Product-free subsets of groups, then and now

Kiran S. Kedlaya

MIT, Department of Mathematics

Communicating Mathematics
University of Minnesota, Duluth
Thursday, June 19, 2007

These slides, and notes for the proceedings, are available at

`http://math.mit.edu/~kedlaya/papers/`.

Money (that's what I want): I'm supported by NSF CAREER grant DMS-0545904 and a Sloan Research Fellowship.

The long and winding road: contents

The long and winding road: contents

Let it be: notation

Throughout this talk, G will denote a finite group of order n.

Definition

A subset S of G is *product-free* if the equation $ab = c$ has no solutions with $a, b, c \in S$. Let $\alpha(G)$ denote the size of the largest product-free subset of G. Put $\beta(G) = \alpha(G)/n$.

Some results will contain an undefined positive constant $c > 0$; this constant may differ at every appearance.

I want to tell you: the basic problem(s)

Problem

Find lower bounds on $\alpha(G)$, by constructing product-free subsets.

Problem

Find upper bounds on $\alpha(G)$, by proving nonexistence of extremely large product-free subsets.

I want to tell you: the basic problem(s)

Problem

Find lower bounds on $\alpha(G)$, by constructing product-free subsets.

Problem

Find upper bounds on $\alpha(G)$, by proving nonexistence of extremely large product-free subsets.

Lemma

If H is a quotient of G, then $\beta(G) \geq \beta(H)$.

Proof.

Think for yourself. □

This suggests focusing attention on simple groups.

Good morning, good morning: origin of the problem

Babai and Sós (1985) tried to construct large Sidon sets in groups. A *Sidon set* in G is a subset S such that the equation $ab^{-1} = cd^{-1}$ has no solutions with $|\{a,b,c,d\}| \geq 3$.

This problem is motivated by the problem of constructing Cayley (di)graphs exhibiting particular induced subgraphs. The special case of stars is related to product-free subsets.

The night before: the abelian case

Abelian cases were studied earlier. E.g., in $\mathbb{Z}/n\mathbb{Z}$, the subset

$$\left\{ \left\lfloor \frac{n+1}{3} \right\rfloor, \ldots, 2\left\lfloor \frac{n+1}{3} \right\rfloor - 1 \right\}.$$

is product-free (Erdős?).

The night before: the abelian case

Abelian cases were studied earlier. E.g., in $\mathbb{Z}/n\mathbb{Z}$, the subset

$$\left\{ \left\lfloor \frac{n+1}{3} \right\rfloor, \ldots, 2\left\lfloor \frac{n+1}{3} \right\rfloor - 1 \right\}.$$

is product-free (Erdős?).

One can use this observation to compute $\alpha(G)$ for any abelian group G; the optimal construction is to project onto some $\mathbb{Z}/n\mathbb{Z}$ and use a middle third. Although this was conjectured around 1970, it was only recently proved!

Theorem (Green-Ruzsa, 2005)

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 of G.*

The long and winding road: contents

A day in the life: arrival at Duluth

I arrived at Duluth in 1994; having expressed some interest in algebra and number theory, I immediately received the Babai-Sós paper. As far as Joe knew (which was correct), nothing had been done on the product-free problem since 1985.

Tell me what you see: the Babai-Sós construction

Theorem

Suppose G has a subgroup H of index $m > 1$. Then $\beta(G) \geq m^{-1}$.

Proof.

For any $g \in G \setminus H$, gH is product-free. □

I've got a feeling: another point of view

The group G acts transitively on the m left cosets by left multiplication. If we label the cosets using $\{1,\ldots,m\}$, we can reformulate the previous construction as considering the set

$$\{g \in G : g(1) = 2\}.$$

We can work it out: an improved construction

Now suppose we allow g to carry 1 into $T = \{2, \ldots, k+1\}$. We get a product-free set if $g(t) \notin T$ for any $t \in T$. That is, consider

$$S = \bigcup_{t \in T} \{g \in G : g(1) = t\} \setminus \bigcup_{t,u,v \in T} \{g \in G : g(1) = t, g(u) = v\}.$$

The average (over T) size of this set is at least

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

Taking $k \sim (m/3)^{1/2}$, we obtain the following.

Theorem (K, 1994)

Suppose G has a subgroup H of index $m > 1$. Then $\beta(G) \geq cm^{-1/2}$.

I'm a loser: no progress on upper bounds

It is trivial to prove $\beta(G) \leq 1/2$. I had no idea how to prove anything stronger. Neither did Babai and Sós, who suggested that perhaps $\beta(G) \geq c$.

So I stopped, wrote this up, and switched to another problem. Once this was published (1997), I stopped thinking about this subject and went into a "respectable" area (number theory). Ten years later...

The long and winding road: contents

Wait: respect catches up

In the past few years, *additive combinatorics* has become an extremely hot area of mathematics, attracting the attentions of at least three Fields medalists (Bourgain, Gowers, Tao).

Nonabelian problems have also proved relevant to areas of theoretical computer science. A beautiful example is the work of Cohn-Umans on fast matrix multiplication, involving subsets A, B, C of a group G for which the equation

$$a_1 a_2^{-1} b_1 b_2^{-1} c_1 c_2^{-1} = e$$

have no solutions with $a_i \in A, b_i \in B, c_i \in C$ unless $a_1 = a_2$ and so forth.

Get back: a forced return to my roots

Recently, a friend of mine mentioned that they heard about my product-free subsets result in a talk describing a result of Tim Gowers.

Theorem (Gowers, 2007)

Let d be the smallest dimension of a nontrivial linear representation of G. Then $\beta(G) \leq d^{-1/3}$.

This in particular disproves the guess of Babai and Sós. Better yet, Gowers's proof is quite simple.

This appears to be the first citation of a Duluth paper (or of any of my own papers, sigh) by a Fields medalist.

Do you want to know a secret: Gowers's method

Gowers actually proves a stronger result.

Theorem (Gowers, 2007)

Let d be the smallest dimension of a nontrivial linear representation of G. For any subsets A, B, C for which the equation $abc = e$ has no solutions with $a \in A, b \in B, c \in C$, we have $|A||B||C| \leq n^3/d$.

The strategy is consider a *bipartite Cayley graph* whose vertices are two copies of G, with an edge xy if $yx^{-1} \in A$. Let N be the incidence matrix; since N is not symmetric, spectral analysis is not useful. Instead...

I'm looking through you: singular values

Theorem

The matrix N can be written as $U\Sigma V$ with U, V orthogonal and Σ diagonal with nonnegative entries. (This is a singular value decomposition of N.)

I'm looking through you: singular values

Theorem

The matrix N can be written as $U\Sigma V$ with U, V orthogonal and Σ diagonal with nonnegative entries. (This is a singular value decomposition of N.)

The largest singular value is $|A|$, achieved by the all-ones vector $\mathbf{1}$. Let λ be the next largest singular value.

Theorem

$\lambda \leq (n|A|/d)^{1/2}$.

I'm looking through you: singular values

Theorem

The matrix N can be written as $U\Sigma V$ with U, V orthogonal and Σ diagonal with nonnegative entries. (This is a singular value decomposition of N.)

The largest singular value is $|A|$, achieved by the all-ones vector $\mathbf{1}$. Let λ be the next largest singular value.

Theorem

$\lambda \leq (n|A|/d)^{1/2}$.

Proof.

The set of vectors $\mathbf{v}$ with $\mathbf{v} \cdot \mathbf{1} = 0$ and $\|N\mathbf{v}\| = \lambda \|\mathbf{v}\|$ is a nontrivial representation of G, so has dimension $\geq d$. The eigenvalues of $N^T N$ are the squares of the entries of Σ; their sum is the number of edges of G, or $n|A|$. □

Come together: end of the proof

Suppose A, B, C are subsets of sizes rn, sn, tn, such that $abc = e$ has no solutions with $a \in A, b \in B, c \in C$; we want $rstd \leq 1$.

Let $\mathbf{v}$ be the characteristic vector of B, and $\mathbf{w} = \mathbf{v} - s\mathbf{1}$. Then

$$\mathbf{w} \cdot \mathbf{1} = 0, \qquad \mathbf{w} \cdot \mathbf{w} = \mathbf{w} \cdot \mathbf{v} = s(1-s)n \leq sn,$$

so $\|N\mathbf{w}\|^2 \leq \lambda^2 \|\mathbf{w}\|^2 \leq rn^2 sn/d$.

However, each zero entry of $N\mathbf{v}$ corresponds to an entry of $N\mathbf{w}$ equal to rsn, so

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

and $rstd \leq 1$, as desired.

Tomorrow never knows: further questions

Problem

Can one close the gap between the lower and upper bounds on $\alpha(G)$? for certain families of groups?

E.g., for $G = A_m$, we have

$$cm^{-1/2} \leq \beta(G) \leq cm^{-1/3}.$$

For $G = \mathrm{PSL}_2(\mathbb{F}_q)$, we have

$$cq^{-1/2} \leq \beta(G) \leq cq^{-1/3}.$$

It might be useful to check some numerical examples, i.e., make some examples from the lower bound construction, then run them through the upper bound proof to see where the proof fails to be sharp.

The end: the end

All together now: they say it's your birthday... we're gonna have a good time!