Approximate groups, growth and width

Nick Gill (OU)

March 12, 2012

Approximate groups

Terry Tao defined approximate subgroups as follows.
Let A be a finite subset of a group G and let $K \geq 1$. We say that A is a *K-approximate group* if

1. $1 \in A$ and A is symmetric (i.e. $A^{-1} = A$), and
2. there exists $X \subset G$ such that $AA \subset AX$ and $|X| \leq K$.

Examples:

1. 1-approximate groups are subgroups.
2. Let A be a 'symmetrized' arithmetic progression:

$$-n, -n+d, ..., n-d, n.$$

   Then A is a ?-approximate group.

Connection to growth

Suppose that $A \subset G$ and A is symmetric. Suppose first that G is abelian.

1. If $|AA| \leq K|A|$ then $|A^n| \leq K^n|A|$ [P-R].
2. If $|AA| \leq K|A|$ then A^2 is a K^5-approximate group.

Now drop the condition that G is abelian.

1. If $|AAA| \leq K|A|$ then $|A^n| \leq K^{2n-5}|A|$ [H-T].
2. If $|AAA| \leq K|A|$ then A^2 is a K^5-approximate group.

Simple groups of Lie type

Let $G = SL_n(q)$. What are the K-approximate subgroups of G? This question is partially answered, for a strong value of K, by a theorem of Pyber-Szabo, Breuillard-Green-Tao building on work of Helfgott, Dinai, Helfgott-G.

Theorem

Let $A \subseteq G = SL_n(q)$. Suppose that $A = A^{-1}$ and $\langle A \rangle = G$. There exists $\varepsilon = f(n)$ such that either

- $|AAA| \geq |A|^{1+\varepsilon}$, *or*
- $AAA = G$.

Examples exist in $SL_n(3)$ due to Pyber-Szabo such that

- $|A| = (q-1)^n + 4 = 2^n + 4$ and
- $AAA \neq G$ and
- $|A^3| \leq 100 \cdot |A| < |A|^{1+\frac{6}{n}}$.

This shows, in particular, that ε **must depend on** n.

Babai's conjecture

There is an easy corollary of this result which partially proves Babai's conjecture:

Corollary

Let A be a symmetric subset of $G = SL_n(q)$. Suppose that $\langle A \rangle = G$. Then $A^x = G$ where $x = (\log |G|)^c$ and $c = f(n)$.

The conjecture states that we should be able to take c as absolute **across all simple groups**.

Width

Let $A \subset G$. We define the *width* of G with respect to A to be the minimum number n such that

$$G = A_1 A_2 \cdots A_n$$

and $A_1, \dots, A_n$ are all conjugates of A in G. Write $w(G, A)$.

Examples for a simple group G.

1. If G is of Lie type, A is a Sylow p-subgroup then $w(G, A) \leq 25$ [LP01].
   In fact $w(G, A) \leq 5$ [BNP08].
2. If $G = G_r(q)$, an untwisted group of Lie type of rank $r > 1$ over a field of q elements and $A \cong SL_2(q)$, then $w(G, A) \leq 5|\Phi^+|$ [LNS11].
   In particular, if $G = SL_n(q)$ and $A \cong SL_2(q)$ then $w(G, A) \leq \frac{5}{2}n(n+1)$.

The Product Decomposition Conjecture

We start with a result of Liebeck and Shalev:

Theorem

There exists a constant $c > 0$ such that, for A a normal subset of G, we have $G = A^x$ where $x \leq c \log |G| / \log |A|$

Note that this is best possible.
Liebeck, Nikolov and Shalev conjectured the following:

Conjecture

There exists a constant $c > 0$ such that, for A any subset of G of size at least 2, we have $G = A^x$ where $x \leq c \log |G| / \log |A|$

Note the similarity to Babai's conjecture - but both the assumptions and the conclusion are much stronger.

Some results

We start with a result of Gill, Pyber, Short, Szabó:

Theorem

Fix $n > 0$. There exists $c > 0$ such that, for A any subset of $G = SL_n(q)$ of size at least 2, we have $G = A_1 A_2 \cdots A_x$ where $x \leq c \log |G| / \log |A|$.

This proves the Product Decomposition Conjecture for groups of bounded rank.

A product theorem for conjugates

On the way to proving this result we came across something like a product theorem for conjugates:

Theorem

Fix $n > 0$. There exists $\varepsilon > 0$ such that, for A any subset of $G = SL_n(q)$, there exists $g \in G$ such that $|A \cdot A^g| \geq |A|^{1+\varepsilon}$ or $A^3 = G$.

We conjecture that the constant ε should be independent of n, indeed it should be uniform **across all simple groups**.

Note too that, when we're allowed to take conjugates, we achieve growth in two steps, not three.

The Skew Doubling Lemma

An explanation for the two step growth is found in the following result:

Theorem

Let A be a non-empty finite set of a group G such that, for some $K > 0$, $|AA'| \leq K|A|$ for every conjugate A' of A. Then

$$|A_1 \cdots A_m| \leq K^{14(m-1)}|A|$$

where $A_1, \ldots, A_m$ are conjugates of A or A^{-1}.

Note that, if A is *normal*, we effectively regain the doubling lemma for abelian groups.

Could it be that classical additive combinatorics for sets in abelian groups is **really** about normal subgroups of arbitrary groups?

K-approximate normal subgroups

Let A be a finite subset of a group G and let $K \geq 1$. We say that A is a *K-approximate normal subgroup* if

1. $1 \in A$ and A is symmetric (i.e. $A^{-1} = A$), and
2. for every conjugate A' of A there exists $X' \subset G$ such that $AA' \subset AX'$ and $|X'| \leq K$.

Is this the right definition? Can we connect this definition to small skew doubling? Can we restate the product theorem for conjugates in terms of K-approximate normal subgroups? What other parts of arithmetic combinatorics generalize in this way?