Eötvös Loránd University
Institute of Mathematics

Summary of the Ph.D. thesis

Directions and other topics in Galois-geometries

Marcella Takáts

Doctoral School: Mathematics
Director: Miklós Laczkovich
Professor, Member of the Hungarian Academy of Sciences

Doctoral Program: Pure Mathematics
Director: András Szűcs
Professor, Corresp. Member of the Hungarian Academy of Sciences

Supervisor: Péter Sziklai, D.Sc.
Associate Professor

Department of Computer Science
Institute of Mathematics
Eötvös Loránd University

2014

Introduction

In the thesis we study geometries over finite fields (Galois-geometries), and "geometry style" properties of finite fields.

The two main ways of finite geometrical investigations are the combinatorial and the algebraic one. In both cases we define a point set by a combinatorial property, e.g. by its intersection numbers with certain subspaces. In the first method we examine the set using combinatorial and geometrical tools; the other way is the algebraic one. The connection between algebra and finite geometry is said to be classical (e.g. Mathieu-groups – Witt-designs). We take a point set in a geometry over a finite field and translate its "nice" combinatorial property to a "nice" algebraic structure. In the thesis we mainly use the so-called polynomial method, created by Blokhuis and Szőnyi and developed by many others: we assign a polynomial over a finite field to the point set, examine it with various tools, then we translate the algebraic information we get back to the original, geometrical language.

There are examples for both ways in the thesis. In the first three chapters we demonstrate algebraic methods, in the last three chapters we do combinatorial investigations.

Stability and extendability questions also arise: we consider structures with a given property and take an extremal one among them (e.g. the largest one), then we show that a structure close to it (in the sense of size) can be achieved only from the extremal one (by deleting some of its points).

The main part of the thesis (Chapters 2, 3 and 4) is related to the so-called *direction problem*. The problem, which was suggested by Rédei, has many non-geometrical applications. Consider a point set U in the affine space over the field $\mathrm{GF}(q)$. We say a *direction* d is *determined* by the set if there is an affine line with the ideal point d containing at least two points of the set. The investigated questions are the *number* of determined directions, and the *size* and the *structure* of sets with few determined directions.

Notation. Throughout the summary, let p be a prime, $q = p^h$ be a prime power, and let $\mathrm{GF}(q)$ be a finite field of q elements. We denote the elements of a field by lower case letters, while variables in an expression are denoted by capital letters. Π_n refers to a (combinatorially defined) projective plane of order n, and let $\mathrm{PG}(n,q)$ denote the projective space of dimension n over $\mathrm{GF}(q)$. We associate a point of the projective space with a homogeneous $(n+1)$-tuple in brackets, so $(x_0, x_1, \ldots, x_n)$, $x_i \in \mathrm{GF}(q)$ refers to a point; an $(n+1)$-tuple in square brackets, $[y_0, y_1, \ldots, y_n]$, $y_i \in \mathrm{GF}(q)$, refers to a hyperplane. A point is incident with a given hyperplane if and only if their scalar product $x_0y_0 + x_1y_1 + \cdots + x_ny_n$ is equal to zero. Let $\mathrm{AG}(n,q)$ denote the affine space of dimension n over $\mathrm{GF}(q)$ that corresponds to the co-ordinate space $\mathrm{GF}(q)^n$ of rank n over $\mathrm{GF}(q)$. We can embed $\mathrm{AG}(n,q)$ into $\mathrm{PG}(n,q)$ in the usual way: $\mathrm{PG}(n,q) = \mathrm{AG}(n,q) \cup H_\infty$, where H_∞ is called the *hyperplane at infinity* or the *ideal hyperplane*,

its points are called *ideal points* or *directions*.

The Rédei-polynomial. Our main tool in the algebraic methods is the careful investigation of a polynomial assigned to the point set. Let $U = \{(1, a_{i1}, a_{i2}, \ldots, a_{in}) : i = 1, ..., m\} \subset \mathrm{AG}(n, q) \subset \mathrm{PG}(n, q)$ be a point set. The *Rédei-polynomial* of U is defined as follows:

$$R(X_0, X_1, X_2, ..., X_n) = \prod_{i=1}^{m} (X_0 + a_{i1}X_1 + a_{i2}X_2 + \cdots + a_{in}X_n).$$

This is clearly a totally reducible polynomial, where each linear factor corresponds to a point of U. We substitute the *hyperplanes* of $\mathrm{PG}(n, q)$ into the polynomial. If a linear factor is equal to zero when we substitute the hyperplane $[x_0, x_1, \ldots, x_n]$, then this hyperplane contains the point that corresponds to the vanishing linear factor. R can be considered as a hypersurface in the dual space, the points of R correspond to such hyperplanes of the original space that intersect the point set. The hyperplane $[x_0, x_1, \ldots, x_n]$ contains exactly k points of U (and so it is a root of the polynomial $R(X_0, X_1, X_2, \ldots, X_n)$ with multiplicity k) if and only if in the dual space $(x_0, x_1, \ldots, x_n)$ is a point of the surface R with multiplicity k. So the Rédei-polynomial contains the intersection properties of the set U with hyperplanes and translates them into algebraic properties. One may investigate the polynomial or the hypersurface defined by R in the dual space.

The direction problem. Consider a point set $U \subset \mathrm{AG}(n, q)$, let D denote the set of directions determined by U. The original problem - due to Rédei - was stated for directions determined by the graph of a function in the plane over $\mathrm{GF}(q)$. Then $|U| = q$, and $\infty \notin D$, the "vertical" direction, i. e. the ideal point of the vertical lines is a *non-determined direction*.

The investigated questions are the number of determined directions and the characterization of the "interesting" point sets. Here "interesting" means that there are only few determined directions. Note that in the n-dimensional space if $|U| > q^{n-1}$ then every direction is determined. In fact, already a random point set of size much less than q^{n-1} determines all the directions. In case of a set of size q^{n-1} we are interested in the number of determined directions and the structure of the set if there are few determined directions. The examination of smaller sets leads to stability questions as well: can we extend such a set to a set of maximal size determining the same directions only.

Sets of maximal size in the plane over $\mathrm{GF}(q)$, i. e. sets of cardinality q are the most studied ones. Rédei and Megyesi proved in [10] that in the plane of p prime order if the points are not collinear then a set of size p determines at least $\frac{p+3}{2}$ directions, while Lovász and Schrijver showed in [9] that a set with that many determined directions is unique (up to an affine transformation). The case of sets of maximal size in a plane of prime power order was completely characterized by Blokhuis, Ball, Brouwer, Storme and Szőnyi in [8].

Theorem 0.16. [8], [7] *Let $U \subset \mathrm{AG}(2,q)$ be a point set, $|U| = q$. Let $s = p^e$ be the largest power of p such that each secant meets U in a multiple of s points. Then one of the following holds:*
(i) $s = 1$ and $\frac{q+3}{2} \leq |D| \leq q+1$;
(ii) $\mathrm{GF}(s)$ is a subfield of $\mathrm{GF}(q)$ and $\frac{q}{s}+1 \leq |D| \leq \frac{q-1}{s-1}$;
(iii) $s = q$ and $|D| = 1$.
If $s \geq 3$ then U is $\mathrm{GF}(s)$-linear.

1 Vandermonde sets and super-Vandermonde sets

In Chapter 1 we describe a problem which seems to be purely algebraic, Vandermonde sets and super-Vandermonde sets [1]. Beyond the algebraic motivation they are also interesting from the finite geometrical point of view.

Let $S = \{x_1, ..., x_n\} \subseteq \mathrm{GF}(q)$ be a subset. The *k-th power sum* of the elements of S is $\pi_k(x_1, ..., x_n) = \sum_{i=1}^{n} x_i^k$. Let $w = w_S$ be the smallest positive integer k such that $\pi_k \neq 0$ if such a k exists, otherwise $w = \infty$.

Definition 1.4. *Let $1 < t < q$. We say that $T = \{y_1, ..., y_t\} \subseteq \mathrm{GF}(q)$ is a Vandermonde set, if $\pi_k = \sum_i y_i^k = 0$ for all $1 \leq k \leq t-2$.*

In other words, the Vandermonde property is equivalent to $w_T \geq t-1$. If $p \mid t$, then a t-set cannot have more than $t-2$ zero power sums, so $w_T \leq t-1$, it follows from the fact that a Vandermonde determinant of distinct elements cannot be zero. So in this sense Vandermonde sets are extremal with $w = t-1$, and the name "Vandermonde" comes from here. In general a t-set cannot have more than $t-1$ zero power sums (so for a Vandermonde set $w_T = t-1$ or t holds). This consideration leads to the following definition.

Definition 1.5. *Let $1 < t < q$. We say that $T = \{y_1, ..., y_t\} \subseteq \mathrm{GF}(q)$ is a super-Vandermonde set, if $\pi_k = \sum_i y_i^k = 0$ for all $1 \leq k \leq t-1$.*

So the super-Vandermonde property is equivalent to $w_T = t$, and the argument above shows that such a set exists only if $p \nmid t$ holds. The power sums do not change if the zero element is added to (or possibly removed from) T, but the cardinality changes hence its "Vandermondeness" is weakened (or strengthened); by this process one gets a Vandermonde set from a super-Vandermonde set (and vice versa). The zero element is never contained in a super-Vandermonde set.

If T is a Vandermonde set and its size is divisible by the characteristic, then for any $a \in T$, the translate $T-a$ is a Vandermonde set, containing the zero element. Any additive subgroup of $\mathrm{GF}(q)$ is a Vandermonde set, and any multiplicative subgroup of $\mathrm{GF}(q)$ is a super-Vandermonde

set. There also exist finite geometrical examples: many interesting point sets can be translated to Vandermonde sets in a natural way.

The aim of this chapter is to describe certain super-Vandermonde sets. We show that a super-Vandermonde set is equivalent to a fully reducible polynomial of the form $f(Y) = Y^t + g^p(Y)$, $t > p \cdot \deg g$. For example, if $q = p$ is a prime then the only possibility is $f(Y) = Y^t + c$, i.e. the set is a transform of the multiplicative group $\{y : y^t = 1\}$, if it exists (so iff $t \mid q-1$).

Our main result here is the characterization of small and large super-Vandermonde sets. What does "small" and "large" mean? We know that by removing the zero element from an additive subgroup of GF(q) one gets a super-Vandermonde set. The smallest and largest non-trivial additive subgroups are of cardinality p and q/p, respectively. This motivates that, for our purposes small and large will mean "of size $< p$" and "of size $> q/p$", resp. Note that the super-Vandermonde set, derived from an additive subgroup of size p, is a transform of a multiplicative subgroup. This does not hold for the super-Vandermonde set got from an additive subgroup of size q/p. We have already mentioned that there exist examples derived from interesting point sets. In fact, between the sizes p and q/p there are so many geometrical examples of different structures as the complete characterization of them seems to be hopeless. Thus we restrict ourselves to examine "small" and "large" super-Vandermonde sets.

Theorem 1.12. *Suppose that $T \subset$ GF(q) is a super-Vandermonde set of size $|T| < p$. Then T is a (transform of a) multiplicative subgroup.*

Theorem 1.13. *Suppose that $T \subset$ GF(q) is a super-Vandermonde set of size $|T| > q/p$. Then T is a (transform of a) multiplicative subgroup.*

Note that we classified the case $q = p^2$: then a super-Vandermonde set of $GF(q)$ is (a coset of) a multiplicative subgroup.

2 Small point sets

In Chapters 2, 3 and 4 we investigate questions concerning the direction problem. In Chapters 2 and 3 we use algebraic tools, namely the polynomial method based on the careful examination of the Rédei-polynomial.

Chapter 2 is based on a joint work with Szabolcs Fancsali and Péter Sziklai. As these results have already appeared in [3] and also in the Ph.D. thesis of Szabolcs Fancsali, here we just give a short summary of the topic; the method and the results. Nevertheless, I did not want to miss it out totally, as it fits into the main topic of the current thesis. For the detailed description see the two works mentioned above.

We have seen that the case of maximal point sets (i. e. of size q) in the plane of order q is completely characterized in Theorem 0.16. The classification of sets of size less than q is

open. Szőnyi's Theorem 0.17 describes the case $q = p$ prime. Here we study the case $q = p^h$ prime power, and give some partial results on the number of determined directions by less than q points.

Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$ be a point set, $|U| < q$. Recall the parameter s appearing in Theorem 0.16: s denotes the greatest power of p such that each line ℓ of a determined direction meets U in 0 modulo s points.

During the examination of the Rédei-polynomial of the set U we define a parameter t (where $s \leq t$), which is somehow an analogue of the parameter s; it will be essential in order to reach the bounds on the number of determined directions.

The main result here is the following analogue of Theorem 0.16.

Theorem 2.14. *Let $U \subset \mathrm{AG}(2,q)$ be an arbitrary set of points and let D denote the directions determined by U. We use the notation s and t defined above. Suppose that $\infty \in D$. One of the following holds:*
(i) $1 = s \leq t < q$ *and* $\dfrac{|U|-1}{t+1} + 2 \leq |D| \leq q+1$;
(ii) $1 < s \leq t < q$ *and* $\dfrac{|U|-1}{t+1} + 2 \leq |D| \leq \dfrac{|U|-1}{s-1}$;
(iii) $1 \leq s \leq t = q$ *and* $D = \{\infty\}$.

In the special case $q = p$ prime we get back the result of Szőnyi, which was mentioned earlier. If $q > p$ the value of this result is decreased by the fact that t was defined in an algebraic way, and its geometrical meaning is not yet clear.

3 Large point sets

In Chapter 3 we study a stability question [4]. Given a point set of size less than q^{n-1} in the n-dimensional affine space, the question is whether we can add some points to it to reach a set of maximal size (i. e. of cardinality q^{n-1}) such that the set of determined directions remains the same.

Earlier results (the strongest ones are known in the case $n = 2$) contain restrictions on the size of the affine point set or on the size of the set of determined directions.

The main result of the chapter is a new method we use in order to tackle the old problem. Instead of investigating the number of non-determined directions, we examine the structure of the set of non-determined directions.

Let $U = \{(1, a_1^i, a_2^i, a_3^i, \ldots, a_n^i) : i = 1, ..., q^{n-1} - \varepsilon\}$ be a subset. The Rédei-polynomial of U is: $R(X_0, X_1, X_2, ..., X_n) = \prod_{i=1}^{q^{n-1}-\varepsilon}(X_0 + a_1^i X_1 + a_2^i X_2 + ... + a_n^i X_n)$. With the help of this we define a polynomial $f(X_0, X_1, \ldots, X_n)$ of degree ε, which describes the deficiency of the set, i. e. its difference from the maximal cardinality. In order to reach the results we examine this

polynomial. The equation $f = 0$ defines an algebraic hypersurface in the dual space $\mathrm{PG}(n, q)$. If the polynomial splits completely into linear factors then in the dual space the surface $f = 0$ is a union of ε hyperplanes. These hyperplanes correspond to exactly ε points in the original space, and by adding these points to the set we reach the maximal size.

An undetermined direction refers to a hyperplane in the dual space such that the intersection of the hyperplane and the surface $f = 0$ is *totally reducible*, i. e. it splits into $(n-2)$-dimensional subspaces. (We call such a hyperplane a TRI hyperplane, where the abbreviation TRI stands for Totally Reducible Intersection.) Thus, if the surface is not totally reducible then the non-determined directions have a very restricted (strong) structure.

We have an extendability result in general dimension for $\varepsilon = 2$.

Theorem 3.10. *Let $n \geq 3$. Let $U \subset \mathrm{AG}(n, q) \subset \mathrm{PG}(n, q)$, $|U| = q^{n-1} - 2$. Let $D \subseteq H_\infty$ be the set of directions determined by U and put $N = H_\infty \setminus D$ the set of non-determined directions. Then U can be extended to a set $\bar{U} \supseteq U$, $|\bar{U}| = q^{n-1}$ determining the same directions only, or the points of N are collinear and $|N| \leq \lfloor \frac{q+3}{2} \rfloor$, or the points of N are on a (planar) conic curve.*

We show a general stability theorem in the 3-space if $\varepsilon < p$.

Theorem 3.11. *Let $U \subset \mathrm{AG}(3, q) \subset \mathrm{PG}(3, q)$, $|U| = q^2 - \varepsilon$, where $\varepsilon < p$. Let $D \subseteq H_\infty$ be the set of directions determined by U and put $N = H_\infty \setminus D$ the set of non-determined directions. Then N is contained in a plane curve of degree $\varepsilon^4 - 2\varepsilon^3 + \varepsilon$ or U can be extended to a set $\bar{U} \supseteq U$, $|\bar{U}| = q^2$.*

We consider the case when U is extendable as the typical one, otherwise the non-determined directions are contained in a (planar) curve of low degree. Although note that there exist examples of maximal point sets of size $q^2 - 2$, $q \in \{3, 5, 7, 11\}$, not determining the points of a conic at infinity.

To reach the total strength of this theory, we would like to use an argument stating that it is a "very rare" situation that the intersection of a hyperplane and the surface is totally reducible - this difficult problem seems to be interesting for its own sake, and it is already unsolved.

Conjecture 3.12. *Let $f(X_0, X_1, ..., X_n)$ be a homogeneous irreducible polynomial of degree $d > 2$ and let F be the hypersurface in $\mathrm{PG}(n, q)$ determined by $f = 0$. Then the number of TRI hyperplanes to F is "small" or F is a cone with a low dimensional base.*

The proof of the conjecture would imply extendability of direction sets under very general conditions.

Finally we describe an application of the result in the theory of ovoids.

Corollary 3.17. *Let $\mathcal{B}$ be a partial ovoid of size $q^2 - 2$ of the partial geometry $T_2^*(\mathcal{K})$, then $\mathcal{B}$ is always extendable to an ovoid.*

4 An extension of the direction problem

In Chapter 4, which is based on [2], to finish this topic we discuss a natural extension of the classical direction problem. Differently from the previous chapters, instead of using algebraic tools, here we make purely geometrical and combinatorial considerations throughout the proofs.

Originally, a direction d (i.e. a point at infinity) was said to be determined by a point set, if there were at least 2 points contained in the set lying on a line which had direction d. In other words, there is a 1-dimensional subspace with ideal point d spanned by 2 points of the set. We extend the definition of *determined direction* in the following way:

Definition 4.1. *Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$ be a point set, and k be a fixed integer, $k \leq n-2$. We say a subspace S_k of dimension k in H_∞ is determined by U if there is an affine subspace T_{k+1} of dimension $k+1$, having S_k as its hyperplane at infinity, containing at least $k+2$ affinely independent points of U (i.e. spanning T_{k+1}).*

The questions here are the analogues of that in the classical problem: that is, for a fixed k we ask for the size of the point set if it does not determine all the k-subspaces of H_∞; and for the structure of U in case of "few" determined subspaces. Note that $|U| \leq q^{n-1}$ if it does not determine all the k-subspaces at infinity. This bound is the same as in the original problem, an "interesting" set contains at most q^{n-1} points. In the thesis we consider point sets of the maximal "interesting" cardinality, i. e. sets of size q^{n-1}.

In **Proposition 4.2** we give a construction for a set with few determined ideal subspaces in arbitrary dimensions: Let $U_0 \subset \mathrm{AG}(m,q) \subset \mathrm{PG}(m,q)$, $|U_0| = q^{m-1}$ such that there are l-subspaces in H_∞ not determined by U_0. We embed U_0 into $\mathrm{AG}(n,q)$, where $n > m$. Consider a subspace V in H_∞ of dimension $n-m-1$, completely disjoint from the original m-dimensional space. We construct a cone (cylinder) with base U_0 and vertex V, and in this way we get a point set U in $\mathrm{AG}(n,q)$, $|U| = q^{n-1}$. Then the ideal subspaces of dimension $n-m+l$ not determined by U are exactly the subspaces spanned by the originally non-determined l-subspaces and V.

As we study determined subspaces (instead of points) of H_∞, we may investigate the relation between determined subspaces of *different* dimensions for a given affine point set. Results on the structure of the set of determined directions in the classical direction problem are already known. From [11] we know that if $|U| = q^{n-1}$ then the set of determined directions is the union of some complete $(n-2)$-dimensional subspaces of H_∞. Analogously, we found that through any determined k-subspace, there exists a determined $(n-2)$-subspace. Between the determined subspaces the following hierarchy holds.

Proposition 4.6. *Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$, $|U| = q^{n-1}$ and k be a fixed integer, $k \leq n-3$. If there is a subspace V_{n-2} of dimension $n-2$, $V_{n-2} \subset H_\infty$ such that all of the k-dimensional subspaces of V_{n-2} are determined by U then V_{n-2} is determined by U as well.*

Our main result here is the complete characterization of point sets of maximal size in 3 dimensions.

Theorem 4.7. *Let $U \subset \mathrm{AG}(3,q) \subset \mathrm{PG}(3,q)$, $|U| = q^2$. Let L be the set of lines in H_∞ determined by U and put N the set of non-determined lines. Then one of the following holds:*
a) $|N| = 0$, *i.e. U determines all the lines of H_∞;*
b) $|N| = 1$ *and then there is a parallel class of affine planes such that U contains one (arbitrary) complete line in each of its planes;*
c) $|N| = 2$ *and then (i) U together with the two undetermined lines in H_∞ form a hyperbolic quadric or (ii) U contains q parallel lines (U is a cylinder);*
d) $|N| \geq 3$ *and then U contains q parallel lines (U is a cylinder).*

It means that if there are "many" (≥ 3) undetermined lines then the point set is somehow "reducible": it must form a cone (cylinder) we have seen in Proposition 4.2. In case of two undetermined lines one other example - the hyperbolic quadric - occured.

Thus we continue to examine quadrics in higher dimensions. Here we found a further example for a point set with relatively many non-determined subspaces. Let $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$, $|U| = q^{n-1}$ be the affine part of a nonsingular quadric which has the ideal hyperplane as a tangent hyperplane (i. e. the intersection of the quadric and the ideal hyperplane is a cone based on an $(n-2)$-dimensional quadric of the same character). Denote by g the projective index of the quadric, i. e. the dimension of the generators, the subspaces of maximum dimension contained in the quadric.

Proposition 4.14. *If $U \subset \mathrm{AG}(n,q) \subset \mathrm{PG}(n,q)$, $|U| = q^{n-1}$ is defined as above then the undetermined g-dimensional subspaces in H_∞ are exactly the generators contained in the intersection of the quadric and the ideal hyperplane, except the cases when $n = 2$ and q is even, or $n = 4$ and $q = 2$, or $n = 5$ and $q = 2$ and the quadric is elliptic.*

5 Resolving sets in finite projective planes

In the last two chapters we show some connections between finite geometries and other fields in combinatorics. In Chapter 5, which is a joint work with Tamás Héger [5], we examine a graph theoretical question due to R. Bailey and P. Cameron. We examine resolving sets of the incidence graph of a finite projective plane. We give the metric dimension of the incidence graph, and classify the smallest resolving sets of it, using combinatorial tools.

Let $\Gamma = (V, E)$ be a simple graph, for $x, y \in V$, $d(x, y)$ denotes the distance of x and y.

Definition 5.1. *$S = \{s_1, \ldots, s_k\} \subset V$ is a* resolving set *in $\Gamma = (V, E)$, if the ordered distance lists $(d(x, s_1), \ldots, d(x, s_k))$ are unique for all $x \in V$. The* metric dimension of Γ, *denoted by $\mu(\Gamma)$, is the size of the smallest resolving set in it.*

Equivalently, S is a resolving set in $\Gamma = (V, E)$ if and only if for all $x, y \in V$, there exists a point $z \in S$ such that $d(x, z) \neq d(y, z)$. In other words, the vertices of Γ can be distinguished by their distances from the elements of a resolving set. We say that a vertex v is *resolved* by S if its distance list with respect to S is unique. A set $A \subset V$ is resolved by S if all its elements are resolved by S. Note that the distance list is ordered, the (multi)set of distances is not sufficient.

Take a projective plane $\Pi = (\mathcal{P}, \mathcal{L})$ of order q, where $\mathcal{P}$ denotes the set of points and $\mathcal{L}$ stands for the set of lines. The incidence graph $\Gamma(\Pi)$ of Π is a bipartite graph with vertex classes $\mathcal{P}$ and $\mathcal{L}$, where $P \in \mathcal{P}$ and $\ell \in \mathcal{L}$ are adjacent in Γ if and only if P and ℓ are incident in Π. By a resolving set or the metric dimension of Π we mean that of its incidence graph.

We prove the following theorem regarding the metric dimension of a finite projective plane.

Theorem 5.2. *The metric dimension of a projective plane of order $q \geq 23$ is $4q - 4$.*

We give the description of all resolving sets of a projective plane Π of size $4q - 4$ ($q \geq 23$).

6 Search problems in vector spaces

The starting point of combinatorial search theory is the following problem: given a set X of n elements out of which one x is marked, what is the minimum number s of queries of the form of subsets $A_1, A_2, \ldots, A_s$ of X such that after getting to know whether x belongs to A_i for all $1 \leq i \leq s$ we are able to determine x. Since decades, the number s is known to be equal to $\lceil \log_2 n \rceil$ no matter if the ith query might depend on the answers to the previous ones (*adaptive search*) or we have to ask our queries at once (*non-adaptive search*).

In the last chapter we address the q-analogue of the basic problem [6]. Let V denote an n-dimensional vector space over GF(q) and let $\mathbf{v}$ be a marked 1-dimensional subspace of V. We will be interested in determining the minimum number of queries that is needed to find $\mathbf{v}$ provided all queries are subspaces of V and the answer to a query U is YES if $\mathbf{v} \leqslant U$ and NO if $\mathbf{v} \not\leqslant U$. This number will be denoted by $A(n, q)$ in the adaptive case and $M(n, q)$ in the non-adaptive case. Note that a set $\mathcal{U}$ of subspaces of V can be used as query set to determine the marked 1-space in a non-adaptive search if and only if for every pair $\mathbf{u}, \mathbf{v}$ of 1-subspaces of V there exists a subspace $U \in \mathcal{U}$ with $\mathbf{u} \leqslant U, \mathbf{v} \not\leqslant U$ or $\mathbf{u} \not\leqslant U, \mathbf{v} \leqslant U$. Such systems of subspaces are called *separating*.

It is easy to show that $A(n, 2) = M(n, 2) = n$ for all $n \geq 2$. Thus we will mainly focus on the case when $q \geq 3$. As usual, the subspaces of an n-dimensional vector space over GF(q) are considered as the elements of the Desarguesian projective geometry PG($n - 1, q$). In the case $n = 3$ we determine $A(3, q)$ for all prime powers q.

Theorem 6.1. *Consider a projective plane Π_q of order q. Let $A(\pi_q)$ denote the minimum number of queries in adaptive search that is needed to determine a point of Π_q provided the queries can be either points or lines of π_q. With this notation we have $A(\Pi_q) \leq 2q-1$; if q is a prime power, then $A(\mathrm{PG}(2,q)) = 2q-1$, that is the equality $A(3,q) = 2q-1$ holds.*

We also address the problem of determining $M(3,q)$. We obtain upper and lower bounds but not the exact value except if $q \geq 121$ is a square. The most important consequence of our results is the following theorem that states that the situation is completely different from that in the classical case where adaptive and non-adaptive search require the same number of queries.

Theorem 6.2. *For $q \geq 9$ the inequality $A(3,q) < M(3,q)$ holds.*

We also address in arbitrary dimensions the general problem of giving upper and lower bounds on $A(n,q)$ and $M(n,q)$. Our main results are the following theorems.

Theorem 6.3. *For any prime power $q \geq 2$ and positive integer n the inequalities $\log_2 \begin{bmatrix} n \\ 1 \end{bmatrix}_q \leq A(n,q) \leq (q-1)(n-1)+1$ hold.*

Theorem 6.4. *There exists an absolute constant $C > 0$ such that for any positive integer n and prime power q the inequalities $\frac{1}{C}q(n-1) \leq M(n,q) \leq 2q(n-1)$ hold. Moreover, if q tends to infinity, then $(1-o(1))q(n-1) \leq M(n,q)$ holds.*

Throughout the proofs we use semi-resolving sets of finite projective planes, which is a variant of resolving sets we mentioned in the previous chapter.

References

[1] P. Sziklai, M. Takáts, Vandermonde sets and super-Vandermonde sets. *Finite Fields Appl.*, **14** (2008), 1056–1067.

[2] P. Sziklai, M. Takáts, An extension of the direction problem. *Discrete Math.*, **312** (2012), 2083–2087.

[3] Sz. L. Fancsali, P. Sziklai, M. Takáts, The number of directions determined by less than q points. *J. Alg. Comb.*, Volume **37**, Issue **1** (2013), 27–37.

[4] J. De Beule, P. Sziklai, M. Takáts, On the structure of the directions not determined by a large affine point set. *J. Alg. Comb.*, Volume **38**, Issue **4** (2013), 888-899.

[5] T. Héger, M. Takáts, Resolving sets and semi-resolving sets in finite projective planes. *Electronic J. of Comb.*, Volume **19**, Issue **4** (2012).

[6] T. Héger, B. Patkós, M. Takáts, Search problems in vector spaces. *Designs, Codes and Cryptography*,(2014), DOI: 10.1007/s10623-014-9941-9.

[7] S. Ball, The number of directions determined by a function over a finite field. *J. Combin. Th. Ser. A*, **104** (2003), 341–350.

[8] A. Blokhuis, S. Ball, A. Brouwer, L. Storme, T. Szőnyi, On the number of slopes determined by a function on a finite field. *J. Comb. Theory Ser. (A)*, **86** (1999), 187–196.

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

[10] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*. Birkhäuser Verlag, Basel (1970). English translation: *Lacunary polynomials over finite fields*. North Holland, Amsterdam (1973).

[11] L. Storme, P. Sziklai, Linear point sets and Rédei type k-blocking sets in PG(n, q). *J. Alg. Comb.*, **14** (2001), 221–228.

[12] P. Sziklai, Polynomials in finite geometry. *Manuscript. Available online at* `http://www.cs.elte.hu/~sziklai/poly.html` (last accessed August 28., 2014.).

[13] T. Szőnyi, A hézagos polinomok Rédei-féle elméletének néhány újabb alkalmazása. *Polygon*, **V.** kötet **2.** szám (1995).