sets in 3-groups*, Des. Codes Cryptogr. **87** (2019), no. 7, 1639–1646.
[26] John Polhill, James A. Davis, Ken W. Smith, and Eric Swartz, *Genuinely nonabelian partial difference sets*, J. Combin. Des. **32** (2024), no. 7, 351–370.
[27] John B. Polhill, *Constructions of nested partial difference sets with Galois rings*, Des. Codes Cryptogr. **25** (2002), no. 3, 299–309.
[28] Ken W. Smith, *Non-abelian Hadamard difference sets*, J. Combin. Theory Ser. A **70** (1995), no. 1, 144–156.
[29] R. G. Stanton and D. A. Sprott, *A family of difference sets*, Canadian J. Math. **10** (1958), 73–77.
[30] Eric Swartz, *A construction of a partial difference set in the extraspecial groups of order p^3 with exponent p^2*, Des. Codes Cryptogr. **75** (2015), no. 2, 237–242.
[31] Eric Swartz and Gabrielle Tauscheck, *Restrictions on parameters of partial difference sets in nonabelian groups*, J. Combin. Des. **29** (2021), no. 1, 38–51.
[32] E. R. van Dam and M. Muzychuk, *Some implications on amorphic association schemes*, J. Combin. Theory Ser. A **117** (2010), no. 2, 111–127.
[33] Edwin R. van Dam, *Strongly regular decompositions of the complete graph*, J. Algebraic Combin. **17** (2003), no. 2, 181–201.
[34] Robert A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009.

James A. Davis, Department of Mathematics & Statistics, University of Richmond, Richmond, VA 23173 (USA)
E-mail : jdavis@richmond.edu

John Polhill, Department of Mathematics, Computer Science, and Digital Forensics, Commonwealth University, Bloomsburg, PA 17815 (USA)
E-mail : jpolhill@commonwealthu.edu

Ken Smith, Huntsville, TX 77340 (USA)
E-mail : kenwsmith54@gmail.com

Eric Swartz, Department of Mathematics, William & Mary, Williamsburg, VA 23187 (USA)
E-mail : easwartz@wm.edu