什么是近似群？

Ben Green

设 A 是群 G 的非空有限子集. 在给出 A 是 G 的近似子群 (approximate subgroup) 的定义前，我们先考虑一个较为简单的问题，即怎样的 A 是 G 的真正的子群. 在本文中我们采用如下标准表示：设 $A, B \subseteq G$, 记 $A^{-1} := \{a^{-1} : a \in A\}$, $AB := \{ab : a \in A, b \in B\}$, 以及 $A^n := \{a_1 \cdots a_n : a_1, \ldots, a_n \in A\}$. 若 $A^{-1} = A$, 则称 A 是对称的.

那么这里有 3 个很容易证明的子群的特征：

(i) 若 $x, y \in A$, 则 $xy^{-1} \in A$;

(ii) A 是对称的，包含单位元，且 $|A^2| = |A|$;

(iii) A 是对称的，包含单位元，且 A^2 与 A 在某个右平移作用下的像 Ax 相等.

近似群理论关注当我们试着放宽这些条件时会产生什么结论. 设 $K \geq 1$ 是参数；K 越大，我们越放宽条件. 考虑集合 A 可能具有如下性质：

(i) 若 x, y 从 A 中随机选取，则 $xy^{-1} \in A$ 的概率至少为 $1/K$;

(ii) A 是对称的且 $|A^2| \leq K|A|$;

(iii) A 是对称的且 A^2 可以被 A 的 K 个右平移作用下的像覆盖.

这些性质中的每一个都是近似群的合理定义，但 (iii) 已经成为了标准定义.

定义 (陶哲轩) 令 A 是群 G 的对称子集. 若 A^2 被 A 的 K 个右 (或左) 平移作用下的像覆盖，则称 A 是 K–近似群.

相当令人惊讶地，只要我们只关心 A 的 "大致的" 本质，选择 (i), (ii) 或 (iii) 中任一个作为近似群的 "定义" 差别都不大. 例如，若 A 是对称的且满足 (i), 则存在集合 $\tilde{A} \subseteq A^4$ 对参数 $\tilde{K}$ 满足 (iii), 且有 $\frac{1}{\tilde{K}} \leq \frac{|\tilde{A}|}{|A|} \leq \tilde{K}$, 其中 $\tilde{K}$ 被 K 的多项式所界. 这个结果一点也不平凡，其实质上是 Balog-Szemerédi (斯泽梅雷迪)–Gowers (高尔斯)(BSG) 定理. 陶哲轩在 Ruzsa 的基础性工作之上，描述了 (i), (ii), (iii) 之间的其它类似类型的等价性.

我们给出一些近似群的例子.

例 1 任意真 (genuine) 子群 A 都是 1–近似群.

例 2 任意几何数列 $A = \{g^n : -N \leq n \leq N\}$, $g \in G$ 是 2–近似群.

例 3 设 $x_1, \ldots, x_d \in \mathbb{Z}$. 则 d 维 *广义等差数列* (*generalised arithmetic progression*) $A = \{n_1x_1 + \cdots + n_dx_d : |n_i| \leq N_i\}$ 是 $\mathbb{Z}$ 的 2^d– 近似子群 (群运算记为加法).

例 4 若

$$S = \left\{ \begin{pmatrix} 1 & n_1 & n_3 \\ 0 & 1 & n_2 \\ 0 & 0 & 1 \end{pmatrix} : |n_1|, |n_2| \leq N, |n_3| \leq N^2 \right\},$$

译自：Notices of the AMS, Vol. 59 (2012), No. 5, p. 655–656, What is an Approximate Group? Ben Green.

Ben Green 是剑桥大学 Herchel Smith 纯数学教授，三一学院院士. 他的邮箱地址为 B.J.Green@dpmms.cam.ac.uk.

则 $A := S \cup S^{-1}$ 是 100–近似群. 这是 **诣零列** (*nilprogression*) 的一个例子.

近似群的定义方式更多是组合的, 但上面一些例子有一种代数的意味. 近似群的 **粗略分类问题** (*rough classification problem*) 是理解任意一个近似群 A 在多大程度上大致看起来像上述例子之一的一个代数例子.

Freiman 和 (稍后给出了一个更简单的证明的) Ruzsa 给出了对 $\mathbb{Z}$ 的近似子群粗略分类问题的解. 他们证明了任意 K–近似群 A 都包含在一个 d 维广义等差数列 P 中, 其中 $d \leq K$, 且对某个函数 f_1 有 $|P|/|A| \leq f_1(K)$. 最近, 基于 Hrushovski 的一项重大突破 (利用模型论) 和受到 Gromov (格罗莫夫) 关于多项式增长的群几乎都是虚幂零的 (virtually nilpotent) 定理的影响, [1] 给出了一般粗略分类问题的一个解. [1] 证明了任意近似群都包含在一个满足 $|P|/|A| \leq f_2(K)$ 的 "陪集诣零列" P 中: 大致地说, 它可由如上面 4 个例子这样的例子构造出来.

这些结果实质上是相当定性的. 尽管函数 $f_1(K)$ 可以取为 K 的指数式, 然而对 $f_2(K)$ 并无已知有效的界, 这是因为 [1] 依赖于超滤子论证且需要用到与 Hilbert (希尔伯特) 第 5 问题相关的 "无穷" 分析的结果. 在一些特定的情形, 已知有一些好的定量结果. 在 Helfgott 一篇影响深远的论文中, 他证明了若 A 是 $G = \mathrm{SL}_2(\mathbb{F}_p)$ 的 K– 近似子群, 则或 $|A|/|G| \geq K^{-C}$, 或至少有 $K^{-C}|A|$ 个 A 中元素包含在一个可解群中 (例如, 上三角矩阵群). 随后, Helfgott 将此结果适当地推广到 $\mathrm{SL}_3(\mathbb{F}_p)$, Pyber-Szabó 和 Breuillard-Green–陶哲轩后续的工作则进一步将此结果推广到 $\mathrm{SL}_n(\mathbb{F}_p)$ 和另一些线性群.

近似群从何而来? 我们给出两个例子. 第 1 个例子与群的增长 (growth in groups) 主题有关. 令群 G 由一个有限对称集 S 生成. 若 G 是一个 (例如) 自由群, 则 $|S^n|$ 关于 n 指数增长. 而另一个极端情形, 我们有 **多项式增长** (*polynomial growth*) 的概念, 即 $|S^n| \leq n^d$ 对所有大的 n 成立. 在此情形有无限多个 n 使得 S^n 是 10^d–近似群.

通过将此观察与粗略分类问题结合起来, 则可得到 Gromov 定理的某些推广. 也许未来的发展将会导致结论: 在弱得多的条件下, 如 $|S^n| \leq \exp(n^c)$ 对无限多个 n 成立, 则 G 是虚幂零的.

第 2 个例子来自 **扩张子** (*expanders*) [2], [3]. 若 G 是一个有限群, 则诸生成元的对称集 S 具有 **关于常数 ε 的扩张性** (*expansion property with constant ε*), 即只要集合 $A \subseteq G$ 满足 $|A| < |G|/2$, 则有 $|AS| \geq (1+\varepsilon)|A|$. Bourgain (布尔盖恩) 和 Gamburd 利用 Helfgott 的工作找到了 $\mathrm{SL}_2(\mathbb{F}_p)$ 以及具有扩张性的另一些群新的生成元族. 例如, 为了回答 Lubotzky 的问题, 他们证明了集合 $S = \{A, A^{-1}, B, B^{-1}\}$ 对独立于 p 的 $\varepsilon > 0$ 具有扩张性, 其中 $A = \left(\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right)$. 我们粗略地概述他们的论证.

已知扩张性等价于具有生成集 S 的随机游动在时间 $\sim \log|G|$ 上的快速等分布. 假设 X_n 是描述该随机游动第 n 步的 G 值随机变量. 则在我们的例子中, X_1 取每个值 A, A^{-1}, B, B^{-1} 的概率都为 $1/4$, 且 X_n 的分布为 n 个独立的 X_1 乘积的分布.

应用 Sarnak 和 Xue 的表示论结果, 只需证明较弱的命题, 即 X_n 在时间 $n \sim \log|G|$ 内 "某种程度上" 是均匀的.

现在不难证明当 n 增大时, X_n 变得 "更加光滑". 对任意 n 都可分为两种截然不同

情形：或者 X_{2n} 比 X_n "光滑得多"，或者在某种意义下 $X_{2n} \approx X_n$. 若前一种情形经常出现，则 X_n 会快速地在 G 上达到 "某种程度的" 均匀，从而完成证明. 与此对照，假设 $X_{2n} \approx X_n$; 则两个独立的 X_n 乘积的分布与 X_n 几乎相同. 这基本上蕴涵了 X_n 的支集 $\mathrm{Supp}(X_n)$ 对相当小的 K 值满足上面的性质 (i). 由 BSG 定理，$\mathrm{Supp}(X_{4n})$ 的很大一部分满足性质 (iii)，从而是 $\tilde{K}$–近似群. 这就是近似群在扩张子的研究中产生的原因.

应用 Helfgott 的结果，我们可以得到或者 $\mathrm{Supp}(X_{4n})$ 几乎就是全部 G，从而推出 X_{4n} 在 G 上某种程度均匀，或者 $\mathrm{Supp}(X_{4n})$ 的大部分生成一个可解群. 然而，第 2 种可能性也许会被排除. 事实上，对 $n \leq \frac{1}{100}\log|G|$，随机游动 X_{4n} 的行为像自由群上的一个随机游动，而当 $\mathrm{Supp}(X_{4n})$ 中大部分是可解的时，我们有很多交换关系 $[[M_1, M_2], [M_3, M_4]] = I$.

以我最喜欢的一个未决问题来结束本文，这个问题现在被称为 多项式 Freiman-Ruzsa 猜想 (*Polynomial Freiman-Ruzsa conjecture*). 假设 $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ 在下述意义下是弱线性函数，即当 x, y 跑遍 $\mathbb{F}_2^n$ 中的元素时，$f(x+y) - f(x) - f(y)$ 只取 K 个不同的值. 是否有 $f(x) = g(x) + h(x)$? 其中 g 是线性的且 $|\mathrm{im}\ h| \leq K^C$. Ruzsa 证明了这等价于对 $\mathbb{F}_2^n$ 的近似子群的一个好的定量分类.

当 $|\mathrm{im}\ h| \leq 2^K$ 时，这是容易得到的. 基于 Schoen 和 Croot-Sisask 的工作，Sanders 在最近的深刻工作中证明了我们能有 $|\mathrm{im}\ h| \leq e^{C(\log K)^4}$，这是该领域现在的最佳结果.

参考文献

[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

(朱力 译　　王润玲 校)

****

(上接 288 页)

[2] D. Gomez, J. Gutierrez, Á. Ibeas, D. Sevilla, Common factors of resultants modulo p, Bull. Aust. Math. Soc. 79 (2009) 299–302.

[3] R. K. Guy,The strong law of small numbers, Amer. Math. Monthly 95 no. 8 (Oct 1988) 697–712.

[4] S. Janson, Resultant and discriminant of polynomials, `http://www2.math.uu.se/~svante/papers/sjN5.pdf`.

[5] D. I. Khomovsky, On the relationship between the number of solutions of congruence systems and the resultant of two polynomials, INTEGERS — Electronic Journal of Combinatorial Number Theory 16 A41.

[6] The Prime Glossary, `http://primes.utm.edu/glossary/page.php?sort=LawOfSmall`.

[7] H. J. S. Smith, On systems of linear indeterminate equations and congruences, Philos. Trans. R. Soc. London 151 no. 1 293–326. Reprinted in The Collected Mathematical Papers of Henry John Stephen Smith I. Ed. J. W. L. Glaisher. Clarendon Press, Oxford, 1894. 367–409.

(陆柱家 译　　童欣 校)