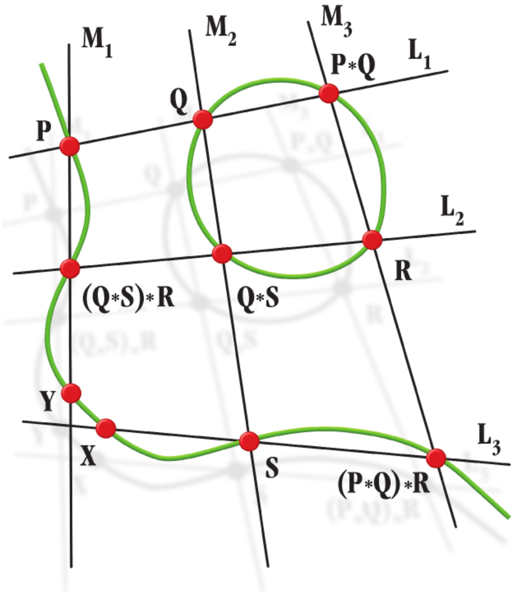
Finite Geometry Conference and Workshop

10-14 June 2013



Bolyai Institute
University of Szeged
Hungary

Description

This is a conference about finite geometry, Galois fields, coding theory and combinatorics.

The talks are intended to give a survey of recent contributions to the following subjects:

- Arcs and caps from cubic curves and their applications in coding theory
- Geometry of the Hermitian varieties
- Objects in finite planes and their collineation groups
- Finite fields and Galois geometries
- Independent sets in hypergraphs

Location: József Attila Study and Information Centre, University of Szeged

Web page: `http://www.math.u-szeged.hu/~nagyg/Egyeb/GeoWs/`

Organizer: Gábor P. Nagy, Bolyai Institute, University of Szeged

Participants

- József Balogh (Szeged)
- Daniele Bartoli (Perugia)
- Norbert Bogya (Szeged)
- Antonio Cossidente (Potenza)
- Bence Csajbók (Potenza)
- Massimo Giulietti (Perugia)
- Tamás Héger (Budapest)
- György Kiss (Budapest)
- Gábor Korchmáros (Potenza)
- József Kozma (Szeged)
- Valentino Lanzone (Potenza)
- Francesco Mazzocca (Napoli)
- Gábor P. Nagy (Szeged)
- Vito Napolitano (Napoli)
- Carmela Nole (Potenza)
- Francesco Pavese (Potenza)
- Alessandro Siciliano (Potenza)
- Angelo Sonnino (Potenza)

- Pietro Speziali (Perugia)
- Tamás Szőnyi (Budapest)
- Andor Táborosi (Szeged)
- Marcella Takáts (Budapest)

Sponsor

The conference is supported by the European Union and co-funded by the European Social Fund.

Project title: *"Broadening the knowledge base and supporting the long term professional sustainability of the Research University Centre of Excellence at the University of Szeged by ensuring the rising generation of excellent scientists."*

Project number: TÁMOP-4.2.2/B-10/1-2010-0012

Abstracts

Author: József Balogh (Szeged)

Coauthors: Robert Morris, Wojciech Samotij

Title: Independent sets in hypergraphs

Summary:

Many important theorems and conjectures in combinatorics, such as the theorem of Szemerédi on arithmetic progressions and the Erdős-Stone Theorem in extremal graph theory, can be phrased as statements about families of independent sets in certain uniform hypergraphs. In recent years, an important trend in the area has been to extend such classical results to the so-called 'sparse random setting'. This line of research has recently culminated in the breakthroughs of Conlon and Gowers and of Schacht, who developed general tools for solving problems of this type. Although these two papers solved very similar sets of longstanding open problems, the methods used are very different from one another and have different strengths and weaknesses.

In this talk, we explain a third, completely different approach to proving extremal and structural results in sparse random sets that also yields their natural 'counting' counterparts. We give a structural characterization of the independent sets in a large class of uniform hypergraphs.

The talk is intended to be a survey type talk, targeting general audience.

Author: Bence Csajbók (Potenza)

Title: Inverse-closed linear subspaces and related problems

Summary:

If D is a planar difference set in an abelian group, then -D is an oval (Jungnickel and Vedder 1987, see also Hall 1984). If A is an inverse-closed additive subgroup of a field F of characteristic different from two, then A is a subfield of F or it is the set of elements of trace zero in some quadratic field extension contained in F (Goldstein, Guralnick, Small and Zelmanov 2006, and Mattarei 2007).

In this talk we present some connections between the above results and show some of their generalizations.

Authors: Massimo Giulietti, Daniele Bartoli (Perugia)

Title: Small complete caps and saturating sets in Galois spaces I-II

Summary:

Galois spaces are well known to be rich of nice geometric, combinatorial and group theoretic properties that have also found wide and relevant applications in more practical areas, notably Coding Theory and Cryptography. Typical objects linked to linear codes are plane arcs and their generalizations, especially caps, saturating sets and arcs in higher dimensions, whose code theoretic counterparts are distinguished types of error-correcting and covering linear codes, such as MDS codes. Their investigation has received a great stimulus from Coding Theory, especially in the last decades.

An important issue in this context is to ask for explicit constructions of small complete caps and saturating sets. A *cap* in a Galois space is a set of points no three of which are collinear. A *saturating set* is a set of points whose secants (lines through at least two points of the set) cover the whole space. A cap is *complete* if it is also a saturating set. From these geometric objects there arise linear codes which turn out to have very good covering properties, provided that the size of the set is small with respect to the dimension N and the order q of the ambient space.

The aim of these talks is to provide a survey on the state of the art of the research on small complete caps and saturating sets, with particular emphasis on recent developments. In the last decade a number of new results have appeared, and new notions have emerged as powerful tools in dealing with the covering problem, including bicovering arcs, translation caps, and (m)-saturating sets. Also, although caps and saturating sets are rather combinatorial objects, constructions and proofs sometimes heavily rely on concepts and results from Algebraic Geometry in positive characteristic.

In the first talk we explain the close relationship between linear codes with covering radius 2 and caps and saturating sets in Galois spaces. We also deal with caps and saturating sets in the plane. A cap in a Galois plane is often called a *plane arc*. The theory of plane arcs is well developed and quite rich of constructions; however, we decided to focus on plane arcs arising from cubic plane curves, which will be relevant for some recursive constructions of small complete caps. For arcs contained in elliptic curves, a new description relying on the properties of the Tate-Lichtenbaum pairing is given. Also, a construction by Szőnyi of complete arcs contained in cuspidal cubics is generalized.

In the second talk we deal with the 3-dimensional case. The even order case

was substantially settled by Segre in 1959, whereas the problem of constructing complete caps of size close to the trivial lower bound is still wide open for odd q's. Here we describe how a construction by Pellegrino çan give rise to very small complete caps in the odd order case. We also present in more detail the notion of a multiple covering of the farthest-off points, and relate it to that of an (m)-saturating set.

In both talks we deal with inductive methods. In particular, we discuss under what conditions the product construction and the blowing-up construction preserve the completeness of a cap. Then the notions of a translation cap in the even order case, and that of a bicovering arc in the odd order case, come into play as powerful tools to construct small complete caps in higher dimensions. Davydov's recursive construction of saturating sets is also described.

Author: Tamás Héger (Budapest)

Coauthor: Marcella Takáts

Title: Semi-resolving sets for $\mathrm{PG}(2, q)$

Summary:

Let $G = (A, B; E)$ be a bipartite graph. A subset $S = \{s_1, \ldots, s_k\} \subset A$ is a *semi-resolving set for* G, if the ordered distance lists $(d(b, s_1), \ldots, d(b, s_k))$ are different for all $b \in B$.

In the talk we consider semi-resolving sets for the incidence graphs of Desarguesian projective planes. In this setting, a semi-resolving set is a point-set $\mathcal{S}$ such that every line has a unique intersection with $\mathcal{S}$. Let $\mu_S(\mathrm{PG}(2, q))$ denote the size of the smallest semi-resolving set in $\mathrm{PG}(2, q)$, and let $\tau_2(q)$ be the size of the smallest double blocking set in $\mathrm{PG}(2, q)$.

We show that $\mu_S(\mathrm{PG}(2, q)) \leq \tau_2(q) - 1$, and if there is a double blocking set of size $\tau_2(q)$ that is the union of two disjoint blocking sets (e.g., if $q \geq 9$ is a square), then $\mu_S(\mathrm{PG}(2, q)) \leq \tau_2(q) - 2$. In the talk we prove the following.

Theorem. *Let $\mathcal{S}$ be a semi-resolving set for* $\mathrm{PG}(2, q)$*,* $q \geq 4$*. If* $|\mathcal{S}| < 9q/4 - 3$*, then one can add at most two points to $\mathcal{S}$ to obtain a double blocking set; thus* $|\mathcal{S}| \geq \tau_2(q) - 2$*.*

As a corollary we obtain a lower bound on the size of a blocking semioval. In the proof we use Rédei polynomials and the Szőnyi–Weiner Lemma.

Author: György Kiss (Budapest)

Title: Semiovals and semiarcs

Summary:

Ovals, k-arcs and semiovals of finite projective planes are not only interesting geometric structures, but they have important applications to coding theory and cryptography, too. Semiarcs are the natural generalizations of arcs. Let Π_q be a projective plane of order q. A non-empty pointset $\mathcal{S}_t \subset \Pi_q$ is called a *t-semiarc* if for every point $P \in \mathcal{S}_t$ there exist exactly t lines $\ell_1, \ell_2, \ldots \ell_t$ such that $\mathcal{S}_t \cap \ell_i = \{P\}$ for $i = 1, 2, \ldots, t$. These lines are called the tangents to $\mathcal{S}_t$ at P. The classical examples of semiarcs are the semiovals $(t = 1)$ and the subplanes $(t = q - m$, where m is the order of the subplane.)

In this talk we survey the known results about semiarcs and present some open problems, too.

Author: Gábor Korchmáros (Potenza)

Title: Intersection of an Oval and a Unital in a finite desarguesian plane

Summary:

A general problem in finite geometry is to determine the possible intersections of two geometric objects. In this talk we deal with the case where the geometric objects are a conic and a unital in a finite desarguesian plane. We give a complete classification of their intersection. Our proof uses some results on algebraic curves defined over a finite field.

Author: József Kozma (Szeged)

Title: Regular Polygons – The transformation approach

Summary:

Basic facts about regular polygons, and the notion of regularity, are well known since the beginning of 70's of last century. Starting with the theorem about a spatial regular pentagon being planar (Van der Waerden, 1970), a whole theory has been built up, mainly in the n-dimensional Euclidean space. Total regularity implies a nice behaviour of the k-gon, depending on the parity of k. Via different models and techniques, similar theorems on properties and classifications were discovered, then rediscovered independently. The very elementary geometric question whether a regular $(n+1)$-gon spans the n-dimensional space, and under what conditions, drew the attention of geometers again and again during last four decades. The same theorems were discovered several times independently, in different interpretations. In an early article, Gabor Korchmaros used geometric transformations to solve the problem completely in three-dimensional spaces. The method is of absolute character, so the result is valid not only in Euclidean space but in absolute geometry, as well. Our efforts for generalizing these results for higher dimensional spaces, lead to some results, already known, however the transformation technics would help us to understand and retrieve the deeper geometric relations.

Author: Valentino Lanzone (Potenza)

Title: Search algorithms in the Hughes plane of order 25

Summary:

We investigate transitive arcs in the Hughes plane π of order 25 using the structure of the collineation group of π. We prove that the only ovals in π which are preserved by a non-trivial collineation group of order at least 4 are the Room ovals that Biliotti and Korchmáros obtained by extending a conic of the Desarguesian subplane π_0 of π to an oval of π.

Author: Francesco Mazzocca (Napoli)

Coauthors: A. Blokhuis, G. Marino

Title: Generalized Hyperfocused Arcs in $PG(2, p)$

Summary:

Let $PG(2, q)$ be the projective plane over F_q, the finite field with q elements. A $k-$arc in $PG(2, q)$ is a set of k points with no 3 on a line. A line containing 1 or 2 points of a $k-$arc is said to be a tangent or secant to the $k-$arc, respectively.

A *blocking set* of a family of lines $\mathcal{F}$ is a point-set $\mathcal{B} \subset PG(2, q)$ having non-empty intersection with each line in $\mathcal{F}$. If this is the case, we also say that the lines in $\mathcal{F}$ are *blocked* by $\mathcal{B}$.

A *generalized hyperfocused arc* $\mathcal{H}$ in $PG(2, q)$ is a k-arc with the property that the $k(k-1)/2$ secants can be blocked by a set $\mathcal{B}$ of $k-1$ points not belonging to the arc. Points of the arc $\mathcal{H}$ will be called *white points* and points of the blocking set $\mathcal{B}$ *black*. In case $k > 1$, since every secant to the arc contains a unique black point, the $k-1$ black points induce a factorization, i.e. a partition into matchings, of the white k-arc and k is forced to be even. For $k = 2$, we only have a trivial example: $\mathcal{B}$ consists of a unique point out of $\mathcal{H}$ on the line through the two points of $\mathcal{H}$.

An non trivial example of generalized hyperfocused arc is any 4-arc of white points with its three black diagonal points and **our main result is that this is the only non trivial example, provided q is an odd prime**.

For q even, there are many examples with all black points on a line; in this case $\mathcal{H}$ is simply called a *hyperfocused arc.* As a consequence of the main result of [3], hyperfocused arcs only exist if q is even. When q is even, a nice result is that generalized hyperfocused arcs contained in a conic are hyperfocused [1]; moreover it is known that there exist examples of generalized hyperfocused arcs which are not hyperfocused [6]. However, although much more is known about hyperfocused arcs, there are still many open problems concerning them [1, 5, 6].

The study of these arcs is motivated by a relevant application to cryptography in connection with constructions of efficient secret sharing schemes [7, 8]. Interestingly, our problem is also related to the (strong) cylinder conjecture [2].

References:

[1] Aguglia A., Korchmáros G., & Siciliano A.: *Minimal covering of all chords of a conic in $PG(2, q)$, q even,* Bulletin of the Belgian Mathematical Society - Simon Stevin, Vol. 12 No.5 (2006), pp.651–655.

[2] Ball S.: *The polynomial method in Galois geometries,* in Current research topics in Galois geometry, Chapter 5, Nova Sci. Publ., New York, (2012) 105–130.

[3] Bichara A. & Korchmáros G.: *Note on $(q + 2)-$sets in a Galois plane of order q.* Combinatorial and Geometric Structures and Their Applications (Trento, 1980). Annals of Discrete Mathematics, Vol.14 (1982), pp.117–121. North-Holland, Amsterdam.

[4] Blokhuis A., Korchmáros G. & Mazzocca F.: *On the structure of 3-nets embedded in a projective plane,* Journal of Combinatorial Theory, Series A; 0097-3165; ; Vol.118 (2011); pp. 1228-1238.

[5] Cherowitzo W.E. & Holder L.D.: *Hyperfocused Arcs,* Bulletin of the Belgian Mathematical Society - Simon Stevin, Vol.12 No.5 (2005), pp. 685–696.

[6] Giulietti M. & Montanucci E.: *On hyperfocused arcs in $PG(2, q)$,* Discr. Math., Vol. 306 No.24 (2006), pp. 3307–3314.

[7] Holder L.D.: *The construction of Geometric Threshold Schemes with Projective Geometry,* Master's Thesis, University of Colorado at Denver, 1997.

[8] Simmons G.: *Sharply Focused Sets of Lines on a Conic in $PG(2, q)$,* Congr. Numer., Vol. 73 (1990), pp. 181–204.

Author: Gábor P. Nagy (Szeged)

Coauthors: G. Korchmáros, N. Pace

Title: Projective realization of finite groups

Summary:

Let G be a (finite) group and $\mathcal{P}$ the set of points of a projective plane over the field K. Assume that $\mathrm{char}(K) > |G|$. We say that the disjoint subsets $\Lambda_1, \Lambda_2, \Lambda_3$ of $\mathcal{P}$ *realize* G if there are bijections $\alpha_i : G \to \Lambda_i$ such that for all $g_1, g_2, g_3 \in G$, the points $\alpha_1(g_1)$, $\alpha_2(g_2)$, $\alpha_3(g_3)$ are collinear if and only if $g_1 g_2 = g_3$. The triple $(\Lambda_1, \Lambda_2, \Lambda_3)$ is said to form a *dual* 3*-net* with *fibers* Λ_i.

We describe some constructions: triangular, conic-line type, algebraic, and tetrahedron type. All but the last one are contained in a (possible reducible) cubic curve. The main result is the following.

Theorem (Korchmáros, Nagy, Pace 2012)**.** *Let* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *be a dual* 3*-net of order* $n \geq 4$ *in the projective plane* $PG(2, K)$ *which realizes a group* G*. Then one of the following holds.*

(I) *G is either cyclic or the direct product of two cyclic groups, and* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *is algebraic.*

(II) *G is dihedral and* $(\Lambda_1, \Lambda_2, \Lambda_3)$ *is of tetrahedron type.*

(III) *G is the quaternion group of order* 8*.*

(IV) *G has order* 12 *and is isomorphic to* Alt_4*.*

(V) *G has order* 24 *and is isomorphic to* Sym_4*.*

(VI) *G has order* 60 *and is isomorphic to* Alt_5*.*

Computer calculations show that Alt_4 has no projective realization. This implies that the cases (IV)-(VI) cannot actually occur.

In my talk I focus on one important aspect of the proof, namely, on the situation when the two dual 3-nets of algebraic type share a fiber.

Author: Vito Napolitano (Napoli)

Title: k-sets of P$G(3,q)$ with two intersection numbers with respect to planes

Summary:

Let $\mathcal{K}$ be a set of points of $\mathbb{P} = \mathrm{P}G(d,q)$, $d \geq 2$, $\mathcal{P}_h$ be the family of all h-dimensional subspaces of $\mathbb{P}$ and let $0 \leq m_1 < \cdot < m_s$ be an increasing finite series of non negative integers. A k–subset $\mathcal{K}$ of $\mathbb{P}$ is of *type* $(m_1, \ldots, m_s)_h$ if:

(i) $|\mathcal{K} \cap \pi| \in \{m_1, \ldots, m_s\}$ *for every subspace* $\pi \in \mathcal{P}_h$,

(ii) *For every* m_j, $j = 1, \ldots, s$ *there is at least one subspace* $\pi \in \mathcal{P}_h$ *such that* $|\mathcal{K} \cap \pi| = m_j$.

In the talk, k-sets of P$G(3,q)$ with two intersection number, say m and n, with respect to planes will be considered.

A lower bound for the size of such sets for $m \leq q+1$ and some characterizations in the minimal size case will be showed. Also, sets of type $(3,n)_2$ will be studied. Finally a characterization of a non singular Hermitian variety of P$G(3,q^2)$ via its intersection numbers with respect to lines and planes will be presented.

Author: Francesco Pavese (Potenza)

Title: Hyperovals on Hermitian Generalized Quadrangles

Summary:

The first part of the talk is about the intersection between an elliptic quadric $Q^{-}(3,q^2)$ and an Hermitian surface $H(3,q^2)$ in $PG(3,q^2)$, q even, such that the tangent lines with respect to $Q^{-}(3,q^2)$ that are generators of $H(3,q^2)$, are extended lines of a symplectic space $W(3,q)$ lying in a subgeometry. In this setting we determine a new hyperoval on $H(3,q^2)$.

Author: Alessandro Siciliano (Potenza)

Title: Translation ovoids of finite classical polar spaces

Summary:

A *classical polar space* $\mathcal{P}$ is the set of all subspaces of a projective space which are totally isotropic with respect to a reflexive sesquilinear form. When the projective space is finite then the polar space is called *finite*.

The *generators* of $\mathcal{P}$ are the subspaces of maximal dimension contained in it.

An *ovoid* of $\mathcal{P}$ is a set of points of $\mathcal{P}$ which meets every generator in a point. An ovoid $\mathcal{O}$ of $\mathcal{P}$ is a *translation ovoid* with respect to a point P of $\mathcal{O}$ if there is a collineation group of $\mathcal{P}$ fixing all totally isotropic lines through P and acting regularly on points of the ovoid different from P. Such a group is called the *translation group (about P)* of $\mathcal{O}$. A translation ovoid $\mathcal{O}$ is said to be *semilinear* if it has a translation group containing non-linear collineations; we call $\mathcal{O}$ *linear* otherwise.

Translation ovoids of finite orthogonal polar spaces have been intensively studied by many authors. Examples of translation ovoids of $Q^+(3, q)$ are non-degenerate conics contained in it. Translation ovoids of $Q(4, q)$ correspond to semifield flocks of the quadratic cone in $\mathrm{PG}(3, q)$ and it is known there exist three infinite families and one sporadic example. Translation ovoids of $Q^+(5, q)$ correspond to semifield spreads of $\mathrm{PG}(3, q)$ and they exists for all values of q.

The understanding of translation ovoids of finite unitary polar spaces is not as deep as that of translation ovoids of orthogonal spaces. Examples of translation ovoids of $H(3, q^2)$ are non-degenerate hermitian curves contained in it. Several other infinite families of translation ovoids of $H(3, q^2)$ are known. The intimate connection between linear translation ovoids of $H(3, q^2)$ and semifield spreads of $\mathrm{PG}(3, q)$ was highlighted by many authors.

In this talk we present results on the existence of translation ovoids of the unitary polar space $H(2m - 1, q^2)$, $m \geq 3$. We also give informations on semilinear translation ovoids of $H(3, q^2)$.

The results are based on a recent joint work with Oliver H. King from Newcastle University.

Author: Angelo Sonnino (Potenza)

Title: Hughes planes and their collineation groups

Summary:

We describe the construction of the Hughes plane π based on a nearfield R of order q^2, with q an odd prime power, whose centre is isomorphic to the finite field $\mathrm{GF}(q)$. Then, we show that the full collineation group of π, say Σ, can be obtained by extending to π the action of all collineations of its Desarguesian subplane π_0, and taking into account the other collineations induced on π by the automorphisms of the nearfield R. That is, $\Sigma = GK$ with $G = \mathrm{P}\Gamma L(3,q)$ and $K = \mathrm{Aut}(R)$. One has $\Sigma = G \times K$ if and only if q is a prime, and in this case each collineation of G commutes with each collineation of K. When $q^2 = 9$, $|\Sigma| = 5616 \cdot 6 = 33{,}696$, whereas for $q^2 = p^{2m} \neq 9$, $|\Sigma| = 2mq^3(q^2{+}q{+}1)(q{-}1)^2(q{+}1)$. Hence, $|\Sigma| = 2\,|\mathrm{P\Gamma L}(3,q)|$; in particular, if $q^2 = 25$, then $|\Sigma| = 2 \cdot 31 \cdot 30 \cdot 25 \cdot 16 = 744{,}000$. Finally, Σ has two orbits on π; namely, π_0 and $\pi \setminus \pi_0$.

Author: Tamás Szőnyi (Budapest)

Title: Lacunary polynomials and finite geometry

Summary:

Fully reducible lacunary polynomials over finite fields were introduced by László Rédei in [2, 3]. He applied them to several problems: directions determined by a set of q points in a Desarguesian affine plane, factorizations of abelian groups, automorphisms of the Paley-graph, sums of roots of unity. An elementary proof of some results of Rédei for $q = p$ prime was given by Lovász and Schrijver [1]. In this talk we briefly survey the main theorems of Rédei's book and the Lovász-Schrijver paper. More recent applications of fully reducible lacunary polynomials in finite geometry will also be mentioned. Some of the results from the nineties can be found in [4].

References:

[1] L. Lovász, A. Schrijver, Remarks on a theorem of Rédei, *Studia Scient. Math. Hungar.* **16** (1981), 449-454.

[2] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser, Basel, 1970.

[3] L. Rédei, *Lacunary polynomials over finite fields*, Akadémiai Kiadó, Budapest, and North-Holland, Amsterdam, 1973

[4] T. Szőnyi, Around Rédei's theorem, *Discrete Math.* **208/209** (1999), 557-575.

Author: Marcella Takáts (Budapest)

Coauthor: Tamás Héger

Title: Resolving sets in finite projective planes

Summary:

In a graph $\Gamma = (V, E)$ a vertex v is *resolved* by a vertex-set $S = \{v_1, \ldots, v_n\}$ if its (ordered) distance list with respect to S, $(d(v, v_1), \ldots, d(v, v_n))$, is unique. A set $A \subset V$ is resolved by S if all its elements are resolved by S. S is a *resolving set* in Γ if it resolves V. The *metric dimension of* Γ is the size of the smallest resolving set in it. In a bipartite graph a *semi-resolving set* is a set of vertices in one of the vertex classes that resolves the other class.

We examine resolving sets of the incidence graphs of finite projective planes. The following theorem holds:

Theorem. *The metric dimension of any projective plane of order $q \geq 23$ is $4q - 4$.*

In the talk we sketch the proof of the above theorem and describe all resolving sets of that size.