Some Restrictions on Orders of Abelian Planar Difference Sets

Daniel M. Gordon
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121
email: gordon@ccrwest.org

ABSTRACT. The Prime Power Conjecture (PPC) states that abelian planar difference sets of order n exist only for n a prime power. Lander and others have shown that orders divisible by certain composites can be eliminated. In this paper we show how to extend this list of excluded orders.

1 Introduction

Let G be a group of order v, and D be a set of k elements of G. If the set of differences $d_i - d_j$ contains every nonzero element of G exactly λ times, then D is called a (v, k, λ)-difference set in G. The order of the difference set is $n = k - \lambda$. If $\lambda = 1$, the difference set is called planar. We will be concerned with abelian planar difference sets.

A *multiplier* is an automorphism α of G which takes D to a translate $g + D$ of itself for some $g \in G$. If α is of the form $\alpha: x \to tx$ for $t \in \mathbf{Z}$ relatively prime to the order of G, then α is called a *numerical* multiplier.

The First Multiplier Theorem says that for a planar abelian difference set of order n any divisor t of n will be a numerical multiplier. A common approach to proving nonexistence of difference sets is to look at the group of numerical multipliers and find necessary conditions on n. One tool for this is the following theorem of Lander [8], which was shown by Hall [6] in the cyclic case:

Theorem 1.1. *Let D be a planar abelian difference set of order n in G. If t_1, t_2, t_3, and t_4 are numerical multipliers such that*

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

JCMCC **29** (1999), pp. 241-246

then $\exp(G)$ *divides the least common multiple of* $(t_1 - t_2, t_1 - t_3)$.

The cyclic version of this test was the main tool used by Evans and Mann [4] to show the nonexistence of non-prime power difference sets for $n \leq 1600$. It was used by the author [5] to show that the Prime Power Conjecture is true for orders less than 2,000,000.

Suppose for given primes $p_1, p_2, \ldots, p_r$, we can find $\{t_1, t_2, t_3, t_4\}$ where the t_i are products of powers of the p_j's and $t_1 - t_2 = t_3 - t_4$. Since the t_i are multipliers of any planar abelian difference set of order n divisible by $p_1 p_2 \ldots p_r$ by the First Multiplier Theorem, and $\exp(G) = |G| = n^2 + n + 1$ for G cyclic, the only possible cyclic difference sets have $n^2 + n + 1 | \mathrm{lcm}(t_1 - t_2, t_1 - t_3)$. For example, any planar cyclic difference set of order dividing 26 has multipliers 1, 4, 13 and 16, and so $n^2 + n + 1 | \mathrm{lcm}(4 - 1, 13 - 1) = 3$.

For non-cyclic groups, the exponent of the group may be much smaller than v. Lander showed that the exponent of G cannot be a multiple of 2, 5 or 9 (since $n^2 + n + 1$ has no root modulo any of those numbers), and so if $\mathrm{lcm}(t_1 - t_1, t_1 - t_3) = 2^a 3^b 5^c$, the only cases we have to worry about $v = 1$ and $v = 3$, which are impossible.

That left open orders a multiple of 22, 46 and 58, where the lcm was $2^a 3^b 5^c 7^d$. Jungnickel and Pott [7] excluded these cases by showing that an abelian planar difference set of even order cannot exist in a group of exponent 7 or 21. These results together show:

Theorem 1.2. *Let D be a planar abelian difference set of order n. Then n cannot be divisible by 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58, 62 or 65.*

In the next section we will generalize these arguments, which will allow us to add many more excluded orders to this list. These excluded orders could have greatly reduced the time needed to eliminate all small orders in [5].

2 Possible Exponents of G

Let D be a difference set of order n in a group G. The order of G is $v = n^2 + n + 1$, and its exponent is a divisor of v.

Theorem 2.1. *The exponent of G is divisible by at most one power of 3. All its other prime divisors are primes $p \equiv 1 \pmod 3$, which may occur to any power.*

Proof: Suppose $p | n^2 + n + 1$. Then $f(x) = x^2 + x + 1$ has a root mod p, and so p splits or ramifies in the field $K = \mathbf{Q}(\sqrt{-3})$. The only prime that ramifies in this field is 3, and only a single power of 3 can divide v. Only primes $\equiv 1 \pmod 3$ split. By Hensel's Lemma, any of these primes can divide v to arbitrarily high powers. □

Corollary 2.2. *Suppose that for an order n, $\{t_1, t_2, t_3, t_4\}$ have been found which are products of prime divisors of n and have $t_1 - t_2 = t_3 - t_4$. If $\text{lcm}(t_1 - t_2, t_1 - t_3)$ is divisible only by powers of 3, primes dividing n, and primes $p \equiv 2 \pmod 3$, then no difference set of order $\equiv 0 \bmod n$ exists.*

Proof: By Theorem 1.1, $\exp(G)$ divides the lcm. By Theorem 2.1, no $p \equiv 2 \pmod 3$ and at most one power of 3 can divide v. Since v and n are relatively prime, primes dividing n are also excluded, so we have $\exp(G) = 3$ and $v = 3^k$, but no such difference sets exist. □

6	10	14	15	21	26	33	34
35	38	39	51	55	57	62	65
91	122	123	133	145	155	219	249
267	301	482	489	505	514	542	671
679	703	723	753				

Table 1. Orders less than 1000 excluded by Theorem 2.3

Lander [8] used a special case of the above corollary to get his result, using t's with least common multiples of the form $2^a 3^b 5^c$ to exclude 13 orders up to 65 (he left out 34, 35 and 39). By carrying the calculations further, we may exclude many more orders:

Theorem 2.3. *There are no planar abelian difference sets with orders a multiple of any of the numbers given in Table 1.*

We omit the $t_1, \ldots t_4$ which provide the proofs for the orders in Table 1. They were found by generating all combinations of powers of divisors of n less than one million, and looking for pairs with common differences. Those for which $\text{lcm}(t_1 - t_2, t_1 - t_3)$ satisfies the conditions of 2.2 cannot have a difference set.

For example, for $n = 753 = 251 \cdot 3$, take $t_1 = 251$, $t_2 = 9 = 3^2$, $t_3 = 243 = 3^5$, and $t_4 = 1$. We have $251 - 9 = 243 - 1$, and $\text{lcm}(251 - 9, 251 - 243) = 2^4 \cdot 11^2$.

3 Dealing with splitting primes

There are many values of n for which $\text{lcm}(t_1 - t_2, t_1 - t_3)$ will always be divisible by a splitting prime. For example, for $n = 22$, since $\langle 11 \mod 7 \rangle$ and $\langle 2 \mod 7 \rangle$ are both $\{1, 2, 4\}$, any set of t's for which $t_1 - t_2 = t_3 - t_4$ will have $\text{lcm}(t_1 - t_2, t_1 - t_3)$ divisible by 7.

Jungnickel and Pott [7] showed that there are no difference sets in groups of exponent 7 or 21. Their arguments, which involve looking at the values of n, divisors of n, and v modulo 3 and 4, could be extended to some other exponents, but would have to be done on a case-by-case basis, and would

not work for all exponents. We take another approach, using the arithmetic of $\mathbf{Q}(\sqrt{-3})$ and results about Diophantine equations to get a method which works for a large family of exponents.

Suppose that for some n we have $\text{lcm}(t_1 - t_2, t_1 - t_3)$ divisible by primes $p_1, p_2, \ldots, p_r$ congruent to 1 mod 3. Any planar abelian difference set of order n is a solution to

$$n^2 + n + 1 = 3^\epsilon \cdot p_1^{k_1} \cdot p_2^{k_2} \ldots p_r^{k_r}, \tag{1}$$

where ϵ is 0 or 1, depending on whether the lcm is divisible by 3. By [5], if we can show that all solutions to (1) have $n < 2,000,000$, then no such difference sets exist.

In the previous section we dealt with the case $r = 0$. For larger r, the following theorem shows that only a finite amount of work is needed for each case.

Theorem 3.1. *For any fixed $r \geq 0$ and $p_1, \ldots, p_r$, there are only a finite number of solutions to (1).*

Proof: Consider how (1) factors in $\mathbf{Q}(\sqrt{-3})$. Let $\beta = (1 + \sqrt{-3})/2$. Then (1) becomes

$$(n - \beta)(n - \overline{\beta}) = 3^\epsilon \wp_1^{k_1} \overline{\wp}_1^{k_1} \ldots \wp_r^{k_r} \overline{\wp}_r^{k_r}$$

where each $p_i = \wp_i \overline{\wp}_i$. Each $\wp_i$ can only divide one of $n - \beta$ and $n - \overline{\beta}$. Thus, for some choice of γ with $\gamma\overline{\gamma} = 3^\epsilon$ and which factor of p_i is called $\wp_i$, we have

$$(n - \beta) = \gamma \wp_1^{k_1} \ldots \wp_r^{k_r}$$

and

$$(n - \overline{\beta}) = \overline{\gamma}\, \overline{\wp}_1^{k_1} \ldots \overline{\wp}_r^{k_r}$$

Subtracting these two equations, we get

$$\beta - \overline{\beta} = \gamma \wp_1^{k_1} \ldots \wp_r^{k_r} - \overline{\gamma}\, \overline{\wp}_1^{k_1} \ldots \overline{\wp}_r^{k_r}.$$

Let $\lambda = \gamma/(\beta - \overline{\beta})$, and

$$G_{k_1,\ldots,k_r} = \lambda \wp_1^{k_1} \ldots \wp_r^{k_r} - \overline{\lambda} \overline{\wp}_1^{k_1} \ldots \overline{\wp}_r^{k_r}.$$

Then we are looking for solutions to $G_{k_1,\ldots,k_r} = 1$, for which

$$\left| \frac{\lambda}{\overline{\lambda}} \left(\frac{\wp_1}{\overline{\wp}_1} \right)^{k_1} \cdots \left(\frac{\wp_r}{\overline{\wp}_r} \right)^{k_r} - 1 \right| = \frac{1}{|\overline{\lambda}|} p_1^{-k_1/2} \ldots p_r^{-k_r/2}.$$

To see that there are only finitely many such solutions, let $\psi = \log(\lambda/\overline{\lambda})$, $\varphi_i = \log(\wp_i/\overline{\wp}_i)$, and choose m such that $|\psi + \sum_{i=1}^r k_i \varphi_i + m| \leq 1/2$. Let $\Lambda = 2\pi i(\psi + \sum_{i=1}^r k_i \varphi_i + m)$.

Then

$$|\Lambda| = 2\pi|\psi + \sum_{i=1}^{r} k_i\varphi_i + m| \le \frac{\pi}{2}\left|e^{2\pi i(\psi+\sum_{i=1}^{r} k_i\varphi_i+m)} - 1\right|$$

$$= \frac{\pi}{2}\left|\left(\frac{\lambda}{\overline{\lambda}}\right)\cdot\prod_{i=1}^{r}\left(\frac{\varphi_i}{\overline{\varphi}_i}\right)^{k_i} - 1\right| = \frac{\pi}{2}\frac{1}{|\mu|}\cdot p_1^{-k_1/2}\ldots p_r^{-k_r/2}. \qquad (2)$$

To prove the theorem, we can combine this equation with lower bounds for linear forms in logarithms. Such bounds were first introduced by Baker [1], and have improved over the years. The following theorem is a special case of the best current result, due to Baker and Wüstholz [2].

Theorem 3.2. *For $\Lambda \neq 0$ defined as above, and $K = \max\{k_1, \ldots, k_r\}$, we have*

$$\log|\Lambda| > -(32r)^{2(r+2)}\log p_1 \ldots \log p_r \log K.$$

Together with (2), this proves that there are only a finite number of solutions to (1). □

Note that the bound of Theorem 3.1 is too large to actually check, even in small cases. Fortunately, de Weger [3] gives algorithms for reducing the bounds to manageable numbers. For $r = 1$, Algorithm I of [3] uses the continued fraction expansion of φ. It finds a new bound on $k = k_1$ such that any solution greater than that bound must be a simple function of the convergents. By repeatedly applying the algorithm, k is typically reduced to a number as small as 6. The largest prime p_1 needed for any of the orders in Table 2 was 103.

22	46	58	86	87	94	134	142
146	158	159	194	226	237	254	262
321	386	526	611	745	766	807	898

Table 2. Orders less than 5000 with $r = 1$

For $r \ge 2$, lattice reduction is used in place of the continued fraction expansion to reduce the bounds (see Chapter 7 of [3] for a discussion of the multidimensional problem). The computational demands go up rapidly with r, but only three orders less than 1000 require $r = 2$: 183, 362 and 382. The first two have $p_1 = 13$, $p_2 = 7$, and for 382 we have $p_1 = 127$, $p_2 = 7$.

Several computer programs were used to form the tables and eliminate each order. The first step was to find sets of t's for each n with the fewest number of primes $\equiv 1 \bmod 3$ dividing the lcm. For each such n, the continued fraction method (for $r = 1$) or L^3 method (for $r = 2$) were used to get reasonable bounds for K. After that, it was a simple matter to

exhaustively check for solutions to $G_{k_1,\ldots,k_r} = 1$. Of the solutions that were found, all had $n < 2,000,000$, and all such orders were eliminated in [5].

References

[1] A. Baker, Linear forms in the logarithms of algebraic numbers, *Mathematika* **13** (1966), 204–216.

[2] A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. reine angew. Math.*, **442** (1993), 19–62.

[3] B.M.M. de Weger, Algorithms for diophantine equations, CWI, 1989.

[4] T.A. Evans and H.B. Mann, On simple difference sets, *Sankhya* **11** (1951), 357–364.

[5] D.M. Gordon, The prime power conjecture is true for $n < 2,000,000$, *Electronic J. Combinatorics* **1** (1994).

[6] M. Hall, Jr., Cyclic projective planes, *Duke J. Math.*, **14** (1947), 1079–1090.

[7] D. Jungnickel and A. Pott, Two results on difference sets, *Coll. Math. Soc. János Bolyai* **52** (1988), 325–330.

[8] E.S. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, 1983.