PROBLEM SESSION

1ST GAPCOMB WORKSHOP
JUNE 2019

Open problems presented at the 1st GapComb Workshop, Campelles, June 2019.

(1) (Simeon Ball) A CONJECTURE CONCERNING QUADRICS

Let $\mathrm{PG}(k-1,\mathbb{F})$ denote the $(k-1)$-dimensional projective space over the field $\mathbb{F}$. If U is a subspace of quadrics defined on $\mathrm{PG}(k-1,\mathbb{F})$, let $V(U)$ denote the set of points of $\mathrm{PG}(k-1,\mathbb{F})$ which is the intersection of all the quadrics in U.

The following theorem is due to Castelnuovo from 1889.

Theorem 1. *Let X be a set of 11 points of $\mathrm{PG}(4,\mathbb{F})$ any five of which span the whole space. Let U be the subspace of quadrics which are zero on X. If $\dim U \geqslant 6$ then the projection of $V(U)$ from any 2 points of $V(U)$ is contained in a conic.*

In 1894 Fano proved the following theorem

Theorem 2. *Let X be a set of 13 points of $\mathrm{PG}(4,\mathbb{F})$ such that the dimension of the space of quadrics which are zero on a subset of X depends only on the size of the subset and is independent of the subset. Let U be the subspace of quadrics which are zero on X. If $\dim U \geqslant 5$ then X is contained in a one-dimensional algebraic variety of degree at most 5.*

I think the following is true, which would be a strengthening of Fano's theorem.

Conjecture 3. *Let X be a set of 13 points of $\mathrm{PG}(4,\mathbb{F})$ any five of which span the whole space. Let U be the subspace of quadrics which are zero on X. If $\dim U \geqslant 5$ then the projection of $V(U)$ from any point of $V(U)$ is contained in the intersection of two linearly independent quadrics.*

Here is a linear algebra proof of Theorem **??**.

Proof. After a suitable change of basis, we can suppose that the canonical basis $\{e_1,\ldots,e_k\} \subseteq X$ and let $V = X \setminus \{e_1,\ldots,e_k\}$.

Let C be a basis for a 6-dimensional subspace of the space of quadrics that are zero on X.

Let $\mathrm{M} = (m_{ij})$ be the 6×6 matrix whose rows are indexed by the elements of C, whose first 3 columns are indexed $X_1,\ldots,X_3$ and whose next 3 columns are indexed by X_iX_j, where $i,j \in \{1,\ldots,3\}$ and $i<j$. The row-column entry, where

the row is indexed by the quadric

$$q(X)=\sum_{1\leqslant i<j\leqslant 5} a_{ij}X_iX_j$$

is defined as

$$a_{i4}X_4+a_{i5}X_5$$

for the first $i=1,\ldots,3$ columns and a_{ij} for the remaining columns.

Let $x=(x_1,\ldots,x_5)$ be a point in the intersection of all the quadrics in C. Then

$$\mathrm{M}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_1x_2 \\ x_1x_3 \\ x_2x_3 \end{pmatrix}=vx_4x_5,$$

where v is the vector whose coordinates are indexed by the quadrics in C and whose coordinate indexed by $q(X)$ has entry $-a_{45}$.

We can solve for x_i $(i=1,2,3)$ and x_ix_j $(i,j=1,2,3,\ i<j)$ by Cramer's method, defining M_i to be the matrix obtained by from M by replacing the column indexed by x_i by v and M_{ij} to be the matrix obtained by from M by replacing the column indexed by x_ix_j by v.

Thus,

$$(\det \mathrm{M})x_i=x_4x_5\det(\mathrm{M}_i)$$

and

$$(\det \mathrm{M})x_ix_j=x_4x_5\det(\mathrm{M}_{ij}).$$

If $\det(\mathrm{M})(x)=0$, for some $x\in V$, then there is a linear combination of the quadrics in C which is a quadric

$$(x_5X_4-x_4X_5)(d_1X_1+\cdots+d_3X_3)=d_4X_4X_5,$$

for some $d_1,\ldots,d_4\in\mathbb{F}$. Since x is a zero of this quadric and $x_4x_5\neq 0$ we have that $d_4=0$, which implies that in the space of quadrics spanned by C there is a hyperplane pair (reducible) quadric. However, the set X is not contained in a hyperplane pair quadric, which is a contradiction. Observe that this implies that $\det(\mathrm{M})(X_4,X_5)$ is not identically zero.

Similarly, if $\det(\mathrm{M})(X_4,0)=0$ then there is a linear combination of the quadrics in C which is a quadric

$$X_5(d_1X_1+\cdots+d_3X_3+d_4X_4),$$

for some $d_1,\ldots,d_4\in\mathbb{F}$, again contradicting the fact that C does not contain a hyperplane pair quadric.

As a homogeneous polynomial in $X=(X_4,X_5)$, the determinants are non-zero and have degree

$$\deg(\det \mathrm{M})=3\ \ \deg(\det \mathrm{M}_i)=4 \text{ and } \deg(\det \mathrm{M}_{ij})=3.$$

Note that we have also proved that the degree of $\det \mathrm{M}$ in X_4 is also 3.

From this we deduce that, for x in the intersection of all the quadrics in C, x is a zero of

$$X_4 X_5 \det(\mathrm{M}_i)\det(\mathrm{M}_j) - \det(\mathrm{M})\det(\mathrm{M}_{ij}),$$

which is a homogeneous polynomial in (X_4, X_5) of degree 6.

This polynomial has a zero $(X_4, X_5) = (a_4, a_5)$ for every $a = (a_1, \dots, a_5) \in V$. Assuming $|X| \geqslant 12$, we have that $|V| \geqslant 7$. Moreover, the pairs (a_4, a_5) are distinct for distinct points in V. Therefore, the polynomial above is identically zero.

We have already proven that $\det(\mathrm{M}) \not\equiv 0$ and $\gcd(X_4X_5, \det(\mathrm{M})) = 1$.

Therefore, for one of i or j, $i = 3$ say the degree of $r = \gcd(M_i, \det(\mathrm{M}))$ is 2 and dividing out by this

$$\frac{(\det \mathrm{M})}{r} x_3 = x_4 x_5 \frac{\det(\mathrm{M}_3)}{r}$$

is a conic degenerate at $\{e_1, e_2\}$, which is in U. Thus, the projection of $V(U)$ from $\{e_1, e_2\}$ is contained in a conic. Likewise, at least one of the projections from either $\{e_1, e_3\}$ or $\{e_2, e_3\}$ is also contained in a conic. Simlarly at least one of the projections from either $\{e_1, e_4\}$ or $\{e_2, e_4\}$ is also contained in a conic. So many projections from two points onto a conic implies that $V(U)$ is contained in a normal rational curve and so the projection of X from any 2 points of X is contained in a conic.

□

To prove Conjecture **??** in the same way we get a 5×6 matrix M and a system of equations we can solve using Gaussian elimination. It gets more complicated but the idea is to reduce everything again to a polynomial in just X_4 and X_5 which doesn't have too high a degree. Assuming X to be large enough this polynomial will be identically zero. From there, using the divisions that this implies prove that this implies a factor in the larger degree curves constructed in X_3, X_4 and X_5.

(2) (Guillem Perarnau) Can colourings be far apart from each other?

Let G be a graph on n vertices and maximum degree Δ. Let $\Omega_k(G)$ be the set of proper k-colourings of G. Define the *recolouring graph* $\mathcal{C}_k(G)$ with vertex set $\Omega_k(G)$ where two colourings are adjacent if they only differ at exactly one vertex. The structural graph properties of $\mathcal{C}_k(G)$ are key to understand the performance of sampling algorithms for colourings (e.g. Glauber dynamics).

For $k \geq \Delta + 2$, it is easy to show that $\mathcal{C}_k(G)$ is connected and the proof implies that $\mathrm{diam}(\mathcal{C}_k(G)) = O(n)$, where constants depending on Δ are hidden in the asymptotic notation. Obviously, $\mathrm{diam}(\mathcal{C}_k(G)) \geq n$ for any graph G, as there exist two colourings that do not agree on any vertex (take a colouring and permute cyclically the colours).

So let us focus on the case $k = \Delta + 1$. In this case, $\mathcal{C}_{\Delta+1}(G)$ (from now on just $\mathcal{C}$) may not be connected due to the so called *frozen colourings*. Johnson, Feghali and Paulusma showed that $\mathcal{C}$ is composed of a single non-trivial component $\mathcal{C}_0$ and many isolated colourings. Their proof implies that $\mathrm{diam}(\mathcal{C}_0) = O(n^2)$.

Question 4 (Bonamy, Bousquet, P.). *For $\Delta \geq 3$, does there exist c_Δ and a sequence of Δ-bounded-degree graphs $(G_n)_{n\geq 1}$ where G_n has n vertices such that $diam(\mathcal{C}_0) \geq c_\Delta n^2$?*

For $\Delta = 2$, the answer is yes and the proof is simple and very nice, I'll show it to you!

(3) (Guillem Perarnau) ROUGH ENUMERATION OF PLANAR-LIKE GRAPHS.

Fix an integer $d \geq 1$. Let $\mathcal{G}_{d,n}$ be the class of $(d+1)$-regular $(d+1)$-edge-coloured graphs on $\{1, \dots, n\}$ such that the graph induced by any triplet of colours is planar.

We are interested in rough estimates of $G_{d,n} = |\mathcal{G}_{d,n}|$, in particular we want to determine its factorial growth rate. This quantity is related to the number of triangulated d-manifolds, which are central in the study of quantum gravity.

Define

$$\beta_d = \limsup_{n\to\infty} \frac{\log(G_{n,d}/n!)}{n \log n}$$

Clearly $\beta_d \geq 0$. As there are at most n^n planar 3-edge-coloured graphs, we have $\beta_d \leq d/3 - 1$, Moreover, β_d is increasing in d. Together with Chapuy, we proved $\beta_3 = 1/6$ and for $d \geq 4$

$$\frac{1}{6} \leq \beta_d \leq \frac{d-2}{6} \,.$$

Question 5 (Chapuy, P.). *What is the correct asymptotic behaviour of β_d?*

(4) Juanjo Rué SUMS AND DIFFERENCES

The following problem fits in the area of additive combinatorics. Let A be a set of positive integers. We denote by $A(n)$ the subset of elements in A smaller or equal than n. We denote by $A+A = \{a+a' : a, a' \in A\}$ and $A-A = \{a-a' : a, a' \in A\}$. The main general problem is to study the cardinality of $A+A$ with respect to $|A-A|$.

In fact, it is proven that a positive proportion of sets in $[n]$ satisfies the three properties, namely $|A+A| > |A-A|$, $|A+A| < |A-A|$ and $|A+A| = |A-A|$. Results for random sets in $[n]$ are also obtained. We want to go through this in a more precise way:

Question 1: study (if any) the existence of limiting distributions for $|A+A|$ and $|A-A|$ in different random models.

Also, many interesting questions can be stated in the infinite setting:

Question 2: is it possible to build an infinite set A such that for infinitely many n, $|A(n) + A(n)| > |A(n) - A(n)|$?

(5) (Oriol Serra) THE DICKS–HAMIDOUNE–IVANOV CONJECTURE

Given finite sets A, B in a group its Minkowski product is $AB = \{ab : a \in A, b \in B\}$. In torsion–free groups and in finite groups of prime order the Cauchy–Davenport inequality

$$|AB| \geq |A| + |B| - 1,$$

holds. In linearly ordered groups there is always one element which can be written in a unique way in AB. Disproving a conjecture by Kemperman, nontrivial examples in general groups where there is no element with unique expression in AB where shown to exist. This brings the question of giving a lower bound for the number of elements which can be written in at least t ways in AB. We denote by

$$A \cdot_i B = \{g \in G : r_{A,B}(g) \geq i\},$$

where $r_{A,B}(g)$ denotes the number of representations of g in AB (as an ordered product in the nonabeleian case). We abbreviate $A \cdot_1 B = AB$. Pollard proved

Theorem 6 (Pollard)**.** *Let A, B be finite subsets of $\mathbb{Z}/p\mathbb{Z}$. For each positive integer r,*

$$|A + B| + |A +_2 B| + \cdots + |A + \cdot_r B| \geq r \cdot \min\{p, |A| + |B| - r\}.$$

Grynkiewicz extended the above theorem to general abelian groups (extending the Theorem of Kneser) and Nazariewicz, O'Brien, O'Neill and Staples characterized the extremal sets for Pollards' s theorem (which are essentially pairs of arithmetic progressions with a common difference). Inspired by a problem by Dicks and Ivanov, Hamidoune formulated the following conjecture.

Conjecture 7. *Let A, B be finite subsets of a group G, $|A|, |B| \geq 2$. Let $H < G$ be the largest subgroup such that $A \cdot_2 B$ contains a full coset of H. Then*

$$|AB| + |N_2(A, B) \geq 2(|A| + |B| - \max\{2, |H|\}.$$

Dicks–Ivanov proved that

$$|AB| + |N_2(A, B) \geq 2 \min\{|A| + |B| - 2, |H|\},$$

where the minimum runs over all subgroups $H < G$ such that $|H| \geq 3$.

The result of Grynkiewicz proves the above conjecture for abelian groups. A simpler proof was given by Hamidoune, which 'only' fails to extend to all groups when $|A \cap B| \geq 2$ and $A \subsetneq AB$

(6) (Oriol Serra) Generating Random Latin Squares

The tight structure of Latin Squares has posed a problem related to random generation of these objects. One of the first attempts was proposed by McKay and Wormald and was followed by a Markov chain approach by Jacobson and Mattews in the context of random generation of contingency tables.

In 2017 Dotan and Linial suggested a new simpler approach to the random generation of symmetric Latin squares by using a Metropolis algorithm. The authors suggest several variations of the algorithms and describe some statistical behavior for small values of n. The simplest procedure they suggest consists in generating proper edge colorings of complete graphs K_n with n even (which provide symmetric Latin Squares). Consider the space $\mathcal{C}_n$ of all colorings of the edges of K_n with $n-1$ colors. For each $C \in \mathcal{C}$ we denote by $a_{i,x}(C)$ the number of edges indicent with $x \in [n]$ colorred with i. Define a potential

$$\phi(C) = \sum_{x\in[n]} \sum_{i=1}^{n-1} a_{x,i}(C).$$

Therefore $n(n-1) \leq \phi(C) \leq n(n-1)^2$ and the lower bound holds if and only if C is proper. Let $\mathcal{G}_n$ be the directed graph with vertex set $\mathcal{C}_n$ and a coloring C is adjacent C' if C and C' they differ precisely on the color of one single edge and $\phi(C') \leq \phi(C)$. Then a simple random walk on $\mathcal{G}_n$ is performed. The simplest conjecture they pose is the following one.

Conjecture 8. *The above random walk converges a.a.s. to a proper coloring. Moreover the expected time of convergence is $O(n^4)$.*

The first part of the conjecture amounts to proving that the graph $\mathcal{G}_n$ is strongly connected. There are colorings such that all neighbours have the same potential function, and the question is that such stable colorings can not form a connected compoment. In her Master Thesis, Julia Calatayud proved the conjecture for $n = 6$ and $n = 8$. It looks that the answer should be positive.

(7) (Dimitrios Thillikos) Structure of the Connectivity Core Decomposition Tree of a graph

Degree degeneracy. We define

$$\delta(G) = \min\{\mathsf{deg}_G(v) \mid v \in V(G)\}$$

and we also define the *degree-degeneracy* of G as

$$\delta^*(G) = \max\{\delta(H) \mid H \text{ is a subgraph of } G\}.$$

Let $d = \delta^*(G)$. The (degree) core decomposition of G is the sequence $\mathcal{C}(G) = \{C_0, \ldots, C_d\}$ where C_i is the vertex set of the *i-core* of G, defined as the maximal subgraph H where $\delta(H) \geq i$.

Connectivity degeneracy. Given a $X \subseteq V(G)$ where $0 < |X| < |V(G)|$, we set

$$\mathsf{cut}(X) = |\{\{x, y\} \in E(G) \mid x \in X \text{ and } y \in V(G) \setminus X\}|.$$

Given a graph G, where $|V(G)| \geq 2$,

$$\lambda(G) = \min\{\mathsf{cut}_G(X) \mid X \subseteq V(G) \text{ and } 0 < |X| < |V(G)|\},$$

while in the special case where $|V(G)| \leq 1$, we set $\lambda(G) = \infty$. We define the *connectivity degeneracy* of a graph G as

$$\lambda^*(G) = \max\{\lambda(H) \mid H \text{ is a subgraph of } G\}.$$

It is known that $\delta^*(G) \leq \lambda^*(G) \leq 2\cdot\delta^*(G)$. Both $\lambda^*(G)$ and $\delta^*(G)$ can be computed in polynomial time, however, only $\delta^*(G)$ has, so far, a linear time algorithm.

Connectivity core decomposition tree. The *k-connectivity partition* of G the partition $\mathcal{P}_k(G) = \{X_1, \ldots, X_\ell\}$ of $V(G)$ such that each X_i is a vertex maximal subset of $V(G)$ such that $\lambda(G[X_i]) \geq k$. This partition is uniquely defined.

It also holds that if $k \geq k'$ then $\mathcal{P}_k(G)$ is a refinement of $\mathcal{P}_{k'}(G)$. Let $\ell = \lambda^*(G)$. Notice that $\mathcal{P}_0(G) = \{V(G)\}$, while $\mathcal{P}_d(G)$ consists of singletons consisting of all the vertices of G. The *connectivity core decomposition tree* of G is a $d+1$-level rooted tree $\mathcal{T}_G$ where each level has as vertices the sets in $\mathcal{P}_k(G)$ for each $k \in \{0, \ldots, d\}$ and where there is an edge from a set $X \in \mathcal{P}_i(G)$ to a set $Y \in \mathcal{P}_{i+1}$ when $Y \subseteq X$. Notice that the root of this tree is $V(G)$ and the leaves are the singletons in $\mathcal{P}_d(G)$.

Question: Due to experiments on graphs emerging from real data sets, it appears that $\mathcal{T}_G$ is typically not far away from a path. Is there any theoretical base on this? Or it is a particularity of the data sets?

(8) (Lluís Vena) Maximal number of edge-disjoint triangles in a graph such that no additional triangle is created.

The maximal configurations known come from sets free of 3 arithmetic progressions.

If A is a set free of 3–AP in $[n]$, then one can create a graph on $[6n]$ vertices with $|A|n$ edge–disjoint triangles and where the total number of triangles is also $|A|n$.

This allows to show that the number of edges-disjoint triangles is at least from the order $|V|^{2-o(1)}$.

Using the triangle removal lemma, one concludes that the upper bound is of the similar type, but where the difference of the two little o's is substantial.

Open problem: reduce the gap.

(have heard talking about it to Rödl)

(9) (Lluís Vena) 'Compactification' of the set of sequences.

Let $S = \{f : N \to R^{>0}\}$ be the set of sequences of real numbers.

Consider the order $<$ such that

$$f < g \Leftrightarrow \lim_{i\to\infty} f(i)/g(i) \text{ exists and is between 0 and 1}$$

(think better as 0)

Does there exists a set $A \subset S$, totally ordered with respect to $<$, such that, for any other $s \in S$, there exists an infinite set of indices I and $a \in A$ such that

$$\lim_{i\to\infty, i\in I} s(i)/a(i) = 1$$

Ideally, one would like to be able to do this when s is an infinite subsequence as well.

A should be a maximally, totally ordered set. Possibly one needs to assume other axioms beyond ZFC, such as continuum hypothesis.

(10) (Enric Ventura) IS THERE AN ALGORITHM TO COMPUTE THE STABLE IMAGE OF AN ENDOMORPHISM OF A FREE GROUP ?

Discussion: Let F be a finitely generated free group and let g be an endomorphism of F, given by the images of a free basis of F. The stable image of g, denoted $Im(g^\infty)$, is defined as the intersection of $Im(g^n)$ for all $n > 0$. It is known that this stable image is always finitely generated (in fact, with rank bounded by that of F). The problem consists on computing a free basis for $Im(g^\infty)$ from the given g.

One can easily compute recursively the Stallings graph (and so a free basis) for $Im(g)$, $Im(g^2)$, $Im(g^3)$, etc. And it is not difficult to see that the Stallings graph for $Im(g^\infty)$ is a subgraph of $Im(g^n)$ for some big enough n. What remains is to be able to decide how tall must we go up this tower of graphs and, whence there, how to choose the appropriate subgraph (out of the finitely many ones).

Inspecting the example $a \mapsto a^2, b \mapsto b$, (with $Im(g^\infty) =< b >$), it seems that the problem is about detecting which parts of the graph grow to infinite, and cut them in finite time. Maybe the problem is related to the foillowing question: can we define a dynamic notion of stable image including the points at infinity ? (in the previous example, this extended stable image should be something like "$< b, a^\infty >$".

The answer to this problem has a direct application: the computability of the fixed subgroup of arbitrary endomorphisms (the corresponding problem for automorphisms has been solved making strong use of train track techniques).