Product-Free Subsets of Groups, Then and Now

Product-free subsets of groups, then and now

Kiran S. Kedlaya

Dedicated to Joe Gallian on his 65th birthday and the 30th anniversary of the Duluth REU

1. Introduction

Let G be a group. A subset S of G is *product-free* if there do not exist $a, b, c \in S$ (not necessarily distinct[1]) such that $ab = c$.

One can ask about the existence of large product-free subsets for various groups, such as the groups of integers (see next section), or compact topological groups (as suggested in [**11**]). For the rest of this paper, however, I will require G to be a finite group of order $n > 1$. Let $\alpha(G)$ denote the size of the largest product-free subset of G; put $\beta(G) = \alpha(G)/n$, so that $\beta(G)$ is the density of the largest product-free subset. What can one say about $\alpha(G)$ or $\beta(G)$ as a function of G, or as a function of n? (Some of our answers will include an unspecified positive constant; I will always call this constant c.)

The purpose of this paper is threefold. I first review the history of this problem, up to and including my involvement via Joe Gallian's REU (Research Experience for Undergraduates) at the University of Minnesota, Duluth, in 1994; since I did this once already in [**11**], I will be briefer here. I then describe some very recent progress made by Gowers [**7**]. Finally, I speculate on the gap between the lower and upper bounds, and revisit my 1994 argument to show that this gap cannot be closed using Gowers's argument as given.

Note the usual convention that multiplication and inversion are permitted to act on subsets of G, i.e., for $A, B \subseteq G$,

$$AB = \{ab : a \in A, b \in B\}, \qquad A^{-1} = \{a^{-1} : a \in A\}.$$

2. Origins: the abelian case

In the abelian case, product-free subsets are more customarily called *sum-free* subsets. The first group in which such subsets were studied is the group of integers $\mathbb{Z}$; the first reference I could find for this is Abbott and Moser [**1**], who expanded

2000 *Mathematics Subject Classification.* Primary 20D60; secondary 20P05.

The author was supported by NSF CAREER grant DMS-0545904 and a Sloan Research Fellowship.

[1] In some sources, one does require $a \neq b$. For instance, as noted in [**9**], I mistakenly assumed this in [**11**, Theorem 3].

upon Schur's theorem that the set $\{1, \dots, \lfloor n!e \rfloor\}$ cannot be partitioned into n sum-free sets. This led naturally to considering sum-free subsets of finite abelian groups, for which the following is easy.

THEOREM 2.1. *For G abelian, $\beta(G) \geq \frac{2}{7}$.*

PROOF. For $G = \mathbb{Z}/p\mathbb{Z}$ with $p > 2$, we have $\alpha(G) \geq \lfloor \frac{p+1}{3} \rfloor$ by taking

$$S = \left\{ \left\lfloor \frac{p+1}{3} \right\rfloor, \dots, 2 \left\lfloor \frac{p+1}{3} \right\rfloor - 1 \right\}.$$

Then apply the following lemma. □

LEMMA 2.2. *For G arbitrary, if H is a quotient of G, then*

$$\beta(G) \geq \beta(H).$$

PROOF. Let S' be a product-free subset of H of size $\alpha(H)$. The preimage of S' in G is product-free of size $\#S'\#G/\#H$, so $\alpha(G) \geq \alpha(H)\#G/\#H$. □

In fact, one can prove an exact formula for $\alpha(G)$ showing that this construction is essentially optimal. Many cases were established around 1970, but only in 2005 was the proof of the following result finally completed by Green and Ruzsa [**8**].

THEOREM 2.3 (Green-Ruzsa). *Suppose that G is abelian.*

(a) *If n is divisible by a prime $p \equiv 2 \pmod 3$, then for the least such p, $\alpha(G) = \frac{n}{3} + \frac{n}{3p}$.*
(b) *Otherwise, if $3|n$, then $\alpha(G) = \frac{n}{3}$.*
(c) *Otherwise, $\alpha(G) = \frac{n}{3} - \frac{n}{3m}$, for m the exponent (largest order of any element) of G.*

One possible explanation for the delay is that it took this long for this subject to migrate into the mathematical mainstream, as part of the modern subject of *additive combinatorics* [**15**]; see Section 4.

The first appearance of the problem of computing $\alpha(G)$ for nonabelian G seems to have been in a 1985 paper of Babai and Sós [**2**]. In fact, the problem appears there as an afterthought; the authors were more interested in *Sidon sets*, in which the equation $ab^{-1} = cd^{-1}$ has no solutions with a, b, c, d taking at least three distinct values. This construction can be related to embeddings of graphs as induced subgraphs of Cayley graphs; product-free subsets arise because they relate to the special case of embedding stars in Cayley graphs. Nonetheless, the Babai-Sós paper is the first to make a nontrivial assertion about $\alpha(G)$ for general G; see Theorem 3.1.

This circumstance suggests rightly that the product-free problem is only one of a broad class of problems about structured subsets of groups; this class can be considered a nonabelian version of additive combinatorics, and progress on problems in this class has been driven as much by the development of the abelian theory as by interest from applications in theoretical computer science. An example of the latter is a problem of Cohn and Umans [**5**] (see also [**6**]): to find groups G admitting large subsets S_1, S_2, S_3 such that the equation $a_1 b_1^{-1} a_2 b_2^{-1} a_3 b_3^{-1} = e$, with $a_i, b_i \in S_i$, has only solutions with $a_i = b_i$ for all i. A sufficiently good construction would resolve an ancient problem in computational algebra: to prove that two $n \times n$ matrices can be multiplied using $O(n^{2+\epsilon})$ ring operations for any $\epsilon > 0$.

3. Lower bounds: Duluth, 1994

Upon my arrival at the REU in 1994, Joe gave me the paper of Babai and Sós, perhaps hoping I would have some new insight about Sidon sets. Instead, I took the path less traveled and started thinking about product-free sets.

The construction of product-free subsets given in [**2**] is quite simple: if H is a proper subgroup of G, then any nontrivial coset of H is product-free. This is trivial to prove directly, but it occurred to me to formulate it in terms of permutation actions. Recall that specifying a transitive permutation action of the group G is the same as simply identifying a conjugacy class of subgroups: if H is one of the subgroups, the action is left multiplication on left cosets of H. (Conversely, given an action, the point stabilizers are conjugate subgroups.) The construction of Babai and Sós can then be described as follows.

THEOREM 3.1 (Babai-Sós). *For G admitting a transitive action on $\{1, \dots, m\}$ with $m > 1$, $\beta(G) \geq m^{-1}$.*

PROOF. The set of all $g \in G$ such that $g(1) = 2$ is product-free of size n/m. □

I next wondered: what if you allow g to carry 1 into a slightly larger set, say a set T of k elements? You would still get a product-free set if you forced each $x \in T$ to map to something not in T. This led to the following argument.

THEOREM 3.2. *For G admitting a transitive action on $\{1, \dots, m\}$ with $m > 1$, $\beta(G) \geq cm^{-1/2}$.*

PROOF. For a given k, we compute a lower bound for the average size of

$$S = \bigcup_{x \in T} \{g \in G : g(1) = x\} - \bigcup_{y \in T} \{g \in G : g(1), g(y) \in T\}$$

for T running over k-element subsets of $\{2, \dots, m\}$. Each set in the first union contains n/m elements, and they are all disjoint, so the first union contains kn/m elements. To compute the average of a set in the second union, note that for fixed $g \in G$ and $y \in \{2, \dots, m\}$, a k-element subset T of $\{1, \dots, m\}$ contains $g(1), y, g(y)$ with probability $\frac{k(k-1)}{m(m-1)}$ if two of the three coincide and $\frac{k(k-1)(k-2)}{m(m-1)(m-2)}$ otherwise. A bit of arithmetic then shows that the average size of S is at least

$$\frac{kn}{m} - \frac{k^3 n}{(m-2)^2}.$$

Taking $k \sim (m/3)^{1/2}$, we obtain $\alpha(G) \geq cn/m^{1/2}$. (For any fixed $\epsilon > 0$, the implied constant can be improved to $e^{-1} - \epsilon$ for m sufficiently large; see the proof of Theorem 6.2. On the other hand, the proof as given can be made constructive in case G is doubly transitive, as then there is no need to average over T.) □

This gives a lower bound depending on the parameter m, which we can view as the index of the largest proper subgroup of G. To state a bound depending only on n, one needs to know something about the dependence of m on n; by Lemma 2.2, it suffices to prove a lower bound on m in terms of n for all *simple* nonabelian groups. I knew this could be done in principle using the classification of finite simple groups (CFSG); after some asking around, I got hold of a manuscript by Liebeck and Shalev [**12**] that included the bound I wanted, leading to the following result from [**10**].

THEOREM 3.3. *Under CFSG, the group G admits a transitive action on a set of size $1 < m \leq cn^{3/7}$. Consequently, Theorem 3.1 implies $\alpha(G) \geq cn^{4/7}$, whereas Theorem 3.2 implies $\alpha(G) \geq cn^{11/14}$.*

At this point, I was pretty excited to have discovered something interesting and probably publishable. On the other hand, I was completely out of ideas! I had no hope of getting any stronger results, even for specific classes of groups, and it seemed impossible to derive any nontrivial upper bounds at all. In fact, Babai and Sós suggested in their paper that maybe $\beta(G) \geq c$ for all G; I was dubious about this, but I couldn't convince myself that one couldn't have $\beta(G) \geq cn^{-\epsilon}$ for all $\epsilon > 0$.

So I decided to write this result up by itself, as my first Duluth paper, and ask Joe for another problem (which naturally he provided). My paper ended up appearing as [**10**]; I revisited the topic when I was asked to submit a paper in connection with being named a runner-up for the Morgan Prize for undergraduate research, the result being [**11**].

I then put this problem in a mental deep freezer, figuring (hoping?) that my youthful foray into combinatorics would be ultimately forgotten, once I had made some headway with some more serious mathematics, like algebraic number theory or algebraic geometry. I was reassured by the expectation that the nonabelian product-free problem was both intractable and of no interest to anyone, certainly not to any serious mathematician.

Ten years passed.[2]

4. Interlude: back to the future

Up until several weeks before the Duluth conference, I had been planning to speak about the latest and greatest in algebraic number theory (the proof of Serre's conjecture linking modular forms and mod p Galois representations, recently completed by Khare and Wintenberger). Then I got an email that suggested that maybe I should try embracing my past instead of running from it.

A number theorist friend (Michael Schein) reported having attended an algebra seminar at Hebrew University about product-free subsets of finite groups, and hearing my name in this context. My immediate reaction was to wonder what self-respecting mathematician could possibly be interested in my work on this problem. The answer was Tim Gowers, who had recently established a nontrivial upper bound for $\alpha(G)$ using a remarkably simple argument.

It seems that in the ten years since I had moved on to ostensibly more mainstream mathematics, additive combinatorics had come into its own, thanks partly to the efforts of no fewer than three Fields medalists (Tim Gowers, Jean Bourgain, and Terry Tao); some sources date the start of this boom to Ruzsa's publication in 1994 of a simplified proof [**14**] of a theorem of Freiman on subsets of $\mathbb{Z}/p\mathbb{Z}$ having few pairwise sums. In the process, some interest had spilled over to nonabelian problems.

[2]If you do not recognize this reference, you may not have read the excellent novel *The Grasshopper King*, by fellow Duluth REU alumnus Jordan Ellenberg.

The introduction to Gowers's paper [**7**] cites[3] my Duluth paper as giving the best known lower bound on $\alpha(G)$ for general G. At this point, it became clear that I had to abandon my previous plan for the conference in favor of a return visit to my mathematical roots.

5. Upper bounds: bipartite Cayley graphs

In this section, I'll proceed quickly through Gowers's upper bound construction. Gowers's paper [**7**] is exquisitely detailed; I'll take that fact as license to be slightly less meticulous here.

The strategy of Gowers is to consider three sets A, B, C for which there is no true equation $ab = c$ with $a \in A, b \in B, c \in C$, and give an upper bound on $\#A\#B\#C$. To do this, he studies a certain *bipartite Cayley graph* associated to G. Consider the bipartite graph Γ with vertex set $V_1 \cup V_2$, where each V_i is a copy of G, with an edge from $x \in V_1$ to $y \in V_2$ if and only if $yx^{-1} \in A$. We are then given that there are no edges between $B \subseteq V_1$ and $C \subseteq V_2$.

A good reflex at this point would be to consider the eigenvalues of the adjacency matrix of Γ. For bipartite graphs, it is more convenient to do something slightly different using singular values; although this variant of spectral analysis of graphs is quite natural, I am only aware of the reference [**3**] from 2004 (and only thanks to Gowers for pointing it out). Let N be the *incidence matrix*, with columns indexed by V_1 and rows by V_2, with an entry in row x and column y if xy is an edge of Γ.

THEOREM 5.1. *We can factor N as a product $U\Sigma V$ of $\#G \times \#G$ matrices over $\mathbb{R}$, with U, V orthogonal and Σ diagonal with nonnegative entries. (This is called a* singular value decomposition *of N.)*

PROOF. (Compare [**7**, Theorem 2.6], or see any textbook on numerical linear algebra.) By compactness of the unit ball, there is a greatest λ such that $\|N\mathbf{v}\| = \lambda\|\mathbf{v}\|$ for some nonzero $\mathbf{v} \in \mathbb{R}^{V_1}$. If $\mathbf{v} \cdot \mathbf{w} = 0$, then $f(t) = \|N(\mathbf{v} + t\mathbf{w})\|^2$ has a local maximum at $t = 0$, so

$$0 = \frac{d}{dt}\|N(\mathbf{v} + t\mathbf{w})\|^2 = 2t(N\mathbf{v}) \cdot (N\mathbf{w}).$$

Apply the same construction to the orthogonal complement of $\mathbb{R}\mathbf{v}$ in $\mathbb{R}^{V_1}$. Repeating, we obtain an orthonormal basis of $\mathbb{R}^{V_1}$; the previous calculation shows that the image of this basis in $\mathbb{R}^{V_2}$ is also orthogonal. Using these to construct V, U yields the claim. □

The matrix $M = NN^T$ is symmetric, and has several convenient properties.

(a) The trace of M equals the number of edges of Γ.
(b) The eigenvalues of M are the squares of the diagonal entries of Σ.
(c) Since Γ is regular of degree $\#A$ and connected, the largest eigenvalue of M is $\#A$, achieved by the all-ones eigenvector $\mathbf{1}$.

LEMMA 5.2. *Let λ be the second largest diagonal entry of Σ. Then the set W of $\mathbf{v} \in \mathbb{R}^{V_1}$ with $\mathbf{v} \cdot \mathbf{1} = 0$ and $\|N\mathbf{v}\| = \lambda\|\mathbf{v}\|$ is a nonzero subspace of $\mathbb{R}^{V_1}$.*

[3]Since Joe is fond of noting "program firsts", I should point out that this appears to be the first citation of a Duluth paper by a Fields medalist. To my chagrin, I think it is also the first such citation of any of my papers.

PROOF. (Compare [**7**, Lemma 2.7].) From Theorem 5.1, we obtain an orthogonal basis $\mathbf{v}_1, \dots, \mathbf{v}_n$ of $\mathbb{R}^{V_1}$, with $\mathbf{v}_1 = \mathbf{1}$, such that $N\mathbf{v}_1, \dots, N\mathbf{v}_n$ are orthogonal, and $\|N\mathbf{v}_1\|/\|\mathbf{v}_1\|, \dots, \|N\mathbf{v}_n\|/\|\mathbf{v}_n\|$ are the diagonal entries of Σ; we may then identify W as the span of the $\mathbf{v}_i$ with $i > 1$ and $\|N\mathbf{v}_i\| = \lambda\|\mathbf{v}_i\|$.

Alternatively, one may note that W is obviously closed under scalar multiplication, then check that W is closed under addition as follows. If $\mathbf{v}_1, \mathbf{v}_2 \in W$, then $\|N(\mathbf{v}_1 \pm \mathbf{v}_2)\| \leq \lambda\|\mathbf{v}_1 \pm \mathbf{v}_2\|$, but by the parallelogram law

$$\begin{aligned}\|N\mathbf{v}_1 + N\mathbf{v}_2\|^2 + \|N\mathbf{v}_1 - N\mathbf{v}_2\|^2 &= 2\|N\mathbf{v}_1\|^2 + 2\|N\mathbf{v}_2\|^2 \\ &= 2\lambda^2\|\mathbf{v}_1\|^2 + 2\lambda^2\|\mathbf{v}_2\|^2 \\ &= \lambda^2\|\mathbf{v}_1 + \mathbf{v}_2\|^2 + \lambda^2\|\mathbf{v}_1 - \mathbf{v}_2\|^2.\end{aligned}$$

Hence $\|N(\mathbf{v}_1 \pm \mathbf{v}_2)\| = \lambda\|\mathbf{v}_1 \pm \mathbf{v}_2\|$. □

Gowers's upper bound on $\alpha(G)$ involves the parameter δ, defined as the smallest dimension of a nontrivial representation[4] of G. For instance, if $G = \mathrm{PSL}_2(q)$ with q*odd*, then then $\delta = (q-1)/2$.

LEMMA 5.3. *If* $\mathbf{v} \in \mathbb{R}^{V_1}$ *satisfies* $\mathbf{v} \cdot \mathbf{1} = 0$*, then* $\|N\mathbf{v}\| \leq (n\#A/\delta)^{1/2}\|\mathbf{v}\|$.

PROOF. Take λ, W as in Lemma 5.2. Let G act on V_1 and V_2 by right multiplication; then G also acts on Γ. In this manner, W becomes a real representation of G in which no nonzero vector is fixed. In particular, $\dim(W) \geq \delta$.

Now note that the number of edges of M, which is $n\#A$, equals the trace of M, which is at least $\dim(W)\lambda^2 \geq \delta\lambda^2$. This gives $\lambda^2 \leq n\#A/\delta$, proving the claim. □

We are now ready to prove Gowers's theorem [**7**, Theorem 3.3].

THEOREM 5.4 (Gowers). *If* A, B, C *are subsets of* G *such that there is no true equation* $ab = c$ *with* $a \in A, b \in B, c \in C$*, then* $\#A\#B\#C \leq n^3/\delta$*. Consequently,* $\beta(G) \leq \delta^{-1/3}$.

For example, if $G = \mathrm{PSL}_2(q)$ with q odd, then $n \sim cq^3$, so $\alpha(G) \leq cn^{8/9}$. On the lower bound side, G admits subgroups of index $m \sim cq$, so $\alpha(G) \geq cn^{5/6}$.

PROOF. Write $\#A = rn, \#B = sn, \#C = tn$. Let $\mathbf{v}$ be the characteristic function of B viewed as an element of $\mathbb{R}^{V_1}$, and put $\mathbf{w} = \mathbf{v} - s\mathbf{1}$. Then

$$\begin{aligned}\mathbf{w} \cdot \mathbf{1} &= 0 \\ \mathbf{w} \cdot \mathbf{w} &= (1-s)^2\#B + s^2(n - \#B) = s(1-s)n \leq sn,\end{aligned}$$

so by Lemma 5.3, $\|N\mathbf{w}\|^2 \leq rn^2sn/\delta$.

Since $ab = c$ has no solutions with $a \in A, b \in B, c \in C$, each element of C corresponds to a zero entry in $N\mathbf{v}$. However, $N\mathbf{v} = N\mathbf{w} + rsn\mathbf{1}$, so each zero entry in $N\mathbf{v}$ corresponds to an entry of $N\mathbf{w}$ equal to $-rsn$. Therefore,

$$(tn)(rsn)^2 \leq \|N\mathbf{w}\|^2 \leq rsn^3/\delta,$$

hence $rst\delta \leq 1$ as desired. □

As noted by Nikolov and Pyber [**13**], the extra strength in Gowers's theorem is useful for other applications in group theory, largely via the following corollary.

[4]One could just as well restrict to real representations, which would increase δ by a factor of 2 in some cases. For instance, if $G = \mathrm{PSL}_2(q)$ with $q \equiv 3 \pmod 4$, this would give $\delta = q - 1$.

COROLLARY 5.5 (Nikolov-Pyber). *If A, B, C are subsets of G such that $ABC \neq G$, then $\#A\#B\#C \leq n^3/\delta$.*

PROOF. Suppose that $\#A\#B\#C > n^3/\delta$. Put $D = G \setminus AB$, so that $\#D = n - \#(AB)$. By Theorem 5.4, we have $\#A\#B\#D \leq n^3/\delta$, so $\#C > \#D$. Then for any $g \in C$, the sets AB and gC^{-1} have total cardinality more than n, so they must intersect. This yields $ABC = G$. □

Gowers indicates that his motivation for this argument was the notion of a *quasi-random graph* introduced by Chung, Graham, and Wilson [**4**]. They show that (in a suitable quantitative sense) a graph looks random in the sense of having the right number of short cycles if and only if it also looks random from the spectral viewpoint, i.e., the second largest eigenvalue of its adjacency matrix is not too large.

6. Coda

As noted by Nikolov and Pyber [**13**], using CFSG to get a strong quantitative version of Jordan's theorem on finite linear groups, one can produce upper and lower bounds for $\alpha(G)$ that look similar. (Keep in mind that the index of a proper subgroup must be at least $\delta + 1$, since any permutation representation of degree m contains a linear representation of dimension $m - 1$.)

THEOREM 6.1. *Under CFSG, the group G has a proper subgroup of index at most $c\delta^2$. Consequently,*

$$cn/\delta \leq \alpha(G) \leq cn/\delta^{1/3}.$$

Moreover, for many natural examples (e.g., $G = A_m$ or $G = \mathrm{PSL}_2(q)$), G has a proper subgroup of index at most $c\delta$, in which case one has

$$cn/\delta^{1/2} \leq \alpha(G) \leq cn/\delta^{1/3}.$$

Since the gap now appears quite small, one might ask about closing it. However, one can adapt the argument of [**10**] to show that Gowers's argument alone will not suffice, at least for families of groups with $m \leq c\delta$. (Gowers proves some additional results about products taken more than two at a time [**7**, §5]; I have not attempted to extend this construction to that setting.)

THEOREM 6.2. *Given $\epsilon > 0$, for G admitting a transitive action on $\{1, \dots, m\}$ for m sufficiently large, there exist $A, B, C \subseteq G$ with $(\#A)(\#B)(\#C) \geq (e^{-1} - \epsilon)n^3/m$, such that the equation $ab = c$ has no solutions with $a \in A, b \in B, c \in C$. Moreover, we can force $B = C$, $C = A$, or $A = B^{-1}$ if desired.*

PROOF. We first give a quick proof of the lower bound cn^3/m. Let U, V be subsets of $\{1, \dots, m\}$ of respective sizes u, v. Put

$$A = \{g \in G : g(U) \cap V = \emptyset\}$$
$$B = \{g \in G : g(1) \in U\}$$
$$C = \{g \in G : g(1) \in V\};$$

then clearly the equation $ab = c$ has no solutions with $a \in A, b \in B, c \in C$. On the other hand,

$$\#A \geq n - u\frac{vn}{m}, \qquad \#B = \frac{un}{m}, \qquad \#C = \frac{vn}{m},$$

and so

$$(\#A)(\#B)(\#C) \geq \frac{n^3}{m}\left(\frac{uv}{m}\right)\left(1 - \frac{uv}{m}\right).$$

By taking $u, v = \lfloor \sqrt{m/2} \rfloor$, we obtain $(\#A)(\#B)(\#C) \geq cn^3/m$.

To optimize the constant, we must average over choices of U, V. Take $u, v = \lfloor \sqrt{m} \rfloor$. By inclusion-exclusion, for any positive integer h, the average of $\#A$ is bounded below by

$$\sum_{i=0}^{2h-1} (-1)^i n \frac{u(u-1)\cdots(u-i+1)v(v-1)\cdots(v-i+1)}{i!m(m-1)\cdots(m-i+1)}.$$

(The i-th term counts occurrences of i-element subsets in $g(U) \cap V$. We find $\binom{v}{i}$ i-element sets inside V; on average, each one occurs inside $g(U)$ for $n\binom{u}{i}/\binom{m}{i}$ choices of g.) Rewrite this as

$$n\left(\sum_{i=0}^{2h-1} (-1)^i \frac{(m^{1/2})^i (m^{1/2})^i}{m^i i!} + o(1)\right),$$

where $o(1) \to 0$ as $m \to \infty$. For any $\epsilon > 0$, we have

$$(\#A)(\#B)(\#C) \geq n^3 \frac{m}{m^2}\left(e^{-1} - \epsilon\right)$$

for h sufficiently large, and m sufficiently large depending on h. This gives the desired lower bound.

Finally, note that we may achieve $B = C$ by taking $U = V$. To achieve the other equalities, note that if the triplet A, B, C has the desired property, so do B^{-1}, A^{-1}, C^{-1} and C, B^{-1}, A. □

I have no idea whether one can sharpen Theorem 5.4 under the hypothesis $A = B = C$ (or even just $A = B$). It might be enlightening to collect some numerical evidence using examples generated by Theorem 3.2; with Xuancheng Shao, we have done this for $\mathrm{PSL}_2(q)$ for $q \leq 19$.

I should also mention again that (as suggested in [**11**]) one can also study product-free subsets of compact topological groups, which are large for Haar measure. Some such study is implicit in [**7**, §4], but we do not know what explicit bounds come out.

References

[1] H.L. Abbott and L. Moser, Sum-free sets of integers, *Acta Arith.* **11** (1966), 393–396.

[2] L. Babai and V.T. Sós, Sidon sets in groups and induced subgraphs of Cayley graphs, *Europ. J. Combin.* **6** (1985), 101–114.

[3] B. Bollobás and V. Nikiforov, Hermitian matrices and graphs: singular values and discrepancy, *Disc. Math.* **285** (2004), 17–32.

[4] F.R.K. Chung, R.L. Graham, and R.M. Wilson, Quasi-random graphs, *Combinatorica* **9** (1989), 345–362.

[5] H. Cohn and C. Umans, A group-theoretic approach to fast matrix multiplication, *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2003, 438–449.

[6] H. Cohn, R. Kleinberg, B. Szegedy, and C. Umans, Group-theoretic algorithms for matrix multiplication, *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2005, 379–388.

[7] W.T. Gowers, Quasirandom groups, arXiv preprint 0710.3877v1 (2007).

[8] B. Green and I.Z. Ruzsa, Sum-free sets in abelian groups, *Israel J. Math* **147** (2005), 157-189.

[9] M. Guiduci and S. Hart, Small maximal sum-free sets, preprint available at `http://eprints.bbk.ac.uk/archive/00000439/`.
[10] K.S. Kedlaya, Large product-free subsets of finite groups, *J. Combin. Theory Series A* **77** (1997), 339–343.
[11] K.S. Kedlaya, Product-free subsets of groups, *Amer. Math. Monthly* **105** (1998), 900–906.
[12] M. W. Liebeck and A. Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky, *J. Algebra* **184** (1996), 31–57.
[13] N. Nikolov and L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem, arXiv preprint math/0703343v3 (2007).
[14] I.Z. Ruzsa, Generalized arithmetical progressions and sumsets, *Acta Math. Hungar.* **65** (1994), 379–388.
[15] T. Tao and V. Vu, *Additive combinatorics*, Cambridge University Press, Cambridge, 2006.

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139
E-mail address: `kedlaya@mit.edu`
URL: `http://math.mit.edu/~kedlaya/`