Final report of the research project entitled "Linear Structures and Segre type methods in finite geometry"

Bence Csajbók

1 Introduction

The aim of this project was to study finite geometric problems with algebraic techniques. The project was planned for 3 years, but it had to be closed after 1 year and 7 months because it was not compatible with the principle investigator's new position. During the project we published 5 articles and submitted 2 other manuscripts which are currently under review. Two of the published articles ([11, 12]) were submitted before the starting date of the project, but the revision process was done during the period of this report. The topics of these papers are closely related to the theme of this project. Two papers are joint works with Hungarian colleagues, the rest of them were done within an (informal) international cooperation, mostly with Italian researchers.

In the research proposal, the topics of the project were divided into two parts: (i) linear structures (such as linearised polynomials, or special subspaces of a vector space) and point sets derived from them and (ii) the study of combinatorially defined point sets, usually by associating algebraic curves, which helps to understand them better. The obtained results are presented in Sections 2 and 3, respectively. As we will see, curves and hypersurfaces play an important role also in the problems of (i), and techniques about linearised polynomials can be useful for problems of (ii) as well.

2 Linear structures

In this section we summarise our results from [3, 4, 12, 11] and their aftermath.

Let V be an r-dimensional vector space over $\mathbb{F}_{q^n}$, the finite field of q^n elements. Then V is also a vector space over $\mathbb{F}_q$ of dimension rn and an $\mathbb{F}_q$-subspace U of V is called scattered if it meets the one-dimensional $\mathbb{F}_{q^n}$-subspaces of V in $\mathbb{F}_q$-subspaces of dimension at most 1. In the seminal paper of Blokhuis and Lavrauw [6] it was proved that the maximum dimension of a scattered subspace U of V is $rn/2$. If the dimension of U reaches this upper bound, then U is called maximum scattered. Maximum scattered subspaces are well-studied objects of finite geometry, which have been linked to $\mathbb{F}_{q^n}$-linear MRD-codes (MRD-codes with a maximum idealiser), two-character sets, two-weight codes, strongly regular graphs.

In [4] with Bartoli and Montanucci we proved a conjecture on the number of inequivalent maximum scattered subspaces constructed in [10] and, as a consequence, we obtained a lower bound on the number of inequivalent MRD-codes contained in the corresponding family. The constructions in [10] produced the first examples of $\mathbb{F}_{q^n}$-linear MRD codes which are not of Gabidulin or Twisted Gabidulin type and hence this family is in the focus of interest since then (see for example [15, 16, 21]). In our proof first we gave a sufficient and necessary condition for $b \in \mathbb{F}_{q^6}$ such that the $\mathbb{F}_q$-subspace $\{(x, f(x)) : x \in \mathbb{F}_{q^6}\}$ is maximum scattered in $\mathbb{F}_{q^6} \times \mathbb{F}_{q^6}$, where $f(x)$ is the linearised polynomial $bx^q + x^{q^4}$. To do this we used some recent results about Dickson matrices and the number of roots of linearised polynomials from [9]. Then we used some delicate counting techniques involving rational points of quadratic surfaces.

In [11] with Marino, Polverino and Zullo we introduced h-scattered subspaces, a natural generalization of scattered subspaces (which is the $h = 1$ case). For the dimension of an h-scattered subspace we proved the upper bound $rn/(h + 1)$, which generalises the Blokhuis–Lavrauw bound. We defined a duality relation among such subspaces, and we gave various examples with maximum dimension. Our examples were linked later by Zini and Zullo to $\mathbb{F}_{q^n}$-linear MRD-codes [22].

In [3] with Bartoli, Marino and Trombetti we generalised further the concept of scatteredness. Let $\mathcal{F}$ be a set of subsets of a set A. A subset S of A is called c-evasive for $\mathcal{F}$ if S meets the elements of $\mathcal{F}$ in at most c points. This definition is due to Pudlák and Rödl [17]. In [3] we investigated the case when A is the set of vectors of an r-dimensional vector space over $\mathbb{F}_{q^n}$, $\mathcal{F}$ is the set of h-dimensional $\mathbb{F}_{q^n}$-subspaces of A and S is an $\mathbb{F}_q$-subspace. We called S $(h,k)_q$-evasive, if S meets the elements of $\mathcal{F}$ in $\mathbb{F}_q$-subspaces of dimension at most k. This notion generalizes the concept of scattered ($h = k = 1$) and h-scattered ($h = k$) subspaces. We proved upper and (via constructions) lower bounds on the maximum dimension of $(h,k)_q$-evasive subspaces. We extended the duality relation introduced in [11] from h-scattered subspaces to evasive subspaces. For $n = 5$, $r = 3$, and infinitely many values of q, we constructed scattered subspaces of maximum possible dimension in the vector space A. These are the first examples with these parameters. In the proof we represented the 3-dimensional $\mathbb{F}_{q^5}$-vector space A as the finite field $\mathbb{F}_{q^{15}}$ and translated the problem of finding the size of intersection of subspaces into the problem of finding the degree of the greatest common divisor of q-polynomials over $\mathbb{F}_{q^{15}}$. This allowed us to use the machineries from [9]. Our construction relies on the fact that certain hypersurfaces cannot have common points of a certain type. To prove this we also used the Magma Computational Algebra System. Our examples were linked later by Alfanaro, Borello, Neri and Ravagnani to cutting blocking sets and minimal codes in the rank metric [1].

In [12] with Marino, Polverino and Zhou we classified MRD-codes with maximum left and right idealisers in the ring of $n \times n$ matrices over $\mathbb{F}_q$ for $n \leqslant 9$. Surprisingly, we found new examples of this kind, which are not of Gabidulin type. These are the only known examples of this kind in the literature. We also proved some non-existence results relying on the fact that certain curves cannot have common $\mathbb{F}_q$-rational points. One of our open questions about the asymptotics of possible examples was answered later by Bartoli and Zhou in [2].

3 Combinatorially defined point sets

In this section we summarise our results from [14, 13, 8].

In [14] with Weiner we investigated generalised Korchmáros-Mazzocca arcs of type $(0, m, t)$, that is, point sets $\mathcal{S}$ of $\mathrm{PG}(2, q)$ (i.e., the projective plane over $\mathbb{F}_q$), such that each point P of $\mathcal{S}$ is incident with a t-secant and the other lines incident with P are m-secants (a k-secant of $\mathcal{S}$ is a line of $\mathrm{PG}(2, q)$ meeting $\mathcal{S}$ in exactly k points). Under certain conditions, we proved the existence of a nucleus: a common point of the t-secants. We also found examples without a nucleus, something which never occur in case of Korchmáros-Mazzocca arcs (which is the $m = 2$ case). We also found relations with group divisible designs and sharply focused arcs. Let q be a power of the prime p. Some of our examples are interesting also from a coding theory point of view, since when p divides m and t then these point sets correspond to code words in the dual of the code generated by the incidence vectors of points and lines of $\mathrm{PG}(2, q)$, and they usually have small, sometimes the smallest possible, weights. When m or t is not divisible by p, then we were able to describe all examples. We also considered mod p variants of such point sets. In the proofs we used polynomial techniques and a result on multisets due to Szőnyi and Weiner [20].

There are many examples for point sets in finite geometry, which behave “almost regularly” in some (well-defined) sense, for instance they have “almost regular” line-intersection numbers. In [13] with Weiner and Sziklai we investigated point sets of $\mathrm{AG}(2, q)$, the affine plane over $\mathbb{F}_q$, for which there exist some (sometimes: many) parallel classes of lines, such that almost all lines of one parallel class intersect our set in the same number of points (possibly modulo p, the characteristic). The lines with exceptional intersection numbers are called renitent, and we proved results on the (regular) behaviour of these renitent lines. We proved that, under some conditions, the renitent lines are contained in a low degree algebraic curve of the dual plane. If we strengthen these conditions, the degree becomes smaller. In the proofs we used polynomial techniques. For illustration, we state here one of our theorems. Let $\mathcal{M}$ be a multiset of $\mathrm{AG}(2, q)$. For some integer $r < q/2$ the direction (d) is called $(q - r)$-uniform, if there are at least $(q - r)$ affine lines with slope d meeting $\mathcal{M}$ in the same number of points modulo p. The rest of the lines with slope d are called renitent. Let $\mathcal{F}$ denote a set of $(q - r)$-uniform directions. Then the renitent lines with slope in $\mathcal{F}$ are contained in an algebraic curve of degree r^2 of the dual plane. With some further restrictions, we can push down the degree in the above result from r^2 to r. These results have immediate applications in the study of point sets $\mathcal{S}$ of $\mathrm{PG}(2,q)$ with the property that each point of $\mathcal{S}$ is incident with r t-secants and $(q+1-r)$ m-secants, and hence they naturally extend some of our results from [14] and some earlier results on semiovals and directions determined by affine point sets due to Blokhuis and Szőnyi from [5, 7, 19]. Indeed, fix an m-secant ℓ and consider it as the line at infinity. Then the t-secants meeting ℓ in $\mathcal{S}$ can be considered as renitent lines. Our manuscript is submitted to the European Journal of Combinatorics.

Let $\mathrm{PG}(r,q)$ denote the r-dimensional projective space over $\mathbb{F}_q$. A k-cap in $\mathrm{PG}(r,q)$ is a set of k points no three of which are collinear. A k-cap is said to be complete if it is not contained in a $(k+1)$-cap. The study of caps is not only of geometrical interest, their concept appears also in coding theory, since complete caps correspond to certain non-extendable linear codes. They are also natural examples of 1-saturating sets. In 1959 Segre proved the lower bound $\sqrt{2}q^{\frac{r-1}{2}}$ for the size of the smallest complete cap in $\mathrm{PG}(r,q)$, [18]. Despite the many efforts made, apart from the case when q is even and r is odd, all known constructions of infinite families of complete caps have size far from this lower bound. In [8] with Cossidente, Marino and Pavese we constructed complete caps in $\Lambda := \mathrm{PG}(4n+1,q)$, $q>2$, of size $2(q^{2n}+q^{2n-1}+\ldots+1)$ and hence we proved that Segre's bound is essentially sharp when $r=4n+1$. To present our construction, first we introduce the $(4n+2)$-dimensional $\mathbb{F}_q$-vector space V whose subspace lattice plays the role of the projective space Λ:

$$V := \{(a,b,a^q,b^q,\ldots,a^{q^{2n}},b^{q^{2n}}) : a,b \in \mathbb{F}_{q^{2n+1}}\}.$$

Denote by $P(a,b)$ the projective point of Λ defined by the vector $(a,b,a^q,b^q,\ldots,a^{q^{2n}},b^{q^{2n}})$ for each $(a,b)\neq(0,0)$. Denote by Π_1 and Π_2 the $2n$-dimensional projective subspaces consisting of the points $P(0,b)$ and $P(a,0)$, respectively, where a and b run over the non-zero elements of $\mathbb{F}_{q^{2n+1}}$. It can be proved that the points of $\Lambda\backslash(\Pi_1\cup\Pi_2)$ can be partitioned into $\bigcup_{\omega\in\mathbb{F}_{q^{2n+1}}\backslash\{0\}}\mathcal{V}_\omega$, where

$$\mathcal{V}_\omega = \left\{P(x^2,\omega x^{q+1}) : x\in\mathbb{F}_{q^{2n+1}}\backslash\{0\}\right\}.$$

It turns out that the set $\mathcal{V}_\omega$ is a cap of Λ of size $(q^{2n}+q^{2n-1}+\ldots+1)$. Let α be -1 if q is odd and an element of $\mathbb{F}_q\backslash\{0,1\}$ if $q>2$ is even. Our main result states that $\mathcal{V}_1\cup\mathcal{V}_\alpha$ is a complete cap. When $n=1$, then $\mathcal{V}_\omega$ is a Veronese variety. In general, $\mathcal{V}_1\cup\mathcal{V}_\alpha$ can be viewed as the projection of two disjoint Veronese varieties of $\mathrm{PG}(2n^2+3n,q)$ from a suitable $(2n^2-n-2)$-dimensional projective subspace. The hardest part was to prove the completeness. After a series of algebraic manipulations this problem boiled down to find a non-zero root in $\mathbb{F}_{q^{2n+1}}$ of certain linearised polynomials, or equivalently, to prove that none of them induces a permutation of $\mathbb{F}_{q^{2n+1}}$. We used a Dickson-like matrix to prove that certain linearised polynomials have a non-zero root in the field of their coefficients if and only if they have a non-zero root in the quadratic extension of this field. This result allowed us to search for the non-zero roots in $\mathbb{F}_{q^{4n+2}}$, where we could explicitly locate them. Our manuscript is submitted to the Journal of the London Mathematical Society.

References

[1] G.N. Alfarano, M. Borello, A. Neri, A. Ravagnani: Linear Cutting Blocking Sets and Minimal Codes in the Rank Metric, https://arxiv.org/abs/2106.12465

[2] D. Bartoli, Y. Zhou: Asymptotics of Moore exponent sets, *J. Combin. Theory, Ser. A* **175** (2020), 105281.

[3] D. Bartoli, B. Csajbók, G. Marino, R. Trombetti: Evasive subspaces, *J. Combin. Des.*, 10.1002/jcd.21783

[4] D. Bartoli, B. Csajbók, M. Montanucci: On a conjecture about maximum scattered subspaces of $\mathbb{F}_q^6\times\mathbb{F}_q^6$, *Linear Algebra Appl.* **631** (2021), 111–135.

[5] A. Blokhuis: Characterization of seminuclear sets in a finite projective plane, *J. Geom.* **40** (1991), 15–19.

[6] A. Blokhuis, M. Lavrauw: Scattered spaces with respect to a spread in $\mathrm{PG}(n,q)$, *Geom. Dedicata* **81** (2000), 231–243.

[7] A. Blokhuis, T. Szőnyi: Note on the structure of semiovals, *Discrete Math.* **106/107** (1992), 61–65.

[8] A. Cossidente, B. Csajbók, G. Marino, F. Pavese: Small comlete caps in $\mathrm{PG}(4n+1,q)$, submitted to the J. Lond. Math. Soc, https://arxiv.org/abs/2105.14939

[9] B. Csajbók: Scalar q-subresultants and Dickson matrices, *J. Algebra* **547** (2020), 116–128.

[10] B. Csajbók, G. Marino, O. Polverino, C. Zanella: A new family of MRD-codes, *Linear Algebra Appl.* **548** (2018), 203–220.

[11] B. Csajbók, G. Marino, O. Polverino, F. Zullo: Generalising the scattered property of subspaces, *Combinatorica* **41** (2021), 237–262.

[12] B. Csajbók, G. Marino, O. Polverino, Y. Zhou: MRD codes with maximum idealizers, *Discrete Mathematics* **343**(9) (2020), 111985.

[13] B. Csajbók, P. Sziklai, Zs. Weiner: Renitent lines, submitted to the European Journal of Combinatorics, https://arxiv.org/abs/2102.11790

[14] B. Csajbók, Zs. Weiner: Generalizing Korchmáros-Mazzocca arcs, *Combinatorica*, 10.1007/s00493-020-4419-z

[15] O. Polverino, F. Zullo: On the number of roots of some linearized polynomials, *Linear Algebra Appl.* **601** (2020), 189–218.

[16] O. Polverino, G. Zini, F. Zullo: On certain linearized polynomials with high degree and kernel of small dimension, *J. Pure Appl. Algebra* **225**(2) (2021), 106491.

[17] P. Pudlák, V. Rödl: Pseudorandom sets and explicit constructions of Ramsey graphs, *Quaderni di Matematica* **13** (2004), 327–346.

[18] B. Segre: On complete caps and ovaloids in three–dimensional Galois spaces of characteristic two, *Acta Arith.* **5** (1959), 315–332.

[19] T. Szőnyi: On the number of directions determined by a set of points in an affine Galois plane, *J. Combin. Theory Ser. A* **74** (1996), 141–146.

[20] T. Szőnyi and Zs. Weiner: Stability of k mod p multisets and small weight codewords of the code generated by the lines of $\mathrm{PG}(2,q)$, *J. Combin. Theory Ser. A* **157** (2018), 321–333.

[21] M. Timpanella, G. Zini: On a family of linear MRD codes with parameters $[8\times 8,16,7]_q$, https://arxiv.org/abs/2108.13082

[22] G. Zini, F. Zullo: Scattered subspaces and related codes, *Designs, Codes and Cryptogr.* **89** (2021), 1853–1873.