Cyclic Relative Difference Sets

Daniel M. Gordon

IDA/CCR-La Jolla

May 26, 2025

Outline

1. Difference Sets, Relative Difference Sets and Related Objects
2. Difference sets $\longrightarrow$ Relative Difference Sets
3. Relative Difference sets $\longrightarrow$ Circulant Weighing Matrices
4. Aside: Online Combinatorial Databases

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 $d_i - d_j$.

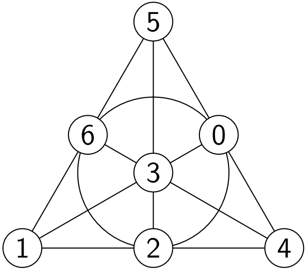
The complement of a (v, k, λ)-DS is a $(v, v-k, v-2k+\lambda)$-DS.

IDA

Example: $(7, 3, 1)$-DS = Projective plane of order 2

$\{1, 2, 4\} \subset \mathbb{Z}_7$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$



Singer Difference Sets

More Examples

A *Singer difference set* has parameters

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

for $d > 1$ and q a prime power. Singer constructed them in 1938 using $PG(d, q)$, the projective geometry of dimension d over $GF(q)$.

Foreshadowing

The complement of a Singer difference set has parameters

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

The La Jolla Difference Set Repository

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:		≤ v ≤	
k range:	50	≤ k ≤	100
λ range:		≤ λ ≤	
n range:		≤ n ≤	
Group:	cyclic		
Comment:			
Status:	exists		

SEARCH RESET

LJDSR Query Results

Search Display

v	k	λ	n	G	status	comment
103	51	25	26	[103]	Yes	Paley
107	53	26	27	[107]	All	Paley
127	63	31	32	[127]	All	(6,2) Singer
131	65	32	33	[131]	Yes	Paley
139	69	34	35	[139]	Yes	Paley
143	71	35	36	[143]	All	TPP(11)
151	75	37	38	[151]	Yes	Paley
163	81	40	41	[163]	All	Paley
167	83	41	42	[167]	Yes	Paley
179	89	44	45	[179]	Yes	Paley
191	95	47	48	[191]	Yes	Paley
199	99	49	50	[199]	Yes	Paley
341	85	21	64	[341]	All	(4,4) Singer
400	57	8	49	[400]	All	(3,7) Singer
585	73	9	64	[585]	All	(3,8) Singer
820	91	10	81	[820]	Yes	(3,9) Singer
2451	50	1	49	[2451]	Yes	(2,49) Singer
2863	54	1	53	[2863]	Yes	(2,53) Singer
3541	60	1	59	[3541]	Yes	(2,59) Singer
3783	62	1	61	[3783]	Yes	(2,61) Singer
4161	65	1	64	[4161]	Yes	(2,64) Singer
4557	68	1	67	[4557]	Yes	(2,67) Singer
5113	72	1	71	[5113]	Yes	(2,71) Singer
5403	74	1	73	[5403]	Yes	(2,73) Singer
6321	80	1	79	[6321]	Yes	(2,79) Singer
6643	82	1	81	[6643]	Yes	(2,81) Singer
6973	84	1	83	[6973]	Yes	(2,83) Singer
8011	90	1	89	[8011]	Yes	(2,89) Singer
9507	98	1	97	[9507]	Yes	(2,97) Singer

LJDSR Query Results, cont'd

Cyclic (127,63,31) difference sets

(6,2) Singer

There are exactly 6 such difference sets

PG(6,2)

```
  1,  2,  3,  4,  5,  6,  8,  9, 10, 11,
 12, 15, 16, 17, 18, 20, 22, 23, 24, 29,
 30, 32, 33, 34, 36, 39, 40, 44, 46, 48,
 49, 55, 57, 58, 59, 60, 64, 65, 66, 68,
 69, 71, 72, 75, 78, 80, 83, 88, 91, 92,
 93, 96, 98, 99,101,105,109,110,113,114,
116,118,120
```

Legendre Sequence

```
  3,  5,  6,  7, 10, 12, 14, 20, 23, 24,
 27, 28, 29, 33, 39, 40, 43, 45, 46, 48,
 51, 53, 54, 55, 56, 57, 58, 59, 63, 65,
 66, 67, 75, 77, 78, 80, 83, 85, 86, 89,
 90, 91, 92, 93, 95, 96, 97,101,102,105,
106,108,109,110,111,112,114,116,118,119,
123,125,126
```

Hall Sextic Residue Sequence

```
  1,  2,  4,  5,  8, 10, 13, 15, 16, 19,
 20, 25, 26, 27, 30, 31, 32, 33, 35, 38,
 40, 47, 50, 51, 52, 54, 60, 61, 62, 63,
```

IDA

Group Rings

For a group G, the group ring $\mathbb{Z}[G]$ is the free $\mathbb{Z}$-module with basis G:

$$\mathbb{Z}[G] = \left\{ \sum_{g \in G} a_g g \mid a_g \in \mathbb{Z} \right\}.$$

Group Ring Operations

$$A + B = \left(\sum_{g \in G} a_g g \right) + \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} (a_g + b_g) g$$

$$AB = \left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h h \right) = \sum_{g,h \in G} a_g b_h (gh)$$

$$A^{-1} = \sum_{g \in G} a_g g^{-1}$$

Difference Sets: group ring version

Definition II

Let $D = \sum_{d_i \in D} d_i$. D is a difference set if:

$$DD^{-1} = k + \lambda(G - 1_G),$$

Example

$G = \mathbb{Z}_7$, $D = g^1 + g^2 + g^4$

$$\begin{aligned} DD^{-1} &= (g^1 + g^2 + g^4)(g^6 + g^5 + g^3) \\ &= 3g^0 + g^1 + g^2 + g^3 + g^4 + g^5 + g^6 \end{aligned}$$

Related object: Circulant Weighing Matrices

Definition

A *circulant weighing matrix* $CW(n,k)$ is an $n \times n$ cyclically symmetric $(0, \pm 1)$-matrix M such that

$$MM^T = kI_n.$$

Example: $CW(7,4)$

$$\begin{bmatrix} - & + & + & 0 & + & 0 & 0 \\ 0 & - & + & + & 0 & + & 0 \\ 0 & 0 & - & + & + & 0 & + \\ + & 0 & 0 & - & + & + & 0 \\ 0 & + & 0 & 0 & - & + & + \\ + & 0 & + & 0 & 0 & - & + \\ + & + & 0 & + & 0 & 0 & - \end{bmatrix}$$

Circulant Weighing Matrices, cont'd

CWM Group Ring Equation

$C = \sum c_g g$ with $c_g \in \{0, \pm 1\}$, and

$$CC^{-1} = k.$$

Facts about CWM's

- $k = s^2$ for some positive integer s,
- Let P be the set of $+1$'s, and N the -1's.
  WLOG $|P| = (s^2 + s)/2$, and $|N| = (s^2 - s)/2$
- A $CW(n,k)$ is called *proper* if no translate has all of P and N in a subgroup of $\mathbb{Z}_n$.

IDA

Related object: Signed Difference set

Signed Difference Set Equation

$D = \sum a_g g$ with $a_g \in \{0, \pm 1\}$, and

$$DD^{-1} = k + \lambda(G - 1_G),$$

Example: $(7, 6, -1)$-SDS in $\mathbb{Z}_7$

$$\begin{bmatrix} 0 & + & + & - & + & - & - \\ - & 0 & + & + & - & + & - \\ - & - & 0 & + & + & - & + \\ + & - & - & 0 & + & + & - \\ - & + & - & - & 0 & + & + \\ + & - & + & - & - & 0 & + \\ + & + & - & + & - & - & 0 \end{bmatrix}$$

Relative Difference Set

Definition

Let $|G| = mn$, N a normal subgroup of order n. A (m, n, k, λ)-*relative difference set* R of G relative to N is a k-element subset such that the differences of distinct elements of R contain every element of $G \backslash N$ exactly λ times, and none of N.

Group Ring Equation

$$RR^{-1} = k + \lambda(G - N),$$

Example

$\{0, 3, 5, 13\}$ is a $(7, 2, 4, 1)$-RDS in $\mathbb{Z}_{14}$ relative to $N = \{0, 7\}$.

Relative Difference Sets $\longrightarrow$ Difference Sets

Lifting Difference sets

If R is an (m, n, k, λ)-RDS in G relative to N, then G/N contains an $(m, k, \lambda n)$-difference set.

Example

The $(7, 2, 4, 1)$-RDS $\{0, 3, 5, 13\}$ is a lift of the $(7, 4, 2)$-DS $\{0, 3, 5, 6\}$ in $\mathbb{Z}_7$.

Main Question

When does a difference set have a lifting?

IDA

Lifts of Trivial Difference Sets

Lifts of (m, m, m)-DS

- These are called *semiregular*
- For p prime, a (p^a, p^b, p^a, p^{a-b})-RDS exists.
- Semiregular RDS are related to Hadamard matrices.

Lifts of $(m, m-1, m-2)$-DS

- For q a prime power, and any divisor d of $q-1$, a $(q+1, (q-1)/d, q, d)$-RDS exists.
- Are there lifts for $m-1$ not a prime power?

Multipliers

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 $\{1, 2, 4\}$, $2D = \{2, 4, 1\} = D$.

Multipliers

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 $\{1, 2, 4\}$, $2D = \{2, 4, 1\} = D$.

Theorem

If G is abelian, some translate of D is fixed by *all* its multipliers.

First Multiplier Theorem

If D is a difference set, $p > \lambda$ is a prime dividing $k - \lambda$, $p \not| v$, then p is a multiplier of D.

Multipliers

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 $\{1, 2, 4\}$, $2D = \{2, 4, 1\} = D$.

Theorem

If G is abelian, some translate of D is fixed by *all* its multipliers.

First Multiplier Theorem

If D is a difference set, $p > \lambda$ is a prime dividing $k - \lambda$, $p \nmid v$, then p is a multiplier of D.

Applications of Multipliers

Theorem (G., 2020)

Let $G = \mathbb{Z}_p \times H$, where $\gcd(p, |H|) = 1$.
If a (v, k, λ)-DS exists in G with multiplier m, $s = \mathrm{ord}_H(m)$, then orbits of $\langle m^s \rangle$ are $(0, h)$ and $(\langle i \rangle_o, h)$, for $o = \mathrm{ord}_p\, m^s$.

If D has a o-orbits and b 1-orbits,

$$\begin{aligned} k &= ao + b, \\ b(b-1) &\leq \lambda(|H| - 1), \\ a \cdot o(o-1) &\leq \lambda(p - 1). \end{aligned}$$

Difference sets with small λ

Planar Abelian Difference Sets

All $(v, k, 1)$ difference sets with $k \leq 2 \cdot 10^{10}$ have $k - 1$ a prime power.
Peluse showed $\#$ non-prime-powers $\leq x$ is $o(x/\log x)$.

Biplanes

The only $(v, k, 2)$ difference sets with $k \leq 10^{10}$ have $k = 3, 4, 5, 6$, or 9, with at most six exceptions.

Triplanes

The only $(v, k, 3)$ difference sets with $k \leq 10^{10}$ have $k = 6$ or 7, with at most six exceptions.

IDA

Multipliers for other objects

Recall:

Some translate of a DS is fixed by *all* its numerical multipliers.

For SDS, CWM and RDS, this isn't always true:

Theorem

Some translate of a (v, k, λ)-SDS, $CW(v, k)$ or (m, n, k, λ)-RDS is fixed by any one of its multipliers.
If $\gcd(v, k) = 1$, then some translate is fixed by *all* its multipliers.

Multipliers

Multiplier Facts

- All of the objects in this talk have some kind of multiplier theorem.
- Weaker than difference set theorems.

Multipliers

Multiplier Facts

- All of the objects in this talk have some kind of multiplier theorem.
- Weaker than difference set theorems.

RDS Multiplier Theorem

Let $\exp(G) = v^*$, and R be an (m, n, k, λ)-RDS. Let t be a multiplier of the $(m, k, n\lambda)$-DS rel prime to $v = mn$. Let $k_1 | k$, $k_1 = p_1^{e_1} \cdots p_r^{e_r}$, and $k_2 = k_1/\gcd(v, k_1)$. For each p_i, define

$$q_i = \begin{cases} p_i & \text{if } p_i \text{ does not divide } v \\ l_i & \text{if } v^* = p_i^r u_i,\ \gcd(p_i, u_i) = 1,\ \text{where } l_i \text{ is an integer such that} \\ & \gcd(l_i, p_i) = 1 \text{ and } \ l_i \equiv p_i^f \pmod{u}_i. \end{cases}$$

If for each i there exists an integer f_i such that $q_i^{f_i} \equiv t \pmod{v^*}$, then t is a multiplier of R.

Cyclic lifts of nontrivial difference sets

Lam, 1977

- Gave conditions for a multiplier of D to be a multiplier of R,
- Many nonexistence results,
- Found all cyclic RDS with $k \leq 50$,
- All are lifts of complements of Singer $PG(d, q)$ difference sets.

d	q	m	n	k	λ	# inequivalent
2	2	7	2	4	1	1
2	3	13	2	9	3	2
2	4	21	6	16	2	1
4	2	31	2	16	4	2
2	5	31	4	25	5	2
3	3	40	2	27	9	3
2	7	57	6	49	7	2

Lifts of nontrivial DS, cont'd

Arasu, Jungnickel, Ma and Pott, 1995

- Looked at $(m, 2, k, \lambda)$-RDS
- No such liftings of Singer, Paley, Twin Prime Power and their complements,...

Conjecture

Only complements of Singer DS have lifts with $n = 2$

Lifts of nontrivial DS, cont'd

Arasu, Dillon, Leung and Ma, 2001

Theorem: A cyclic

$$\left(\frac{q^{d+1}-1}{q-1}, n, q^d, \frac{q^{d-1}(q-1)}{n}\right) - RDS$$

exists iff

$$\begin{array}{ll} n \mid (q-1) & q \text{ odd or } d \text{ odd} \\ n \mid 2(q-1) & q \text{ and } d \text{ even} \end{array}$$

This settles the case of lifts of complements of Singer DS.

Lifts of nontrivial DS, cont'd

Pott, 1995

- Extended Lam's table to extensions of Singer DS, $k \leq 64$ for n odd.
- Asked whether any other difference sets have liftings for *any* n.

30 years later, can we extend the computations?

Given a $(m, k, \lambda n)$-DS:

1. Check nonexistence theorems.
2. Find its set of multipliers M_1.
3. Find multipliers $M_2 = \{t_1, t_2, \ldots, t_s\} \subset M$ of R.
4. $M = \begin{cases} \langle M_2 \rangle, & \gcd(mn, k) = 1, \\ \langle t \rangle, & \text{else} \end{cases}$
5. Search for a collection of orbits of M which form an RDS.

Intersection Numbers

Definition

Let b_i be the number of elements of an RDS equal to i mod n.

Lemma

For a (m, n, k, λ)-RDS with $d = \gcd(n, m)$:

$$\sum_{i=0}^{n-1} b_i = k,$$

$$\sum_{i=0}^{n-1} b_i^2 = k + \lambda \cdot (m - d),$$

where $|b_i| \leq m$.

Example: Complement of the $(73, 9, 1)$-Singer difference set D

Does the $(73, 64, 56)$-DS lift to a $(73, 7, 64, 8)$-RDS?

- 2 is a multiplier of D, so $M_1 = \langle 2 \rangle_9$
- $M = \langle 2 \rangle_9$ in $\mathbb{Z}_{511}$
- $\gcd(73, 7) = 1$, so $\mathbb{Z}_{511} = \mathbb{Z}_{73} \times \mathbb{Z}_7$.
- Orbits of M are $\langle 0 \rangle_1$ and $\langle o_1 \rangle_9, \ldots \langle o_8 \rangle_9$.
- $D = \langle 1 \rangle_9$ (or any of the 9-orbits)

IDA

Orbits in the $(73, 7, 64, 8)$-RDS

	[7]			
[73]	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 3\rangle_3$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$	$\langle 219\rangle_3$	$\langle 73\rangle_3$	1
$\langle 1\rangle_9$	$\langle 77\rangle_9$	$\langle 1\rangle_9$ $\langle 37\rangle_9$ $\langle 183\rangle_9$	$\langle 55\rangle_9$ $\langle 75\rangle_9$ $\langle 223\rangle_9$	0
$\langle 3\rangle_9$	$\langle 119\rangle_9$	$\langle 23\rangle_9$ $\langle 79\rangle_9$ $\langle 85\rangle_9$	$\langle 3\rangle_9$ $\langle 19\rangle_9$ $\langle 111\rangle_9$	9
$\langle 5\rangle_9$	$\langle 7\rangle_9$	$\langle 39\rangle_9$ $\langle 93\rangle_9$ $\langle 239\rangle_9$	$\langle 5\rangle_9$ $\langle 83\rangle_9$ $\langle 87\rangle_9$	9
$\langle 9\rangle_9$	$\langle 91\rangle_9$	$\langle 9\rangle_9$ $\langle 57\rangle_9$ $\langle 109\rangle_9$	$\langle 41\rangle_9$ $\langle 187\rangle_9$ $\langle 255\rangle_9$	9
$\langle 11\rangle_9$	$\langle 21\rangle_9$	$\langle 11\rangle_9$ $\langle 15\rangle_9$ $\langle 95\rangle_9$	$\langle 47\rangle_9$ $\langle 103\rangle_9$ $\langle 117\rangle_9$	9
$\langle 13\rangle_9$	$\langle 175\rangle_9$	$\langle 43\rangle_9$ $\langle 29\rangle_9$ $\langle 51\rangle_9$	$\langle 13\rangle_9$ $\langle 31\rangle_9$ $\langle 125\rangle_9$	9
$\langle 17\rangle_9$	$\langle 63\rangle_9$	$\langle 53\rangle_9$ $\langle 191\rangle_9$ $\langle 107\rangle_9$	$\langle 17\rangle_9$ $\langle 45\rangle_9$ $\langle 59\rangle_9$	9
$\langle 25\rangle_9$	$\langle 35\rangle_9$	$\langle 25\rangle_9$ $\langle 123\rangle_9$ $\langle 127\rangle_9$	$\langle 27\rangle_9$ $\langle 61\rangle_9$ $\langle 171\rangle_9$	9
	10	18	36	

Orbits in the $(73, 7, 64, 8)$-RDS

	$[7]$			
$[73]$	$\langle 0\rangle_1$	$\langle 1\rangle_3$	$\langle 3\rangle_3$	
$\langle 0\rangle_1$	$\langle 0\rangle_1$			1
$\langle 1\rangle_9$				0
$\langle 3\rangle_9$	$\langle 119\rangle_9$			9
$\langle 5\rangle_9$			$\langle 83\rangle_9$	9
$\langle 9\rangle_9$			$\langle 187\rangle_9$	9
$\langle 11\rangle_9$			$\langle 103\rangle_9$	9
$\langle 13\rangle_9$		$\langle 29\rangle_9$		9
$\langle 17\rangle_9$		$\langle 191\rangle_9$		9
$\langle 25\rangle_9$			$\langle 61\rangle_9$	9
	10	18	36	

Results

Known difference sets with $50 < k \leq 256$

- 93 non-Singer-DS-complements, all eliminated except:
  - $PG(5,3)$: $(364, 121, 40)$, $n = 5$
  - $PG(7,2)$: $(255, 127, 63)$, $n = 3, 7$
- 8 Singer complements, found all lifts except
  - $PG(2,11)$: $(133, 121, 110)$, $n = 5, 10$
  - $PG(2,13)$: $(183, 169, 156)$, $n = 2, 3, 4, 6, 12$
- Some DS parameters are open ($(2185, 105, 5)$, $(1561, 105, 7)$, $(1111, 111, 11)$, $\ldots$)
- Some parameters may have other difference sets

Conjecture

The only nontrivial difference sets with lifts are Singer complements.

$RDS \longrightarrow CW$

Recall

A $CW(n,k)$ is an $n \times n$ $(0,\pm 1)$-matrix M such that $MM^T = kI_n$.

Theorem (Ang, 2003)

If a cyclic (m,n,k,λ)-RDS exists with m odd and $n \equiv 2 \pmod 4$, then there is a proper $CW(mn/2,k)$.

Product construction (Arasu and Seberry, 1998)

If proper $CW(n_1,k_1)$ and $CW(n_2,k_2)$ exist with $\gcd(n_1,n_2)=1$, then there is a proper $CW(n_1 n_2, k_1 k_2)$.

Other CW Facts

Theorem (Leung and Schmidt, 2011)

For k an odd prime power, there are a finite number of proper $CW(n, k)$.

Settled Cases

All proper $CW(n, k)$ are known for $k = 2$, 3, 4 (and maybe 5).

k	Known Proper $CW(n,k)$
2^2	$2m$, 7
3^2	13, 24, 26
4^2	$14m$, 21, 31, 62, 63
5^2	31, 33, 62, 71, 124, 142
6^2	$26m$, $48m$, 91, 168, 182
7^2	57, 87, 114, 171
8^2	$42m$, $62m$, 73, 127, 217, 254, 511
9^2	91, 121, 182, 312, 364
10^2	$62m$, $66m$, $142m$, 217, 231, 434, 497, 868, 994
11^2	133, 665
12^2	$182m$, $336m$, 273, 403, 744, 806, 819
13^2	183, 549
14^2	$114m$, $174m$, $342m$, 399, 609, 798
15^2	403, 429, 744, 806, 858, 923
16^2	$146m$, $254m$, 273, 341, $434m$, 511, 651, 682, 819, 889
17^2	307
18^2	$182m$, $242m$, $624m$, 847
19^2	381

Types

- RDS
- product construction
- other constructions
- computer search
- RDS & product

Aside: Online Combinatorial Databases

October 2021 email from Robert Craigen

- Arranged a Zoom meeting to discuss archiving "Hadamardish" material,
- Ideally comprehensive, permanent, up-to-date,...
- Email followups, but no consensus about the "right" way.

The discussion had a big impact on my thinking

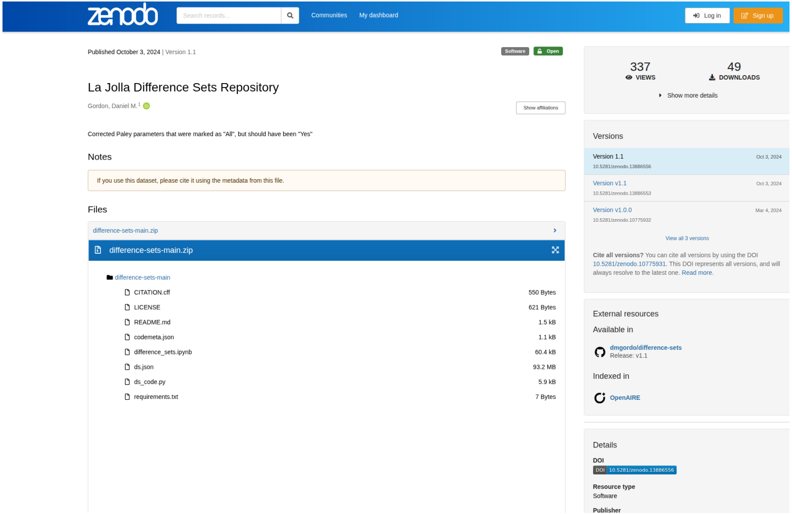
- I worry about my site's permanence,
- Went down many rabbit holes about FAIR data,...
- Mathematics is *way* behind other disciplines
- Progress is happening, slowly.

One Solution

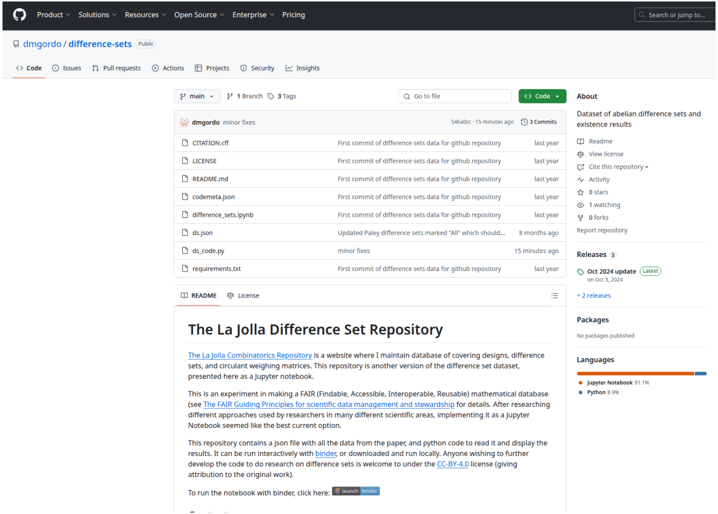
LJDSR 2.0

- Save data as a `json` file
- Write basic `python` or `sage` code to read, manipulate it in a `jupyter notebook`,
- Save as a `github` repo,
- Mirror on `zenodo`, getting permanence and a DOI.

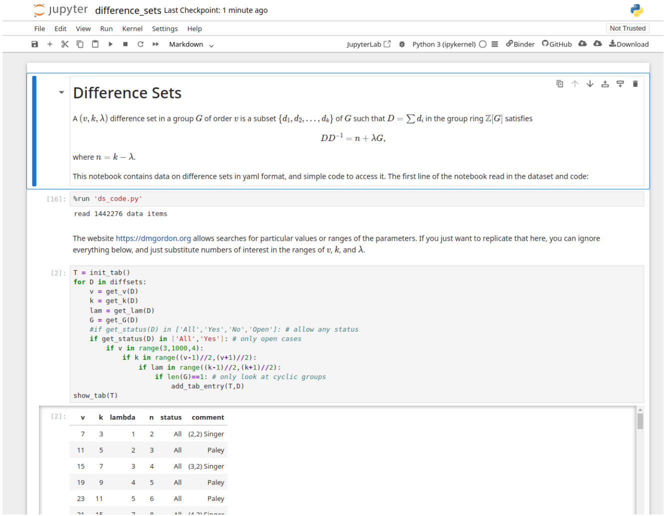
Zenodo Mirror



Github Repo



Product Solutions Resources Open Source Enterprise Pricing
Search or jump to...
dmgordo / difference-sets Public
Code Issues Pull requests Actions Projects Security Insights
main 1 Branch 3 Tags
Go to file
Code
dmgordo minor fixes
546a0cc · 15 minutes ago 3 Commits
CITATION.cff First commit of difference sets data for github repository last year
LICENSE First commit of difference sets data for github repository last year
README.md First commit of difference sets data for github repository last year
codemeta.json First commit of difference sets data for github repository last year
difference_sets.ipynb First commit of difference sets data for github repository last year
ds.json Updated Paley difference sets marked "All" which should... 8 months ago
ds_code.py minor fixes 15 minutes ago
requirements.txt First commit of difference sets data for github repository last year
README License
The La Jolla Difference Set Repository
The La Jolla Combinatorics Repository is a website where I maintain database of covering designs, difference sets, and circulant weighing matrices. This repository is another version of the difference set dataset, presented here as a Jupyter notebook.
This is an experiment in making a FAIR (Findable, Accessible, Interoperable, Reusable) mathematical database (see The FAIR Guiding Principles for scientific data management and stewardship for details. After researching different approaches used by researchers in many different scientific areas, implementing it as a Jupyter Notebook seemed like the best current option.
This repository contains a json file with all the data from the paper, and python code to read it and display the results. It can be run interactively with binder, or downloaded and run locally. Anyone wishing to further develop the code to do research on difference sets is welcome to under the CC-BY-4.0 license (giving attribution to the original work).
To run the notebook with binder, click here: launch binder
About
Dataset of abelian difference sets and existence results
Readme
View license
Cite this repository
Activity
0 stars
1 watching
0 forks
Report repository
Releases 3
Oct 2024 update Latest
on Oct 3, 2024
+ 2 releases
Packages
No packages published
Languages
Jupyter Notebook 91.1%
Python 8.9%



jupyter difference_sets Last Checkpoint: 1 minute ago

File Edit View Run Kernel Settings Help — Not Trusted

Markdown — JupyterLab — Python 3 (ipykernel) — Binder — GitHub — Download

Difference Sets

A (v, k, λ) difference set in a group G of order v is a subset $\{d_1, d_2, \ldots, d_k\}$ of G such that $D = \sum d_i$ in the group ring $\mathbb{Z}[G]$ satisfies

$$DD^{-1} = n + \lambda G,$$

where $n = k - \lambda$.

This notebook contains data on difference sets in yaml format, and simple code to access it. The first line of the notebook read in the dataset and code:

[16]:
```
%run 'ds_code.py'
```

```
read 1442276 data items
```

The website https://dmgordon.org allows searches for particular values or ranges of the parameters. If you just want to replicate that here, you can ignore everything below, and just substitute numbers of interest in the ranges of v, k, and λ.

[2]:
```
T = init_tab()
for D in diffsets:
    v = get_v(D)
    k = get_k(D)
    lam = get_lam(D)
    G = get_G(D)
    #if get_status(D) in ['All','Yes','No','Open']: # allow any status
    if get_status(D) in ['All','Yes']: # only open cases
        if v in range(3,1000,4):
            if k in range((v-1)//2,(v+1)//2):
                if lam in range((k-1)//2,(k+1)//2):
                    if len(G)==1: # only look at cyclic groups
                        add_tab_entry(T,D)
show_tab(T)
```

[2]:

v	k	lambda	n	status	comment
7	3	1	2	All	(2,2) Singer
11	5	2	3	All	Paley
15	7	3	4	All	(3,2) Singer
19	9	4	5	All	Paley
23	11	5	6	All	Paley
31	15	7	8	All	(4,2) Singer

Questions?