The even and odd sets of PG(2,8)

Kris Coolsaet — Ghent University

with Silvia Pagani, Arne Botteldoorn

Irsee, September 1–5, 2025

Definition

A set S of points of a projective plane Π is an **even set** iff all lines of Π intersect S in an *even* number of points.

A set S of points of a projective plane Π is an **odd set** iff all lines of Π intersect S in an *odd* number of points.

Definition

A set S of points of a projective plane Π is an **even set** iff all lines of Π intersect S in an *even* number of points.

A set S of points of a projective plane Π is an **odd set** iff all lines of Π intersect S in an *odd* number of points.

Notation: $w_S(\ell) \overset{\text{def}}{=} |S \cap \ell|$ is the **weight** of the line ℓ w.r.t. S.

Non-trivial odd and even sets only exist when the order q of Π is *even*.

When q is even, the *complement* of an even set is an odd set, and conversely.

Linear codes

Let Π be a plane of even order.

Let $\mathcal{C}$ denote the *binary projective code* of Π, i.e., the vector space over the field $\mathbb{F}_2$ generated by the rows of the incidence matrix of Π.

Then, the code words of the *dual code* $\mathcal{C}^\perp$ (of code words orthogonal to $\mathcal{C}$), correspond to the *even* sets of Π.

Extending the code $\mathcal{C}^\perp$ with the all-1-vector then yields a code whose code words correspond to all odd and even sets.

Linear codes — cntd.

Properties

A line is an odd set.

The *symmetric difference* (sum) of even sets is an even set.

Properties

A line is an odd set.

The *symmetric difference* (sum) of even sets is an even set.

Theorem (Graham-MacWiliams)

In PG(2,q), $q = p^h$.

- $\dim \mathcal{C} = \binom{p+1}{2}^h + 1$
- $\dim \mathcal{C}^\perp = q^2 + q + 1 - \binom{p+1}{2}^h$

Corollary

In PG(2,8) there are $2^{45} \approx 3.5 \cdot 10^{13}$ even sets.

The field of order 8

Elements: $0, 1, \alpha, \ldots, \alpha^6$,

with $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^2 + 1$.

Field automorphism (Frobenius): $x \mapsto x^2$.

Trace:

- $T(x) = x + x^2 + x^4$.
- $T(0) = T(\alpha) = T(\alpha^2) = T(\alpha^4) = 0$,
- $T(1) = T(\alpha^3) = T(\alpha^6) = T(\alpha^5) = 1$.
- $T(x + y) = T(x) + T(y)$.

Research goals

1. Generate a list of **all** odd and even sets in PG(2,8), **up to equivalence**.
   Two sets S, S' are **equivalent** if there exists a *collineation* of PG(2,8) that maps S onto S'.

Research goals

1. Generate a list of **all** odd and even sets in PG(2,8), **up to equivalence**.
   Two sets S, S' are **equivalent** if there exists a *collineation* of PG(2,8) that maps S onto S'.
2. Give a **geometric description** of the sets with an automorphism group of reasonable order, and provide computer-free proofs.

Generation algorithm — classical

Classical technique for isomorph-free generation of all point sets that satisfy a given property (arc, blocking set, …)

- (Recursively) generate larger sets from smaller sets
- At each step extend a set in all possible ways with a single point, while preserving the property
- Make sure that you do not generate more than one set of the same equivalence class
    - Orderly generation
    - Canonical path method

Generation algorithm — classical

Classical technique for isomorph-free generation of all point sets that satisfy a given property (arc, blocking set, …)

- (Recursively) generate larger sets from smaller sets
- At each step extend a set in all possible ways with a single point, while preserving the property
- Make sure that you do not generate more than one set of the same equivalence class
    - Orderly generation
    - Canonical path method

Works only when the property is/can be made **hereditary**. **Not** for even/odd sets.

Irreducible odd/even sets

In a projective plane of even order q :

Lemma

Let S denote an even (resp. odd) set. Let ℓ be a line. Then $S' = S \triangle \ell$ is an odd (resp. even) set, and

$$|S'| = |S| + q + 1 - 2w_\ell(S).$$

Irreducible odd/even sets

In a projective plane of even order q :

Lemma

Let S denote an even (resp. odd) set. Let ℓ be a line. Then $S' = S \triangle \ell$ is an odd (resp. even) set, and

$$|S'| = |S| + q + 1 - 2w_\ell(S).$$

Definition

A set S is called **irreducible** iff $w_\ell(S) \leq q/2$, for all lines ℓ

A set can be reduced by taking the symmetric difference with a line of large enough weight.

Generation algorithm — actual

1. Generate, up to isomorphism, all sets S satisfying

$$w_S(\ell) \leq 4, \text{ for all lines } \ell$$

   Result: 75 227 336 sets
2. Filter out the odd and even sets.
   Result: 78 sets, of size $0, 10, 12, 14, 16, 18, 20, 22, 24, 28$.
   These are all the *irreducible* odd and even sets.
3. Extend the irreducible sets step by step, at each step taking the symmetric difference with a line of weight ≤ 4 (= 'inverse' of reduction).
   Result: 1 437 256 sets.

(Canonical path method to ensure isomorph-free generation.)

Results

After $\pm\frac{1}{2}$ hour of computer time, we find …

%0%4%11%17%20%48%50%58%72
%0%3%4%10%11%16%17%19%20%47%48%49%50%57%58%71
%0%2%3%4%9%10%11%15%16%17%18%19%20%46%47%49%50%56%57%58%70
%0%1%2%3%4%8%9%10%11%14%15%16%18%19%20%45%46%49%50%55%56%57%58%69
%1%2%3%4%7%8%9%10%11%13%14%15%18%19%20%44%45%49%50%54%55%56%57%58%68
%1%2%3%4%6%7%8%9%10%11%12%13%14%18%19%20%43%44%49%50%53%54%55%56%57%58%67%72
%1%2%3%4%6%7%8%9%10%11%12%13%14%18%19%20%23%25%33%43%44%47%48%49%50%52%53%54%55%
56%57%58%59%65%67%68%72
%1%2%3%4%6%7%8%9%10%11%12%13%14%18%19%20%22%24%32%43%44%46%47%49%50%51%53%54%55%
56%57%64%72
%0%1%2%3%4%6%7%8%10%11%13%14%15%18%19%20%37%39%44%45%47%49%50%54%55%56%57%58%61%
62%66%68
%1%2%3%4%6%7%8%10%11%13%14%15%18%19%20%28%30%37%38%39%44%45%47%49%50%52%53%54%55
%56%58%61%62%64%66%68%70
%0%1%2%3%4%6%8%10%11%13%14%15%18%19%20%21%22%26%33%37%42%44%45%47%49%50%54%55%56
%57%58%61%62%66%68%70%72
%1%2%3%4%5%7%9%10%11%13%14%15%18%19%20%36%38%44%45%46%49%50%54%55%56%57%58%60%61
%65%68%72
%0%1%2%3%4%5%6%7%10%11%13%14%15%18%19%20%36%37%38%39%44%45%46%47%49%50%54%55%56%
57%58%60%62%65%66%68%72
%0%1%2%3%4%5%7%8%10%11%13%14%15%16%18%19%20%30%31%35%36%37%38%39%42%44%45%46%47%
48%49%50%51%54%55%56%57%58%60%62%65%66%68%72
%0%1%2%3%4%5%7%8%9%10%11%13%14%15%18%19%20%22%23%27%34%36%38%40%43%44%45%46%49%5
0%54%55%56%57%58%60%61%65%68%71%72
%1%3%4%5%7%8%9%10%11%13%14%15%18%19%20%33%35%43%44%45%49%50%54%55%56%62%68%69
%0%1%3%4%5%6%7%8%10%11%13%14%15%18%19%20%33%35%37%39%43%44%45%47%49%50%54%55%56%
61%66%68%69
%1%3%4%5%6%7%8%10%11%13%14%15%18%19%20%28%30%33%35%37%38%39%43%44%45%47%49%50%52
%53%54%55%56%57%61%64%66%68%69%70
%0%1%3%4%5%6%7%8%10%11%13%14%15%18%19%20%27%29%33%35%39%43%44%45%47%49%50%51%52%
54%55%61%63%66%68%72
%0%1%2%3%4%5%6%7%8%10%11%13%14%15%16%17%18%19%20%21%27%28%29%33%34%35%37%39%43%4
4%45%47%49%50%51%52%54%55%61%63%65%66%67%68%72
%0%1%3%4%5%6%7%8%10%12%13%14%15%16%18%19%20%23%29%32%33%35%37%39%43%44%45%47%49%
50%54%55%56%60%61%62%66%68%69%70
%0%1%3%4%5%7%8%9%10%11%13%14%15%18%19%20%28%30%33%35%38%43%44%45%49%50%52%53%54%
55%56%57%62%64%68%69%70
%0%1%2%3%4%5%7%8%9%10%11%13%14%15%16%17%18%19%20%21%30%33%34%35%37%38%43%44%45%4
9%50%52%53%54%55%56%57%62%64%65%67%68%69%70
%0%1%2%3%4%6%8%9%10%11%12%14%16%18%19%20%43%46%49%50%53%55%56%57%58%67%68%69%72
%0%1%2%3%6%7%8%9%10%11%12%14%16%18%19%20%35%37%43%45%46%49%50%53%55%56%57%58%59%

Odd/even sets up to size 36 **Complements of sets in first columns** **Actual count (not isomorph free)**

(Groups are full collineation groups, including semi-linear maps.)

count	set size	group size				count per size		Actual count/per s
1	0	49448448	1	73	49448448	1	1	1
1	9	677376	1	64	677376	1	73	73
1	10	1512	1	63	1512	1	32704	32704
1	12	288	1	61	288	1	171696	171696
1	13	288	1	60	288	1	171696	171696
1	14	14	1	59	14	1	3532032	3532032
1	15	168	1	58	168		294336	
1	15	42	1	58	42		1177344	
1	15	6	1	58	6	3	8241408	9713088
1	16	18816	1	57	18816		2628	
1	16	288	1	57	288		171696	
1	16	24	1	57	24		2060352	
1	16	18	1	57	18		2747136	
1	16	12	1	57	12		4120704	
1	16	6	1	57	6		8241408	
1	16	2	1	57	2	7	24724224	42068148
1	17	96	1	56	96		515088	
1	17	24	1	56	24		2060352	
1	17	12	1	56	12		4120704	
1	17	6	1	56	6		8241408	
1	17	3	1	56	3		16482816	
2	17	2	2	56	2		49448448	
1	17	1	1	56	1	8	49448448	130317264
1	18	18	1	55	18		2747136	
1	18	12	1	55	12		4120704	
1	18	9	1	55	9		5494272	
4	18	6	4	55	6		32965632	
2	18	4	2	55	4		24724224	
1	18	3	1	55	3		16482816	
7	18	2	7	55	2		173069568	
3	18	1	3	55	1	20	148345344	407949696
1	19	54	1	54	54		915712	
1	19	6	1	54	6		8241408	
4	19	3	4	54	3		65931264	
13	19	2	13	54	2		321414912	
16	19	1	16	54	1	35	791175168	1187678464
1	20	48	1	53	48		1030176	
2	20	12	2	53	12		8241408	
3	20	8	3	53	8		18543168	
4	20	6	4	53	6		32965632	
5	20	4	5	53	4		61810560	
3	20	3	3	53	3		49448448	
24	20	2	24	53	2		593381376	
49	20	1	49	53	1	91	2422973952	3188394720
1	21	882	1	52	882		56064	
1	21	48	1	52	48		1030176	

$\lvert S\rvert$	$\lvert\Gamma\rvert$	$\lvert G\rvert$	
10^i	1 512	504	Hyperoval
12^i	288	96	Theorem 1
13	288	96	Theorem 2. Projective triad. Linear set
14^i	14	14	Sum of two hyperovals. Theorem 3
15	168	56	Linear set. Hyperoval + bisecant through nucleus.
15	42	14	Hyperoval + bisecant not through nucleus.
15	6	6	Theorem 11.
16	18 816	6 272	Sum of two lines
16^i	288	96	Theorem 12. Linear set with line removed.
16^i	24	8	Sum of two hyperovals. Theorem 4.
17	96	32	Theorem 13
18	18	18	Sum of two hyperovals. Theorem 5.
19	54	18	Hyperoval + external line. Theorem 5 (complement).
20	48	16	Projective triad + line of weight 1
21	882	294	Sum of the sides of a triangle
24^i	504	168	Complement of linear set. External points to subplane. Theorem 9
24	96	32	Section 9
24	72	24	Sum of a dual 4-arc. Section 5. Theorem 9.
24^i	42	14	Sum of three hyperovals. Theorem 3.
24^i	24	24	Theorem 10
24	14	14	Sum of three hyperovals. Theorem 3
25	8 064	2 688	Sum of 3 concurrent lines. Linear set. Section 7
25	288	96	Linear set. Section 7
25	36	12	Sum of a dual 5-arc. Section 5
25	24	24	Theorem 10.
25	24	8	Complement of sum of 6 hyperovals. Theorem 4.
26	24	8	Sum of three hyperovals. Theorem 4.
27	18	18	Complement of sum of 5 hyperovals. Theorem 5.
28^i	1 512	504	External points of a dual hyperoval. Ree unital. Theorem 6

The small cases

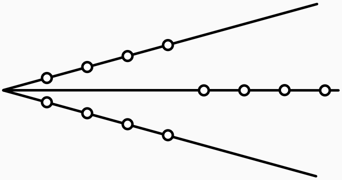
- The empty set. $|S| = 0$, $|G| = 49\,448\,448$
- None with $1 \leq |S| \leq 8$
- The line. $|S| = 9$, $|G| = 677\,376$
- The **regular hyperoval**. $|S| = 10$, $|G| = 1\,512$.
    - Weights : 0 or 2
    - Conic + nucleus

The small cases

- The empty set. $|S| = 0$, $|G| = 49\,448\,448$
- None with $1 \leq |S| \leq 8$
- The line. $|S| = 9$, $|G| = 677\,376$
- The **regular hyperoval**. $|S| = 10$, $|G| = 1\,512$.
    - Weights : 0 or 2
    - Conic + nucleus
- None with $|S| = 11$.

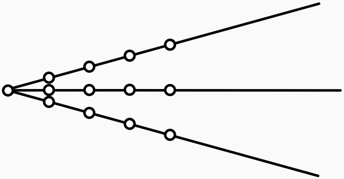
The small cases — cntd.

- $|S| = 12$, $|G| = 288$. Unique!

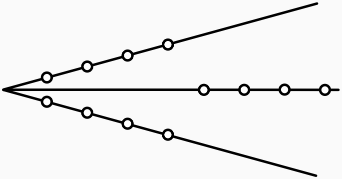


- $|S| = 13$, $|G| = 288$. **Projective triad** — linear set. Unique!

$$(0,0,1); \quad (1,0,z),\ (0,1,z),\ (1,1,z) \text{ with } T(z) = 0$$



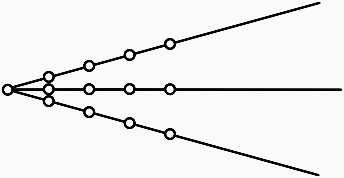
- $|S| = 12$, $|G| = 288$. Unique!



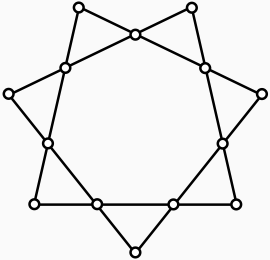
$$(1, 0, z),\ (0, 1, z),\ (1, 1, z) \text{ with } T(z) = 1$$

- $|S| = 13$, $|G| = 288$. **Projective triad** — linear set. Unique!

$$(0, 0, 1); \quad (1, 0, z),\ (0, 1, z),\ (1, 1, z) \text{ with } T(z) = 0$$

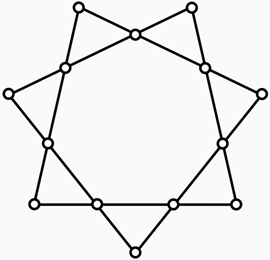


- $|S| = 14$, $|G| = 14$. Unique!
  Symmetric difference of two regular hyperovals = union of two 7-arcs from conics.



The small cases — cntd.

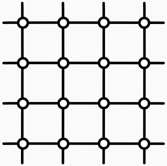
- $|S| = 14$, $|G| = 14$. Unique!
  Symmetric difference of two regular hyperovals = union of two 7-arcs from conics.
- $|S| = 15$. Three cases.
  - Hyperoval + bisecant through nucleus
  - Hyperoval + bisecant
  - S_{14} + 4-secant. $|G| = 6$.



The small cases — cntd.

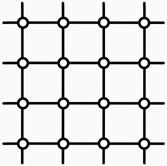
- $|S| = 16$, $|G| = 288$. (Example)

$$(1, y, z) \text{ with } T(y) = T(z) = 0$$

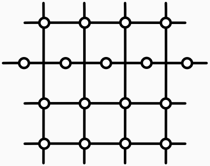


- $|S| = 16$, $|G| = 288$. (Example)

$$(1, y, z) \text{ with } T(y) = T(z) = 0$$



- $|S| = 17$, $|G| =$ **96** (Example)
  = S_{16} + 4-secant.



Sums of odd/even sets

Sums of lines

- One line. $|S| = 9$, $|G| = 677\,676$,
- Two lines. $|S| = 16$, $|G| = 18\,816$,
- Triangle. $|S| = 21$, $|G| = 886$,
- Dual 4-arc. $|S| = 24$, $|G| = 72$,
- Dual 5-arc. $|S| = 25$, $|G| = 36$.

Sum of two hyperovals H, H'

- $|H \cap H'| = 5$. $|S| = 10$. Unique
- $|H \cap H'| = 4$. $|S| = 12$. Unique
- $|H \cap H'| = 3$. $|S| = 14$. Unique
- $|H \cap H'| = 2, 1, 0$. $|S| = 16, 18, 20$. Many examples.

Bundles of hyperovals

H from conic with equation $\phi(x, y, z) = 0$, + nucleus.

H' from conic with equation $\phi'(x, y, z) = 0$, + nucleus.

$H(k, l)$ from conic with equation $k\phi(x, y, z) + l\phi'(x, y, z)$, + nucleus (except degenerate cases).

Bundles of hyperovals

H from conic with equation $\phi(x, y, z) = 0$, + nucleus.

H' from conic with equation $\phi'(x, y, z) = 0$, + nucleus.

$H(k, l)$ from conic with equation $k\phi(x, y, z) + l\phi'(x, y, z)$, + nucleus (except degenerate cases).

Sums of several hyperovals in the same bundle:

- Intersect in 2 points and nucleus:
  $|S| = 14, 24, 28, 38, 42, 52$, $|G| \geq 14$.
- Intersect in 1 point and nucleus:
  $|S| = 16, 26, 32, 42, 48, 58, 64$, $|G| \geq 8$.
- Intersect in nucleus:
  $|S| = 18, 28, 36, 46, 54, 64$, $|G| \geq 18$.

Special cases with larger group. In particular …

Ree unital

Theorem

There is a unique irreducible even set R of size 28. R contains precisely the external points of a dual hyperoval. Lines intersect R in 0 or 4 points.

The automorphism group is that of the (dual) hyperoval.

Can be constructed as sums of 3 or 4 hyperovals in several ways.

Subfield related

Linear sets of rank ≥ 4 are *odd sets*.

= points (x, y, z) satisfying conditions:

Size	Rank	$\lvert\Gamma\rvert$	$\lvert G\rvert$	x	y	z
13	4	288	96	$x \in \mathbb{F}_2$	$y \in \mathbb{F}_2$	$T(z) = 0$
15	4	168	56	$x \in \mathbb{F}_2$	$y \in \mathbb{F}_8$	$z = y^2$
25	5	8064	2688	$x \in \mathbb{F}_2$	$y \in \mathbb{F}_2$	$z \in \mathbb{F}_8$
25	5	288	96	$x \in \mathbb{F}_2$	$T(y) = 0$	$T(z) = 0$
29	5	168	56	$T(x) = 0$	$y \in \mathbb{F}_8$	$z = y^2$
41	6	5376	1792	$x \in \mathbb{F}_2$	$T(y) = 0$	$z \in \mathbb{F}_8$
49	6	504	168	$T(x) = 0$	$T(y) = 0$	$T(z) = 0$

Subfield related (cntd.)

The points of PG(2,8) can be partitioned into a triangle and 7 Fano subplanes $F(b)$, $b \neq 0$:

$$F(b) = \{(y, y^2, by^4) \mid y \in \mathbb{F}_8, y \neq 0\}$$

Some unions of Fano planes provide even sets

$$F(1) \cup F(\alpha^3) \cup F(\alpha^5) \cup F(\alpha^6),$$

$$|S| = 28, |G| = 63$$

$$F(\alpha) \cup F(\alpha^2) \cup F(\alpha^4) \cup \{(1,0,0),(0,1,0),(0,0,1)\},$$

$$|S| = 24, |G| = 504.$$

= external points to $F(1)$ = complement of linear set.

Even/odd sets from Sym(4)

PGL(3,8) has two conjugacy classes of groups isomorphic to Sym(4):

- Acting as permutations of the coordinates $(x, y, z; x + y + z)$. Fixes point $(1, 1, 1; 1)$.
- Dual of the above. Fixes line $x + y + z = 0$.

Some units of orbits of Sym(4) provide even sets with automorphism group (at least) Sym(4) :

- $|S| = 12$ (see earlier)
- $|S| = 24$ (external points of subplane)
- $|S| = 24$ (sum of dual 4-arc)
- $|S| = 48$ (sum of 6 concurrent lines)
- $|S| = 24$, $|G| = 24$, irreducible
- $|S| = 48$, $|G| = 24$

Other examples

Dual even set: **bisecants** of hyperoval H that do **not** contain a fixed point $P \in H$:

- $|S| = 36$, $|G| = 1\,512$ (P = nucleus)
- $|S| = 36$, $|G| = 168$ ($P \neq$ nucleus)

Weights of lines: 0, 4, 8.

Other examples (cntd.)

Points $(1, y, z)$ with

$y =$	0	1	α	α^3	α^2	α^6	α^3	α^5
$z = 0$			$\star$	$\star$	$\star$	$\star$	$\star$	$\star$
1			$\star$	$\star$	$\star$	$\star$	$\star$	$\star$
α	$\star$	$\star$			$\star$	$\star$	$\star$	$\star$
α^3	$\star$	$\star$			$\star$	$\star$	$\star$	$\star$
α^2					$\star$	$\star$		
α^6					$\star$	$\star$		
α^4							$\star$	$\star$
α^5							$\star$	$\star$

$|S| = 32$, $|G| = 96$.

Thank you for your attention