Journal of Algebraic Combinatorics
https://doi.org/10.1007/s10801-020-00992-x

# On difference sets with small $\lambda$

**Daniel M. Gordon**[1]

Received: 14 January 2020 / Accepted: 5 November 2020


## Abstract
In a 1989 paper, Arasu (Arch Math 53:622–624, 1989) used an observation about multipliers to show that no $(352, 27, 2)$ difference set exists in any abelian group. The proof is quite short and required no computer assistance. We show that it may be applied to a wide range of parameters $(v, k, \lambda)$, particularly for small values of $\lambda$. With it, a computer search was able to show that the Prime Power Conjecture is true up to order $2 \cdot 10^{10}$, extend Hughes and Dickey's computations for $\lambda = 2$ and $k \leq 5000$ up to $10^{10}$, and show nonexistence for many other parameters.

**Keywords** Difference sets · Biplanes · Prime Power Conjecture

## 1 Introduction

A $(v, k, \lambda)$-difference set $D$ in a group $G$ of order $v$ is a set $\{d_1, d_2, \ldots, d_k\}$ of elements from $G$ such that every nonzero element of $G$ has exactly $\lambda$ representations as $d_i - d_j$. The *order* of $D$ is $n = k - \lambda$.

A *(numerical) multiplier* is an integer $m$ for which multiplication of each $d_i$ by $m$ produces a shift of the original difference set: $mD = D + g$ for some $g \in G$. The set of multipliers form a group $M$, and it is well-known that some translate of $D$ is fixed by $M$. This implies that a shift of $D$ can be written as a union of orbits of $G$ under $M$.

The First Multiplier Theorem states that any prime $p > \lambda$ which divides $n$ and not $v$ must be a multiplier of $D$. The Multiplier Conjecture is that the $p > \lambda$ condition is not needed. This is still open, but there have been many strengthenings of the First Multiplier Theorem; see [8] for recent results.

Many difference set parameters can be dealt with by finding a group of multipliers $M$ and looking at the resulting orbits. For instance, it may be that no union of orbits has

Dedicated to K.T. Arasu on the occasion of his 65th birthday.

✉ Daniel M. Gordon
gordon@ccrwest.org

[1] IDA Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121, USA

Published online: 21 November 2020 

size $k$, or the set of orbits may be small enough that all possibilities may be checked with a short search. Lander [10], gives many such examples.

Arasu [1] showed that no abelian biplanes (difference sets with $\lambda = 2$) of order 25 exist. Our main tool will be a generalization of his argument, which we restate here.

**Theorem 1** *No* $(352, 27, 2)$ *difference set exists in any abelian group* $G$.

***Proof*** Any such difference set has 5 as a multiplier. Take $p = 11$, and $H$ a group of order 32 so that $G = \mathbb{Z}_{11} \times H$. Then, $5^8 \equiv 1 \pmod{32}$, and so fixes $H$. The orbits of $\langle 5^8 \rangle$ in $\mathbb{Z}_{11}$ are $\{0\}$, $\{1, 3, 4, 5, 9\}$, and $\{2, 6, 7, 8, 10\}$. The orbits in $G$ are just these orbits with a fixed element $h \in H$.

A difference set $D$ made up of these orbits will have a certain number $a$ of 5-orbits $\langle (1, h) \rangle$ and $\langle (2, h) \rangle$, and $b = 27 - 5a$ 1-orbits. There are $b(b - 1)$ differences of the singleton orbits, each of which is of the form $(0, h)$ with $h \neq 0$. There are 31 such elements, and each must occur exactly twice as a difference of elements of $D$, and so $b(b - 1) \leq 31 \cdot 2 = 62$.

This means that we must have $b < 9$, and so $a \geq 4$. But the 20 differences from elements in one 5-orbit are all of the form $(x, 0)$, $x \neq 0$. There are 10 such elements, and in fact each of them occurs exactly twice in the differences of one 5-orbit. Since we have multiple 5-orbits, these elements will occur as differences too many times. □

One nice feature of this argument is that it takes care of all abelian groups $G$ of order 352 at once. Other arguments [2,10] only handle specific groups.

## 2 Extending the method

It is clear that Arasu's method can be applied to other parameter sets. In this section, we give a generalization of Theorem 1.

**Lemma 1** *Let* $G = \mathbb{Z}_p \times H$*, where* $H$ *is abelian and* $\gcd(p, |H|) = 1$*. Let* $m$ *be a multiplier of a* $(v, k, \lambda)$ *difference set, and* $s$ *be the smallest positive integer for which* $m^s \equiv 1 \pmod{\exp(H)}$*. Then, the orbits of* $G$ *under* $\langle m^s \rangle$ *are of the form* $(\mathcal{O}, h)$*, for fixed* $h \in H$*. There are exactly* $|H|$ *orbits* $(0, h)$ *of size 1, and the remaining orbits all have the same size* $o = \mathrm{ord}_p(m^s)$*.*

***Proof*** The proof of this is the same as for Theorem 1. The group of multipliers generated by $m^s$ will fix all $h \in H$ Because $p$ is prime, all the nonzero orbits of $\mathbb{Z}_p$ under this group will have the same size, some divisor of $p - 1$.

Now for any $(v, k, \lambda)$, if we can find a prime $p | v$ and multiplier $m$ for which $m^s$ has a reasonably large order mod $p$, we can look at differences of the 1-orbits and $o$-orbits and try to get a contradiction: if there are $a$ orbits of size $o$, and $b$ 1-orbits, then we have:

**Theorem 2** *Let* $G = \mathbb{Z}_p \times H$*, where* $H$ *is abelian and* $\gcd(p, |H|) = 1$*. Let* $m$ *be a multiplier of a* $(v, k, \lambda)$ *difference set, and* $s$ *be the smallest positive integer for which*

*$m^s \equiv 1 \pmod{\exp(H)}$, and $o = \mathrm{ord}_p(m^s)$. If there is no solution in positive integers $a$ and $b$ to:*

$$k = ao + b, \tag{1}$$

$$b(b-1) \leq \lambda(|H|-1), \tag{2}$$

$$a \cdot o(o-1) \leq \lambda(p-1), \tag{3}$$

*then no $(v, k, \lambda)$ difference set exists in $G$.*

This method will be most useful when $\lambda$ is small, since each element can only occur $\lambda$ times as a difference, so whatever the choice of orbits either elements of the form $(x, 0)$ or $(0, h)$ are likely to occur too many times. Still, when $n$ and $v$ have large prime factors ($n$ so that we have a known multiplier, and $v$ so that we have a suitable $p$ to use in Theorem 2), it can still often be applied.

When Theorem 2 fails, if $G$ is cyclic we will sometimes use the theorem of Xiang and Chen [11]:

**Theorem 3** *Let $D$ be a $(v, k, \lambda)$ difference set in a cyclic group $G$ with multiplier group $M$. Except for the $(21, 5, 1)$ difference set, $|M| \leq k$.*

This theorem may be extended to contracted multipliers as well (see Section VI.5 of [4] for information about difference lists and contracted multipliers).

**Theorem 4** *Let $D$ be a $(v, k, \lambda)$ difference set in a cyclic group $G$, and $H$ be the subgroup of $G$ of order $h$ and index $u$. Then, with the same exception, the group $M$ of $G/H$-multipliers has order $|M| \leq k$.*

***Proof*** The proof is exactly the same as the proof of Theorem 3 in [11], replacing multipliers with contracted multipliers. $M$ is isomorphic to a subgroup of Gal $\mathbb{Q}(\zeta_u)/\mathbb{Q}$, where $\zeta_u$ is a primitive $u$th root of unity. Let

$$S = \overline{D} = \{\overline{d_1}, \overline{d_2}, \ldots, \overline{d_k}\}$$

be the $(u, k, h, \lambda)$ difference list over $G/H$ obtained by sending the elements of $D$ to their image in $G/H$. By Theorem 5.14 of [4], we may assume that $S$ is fixed by $M$. Let $\chi$ be a generator of the character group of $G/H$, $K = \mathbb{Q}\left(\chi(S), \chi^2(S), \ldots, \chi^{u-1}(S)\right)$, and $\alpha_t$ be the field automorphism sending $\zeta_u \mapsto \zeta_u^t$. As in [11], we may show that Gal $\mathbb{Q}(\zeta_u)/K = M$. If $t \in M$, it fixes $S$, so $\alpha_t$ fixes $\chi(S)$. If $\alpha_t$ fixes $\chi^i(S)$ for $i = 1, 2, \ldots, u-1$, then by Fourier inversion $t$ fixes $S$, and so is in $M$.

Now, let

$$f(X) = \prod_{i=1}^{k} \left(X - \chi(\overline{d_i})\right).$$

The coefficients of $f(X)$ are elementary symmetric polynomials in the $\chi(\overline{d_i})$, which are fixed by $\alpha_t$ for any $t \in M$, so $f(X) \in K[X]$.

By Theorem 1 of Cohen [5], if $D$ is not the (21,5,1) difference set, then at least one of the $d_i$ is relatively prime to $v$, and so $\chi(\overline{d_i})$ is a primitive $u$th root of unity. It is also a root of $f(X)$, and so

$$|M| = [\mathbb{Q}(\zeta_u) : K] \leq \deg f(X) = k.$$

□

## 3 The prime power conjecture

A $(v, k, 1)$ difference set is called a planar abelian difference set. These exist if $n = k - 1$ is a prime power, and the Prime Power Conjecture (PPC) is that these are the only ones. In [6], it was shown that the PPC is true for all groups for orders up to $2 \cdot 10^6$, and in [3] for cyclic groups for orders up to $2 \cdot 10^9$.

In these papers, non-prime power orders were eliminated by a series of tests; see [6] for details. The initial tests only depended on the prime factors of $n$ and $v$, and were very fast. Tables 1 and 2 in [6] gave lists of $(v, k, 1)$ planar abelian difference set parameters which could not be eliminated with these tests. To show they did not exist, Proposition 5.11 of Lander [10] was used:

**Theorem 5** *If $t_1, t_2, t_3, t_4$ are numerical multipliers of a $(v, k, 1)$ difference set in G, and*

$$t_1 - t_2 \equiv t_3 - t_4 \pmod{\exp(G)},$$

*then* $\exp(G)$ *divides* $\operatorname{lcm}(t_1 - t_2, t_1 - t_3)$.

For each case, a large number of multipliers were generated, until either a prime known not to be an extraneous multiplier was discovered, or two pairs of multipliers with the same difference modulo $\exp(G)$ were found, so that Theorem 5 could be applied. These calculations required a substantial amount of computation time and memory.

With Theorem 2, the hard cases from [6] can be eliminated quickly. To illustrate the power of the theorem, Table 1 gives parameters used in Theorem 2 to eliminate some of the parameters in the tables in [6]; with the value of $o$ in the last column, it is easy to check that there are no positive integers $a$ and $b$ solving Eqs. (1), (2) and (3).

Using Arasu's method allows the computations to be redone in a different manner. In addition, it requires far less work for the hard cases, so it was possible to take the computations further. Replicating the search up to $2 \cdot 10^6$ took under a minute on a workstation. A longer run using the fast tests from [6] and Theorem 2 eliminated every order up to $2 \cdot 10^{10}$ except for the ones given in Table 2, which were then eliminated using Theorem 5. Note that the first two values of $k$ were missing from the tables in [6].

Unlike the fast tests in [6], for which the number passing was roughly linear in the bound on $n$, Theorem 2 gets more effective for larger orders, since it becomes increasingly likely that $v$ will have a large prime factor $p$ for which some prime divisor of $n$ has large order mod $p$. All values of $k$ between $7.7 \cdot 10^9$ and $2 \cdot 10^{10}$ were

**Table 1** Small $(v, k, 1)$ parameters from Tables 1 and 22 of [6] eliminated by Theorem 2

| $k$ | $p$ | $\|H\|$ | $m^s$ | $\mathrm{ord}_p(m^s)$ |
|---|---|---|---|---|
| 2436 | 5,931,661 | 1 | $5^1$ | 435 |
| 24,452 | 199,291,951 | 3 | $499^1$ | 6175 |
| 45,152 | 22,651 | 90,003 | $277^{789}$ | 25 |
| 56,408 | 24,781 | 128,397 | $4339^{63}$ | 295 |
| 58,724 | 450,601 | 7653 | $8389^{75}$ | 751 |
| 2444 | 109 | 54,777 | $7^{465}$ | 9 |
| 3234 | 4759 | 2197 | $61^{507}$ | 61 |
| 72,012 | 35,911 | 144,403 | $673^{245}$ | 513 |
| 73,482 | 149,113 | 36,211 | $373^9$ | 2071 |

**Table 2** $(v, k, 1)$ parameters up to $k = 2 \cdot 10^{10}$ not eliminated by Theorem 2

| $k$ | $n$ | $v$ |
|---|---|---|
| 1,096,386 | $5 \cdot 219{,}277$ | $79 \cdot 109 \cdot 1951 \cdot 71{,}551$ |
| 1,320,794 | $373 \cdot 3541$ | $3 \cdot 11{,}551 \cdot 50{,}341{,}831$ |
| 2,378,196 | $5 \cdot 475{,}639$ | $211 \cdot 631 \cdot 3319 \cdot 12{,}799$ |
| 20,846,324 | $61 \cdot 341{,}743$ | $3 \cdot 88{,}951 \cdot 1{,}628{,}496{,}601$ |
| 40,027,524 | $107 \cdot 374{,}089$ | $7 \cdot 13 \cdot 3541 \cdot 54{,}163 \cdot 91{,}801$ |
| 2,830,957,656 | $5 \cdot 566{,}191{,}531$ | $109^2 \cdot 1171 \cdot 1231 \cdot 1951 \cdot 239{,}851$ |
| 7,700,562,788 | $9817 \cdot 784{,}411$ | $3 \cdot 61^2 \cdot 1831 \cdot 1{,}703{,}287^2$ |

eliminated, and a heuristic argument suggests that the number of cases up to order $n$ passing Theorem 2 will be at most $O(\log n)$.

## 4 Biplanes

Theorem 1 was also shown by Hughes in [9]. Computations by Hughes and Dickey reported in that paper showed that no abelian $(v, k, 2)$ difference sets exist with order less than 5000, except for the known cases $k = 3, 4, 5, 6$ and 9. They give few details about their method; it is possible that their method was something similar to that of Arasu.

A run up to order $10^{10}$ eliminated all but 24 parameters. Most of the rest were dealt with using Theorems 4.19 and 4.38 of Lander [10]. Table 3 gives the remaining open cases.

Theorem 4 was an important tool for eliminating open cases in this and the next table. Biplanes of order a power of 4, such as (525826, 1026, 2), pass Theorem 2 and have no known multipliers, so the standard methods are no help. However, in each case up to order $2^{30}$ we have that $G$ is cyclic, 2 is a $G/H$ multiplier for $H$ the group of order 2 by the Contracted Multiplier Theorem (Corollary 5.13 of [4]), and the order $\mathrm{ord}_{v/2}(2)$ is larger than $k$, showing that those biplanes do not exist.

**Table 3** Open $(v, k, 2)$ cases for $k \leq 10^{10}$

| $k$ | $n$ | $v$ |
|---|---|---|
| 47,433 | 47,431 | $13{,}693 \cdot 82{,}153$ |
| 86,013 | 86,011 | $7 \cdot 71 \cdot 883 \cdot 8429$ |
| 890,196 | $2 \cdot 445{,}097$ | $396{,}224{,}014{,}111$ |
| 1,120,521 | 1,120,519 | $83{,}059 \cdot 7{,}558{,}279$ |
| 1,767,189 | 1,767,187 | $7 \cdot 223{,}068{,}228{,}181$ |
| 937,097,469 | 937,097,467 | $19{,}942{,}759 \cdot 22{,}016{,}804{,}833$ |

**Table 4** Open $(v, k, 3)$ cases for $k \leq 10^{10}$

| $k$ | $n$ | $v$ |
|---|---|---|
| 120 | $3^2 \cdot 13$ | $3^2 \cdot 23^2$ |
| 441 | $2 \cdot 3 \cdot 73$ | $71 \cdot 911$ |
| 2350 | 2347 | 1840,051 |
| 740,406 | $3^2 \cdot 82{,}267$ | $3^4 \cdot 19{,}391 \cdot 116{,}341$ |
| 3,793,567 | $2^2 \cdot 948{,}391$ | $5^2 \cdot 251 \cdot 397 \cdot 463 \cdot 4159$ |
| 28,9842,739 | $2^4 \cdot 18{,}115{,}171$ | $3 \cdot 5 \cdot 23 \cdot 103^2 \cdot 137 \cdot 223^2 \cdot 1123$ |

## 5 General parameters

Theorem 2 may be applied for larger $\lambda$; while more parameters will slip through because of a lack of known multipliers or Equations (2) and (3) being less restrictive, many may still be eliminated. A run was done for difference sets with $\lambda = 3$ up to order $10^{10}$. There were 269 parameters that passed Theorem 2, but most were then eliminated with Theorems 3 and 4, the Lander tests, and the Mann test ([4], Theorem VI.6.2). Table 4 shows the six remaining cases.

The author has set up the La Jolla Difference Set Repository [7], an online database containing existence results for parameters up to $v = 10^6$, as well as a large number of known difference sets. There are 1.44 million parameters that pass basic counting and the BRC theorem, of which about 180,000 were open. Applying Theorems 2 and 4 resolved over 50,000 of them.

**Acknowledgements** We thank the anonymous referee for suggestions that led to Theorem 4.

## References

1. Arasu, K.T.: Singer groups of biplanes of order 25. Arch. Math. **53**, 622–624 (1989)
2. Arasu, K.T., Davis, J., Jungnickel, D., Pott, A.: A note on intersection numbers of difference sets. European J. Combin. **11**, 95–98 (1990)
3. Baumert, L.D., Gordon, D.M.: On the existence of cyclic difference sets with small parameters. In: Van Der Poorten, Stein (eds.) High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday

of Hugh Cowie Williams. Conference in Number Theory in Honour of Professor H.C. Williams, pp. 61–68 (2004)
4. Beth, T., Jungnickel, D., Lenz, H.: Design Theory, Volume 1 of Encyclopedia of Mathematics and Its Applications, 2nd edn. Cambridge University Press, Cambridge (2011)
5. Cohen, Stephen D.: Generators in cyclic difference sets. J. Combin. Theory Ser. A **51**, 227–236 (1989)
6. Gordon, D.M.: The prime power conjecture is true for $n < 2{,}000{,}000$. Electron. J. Combin. **1**, R6 (1994)
7. Gordon, D.M.: La Jolla difference set repository. https://www.dmgordon.org/diffset (2020)
8. Gordon, D.M., Schmidt, B.: A survey of the multiplier conjecture In: Designs, Codes and Crypt., pp. 221–236 (2016)
9. Hughes, D.: Biplanes and semi-biplanes. In: Holton, D.A., Seberry, J. (eds.) Combinatorial Mathematics, pp. 55–58. Springer, Berlin (1978)
10. Lander, E.S.: Symmetric Designs: An Algebraic Approach, Volume 74 of LMS Lecture Note Series. Cambridge (1983)
11. Xiang, Q., Chen, Y.Q.: On the size of the multiplier groups of cyclic difference sets. J. Combin. Theory Ser. A **69**, 168–169 (1995)