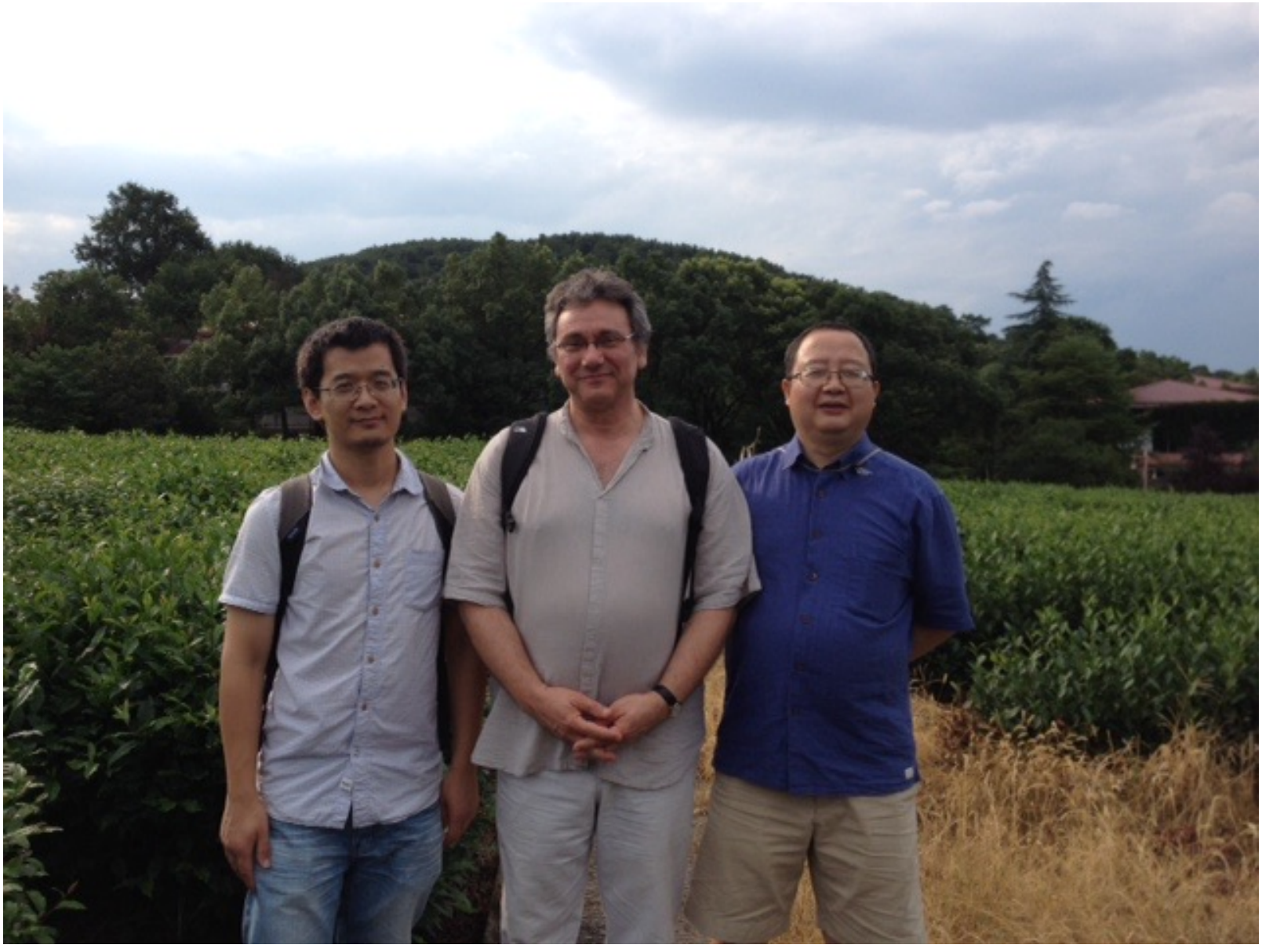
Applications of Linear Algebraic Methods in Combinatorics and Finite Geometry

Qing Xiang
Department of Mathematical Sciences
University of Delaware
Newark, DE 19716

AEGT 2017, in honor of Haemers, Lazebnik and Woldar



1. Cap-sets
2. Partial ovoids in $Q^-(5, q)$
3. Partial ovoids in the Ree-Tits Octagon

} Joint work with Ihringer & Sin

Cap-sets (affine caps)

Definition. Let $A \subseteq \mathbb{F}_3{}^n$. We say that A is a cap-set if there are no nontrivial solutions to

3-term progression

$$x + y + z = 0, \qquad x - y = y - z$$

where $x, y, z \in A$. (Here "trivial" means that $x = y = z$.)

Question. What is the largest size of a cap-set in $\mathbb{F}_3{}^n$? (We will denote the largest size by $r_3(n)$.)

The first few terms of the sequence are $2, 4, 9, 20, 45, 112$. See A090245 in Sloane's encyclopedia of integer sequences.

You probably encountered the number $r_3(4) = 20$ if you played the card game SET.

One can easily show that $r_3(n) \geq 2^n$. Simply note that $\{0, 1\}^n$ is a cap-set in $\mathbb{F}_3{}^n$.

A more sophisticated construction by Edel shows that $r_3(n) \geq (2.2174...)^n$ when n is large.

Upper Bounds

- Meshulam (1995, JCTA) $r_3(n) \leq c\frac{3^n}{n}$. Roth's thm (Disc. Fourier)
- Bateman-Katz (2012, JAMS) $r_3(n) \leq c\frac{3^n}{n^{1+\epsilon}}$, where ϵ is a small positive constant.
- Croot-Lev-Pach; Ellenberg-Gijswijt (May 2016, Annals Math) $r_3(n) \leq 3 \cdot (2.7551...)^n$.

The proof uses polynomials and linear algebra. Let's fix some notation.

We will consider various subspaces of the polynomial ring $V = \{f : \mathbb{F}_3{}^n \to \mathbb{F}_3\} = \mathbb{F}_3[X_1, \ldots, X_n]/(X_1^3 - X_1, \ldots, X_n^3 - X_n)$.

For an integer $0 \leq d \leq 2n$, let Pol_d =the $\mathbb{F}_3$-vector subspace of cube-free polynomials in n variables of degree $\leq d$ $=\mathrm{Span}\{X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \mid i_1 + i_2 + \cdots + i_n \leq d,\ 0 \leq i_j \leq 2\ \forall j\}$.

For example, $\dim(\mathrm{Pol}_{2n}) = 3^n$. Write $D = \dim(\mathrm{Pol}_{2n/3})$.

With a little bit "generating function" argument one finds that $D = (2.7551...)^n$. Also note that $\dim(\mathrm{Pol}_{4n/3}) = 3^n - D$.

Lemma

Let $A \subseteq {\mathbb{F}_3}^n$ with $|A| > 3D$. Then there is a subset $A' \subset A$ and some $p \in \mathrm{Pol}_{4n/3}$ such that $|A'| \geq |A| - D$, $p(b) \neq 0$ for all $b \in A'$ and $p(x) = 0$ for all $x \notin A$.

Proof. For any $x \notin A$, the condition that $p(x) = 0$ is a linear relation on the coefficients of p. So by linear algebra the subspace W consisting of $p \in \mathrm{Pol}_{4n/3}$ with $p(x) = 0$ for all $x \notin A$ has dimension

$$\geq (3^n - D) - (3^n - |A|) = |A| - D.$$

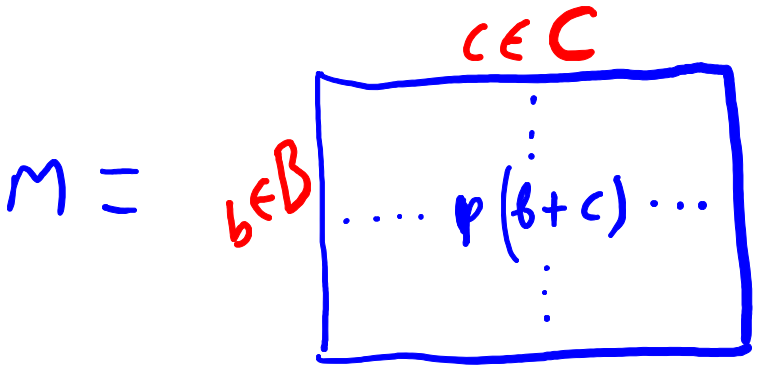
Furthermore there is some $p \in W$ which is nonzero on a subset $A' \subset A$ of size $\geq \dim W$.

The Croot-Lev-Pach Principle

Lemma

Let $B, C \subseteq \mathbb{F}_3{}^n$. Assume that $p \in \mathrm{Pol}_d$. Form the matrix M whose rows are indexed by elements $b \in B$, whose columns are indexed by elements $c \in C$, and with (b, c)-entry equal to $p(b + c)$. Then the rank of M over $\mathbb{F}_3$ is less than or equal to $2 \cdot \dim(\mathrm{Pol}_{d/2})$.

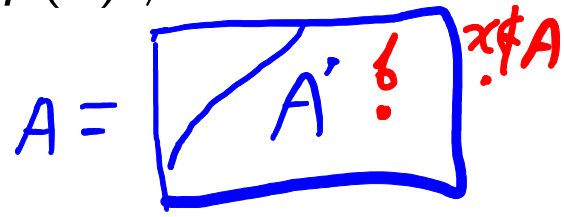
Proof. Factorize $M = XNY$, where X, Y are Vandermonde-like matrices and the entries of N consist of coefficients of $p(b + c)$.



Proof of the Bound of Ellenberg and Gijswijt

Let $A \subseteq \mathbb{F}_3{}^n$ be a cap-set. Suppose that $|A| > 3D$, where $D = \dim(\mathrm{Pol}_{2n/3})$.

By Lemma 1, there exist a subset $A' \subset A$, $|A'| > 2D$, and $p \in \mathrm{Pol}_{4n/3}$ such that $p(x) = 0$ for all $x \notin A$, and $p(b) \neq 0$ for all $b \in A'$.



Apply Lemma 2 to $B = C = -A'$. Note that

$$M_{b,c} = p(b + c),$$

which is 0 if $b \neq c$ since $b + c \notin A$, and is nonzero if $b = c$ since $b + c = 2b = -b \in A'$.

a cap-set

If $b + c \in A$, then $b + c = a \in A \Rightarrow a + (-b) + (-c) = 0$

$a \in A$, $-b \in A'$, $-c \in A'$

So M is a diagonal matrix with nonzero diagonal entries. Hence

$$\mathrm{rank}_{\mathbb{F}_3}(M) = |A'| \geq |A| - D > 2D.$$

But by Lemma 2,

$$\mathrm{rank}_{\mathbb{F}_3}(M) \leq 2 \cdot \dim(\mathrm{Pol}_{2n/3}) = 2D,$$

a contradiction. Therefore $|A| \leq 3D$.

(1) Main innovation: Constructing the matrix M

(2) This is not the first time a rank argument proved to be so successful. For example, see Blokhuis/Moorhouse, p-ranks related to orthspaces, JACO 1995

Generalized n-gons

A *generalized n-gon* of order (s, r) is a triple $\Gamma = (\mathcal{P}, \mathcal{L}, \mathsf{I})$, where elements of $\mathcal{P}$ are called *points*, elements of $\mathcal{L}$ are called *lines*, and $\mathsf{I} \subseteq \mathcal{P} \times \mathcal{L}$ is an *incidence relation* between the points and lines, which satisfies the following axioms:

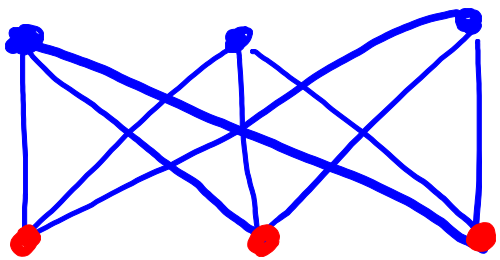
(a) Each line is incident with $s + 1$ points.

(b) Each point is incident with $r + 1$ lines.

(c) The *incidence graph* has diameter n and girth $2n$.

Here the incidence graph is the bipartite graph with $\mathcal{P} \cup \mathcal{L}$ as vertices, $p \in \mathcal{P}$ and $\ell \in \mathcal{L}$ are adjacent if $(p, \ell) \in \mathsf{I}$. If s=1 or $r = 1$, the generalized n-gon is called *thin*. Otherwise, it is called *thick*.

Example. A generalized 2-gon of order $(2, 2)$.



The incidence graph

For $n = 2$, a generalized 2-gon is just a complete bipartite graph $K_{s+1,r+1}$.

For $n = 3$, a thick generalized 3-gon is a projective plane.

Generalized quadrangles have been extensively studied.

Theorem (Feit-Higman, 1964)

Finite thick generalized n-gons exist only for $n \in \{2, 3, 4, 6, 8\}$.

The only known thick finite generalized octagons are the *Ree-Tits octagons* $\mathcal{O}(q)$ (sometimes also called generalized octagons of type ${}^2F_4(q)$) , where $q = 2^t$ and t is odd, and their duals.

The Ree-Tits octagon $\mathcal{O}(q)$ has $(q+1)(q^3+1)(q^6+1)$ points and $(q^2+1)(q^3+1)(q^6+1)$ lines. The smallest example, $\mathcal{O}(2)$, has 1755 points and 2925 lines.

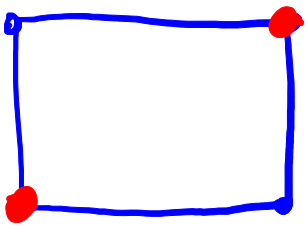
It is a big open problem whether there exist other generalized octagons.

Even from the point of view of graph theory, generalized n-gons are very interesting because they provide sparse but highly connected graphs. The competing goals of being sparse and highly connected are desirable in the design of efficient communication networks and for constructions of LDPC codes.

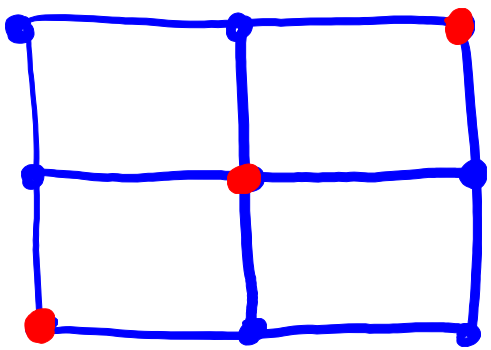
Partial Ovoids in Generalized n-gons

A *partial ovoid* of a generalized n-gon Γ is a set of points pairwise at distance n in the incidence graph.

Example. Ovoids in thin generalized quadrangles.



$GQ(1,1)$



$GQ(2,1)$

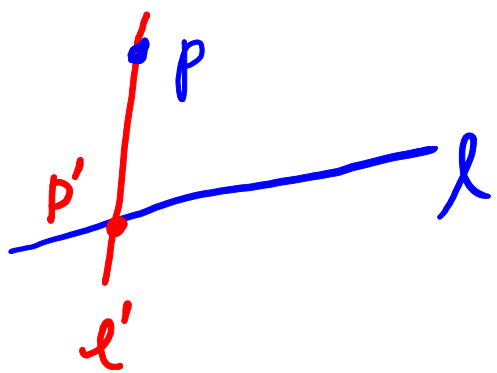
Generalized Quadrangles

A *generalized quadrangle* (GQ) of order (s, r) is a triple $(\mathcal{P}, \mathcal{L}, \mathsf{I})$, where elements of $\mathcal{P}$ are called *points*, elements of $\mathcal{L}$ are called *lines*, and $\mathsf{I} \subseteq \mathcal{P} \times \mathcal{L}$ is an *incidence relation* between the points and lines, which satisfies the following axioms:

(a) Each line is incident with $s + 1$ points.

(b) Each point is incident with $r + 1$ lines.

(c) For every point p not on a line ℓ, there exists a unique point $p' \,\mathsf{I}\, \ell$ and a unique line ℓ' such that $p' \,\mathsf{I}\, \ell'$.



Examples

order (q, q) (q, q)

Finite classical polar spaces of rank 2: $W(3, q)$, $Q(4, q)$, $Q^-(5, q)$, $H(3, q^2)$, $H(4, q^2)$

Example: $Q^-(5, q)$

Let $Q : {\mathbb{F}_q}^6 \to \mathbb{F}_q$ be the quadratic form $Q(x) = x_1x_2 + x_3x_4 + f(x_5, x_6)$, where $f(x_5, x_6)$ is an irreducible quadratic form.

1. Let $\mathcal{P}$ be the set of all totally singular 1-spaces.
2. Let $\mathcal{L}$ be the set of all totally singular 2-spaces.
3. Let I be the inclusion relation.

Then $(\mathcal{P}, \mathcal{L}, \mathrm{I})$ is a GQ(q, q^2).

A *strongly regular graph* (SRG) with parameters (v, k, λ, μ) is a k-regular graph on v vertices such that two adjacent vertices have λ common neighbors and two non-adjacent vertices have μ common neighbors.

The *point graph* of a generalized quadrangle $(\mathcal{P}, \mathcal{L}, \mathsf{I})$ is the graph with vertex set $\mathcal{P}$, where two elements of $\mathcal{P}$ are adjacent if and only if they are on a common line of the GQ.

Lemma

The point graph of a GQ of order (s, r) is an SRG with $v = (s+1)(sr+1)$, $k = (r+1)s$, $\lambda = s-1$, and $\mu = r+1$.

Partial Ovoids in GQs

Definition. (Thas, 1981) A partial ovoid $\mathcal{O}$ of a GQ is a subset of points, which meet every line at most once (equivalently, no two points of $\mathcal{O}$ are collinear).

Definition. (Alternative) A partial ovoid of a GQ is a coclique of its point graph.

Lemma

A partial ovoid of a GQ(s, r) *has size at most* $sr + 1$.

① Counting

② Hoffman's bound

A partial ovoid of a GQ(s, r) having size $sr + 1$ is called an *ovoid*.

Question. Which GQs possess ovoids? If a GQ does not possess ovoids, what is the largest size of a partial ovoid of the GQ?

A thin GQ(s, r) always has an ovoid.

As another example, $Q(4, q)$ (the parabolic quadric) has ovoids. Some hyperplane of $\mathbb{F}_q{}^5$ meets $Q(4, q)$ in an elliptic quadric, which is an ovoid of $Q(4, q)$.

Lemma (Thas, 1981)

A partial ovoid $\mathcal{O}$ of a $GQ(q, q^2)$ has size at most $q^3 - q^2 + q$. In particular, $Q^-(5, q)$ does not have an ovoid.

Proof. (argument due to Godsil)

1. As the point graph is an SRG, the adjacency matrix of the point graph has THREE eigenspaces.
2. One eigenspace V has dimension $q^3 - q^2 + q$.
3. Let E be the orthonormal projection onto V.
4. The submatrix $E_{\mathcal{O}}$ of E indexed by $\mathcal{O}$ has form $\alpha I + \beta J$.
5. The matrix $E_{\mathcal{O}}$ has full rank.

Theorem (De Beule, Klein, Metsch, Storme, 2008)

A partial ovoid $\mathcal{O}$ of $Q^-(5,q)$ has size at most $(q^3+q+2)/2$.

This bound is tight for $q = 2, 3$.

Theorem (Ihringer, Sin, X, April 2016)

A partial ovoid $\mathcal{O}$ of $Q^-(5,q)$, $q = p^t$, has size at most

$$\left(\frac{2p^3+p}{3}\right)^t + 1.$$

Proof. Use p-ranks instead of ranks over **R**.

For $p = 2$ fixed, we obtain the bound $\approx q^{2.59}$.
For $p = 3$ fixed, we obtain the bound $\approx q^{2.68}$.
The largest known infinite family has size $\approx 3q^2/2$.

Partial Ovoids in the Ree-Tits Octagon

Recall: A *partial ovoid* of a generalized octagon Γ is a set of points pairwise at distance 8 in the incidence graph.

An easy counting argument shows that the size of a partial ovoid of a generalized octagon of order (s, r) is at most $(sr)^2 + 1$. A partial ovoid of a generalized octagon of order (s, r) is called an *ovoid* if it has the maximum possible size $(sr)^2 + 1$. The Ree-Tits octagon $\mathcal{O}(2^t)$ is a generalized octagon of order $(2^t, 4^t)$, so the size of a partial ovoid is at most $64^t + 1$.

Theorem (Ihringer, Sin, X. April 2016)

The size of a partial ovoid of the Ree-Tits octagon $\mathcal{O}(2^t)$, t odd, is at most $26^t + 1$.

Corollary

The Ree-Tits octagon does not have an ovoid.

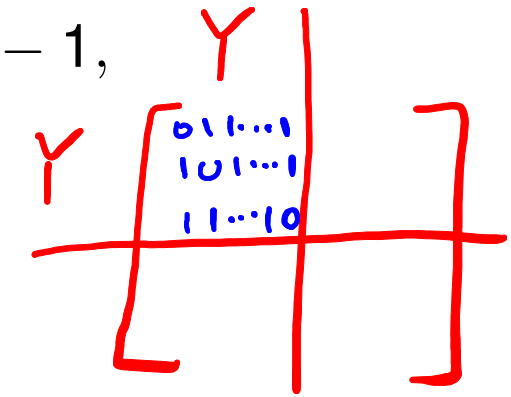
Remarks. (1) In the case where $t = 1$, the theorem was proved by Coolsaet and Van Maldeghem in 2000.

(2) The corollary was conjectured by Coolsaet and Van Maldeghem in 2000.

Lemma

Let $(X, \sim)$ be a graph. Let A be the adjacency matrix of X. Let Y be a clique of X. Then

$$|Y| \leq \begin{cases} \operatorname{rank}_p(A) + 1, & \text{if } p \text{ divides } |Y| - 1, \\ \operatorname{rank}_p(A), & \text{otherwise.} \end{cases}$$



Proof.

Let J be the all-ones matrix of size $|Y| \times |Y|$. Let I be the identity matrix of size $|Y| \times |Y|$. As Y is a clique, the submatrix A' of A indexed by Y is $J - I$. Hence, the submatrix has p-rank $|Y| - 1$ if p divides $|Y| - 1$, and it has p-rank $|Y|$ if p does not divide $|Y| - 1$. As $\operatorname{rank}_p(A') \leq \operatorname{rank}_p(A)$, the assertion follows. □

Now we consider the oppositeness graph of the Ree-Tits octagon. The vertices of the graph are the points of the octagon and two vertices are connected by an edge if and only if they are opposite (i.e., the two points have distance 8 in the incidence graph of the octagon).

A partial ovoid of the octagon corresponds to a clique in the oppositeness graph.

Theorem (Peter Sin)

Let $A_R(q)$ denote the oppositeness matrix for objects of one fixed type in a building with root system R over $\mathbb{F}_q$, where $q = p^t$, p is a prime. Then

$$\mathrm{rank}_p(A_R(q)) = \mathrm{rank}_p(A_R(p))^t.$$

For the Ree-Tits octagon $\mathcal{O}(2)$, it was known that the oppositeness matrix has 2-rank 26. (Veldkamp 1970, and Sin 2012)

By the above theorem, the oppositeness matrix of the Ree-Tits octagon $\mathcal{O}(2^t)$ has 2-rank 26^t for all odd t. Hence by the lemma about the clique sizes of graphs, we see that the size of a partial ovoid of $\mathcal{O}(2^t)$ is at most $26^t + 1$.

Thank you for your attention!