GROWTH AND EXPANSION: PROJECT DESCRIPTIONS

HARALD ANDRÉS HELFGOTT, ASSISTED BY HENRY BRADFORD

Notes for the Arizona Winter School 2016
Preliminary version

The following problems vary in scope and character, as well as difficulty. They are all open-ended: readers are encouraged to continue their work and look for questions beyond what is stated here.

Problem 1(a) consists essentially in applying a result in a different field in a not completely obvious way. (Thanks are due to E. Lindenstrauss for the reference. The application came out of a discussion between B. Bukh and the author, with further participation by A. Harper.) Problem 1(b) is open, and may be hard; B. Bukh, M. Kassabov and the author did some initial exploration.

Problem 2 is related to Problem 1(b). It is also open. It may be relevant to practical applications, related to *hashing* [BSV].

Problem 3 is essentially asking the reader to give what would presumably be the "right" (still unknown) proof of a known result. As is usual, the "right" proof might give a result more general than what we know.

Problem 4 is very challenging but not completely beyond what can arguably be reached given the current state of knowledge. It is very much a longer-term project; its presence here is meant to encourage readers to become familiar with the literature.

Problem 1. Let p be a prime, $\lambda \in \mathbb{F}_p^*$. Assume λ has order $\geq \log p$.

(a) Write $e_p(t) = e^{2\pi i t/p}$. Konyagin [Kon92, Lemma 6] showed that, for any $\epsilon > 0$, there is a $c_\epsilon > 0$ such that, for any $p \geq c_\epsilon$ prime and $\alpha, \lambda \in (\mathbb{Z}/p\mathbb{Z})^*$ with λ of order $\geq c_\epsilon (\log p)/(\log \log p)^{1-\epsilon}$ in the group $(\mathbb{Z}/p\mathbb{Z})^*$,

$$\sum_{j=0}^{J} |\{\alpha \lambda^j / p\}|^2 \geq \frac{1}{(\log p)^{3^{\epsilon/4}}},$$

where $J = \lfloor c_\epsilon \log p (\log \log p)^4 \rfloor$ and $\{x\}$ is the element of $(-1/2, 1/2]$ such that $x - \{x\}$ is an integer.

Show that this means that $S(\alpha) = \sum_{j=0}^{J} e(\alpha \lambda^j / p)$ satisfies $|S(\alpha)| \leq J + 1 - 1/(\log p)^{3^{\epsilon/4}/2}$ for every $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$. Use this to show that every element of $\mathbb{Z}/p\mathbb{Z}$ can be written as a sum $\sum_{i=1}^{K} \lambda^{j_i}$, where $0 \leq j_i \leq J$ and K is bounded by

$$K \ll J (\log p)^{3^{\epsilon/4}/2} (\log p) \ll_\epsilon (\log p)^{2 + 3^{\epsilon/4}/2} (\log \log p)^4 \ll_\epsilon (\log p)^{5/2 + \epsilon}.$$

(Hint: show that for any sequence $r_0, \ldots, r_j \in \mathbb{Z}/p\mathbb{Z}$, the number of ways of expressing $x \in \mathbb{Z}/p\mathbb{Z}$ as a sum of K elements (not necessarily distinct) of a subset $A \subset \mathbb{Z}/p\mathbb{Z}$ equals

$$\frac{1}{p} \sum_{\alpha \in \mathbb{Z}/p\mathbb{Z}} S_A(\alpha)^K e(-\alpha x/p),$$

where $S_A(\alpha) = \sum_{a \in A} e(\alpha a)$. This is the *circle method* over $\mathbb{Z}/p\mathbb{Z}$.)

Conclude that the graph $\Gamma_{p,\lambda}$ with vertex set $\mathbb{F}_p$ and edge set

$$\{(x, x+1) : x \in \mathbb{F}_p\} \cup \{(x, \lambda x) : x \in \mathbb{F}_p\}$$

has diameter $\ll_\epsilon (\log p)^{5/2+\epsilon}$.

(b) Given $\lambda \in \mathbb{F}_p^*$ of order $\gg \log p$ and an element $x \in \mathbb{F}_p$, can you find a path from 0 to x of length $O((\log p)^{O(1)})$, in time $O((\log p)^{O(1)})$?

We may call this a *navigation* problem, to borrow a term from [Lar03].

Notice that the bounds should be independent of λ and x. You should *not* assume that λ is the reduction mod p of a fixed integer λ_0. (If you assume that, the task is trivial: write x in base λ_0.) You may allow travel on edges in either direction – i.e., you may consider the undirected graph

$$\{\{x, x+1\} : x \in \mathbb{F}_p\} \cup \{\{x, \lambda x\} : x \in \mathbb{F}_p\}$$

(How does the problem on the directed graph Γ_p reduce to this?

Some simple special cases:

- λ a root of $\lambda^2 - \lambda - 1 \equiv 0 \bmod p$ (Kassabov). Hint: let r be either of the real roots of $r^2 - r - 1 = 0$. Then $r^n - r^{-n}$ is the nth Fibonacci number. Start by showing that every integer n can be written as a short (length $O(\log n)$) sum of Fibonacci numbers quickly.
- λ a root of $P(\lambda) = 0$, where $P(x) = a_n x^n + \ldots + a_0$, $a_i \in \mathbb{Z}$ and there is an $0 \le i \le n$ such that $\sum_{j \ne i} |a_j| < |a_i|$ (Bukh). *Hint:* think of the Euclidean algorithm. The constants in the diameter bound will depend on the a_j's.

Problem 2: Navigation in SL_2.

Let $g_1, g_2 \in G = \mathrm{SL}_2(\mathbb{F}_p)$ generate G. We know that the diameter of the Cayley graph of G with respect to $\{g_1, g_2\}$ is $O((\log p)^{O(1)})$, where the implied constants are absolute. The navigation problem here is as follows: given g_1, g_2 as above, and $h \in \mathrm{SL}_2(\mathbb{F}_p)$, find a path in the Cayley graph from the identity to h of length $O((\log p)^{O(1)})$, in time $O((\log p)^{O(1)})$, say.

It is enough to be able to solve the problem for every h of the form

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}. \tag{1}$$

(Sketch why.) It would also be enough to solve it for every h of the form

$$\begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix},$$

say. (Again, sketch why.)

The problem was solved in [Lar03] for the special case

$$\{g_1, g_2\} = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}. \tag{2}$$

The solution is based on the Euclidean algorithm; it constructs any h of the form (1) quickly. It is a probabilistic algorithm: it finds a short path with probability $\geq 1/2$ at any given try.

Unfortunately, the algorithm breaks down already for

$$\{g_1, g_2\} = \left\{ \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \right\}. \tag{3}$$

A solution valid for the set of generators (3) and h arbitrary would already be noteworthy.

Problem 3. Bourgain, Konyagin and Glibichuk [BGK06] proved that, if H is a subgroup of $\mathbb{F}_p^*$ with $|H| > p^\delta$, and $a \in \mathbb{F}_p^*$, then

$$\left| \sum_{x \in H} e(ax/p) \right| \leq p^{-\delta'} |H|, \tag{4}$$

where $\delta' > 0$ depends only on δ. There are also more general versions, where, instead of H, we have the product of r arbitrary sets (provided the product of their sizes is at least $p^{1+\delta}$), or where the condition $|H| > p^\delta$ is relaxed. See later versions of the method in, e.g., [Bou10].

The proof relies crucially on the sum-product theorem, or rather on intermediate results leading to it, such as the fact that

$$|6Y^2X| \geq \frac{1}{2} \max(|X||Y|, p) \tag{5}$$

for any $X \subset \mathbb{F}_p$, $Y \subset \mathbb{F}_p^*$ with $X = -X$, $0 \in X$, $1 \in Y$. As we have already seen, (5) can be derived naturally from statements on growth in the affine group.

The (rather open-ended) task here would be to see whether one can prove estimates on exponential sums in a natural way by using a statement on growth in the affine group directly. Can one obtain a family of results by considering the action of a solvable group on a nilpotent subgroup, in general?

Quite incidentally, there is a classic problem in number theory that remains open, namely, that of showing that, for any interval I in $\mathbb{Z}/p\mathbb{Z}$ of length $\geq p^\delta$ and any character χ of $(\mathbb{Z}/p\mathbb{Z})^*$,

$$\left| \sum_{x \in I} \chi(x) \right| \leq p^{-\delta'} |I|, \tag{6}$$

where $\delta' > 0$ depends only on δ. This is unknown for $\delta \leq 1/4$. There were once hopes that (4) might lead to a proof for (6), but this hasn't been the case. There is a hidden asymmetry here: a maximal torus defined over K in $\mathrm{SL}_2(K)$ acts on a unipotent subgroup, but not viceversa. Discuss.

Problem 4. The *symmetric group* $\mathrm{Sym}(n)$ is the group of all permutations of n elements. The best known bound for the diameter of the Cayley graph of the symmetric group $\mathrm{Sym}(n)$ with respect to arbitrary generators is $\exp((\log n)^{4+\epsilon})$ [HS14]. A folk conjecture (predating *Babai's conjecture* [BS92], which is more general) states that the diameter should be $O(n^{O(1)})$.

This is a difficult problem of interest in itself. There is also the additional motivation of its probable relevance to bounding the diameter of linear algebraic groups with unbounded rank. That is: yes, we have good bounds (of the form $(\log |G|)^{O_n(1)}$) on the diameter of any Cayley graph of $G = \mathrm{SL}_n(\mathbb{F}_p)$, where n is bounded and p is arbitrary; however, can we give good bounds (ideally $(\log |G|)^{O(1)}$) on the diameter of any Cayley graph of $\mathrm{SL}_n(\mathbb{F}_3)$, say? Here 3 can be your favorite prime instead.

Part of the rationale here is the common view of $\mathrm{Sym}(n)$ as SL_n over the non-existent field $\mathbb{F}_{\mathrm{un}}$ with one element. How to make sense of objects over $\mathbb{F}_{\mathrm{un}}$ is itself an interesting, open-ended topic, with plenty of interesting literature.

References

[BGK06] J. Bourgain, A.A. Glibichuk, and S.V. Konyagin. Estimates for the number of sums and products and for exponential sums in fields of prime order. *J. Lond. Math. Soc., II. Ser.*, 73(2):380–398, 2006.

[Bou10] Jean Bourgain. On exponential sums in finite fields. In *An irregular mind. Szemerédi is 70. Dedicated to Endre Szemerédi on the occasion of his seventieth birthday.*, pages 219–242. Berlin: Springer, 2010.

[BS92] L. Babai and Á. Seress. On the diameter of permutation groups. *European J. Combin.*, 13(4):231–243, 1992.

[BSV] L. Bromberg, V. Shpilrain, and A. Vdovina. Navigating in the Cayley graph of $\mathrm{SL}_2(\mathbb{F}_p)$ and applications to hashing. Available as `arxiv.org:1409.4478`.

[HS14] H. A. Helfgott and Á. Seress. On the diameter of permutation groups. *Ann. of Math. (2)*, 179(2):611–658, 2014.

[Kon92] S. V. Konyagin. Estimates for Gaussian sums and Waring's problem modulo a prime. *Trudy Mat. Inst. Steklov.*, 198:111–124, 1992.

[Lar03] M. Larsen. Navigating the Cayley graph of $\mathrm{SL}_2(\mathbb{F}_p)$. *Int. Math. Res. Not.*, (27):1465–1471, 2003.