Capítulo 4

Una conjetura de Babai

En esta lectura, $(G, \cdot)$ es un grupo (usualmente finito) y A es un subconjunto (siempre finito) de G. Vamos a considerar una variación de una conjetura de Babai:[1]

Conjetura 20. *Hay $c > 0$ tal que, para todo $n \in \mathbb{Z}^+$ y todo $A \subseteq G = S_n$ con $\langle A \rangle = G$, tenemos*

$$\operatorname{diam}(\Gamma(G, A)) \leq (\log |G|)^c.$$

Recuerde que en la lectura anterior, probamos que

$$\operatorname{diam}(\Gamma(G, A)) \geq \frac{\log |G|}{\log |A|}.$$

Entonces, esta conjetura dice que, no importa cual conjunto de generadores que escogemos para S_n, el grafo de Cayley que obtenemos es casi tan "compacto" como posible.[2]

Conjetura 20 se queda abierta, aunque han estado mucho trabajo hasta una demostración por muchos autores. En esta lectura, vamos a probar un caso muy especial.

[1] La conjetura original de Babai dice el siguiente:
Hay $c > 0$ tal que, para todo grupo finito simple no-abeliano G, y todo $A \subseteq G$ con $\langle A \rangle = G$, tenemos

$$\operatorname{diam}(\Gamma(G, A)) \leq (\log |G|)^c.$$

El grupo S_n no es simple, entonces la conjetura no aplica directamente a S_n. Pero, por supuesto, el grupo A_n es simple para $n > 5$ y en ejercicos vamos a ver que la conjetura es verdadera para A_n si y sólo si es verdadera para S_n. Entonces, Conjetura 20 es equivalente a un caso especial del conjetura original.

La clasificación de grupos finitos y simples dice que un grupo finito simple es un los siguientes:

1. cíclico de orden un primo;
2. A_n con $n > 5$;
3. un "grupo de tipo de Lie";
4. un de 26 grupos sporádicos.

Por lo tanto, para probar la conjetura original, se necesitaría probar la conjetura para los grupos de tipo de Lie en adición a los grupos alternantes. En esta situación la conjetura se queda abierta, pero ha estado probado en casos especiales – mire, por ejemplo, Ejercicio (4) . (¿Porqué no necesitamos considerar los 26 grupos finitos simples?)

Note que la conjetura es definitivamente no verdadera para grupos finitos simples y **abelianos** – mire Ejemplo 2 en la lectura anterior.

Por fin, note que la conjetura pareció primeramente en un artículo de Babai y Seress [2], entonces debemos llamarlo *una conjetura de Babai–Seress....* No hago este porque, usualmente, en la literatura la conjetura es atributado a Babai solamente (no se porqué).

[2] De hecho, creo que no sea sabido si hay una familia infinita de conjuntos de generadores s en S_n para que el

4.1 Primeras observaciones

De aquí, vamos a suponer que el conjunto A satisface $A = A^{-1}$ y $1 \in A$. Vamos a ver en ejercicios que este supuesto no importa – si podríamos probar Conjetura 20 para conjuntos generandos de esta forma, podríamos probar Conjetura 20 completamente.

Ahora, gracias a Corolario 18 de Lectura 3, podemos reescribir Conjetura 20 en una forma equivalente:

Conjetura 21. *Hay $c > 0$ tal que, para todo $n \in \mathbb{Z}^+$ y todo $A \subseteq G = S_n$ con $\langle A \rangle = G$, tenemos $A^k = G$ para algún $k \leq (\log |G|)^c$.*

Sabemos que $|S_n| = n!$ y el crecimiento de la función ha estado estudiado después de muchos años. El siguiente es una versión debil de la aproximación de Stirling.[3]

Teorema 22. *Hay constantes $d_1, d_2 > 0$ tal que*

$$e^{d_1 n} < n! < e^{d_2 n^2}$$

Con este teorema, podemos reescribir Conjetura 20 una tercera vez:

Conjetura 23. *Hay $c \in \mathbb{Z}^+$ tal que, para todo $n \in \mathbb{Z}^+$ y todo $A \subseteq G = S_n$ con $\langle A \rangle = G$, tenemos $A^k = G$ para $k = n^c$.*

Note que el 'c' aquí es diferente al 'c' en Conjetura 21.

4.2 Un caso simple

En esta sección, vamos a probar la proposición siguiente:

Proposición 24. *Para todo $n \in \mathbb{Z}^+$ y todo $A \subseteq G = S_n$ que genera G* **y contiene una transposición**, *tenemos $A^{2n^3+n} = G$.*

La condición en negro es importante: vamos probar la conjetura de Babai solamente para conjuntos que contienen una transposición (observe que $2n^3 + n \leq n^5$ para $n \geq 2$). Vamos a probar la proposición en tres lemas fáciles:

Lema 25. *Todo elemento en S_n es un product de n transposiciones.*

Demostración. Este es una consecuencia de Ejercicio (7) de Capítulo 3. □

Lema 26. *El conjunto A^{2n^2+1} contiene todas las transposiciones de S_n.*

diametro es super-lineal en $\log |G|$. Es decir, es posible que se puede mejorar la conclusíon de la conjetura a

$$\operatorname{diam}(\Gamma(G, A)) > c(\log |G|).$$

[3]Para una introducción corta a esta aproximación, va a `http://www.math.uconn.edu/~kconrad/blurbs/analysis/stirling.pdf`.

Demostración. La acción de S_n es 2-transitivo, entonces Corolario 13 de Capítulo 2 implica que A^{n^2} es 2-transitivo.

Por supuesto A contiene una transposición g y, podemos renombrar Ω tal que $g = (1, 2)$. Supóngase que (a, b) es una transposición en S_n. Ya que A^{n^2} es 2-transitivo, hay $h \in A^{n^2}$ tal que $h(1) = a$ y $h(2) = b$. Ya que $A = A^{-1}$, tenemos $A^{n^2} = (A^{n^2})^{-1}$, entonces $h^{-1} \in A^{n^2}$. Ahora observe que

$$h \cdot (1, 2) \cdot h^{-1} = (a, b)$$

y, además $h \cdot (1, 2) \cdot h^{-1} \in A^{2n^2+1}$. □

Lema 27. $A^{2n^3+n} = S_n$.

Demostración. Observe que $\underbrace{A^{2n^2+1} \times A^{2n^2+1} \times \cdots \times A^{2n^2+1}}_{n}$ contiene todos productos de n transposiciones en S_n. Entonces este conjunto es igual a S_n. □

Note que en estos lemas, hemos usado el hecho que A genera G solamente para concluir que podemos multiplicar A por sí mismo para obtener un conjunto 2-transitivo. Si habimos supuesto que A sae un conjunto 2-transitivo, haríamos obtenido la misma conclusión – que podriámos multiplicar A por sí mismor para obtener S_n. Recordemos este resultado para el caso especial donde A es un subgrupo:

Proposición 28. *Supóngase que G es un subgrupo 2-transitivo de S_n* **que contiene una transposición**. *Entonces $G = S_n$.*

Esta proposición es una versión debil de un caso especial de un teorema de Jordan – mire Ejercicio (5) abajo.

4.3 Resultados más fuertes

4.3.1 3-ciclos

Es posible probar resultados similar pero más fuerte de Proposión 28. Por ejemplo, por estudiando 3-ciclos en lugar de transposiciones, se puede versiones de Lema 25, 26 y 27 para obtener

Proposición 29. *Hay un $c > 0$ tal que para todo $n \in \mathbb{Z}^+$ y todo $A \subseteq G = S_n$ que genera G* **y contiene un 3-ciclo**, *tenemos $A^{n^c} = G$.*

Otra vez, se puede aplicar el método de demostración para obtener un teorema clásico:

Proposición 30. *Supóngase que G es un subgrupo 3-transitivo de S_n* **que contiene un 3-ciclo**. *Entonces $G = A_n$ o S_n.*

Y, otra vez, es posible mejorar esta proposición para obtener un caso especial de un teorema de Jordan – mire Ejercicio (6) .

4.3.2 Otros elementos especiales

Podríamos continuar en una manera similar para obtener resultados similares. Se puede probar el siguiente:

Proposición 31. *Para todo $d > 0$, hay un $c > 0$ tal que para todo $n \in \mathbb{Z}^+$ y todo $A \subseteq G = S_n$ que genera G* **y contiene un elemento que mova menor que** d **puntos de** Ω*, tenemos $A^{n^c} = G$.*

Los métodos son muy similares. Sin embargo, se necesitar tener cuidado si quiere probar teoremas clásicos en la misma manera. Por ejemplo, en adición a A_n y S_n, el grupo D_5 en su acción sobre el pentágono es (a) primitivo, y (b) tiene elementos que movan 4-puntos (son productos de 2 transposiciones – mire Ejemplo 2 de Capítulo 2).

Sin embargo, si restrigimos nuestra atención a **ciclos de orden primo**, podemos obtener el teorema de Jordan. Para detalles, mire [9, p. 39].

Teorema 32. *Si G es un subgrupo primitivo de S_n que contiene un p-ciclo donde p es un primo tal que $p \leq n - 3$, entonces $G = A_n$ o S_n.*

4.3.3 Grandes conjuntos

Por fin, vamos a usar el método de demostración de un teorema de Bochert [5] sobre el tamaño de grupos finitos primitivos. El resultado de Bochert es el siguiente:

Teorema 33. *Sea G un grupo finito primitivo y G no es igual a A_n o S_n. Entonces*

$$|G| \leq \frac{n!}{\lfloor \frac{n+1}{2} \rfloor !}.$$

Podemos editar la demostración de este teorema para probar el teorema de Babai para grandes conjuntos:

Proposición 34. *Supóngase que A es un subgrupo de S_n que genera S_n y para que $A = A^{-1}$. Hay un constante $c \in \mathbb{Z}^+$ tal que si $|A| > \frac{n!}{\lfloor \frac{n+1}{2} \rfloor !}$, entonces $A^{n^c} = S_n$.*

Demostración. Sea H un subgrupo de S_n de índice m. Entonces hay m cosets de H en S_n y estos cosets forman una partición de S_n. Entonces, si K es un subconjunto de S_n tal que $|K| > m$, por el principio de palomar, hay un coset de H, gH, tal que $|K \cap gH| \geq 2$. Sea $h_1, h_2 \in H$ tal que $gh_1, gh_2 \in K \cap gH$, y ahora observe que

$$(gh_1)^{-1} \cdot (gh_2) = h_1^{-1} g^{-1} g h_2 = h_1^{-1} \cdot h_2 \in H.$$

Además $(gh_1)^{-1} \cdot (gh_2) \in K^{-1}K$ y concluimos que $K^{-1}K \cap H \neq \{1\}$.

Ses Λ un subconjunto de $\Omega = \{1, \ldots, n\}$. Voy a escribir

$$S_\Lambda = \{g \in S_n \mid g(i) = i \text{ para todo } i \in \Omega \setminus \Lambda\}.$$

Entonces S_Λ es el conjunto de permutaciones que movan elementos de Λ y fijan elementos de $\Omega \setminus \Lambda$. Observe que, si $|\Lambda| = k$, entonces $|S_\Lambda| = k!$.

Ahora vamos a usar el supuesto que $|A| > \frac{n!}{\lfloor \frac{n+1}{2} \rfloor !}$. Este supuesto, y la discusión del primer párrafo implica que para cualquier Λ de tamaño $k \geq \lfloor \frac{n+1}{2} \rfloor !$, $A^2 = A^{-1}A$ contiene un elemento de S_Λ.

Ahora sea ℓ el número mayor tal que $A^2 \cap S_\Lambda = \{1\}$ para algún $\Lambda \subset \Omega$ con $|\Lambda| = \ell$. Etonces $1 \leq \ell < \lfloor \frac{n+1}{2} \rfloor !$.

Sea Λ_1 un conjunto de tamaño $\ell + 1$; entonces, hay un elemento $g \in A^2 \cap S_{\Lambda_1}$ tal que g movan todos los elementos de Λ_1. Sea Λ_2 un conjunto de tamaño $\ell + 1$ tal que $|\Lambda_1 \cap \Lambda_1| = 1$; entonces, hay un elemento $h \in A^2 \cap S_{\Lambda_1}$ tal que h movan todos los elementos de Λ_2.

Por Ejercicio (7) , $f = ghg^{-1}h^{-1}$ es 3-ciclo y, por construcción, $f \in A^8$. Ahora, Proposición 29 implica que hay un $c \in \mathbb{Z}^+$ tal que $(A^8)^{n^c} = S_n$ y, ya que $n \geq 2$, tenemos $A^{n^{c+3}} = S_n$. □

Hay varios otros resultados que probar la conjetura de Babai en casos especiales, por ejemplo [1, 4]. Sin embargo, sin duda, el teorema de Helfgott–Seress es el resultado definitivo hasta ahora [8]: su teorema es completamente general – no hay un supuesto especial sobre el conjunto generando – y la conclusión es fuerte... pero no del todo tan fuerte como la conjetura.

4.4 Ejercicios

(1) Supóngase que hay $c > 0$ tal que, para todo $n \in \mathbb{Z}^+$ y todo $A \subseteq G = A_n$ con $\langle A \rangle = G$, tenemos

$$\operatorname{diam}(\Gamma(G, A)) \leq (\log |G|)^c.$$

Pruebe que, entonces, hay $d > 0$ tal que, para todo $n \in \mathbb{Z}^+$ y todo $A \subseteq G = S_n$ con $\langle A \rangle = G$, tenemos

$$\operatorname{diam}(\Gamma(G, A)) \leq (\log |G|)^d.$$

(2) Pruebe el converso del ejercicio anterior.

(3) (Difícil) Pruebe que si Conjetura 20 es verdadera para todos los conjuntos de generadores A tal que $A = A^{-1}$ y $1 \in A$, entonces es verdadera para todos los conjuntos de generadores.

(4) Escribe $\mathbb{F}_p$ para el cuerpo de tamaño p, donde p es un primo. Defina el grupo

$$\mathrm{SL}_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{F}_p,\ ad - bc = 1 \right\}.$$

Este grupo es simple para $p \geq 5$ (y es un subgrupo del grupo $\mathrm{GL}_2(\mathbb{F}_p)$ definido en Capítulo 2). Helfgott ha probado el teorema siguiente [7]:
Hay un $\varepsilon > 0$ tal que, para todo $p > 0$ y para todo $A \subseteq G = \mathrm{SL}_2(\mathbb{F}_p)$ con $\langle A \rangle = G$, tenemos uno del siguiente:

1. $|AAA| \geq |A|^{1+\varepsilon}$*; o*
2. $AAA = G$.

Pruebe que este teorema implica que la conjetura de Babai es verdadera para los grupos $\mathrm{SL}_2(\mathbb{F}_p)$.

(5) Recuerde la definición de una acción primitiva en Ejercicio (11) de Capítulo 2. Mejore Proposición 28, y pruebe que si G es un subgrupo primitivo de S_n **que contiene una transposición**, entonces $G = S_n$.

(6)

(a) Pruebe Proposición 29.

(b) Pruebe Proposición 30.

(c) Mejore Proposición 30 y pruebe que si G es un subgrupo primitivo de S_n **que contiene un 3-ciclo**, entonces $G = A_n$ o S_n.

(7) Sea $g, h \in S_n$; Λ_g los elementos de Ω movado por g; y Λ_h los elementos de Ω movado por h. Probar que, si $|\Lambda_g \cap \Lambda_h| = 1$, entonces $g^{-1}h^{-1}gh$ es un 3-ciclo.

(8) Use la demostración de Proposición 34 para probar Teorema 33.

(9) ¿Puede debilitar la cota en Proposicion 34 a $|A| > \frac{n!}{\lfloor \frac{n+3}{2} \rfloor !}$ y obtener la misma conclusión?