Fields Institute Communications
Volume **00**, 0000

On the existence of cyclic difference sets with small parameters

Leonard D. Baumert
325 Acero Place
Arroyo Grande, CA 93420

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

This paper is dedicated to Hugh Williams on the occasion of his 60th birthday.

Abstract. Previous surveys by Baumert [3] and Lopez and Sanchez [12] have resolved the existence of cyclic (v, k, λ) difference sets with $k \leq 150$, except for six open cases. In this paper we show that four of those difference sets do not exist. We also look at the existence of difference sets with $k \leq 300$, and cyclic Hadamard difference sets with $v \leq 10{,}000$. Finally, we extend [6] to show that no cyclic projective planes exist with non-prime power orders $\leq 2 \cdot 10^9$.

1 Introduction

A (v, k, λ) difference set is a subset $D = \{d_1, d_2, \ldots, d_k\}$ of a group G such that each nonidentity element $g \in G$ can be represented as $g = d_i d_j^{-1}$ in exactly λ ways. In this paper we will be concerned with *cyclic* difference sets, where G will be taken to be the cyclic group $\mathbf{Z}/v\mathbf{Z}$. The *order* of a difference set is $n = k - \lambda$.

Baumert [3] gave a complete list of parameters for cyclic difference sets with $k \leq 100$. Lander gave a table of possible abelian difference set parameters with $k \leq 50$. Kopilovich [9] extended the search to $k < 100$, and Lopez and Sanchez [12] looked at all possible parameters for abelian difference sets with $k \leq 150$. Table 1 shows their open cases for cyclic difference sets, four of which we show do not exist.

In addition to settling some of these open cases, we have extended these calculations to larger values of k, using the same procedure of applying the numerous known necessary conditions. The open cases for $k \leq 300$ are given in Tables 2 and 3. The cases with $\gcd(v, n)$ greater than one are given separately, because of Ryser's conjecture that no cyclic difference sets exist with $\gcd(v, n) > 1$.

1991 *Mathematics Subject Classification.* Primary 05B10.

©0000 American Mathematical Society

v	k	λ	n	Status	Reference
429	108	27	81	No	Theorem 3.3
715	120	20	100	No	Theorem 4.20 of [10]
351	126	45	81	No	Schmidt Test [14]
837	133	21	112	No	Schmidt Test [14]
419	133	42	91	Open	
465	145	45	100	Open	

Table 1 Possible Cyclic Difference Sets with $k \leq 150$

v	k	λ	n	$\gcd(v,n)$
945	177	33	144	9
5859	203	7	196	7
1785	224	28	196	7
2574	249	24	225	9
2160	255	30	225	45
1925	260	35	225	25

Table 2 Possible CDS with $150 \leq k \leq 300$ and $\gcd(v,n) > 1$

v	k	λ	n
1123	154	21	133
645	161	40	121
1093	169	26	143
1111	186	31	155
469	208	92	116
1801	225	28	197
2291	230	23	207
639	232	84	148
2869	240	20	220
1381	276	55	221
817	289	102	187
781	300	115	185

Table 3 Possible CDS with $150 \leq k \leq 300$ and $\gcd(v,n) = 1$

We will give the details of computations that excluded possible difference sets in these tables. Most of the techniques are well known, and are described briefly in Section 2. A few parameters require more effort, such as the $(429, 108, 27)$ difference set which is shown not to exist in Section 3.3.

In Section 4 we look at cyclic Hadamard difference sets, with $v = 4n - 1$, $k = 2n - 1$, $\lambda = n - 1$. There are three known families, and it is conjectured that no others exist.

In Section 5 we look at the Prime Power Conjecture, which states that all abelian difference sets with $\lambda = 1$ have n a prime power. For the cyclic case we extend earlier computations by the second author [6] to $2 \cdot 10^9$, showing that no such difference sets exist when n is not a prime power.

Details of the computations, such as nonexistence proofs for the hard cases of cyclic projective planes mentioned in Section 5, are not included in the paper.

A web site `http://www.ccrwest.org/diffsets.html`, maintained by the second author, lists many known difference sets and gives nonexistence proofs.

2 Necessary Conditions

As in other searches ([2], [9], [10], [12]) we will go through values of (v, k, λ) up to a given k, applying known necessary conditions to eliminate most parameters, and dealing with survivors on a case-by-case basis. By a simple counting argument we must have $(v-1)\lambda = k(k-1)$. We may assume $k \le v/2$, since the complement of a (v, k, λ) difference set is a $(v, v-k, v-2k+\lambda)$ difference set. Some other conditions (see [7] for references) are:

Theorem 2.1 *(Schutzenberger) If v is even, n must be a square.*

Theorem 2.2 *(Bruck-Chowla-Ryser) If v is odd, the equation*

$$nX^2 + (-1)^{(v-1)/2}\lambda Y^2 = Z^2$$

must have a nontrivial integer solution.

Theorem 2.3 *(Mann) If $w > 1$ is a divisor of v, p is a prime divisor of n, p^2 does not divide n, and $p^j \equiv -1 \pmod{w}$, then no (v, k, λ) difference set exists.*

Theorem 2.4 *(Arasu [1]) If $w > 1$ is a divisor of v, p is a prime divisor of n, and*

- $\gcd(v, k) = 1$,
- *n is a nonsquare,*
- $\gcd(p, v) = 1$,
- *p is a multiplier,*

then

$$wv(-1)^{(v/w-1)/2}$$

is a square in the ring of p-adic integers.

Baumert gives four necessary tests used for his search in [2], which include Theorem 2.1 and three theorems of Yamamoto [15]. Lander gives a number of conditions in Chapter 4 of [10]. Ones that are used to exclude possible difference sets include Theorems 4.19, 4.20, 4.27, 4.30, 4.31, 4.32, 4.33, and 4.38.

3 Constructing the Tables

To extend previous tables of possible cyclic difference sets, we apply the theorems of the previous section to eliminate most possible parameters. Ones that survive these tests are dealt with on a case by case basis. In this section we give methods from [3] for dealing with certain difficult cases, and show an example of their application.

3.1 Polynomial Congruences. Let $\theta(x)$ be the difference set polynomial

$$\theta(x) = x^{d_1} + x^{d_2} + \ldots + x^{d_k},$$

and ζ_v be a primitive vth root of unity. Then D is a difference set if and only if

$$\theta(\zeta_v)\,\theta(\overline{\zeta_v}) = n.$$

In [2] and [3] a method is given for constructing or showing the nonexistence of difference sets. Define

$$\theta_w(x) \equiv \theta(x) \pmod{f_w(x)}$$

where $f_w(x)$ is the wth cyclotomic polynomial, and

$$\theta_{[w]}(x) \equiv \theta(x) \pmod{x^w - 1}.$$

The method is based on the congruences proved in [3]:

$$w\,\theta_{[w]} \equiv w\,\theta_w - \sum_{\substack{r|w \\ r \neq w}} \mu(w/r) r \left(\theta_{[r]} - \theta_w\right) \frac{x^w - 1}{x^r - 1} \pmod{x^w - 1}, \tag{1}$$

and

$$\theta_w \equiv \theta_{[w/p]} \pmod{p, f_{w_1}^{p^{a-1}}} \tag{2}$$

where $w = p^a w_1$, with $\gcd(p, w_1) = 1$.

Thus, given θ_w for a divisor of v and $\theta_{[r]}$ for all divisors r of w, one may compute $\theta_{[w]}$. To find θ_w, we may use the equation

$$\theta(\zeta_w)\,\theta(\overline{\zeta_w}) = n.$$

Furthermore, if $\mathfrak{a}$ is an ideal in $\mathbf{Q}(\zeta_w)$ for which $\mathfrak{a}\overline{\mathfrak{a}} = (n)$ with generator $\sum a_i \zeta_w^i$, then if $\theta_w(\zeta_w) \in \mathfrak{a}$ we have

$$\theta_w(x) = \pm x^j \sum a_i x^i \tag{3}$$

by a theorem of Kronecker that any algebraic integer, all of whose conjugates have absolute value 1, must be a root of unity.

So to determine the existence of a particular (v, k, λ) difference set, we may factor n in cyclotomic fields $\mathbf{Q}(\zeta_w)$ for $w|v$, and apply congruences (1) and (2) to construct $\theta_{[w]}$ or show that none exists. This approach was used by Howard Rumsey to prove the nonexistence of difference sets $(441, 56, 7)$ and $(891, 90, 9)$ [2].

3.2 Contracted Multipliers. The following two theorems, both proved in [3], are very useful:

Let

$$\theta_{[w]}(x) = b_0 + b_1 x + \ldots b_{w-1} x^{w-1}.$$

The following is Lemma 3.8 of [3]:

Theorem 3.1 *For every divisor w of v, there exists integers $b_i \in [0, v/w]$ such that*

$$\sum_{i=0}^{w-1} b_i = k, \tag{4}$$

$$\sum_{i=0}^{w-1} b_i^2 = n + \lambda v/w, \tag{5}$$

and

$$\sum_{i=0}^{w-1} b_i b_{i-j} = \lambda v/w \tag{6}$$

for $j = 1, \ldots, w-1$, where $i - j$ is taken modulo w.

The b_i's are the number of d_j's in D satisfying $d_j \equiv i \pmod{w}$. These equations often are sufficient to show nonexistence of a difference set. When they are not, we may sometimes use multipliers to get further conditions.

A w-multiplier of a difference set is an integer t prime to w for which there is an integer s such that

$$\theta(x^t) \equiv x^s \theta(x) \pmod{x^w - 1}.$$

The following is Theorem 3.2 in [3], and a generalization is given as Theorem 5.6 in [10].

Theorem 3.2 *Let D be a (v, k, λ) cyclic difference set with $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Let w be a divisor of v and t be an integer relatively prime to w. If for $i = 1, 2, \ldots, s$ there is an integer $j = j(i)$ such that*

$$p_i^j \equiv t \pmod{w},$$

then t is a w-multiplier of D.

If we have a w-multiplier for D, this gives us further restrictions on the b_i's, since if i and j are in the same orbit of t modulo w, then we must have $b_i = b_j$.

3.3 Using Contracted Multipliers. As an example of using these methods to eliminate a possible cyclic difference set, consider the first open case of Ryser's conjecture, $(429, 108, 27)$.

Theorem 3.3 *No $(429, 108, 27)$ difference set exists.*

Proof By Theorem 3.2, 3 is a 143-multiplier.
The orbits of the residues modulo 143 have sizes

$$1^1 3^4 5^2 15^8.$$

Let

$$\theta_{[143]}(x) = c_0 + c_1 x + \ldots c_{142} x^{142}.$$

From Theorem 3.1 we have $\sum c_i = k = 108$, and $\sum c_i^2 = n + \lambda v/w = 162$, so

$$162 = c_0^2 + 15(c_1^2 + \ldots + c_{29}^2) + 5(c_{13}^2 + c_{26}^2) + 3(c_{11}^2 + c_{22}^2 + c_{44}^2 + c_{77}^2)$$

and

$$\sum c_i c_{i+j} = 81, \quad \text{for } j = 1, \ldots, 142$$

There are $14,896$ solutions to the first equation, and a quick computer search shows that none of these satisfy the second.

□

This method still works when $w = v$. For example, consider a $(303, 151, 75)$ difference set. By Theorem 3.2, which for $w = v$ is known as the Second Multiplier Theorem, 16 is a multiplier, with three orbits of size 1 and 12 orbits of size 25. Therefore a difference set would have to be a union of one of the size-1 orbits and six of the size-25 ones. None of these 2772 possibilities form a difference set, and so no (303,151,75) difference set exists. Several other similar cases are given in Table 4.

v	k	λ	multiplier	w	solutions to (4) and (5)
429	108	27	3	143	14896
303	151	75	16	303	2772
2585	153	9	2	235	0
616	165	44	11	56	301485532
407	175	75	2	37	0
4401	176	7	13	489	504
544	181	60	3	68	96
3949	189	9	3	3949	2
1545	193	24	8	515	0
1380	197	28	2	115	0
1609	201	25	2	1609	8
6271	210	7	29	6271	30
1056	211	42	13	44	6240
2233	217	21	16	319	8512
6301	225	8	31	6301	0
601	225	84	3	601	56
595	243	99	2	119	216
611	245	98	2	47	0
2057	257	32	3	187	0
2591	260	26	3	2591	10
3181	265	22	3	3181	12
1061	265	66	199	1061	4
531	265	132	4	177	0
1615	270	45	4	323	17024
2691	270	27	3	299	114592
28325	292	3	2	103	0
591	295	147	16	591	2772
10990	297	8	9	157	0

Table 4 Cases eliminated by Theorem 3.1

3.4 Schmidt's Test. Schmidt ([13], [14]) has shown that, under certain conditions, a root of unity times $\theta(\zeta_v)$ must be in a subfield of $\mathbf{Q}(\zeta_v)$. For a prime q and integer m with prime factorization $\prod_{i=1}^{t} p_i^{c_i}$, let

$$m_q = \begin{cases} \prod_{p_i \neq q} p_i & \text{if } m \text{ is odd or } q = 2, \\ 4 \prod_{p_i \neq 2,q} p_i & \text{otherwise.} \end{cases}$$

Define $F(m,n) = \prod_{i=1}^{t} p_i^{b_i}$ to be the minimum multiple of $\prod_{i=1}^{t} p_i$ such that for every pair (i,q), $i \in \{1,\ldots,t\}$, q a prime divisor of n, at least one of the following conditions is satisfied:

1. $q = p_i$ and $(p_i, b_i) \neq (2,1)$,
2. $b_i = c_i$,
3. $q \neq p_i$ and $q^{\mathrm{ord}_{m_q}(q)} \not\equiv 1 \pmod{p_i^{b_i+1}}$.

Schmidt then shows

Theorem 3.4 *Assume $|X|^2 = n$ for $X \in \mathbf{Z}[\zeta_v]$. Then $X\zeta_v^j \in \mathbf{Z}[\zeta_{F(v,n)}]$ for some j.*

When $F(v,n)$ is significantly less than v, this theorem gives a powerful condition on the difference set. Schmidt uses it to show

Theorem 3.5 *For a (v,k,λ) cyclic difference set, we have*

$$n \leq \frac{F(v,n)^2}{4\varphi(F(v,n))},$$

where φ denote's Euler's totient function.

Theorem 3.5 eliminates 29 difference sets with $k \leq 300$.

Very recently, Leung, Ma and Schmidt [11] have shown that no cyclic difference set exists with order n a power of a prime > 3 and $(n,v) > 1$. This eliminates the difference set $(505, 225, 100)$. They also eliminate certain cases for powers of 3, such as $(2691, 270, 27)$.

4 Cyclic Hadamard Difference Sets

A cyclic Hadamard difference set is a difference set with parameters $v = 4n-1$, $k = 2n-1$, $\lambda = n-1$. All known cyclic Hadamard difference sets are of one of the following types:

1. v prime.
2. v a product of twin primes.
3. $v = 2^n - 1$.

It has been conjectured that no others exist. Song and Golomb [5] excluded all but 17 cases up to $v = 10,000$. Kim and Song [8] eliminated four of those. The remaining ones are listed in Table 5, along with their current status. Six can be shown not to exist by theorems in Lander's book [10].

v	k	λ	Status	Comment
3439	1719	859	Open	
4355	2177	1088	Open	
4623	2311	1155	No	Thm. 4.19 of [10]
5775	2887	1443	No	Thm. 4.19 of [10]
7395	3697	1848	No	Thm. 4.20 of [10]
7743	3871	1935	No	Thm. 4.19 of [10]
8227	4113	2056	No	Thm. 4.20 of [10]
8463	4231	2115	No	Thm. 4.19 of [10]
8591	4295	2147	Open	
8835	4417	2208	Open	
9135	4567	2283	Open	
9215	4607	2303	Open	
9423	4711	2355	Open	

Table 5 Open Cases for Cyclic Hadamard Difference Sets

5 Cyclic Projective Planes

A difference set with $\lambda = 1$ is called a planar difference set. The Prime Power Conjecture (PPC) states that all abelian planar difference sets have order n a prime power. In [6], it was shown that the PPC is true for $n <$ 2,000,000.

Since that paper, several developments have made it possible to extend those computations. Faster computers with more memory are part of it, but also 64-bit computing allow calcuations to be done in single-precision, which results in a large speedup. Using the methods of [6], we have shown that no cyclic planar difference sets of non-prime power order n exist with $n < 2 \cdot 10^9$.

Most orders can be eliminated by various quick tests given in [6]. There were 605 orders which survived these tests, and were dealt with using a theorem of Evans and Mann [4] (Lander [10] proved a generalization for abelian groups):

Theorem 5.1 *Let D be a $(v, k, 1)$ planar cyclic difference set of order $n = k-1$. If t_1, t_2, t_3, and t_4 are numerical multipliers such that*

$$t_1 - t_2 \equiv t_3 - t_4 \pmod{v},$$

then v divides the least common multiple of $(t_1 - t_2, t_1 - t_3)$.

In [6] this theorem was used to create a hash table for differences $t_i - t_j$ less than one million, to find a collision that could be used to eliminate an order. For orders up to $2 \cdot 10^9$, all but two could be eliminated with differences up to $4 \cdot 10^8$. The two most difficult were $n = 40027523$ and $n = 883007071$. These were finally eliminated with pairs with differences 420511455 and 164204313, respectively.

References

[1] K. T. Arasu. On abelian difference sets. *Arch. Math.*, 48:491–494, 1987.

[2] Leonard D. Baumert. Difference sets. *SIAM J. Appl. Math.*, 17:826–833, 1969.

[3] Leonard D. Baumert. *Cyclic Difference Sets*, volume 182 of *Lecture Notes in Mathematics*. Springer-Verlag, 1971.

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

[5] S. W. Golomb and H.-Y. Song. On the existence of cyclic Hadamard difference sets. *IEEE Trans. Info. Theory*, 40:1266–1268, 1994.

[6] Daniel M. Gordon. The prime power conjecture is true for $n <$ 2,000,000. *Electronic J. Combinatorics*, 1, 1994. R6.

[7] 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.

[8] Jeong-Heon Kim and Hon-Yeop Song. Existence of cyclic Hadamard difference sets and its relation to binary sequences with ideal autocorrelation. *J. Comm. and Networds*, 1, 1999.

[9] L. E. Kopilovich. Difference sets in noncyclic abelian groups. *Cybernetics*, 25(2):153–157, 1989.

[10] Eric S. Lander. *Symmetric Designs: An Algebraic Approach*, volume 74 of *LMS Lecture Note Series*. Cambridge, 1983.

[11] Ka Hin Leung, Siu Lun Ma, and Bernhard Schmidt. Nonexistence of abelian difference sets: Lander's conjecture for prime power orders. Trans. AMS, to appear.

[12] A. Vera Lopez and M. A. Garcia Sanchez. On the existence of abelian difference sets with $100 < k \leq 150$. *J. Comb. Math. Com. Comp.*, pages 97–112, 1997.

[13] Bernhard Schmidt. Cyclotomic integers and finite geometry. *J. Amer. Math. Soc.*, 12:929–952, 1999.

[14] Bernhard Schmidt. Towards Ryser's conjecture. In C. Casacuberta et. al., editor, *Proc. Third European Congress of Mathematics*, pages 533–541. Birkhäuser, 2000.

[15] K. Yamamoto. Decomposition fields of difference sets. *Pacific J. Math.*, 13:337–352, 1963.