8-1994

Partial Difference Sets in *p*-groups

James A. Davis
University of Richmond, jdavis@richmond.edu

Recommended Citation

Davis, James A. "Partial Difference Sets in *p*-groups." *Archiv Der Mathematik* 63, no. 2 (August 1994): 103-10. doi: 10.1007/BF01189882.

Arch. Math., Vol. 63, 103–110 (1994)

0003-889X/94/6302-0103 $ 3.10/0

Partial difference sets in p-groups

By

JAMES A. DAVIS*)

1. Introduction. Let G be a group of order v and D a subset of cardinality k. If every (nonidentity) element of D is represented exactly λ times as dd'^{-1} for $d, d' \in D$, and every (nonidentity) element of $G - D$ exactly μ times as dd'^{-1}, then D is called a (v, k, λ, μ) partial difference set (PDS). Another useful parameter for PDS is $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$. See [7] for a survey of PDS , including their connections to strongly regular graphs. Most of the examples of PDS have come in p-groups, and most of these examples are in elementary abelian p-groups. In this paper, we will show an exponent bound for PDS with the same parameters as the elementary abelian case.

There are several important observations about PDS that we will need later, and we include them in the following theorem.

Theorem 1.1 ([6]). *If D is a (v, k, λ, μ) partial difference set and $\lambda \neq \mu$, then $D^{(-1)} = D$. If $1 \in D$, then $D - \{1\}$ is also a* PDS.

In general, when any type of difference set has the property that $D^{(-1)} = D$, that difference set is called *reversible*. If D does not contain the identity, then D is called a regular PDS. We will only consider regular PDS in this paper.

A useful context to study PDS is in the group ring $Z[G]$. If S is a subset of G, we write $\bar{S} = \sum_{s \in S} s$ and $\bar{S}^{(-1)} = \sum_{s \in S} s^{-1}$. The definition of the PDS implies the following group ring equation.

$$\overline{D}\overline{D}^{(-1)} = \mu\bar{G} + (\lambda - \mu)\bar{D} + \gamma 1,$$

where $\gamma = k - \mu$ when $1 \notin D$. Since $D^{(-1)} = D$, we can rewrite this equation into the quadratic equation in $\bar{D}$ listed below.

$$\bar{D}^2 = \mu\bar{G} + (\lambda - \mu)\bar{D} + \gamma 1.$$

Another useful technique is to consider contracted difference sets. If we map $\phi: Z[G] \to Z[G/H]$ in the natural way, the difference set will be mapped to $\phi(D)$, where $\phi(D)$ may have coefficients that are not either 0 or 1. The coefficients will be integers between 0 and $h = |H|$; they are called the *intersection numbers* of the contraction, and

*) This work is partially supported by NSA grant # MDA 904-92-H-3067

are labeled a_i. If we apply ϕ to the equation above, we get

$$\overline{\phi(D)}^2 = (\sum_i a_i gH)^2 = h\mu\overline{G/H} + (\lambda - \mu)\,\overline{\phi(D)} + \gamma 1.$$

One of the main examples of PDS is due to Paley [9], who showed the following theorem (he did not phrase his result in the language of PDS).

Theorem 1.2. *Let G be the additive group of the finite field F_{p^r}, where p is a prime, and $p^r \equiv 1 \pmod 4$. The nonzero squares in F_{p^r} form a $\left(p^r, \frac{p^r-1}{2}, \frac{p^r-5}{4}, \frac{p^r-1}{4}\right)$ PDS in G.*

The additive group of the finite field is an elementary abelian p-group; this paper examines other abelian p-groups to see if any have a PDS with these parameters. Note that this theorem is true for any power of an odd prime p that is 1 mod 4, and any even power of an odd prime that is 3 mod 4. Also note that $\lambda - \mu = -1$ for these parameters. The following theorem due to Arasu, Jungnickel, Ma, and Pott [3] shows that PDS with $\lambda - \mu = -1$ must be of this form (with one exception).

Theorem 1.3. *The following are all possible parameters for the existence of a nontrivial abelian regular PDS with $\lambda - \mu = -1$:*

(a) $(v, k, \lambda, \mu) = \left(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4}\right)$ *where* $v \equiv 1 \pmod 4$.

(b) $(v, k, \lambda, \mu) = (243, 22, 1, 2)$ *or* $(243, 220, 199, 200)$.

PDS with $\lambda - \mu = -1$ have applications to reversible divisible difference sets. An $(m, n, k, \lambda_1, \lambda_2)$ divisible difference set (DDS) in a group G with respect to a normal subgroup N of order n is a k-element subset D so that every (nonidentity) element of N is represented exactly λ_1 times as dd'^{-1} and every element of $G - N$ exactly λ_2 times as dd'^{-1}. A DDS is called reversible if $D^{(-1)} = D$. The following theorem due to Arasu, Jungnickel, and Pott [1] establishes the connection between PDS with $\lambda - \mu = -1$ and reversible DDS with $k - \lambda_1 = 1$.

Theorem 1.4 ([1]). *If there is a $(m, k, \lambda, \lambda + 1)$ PDS in an abelian group H, then there is a reversible $(m, 2, 2k + 1, 2k, 2(\lambda + 1))$ DDS in an abelian group G of order $2m$ that contains a subgroup isomorphic to H. Moreover, every proper reversible DDS with $k - \lambda_1 = 1$ arises in this way.*

We can combine Theorems 1.3 and 1.4 to show that there is a $\left(p^r, 2, p^r, p^r - 1, \frac{p^r-1}{2}\right)$ reversible DDS in $Z_p^r \times Z_2$ when $p^r \equiv 1 \pmod 4$.

One other important feature about these parameters involves a theorem by Ma [6].

Theorem 1.5. *Suppose that there is an abelian regular (v, k, λ, μ) PDS so that Δ is not a square. Then $(v, k, \lambda, \mu) = (p^{2s+1}, (p^{2s+1} - 1)/2, (p^{2s+1} - 5)/4, (p^{2s+1} - 1)/4)$ where p is a prime $1 \pmod 4$. Note that $\Delta = p^{2s+1}$.*

Note that Paley's construction in the elementary abelian group fits these parameters.

In [10], Turyn initiated the use of character theory for studying difference sets in abelian groups. A character of an abelian group is a homomorphism from the group to the complex numbers. This technique has been generalized to aid in the study of other types of difference sets, including PDS and DDS. One way to see how character theory gets involved is to extend the homomorphism to the group ring, and apply the extended homomorphism to the group ring equation developed in the introduction. Thus, if χ is a character of G, then the PDS equation becomes

$$(\chi(D))^2 = (\lambda - \mu)\,\chi(D) + \gamma.$$

By using the quadratic formula and the Fourier inversion formula (see [10] for similar arguments), we get the following theorem.

Theorem 1.6. *The subset D of the abelian group G is a (v, k, λ, μ) PDS iff $\chi(D) = \dfrac{\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4\gamma}}{2} = \dfrac{\lambda - \mu \pm \sqrt{\Delta}}{2}$ for every nonprincipal character χ.*

One important thing to note here is that the character sum equation does not require that we take the absolute value of $\chi(D)$ as we do for other types of difference sets because the PDS is reversible.

To each character χ we have the associated contraction of the group $\phi_\chi\colon G \to G/\mathrm{Ker}(\chi)$. If χ is a character of order r, then the intersection number a_i under the contraction by ϕ_χ is the number of elements of the PDS that are sent to ζ^i, ζ a primitive rth root of unity. Thus, we have changed a question of PDS into a question of sums of roots of unity in a cyclotomic field. We need to consider the cyclotomic field $\mathbb{Q}[\zeta]$, where ζ is a primitive p^{s+1} root of unity. By basic number theory (see [8] for example), a basis for $\mathbb{Q}[\zeta]$ is $\{\zeta^{i+p^s j} \mid i = 0, 1, 2, \ldots, p^s - 1; j = 1, 2, \ldots, p - 1\}$. Notice that there are $p^s(p-1)$ elements in this basis. If $A \in \mathbb{Q}[\zeta]$, and if $A = \sum_{i=0}^{p^s-1} a_i \zeta^i$, then when we write A in terms of the basis, we get $A = \sum_{i=0}^{p^s-1} \sum_{j=1}^{p-1} (a_{i+jp^s} - a_i)\zeta^{i+jp^s}$.

2. Nonexistence result. We consider the parameters $\left(p^{2s+1}, \dfrac{p^{2s+1}-1}{2}, \dfrac{p^{2s+1}-5}{4}, \dfrac{p^{2s+1}-1}{4}\right)$. Suppose that there is a character χ nonprincipal on the group G. The following corollary describes how to get the correct character sum (this follows from Theorem 1.6).

Corollary 2.1. *There is a $\left(p^{2s+1}, \dfrac{p^{2s+1}-1}{2}, \dfrac{p^{2s+1}-5}{4}, \dfrac{p^{2s+1}-1}{4}\right)$ PDS in an abelian group G iff $\chi(D) = \dfrac{-1 \pm \sqrt{1 + p^{2s+1} - 1}}{2} = \dfrac{-1 \pm p^s\sqrt{p}}{2}$ for every nonprincipal character χ of G.*

Leung, Ma, and Tan [5] have shown the following exponent bound on the group for these parameters.

Theorem 2.1. *If there exists a* $\left(p^{2s+1}, \frac{p^{2s+1}-1}{2}, \frac{p^{2s+1}-5}{4}, \frac{p^{2s+1}-1}{4}\right)$*-PDS* D *in an abelian group* G $(p \equiv 1 \bmod 4$ *a prime), then the exponent of* G *is less than or equal to* p^{s+1}.

We consider the case on the boundary, namely groups G with exponent equal to p^{s+1}. We are working with the cyclotomic fields generated by ζ, where ζ is a primitive p^{s+1} root of unity. In this cyclotomic field, we need to know how we can get a sum of $\frac{-1 \pm p^s \sqrt{p}}{2}$. The following lemma tells us how to do that.

Lemma 2.1. *Let* p *be a prime;* $\frac{-1 \pm p^s \sqrt{p}}{2} = -\frac{p^s-1}{2} \sum_{k=1}^{p-1} \zeta^{kp^s} + p^s \sum_n \zeta^{p^s n}$, *where* n *is summed over the quadratic residues* mod p *for the positive sum and the quadratic nonresidues for the negative sum.*

Proof. The sum uses the basic number theory fact [8] which shows that $\sum_n \zeta^{p^s n} = \frac{\sqrt{p}-1}{2}$ where n ranges over the quadratic residues mod p, and the sum over the nonresidues mod p is $\frac{-\sqrt{p}-1}{2}$. The lemma is a simple calculation from this result. □

Notice that the sums only use powers of ζ that are actually powers of ζ^{p^s}. Since all of the coefficients on this sum must be positive when we look at $\chi(D)$ (they are the intersection numbers), we have that the coefficients on the powers $\zeta^{p^s n}$, n a residue (or nonresidue) must be p^s. Also, the intersection number for the nonresidues (or residues) will be 0. The intersection number of p^s implies that a coset of the kernel of χ will be contained in the PDS, while the intersection number of 0 implies that the coset will not intersect the PDS. We can use that to prove the following theorem.

Theorem 2.2. *If there exists a* $\left(p^{2s+1}, \frac{p^{2s+1}-1}{2}, \frac{p^{2s+1}-5}{4}, \frac{p^{2s+1}-1}{4}\right)$ *PDS* D *in an abelian group* G $(p \equiv 1 \bmod 4$ *a prime), then the exponent of* G *is less than or equal to* p^s.

Proof. Suppose that the group is $G = \langle x \rangle \times H$, where x has order p^{s+1} (we know the exponent cannot be any bigger than this by Theorem 2.1), and the character χ maps x to a primitive p^{s+1} root of unity ζ and H to 1. By the remarks before the theorem, the cosets $x^{p^s n}H$ are contained in the difference set when n is a quadratic residue mod p, and those cosets are disjoint with the difference set when n is a non-quadratic residue (or vice versa). Now consider the character χ_1 that maps x to ζ and has order p on H: there will be $\frac{p-1}{2} p^{s-1}$ elements mapped to each root of unity $\zeta^{p^s i}$ for $i = 0, 1, \ldots, p-1$. This means that χ_1 will not have an intersection number $a_{p^s i}$ of 0 for either the residues or nonresidues. This is a contradiction, so there is not a PDS with these parameters. □

Corollary 2.2. *Let $p \equiv 1 (\mathrm{mod}\, 4)$, p a prime: there is a* $\left(p^3, \frac{p^3-1}{2}, \frac{p^3-5}{4}, \frac{p^3-1}{4}\right)$ PDS *in an abelian group if and only if the group is elementary abelian.*

3. Construction. In [4], Leung and Ma provided a construction of a PDS in an abelian p-group that is not elementary abelian. We state one special case of that theorem in the following.

Theorem 3.1. *The group $G = Z_{p^2}^2$ has a $(p^4, ep(p^2-1), (e^2+1)p^2 - 3ep, (ep)^2 - ep)$* PDS *for $1 \leqq e \leqq p-1$.*

Proof. The construction is phrased in terms of finite local rings: I would like to view the PDS in a different way, similar to PDS of the PCP type. In the PCP construction, we need r mutually disjoint (with the exception of the identity) subgroups. One way to view the Leung-Ma construction is that it uses $e(p+1)$ cyclic subgroups of order p^2 in the group $Z_{p^2}^2$, and only takes the elements of order p^2 from those subgroups to form the PDS. Define the set C to be the elements of order p^2 from the subgroups $\langle(1,1)\rangle, \langle(1,2)\rangle, \ldots, \langle(1,ep)\rangle, \langle(p,1)\rangle, \ldots, \langle(ep,1)\rangle$.

We want to consider the character sums over the set C. There are three possible sums over the elements of order p^2 of a cyclic subgroup H of G of order p^2. If χ_0 is a character that is principal on a generator $h \in H$ (and nonprincipal on G), then the sum is the number of elements of order p^2 in the subgroup, which is $p^2 - p$. If χ_1 is a character that sends h to a primitive pth root of unity, then the sum over the whole subgroup H will be 0. Since we only want the sum over the elements of order p^2, and χ_1 is principal on the elements of order p, we get $\sum_{\text{elts of order } p^2} \chi_1(x) = \sum_{h' \in H} \chi_1(h') - \sum_{j=1}^{p} \chi_1(h^{pj}) = 0 - p = -p$. Finally, if χ_2 is a character that sends h to a primitive p^2 root of unity, then $\sum_{\text{elts of order } p^2} \chi_2(g) = 0$. If χ is a character of order p^2, then χ is principal on at most 1 of the subgroups that is used to build C. If χ is nonprincipal on all of those subgroups, then it will send e of the generators of the subgroups to a primitive pth root of unity, and the other generators (there are ep of these) will be sent to a primitive p^2 root of unity. Thus, the character sum for this type of character is $-ep$. If χ is principal on one of these subgroups, then it will send $e-1$ of the generators to a primitive pth root of unity and the rest to a primitive p^2 root of unity. The character sum will be $p^2 - p + (e-1)(-p) = p^2 - ep$. If χ is a character of order p, then it will be principal on e of the subgroups, and will send the generators of the remaining subgroups to a primitive pth root of unity. Thus, the character sum there will be $e(p^2 - p) + ep(-p) = -ep$. By Theorem 1.6, C is a $(p^4, ep(p^2-1), (e^2+1)p^2 - 3ep, (ep)^2 - ep)$ PDS for $1 \leqq e \leqq p-1$. □

We will now construct a different PDS in the same group $G = Z_{p^2}^2$ (see [7] for the general construction). A *partial congruence partition* of G of degree t (a (p^2, t)-PCP) is a set of t subgroups of G of order p^2 so that $U \cap V = \{1\}$ for every choice of subgroups U, V. There are many ways to construct these: we will choose the subgroups $\langle(1,0)\rangle, \langle(0,1)\rangle, \langle(1, ep+1)\rangle, \ldots, \langle(1, ep+t-2)\rangle$.

Theorem 3.2. *The set* $E = \langle(1,0)\rangle \cup \langle(0,1)\rangle \cup \langle(1, ep + 1)\rangle \cup \ldots \cup \langle(1, ep + t - 2)\rangle - \{(0,0)\}$ *is a* $(p^4, t(p^2 - 1), p^2 + t^2 - 3t, t^2 - t)$ PDS *for* $3 \leqq t \leqq p + 1$, $1 \leqq e \leqq p - 1$.

We have chosen the subgroups in this way so that they will not intersect with the PDS that we defined in the first theorem. We now want to calculate the character theory for E. If χ is a character of order p^2 that is nonprincipal on all of the subgroups in the definition of E, then $\chi(E) = -t$. If χ is principal on one of the subgroups, then $\chi(E) = p^2 - 1 - (t - 1) = p^2 - t$. If χ is a character of order p, then $\chi(E)$ will be principal on at most one of the subgroups (this is where the restrictions on t are used), and $\chi(E)$ could be either $-t$ or $p^2 - t$. Since C and E are disjoint, consider $D = C \cup E$.

Theorem 3.3. *The set* $D = C \cup E$ *is a* $(p^4, (t + ep)(p^2 - 1), p^2 + (t + ep)^2 - 3(t + ep), (t + ep)^2 - (t + ep))$ PDS *in* $Z_{p^2}^2$ *for* $3 \leqq t \leqq p + 1$, $1 \leqq e \leqq p - 1$.

Proof. Suppose that χ is a character of order p^2. χ will be principal on a cyclic subgroup of order p^2: that subgroup is either in C or E or neither. If the kernel is in C, then the character sum is $\chi(D) = \chi(C) + \chi(E) = p^2 - ep + -t$. If the kernel is in E, then the character sum is $\chi(D) = \chi(C) + \chi(E) = -ep + p^2 - t$. Finally, if the kernel is not in either, then $\chi(D) = \chi(C) + \chi(E) = -ep + -t$. All of these are the correct value. If the character has order p, then $\chi(C) = -ep$, and $\chi(E)$ can be either of its possible values to get the correct sum. Thus, Theorem 1.6 implies that D is a PDS. □

Notice that all of these have the *Latin square type* as defined in [7]. This gives a new family of PDS of this type in a nonelementary abelian group. If we set $t = \frac{p+1}{2}$, $e = \frac{p-1}{2}$, we get the following important corollary.

Corollary 3.1. *The group* $Z_{p^2} \times Z_{p^2}$ *has a* $\left(p^4, \frac{p^4 - 1}{2}, \frac{p^4 - 5}{4}, \frac{p^4 - 1}{4}\right)$ *Paley* PDS. *This implies that* $\left(p^4, 2, p^4, p^4 - 1, \frac{p^4 - 1}{2}\right)$ *is a reversible* DDS.

Most examples of reversible DDS are constructed by using elementary abelian p-groups, so this construction is different than the usual way to get reversible DDS.

We can further extend the groups that contain PDS with the Paley parameters with the following product theorem.

Theorem 3.4. *Suppose that* G *and* G' *have* $\left(p^r, \frac{p^r - 1}{2}, \frac{p^r - 5}{4}, \frac{p^r - 1}{4}\right)$ PDS, *respectively* D *and* D'. *Then the set* $E = (1 + D)D' + (G - D)(G' - D' - 1)$ *is a* $\left(p^{2r}, \frac{p^{2r} - 1}{2}, \frac{p^{2r} - 5}{4}, \frac{p^{2r} - 1}{4}\right)$ PDS *in* $G \times G'$.

Proof. Consider the following characters on $G \times G'$: χ nonprincipal on G but principal on G', χ_1 principal on G but nonprincipal on G', and χ_2 nonprincipal on both G and G'

$$\chi(E) = (1 + \chi(D))\,|D'| + (-\chi(D))\,|G' - D' - 1| = \frac{p^r - 1}{2}$$

$$\chi_1(E) = (|D| + 1)\,\chi_1(D') + |G - D|\,(-1 - \chi_1(D')) = \frac{-p^r - 1}{2}.$$

In the χ_2 calculations, there are 4 cases, depending on the values of $\chi_2(D)$ and $\chi_2(D')$. We will only do 1 of the cases here

$$\begin{aligned}\chi_2(E) &= \left(1 + \frac{-1 + \sqrt{p^r}}{2}\right)\left(\frac{-1 - \sqrt{p^r}}{2}\right)\\ &\quad + \left(-\frac{-1 + \sqrt{p^r}}{2}\right)\left(-1 - \frac{-1 - \sqrt{p^r}}{2}\right)\\ &= \frac{-1 - 2\sqrt{p^r} - p^r - 1 + 2\sqrt{p^r} - p^r}{4} = \frac{-1 - p^r}{2}.\end{aligned}$$

Since all of the character sums are correct, this is a PDS in the direct product of G and G'. □

If we apply this product construction inductively to the two constructions in this paper (the one due to Paley and the one in Corollary 3.1), we get the following family of groups that support a Paley PDS.

Corollary 3.2. *Any group of the form* $Z_{p^2}^{2a} \times Z_p^{4b}$ *will have a* $\left(p^{4a+4b}, \frac{p^{4a+4b} - 1}{2}, \frac{p^{4a+4b} - 5}{4}, \frac{p^{4a+4b} - 1}{4}\right)$ *Paley* PDS *whenever* $a + b$ *is a power of* 2. *This implies that the group* $Z_{p^2}^{2a} \times Z_p^{4b} \times Z_2$ *will have a* $\left(p^{4a+4b}, 2, p^{4a+4b}, p^{4a+4b} - 1, \frac{p^{4a+4b} - 1}{2}\right)$ *reversible* DDS.

Finally, we note that we can generalize the idea of combining the Leung-Ma construction together with PCP-type PDS for higher powers of the prime, but it is much more difficult to keep track of the character theory. We did not see any applications to the Paley parameters, so those results are not included in this paper.

Acknowledgement. The author would like to thank the referee for the very careful reading that was done.

References

[1] K. T. Arasu, D. Jungnickel and A. Pott, Divisible difference sets with multiplier -1. J. Algebra **133**, 35–62 (1990).

[2] K. T. Arasu, D. Jungnickel and A. Pott, Symmetric divisible designs with $k - \lambda_1 = 1$. Discrete Math. **97**, 25–38 (1991).

[3] K. T. Arasu, D. Jungnickel, S. L. Ma and A. Pott, Strongly regular Cayley graphs with $\lambda - \mu = -1$. To appear in J. Comb. Theory Ser. A.

[4] K. H. Leung and S. L. Ma, Construction of partial difference sets and relative difference sets on p-groups. J. Comb. Theory Ser. A **59**, 51–72 (1992).

[5] K. H. LEUNG, S. L. MA and V. TAN, Abelian divisible difference sets and relative difference sets on p-groups. Bull. London Math. Soc. **22**, 533–539 (1990).
[6] S. L. MA, Partial difference sets. Discrete Math. **52**, 75–89 (1984).
[7] S. L. MA, A survey or partial difference sets. To appear in Designs, Codes, and Cryptography.
[8] D. A. MARCUS, Number Fields. Berlin-Heidelberg-New York 1977.
[9] R. E. A. C. PALEY, On orthogonal matrices. J. Math. Phys. **12**, 311–320 (1933).
[10] R. J. TURYN, Character sums and difference sets. Pacific J. Math. **15**, 319–346 (1965).

Eingegangen am 9. 9. 1993 *)

Anschrift des Autors:

James A. Davis
Department of Mathematics
and Computer Science
University of Richmond
Richmond, VA 23173
USA

*) Eine Neufassung ging am 22. 2. 1994 ein.