Projective two-weight sets

Stefaan De Winter[1]
National Science Foundation, USA

July 6th, 2023

[1] This material is based upon work supported by and while serving at the National Science Foundation. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

Throughout p will be a prime and q a power of p.

$V(n, q)$: The n-dimensional vector space over GF(q).

PG(n, q): The n-dimensional projective space over GF(q), that is, the geometry "at infinity" of $V(n+1, q)$.

We have the following connections ("Blow-up"):

$\mathrm{PG}(n, q^k) \to V(n+1, q^k) \to V((n+1)k, q) \to$
$\mathrm{PG}((n+1)k-1, q)$

Definition: A projective two-weight set $\mathcal{S}$ is a set of points in PG(n, q) with the property that every hyperplane intersects $\mathcal{S}$ in either a or b points with $a < b$.

Examples:

- unitals in PG$(2, q^2)$;
- hyperovals in PG$(2, 2^k)$;
- Baer-subspaces in PG(n, q^2);
- maxima arcs in PG$(2, 2^k)$;
- ....

We care because these are beautiful objects but also because of the important connections as described in the celebrated Calderbank-Kantor paper “The geometry of two-weight codes”:

Every projective two-weight set

$\leftrightarrow$

A linear two-weight code

$\leftrightarrow$

A strongly regular graph admitting an elementary abelian Singer group

The examples that inspired this work: maximal arcs.

Apart from the earlier mentioned connections maximal arcs also yield partial geometries.

Definition: A maximal d-arc $\mathcal{K}$ in PG$(2, q)$ is a non-empty set of points with the property that every line intersects $\mathcal{K}$ in either 0 or $0 < d < q$ points. (d is necessarily a power of p)

A by now classical result (Ball, Blokhuis and Mazzocca) states that necessarily q is even.

The basic example is the hyper-conic (= conic plus its nucleus) which is a maximal 2-arc.

The most important other examples are due to Denniston and Mathon, the so-called Denniston-arcs and Mathon-arcs.

In both cases these maximal d-arcs are constructed as a union of conics on a common nucleus.

What if q is odd?

We can clearly not hope for a maximal arc. However:

$\mathrm{PG}(2, q^2) \to V(3, q^2) \to V(6, q) \to PG(5, q)$

Two-weight sets in $\mathrm{PG}(2, q^2)$ yield two-weight sets in $\mathrm{PG}(5, q)$. Hence a maximal arc in $\mathrm{PG}(2, q^2)$ yields two-weight sets in $\mathrm{PG}(5, q)$ with certain specific parameters. (Other powers of q yield examples in other dimensions.)

Do such two weight-sets exist when q is odd?

As such sets yield strongly regular graphs, what better place than Brouwer's table to check what is known.

A couple of sporadic examples by Kohnert (computer construction of codes) and Gulliver and a by now famous example by Mathon in $PG(5, 3)$. The Mathon example is particularly interesting in that it consists of a union of 21 lines and hence also yields a partial geometry. It is the closest one can hope to get to a "blow-up" of a non-existing maximal 3-arc in $PG(2, 9)$.

Any general constructions?

A little surprise to come later on ....

As (hyper-)conics seem to be at the basis of most constructions of maximal arcs, the question becomes:

"How to generalize the hyper-conic to odd characteristic in higher dimension?"

There are a gazillion wonderful properties the hyper-conic has, and so I tried and failed a gazillion of times

A property of interest:

The hyper-conic is stabilized by a group G that fixes the nucleus, acts as a Singer group on the remaining $q + 1$ points and also as a Singer group on a line of $\mathrm{PG}(2, q)$ (let's call it the line at infinity).

For peace of mind consider the situation in $\mathrm{PG}(2, q^2)$ and correspondingly in $\mathrm{PG}(5, q)$.

In $PG(5, q)$ the nucleus becomes a line and the line at infinity becomes a 3-space. We can translate a Singer group on the line at infinity to a Singer group of this 3-space. What about fixing the nucleus?

With a little imagination the identity on a point is a Singer group on that point, so why not making this into a Singer group on the resulting line in $PG(5, q)$.

We can somewhat unconventionally coordinate $\mathrm{PG}(5, q)$ as follows:

Let Π be a 3-space and L be a disjoint line (hence Π and L span $\mathrm{PG}(5, q)$). Now we coordinate the full space by a 2-tuple $(\alpha, \beta) \neq (0, 0)$ with α in $\mathrm{GF}(q^4)$ and β in $\mathrm{GF}(q^2)$ and (α, β) determined up to a scalar λ in $\mathrm{GF}^*(q)$.

Here $(\alpha, 0)$ represents Π and $(0, \beta)$ represents L.

We consider the following group:

$G =< (\gamma, \delta) >$ where γ is a primitive element of GF(q^4) and δ is a primitive element of GF(q^2) acting naturally (multiplication) on the points (α, β) of PG$(5, q)$.

Then G induces a Singer group on Π and on L.

We now consider the stabilizer of a point of L:

$$< \gamma^{(q+1)}, \delta^{(q+1)} >.$$

What does this group generate in Π*?*

With a little work one figures out that $\gamma^{(q+1)}$ generates an ovoid (elliptic quadric) in Π (traced out $q-1$ times). This is actually well described by Ebert. Hence $< \gamma^{(q+1)} >$ yields a so-called elliptic fibration of Π, that is a partition of the point set into $q+1$ disjoint ovoids (see Ebert). Each of these ovoids naturally corresponds to a point of L under G.

Now consider the following "cones" $C_p := p\mathcal{Q}_p \setminus \mathcal{Q}_p$ where p is a point on L and $\mathcal{Q}_p$ is the ovoid corresponding to p as in the previous slide.

Define $\mathcal{S} := \bigcup_{p \in L} C_p$.

Theorem

The set $\mathcal{S}$ is a two-weight set in $PG(5, q)$ with the same parameters as would arise from the blow-up of a maximal q-arc in $PG(2, q^2)$.

What about higher dimensions?

Consider Π a $\mathrm{PG}(2n-1, q)$ and L a $\mathrm{PG}(n-1, q)$ spanning $\mathrm{PG}(3n-1, q)$.

Coordinate as before and consider the point stabilizer of a point of L. Not that trivial, but Cossidente and Storme come to the rescue!

Theorem (C-S)

For every $a \in \mathbb{F}^*_{q^n}$ the set $\mathcal{Q}_a = \{x \in \mathrm{PG}(2n-1,q) \mid \mathrm{Tr}(ax^{q^n+1}) = 0\}$, with Tr the usual trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, is an elliptic quadric of PG$(2n-1,q)$ and the elliptic quadrics $\mathcal{Q}_a$ form, through the parameter a, a projective space $\mathrm{PG}(n-1,q)$. Any linear combination $\lambda\mathcal{Q}_a + \mu\mathcal{Q}_b$, $\lambda,\mu \in \mathbb{F}_q$, of two elliptic quadrics $\mathcal{Q}_a$ and $\mathcal{Q}_b$ defines a new elliptic quadric $\mathcal{Q}_{\lambda a+\mu b}$.

Theorem (C-S)

Let $\xi = \beta^{(q^n-1)/(q-1)}$, with β a primitive element of $\mathbb{F}_{q^{2n}}$. Then an orbit in $\mathrm{PG}(2n-1, q)$ under $< \xi >$ has size $q^n + 1$ and is either contained in or disjoint from $\mathcal{Q}_a$, $a \in \mathbb{F}_{q^n}$. Furthermore, each such orbit is either a cap (when n is even) or a union of disjoint lines (when $n \geq 3$ is odd) that is the intersection of $n-1$ linearly independent $\mathcal{Q}_a$.

As a result we can view the elliptic quadrics $\mathcal{Q}_a$ as the points of a PG$(n-1, q)$ (see above) and the orbits under $< \xi >$ as the hyperplanes H of this projective space $\mathcal{P}$.

Let δ be an anti-automorphism between $\mathcal{P}$ and L such that hyperplane H_p gets mapped to point p.

Now consider the following "cones" $C_p := pH_p \setminus H_p$ where p is a point on L and H_p is the hyperplane $\delta(p)$.

Define $\mathcal{S} := \bigcup_{p \in L} H_p$.

Theorem

The set $\mathcal{S}$ is a two-weight set in PG$(3n-1, q)$ with the same parameters as would arise from the blow-up of a maximal q-arc in PG$(2, q^n)$.

The two-weight set $\mathcal{S}$ admits $G = < \gamma, \beta >$ acting cyclicly on the points of $\mathcal{S} \setminus L$.

This allows for a nice group theoretic construction of our two-weight sets that shows the direct connection with our initial hyperconic property.

The little surprise promised earlier, discovered by cleaning my office and finding an unfortunately never read paper given to me by Jurgen Bierbrauer: Bierbrauer and Edel constructed linear two-weight codes with the same parameters using a rather intricate coding theoretic construction in an unfortunate obscure paper published in 1998! (*Journal of Combinatorial Designs*).

It is unclear to me if the two-weight sets constructed here are isomorphic to those arising from the codes of Bierbrauer and Edel. And this seems like a nice open problem.

A key open question?

Can we use the two-weight sets constructed here as true generalizations of hyper-conics? That is, can they be building blocks of other interesting combinatorial structures, especially in odd characteristic? For example, can we take unions of such sets on the same “base” L to build larger two-weight sets? (I am rather convinced the answer is yes.)

THANKS!