PhD projects

Misha Rudnev

March 9, 2012

General area: Geometric/arithmetic combinatorics, geometric incidence theory, geometric measure theory.

Description of possible PhD projects

This document may appear somewhat vague. It mostly contains my general research interests an ambition for the near future, in view of some exciting developments that this research are has seen lately. A person who shares these interests and wishes to do a PhD with me is free to choose any aspect of these or try to synthesize something of their own.

The term *combinatorics* rarely appears in modern mathematical literature without an additional appellation. *Geometric* combinatorics usually refers to a growing body of mathematics concerned with counting properties of arrangements of a large number of geometric objects in space. *Arithmetic* combinatorics, a closely related and active area of research, deals with combinatorial estimates associated with the arithmetic operations (addition, multiplication and their inverses) in groups, rings and fields. The wealth of tools used in both geometric and arithmetic combinatorics, ranging from elementary counting arguments and graph theory to harmonic analysis, probability, ergodic theory, algebraic geometry, etc., accounts for their remarkable wealth of perspective.

Arithmetic and geometric combinatorics interact with one another by way of formulating the former's questions as *incidence* problems: one has a set of geometric objects X of some type and a set of points P in some space, and asks for the bound on the cardinality of the set of incidences $I = \{(p,x) : p \in x\}$, in terms of the cardinalities $|L|, |P|$. *Incidence theory* constitutes one of my core research interests. In a notable case the space is a projective plane and the sets are straight lines. If the plane is Euclidean then a sharp incidence bound is given by the famous Szemerédi-Trotter theorem (1981).

Szemerédi-Trotter theorem. *For any point set P and any line set L in $\mathbb{R}^2$, the total number of incidences*

$$|I(L,P)| \ll \left(|L| + |P| + (|L||P|)^{\frac{2}{3}}\right). \tag{1}$$

All the known proofs of the Szemerédi-Trotter theorem rely heavily on the order property of the reals. If the plane is defined over a finite field, then basically all that is known about non-trivial geometric incidence theory therein is that it exists. This fact follows from a rather awkward backward conversion of the arithmetic sum-product estimates discussed below into geometric incidence statements. Mechanisms for such conversion have been developed by Bourgain, Katz, and Tao in 2003, and more recently myself and Helfgott (2011) and Jones (2011), my PhD student. However, creating a *genuine* geometric incidence theory over a finite plane is a recognised and challenging open problem, of great appeal to me.

The two other catchwords to highlight my current and anticipated research are two classical problems: the *Erdős distance problem* (1946) and the *Erdős-Szemerédi, or sum-product* problem (known as such since ≈ 1983), as two key examples of the general *growth*, or *expander* phenomenon in combinatorics[1].

The Erdős distance conjecture in $\mathbb{R}^2$, claiming that N points in the plane determine at least $|N|^{1-o(1)}$ distinct distances was triumphantly resolved in the end of 2010 by Guth and Katz. What remains is the case of higher dimensions $d \geq 3$ (proving that there are at least $|N|^{\frac{2}{d}-o(1)}$ distinct distances; the case $d = 3$ being not unrelated to crystallography) as well as stronger versions of the statement, such as the *pinned* one: does there exist a point wherefrom $|N|^{\frac{2}{d}-o(1)}$ distances are realised? Curiously enough, the whole range of incremental results towards proving the conjecture, which would step-by-step vindicate exponents closer and closer to one (although without much hope of finally getting there), eventually some .86, largely apply to pinned distances. But the Guth-Katz theorem as it is fails to tell anything about pinned distances. On the other hand, the recent developments have created ground for cautious optimism that these questions maybe much closer to their nearly full resolution than it appeared just a few years ago. My recent work with Iosevich and Roche-Newton (my PhD student) took up on the ideas of Guth and Katz and solved another "hard Erdős problem": any set of N vectors in the Euclidean plane determines $\gg |N|^{1-o(1)}$ distinct dot products. Therefore, *I would really like to see pinned versions of the two results to be proven, but have no idea how this can be done.*

[1] A particular example of *growth* in the Euclidean plane is the Beck theorem (1983). *Given N points in the plane, either their positive proportion is supported on same straight line, or distinct pairs of points generate $\gg N^2$ distinct straight lines.* Beck's theorem follows from the Szemerédi-Trotter theorem.

Sum-product estimates, alias Erdős-Szemerédi conjecture, constitute a major open question in arithmetic combinatorics. The original conjecture is that for any finite set A of integers, the cardinality of the set of all sums or products (denoted respectively by $A+A$ and $A\cdot A$) generated by pairs of elements of A is almost as great as the cardinality of A, squared. That is:

$$\max(|A+A|,\, |A\cdot A|) \gg |A|^{2-o(1)}. \tag{2}$$

Today, the question is primarily asked in the context of reals $A\subset\mathbb{R}$ (as well as the complex field $\mathbb{C}$) or the prime residue field $A\subset\mathbb{F}_p$, with p large and $|A|$ sufficiently small relative to p (usually $|A|<\sqrt{p}$). Today's standing "world record" for $A\subset\mathbb{R}$ is due to Solymosi (2008), who proved (2) with the exponent $\frac{4}{3}$ instead of 2. The best known exponent for $A\subset\mathbb{C}$ is $1+\frac{19}{69}$, proved in my recent work. In $\mathbb{F}_p$, due to the lack of the notion of order, the best known exponent is substantially worse: $\frac{12}{11}$, proved in my other 2011 paper. Previously known estimates had developed from $1+\epsilon$ in 2003 by Bourgain, Katz, Konyagin, and Tao to $\frac{13}{12}$ by Bourgain and Garaev in 2008. There is an easy counterexample of Bourgain that in the $\mathbb{F}_p$ case, with $|A|\sim\sqrt{p}$ showing that the exponent in (2) can not exceed $\frac{3}{2}$. This counterexample, however, does not rule out a weaker form of (2):

$$|A+A|\cdot|A\cdot A| \gg |A|^{3-o(1)}.$$

I do not know how the current state-of-the art can be improved. The breakthrough by Guth-Katz has also raised expectations, and anything short of resolving the conjecture completely may be scoffed at by some people. However, making any further progress in this direction, as far as I am concerned, is interesting.

The two classical problems above are examples of the general *expander* concept, introduced in their context by Bourgain around 2005. In both cases, given a set of reals A, there is a function of four variables in A, which would return at least $|A|^{2-o(1)}$ distinct values. Much less is known about expanders with fewer variables. Garaev and Shen proved, for instance, that $f(a,b)=ab+a$ will return at least $\gg|A|^{\frac{5}{4}}$ values for a real A and $\gg|A|^{\frac{106}{105}}$ values for a small enough $A\subset\mathbb{F}_p$. (Tim Jones seem to know how to improve these exponents a little bit.) *However, finding and estimating some new expanders would be a nice thing, especially if one can come up with a really good estimate. One interesting function may be* $f(a,b)=a+\frac{1}{b}$.

Expander problems require an underlying algebraic *field structure*, which sets them apart from purely *additive combinatorics*. The latter subject has experienced an explosive development after Ruzsa gave his new proof of the celebrated Freiman theorem in 1994, and Gowers his new proof of the Szemerédi theorem in 1998, and whose holy grail today is the Polynomial Freiman-Ruzsa conjecture. The striking theorem of Green and Tao about arithmetic progressions in primes is partially based on Gowers' work. Altogether, these powerful ideas have generated an impressive body of work, which has not thinned out as of today, one fundamental innovation being, e.g. a well-known 2010 paper by Croot and Sisask. Much of this work has not unexpectedly come from Cambridge (Gowers, Green, Sanders). *I have read the original work and gave some lectures about these problems, but here my expertise ends. However, I would be very much interested to get involved, in case there is an ambitious and independent PhD student who will be willing to enter this field more deeply and take me on board.*

The situation in *field combinatorics* today may be somewhat reminiscent of what was happening in additive combinatorics in the late 1990s. In the end of the first decade of this century two events shook the area. In 2008 Dvir resolved the Kakeya conjecture over finite fields. And in 2010 Guth and Katz, relying heavily on the polynomial method used by Dvir, settled the Erdős distance problem in the Euclidean plane. One principal geometric component used by Guth and Katz came from a half-a-year earlier work of Elekes and Sharir where they gave a "Kleinian geometry" reformulation of the distance problem in $\mathbb{R}^2$ as a point-line incidence problem in $\mathbb{R}^3$ and conjectured an incidence theorem in $\mathbb{R}^3$. Guth and Katz succeeded in proving that theorem by using a cell decomposition method furnished by the Polynomial Ham Sandwich Theorem by Stone and Tukey (1942), a corollary of the famous Borsuk-Ulam theorem in algebraic topology.[2] It quickly became clear that these ideas have further applications, and in 2011 Solymosi and Tao and then Zahl established several earlier unaccessible higher-dimensional

[2] The Borsuk-Ulam theorem was no stranger to geometric combinatorics before the work of Guth and Katz: a whole monograph of Matoušek (Springer, 2003) is dedicated to it. But it was not until 2008 that Guth demonstrated the power of its corollary, the polynomial Ham Sandwich theorem. Combined with the polynomial method used by Dvir to prove the finite field Kakeya conjecture, it enabled Guth (2008) to settle the hard endpoint case of the multi-linear Kakeya problem.

Szemerédi-Trotter-type incidence theorems, and myself and collaborators proved what can be regarded as the first sharp-to-endpoint sum-product inequality of Erdős-Szemerédi type over $\mathbb{R}$:

$$|A \cdot A + A \cdot A| \gg |A|^{2-o(1)}. \tag{3}$$

Most recently, Jones (my PhD student) has produced a similar in spirit result for cross-ratios of quadruples of points on the projective line. His result may appear, in fact, stronger: the cross-ratios are pinned at zero, namely he gets what is a *three-variable expander* as follows:

$$\left|\left\{\frac{a(b-c)}{c(a-b)} : a,b,c \in A\right\}\right| \gg |A|^{2-o(1)}.$$

His result, however, does not use the Guth-Katz theorem and there is no evidence that the power 2 cannot be, in fact, replaced by 3. Roche-Newton (also my PhD student) succeeded in essentially swapping addition and multiplication in the inequality (3), having thus made another important step towards the Erdős-Szemerédi conjecture. Both estimates are sharp up to the endpoint.

The polynomial method, whose essence is to judge about the size of a discrete set by studying polynomials which have zeroes on this set is not new: it goes back at least as far as Hilbert's *nullstellensatz*. In the 1970s it made way into number theory as *Stepanov's method*, having enabled transparent proofs of some classical exponential sum bounds, which had earlier been accessible by means of advanced algebraic geometry only. It was brought into additive combinatorics by Alon and collaborators in the 1990s, where it allowed for extremely elegant proofs of, e.g., the classical Cauchy-Davenport theorem and Erdős-Heilbronn conjecture by Alon, Nathanson, and Ruzsa in 1995. In 2000 Heath-Brown and Konyagin used the Stepanov method to prove spectacular (and I believe yet to be generalised) results about additive properties of multiplicative subgroups in $\mathbb{F}_p$. Altogether on many occasions arithmetic combinatorics has proved to be very successful, dealing with classical number theory problems.

Elekes and Sharir (2010) essentially pioneered a Kleinian geometry approach to geometric combinatorics. Its main paradigm is to interpret a geometric combinatorics question in terms of the action of an underlying classical symmetry group on the space where the original question has been posed. I regard this geometric paradigm, together with the powerful analytic tool, the polynomial method, as a genuine breakthrough, which together have furnished a new language, fit for describing the whole class of "hard Erdős problems" which owe the epithet primarily to the fact that there is very little structure in the original formulation of the problem that one can start building up on. In short, this research area has been brought to a qualitatively new level (and one cannot help feeling lucky working in it).

Pushing this language and the state-of-the-art further, extending its powers to higher dimensions in the Euclidean space, where the symmetry group geometry is much more involved is a key theme of my future research, especially the case $d = 3$. Doing this as a PhD thesis would be excellent, but the problem may be quite hard and possibly require more than trivial algebraic geometry. (For Guth and Katz, the Bezout theorem was more or less all they needed.) It appears that a more natural space to look at is the sphere S^3 rather than $\mathbb{R}^3$, and one needs to prove an incidence theorem in the group $SO(4,\mathbb{R})$, based on its action on the unit quaternion sphere. The "lines" involved are now three-dimensional, they are cosets of $SO(3)$-type subgroups of $SO(4,\mathbb{R})$, stabilising the points of the original point set on S^3.

The other key planned research direction is adaptation of the polynomial method to the $\mathbb{F}_p$-geometry. Neither the proof of the Szemerédi-Trotter, nor of the Guth-Katz theorem work in $\mathbb{F}_p^2$, due to the lack of the notion of order, compatible with the algebra of field operations. Nor can their statements be transferred verbatim. However, the polynomial method has worked beautifully in Dvir's proof of the finite field Kakeya conjecture, and part of the Guth-Katz proof is amenable to the $\mathbb{F}_p$ case.

If one wants to build an incidence theory over finite fields, I do not see an alternative to the polynomial method. The first question may be to identify at least easier incidence type problems in $\mathbb{F}_p^2$, which can be satisfactorily resolved thereby. For instance: is this true that a non-collinear set of $N \ll p$ points in $\mathbb{F}_p^2$ determines at least $N^{1-o(1)}$ distinct directions of lines drawn through pairs of distinct points? In the Euclidean case the answer is $N/2$ and has been known since the 1970s, it takes a much easier argument than the Szemerédi-Trotter theorem.[3] In the $\mathbb{F}_p^2$ case it is nearly trivial to prove that any set of $N \gg p$ points determines $\gg p$ distinct directions. Yet the case of small N appears to be much more difficult.

[3]This is a good indication of the subtlety of the matter. If the point set is $A \times A$, the fact of it generating at least $N/2$ directions yields the sum-product type inequality $\left|\frac{A-A}{A-A}\right| \geq \frac{|A|^2}{2}$. But it was not until 2012 that Roche-Newton succeeded in what can be viewed as merely replacing division by multiplication and proving that $|(A-A)\cdot(A-A)| \gg |A|^{2-o(1)}$.

The relevant aspects of finite field combinatorics per se have also experienced an influx of new techniques. One was set out in the above-mentioned 2000 paper of Heath-Brown and Konyagin. The paper applied the polynomial method to a variant of the following problem. If H is a multiplicative subgroup from $\mathbb{F}_p$, what is the minimum number of cosets of H that a single additive shift of H, is going to intersect? They succeeded in giving an apparently sharp estimate, which looks temptingly like the Szemerédi-Trotter one (1). In 2003 it was used by Konyagin to give estimates on sum-products in $\mathbb{F}_p$. However, further improvements of the prime field sum-product inequality have given up this method in favour of a subterfuge, known as *additive pivot*, introduced in a 2005 work of Bourgain, Glibichuk and Konyagin. It was not until 2011 when Shkredov and Collaborators pushed it (literally) one step further to obtain a state-of-the-art estimate on the size of the sumset of a multiplicative subgroup. Together with the aforementioned work by Konyagin, which brings multiplicative subgroups into the general context, this may be gateway towards improvement of sum-product type results over $\mathbb{F}_p$, as well as building a genuine geometric incidence theory in $\mathbb{F}_p^2$.