Final report for Ernie Croot's NSA grant (3706AK9)

January 9, 2011

1 Objectives and statement of the work

1.1 The paper with Olof Sisask

Olof Sisask and I wrote a paper titled *A Probabilistic Technique for Finding Almost-Periods in Additive Combinatorics*, which has now been accepted by *Geometric and Functional Analysis* and is scheduled to appear. Among the results in this paper is the following theorem:

Theorem 1. Suppose that A and B are subsets of $\mathbb{Z}_p$, having densities α and β, respectively. Then, $A+B$ contains an arithmetic progression of length at least

$$\exp(c(\alpha \log p/\log(2/\beta))^{1/4}),$$

where $c > 0$ is some absolute constant.

For when A and B have fairly high density – near to 1 – the theorems of Bourgain, Green, and Sanders give much stronger estimates; however, when α and β are much smaller, my theorem with Sisask gives the best bounds. Indeed, our theorem guarantees that $A + B$ has very long APs even when, say, $\alpha = 1/(\log p)^{1-\delta-\delta'}$ and $\beta = \exp(-c'(\log p)^{\delta})$, which is far beyond what other approaches have been able to deliver so far.

Furthermore, our method is very elementary, and unlike the Fourier proofs of Green, Bourgain and Sanders, extends with no additional effort to the non-abelian setting. In total, it takes only about 3 pages to prove the above theorem.

Our method also leads to a great many other results on arithmetic structures in subsets of finite groups, abelian or otherwise. Recently, for example, Tom Sanders used the ideas in our paper to prove the following result:

Theorem (T. Sanders). let $r_3(N)$ denote the size of the largest subset of $\{1, 2, ..., N\}$ having no three-term arithmetic progressions. Then,

$$r_3(N) \ \leq \ \frac{N(\log\log N)^5}{\log N}.$$

Not only are the bounds here the best to date, but also they are of the same general quality as those in $\mathbb{F}_p^n$ for fixed characteristic p and arbitrarily large dimension n. The bounds in the $\mathbb{F}_p^n$ case, first proved by R. Meshulam (who adapted Roth's 'density increment' approach to that setting), were $r_3(\mathbb{F}_p^n) < c_p p^n/n$, where c_p is a constant depending only on p and where $r_3(G)$ now denotes the largest subset of an additive abelian group G (when G is the vector space $\mathbb{F}_p^n$ we only consider the additive structure) having no non-trivial solutions to $x+y=2z$; notice that the factor c_p/n is proportional to $\log|G| = \log|p^n|$.

Also, if Sanders's result could be improved only a tiny bit, say replacing the $(\log\log N)^5$ factor with a factor of size $1/(\log\log N)^{1+\delta}$, $\delta > 0$, then it would prove the famous Erdős-Turan conjecture in the case of three-term progressions – namely, that any subset S of the positive integers such that $\sum_{s\in S} 1/s$ diverges, must necessarily have a three-term arithmetic progression.

I believe that it might be possible to modify our (mine and Olof's) methods to give further improvements to the $\mathbb{F}_p^n$ case, which perhaps then will eventually lead to improvements in the upper bound for $r_3(N)$. Olof and I are currently looking at these possibilities, and he wrote me that perhaps T. Gowers might be interested in working on it with us as well.

We also think we will be able to use it to give another proof of the existence of 2D corners in high-density subsets of the $n \times n$ grid $\{1, 2, ..., n\}^2$. Concerning corners, Shkredov has the best results on this so far – he showed that if S is a subset of the grid having at least $n/(\log\log n)^c$ elements, then it contains a triple $(x, y), (x+t, y), (x+t, y+t)$. We have some hope of either improving this constant c, or possibly replacing the $\log\log n$ with a better function (i.e. one growing to infinity faster than $\log\log n$).

1.2 Recent work on sum-product inequalities

Todd Cochrane is visiting me in the Fall of 2010 and Spring of 2011, and we have been working on sum-product inequalities in finite fields. Specifically, we have been working on the following problem:

Finite Field Waring Problem. Suppose that A is a multiplicative subgroup of $\mathbb{F}_p$ of size p^δ. Determine the smallest integer $k = k(\delta)$ such that

$$kA \;=\; A + A + \cdots + A \;=\; \mathbb{F}_p.$$

We have been trying to modify ideas due to myself and Derrick Hart on sum-product inequalities over $\mathbb{R}$, to improve upon the bound $k \lesssim 4^{1/\delta}$ due to Konyagin and Glibichuk.

Just recently we found another method (different from the Croot-Hart proof) to produce upper bonds on k that so far achieves $k < 7^{1/\delta}$, which is somewhat worse than G-K; however, we have several ideas on how to improve the method.

1.3 Polymath4

I undertook a new research project starting in the late summer of 2009, which was the Polymath 4 project to produce a deterministic algorithm to find large prime numbers efficiently. This was a "massively collaborative" online project, though I contributed several worthwhile ideas to it; in particular, I was able to prove:

Theorem 2. There exists a deterministic algorithm that given a positive integer n sufficiently large, and given polynomials $p(x), q(x) \in \mathbb{F}_2[x]$ of degrees d and e respectively, will evaluate

$$\sum_{\substack{n \le m \le n + n^{0.51} \\ m \text{ prime}}} q(x)^m \pmod{2, p(x)} \tag{1}$$

using only

$$n^{0.49}((d+1)(e+1)\log n)^{O(1)} \text{ bit operations.}$$

I have some good reasons to believe that this polynomial cannot vanish mod $(2, p(x))$ at all the places $q(x) = 1, x, x^2, ..., x^{\lfloor n^{0.49} \rfloor}$, at least if $d > (\log n)^2$ or so. If this is so, and if we could speed up the evaluation process so that all these could be done simultaneously (perhaps using FFTs somehow) using still only $n^{0.49}((d+1)(e+1)\log n)^{O(1)}$ bit operations, then it would imply the following conjecture:

Conjecture. There exists a deterministic algorithm that given a positive integer n sufficiently large, will produce a prime number exceeding n using only

$$n^{0.49+o(1)} \text{ bit operations.}$$

If the algorithm could be suitably developed to prove this conjecture, it would mean we have the fastest-running deterministic algorithm to locate prime numbers so far known to exist.

An alternative approach is to bypass this conjecture altogether, and to generalize Theorem 2 so that it works in other rings. The idea would be to have it work in a ring where only a small number of evaluations of the natural analogue of the sum suffices, in order to reach non-vanishing. One such type of ring that seems promising to consider is matrix rings. Indeed, it seems as though Theorem 2 should generalize nicely so that the sum in (1) is replaced with one where the x is some $h \times h$ matrix, and for the mod operation one just mods the entries out by 2 and by $p(x)$. There may be other rings that could be used as well. I have not yet had time to explore this possibility.

After this project was finished, I continued working on it with two undergraduates as part of an REU project. These students are David Lowry and David Hollis. Although we weren't able to solve the above conjectures, we pursued a few side projects, one of which was to find a quick way of evaluating the sum

$$\sum_{\substack{n \le m \le n+n^{0.51} \\ m \text{ prime}}} x^{m^2} \pmod{2, p(x)}.$$

quickly – in time $n^{0.49}$, say, given that $p(x)$ has degree at most $n^{o(1)}$. We were not able to succeed in solving this, but did develop a number of ideas that might lead to a solution one day.

2 Publications

- On sums and products in $\mathbb{C}[x]$ (with D. Hart), *Ramanujan J.* **22** (2010), 33-54.
- h-fold sums from a set with few products (with D. Hart), *SIAM J. of Discrete Math.* **24** (2010), 505-519.
- The structure of critical sets for $\mathbb{F}_p$ arithmetic progressions, submitted to Israel Jour. (positive referee report, revision requested)
- Sum-product inequalities with perturbation (with D. Hart, M. Hamel, and S. Backman), accepted to INTEGERS.
- A probabilistic technique for finding almost-periods in additive combinatorics (with O. Sisask), to appear in Geom. and Funct. Anal.
- On the structure of sets with few three-term arithmetic progressions, Electronic J. of Comb. **17** (2010), R128.

3 Collaborators

- Spencer Backman, an ACO (=Algorithms, Combinatorics and Optimization) student at Georgia Institute of Technology working with me this summer (more on his own than with me, though we have worked on a paper together).
- Evan Borenstein, my ph.d. student, recently finished, submitted, and defended his thesis, awaiting graduation from Georgia Institute of Technology, early Fall 2009.
- Albert Bush, my new ph.d. student at Georgia Tech.
- Nathaniel Chen, undergraduate REU (=Research Experience for Undergraduates) math major worked with me last summer.
- Todd Cochrane, professor at Kansas State University, visiting me Fall 2010 and Spring 2011.
- William Drobny, also an undergraduate REU math major.

- Mariah Hamel, awarded ph.d. from University of British Columbia under the direction of Izabella Laba. Presently, she is a postdoc working with Neil Lyall at the University of Georgia.

- Derrick Hart, awarded ph.d. in 2008 at the University of Illinois under the direction of Alex Iosevich. Presently, he is a postdoc with Van Vu at Rutgers University.

- David Hollis, REU student. Presently an undergraduate at Georgia Tech

- David Lowry, REU student. Presently an undergraduate at Georgia Tech.

- Olof Sisask, recently finished submitting his ph.d. at Cambridge University under the direction of Ben Green. He is presently a post-doc at Queen Mary in London, England.

4 Presentations

I gave a presentation at IPAM in December on my work with Olof Sisask, and also some work with D. Hart on sum-product inequalities. I have been invited to give taks in 2010 at: Kansas State University (colloquium, April 2009); Additive Combinatorics Conference (I am co-organizer, along with M. Hamel and N. Lyall); SIAM Discrete Math conference at CMU (July); ICM Satellite conference in Chennai (August-September).