The La Jolla Difference Set Repository

Daniel M. Gordon

IDA/CCR

August 3, 2019

Outline

Outline

1. Difference Sets
2. What We Know
3. What We Don't Know

Definition

A (v, k, λ) *difference set* in a group G of order v is a subset

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

of G such that every nonzero element of G has exactly λ representations as $d_i - d_j$.

The *order* of D is $n = k - \lambda$.

Difference Sets

Definition

A (v, k, λ) *difference set* in a group G of order v is a subset

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

of G such that every nonzero element of G has exactly λ representations as $d_i - d_j$.

The *order* of D is $n = k - \lambda$.

Example

$\{0, 1, 3\}$ is the $(7, 3, 1)$ difference set (also projective plane of order 2)

Outline

History

Cyclic Projective Planes: $G = \mathbb{Z}_v$, $\lambda = 1$

- Singer (1938) showed they exist when n is a prime power.
- Hall (1947) found necessary conditions, introduced multipliers.

General Difference Sets

- Work on $\lambda > 1$ and general G from 1950's on.
- A Google Scholar search for "difference sets" gets over 13000 results.
- A great source of open problems.

Some Necessary Conditions

Counting Condition

$$\lambda(v-1) = k(k-1)$$

Bruck-Ryser-Chowla

If a (v, k, λ)-difference set exists, then

- If v is even, then n is a square.
- If v is odd, then the equation

$$x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2$$

has a nontrivial integer solution.

Existence

Basic Question

For which (v, k, λ) and groups G do difference sets exist?

Existence

Basic Question

For which (v, k, λ) and groups G do difference sets exist?

Existence Surveys

Year	Authors	Groups	Bound
1971	Baumert	Cyclic	$k \leq 100$
1978	Kibler	Noncyclic	$k < 20$
1983	Lander	Abelian	$k \leq 50$
1987	Kopilovic	Abelian	$k \leq 100$
1997	López and Sánchez	Abelian	$100 \leq k \leq 150$
2003	Baumert and G.	Cyclic	$k \leq 300$

Existence, cont'd

Other results

- Surveys (1955, 1992,...,2007)
- *Many* papers on particular parameters
- A small number of infinite families known

Existence, cont'd

Other results

- Surveys (1955, 1992,...,2007)
- *Many* papers on particular parameters
- A small number of infinite families known

Subject of this talk

The La Jolla Difference Set Repository: an online database of known existence results for abelian difference sets with $v < 10^6$

Difference Sets

A *(v,k,λ)-difference set in a group* G is a subset D = {$d_1, d_2, \ldots, d_k$} of G such that each nonzero element of G can each be represented as a difference ($d_i - d_j$) in exactly λ different ways.

This page gives information about possible parameters for difference sets in abelian groups *G*. All parameters with *v<100000* passing basic tests (counting, Schutzenberger, BRC) are listed here, and an attempt has been made to include all known difference sets. Most known for large *v* are Paley, which are easily constructed, so those are omitted for *v>1000*.

Some constructions have not been included yet. If you have any difference sets or nonexistence results not in this database, or find any errors, please let me know. The Multiplier Conjecture link below has information about recent computations for $v<10^6$.

Search for Difference Sets

v range:		≤ v ≤	500
k range:		≤ k ≤	
λ range:		≤ λ ≤	
n range:		≤ n ≤	
Group:			
Comment:			
Status:	open		

Query Results

Search Display

v	k	λ	n	G	status	comment
243	121	60	61	[3,9,9]	Open	
343	171	85	86	[7,49]	Open	
400	190	90	100	[10,40]	Open	
400	190	90	100	[20,20]	Open	
400	190	90	100	[2,10,20]	Open	
416	166	66	100	[2,208]	Open	
416	166	66	100	[4,104]	Open	
416	166	66	100	[2,2,104]	Open	
425	160	60	100	[5,85]	Open	
448	150	50	100	[2,224]	Open	
448	150	50	100	[4,112]	Open	
448	150	50	100	[2,2,112]	Open	
448	150	50	100	[8,56]	Open	
448	150	50	100	[2,4,56]	Open	
465	145	45	100	[465]	Open	
469	208	92	116	[469]	Open	
477	204	87	117	[3,159]	Open	
495	247	123	124	[3,165]	Open	

Another query

Difference Sets

A *(v,k,λ)-difference set in a group* G is a subset D = {d_1, d_2, ..., d_k} of G such that each nonzero element of G can each be represented as a difference (d_i – d_j) in exactly λ different ways.

This page gives information about possible parameters for difference sets in abelian groups *G*. All parameters with *v<100000* passing basic tests (counting, Schutzenberger, BRC) are listed here, and an attempt has been made to include all known difference sets. Most known for large *v* are Paley, which are easily constructed, so those are omitted for *v>1000*.

Some constructions have not been included yet. If you have any difference sets or nonexistence results not in this database, or find any errors, please let me know. The Multiplier Conjecture link below has information about recent computations for $v<10^6$.

Search for Difference Sets

v range:	500	≤ v ≤	520
k range:		≤ k ≤	
λ range:		≤ λ ≤	
n range:		≤ n ≤	
Group:			
Comment:			
Status:			

Query Results

Search Display

v	k	λ	n	G	status	comment
503	251	125	126	[503]	All	Paley
505	64	8	56	[505]	No	Mann Test
505	217	93	124	[505]	No	Mann Test
505	225	100	125	[505]	No	Leung, Ma and Schmidt
506	101	20	81	[506]	No	Lopez and Sanchez
507	253	126	127	[507]	No	Mann Test
507	253	126	127	[13,39]	No	Mann Test
511	51	5	46	[511]	No	Mann Test
511	85	14	71	[511]	No	Mann Test
511	120	28	92	[511]	No	Mann Test
511	136	36	100	[511]	No	Lander, Theorem 4.19
511	255	127	128	[511]	All	(8,2) Singer
515	257	128	129	[515]	No	Mann Test
517	129	32	97	[517]	No	Lander, Theorem 4.38
519	112	24	88	[519]	No	Mann Test
519	148	42	106	[519]	No	Mann Test
519	259	129	130	[519]	No	Mann Test

Query Results, cont'd

Cyclic (511,255,127) difference sets

(8,2) Singer

There are exactly 5 such difference sets

PG(8,2)

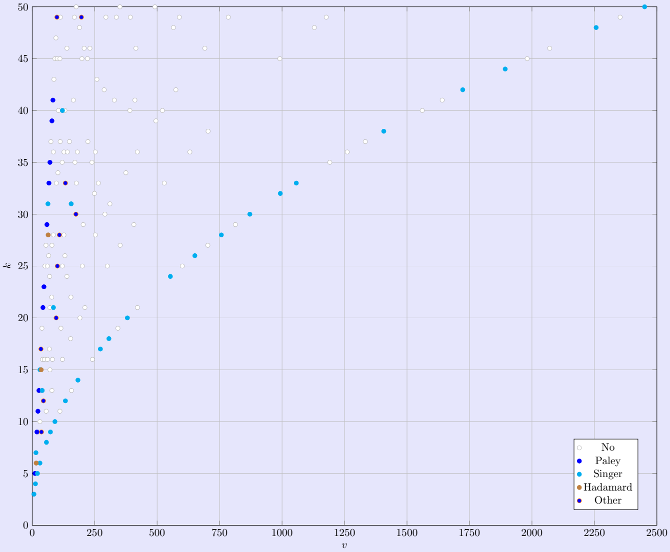
```
  1,  2,  3,  4,  6,  7,  8, 11, 12, 13,
 14, 16, 17, 21, 22, 24, 26, 28, 31, 32,
 33, 34, 37, 42, 44, 45, 48, 52, 53, 55,
 56, 57, 59, 61, 62, 63, 64, 66, 68, 71,
 73, 74, 81, 84, 85, 87, 88, 90, 91, 93,
 96,103,104,106,107,110,112,114,115,118,
119,122,123,124,125,126,127,128,131,132,
133,136,137,139,141,142,143,146,148,149,
151,159,161,162,163,165,168,169,170,174,
176,179,180,182,185,186,191,192,193,199,
203,205,206,207,208,209,212,214,217,220,
224,227,228,229,230,231,233,236,238,244,
246,248,250,252,253,254,255,256,257,259,
261,262,264,266,271,272,274,278,282,283,
284,285,286,287,291,292,296,298,299,301,
302,307,309,313,315,317,318,319,321,322,
324,325,326,327,330,331,335,336,337,338,
340,345,348,351,352,355,357,358,359,360,
364,369,370,371,372,382,383,384,385,386,
391,397,398,399,401,405,406,409,410,412,
413,414,415,416,418,419,421,423,424,428,
431,433,434,435,440,441,447,448,451,454,
455,456,458,460,462,463,465,466,467,471,
472,473,476,479,481,483,487,488,489,491,
492,495,496,497,499,500,501,503,504,505,
506,507,508,509,510
```

GMW

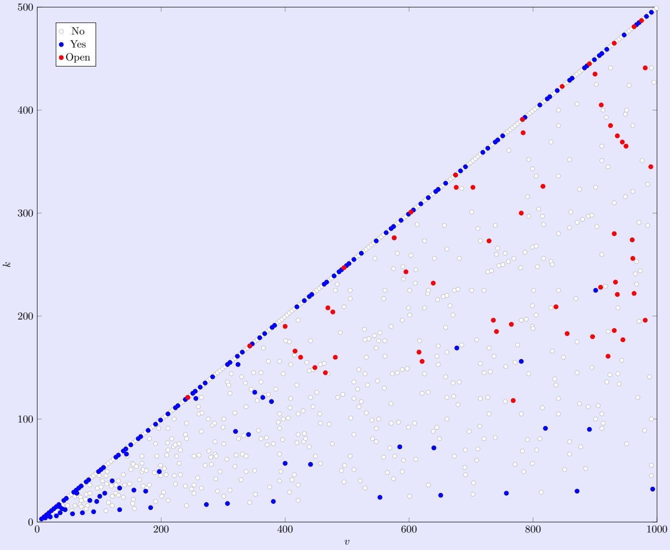
```
  5, 10, 13, 15, 19, 20, 23, 25, 26, 27,
 29, 30, 31, 37, 38, 40, 43, 46, 50, 51,
 52, 53, 54, 57, 58, 59, 60, 62, 67, 71,
 73, 74, 75, 76, 77, 80, 81, 83, 86, 87,
 89, 92, 95, 97, 99,100,101,102,103,104,
105,106,108,109,114,115,116,118,119,120,
123,124,125,129,131,134,135,137,141,142,
146,147,148,150,152,153,154,155,159,160,
162,163,166,172,174,175,177,178,184,185,
187,189,190,191,194,195,197,198,199,200,
201,202,204,206,207,208,210,211,212,215,
216,218,225,228,229,230,231,232,236,237,
238,240,245,246,248,249,250,253,258,262,
263,265,267,268,269,270,271,274,277,281,
282,284,285,289,291,292,293,294,296,297,
299,300,303,304,305,306,307,308,310,313,
315,317,318,320,321,323,324,326,329,332,
333,335,337,343,344,348,349,350,351,353,
354,355,356,359,361,363,368,370,371,374,
378,380,382,387,388,389,390,391,394,396,
398,400,401,402,404,405,407,408,409,412,
413,414,416,417,420,422,423,424,427,430,
431,432,433,435,436,437,441,449,450,451,
456,458,459,460,462,464,467,469,471,472,
473,474,476,480,481,485,489,490,491,492,
496,498,500,501,506
```

```
  5,  7,  9, 10, 14, 17, 18, 20, 28, 31,
 33, 34, 35, 36, 37, 39, 40, 49, 55, 56,
 57, 59, 62, 63, 65, 66, 68, 70, 71, 72,
 74, 75, 77, 78, 80, 81, 85, 89, 93, 95,
 98,103,105,107,110,111,112,113,114,115,
117,118,119,123,124,126,129,130,132,136,
137,140,142,144,147,148,149,150,151,154,
156,157,160,162,165,167,169,170,171,173,
178,179,181,183,186,187,190,191,196,199,
201,205,206,207,210,213,214,215,219,220,
```

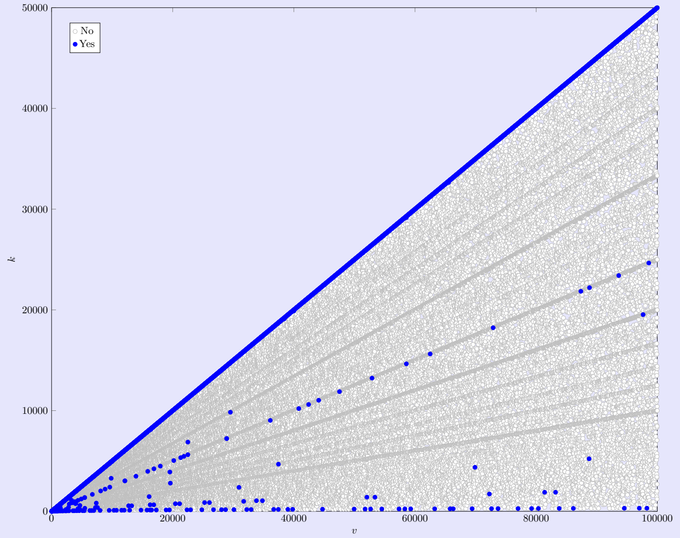
Lander's Tables



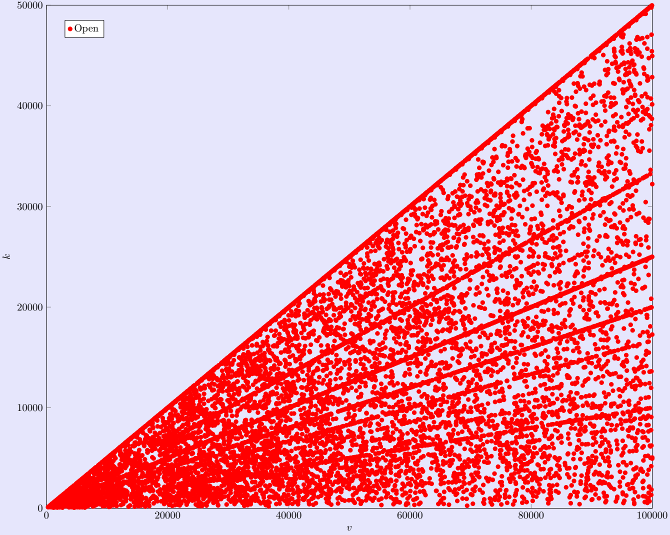
DS Params: $v \leq 1000$



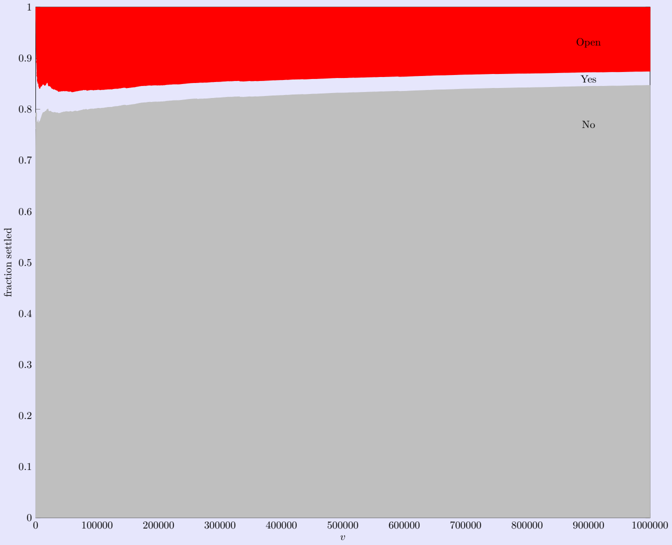
DS Params: $v \leq 100000$: what we know



DS Params: $v \leq 100000$: what we don't know



DS Params: $v \leq 1000000$: how we're doing



LJDSR Statistics

Parameters with $v \leq 10^6$

- 1442276 (v, k, λ) and G passing counting and BRC
- 40762 known to exist (39334 Paley)
- 7036 difference sets
- 180842 open

Nonexistence Reasons

- Mann's Theorem: 1029899
- Lander Theorems: 147740
- BJL Theorems: 14318
- Turyn: 13993
- Field Descent: 13254
- Computation: 1200

Difference sets with gcd$(v, n) = 1$

Paley

$(4n-1, 2n-1, n-1)$ in $\mathrm{GF}(q)$

Singer

$\left(\frac{q^m-1}{q-1}, \frac{q^{m-1}-1}{q-1}, \frac{q^{m-2}-1}{q-1}\right)$ in $\mathbb{Z}_v$

Twin Prime Power

$\left(q(q+2), \frac{q^2+2q-1}{2}, \frac{q^2+2q-3}{4}\right)$ in $\mathrm{GF}(q) \oplus \mathrm{GF}(q+2)$

Cyclotomic

mth power residues, with or without 0, in $\mathrm{GF}(q)$.

Difference sets with gcd$(v, n) > 1$

Hadamard ($n = u^2$)

$(4u^2, 2u^2 - u, u^2 - u)$ in $H \times M$

McFarland ($n = q^{2d}$)

$\left(q^{d+1}\left(1 + \frac{q^{d+1}-1}{q-1}\right), q^d\left(\frac{q^{d+1}-1}{q-1}\right), q^d\left(\frac{q^d-1}{q-1}\right)\right)$ in $K \times EA(q^{d+1})$

Chen ($n = q^{4d-2}$)

$\left(\frac{4q^{2d}(q^{2d}-1)}{q^2-1}, \frac{q^{2d-1}(2q^{2d}+q-1)}{q+1}, \frac{q^{2d-1}(q-1)(2q^{2d-1}+1)}{q+1}\right)$ in $K \times EA(q^{2d})$

IDA

Difference sets with gcd$(v, n) > 1$, cont'd

Davis-Jedwab ($n = 2^{4d+2}$)

$\left(\frac{2^{2d+4}(2^{2d+2}-1)}{3}, \frac{2^{2d+1}(2^{2d+3}+1)}{3}, \frac{2^{2d+1}(2^{2d+1}+1)}{3}\right)$ in $H \times M$

Spence ($n = 3^{2d}$)

$\left(\frac{3^{d+1}(3^{d+1}-1)}{2}, \frac{3^{d}(3^{d+1}+1)}{2}, \frac{3^{d}(3^{d}+1)}{2}\right)$ in $H \times M$

Outline

Conjectures

~~Conjectures~~ Open Problems

Difference set theory has a wealth of open problems

- Many have been open for decades
- Often the correct conjecture is not clear
- Maybe having a database of known difference sets could shed some light...

Multiplier Conjecture

Definition

For $t \in \mathbb{Z}$, if $x \mapsto tx$ takes D to $D + g$ for some $g \in G$, then t is called a (numerical) *multiplier*.

Multiplier Conjecture

Definition

For $t \in \mathbb{Z}$, if $x \mapsto tx$ takes D to $D + g$ for some $g \in G$, then t is called a (numerical) *multiplier*.

Example

For the $(7, 3, 1)$ DS $\{0, 1, 3\}$, $2D = D + 6$

Multiplier Conjecture

Definition

For $t \in \mathbb{Z}$, if $x \mapsto tx$ takes D to $D + g$ for some $g \in G$, then t is called a (numerical) *multiplier*.

Example

For the $(7, 3, 1)$ DS $\{0, 1, 3\}$, $2D = D + 6$

First Multiplier Theorem

If $p > \lambda$ is a prime dividing n, $p \not| v$, then p is a multiplier of D.

Multiplier Conjecture

Definition

For $t \in \mathbb{Z}$, if $x \mapsto tx$ takes D to $D + g$ for some $g \in G$, then t is called a (numerical) *multiplier*.

Example

For the $(7, 3, 1)$ DS $\{0, 1, 3\}$, $2D = D + 6$

First Multiplier Theorem

If $p > \lambda$ is a prime dividing n, $p \not| v$, then p is a multiplier of D.

Multiplier Conjecture

Still true for $p \leq \lambda$.

Why do we care?

Theorem

Some translate of D is fixed by all multipliers

Consequences

- A difference set is a union of orbits of G under the multiplier group
- This often makes searches and nonexistence proofs *much* easier

Multiplier Conjecture, cont'd

Many partial results

- True for all known difference sets
- Many strengthenings of FMT

MC in Familes

- Hadamard, McFarland, Spence, Davis-Jedwab, Chen: vacuously true
- Singer: True by Second Multiplier Theorem
- mth power residues: True (Lehmer)
- Paley, TPP: Open

Multiplier Conjecture, cont'd

Statistics

For possible difference sets with $v < 10^6$:

- For Paley parameters $(4n-1, 2n-1, n-1)$, there are 116386 primes, of which 99% are known to satisfy the MC
- For others there are 294797, of which 51% satisfy the MC

Multiplier Conjecture, cont'd

Statistics

For possible difference sets with $v < 10^6$:

- For Paley parameters $(4n-1, 2n-1, n-1)$, there are 116386 primes, of which 99% are known to satisfy the MC
- For others there are 294797, of which 51% satisfy the MC

Presumably most of the latter parameters don't have difference sets

Multiplier Conjecture, cont'd

Cases where difference sets exist

v	k	λ	G	n	MC primes	comment
343	171	85	[7, 7, 7]	$2 \cdot 43$	2 43	Paley
631	315	157	[631]	$2 \cdot 79$	2 79	Paley
783	391	195	[3, 3, 87]	$2^2 \cdot 7^2$	2 7	TPP(27)
911	455	227	[911]	$2^2 \cdot 3 \cdot 19$	2 3 19	Paley

Circled primes are not known to be multipliers for these parameters, but are for all known difference sets.

Multiplier Conjecture, cont'd

Cases where difference set existence is open

v	k	λ	G	n	MC primes
343	171	85	[7, 49]	$2 \cdot 43$	2 43
416	166	66	various	$2^2 \cdot 5^2$	5
425	160	60	[5, 85]	$2^2 \cdot 5^2$	2
448	150	50	various	$2^2 \cdot 5^2$	5
465	145	45	[465]	$2^2 \cdot 5^2$	2
469	208	92	[469]	$2^2 \cdot 29$	$\boxed{2}$ 29
781	300	115	[781]	$5 \cdot 37$	$\boxed{5 \quad 37}$

Squared primes cannot be multipliers.

Group Rings

Definition

For a group G, the *group ring* $\mathbb{Z}G$ is the free $\mathbb{Z}$-module of elements

$$\sum_{g \in G} a_g g.$$

Group Rings

Definition

For a group G, the *group ring* $\mathbb{Z}G$ is the free $\mathbb{Z}$-module of elements

$$\sum_{g \in G} a_g g.$$

Theorem

$D = \sum_i d_i$ is a difference set in G iff

$$D \cdot D^{-1} = n + \lambda G$$

Group Characters

Definition

A *character* of G is a homomorphism χ from G to $\mathbb{C}$
(in particular powers of ζ_v).

Group Characters

Definition

A *character* of G is a homomorphism χ from G to $\mathbb{C}$ (in particular powers of ζ_v).

Theorem

$D = \sum_i d_i$ is a difference set in G iff

$$\chi(D)\overline{\chi(D)} = \begin{cases} n & \text{for } \chi \neq \chi_0 \\ k^2 & \text{for } \chi = \chi_0 \end{cases}$$

for all characters χ of G.

Difference sets with gcd$(v, n) > 1$

Character Divisibility Property

For all such known difference sets D and nontrivial characters χ of G:

$$\chi(D) = \zeta_v^i \sqrt{n}$$

A Good Question (Jungnickel and Schmidt, 1997)

Are the counterexamples?

Difference sets with $\gcd(v, n) > 1$

Character Divisibility Property

For all such known difference sets D and nontrivial characters χ of G:

$$\chi(D) = \zeta_v^i \sqrt{n}$$

A Good Question (Jungnickel and Schmidt, 1997)

Are the counterexamples?

Conjecture

Lots!

Difference sets with gcd$(v, n) = 1$

Arasu, Chen, Dillon, Liu, Player (2007)

Most such difference sets have $n \equiv 1 \pmod{\lambda}$.

Only exceptions

Quartic or octic residues with 0 have $n \equiv 0 \pmod{\lambda}$.

Recall $\lambda(v - 1) = k(k - 1)$.

Difference sets with gcd$(v, n) = 1$

Arasu, Chen, Dillon, Liu, Player (2007)

Most such difference sets have $n \equiv 1 \pmod{\lambda}$.

Only exceptions

Quartic or octic residues with 0 have $n \equiv 0 \pmod{\lambda}$.

Recall $\lambda(v-1) = k(k-1)$.

Question

Any others? Can $n \bmod \lambda$ take on any other values?

Smallest open case

Cyclic $(469, 208, 92)$, $n \bmod \lambda = 24$

Cyclotomic Difference Sets

mth power difference sets

- Many for $m = 2$ (Paley)
- Rare for $m = 4, 8$ (Lehmer)
- None for odd m
- No others for $m \leq 22$ (Xia)

Question

Are there others?

Does existence in an Abelian group G only depend on $\exp(G)$?

No! (in these two cases)

v	k	λ	G	status
324	153	72	[9,36]	Yes (Davis and Jedwab)
324	153	72	[3,3,36]	No (Jedwab)
324	153	72	[18,18]	Yes (Davis and Jedwab)
324	153	72	[3,6,18]	No (Jedwab)

Smallest Open Case

v	k	λ	G	status
243	121	60	[3,3,3,9]	No (López and Sánchez)
243	121	60	[3,9,9]	Open

Ryser's Conjecture

Conjecture

If G is cyclic, $\gcd(v, n) = 1$.

Small Open Cases

v	k	λ	n
465	145	45	100
616	165	44	121
910	405	180	225
936	375	150	225
963	222	51	171
990	345	120	225

Lander's Conjecture

Conjecture

If $p|\gcd(v, n)$, then the Sylow p-subgroup of G cannot be cyclic.

Theorem (Leung, Ma, Schmidt, 2003)

Lander's Conjecture is true for n a power of a prime > 3.

Small Open Cases

v	k	λ	n	G	p
465	145	45	100	[3,5,31]	5
910	405	180	225	[2,5,7,13]	5
936	375	150	225	[8,9,13]	3
936	375	150	225	[2,4,9,13]	3
963	222	51	171	[9,107]	3
990	345	120	225	[2,G_9,5,11]	3,5
1008	266	70	196	[G_{16}, G_9,7]	7

Conjecture

All cyclic difference sets with parameters $(4n-1, 2n-1, n-1)$ have v either

- prime,
- a product of twin primes,
- $2^m - 1$.

Confirmed for all but seven cases with $v \leq 10000$.

Cyclic Hadamard Difference Sets, cont'd

Small Open Cases

v	k	λ	n
3439	1719	859	$2^2 \cdot 5 \cdot 43$
4355	2177	1088	$3^2 \cdot 11^2$
8591	4295	2147	$2^2 \cdot 3 \cdot 179$
8835	4417	2208	47^2
9135	4567	2283	$2^2 \cdot 571$
9215	4607	2303	$2^8 \cdot 3^2$
9423	4711	2355	$2^2 \cdot 19 \cdot 31$

Prime Power Conjecture

PPC

if D is a $(v, k, 1)$-difference set, then $n = k - 1$ is a prime power.

True up to $2 \cdot 10^6$ for abelian groups, $2 \cdot 10^9$ for cyclic.

Prime Power Conjecture

PPC

if D is a $(v, k, 1)$-difference set, then $n = k - 1$ is a prime power.

True up to $2 \cdot 10^6$ for abelian groups, $2 \cdot 10^9$ for cyclic.

Possible results coming

Jonathan Webster and Ankur Gupta are working on extending these computations.

Uniqueness of Projective Planes

Conjecture

Every finite cyclic projective plane is desarguesian

Uniqueness of Projective Planes

Conjecture

Every finite cyclic projective plane is desarguesian

Some (not much) evidence

- PPC calculations
- Hall, Bruck, Huang and Schmidt showed true for $n < 41$ and $n \in \{121, 125, 128, 169, 256, 1024\}$.

Circulant Hadamard Matrices

Definition

A circulant Hadamard matrix is an $n \times n$ matrix H of ± 1's with cyclic symmetry for which $HH^T = nI$.

Such a matrix is equivalent to a difference set with parameters $(4u^2, 2u^2 \pm u, u^2 \pm u)$.

Conjecture

They exist only for $n = 1, 4$.

Leung and Schmidt showed it's true for $n < 4 \cdot 11715^2$.
Logan and Mossinghoff showed only 4489 possible examples less than $4 \cdot 10^{30}$.

Barker Sequences

Definition

A Barker sequence is a finite sequence $a_1, \ldots, a_n$ of ± 1's such that

$$c_k = \sum_{i=1}^{n-k} a_i a_{i+k}$$

for which $|c_k| \leq 1$ for all $k \geq 1$

Examples

$[+ \ + \ -]$, $[+ \ + \ + \ - +]$
They exist for $n = 3, 5, 7, 11, 13.$
Any larger Barker sequence would give a circulant Hadamard matrix

Barker Sequences

Definition

A Barker sequence is a finite sequence $a_1, \ldots, a_n$ of ± 1's such that

$$c_k = \sum_{i=1}^{n-k} a_i a_{i+k}$$

for which $|c_k| \leq 1$ for all $k \geq 1$

Examples

$[+ \ + \ -]$, $[+ \ + \ + \ - +]$
They exist for $n = 3, 5, 7, 11, 13$.
Any larger Barker sequence would give a circulant Hadamard matrix

Conjecture

No others exist. (one open case $< 4 \cdot 10^{33}$ (Borwein and Mossinghoff))

Difference Sets in Elementary Abelian Groups

Question

Are all difference sets in non-cyclic elementary abelian groups either Hadamard or Paley?

Small Open Cases

v	k	λ	G
729	273	102	[3,3,3,3,3,3]
961	256	68	[31,31]
1849	561	170	[43,43]
3125	1420	645	[5,5,5,5,5]
3721	1240	413	[61,61]
4489	561	70	[67,67]
5041	225	10	[71,71]

Conclusion

La Jolla Difference Set Repository

- Located at `https://dmgordon.org/diffset`
- Useful tool for investigating difference sets
- Please let me know about errors, omissions,...

Questions?