Classification of the Hyperovals in PG(2,64)

Peter Vandendriessche

September 15, 2017

GHENT UNIVERSITY

2 Overview

3 All you need to know

Definition

A *hyperoval* is a set of $q+2$ points in $\mathrm{PG}(2,q)$, no three collinear.

$\Leftrightarrow$ Every line in $\mathrm{PG}(2,q)$ contains 0 or 2 points of the hyperoval.

Remark

Hyperovals in $\mathrm{PG}(2,q)$ exist if and only if $q=2^h$.

Example (Regular hyperoval)

Since all tangents to a conic in $\mathrm{PG}(2,q)$ are concurrent for q even, adding this point to the conic yields a hyperoval.

Classification Result (before I started)

What hyperovals are there in small Desarguesian planes?

Theorem (Classification in Small Desarguesian Planes)

- *In* $\mathrm{PG}(2,2)$ *and* $\mathrm{PG}(2,4)$*, all hyperovals are regular. [trivial]*
- *In* $\mathrm{PG}(2,8)$*, all hyperovals are regular. [Segre, 1957]*
- *In* $\mathrm{PG}(2,16)$*, there are exactly two types of hyperovals up to projective equivalence. [Hall, 1975]*
- *In* $\mathrm{PG}(2,32)$*, there are exactly six types of hyperovals up to projective equivalence. [Penttila and Royle, 1994]*
- *In* $\mathrm{PG}(2,64)$*, there are exactly four types of hyperovals up to projective equivalence that admit a collineation of order* > 1*. [Penttila and Royle, 1995]*

Main goal: classify $q = 64$ regardless of collineation orders.

5 Nonregular hyperovals for $q \leq 64$

All but one examples for $q \leq 64$ were embedded in infinite families

q	Family name	$\lvert P\Gamma L_{hyperoval} \rvert$
16	Subiaco3	144
32	Translation/Glynn	4960
32	Segre	465
32	Payne/Subiaco3	10
32	Cherowitzo	5
32	(sporadic)	3
64	Subiaco2	60
64	Subiaco1	15
64	Adelaide	12
(64	**??**	**1)**

Table: All nonregular hyperovals in $PG(2, q)$, $q \leq 64$

Overview

What is classifying?

Let $G =$PΓL$(3, q)$, the collineation group of PG$(2, q)$.

Primary Objective

Partition the set of hyperovals in PG$(2, q)$ into orbits $H_1^G, \ldots, H_k^G$.

Both the previous classifications and mine consist of two steps:

1) get list of orbits guaranteed to contain each orbit at least once;
2) test for equivalence to retain one copy of each at the end.

8 Search Trees

We will represent the search as a rooted tree.

- Nodes of the tree are sets (representing their PΓL-orbits)
- The root is the empty set.
- A child node is obtained by adding one point to their parent.
- Nodes at depth $q+2$ will be hyperovals
- In the choice of the children we will guarantee that every H^G appears at least once at depth $q+2$

Example: Best Line Approach

Example

Start from $\mathcal{S} = \{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}$ (depth 4).
For $d = 4, \dots, q+1$:

- for each arc $\mathcal{S}$ at maximum depth ($= d$):
  - pick a well-chosen tangent L to $\mathcal{S}$
  - for each $s \in L \setminus \mathcal{S}$ add the child node $\mathcal{S} \cup \{s\}$ to $\mathcal{S}$

The arcs at depth $q+2$ are hyperovals, which then have to be tested for equivalence.

Example: Lexicographic Approach

$$\begin{aligned}
\text{Let } (0,0,1) &< (0,1,0) < (0,1,1) < (0,1,\alpha) < \cdots && \text{(call this line } L_1\text{)}\\
&< (1,0,0) < (1,0,1) < (1,0,\alpha) < \cdots && \text{(call this line } L_2\text{)}\\
&< (1,1,0) < (1,1,1) < (1,1,\alpha) < \cdots && \text{(call this line } L_3\text{)}\\
&< (1,\alpha,0) < (1,\alpha,1) < (1,\alpha,\alpha) < \cdots && \text{(call this line } L_4\text{)}\\
&< \cdots
\end{aligned}$$

Example (Simplification of Penttila and Royle (1994), q=32)

Start from $\mathcal{S} = \{(0,0,1)\}$ (depth 1). For $i = 1, \ldots, q+1$:

- For each $\mathcal{S}$ at depth i, for each $s \in L_i$:
  - Add $\mathcal{S} \cup \{s\}$ as a child of $\mathcal{S}$ if and only if $\mathcal{S} \cup \{s\}$ is an arc and is the lexicographic minimum of $(\mathcal{S} \cup \{s\})^G$.

The child nodes at maximum depths are now one H of each H^G.

11 Feasibility for $q = 64$

For $q = 64$, both techniques are insufficient. On modern hardware:

- Best line technique: $\approx 10^7$ years
- Penttila and Royle: $\approx 10^6$ years
- Hybrid version: $\approx 10^5$ years

Budget: 100-1000 years $\Rightarrow$ fundamentally new techniques needed

Overview

Beyond Orbits

Many search techniques compute the G_S-orbits and structure the search in such a way that only one point per G_S-orbit needs to be considered for addition. But we can do better.

Definition

For $S \subseteq H$ point sets in $\mathrm{PG}(2, q)$, let $R_{H,S} = \{H' \in H^G | S \subseteq H'\}$.

When $S \neq \emptyset$, $R_{H,S}$ is not an orbit of a group action.

Beyond Orbits

Notation

A set S defines an equivalence relation on the points outside of S:

$$a \equiv_S b \Leftrightarrow R_{S\cup\{a\},S} = R_{S\cup\{b\},S}.$$

Remark

G_S-oribts refine $\equiv_S$; every $\equiv_S$-class is a union of G_S-orbits.

We structured the search in such a way that only one point per $\equiv_S$-class needs to be considered, rather than one per G_S-orbit as in most group-based search techniques.

15 Beyond Disjointness

Group-based searches commonly make use of the fact that if a given point of an orbit can be excluded, all points of the orbit can be. But what if we can do more?

Definition

Let E, S be points sets in $\mathrm{PG}(2, q)$. A set $H \supseteq S$ is *strongly S-disjoint* from E if all elements in $R_{H,S}$ are disjoint from E.

Initial Branching

- we can start from $\mathcal{H}_4 = \{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}$ since G acts transitively on the 4-arcs.
- G_{H_4} partitions in 43 orbits, min. 7 on a tangent
- but $\equiv_{H_4}$ partitions it in 11, min. 3 on a tangent
- best tangent classes $\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3$ have sizes 240, 360, 2

Initial Branching

Lemma

Let H be any hyperoval in $\mathrm{PG}(2,64)$ containing H_4, let o_1 be any element of $\mathcal{O}_1$, o_2 be any element of $\mathcal{O}_2$ and o_3 be any element of $\mathcal{O}_3$. Then exactly one of the following statements is true.

- *Some element in R_{H,H_4} contains o_1.*
- *Some element in R_{H,H_4} contains o_2, and H is strongly H_4-disjoint from $\mathcal{O}_1$.*
- *Some element in R_{H,H_4} contains o_3, and H is strongly H_4-disjoint from $\mathcal{O}_1 \cup \mathcal{O}_2$.*

The latter two branches die off quickly $\Rightarrow$ free point!

New Node Type

Definition

A *node* is a pair $(S, \mathcal{C})$ where S is a set of points in $\mathrm{PG}(2, q)$ and $\mathcal{C}$ is a set of pairs (S_i, C_i) with $S_i \subseteq S$ and $C_i \cap S = \emptyset$.

Definition

The *solution set* $\psi(S, \mathcal{C})$ is the set of all hyperoval orbits such that

- for all $(S_i, C_i) \in \mathcal{C}$ one has $C_i \cap H' = \emptyset$ for all $H' \in R_{H,S_i}$;
- and at least one representative H' contains S.

Goal: compute $\psi(\emptyset, \emptyset)$.

New Node Type

The Lemma that provided three cases can now be written as

$$\begin{aligned}\psi(H_4, \emptyset) \quad = \quad & \psi\big(H_4 \cup \{o_1\}, \emptyset\big) \\ & \cup\, \psi\big(H_4 \cup \{o_2\}, \{(H_4, \mathcal{O}_1)\}\big) \\ & \cup\, \psi\big(H_4 \cup \{o_3\}, \{(H_4, \mathcal{O}_1 \cup \mathcal{O}_2)\}\big).\end{aligned}$$

We generalize this idea in the following (rather technical) lemma.

Technical Lemma

Lemma

Let $(S, \mathcal{C})$ be a node, and let L be a projective line tangent to S. Partition the points that can be added to the arc while keeping it an arc, minus $\cup_{(S_i, C_i) \in \mathcal{C}} C_i$, into its $\equiv_S$-equivalence classes. Let $W_1, \ldots, W_m$ be the classes that have nonempty intersection with L and simultaneously have $R_{S \cup \{w\}, S_i} \cap C_i = \emptyset$ for all $(S_i, C_i) \in \mathcal{C}$. Pick arbitrary $w_i \in W_i \cap L$ for $i = 1, \ldots, m$ and let $W = \{w_1, \ldots, w_m\}$. Then, regardless of the choice of the w_i and regardless of the ordering of $W_1, \ldots, W_m$,

$$\psi(S, \mathcal{C}) = \bigcup_{i=1}^{m} \psi\left(S \cup \{w_i\}, \mathcal{C} \cup \{(S, W_1 \cup \cdots \cup W_{i-1})\}\right).$$

Now what?

At the end of the search, we end up with thousands of hyperovals, at least one of each type. Now what?

- Classical equivalence testing to divide N hyperovals into k classes, takes $\mathcal{O}(kNq^4 \log q)$ time, which is a significant cost.
- We found a better trick, completing the task in $\mathcal{O}(k(N + q^4) \log q)$ time:
  - First, we explicitly compute R_{H,H_4} for one hyperoval
  - $H \cong H' \Leftrightarrow H' \in R_{H,H_4}$ (tested N times at $\mathcal{O}(k \log q)$ each)
  - If not, compute new R_{H',H_4} (k times at $\mathcal{O}(q^4 \log q)$ each)

Remark

Knowing each R_{H',H_4} also allows extensive verification of the correctness of our search, but this is beyond the scope of this talk.

Overview

Classification Result

Theorem (Classification in Small Desarguesian Planes)

- *In* $\mathrm{PG}(2,2)$ *and* $\mathrm{PG}(2,4)$*, all hyperovals are regular. [trivial]*
- *In* $PG(2,8)$*, all hyperovals are regular. [Segre, 1957]*
- *In* $\mathrm{PG}(2,16)$*, there are exactly two types of hyperovals up to projective equivalence. [Hall, 1975]*
- *In* $\mathrm{PG}(2,32)$*, there are exactly six types of hyperovals up to projective equivalence. [Penttila and Royle, 1994]*
- *In* $\mathrm{PG}(2,64)$*, there are exactly four types of hyperovals up to projective equivalence. [Vandendriessche, 2017]*

Nonregular Hyperovals for $q \leq 64$

q	Family name	$\lvert P\Gamma L_{hyperoval} \rvert$
16	Subiaco3	144
32	Translation/Glynn	4960
32	Segre	465
32	Payne/Subiaco3	10
32	Cherowitzo	5
32	(sporadic)	3
64	Subiaco2	60
64	Subiaco1	15
64	Adelaide	12

Overview

Can we do $q = 128$?

Using these techniques, tackling $q = 128$ would take a whopping 20 000 000 000 000 000 000 000 000 years to complete. So no.

On the other hand, history gives hope:

- $q = 8$: exactly one type [Segre, 1957]
- $q = 16$: exactly two types [Hall, 1975]
- $q = 32$: exactly six types [Penttila and Royle, 1994]
- $q = 64$: exactly four types [Vandendriessche, 2017]

$\Rightarrow$ new breakthrough approximately every 20 years, so who knows?

Future plans

More short-term goals:

- Try $q = 128$ under the assumption of a nontrivial collineation
- Try to extend these techniques to KM-arcs
- Find more interesting and challenging computational problems (suggestions are welcome!)

Thank you for your attention!