WHAT IS...

an Approximate Group?

Ben Green

Let A be a nonempty finite subset of a group G. Before saying what it means for A to be an approximate subgroup of G, let us consider the easier question of what it means for A to be an actual subgroup of G. Throughout this article we adopt the following standard notation. If $A, B \subseteq G$ we write $A^{-1} := \{a^{-1} : a \in A\}$, $AB := \{ab : a \in A, b \in B\}$ and $A^n := \{a_1 \dots a_n : a_1, \dots, a_n \in A\}$. We say that A is *symmetric* if $A^{-1} = A$.

Here, then, are three easily proven characterisations of what it means to be a subgroup:

(i) If $x, y \in A$, then $xy^{-1} \in A$;
(ii) A is symmetric, contains the identity, and $|A^2| = |A|$;
(iii) A is symmetric, contains the identity, and A^2 coincides with some right-translate Ax of A.

Approximate group theory is concerned with what happens when we try to relax these statements. Let $K \geqslant 1$ be a parameter; the bigger K is, the more relaxed we are going to be. Consider the following properties that a set A may have:

(i) If x, y are selected randomly from A, then $xy^{-1} \in A$ with probability at least $1/K$;
(ii) A is symmetric and $|A^2| \leqslant K|A|$;
(iii) A is symmetric and A^2 can be covered by K right-translates of A.

Each of these is a reasonable notion of approximate group, but (iii) has become standard.

Definition (Tao). Let A be a symmetric subset of a group G. Then we say that A is a K-approximate group if A^2 is covered by K right- (or left-) translates of A.

Rather surprisingly, it hardly matters which of (i), (ii), or (iii) one chooses as "the" definition so long as one is only interested in the "rough" nature of A. For example, if A is symmetric and satisfies (i) then there is a set $\tilde{A} \subseteq A^4$ satisfying (iii) with parameter $\tilde{K}$, and with $\frac{1}{\tilde{K}} \leqslant \frac{|\tilde{A}|}{|A|} \leqslant \tilde{K}$, where $\tilde{K}$ is bounded polynomially in K. This result, which is not at all obvious, is essentially the Balog-Szemerédi-Gowers (BSG) theorem. Other equivalences of a similar type between (i), (ii), and (iii) were described by Tao, building on fundamental work of Ruzsa.

Let us give some examples of approximate groups.

Example 1. Any genuine subgroup A is a 1-approximate group.

Example 2. Any geometric progression $A = \{g^n : -N \leqslant n \leqslant N\}$, $g \in G$, is a 2-approximate group.

Example 3. Let $x_1, \dots, x_d \in \mathbb{Z}$. Then the d-dimensional *generalised arithmetic progression* $A = \{n_1 x_1 + \cdots + n_d x_d : |n_i| \leqslant N_i\}$ is a 2^d-approximate subgroup of $\mathbb{Z}$ (written with additive notation).

Example 4. If

$$S = \{\left(\begin{smallmatrix} 1 & n_1 & n_3 \\ 0 & 1 & n_2 \\ 0 & 0 & 1 \end{smallmatrix}\right) : |n_1|, |n_2| \leqslant N, |n_3| \leqslant N^2\},$$

then $A := S \cup S^{-1}$ is a 100-approximate group. This is an example of a *nilprogression*.

The definition of approximate group is rather combinatorial, but the above examples have an algebraic flavour. The *rough classification problem* for approximate groups is to understand the extent to which an arbitrary approximate group A looks roughly like an algebraic example such as one of those described above.

A solution to the rough classification problem for approximate subgroups of $\mathbb{Z}$ was given by

---

Ben Green is the Herchel Smith Professor of Pure Mathematics at the University of Cambridge and Fellow of Trinity College. His email address is B.J.Green@dpmms.cam.ac.uk.

DOI: http://dx.doi.org/10.1090/noti829

Freiman and (later with a simpler proof) by Ruzsa. They showed that every K-approximate group A is contained in P, a d-dimensional generalised arithmetic progression, where $d \leqslant K$ and $|P|/|A| \leqslant f_1(K)$ for some function f_1. Very recently a solution to the rough classification problem in general was given in [1], building on a major breakthrough (using model theory) by Hrushovski and influenced by Gromov's theorem that groups of polynomial growth are virtually nilpotent. [1] shows that any approximate group is contained in a "coset nilprogression" P with $|P|/|A| \leqslant f_2(K)$: roughly speaking, an object built from examples such as the four described above.

These results are rather qualitative in nature. Whilst $f_1(K)$ can be taken to be merely exponential in K, no effective bound is known for $f_2(K)$ because [1] relies on an ultrafilter argument and an appeal to "infinitary" analysis results connected with Hilbert's fifth problem. In certain specific situations good quantitative results are known. In a seminal paper, Helfgott showed that if A is a K-approximate subgroup of $G = \mathrm{SL}_2(\mathbb{F}_p)$, then either $|A|/|G| \geqslant K^{-C}$ or else at least $K^{-C}|A|$ elements of A are contained in a soluble group (for example, the upper-triangular matrices). He later obtained an appropriate generalisation of this to $\mathrm{SL}_3(\mathbb{F}_p)$, and subsequent work of Pyber-Szabó and Breuillard-Green-Tao further generalised this to $\mathrm{SL}_n(\mathbb{F}_p)$ and other linear groups.

Where do approximate groups arise? We give two examples. The first is in connection with the topic of growth in groups. Let G be a group generated by a finite symmetric set S. If G is a free group (say), then $|S^n|$ will grow exponentially in n. At the other extreme we have the notion of *polynomial growth*, where $|S^n| \leqslant n^d$ for all large n. In this case there are infinitely many n for which S^n is a 10^d-approximate group.

By combining this observation with the rough classification, one obtains certain extensions of Gromov's theorem. Perhaps future developments will lead to the conclusion that G is virtually nilpotent under much weaker assumptions such as $|S^n| \leqslant \exp(n^c)$ for infinitely many n.

The second example comes from *expanders* [2], [3]. If G is a finite group then a symmetric set S of generators has the *expansion property with constant* ε if whenever $A \subseteq G$ is a set with $|A| < |G|/2$, we have $|AS| \geqslant (1+\varepsilon)|A|$. Bourgain and Gamburd used Helfgott's work to find new families of generators for $\mathrm{SL}_2(\mathbb{F}_p)$ and other groups with the expansion property. For example, answering a question of Lubotzky, they showed that the set $S = \{A, A^{-1}, B, B^{-1}\}$ has this property with $\epsilon > 0$ independent of p, where $A = \left(\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right)$. We give a rough sketch of their argument.

It is known that the expansion property is equivalent to the rapid equidistribution, in time $\sim \log |G|$, of the random walk with generating set S. Suppose that X_n is the G-valued random variable describing the nth step of this walk. Thus, in our example, X_1 takes each of the values A, A^{-1}, B, B^{-1} with probability $\frac{1}{4}$, and X_n is distributed as the product of n independent copies of X_1.

By an application of representation theory due to Sarnak and Xue it suffices to prove the weaker statement that X_n is "somewhat" uniform at time $n \sim \log |G|$.

Now it is not hard to show that X_n becomes "smoother" as n increases. For each n there is a dichotomy: either X_{2n} is "much" smoother than X_n or $X_{2n} \approx X_n$ in some sense. If the former option occurs frequently, then X_n will rapidly become somewhat uniform on G, thereby concluding the proof. Suppose, by contrast, that $X_{2n} \approx X_n$; then the product of two independent copies of X_n has almost the same distribution as X_n. This basically implies that the support $\mathrm{Supp}(X_n)$ of X_n satisfies property (i) above with some smallish value of K. By the BSG theorem a large chunk of $\mathrm{Supp}(X_{4n})$ satisfies property (iii) and so is a $\tilde{K}$-approximate group. This is how approximate groups arise in the study of expanders.

Applying Helfgott's result we conclude that either $\mathrm{Supp}(X_{4n})$ is almost all of G, which implies that X_{4n} is somewhat uniform on G, or else a large part of $\mathrm{Supp}(X_{4n})$ generates a soluble group. This second possibility, however, may be ruled out. In fact, for $n \leqslant \frac{1}{100} \log |G|$ the random walk X_{4n} behaves like a random walk on a free group, whilst if a large chunk of $\mathrm{Supp}(X_{4n})$ were soluble one would have many commutation relations $[[M_1, M_2], [M_3, M_4]] = I$.

Let me conclude by stating one of my favourite open problems, now known as the *Polynomial Freiman-Ruzsa conjecture*. Suppose that $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a function which is weakly linear in the sense that $f(x+y) - f(x) - f(y)$ takes only K different values as x, y range over $\mathbb{F}_2^n$. Is $f(x) = g(x) + h(x)$, where g is linear and $|\operatorname{im} h| \leqslant K^C$? Ruzsa showed that this is equivalent to a good quantitative classification of the approximate subgroups of $\mathbb{F}_2^n$.

This is easy to achieve with $|\operatorname{im} h| \leqslant 2^K$. In deep recent work Sanders, building on work of Schoen and Croot-Sisask, showed that we can have $|\operatorname{im} h| \leqslant e^{C(\log K)^4}$, the current state of the art.

References

[1] E. Breuillard, B J. Green, and T. C. Tao, The structure of approximate groups, preprint.

[2] B. J. Green, *Approximate groups and their applications: Work of Bourgain, Gamburd, Helfgott and Sarnak*, Current Events Bulletin of the AMS, 2010.

[3] P. Sarnak, What is…an expander? *Notices Amer. Math. Soc.* **51** (2004), no. 7, 762–763.