6th Emléktábla Workshop

Finite Geometry 07. 28-31. 2014.

Preliminary Schedule

Day 1:
9:29 Welcome
9:30 - 10:15 Leo Storme, Gent Universiteit
10:30 - 11:15 Péter Sziklai, MTA-ELTE GAC
11:30 - 12:15 Willem H. Haemers, Tilburg University
Lunch Break
14:00 - 14:45 Aart Blokhuis, Technishce Universiteit Eindhoven
15:30 from in front of Rényi: Traveling together to Eger by private bus.

Other Days:
9:29 Waking up
8:30 - 9:30 Breakfast
9:30 Partitioning to Groups of 3-5 for the day
9:30 - 12:30 Work in Groups of 3-5
12:30 - 14:00 Lunch Break
14:00 Optional Repartitioning for the afternoon
14:00 - 17:00 Work in Groups of 3-5
17:00 - 18:30 Discussion of Results
18:30 - Dinner and other activities

Last Day:
Discussion from after lunch and then Return to Budapest starting 16:00 (ETA 17:30).

List of Participants

József Balogh, University of Szeged and UIUC
János Barát, MTA-ELTE GAC
Zoltán Blázsik, Eötvös Univeristy
Bence Csajbók, MTA-ELTE GAC
Péter Csikvári, Massachussets Institute of Technology
Jay Cummings, UC San Diego
Dániel Gerbner, MTA Rényi Institute
Tamás Héger, MTA-ELTE GAC
Nóra Harrach, MTA Rényi Institute
Balázs Keszegh, MTA Rényi Institute
Michał Lasoń, Institute of Mathematics of the Polish Academy of Sciences
Wojciech Lubawski, Jagiellonian University
Zoltán Lóránt Nagy, MTA Rényi Institute
Cory Palmer, University of Montana
Dömötör Pálvölgyi, Eötvös University
Balázs Patkós, MTA-ELTE GAC
Alexander Pokrovskiy, FU Berlin
Ago Riet, University of Tartu
Tamás Szőnyi, MTA-ELTE GAC
Adrian Claudiu Valculescu, École Plytechnique de Lausanne
Tomas Valla, Czech Technical University
Máté Vizer, MTA Rényi Institute
Dominik Vu, University of Memphis

Problems for Emlék Tábla

by Aart Blokhuis

Nuclei Let B be a set of $q+1$ points in $\mathcal{A} = AG(2,q)$, the (desarguesian) affine plane of order q. A point $P \notin B$ is called a *nucleus* of B if every line through it contains a (unique) point of B. An old result of Henny Wilbrink and me says that there are at most $q-1$ nuclei. The first two exercises are to prove this.

Exercise 1 Identify in a natural way the points of $\mathcal{A}$ with the elements of the field $GF(q^2)$ and define the polynomial $p(x) = \sum_{b\in B}(x-b)^{q-1}$. Show that $p(a) = 0$ when a is a nucleus, and conclude that there are at most $q-1$ nuclei.

Exercise 2 Let A_0, A_1 and A_2 be three nuclei, that are not collinear. Let B_{i+2} on A_iA_{i+1} (indices mod 3) be the (unique) points of B on the sides of the triangle $A_0A_1A_2$. Show that $B_{1,2,3}$ are collinear. Using this result, together with Desargues theorem, show that it is possible to 'lift' the set N of nuclei into three-space $AG(3,q)$ by adding to each nucleus a (different) z-coordinate, in such a way that collinear subsets of $B \cup N$ remain collinear (the set B stays in the plane $z = 0$).

Research problem 3 The only known examples of $q+1$ sets with the maximal number $q-1$ of nuclei are: (i) B consists of a line l plus an additional point P, N consists of the remaining points on the line through P parallel to l; (ii) the 10 points of a Desargues configuration in $AG(2,5)$ can be partitioned into $|B| + |N| = 6 + 4$ points.
Show that there are no other examples.

Lacunary Polynomials In the proof for the lower bound on the size of non-trivial blocking sets in projective planes of prime order the following lemma is central:
Let $f(x) \in GF(p)[x]$ be a fully reducible, lacunary polynomial of the following form: $f(x) = x^p g(x) + h(x)$, with $\deg(h) =: h^\circ \leq g^\circ$, g and h coprime. Then either g is constant, or $g^\circ \geq (p+1)/2$.
Here fully reducible means that it factors over $GF(p)$ into linear factors, lacunary stands for the property that many coefficients are zero (all between $h^\circ + 1$ and $p-1$).
The short proof is as follows: write $f = s \cdot r$, where s is the product of the different linear factors of f, and r the rest. So s divides not only f but also $x^p - x$, and as a consequence $s(x) \,|\, xg(x)+h(x)$. The polynomial r divides $f' = x^p g'(x)+h'(x)$ and also f, so also $g'f - f'g = g'h - h'g$. Combining this we get

$$x^p g(x) + h(x) \,|\, (xg(x) + h(x))(g'(x)h(x) - g(x)h'(x)).$$

Comparing degrees we get $g^\circ + 1 + 2g^\circ - 2 \geq p + g^\circ$ (unless g and h are constant).

Research Problem 4 Find the (fully reducible) polynomials $f = x^p g + h$ that realize equality in this bound, in other words: solve the differential equation

$$x^p g(x) + h(x) = a(xg(x) + h(x))(g'(x)h(x) - g(x)h'(x)),$$

where $a \in GF(p)$, $g, h \in GF(p)[x]$ $h^\circ \leq g^\circ = (p+1)/2$.

Remark For $p \leq 41$ we managed (with a computer) to find all solutions based on the following idea: The polynomial $s \hat{=} xg + h$ has degree $(p+3)/2$ and factors in different linear factors, so it corresponds with a subset of size $(p+3)/2$ of $GF(p)$, its complement has size $(p-3)/2$, and we still have a 2-transitive group acting, so we have to investigate $\binom{p}{(p-3)/2}/p^2$ cases.

Small sets determining all directions Let B be a set of points in $\mathcal{A} = AG(2,q)$. Every pair determines a line and hence a direction. We want to minimize the size of B such that it determines all directions.

Exercise 5 Show that $\binom{|B|}{2} \geq q+1$, so $B \geq \sqrt{2q}$ (roughly).

Exercise 6 Show that the minimal $|B|$ is at most $2\sqrt{q}$ (roughly).

Exercise 7 Produce good examples (in planes of odd order ≤ 97 say) by starting with a set of points on the parabola $y = x^2$.

Research Problem 8 Improve the lower bound or the upper bound or anything.

Small complete arcs An arc A in $PG(2,q)$ or $AG(2,q)$ is a set of points, such that no three are collinear. An arc is complete if it is not contained in a larger one. We want to know the size of the smallest complete arc.

Exercise 9 Show that $\binom{|A|}{2}(q-1) \geq (q^2+q+1) - |A|$, so $|A| \geq \sqrt{2q}$ (roughly).

Blocking sets The secants of a complete arc (the lines that intersect it in more than one, and therefore two points) cover the plane, so they form a dual blocking set. A blocking set is a set of points intersecting every line, a blocking set of the projective plane containing a line is called trivial. For planes of prime order we know that a non-trivial blocking set has at least $3(p+1)/2$ points, for complete arcs this implies $|A| \geq \sqrt{3p}$ (roughly). For planes of non-prime order smaller blocking sets exist, but they have the 1 mod p property: A small minimal blocking set in $PG(2, q = p^h)$ intersects every line in 1 mod p points.

Research Problem 10 Show that $|A| \geq \sqrt{3q}$ holds in general. The problem is that the dual blocking set obtained from the secants may be small, but not minimal, so you cannot apply the 1 mod p result directly.

Some problems on graph spectra

by Willem H. Haemers

1 How tight is the Cvetković bound?

Let A be a symmetric $n \times n$ matrix with eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$, and let B be an $m \times m$ principal submatrix of A with eigenvalues $\mu_1 \geq \ldots \geq \mu_m$. Then the following inequalities hold (interlacing).

$$\lambda_i \geq \mu_i \geq \lambda_{n-m+i} \quad \text{for} \quad i = 1, \ldots, m$$

If A is the adjacency matrix of a graph with a coclique O (independent set of vertices) of size m, then we can take $B = O$. Then $\mu_1 = \mu_m = 0$ and the above inequalities imply that A has at least m nonnegative, and at least m nonpositive eigenvalues. This gives a bound for the maximum size of a coclique, known as Cvetković bound.

However, we can improve the bound. If we replace every nonzero entry of A by an arbitrary real number, such that A remains symmetric, then the above argument still works and the same conclusion holds.

Problem: Find a graph for which there exists no 'generalized adjacency matrix' A for which the Cvetković bound is tight.

2 Finding Godsil-McKay switching sets

Graphs with the same adjacency eigenvalues are called cospectral. A method to construct cospectral graphs is the following result of Godsil and McKay.

Theorem 1. *Let G be a graph and let $\{X_1, \ldots, X_\ell, Y\}$ be a partition of the vertex set $V(G)$ of G. Suppose that for every vertex $x \in Y$ and every $i \in \{1, \ldots, \ell\}$, x has either 0, $\frac{1}{2}|X_i|$ or $|X_i|$ neighbors in X_i. Moreover, suppose that for all $i, j \in \{1, \ldots, \ell\}$ every vertex $x \in X_i$ has the same number of neighbors in X_j. Make a new graph G' as follows. For each $x \in Y$ and $i \in \{1, \ldots, \ell\}$ such that x has $\frac{1}{2}|X_i|$ neighbors in X_i delete the corresponding $\frac{1}{2}|X_i|$ edges and join x instead to the $\frac{1}{2}|X_i|$ other vertices in X_i. Then G and G' are cospectral.*

The operation that changes G into G' is called *Godsil-McKay switching*, and the considered partition is a *(Godsil-McKay) switching partition*. If $|X_i| = 2$ for $i = 1, \ldots, \ell$, then G and G' are isomorphic. Otherwise, the graphs are usually (but not always) nonisomorphic. Godsil-McKay switching is an important tool in proving that certain graphs, or graph properties are not determined by the spectrum. However, for many cases the question is still open.

Two specific problems are:

1. Find two regular cospectral graphs, where one has a perfect matching and the other has none.

2. Which Kneser graphs $K(k, \ell)$ are determined by their spectrum?
If $\ell \leq 2$ and $(k, \ell) \neq (8, 2)$, or if $\ell \geq (k-1)/2$ the answer is 'yes'. If $k = 3\ell - 1 \geq 8$, $k = 3\ell - (3 - \sqrt{8\ell^2 + 1})/2 \geq 25$, or if $(k, \ell) = (8, 2)$ the answer is 'no'. For other values of (k, ℓ) the answer is unknown.

3 The minimal Seidel energy

If A is the adjacency matrix of a graph G, then $S = J - 2A - I$ (as usual, I and J are the identity matrix and the all-ones matrix, respectively) is the Seidel matrix G. The energy of G is the sum of the absolute values of the eigenvalues of A, and the Seidel energy is the sum of the absolute values of the eigenvalues of S. (Note that for both type of matrices the sum of the eigenvalues equals 0.) It is easy to prove that the Seidel energy is at most $n\sqrt{n-1}$ with equality if and only if $S^2 = (n-1)I$. Such Seidel matrices are known as conference matrices. They are known to exist for infinitely many values of n. The Seidel energy is invariant under taking complements (multiplying S by -1), and Seidel switching (multiplying some rows and the corresponding columns by -1).

Problem: Determine the minimum value of the Seidel energy for a graph on n vertices. It is conjectured that the complete graph has minimal Seidel energy (equal to $2(n-1)$).

References

[1] A.E Brouwer and W.H. Haemers, Spectra of Graphs, Springer 2012; see `http://homepages.cwi.nl/~aeb/math/ipm/ipm.pdf`

Random network coding: a new direction in coding theory

by Leo Storme

Abstract

This text draws the attention to open problems in random network coding: a new direction in coding theory, which presently receives a lot of attention. Many of these problems are q-analog problems.

4 Classical coding theory

Consider an *alphabet* F_q of size q.

An (n, M, d)-*code* C *over* F_q is a subset of F_q^n, consisting of M different n-tuples, of minimum distance d.

Here, the *minimum (Hamming) distance* d is the minimal number of positions in which two distinct codewords differ.

The importance of the minimum distance d lies in the error-correcting capacity of this code C. If during transmission, in a transmitted codeword c of C, at most t errors occur, with $d = 2t + 1$ or $d = 2t + 2$, then these errors can be corrected if we replace the received n-tuple w by the codeword of C that is at smallest Hamming distance of w [9]. We say that the code C is t-*error correcting*.

Example 1. *An easy example is the binary repetition code of length 5.*

Here, C *is equal to the code of the two codewords:*

$$C = \{(0, 0, 0, 0, 0), (1, 1, 1, 1, 1)\}.$$

We denote this by $C = (n = 5, M = 2, d = 5)$*-code.*

As a concrete example: if the codeword $c = (0, 0, 0, 0, 0)$ *is transmitted, but the 5-tuple* $w = (1, 1, 0, 0, 0)$ *is received, then the received 5-tuple* $w = (1, 1, 0, 0, 0)$ *is decoded as* $(0, 0, 0, 0, 0)$*, and so the transmitted codeword is reconstructed.*

In coding theory, there are many bounds on the three fundamental parameters n, M, d of a q-ary code C. We discuss in particular the *Johnson bound for constant weight codes*. Here, the *weight* of a codeword is the number of nonzero symbols in the codeword.

The parameter $A_q(n, d, w)$ is the largest number of codewords in a q-ary code of codewords of weight w and with minimum distance d.

- For $d \leq 2w$, let $d = 2e$ if d even, and $d = 2e - 1$ if d odd.

$$A_q(n, d, w) \leq \lfloor \frac{n(q-1)}{w} A_q(n-1, d, w-1) \rfloor$$

- (Let $q^* = q - 1$)

$$A_q(n, d, w) \leq \lfloor \frac{nq^*}{w} \lfloor \frac{(n-1)q^*}{w-1} \lfloor \cdots \lfloor \frac{(n-w+e)q^*}{e} \rfloor \cdots \rfloor \rfloor$$

5 Random network coding

Consider a network with varying topology, where users come and go. How is it possible to transmit quickly information through the network?

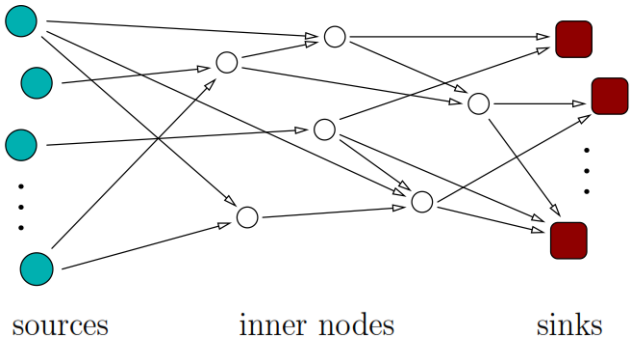

Figure 1: Transmission through a network

R. Kötter and F. Kschischang suggested to use *network codes*.

In a *random network code*, the codewords are subspaces U of $V(n,q)$, the n-dimensional vector space over the finite field $\mathbb{F}_q$ of order q. To transmit a codeword U, it is sufficient to transmit a basis of U, but intermediate nodes are allowed to transmit linear combinations of incoming basis vectors. Kötter and Kschischang noticed that this speeds up the transmission.

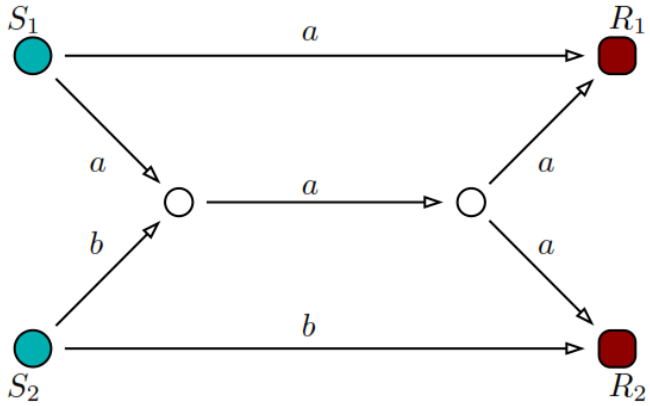

Figure 2: Intermediate nodes cannot transmit linear combinations of incoming basis vectors

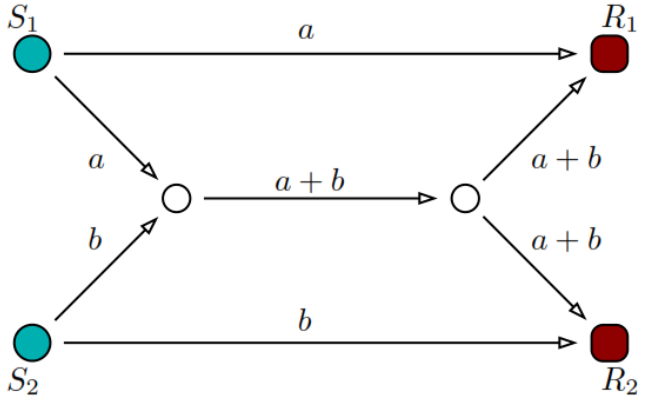

Figure 3: Intermediate nodes can transmit linear combinations of incoming basis vectors

We see this by comparing Figures 2 and 3. In Figure 2, the intermediate node cannot transmit a linear combination of incoming basis vectors. In this way, the two basis vectors a and b cannot both reach the destination R_1. But in Figure 3, the intermediate node can transmit the linear combination $a + b$ of the incoming basis vectors a and b. In this way, the two basis vectors a and b can reach the destinations R_1 and R_2, because R_1 can recover b from a and $a + b$, and R_2 can recover a from b and $a + b$.

This idea opens up a complete new theory: from classical coding theory to random network coding.

In the remainder of this text, we will consider a *Constant dimension code*, i.e., all codewords have the same dimension k.

To determine the error-correcting capacity of such a random network code, we need to define a distance. Here, we use the *subspace distance*.

Let U, V be subspaces of $V(n, q)$, then

$$d(U, V) = \dim(U) + \dim(V) - 2\dim(U \cap V).$$

As a consequence, the *minimum distance* $d(C) = \min_{\{U,V \in C, U \neq V\}} d(U, V)$. So the larger d, the smaller $\dim(U \cap V)$.

In this completely new theory, many times the new type of problems that arise are:

q-analog problems*: replace problems on sets by corresponding q-analog problems on subspaces of $V(n, q)$.*

We illustrate this via the q-analog of the Johnson bound for constant weight codes. The Johnson bound for constant dimension random network codes is as follows:

$\mathcal{A}_q(n, d, k)$: largest number of codewords in random network code of k-dimensional codewords in $V(n, q)$ having minimum distance d.

1.
$$\mathcal{A}_q(n, d, k) \leq \frac{q^n - 1}{q^k - 1}\mathcal{A}_q(n - 1, d, k - 1).$$

2.
$$\mathcal{A}_q(n, 2k, k) \leq \frac{q^n - 1}{q^k - 1}$$

and equality holds if and only if k divides n, because equality holds if and only if $V(n, q)$ has a partitioning into k-dimensional subspaces.

Let

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}$$

(this number is the number of k-dimensional subspaces in $V(n, q)$).

Let

$$t = k - d/2 + 1.$$

Then

$$\mathcal{A}_q(n,d,k) \leq \frac{\begin{bmatrix} n \\ t-1 \end{bmatrix}_q}{\begin{bmatrix} k \\ t-1 \end{bmatrix}_q} \mathcal{A}_q(n-k+d/2, d, d/2),$$

where

$$\mathcal{A}_q(n-k+d/2, d, d/2)$$

equals the maximum size of a partial $(d/2)$-spread in $V(n-k+d/2, q)$.

As a concrete example:

- $$\mathcal{A}_q(6,4,3) \leq (q^3+1)^2$$

  which has the following vector meaning: The upper bound on the number of 3-dimensional subspaces of $V(6,q)$ pairwise intersecting in at most a vector line is $(q^3+1)^2$.

There is one recent result in which we have the exact value for $\mathcal{A}_q(6,4,3)$.

Theorem 2 (Honold, Kiermaier, Kurz)**.** [7]

$$\mathcal{A}_2(6,4,3) = 77.$$

The maximal number of 3*-dimensional subspaces in* $V(6,2)$ *pairwise intersecting in at most a vector line* $V(1,2)$ *is* 77*.*

Theorem 3 (Honold, Kiermaier, Kurz, Cossidente, Pavese)**.** [2, 7]

$$q^6 + 2q^2 + 2q + 1 \leq \mathcal{A}_q(6,4,3) \leq (q^3+1)^2.$$

There is an example of $q^6 + 2q^2 + 2q + 1$ *distinct* 3*-dimensional subspaces in* $V(6,q)$ *pairwise intersecting in at most a vector line* $V(1,q)$*.*

6 Finite projective spaces

In the preceding section, random network coding was described in a vector space setting $V(n,q)$. The codewords consist of k-dimensional vector subspaces $V(k,q)$ in this given vector space $V(n,q)$.

But this has an equivalent formulation in a projective space setting. In a projective space setting, a k-dimensional vector space $V(k,q)$ corresponds to a $(k-1)$-dimensional projective space $\mathrm{PG}(k-1,q)$, and the n-dimensional vector space $V(n,q)$ corresponds to the $(n-1)$-dimensional projective space $\mathrm{PG}(n-1,q)$ [5, 6].

So many problems on random network codes have an equivalent formulation as a problem in finite projective spaces. In this projective spaces setting, specific techniques can be used.

For instance, Cossidente and Pavese constructed their example of $q^6 + 2q^2 + 2q + 1$ distinct 3-dimensional subspaces in $V(6,q)$ pairwise intersecting in at most a vector line $V(1,q)$, in the projective space setting [2]. They constructed a set of q^6+2q^2+2q+1 projective planes in $\mathrm{PG}(5,q)$ pairwise intersecting in at most a projective point. The crucial ideas in their construction methods were: bundles of conics in a fixed plane $\mathrm{PG}(2,q)$ of $\mathrm{PG}(3,q)$, hyperbolic quadrics of $\mathrm{PG}(3,q)$ through the conics of this bundle, reguli and opposite reguli of these hyperbolic quadrics, the Klein

correspondence which associates Plücker coordinates to the lines of these reguli and opposite reguli and which associates planes of $\mathrm{PG}(5,q)$ to these reguli and opposite reguli, and the Klein quadric $Q^+(5,q)$.

Due to this equivalence between problems on random network codes and problems on substructures in finite projective spaces, it is of the greatest importance to also keep up-to-date with the research results on substructures in finite projective spaces.

7 Open problems

The preceding theorems are intended to give a flavour of the type of problems that occur in random network coding.

7.1 Problem 1

The first problem can be stated very general:

Problem 1: *Investigate the parameter* $\mathcal{A}_q(n,d,k)$.

This translates to different types of problems. First of all:

Problem 1.1: *Find geometrical constructions of large sets* $\mathcal{S}$ *of* k*-dimensional subspaces in* $V(n,q)$ *pairwise intersecting in at most a vector space of dimension* $k-d/2$.

As a concrete example, for $d=2k$, this means that two different k-dimensional subspaces of $\mathcal{S}$ pairwise intersect in the zero-vector. Then $\mathcal{S}$ is called a *partial* k*-spread* of $V(n,q)$.

Here, the upper bound is known when k divides n, since then it is possible to partition the non-zero vectors of $V(n,q)$ into k-dimensional subspaces.

But if k does not divide n, then in many cases, the upper bound on the size of a partial k-spread of $V(n,q)$ is not known [1]. So here, an important problem is to improve the known upper bounds on the sizes of these partial k-spreads of $V(n,q)$.

But when $d<2k$, also then there are still many cases in which we are looking for large sets $\mathcal{S}$ of k-dimensional subspaces in $V(n,q)$ pairwise intersecting in at most a vector space of dimension $k-d/2$.

Problem 1.2: *Eliminate possible sizes for large sets* $\mathcal{S}$ *of* k*-dimensional subspaces in* $V(n,q)$ *pairwise intersecting in at most a vector space of dimension* $k-d/2$.

In many cases, there are no sets $\mathcal{S}$ of k-dimensional subspaces in $V(n,q)$ pairwise intersecting in at most a vector space of dimension $k-d/2$, meeting the upper bound for the Johnson bound $\mathcal{A}_q(n,d,k)$.

So the problem is whether the present upper bounds on $\mathcal{A}_q(n,d,k)$ can be improved? Sometimes imposing that a set $\mathcal{S}$ of k-dimensional subspaces in $V(n,q)$ pairwise intersecting in at most a vector space of dimension $k-d/2$ has a very large size leads to geometrical information on the k-dimensional subspaces in this set $\mathcal{S}$, which then leads to contradictory information, thus eliminating such sets $\mathcal{S}$ of that large size.

Problem 1.3: *Prove extendability results on random network codes.*

The third problem originates from coding theory. In classical coding theory, there are different types of *extendability results*. Here, *extendability* can relate to enlarging the length of the code and simultaneously increasing the minimum distance d of the code, or can relate to increasing the number of codewords of the code, without decreasing the minimum distance d.

A very well-known example in classical coding theory is the extendability of q-ary $(4, q^2-1, 3)$-codes to $(4, q^2, 3)$-codes.

In random network coding, recently, A. Nakić and L. Storme proved a similar extendability result for random network codes satisfying specific divisibility conditions for their parameters [8].

So, here the open problem is to improve these extendability results.

7.2 Problem 2

It is clear from Problem 1 that many problems on random network codes are equivalent to particular problems on substructures in finite projective spaces.

In fact, random network coding has led to new interesting problems on substructures in finite projective spaces. Problem 1 focusses precisely on this type of problems.

But there are also specific problems, closely related to problems from random network codes, which are of a geometrical interest or importance.

We mention two particular examples of such problems.

Problem 2.1: *Construct small maximal sets $\mathcal{S}$ of k-dimensional subspaces in $V(n,q)$ pairwise intersecting in at most a vector space of dimension $k-d/2$.*

Here, *maximal* means that these sets $\mathcal{S}$ are not strictly contained in a larger set $\mathcal{S}$ of k-dimensional subspaces in $V(n,q)$ pairwise intersecting in at most a vector space of dimension $k-d/2$.

For instance, let $d = 2k$, then this problem asks for the smallest maximal partial k-spreads in $V(n,q)$ [4].

Problem 2.2: *Construct for many values of s, maximal sets $\mathcal{S}$ of s distinct k-dimensional subspaces in $V(n,q)$ pairwise intersecting in at most a vector space of dimension $k-d/2$.*

This type of problem is called a *spectrum problem*. In this problem, the spectrum for a parameter s is investigated [10].

7.3 COST project

Since 2012, there is a COST project focusing on Random network coding. The COST project IC-1104 *Random network coding and designs over GF(q)* [3] investigates a large variety of problems on random network coding.

Under `http://www.network-coding.eu/pubs.html`, T. Etzion has made available an article, entitled *Problems on q-Analogs in Coding Theory*, listing many problems on random network coding.

Similarly, under the same webpage, L. Lambert has put available her master project *Random network coding and designs over* $\mathbb{F}_q$, written during the academic year 2012-2013 at Ghent University. This master project was specifically intended to write a text which, as quickly as possible, introduces random network coding to new researchers wishing to work on this topic.

References

[1] A. Beutelspacher, Partial spreads in finite projective spaces and partial designs. *Math. Z.* **145** (1975), 211-230.

[2] A. Cossidente and F. Pavese, On subspace codes. *Des. Codes Cryptogr.*, submitted.

[3] `http://www.network-coding.eu/`

[4] P. Govaerts, Small maximal partial t-spreads. *Bull. Belg. Math. Soc. - Simon Stevin* **12** (2005), 607-615.

[5] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries.* Oxford Mathematical Monographs. Oxford Science Publications. The Clarendon Press, Oxford University Press, Oxford, 1991.

[6] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields, Second Edition.* Oxford University Press, New York, 1998.

[7] T. Honold, M. Kiermaier, and S. Kurz, Optimal Binary Subspace Codes of Length 6, Constant Dimension 3 and Minimum Distance 4. *Contemp. Math.*, accepted.

[8] A. Nakić and L. Storme, On the extendability of particular classes of random network codes. (In preparation).

[9] V.S. Pless and W.C. Huffman, Eds., *Handbook of Coding Theory.* Elsevier 1998.

[10] L. Storme, Spectrum results in Galois geometries. *Advances in Mathematics Research, Volume* 12 (A.R. Baswell, Ed.), NOVA Academic Publishers (2012), 147-172.

Cim

by Péter Sziklai

We work over the finite field GF(q) having q elements, $q = p^h$ a prime power. AG(n, q) is the n-dimensional affine (or vector-) space over GF(q), PG(n, q) is the n-dimensional projective space, and we imagine PG(n, q) as AG(n, q)$\cup H_\infty$, where H_∞ is the "hyperplane at infinity". The points of H_∞ are sometimes called **directions**.

A point set U **determines a direction** $d \in H_\infty$ if a secant line of U hits H_∞ at d. Then D_U or simply $D \subseteq H_\infty$ is the set of directions determined by U, $N = H_\infty \setminus D$ is the set of nondetermined directions.

Exercise. Show that $|U| > q^{n-1}$ implies that every direction in H_∞ are determined.

Basically, we are interested in two questions.

Research problem.
(a) What are the possible (feasible) direction sets D for which there exists an affine point set U such that $D = D_U$?
(b) Given a feasible direction set D, which are the minimal and the maximal affine point sets U such that $D = D_U$? This is very general. Every subcase is interesting, i.e. restriction to the plane ($n = 2$), asking the possible numbers $|D_U|$, fixing the size $|U|$, etc. A well-known (difficult) case is when $n = 2, |U| = q$ and $|D_U| < \frac{q+3}{2}$: in this case the points of U (if you suppose that the origin is in U) form a linear subspace over a suitable subfield of GF(q). In particular, if $q = p$ is a prime then U must be a line.

Exercise. Show that a random pointset of size at least $\sqrt{2q\log(q)}$ determines every direction with high probability.

Rédei and Megyesi proved that in AG($2, p$), p prime, a set U of p points determines at least $\frac{p+3}{2}$ directions, unless U is a complete affine line. Lovász and Schrijver proved that in the case of equality the set is unique (the origin plus the square elements of the field on the two coordinate axes). Later Szőnyi (and even later Blokhuis) proved the analogue of the Rédei-Megyesi result: a set U of $k \leq p$ points determines at least $\frac{k+3}{2}$ directions, unless the points of U are collinear. The analogue of the construction above shows that the bound is sharp: if you take the origin plus a multiplicative subgroup of size $\frac{k-1}{2}$ on each coordinate axes, then the resulting k points determine $\frac{k+3}{2}$ directions precisely.
Problem. Show the analogue of the Lovász-Schrijver result, i.e. that if $|U| = k$ determines precisely $\frac{k+3}{2}$ directions then U is the point set coming from the construction above.

Problem. Show that in AG($2, p$), p prime, a set U of $p - \varepsilon$ points ($0 \leq \varepsilon \leq$ ... small) cannot determine $|D_U| = \frac{p+1}{2}$ directions.

As we have seen, in AG(n, q) the largest "meaningful" point sets are of size q^{n-1}. Suppose that we have a slightly smaller pointset $|U| = q^{n-1} - \varepsilon$. A *stability result* says that in such a case one can find the "missing" $|U_0| = \varepsilon$ points such that $U \cup U_0$ together determines the same directions as U did.

Exercise. Let $U = \{P_i = (a_i, b_i) : i = 1, ..., q-1\}$ be a set of $q-1$ points in the plane, given by their coordinates. Find the "missing" point $P_q = (a_q, b_q)$ such that $U \cup \{P_q\}$ together determines the same directions as U did. **Hint:** try $P_q = (-\sum a_i, -\sum b_i)$.

Theorem. Let $n \geq 3$. Let $U \subset AG(n,q) \subset PG(n,q)$, $|U| = q^{n-1} - 2$. 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.

Theorem. Let $U \subset AG(3,q) \subset PG(3,q)$, $|U| = q^2 - \varepsilon$, 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 $\bar{U} \supseteq U$, $|\bar{U}| = q^2$.

The proofs and much stronger results would follow from the following.

Research problem. Show that it is a "very rare" situation that in $\mathrm{PG}(n,q)$ a hypersurface $f = 0$ with $d = \deg f > 2$ admits a hyperplane H such that the intersection of H and the hypersurface splits into d linear factors, i.e. $(n-2)$-dimensional subspaces (Totally Reducible Intersection, TRI hyperplane). We conjecture the following.

Conjecture. 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" (maybe ≤ 45 but any bound is welcome) or F is a cone with a low dimensional base.

The direction problems have many applications in other parts of mathematics.

Let $G = \mathbb{Z}_p \times \mathbb{Z}_p$ (we are going to use the additive notation) and suppose that $G = A + B$ with $A, B \subset G$, $(0,0) \in A, B$ and for each $g \in G$ there is a unique way to write it as $g = a + b, a \in A, b \in B$. Then we say that $G = A + B$ is a *normal factorization* of G.

Theorem. In every normal factorization of $G = \mathbb{Z}_p \times \mathbb{Z}_p$, either A or B is a subgroup.

The "stability version" of this result is the following: let $G = \mathbb{Z}_p \times \mathbb{Z}_p$ and $A, B \subset G$, $(0,0) \in A, B$, $|A| > p - \varepsilon, |B| > p - \varepsilon$, where $\varepsilon \leq cp$ for a small constant c. Suppose that if for some $g \in G$ $g = a_1 + b_1 = a_2 + b_2, a_i \in A, b_i \in B$ then $a_1 = a_2$ and $b_1 = b_2$. (We may say that $A + B \subseteq G$ is a *partial normal factorization* of G.)

Problem. Show that in every partial normal factorization of $G = \mathbb{Z}_p \times \mathbb{Z}_p$, either A or B can be extended to a subgroup of order p, if $\varepsilon \leq ....$

Contributed Problems

An extremal problem on crossing vectors

by Michał Lasoń

For positive integers w and k, two vectors A and B from $\mathbb{Z}^w$ are called k-crossing if there are two coordinates i and j such that $A[i] - B[i] \geq k$ and $B[j] - A[j] \geq k$.

Problem 1. *What is the maximum size of a family of pairwise* 1*-crossing and pairwise non-*k*-crossing vectors in* $\mathbb{Z}^w$*?*

Let $f(k, w)$ denote the maximum size of such a family. In other words, $f(k, w)$ is the maximum size of an antichain in $\mathbb{Z}^w$ with no two k-crossing vectors.

Conjecture 2 (Felsner, Krawczyk, Micek 2010; cf. [1])**.** *For* $k, w \geq 1$ *we have*

$$f(k, w) = k^{w-1}.$$

It is fairly easy to construct several quite different examples of families of desired size k^{w-1}. Thus the inequality $f(k, w) \geq k^{w-1}$ is always true. The hard part is to prove the opposite. We prove the conjecture for $w \leq 3$ (for $w = 1$ it is trivial, for $w = 2$ easy, but for $w = 3$ already hard). We provide also weaker upper bounds for $w \geq 4$.

Theorem 1 ([1])**.** *For every* k *and* $1 \leq w \leq 3$ *we have*

$$f(k, w) = k^{w-1},$$

and for every k *and arbitrary* w *we have*

$$f(k, w) \leq k^w - (k - 1)^w.$$

This problem is motivated by a natural question concerning the width of the family of maximum antichains of a partially ordered set.

References

[1] M. Lasoń, P. Micek, N. Streib, T. Trotter, B. Walczak, An extremal problem on crossing vectors, to appear in Journal of Combinatorial Theory, Series A, arXiv:1205.1824

Embedding generalized quadrangles in the plane

by János Barát

Péter Maga posed a question for the Second Emléktábla Workshop, which I tried to solve with Zoli Nagy and Dave Pritchard.

Problem Characterize the graphs whose vertices can be mapped into different points of the plane in such a way that any $k > 2$ points are collinear if and only if the corresponding vertices form a clique.

In the aftermath, we ran into a few interesting open problems about embeddability of generalized quadrangles. I would like to resuscitate our efforts and list these questions.

A generalized quadrangle is an incidence structure that satisfies certain axioms [1]. A generalized quadrangle with parameters (s, t) is often denoted by $GQ(s, t)$.

The smallest non-trivial generalized quadrangle is $GQ(2, 2)$. It is usually depicted with curly lines in the plane. However, it has a straight-line representation in the real plane, probably first proved in [2]. There are two GQ of order three: $Q(4, 3)$ and its dual $W(3)$.

Problem The smallest example not admitting a real embedding in 3-space is $Q(4, 3)$. It may not have a realization in the plane either, but I cannot prove this.

Problem The generalized quadrangle $W(3)$ cannot be embedded in 4-space, but can one realize it in (3-space or) 2-space?

References

[1] S. E. Payne and J. A. Thas. Finite generalized quadrangles. Research Notes in Mathematics, 110. Pitman (Advanced Publishing Program), Boston, MA, 1984. vi+312 pp retrieved from cage.ugent.be/∼ bamberg/FGQ.pdf

[2] J.A. Thas and H. Van Maldeghem, Generalized quadrangles weakly embedded in finite projective space, J. Statistical Planning and Inference 73 (1998), 353–361.

Problem 38 from Peter Cameron's collection

due to R. A. Bailey, suggested by Tamás Héger

Let A be an affine plane of order q. Is it possible to find, for each point x of A, a permutation p_x of the set of parallel classes of A with the properties

1. for all x, p_x is a derangement (a fixedpoint-free permutation);

2. for all distinct x, y, if the line xy lies in parallel class C, then Cp_x is different from Cp_y?

There is no solution for $q = 2$, since there are only two derangements and four points. For $q = 3$, there is a solution. It is conjectured that a solution exists for all larger q.

Turán's problem for vector spaces

by Zoltán Lóránt Nagy and Balázs Patkós

A well-known problem of Turán is the following: given $k < l < n$ what is the maximum number $t = t(k, l, n)$ of k-subsets $F_1, F_2, \ldots, F_t$ of $[n] = \{1, 2, \ldots, n\}$ such that for every l-subset L of $[n]$ there exists a k-subset $K \subset L$ that is not equal to any F_i, $i = 1, 2, \ldots, t$. Even determining the asymptotics of $t(3, 4, n)$ is known to be a hard problem open for more than 50 years.

We propose the q-analog of the above problem for which even less is known (as for subsets, fairly much is known about the case $k = 2$): let V be an n-dimensional vector space over the finite field $\mathbb{F}_q$. What is the largest size that a family $\mathcal{F}$ of k-subspaces of V can have with the property that for any l-subspace U of V at least one k-subspace G of U is not in $\mathcal{F}$. There are sporadic results for small values of k, l, n or when k grows with n. We are interested in the q-Mantel problem of determining

$$\lim_{n\to\infty} \frac{t_q(2, 3, n)}{\begin{bmatrix} n \\ 2 \end{bmatrix}_q}.$$

A family of 2-spaces with the above property is $\begin{bmatrix} V \\ 2 \end{bmatrix} \setminus \begin{bmatrix} U \\ 2 \end{bmatrix}$ where U is any $(n-1)$-subspace of V. Does there exists an infinite sequence of n for which there is a better (i.e. larger) construction?

Can we sometimes define the parity of a set?

by Dömötör Pálvölgyi

Suppose that $\binom{n}{k}, \binom{n-1}{k-1}, \ldots, \binom{n-k+1}{1}$ are all even. (This happens for example if $k = 2^\alpha - 1$ and $n = 2k$.) In this case, can we select $\binom{n}{k}/2$ sets of size k from an n element set such that any $i < k$ elements are contained in exactly $\binom{n-i}{k-i}/2$ of the selected sets?

This would be somekind of parity for the sets. If true, I am also interested in the natural generalization for $p \neq 2$ to define some $\mod p$ of a set.

As I have learned from Peter Dukes, this question is almost the same as the "Halving conjecture" of Reza Khosrovshahi. You can find his survey with B. Tayfeh-Rezaie titled Trades and t-designs here: `http://math.ipm.ac.ir/combin/publications/files/2009/PA0900076.pdf`