The Prime Power Conjecture is True for $n < 2{,}000{,}000$

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

Submitted: August 11, 1994; Accepted: August 24, 1994.

Abstract

The Prime Power Conjecture (PPC) states that abelian planar difference sets of order n exist only for n a prime power. Evans and Mann [2] verified this for cyclic difference sets for $n \leq 1600$. In this paper we verify the PPC for $n \leq 2{,}000{,}000$, using many necessary conditions on the group of multipliers.

AMS Subject Classification. 05B10

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 $n = k - \lambda$. We will be concerned with abelian planar difference sets: those with G abelian and $\lambda = 1$.

The Prime Power Conjecture (PPC) states that abelian planar difference sets of order n exist only for n a prime power. Evans and Mann [2] verified this for cyclic difference sets for $n \leq 1600$.

In this paper we use known necessary conditions for existence of difference sets to test the PPC up to two million. Section 2 describes the tests used, and Section 3 gives details of the computations. All orders not the power of a prime were eliminated, providing stronger evidence for the truth of the PPC.

2 Necessary Conditions

We begin by reviewing known necessary conditions for the existence of planar difference sets. The oldest is the Bruck-Ryser-Chowla Theorem, which in the case we are interested in states:

Theorem 1 *If $n \equiv 1, 2 \pmod 4$, and the squarefree part of n is divisible by a prime $p \equiv 3 \pmod 4$, then no difference set of order n exists.*

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 $t \in \mathbb{Z}$ relatively prime to the order of G, then α is called a *numerical* multiplier. Most nonexistence results for difference sets rely on the properties of multipliers.

Theorem 2 *(First Multiplier Theorem) Let D be a planar abelian difference set, and t be any divisor of n. Then t is a numerical multiplier of D.*

Investigating the group of numerical multipliers is a powerful tool for proving nonexistence. McFarland and Rice [7] showed:

Theorem 3 *Let D be an abelian (v, k, λ)-difference set in G, and M be the group of numerical multipliers of D. Then there exists a translate of D that is fixed by every element of M.*

This implies that D is a union of orbits of M. Many sets of parameters for abelian difference sets can be eliminated by finding the orbits of M and showing that no combination of them has size k.

The following theorem of Ho [3] shows that M cannot be too large.

Theorem 4 *Let M be the group of multipliers of an abelian planar difference set of order n. Then $|M| \leq n + 1$, unless $n = 4$ (where $|M| = 6$).*

A number of necessary conditions on the multipliers have been proved by various authors. Theorem 8.8 of [5] gives the following useful conditions:

Theorem 5 *Let D be a planar abelian difference set of order n. Let p be a prime divisor of n and q be a prime divisor of v. Then each of the following conditions implies that n is a square:*

$$D \text{ has a multiplier which has even order} \pmod q. \tag{1}$$

$$p \text{ is a quadratic nonresidue} \pmod q. \tag{2}$$

$$n \equiv 4 \text{ or } 6 \pmod 8. \tag{3}$$

$$n \equiv 1 \text{ or } 2 \pmod 8 \text{ and } p \equiv 3 \pmod 4. \tag{4}$$

$$n \equiv m \text{ or } m^2 \pmod{m^2 + m + 1} \text{ and } p \text{ has even order} \pmod{m^2 + m + 1}. \tag{5}$$

This is particularly useful when combined with the following theorem of Jungnickel and Vedder [4]:

Theorem 6 *If a planar difference set of order $n = m^2$ exists in G, then there exists a planar difference set of order m in some subgroup of G.*

In that paper, it is also shown that

Theorem 7 *If a planar difference set has even order n, then $n = 2$, $n = 4$, or n is a multiple of* 8.

Wilbrink [8] proved the following:

Theorem 8 *If a planar difference set has order n divisible by* 3*, then $n = 3$ or n is a multiple of* 9.

The following result is due to Lander [6]:

Theorem 9 *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*

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

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 [2] to show the nonexistence of non–prime power difference sets for $n \leq 1600$. It can be used to immediately rule out many possible orders [5]:

Corollary 1 *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.

Evans and Mann also used the following tests to eliminate possible orders for planar cyclic difference sets. By Theorem 5, condition 5, they also apply to planar abelian difference sets:

Theorem 10 *Let D be a planar abelian difference set of order n. Let p be a prime divisor of n. Then each of the following conditions implies that n is a square:*

$$\begin{aligned}
n &\equiv 1 \pmod 3, p \equiv 2 \pmod 3. \\
n &\equiv 2,4 \pmod 7, p \equiv 3,5,6 \pmod 7. \\
n &\equiv 3,9 \pmod{13}, p \not\equiv 1,3,9 \pmod{13}. \\
n &\equiv 5,25 \pmod{31}, \left(\frac{p}{31}\right) = -1. \\
n &\equiv 6,36 \pmod{43}, \left(\frac{p}{43}\right) = -1. \\
n &\equiv 7,11 \pmod{19}, \left(\frac{p}{19}\right) = -1.
\end{aligned}$$

A prime p in the multiplier group is called an *extraneous* multiplier if $p \not| n$. A theorem due to Ho (see [1]), uses extraneous multipliers to rule out some orders.

Theorem 11 *Let p be a prime, which is a multiplier of an abelian planar difference set of order n. If $3 | n^2 + n + 1$ or $(p + 1, n^2 + n + 1) \neq 1$, then n is a square in $GF(p)$.*

3 Eliminating Possible Orders

In order to prove the PPC for $n \leq N$, we first use the following quick tests to eliminate most values of n:

1. Eliminate prime powers in $\{1, \ldots, N\}$.
2. Eliminate squares by Theorem 6.
3. Eliminate n which do not satisfy the Bruck-Chowla-Ryser theorem.
4. Use Corollary 1 to eliminate multiples of 6, 10, ...
5. Eliminate even n which are not multiples of 8, by Theorem 7.
6. Eliminate $n \equiv 3, 6 \pmod 9$, by Theorem 8.
7. Eliminate $n \equiv 1, 2 \pmod 8$ with a prime divisor $p \equiv 3 \pmod 4$, by Theorem 5, condition 4.
8. Eliminate n excluded by Theorem 10.

These tests can be done very quickly, and leave 173,596 possible orders less than two million.

The next test is to factor n and v, and use condition 2 of Theorem 5. For each $p|n$ and $q|v$, we check if $(p|q) = -1$. This leaves 85516 possible orders, of which 83222 have squarefree v (and so must be cyclic) and 2294 do not.

The next step is to use the First Multiplier Theorem and Theorem 4. Let v^* be the minimal possible order of $\exp(G)$ for an abelian group of order v. We have

$$v^* = \prod_{\substack{p|v \\ p \text{ prime}}} p,$$

and $v^* | \exp(G)$.

Let $p_1, p_2, \ldots p_r$ be primes dividing n. Then $\langle p_1, \ldots, p_r \rangle$, the subgroup of $\mathbb{Z}/v^*\mathbb{Z}$ generated by $p_1, \ldots, p_r$, is a subgroup of the group of numerical multipliers of any difference set of order n. If the size of this group is greater than $n+1$, then by Theorem 4 we cannot have a difference set of order n.

This test eliminated almost all of the remaining possible orders. The rest were eliminated using Theorems 9 and 11. For each order the multiplier group M was generated, and differences $t_i - t_j \pmod v$ less than one million were stored in a hash table. The process continued until a prime multiplier which satisfied the conditions of Theorem 11 was encountered, or a collision was found. A collision gave a set of multipliers t_1, t_2, t_3 and t_4 with $t_1 - t_2 \equiv t_3 - t_4 \pmod v$. If $v^* \not| \operatorname{lcm}(t_1 - t_2, t_3 - t_4)$, then we have a proof that no difference set of order n exists.

The orders eliminated in this way are given in Table 1 and 2. Table 1 gives the squarefree orders, and Table 2 the nonsquarefree ones. For the latter orders, each possible exponent v' with $v^*|v'|v$ was tested separately. If the multiplier group for an exponent larger than v^* was greater than $n+1$, it could be eliminated immediately, and was not included in the table.

n	$\exp(G)$	Nonexistence proof
2435	5931661	$238654 - 63632 = 175023 - 1$
24451	597875853	$691945 - 278968 = 661978 - 249001$
45151	2038657953	$p = 347821$ is an extraneous multiplier, $(n\|p) = -1$
56407	3181806057	$2801176 - 1783075 = 2544382 - 1526281$
58723	3448449453	$2243179 - 1211197 = 1034383 - 2401$
176723	31231195453	$60728299 - 60182930 = 31325592 - 30780223$
257083	66091925973	$375477574 - 375165064 = 74530342 - 74217832$
339203	115059014413	$3375768433 - 3375251728 = 1816976863 - 1816460158$
357575	127860238201	$91601372 - 90598866 = 49830631 - 48828125$
381959	145893059641	$719055731 - 718803023 = 64826764 - 64574056$
424733	180398546023	$1158732738 - 1158508082 = 268638427 - 268413771$
474563	225210515533	$39091685 - 38943434 = 8015875 - 7867624$
632663	400263104233	$3599415514 - 3598770282 = 908866176 - 908220944$
660323	436027124653	$61400216 - 61255940 = 45722527 - 45578251$
720287	518814082657	$4307002579 - 4306857623 = 3905399286 - 3905254330$
723719	523769914681	$3784025046 - 3783677394 = 1861644742 - 1861297090$
838487	703061287657	$43760576 - 43118230 = 41161497 - 40519151$
882671	779108976913	$132083219835 - 132082512788 = 44141413687 - 44140706640$
912425	832520293051	$101269095 - 100356671 = 912425 - 1$
1053619	1110114050781	$668690929 - 667759090 = 659905024 - 658973185$
1085363	1178013927133	$28212681427 - 28212634691 = 2672490749 - 2672444013$
1585651	2514290679453	$13288521241 - 13288488364 = 11908956544 - 11908923667$

Table 1: Squarefree orders with small multiplier groups

The calculations took roughly a week on DEC Alpha workstation. They could of course be taken further with more work. The number of orders passing each test seems to grow roughly linearly with the range being checked.

An alternative approach would be to search for a possible counterexample to the PPC. The most likely form for such an order would be of the form $n = pq$, where p and q have small order modulo v. This seems improbable, and a lower bound on the size of the multiplier group for non-prime power orders might be an approach towards proving the PPC.

n	$\exp(G)$	Nonexistence proof
2443	5970693	$p = 395173$ is an extraneous multiplier, $(n\|p) = -1$
2443	192603	$p = 41389$ is an extraneous multiplier, $(n\|p) = -1$
3233	804271	$65599 - 53 = 65547 - 1$
3233	61867	$61 - 9 = 53 - 1$
72011	740808019	$265903 - 673 = 265337 - 107$
72011	105829717	$504044 - 107 = 503938 - 1$
73481	5399530843	$906334 - 185809 = 720722 - 197$
73481	771361549	$612117 - 6876 = 605614 - 373$
96183	711635821	$202946 - 41174 = 161781 - 9$
128251	16448447253	$p = 758101$ is an extraneous multiplier, $(n\|p) = -1$
128251	2349778179	$p = 758101$ is an extraneous multiplier, $(n\|p) = -1$
135053	107925727	$613551 - 29 = 613523 - 1$
229952	4984273	$9 - 2 = 8 - 1$
318089	14454418573	$2094691 - 1306617 = 1036302 - 248228$
636479	9421073347	$166476 - 23 = 166454 - 1$
636479	1345867621	$71360 - 23 = 71338 - 1$
748421	685599439	$173657 - 26454 = 148416 - 1213$
769607	13774318699	$2350716 - 1337224 = 1660397 - 646905$
991937	20080408243	$529839 - 208385 = 410265 - 88811$
1615303	2609205397113	$816469390 - 816125185 = 773267854 - 772923649$
1615303	372743628159	$9618478 - 9164122 = 9164122 - 8709766$
1982923	3931985606853	$122491576 - 121569202 = 6485290 - 5562916$
1982923	49771969707	$122491576 - 121569202 = 6485290 - 5562916$

Table 2: Nonsquarefree orders with small multiplier groups

References

[1] K. T. Arasu. Recent results on difference sets. In Dijen Ray-Chaudhuri, editor, *Coding Theory and Design Theory, Part II*, pages 1–23. Springer–Verlag, 1990.

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

[3] C. Y. Ho. On bounds for groups of multipliers of planar difference sets. *J. Algebra*, 148:325–336, 1992.

[4] D. Jungnickel and K. Vedder. On the geometry of planar difference sets. *Europ. J. Combin.*, 5:143–148, 1984.

[5] Dieter Jungnickel. Difference sets. In Jeffrey H. Dinitz and Douglas R. Stinson, editors, *Contemporary Design Theory: A Collection of Surveys*, pages 241–324. Wiley, 1992.

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

[7] R. L. McFarland and B. F. Rice. Translates and multipliers of abelian difference sets. *Proc. Amer. Math. Soc.*, 68:375–379, 1978.

[8] H. A. Wilbrink. A note on planar difference sets. *J. Combin. Theory A*, 38:94–95, 1985.