Contents

Capítulo 1

Introducción al crecimiento

1.1 Definiciones

En esta lectura, queremos estudiar subconjuntos finitos de grupos. Sea $(G, \cdot)$ un grupo y sea A un subconjunto no vacío de G. Podemos definir

$$A^2 = A \cdot A = \{a_1 \cdot a_2 \mid a_1, a_2 \in A\},$$
$$A^3 = A \cdot A \cdot A = \{a_1 \cdot a_2 \cdot a_3 \mid a_1, a_2, a_3 \in A\},$$

y, similarmente, tenemos $A^4, A^5, \ldots, A^k, \ldots$, para todo $k \in \mathbb{Z}^+$. En este curso queremos estudiar el *tamaño* de estos conjuntos. Entonces, estudiamos la secuencia de enteros positivos

$$|A|, |A^2|, |A^3|, |A^4|, \ldots \tag{1.1}$$

Lema 1. *La secuencia* (1.1) *es no decreciente.*

Demostración. Sea $a \in A$. El conjunto A^k contiene el conjunto

$$\{a \cdot b \mid b \in A^{k-1}\}.$$

Ahora observe que la función $\rho_a : G \to G, g \mapsto a \cdot g$ es inyectiva (tiene una inversa). □

A la luz del Lema 1, podemos decir que el conjunto A *crece* cuando es multiplicado por sí mismo. Entonces, llamamos el estudio de la secuencia (1.1) el estudio del *crecimiento* de A.

En este curso, vamos a considerar crecimiento en varios grupos. Ustedes necesitan estar familiarizados con estos grupos:

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}^*, \cdot), (\mathbb{R}, +), (\mathbb{R}, \cdot), (\mathbb{Z}/n\mathbb{Z}, +), (S_n, \cdot), (A_n, \cdot), \cdots$$

Hay dos casos más que son útiles considerar aunque no son exactamente grupos:

1. Si $(\mathbb{F}, +, \cdot)$ es un cuerpo, entonces $(\mathbb{F}^*, \cdot)$ es un grupo. A veces, sera útil considerar subconjuntos de $\mathbb{F}$ que contiene 0 y examinar el compartamiento de tales conjuntos con respecto a "$\cdot$". Es fácil ver que Lema 1 aplica a tales conjuntos también (Verifíquelo!).

2. Si $(R, +, \cdot)$ es un anillo y no es un cuerpo, entonces $(R, \cdot)$ es lejos de ser un grupo. En esta situación es posible encontrar conjuntos que no crecen con respecto a "$\cdot$". Por ejemplo, tome $R = \mathbb{Z}/4\mathbb{Z}$ y sea $A = \{0, 2\}$. En este caso $A \cdot A = \{0\}$ y tenemos $|A \cdot A| < |A|$. Mire Ejercicios 1 para más sobre tales conjuntos.

Necesitamos un poco más terminología: podemos escribir grupos multiplicativamente – $(G, \cdot)$ – como anteriormente o aditivamente – $(G, +)$. En el caso posterior, escribiremos

$$2A = A + A = \{a_1 + a_2 \mid a_1, a_2 \in A\},$$
$$3A = A + A + A = \{a_1 + a_2 + a_3 \mid a_1, a_2, a_3 \in A\}.$$

Es importante notar que si escribo un grupo aditivamente este grupo será siempre abeliano. Si escribo un grupo multiplicativamente este grupo puede ser abeliano o no-abeliano.

Por fin, vamos a escribir cosas como A^{-1}, $A + B$, $A - B$, $A \cdot B$ (para conjuntos A, B); $b + A$ o $b \cdot A$ (para A un conjunto y b un elemento). Espero que las definiciones sean obvias.

1.2 Primeras observaciones

Después de ahora, $(G, \cdot)$ es un grupo y $A, B \subseteq G$. Observe que

$$|A| \leq |A + A| \leq |A|^2.$$

Entonces, concluimos que el crecimiento está siempre entre una función lineal y una función cuadŕatica. Si G es abeliano, podemos mejorar estas cotas:

$$|A| \leq |A + A| \leq \frac{|A|(|A| + 1)}{2}.$$

Ejemplo 1. Sea $A = \{2, 4, 6, 8, 10\}$ y $B = \{2, 4, 8, 16, 32\}$ conjuntos de enteros. Vamos a considerar estos conjuntos como subconjuntos de varios grupos abelianos:

1. Tome $A \subset (\mathbb{Q}, +)$. Entonces $|A + A| = 9 = 2|A| - 1$.
2. Tome $B \subset (\mathbb{Q}^*, \cdot)$. Entonces $|B \cdot B| = 9 = 2|B| - 1$.
3. Tome $A \subset (\mathbb{Q}^*, \cdot)$. Entonces $|A \cdot A| = 14 > \frac{|A|}{2}$.
4. Tome $C = \{1, 2, 4, 6, 8, 9, 10\} \subset (\mathbb{Z}/11\mathbb{Z}, +, \cdot)$. Entonces $|C \cdot C| = 10$ y $|C + C| = 11$.
5. Tome $D = \{(1), (1, 2)(3, 4), (1, 4)(3, 2), (1, 3)(2, 4)\} \subset (S_4, \cdot)$. Entonces $|D \cdot D| = 4 = |D|$.

Un principio importante en el estudio de crecimiento es que "usualmente" los conjuntos crecen. Es decir, si escogemos un conjunto aleatoriamente en algún grupo, es probable que el conjunto crecerá cuadraticamente (o casi cuadraticamente).

Desde otro punto de vista, si encontramos conjuntos que no crecen, queremos probar que estos conjuntos tienen algún tipo de estructura. Tal tipo de resultado se llama un *teorema inverso*. Consideremos Ejemplo 1:

1. El conjunto A es una progresión aritmética. Ustedes probarán en ejercicios que progresiones aritméticas son los conjuntos en $(\mathbb{Q}, +)$ con crecimiento minimal.

2. El conjunto B es una progresión geométrica. Ustedes probarán en ejercicios que progresiones geométricas son los conjuntos en $(\mathbb{Q}, \cdot)$ con crecimiento minimal.

3. El conjunto C es un **gran** conjunto en el cuerpo $(\mathbb{Z}/11\mathbb{Z}, +, \cdot)$. Ya que un cuerpo es cerrado con respecto a "+" y "·", es claro que los grandes conjuntos no pueden crecer mucho.

4. Por fin, el conjunto D es un **subgrupo** en el grupo $(S_4, \cdot)$. Ya que los subgrupos son cerrados con respecto a la operación del grupo, luego D no puede crecer nada.

¿Qué pasa cuando tenemos el menor crecimiento? Ya se puede dar el primer teorema inverso:

Proposición 2. *Supóngase que $A \subset G$ donde $(G, +)$ es abeliano. Los siguientes son equivalentes:*

1. $|A + A| = |A|$;
2. $|A - A| = |A|$;
3. $|nA| = |A|$ *para un entero positivo* $n \neq 1$;
4. $|nA| = |A|$ *para todos enteros positivos;*
5. *Hay un subgrupo finito* $H \leq G$ *tal que* A *es un coset de* H.

Demostración. Vamos a probar (1) implica (5) y los otras se dejan ejercicios.

Escoga $g \in G$ tal que $B = g + A$ y B contiene 0. Observe que

$$|B + B| = |A + A| = |A| = |B|.$$

Además, $B + B \supset \{0\} + B = B$, entonces $B + B = B$. Por un ejercicio, concluimos que B es un subgrupo finito de G y $A = -g + B$ es un un coset de B. □

Lema 3. (Desigualdad triangular de Ruzsa) *Sean A, B y C subconjuntos finitos de un grupo $(G, \cdot)$. Entonces*

$$|A \cdot C^{-1}||B| \leq |A \cdot B^{-1}||B \cdot C^{-1}|.$$

Demostración. Construiremos una inyección $\iota : A \cdot C^{-1} \times B \to A \cdot B^{-1} \times B \cdot C^{-1}$. Para cada $d \in A \cdot C^{-1}$, escojamos $(f_1(d), f_2(d)) = (a, c) \in A \times C$ tal que $d = a \cdot c^{-1}$. Definamos $\iota(d, b) = (f_1(d) \cdot b^{-1}, b \cdot (f_2(d))^{-1})$. Podemos recuperar $d = f_1(d) \cdot (f_2(d))^{-1}$ de $\iota(d, b)$; por lo tanto, podemos recuperar $(f_1, f_2)(d) = (a, c)$, y así también b. Por lo tanto, ι es una inyección. □

Corolario 4. *Sea $X = A \cup A^{-1} \cup \{0\}$.*

1. $\frac{|X^2|}{|A|} \leq 6 \left(\frac{|A^2|}{|A|}\right)^2$.
2. $\frac{|X^3|}{|A|} \leq 14 \left(\frac{|A^3|}{|A|}\right)^3$.
3. *Si $A = A^{-1}$ y $k \geq 3$, entonces* $\frac{|A^k|}{|A|} \leq \left(\frac{|A^3|}{|A|}\right)^{2k-5}$.

Demostración. Mostraremos (1) y dejamos (2) y (3) como ejercicios.

Observe que

$$X^2 = A^2 \cup (A^{-1})^2 \cup (A \cdot A^{-1}) \cup (A^{-1} \cdot A) \cup A \cup A^{-1}.$$

Para mostrar el resultado, es suficiente demostrar que $\frac{|A \cdot A^{-1}|}{|A|} \leq \left(\frac{|A \cdot A|}{|A|}\right)^2$. Por eso, tomamos $C = A$, $B = A^{-1}$ en la desigualdad triangular de Ruzsa. □

Si G es abeliano, es posible probar un resultado más fuerte que 3.[1]

[1]Este resulto puede ser probado en dos maneras: la primera demostración de Plünnecke-Ruzsa usa métodos de la teoría de grafos y es un poco complicada. Recientemente, Petridis encontró una demostración más elementaria.

Teorema 5. (Plünnecke-Ruzsa) *Si A es un subconjunto de un grupo abeliano $(G,+)$. Entonces,*

$$\frac{|kA-\ell A|}{|A|} \leq \left(\frac{|2A|}{|A|}\right)^{k+\ell}.$$

Podemos reescribir este teorema y parte (2) del Corolario 4 de la manera siguiente:

- Supóngase que A es un subconjunto de un grupo $(G,\cdot)$ con $A = A^{-1}$, y sea $K \in \mathbb{R}^+$. Si A *tiene triplicación* K, es decir, si $|A\cdot A\cdot A| \leq K|A|$, entonces $|A^k| \leq K^{2k-5}|A|$ para todo $k \geq 3$.
- Supóngase que A es un subconjunto de un grupo abeliano $(G,+)$, y sea $K \in \mathbb{R}^+$. Si A *tiene duplicación* K, es decir, si $|A+A| \leq K|A|$, entonces $|kA| \leq K^k|A|$ para todo $k \geq 1$.

Entonces, en un grupo abeliano el tamaño de $A+A$ controla la velocidad del crecimiento de A siempre, mientras que en un grupo general el tamaño de $A\cdot A\cdot A$ controla la velocidad de crecimiento de A siempre.

1.3 Ejercicios

(1) Sea A un subconjunto de $\mathbb{Z}$.
(a) Muestre que $|A+A| \geq 2|A|-1$.
(b) Muestre que si A es una progresión aritmética, entonces $|A+A| = 2|A|-1$.
(c) Muestre que si $|A+A| = 2|A|-1$, entonces A es una progresión aritmética.[2]

(2) Sea B un subconjunto de $\mathbb{Z}^+$.
(a) Muestre que $|B \cdot B| \geq 2|B|-1$.
(b) Muestre que B es una progresión geométrica si y sólo si $|B \cdot B| = 2|B|-1$.
(c) ¿Porqué la restricción a los enteros **positivos**?

(3) (a) Sea A una progresión aritmética. Encuentre una buena cota inferior para $|A \cdot A|$.
(b) Sea B una progresión geométrica. Encuentre una buena cota inferior para $|B+B|$.[3]

(4) Complete la demostración de Proposición 2. ¿Puede escribir y probar una versión no-abeliana?

(5) Sea A un conjunto en un grupo $(G, \cdot)$. Muestre que $A^2 = A$ si y sólo si A es un grupo.

(6) Sea G un grupo finito, y supóngase que A y B son subconjuntos de G tal que

$$|A| + |B| > |G|.$$

Muestre que $A \cdot B = A \cdot B^{-1} = G$. De un ejemplo de conjuntos tal que

$$|A| + |B| = |G| \text{ y } A \cdot B \neq G.$$

---

[2]Partes (b) y (c) juntos forman un caso especial del **teorema de Freiman**. Este teorema da una descripción completa de los subconjuntos de $\mathbb{Z}$ que satisface una cota superior lineal por duplicación. El teorema dice lo siguiente:
Para todo $C > 0$, existe $d, k \in \mathbb{Z}^+$ tal que para todo $A \subseteq \mathbb{Z}$ con $|A+A| < C|A|$, hay una progresión aritmética P de dimensión d y largo k tal que $A \subseteq P$.
En otras palabras, el teorema de Freiman dice que los todos subconjuntos de $\mathbb{Z}$ que tienen duplicación pequeña son subconjuntos de las progresiones aritméticas de dimensión a cotada y largo a cotado. Tal vez, usted no sabe lo que significa la *dimensión* de una progresión – por eso se necesita generalizar la definición de una progresión aritmética. Con esta generalización los progresiones aritméticas usuales son las progresiones aritméticas de dimensión 1. Visite wikipedia para más detalles!

[3] Los primeros dos ejercicios muestran que podemos encontrar subconjuntos de $\mathbb{Z}$ que respectan una cota superior lineal con respecto una de las operaciones disponibles: para "+", podemos tomar las progresiones aritméticas; similarmente podemos tomar las progresiones geométricas para "$\cdot$".
El tercer ejercicio muestra que, en cada caso, los conjuntos que hemos encontrado no respecten una cota superior lineal con respecto a la otra operación. Una pregunta natural es encontrar subconjuntos que respectan cotas superiores con respecto a las dos operaciones simultaneamente. Una **conjetura de Erdös y Szemerédi** dice que este no es posible. La conjetura completa todaviía está abierta pero una versión más debil (con una demostración muy hermosa) es un **teorema de Solymosi**. Su resultado es el siguiente:
Para todo $\varepsilon > 0$, hay un $C > 0$ tal que, para todo finito $A \subset \mathbb{Z}$,

$$\max\{|A \cdot A|, |A+A|\} \geq C|A|^{4/3-\varepsilon}.$$

La conjetura de Erdös y Szemerédi es la misma proposición con $4/3$ reemplazado con 2. En otra palabras, la conjetura dice que todos subconjuntos de $\mathbb{Z}$ crecen con respecto a "+" o "$\cdot$" y, además, este crecimiento es lo mas cercana posible al crecimiento cuadrático... sin ser siempre cuadrático.

(7) (Tao-Vu, 2.3.7) Sea G un grupo abeliano, y supóngase que A y B son subconjuntos de G. Muestre que

$$|A - B| = |A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$$

si y sólo si A, B son cosets de un subgrupo finito H de G.

(8) Muestre las partes 2 y 3 de Corolario 4.

(9) (Breuillard, Ejercicio 2.8) Sea G un grupo abeliano, y supóngase que A es un subconjuntos de G. Muestre que si $|AA| < \frac{3}{2}|A|$, entonces A^2 es un coset de un subgrupo de G. Dar un ejemplo de un conjunto A tal que $|AA| = \frac{3}{2}|A|$ pero A no es un coset de un subgrupo.

(10) ¿Para cuales valores de n, puede usted encontrar un subconjunto A del anillo $\mathbb{Z}/n\mathbb{Z}$ tal que $|A \cdot A| < |A|$? Escriba la mejor proposición posible sobre esta pregunta para todos los valores de $n \geq 2$.

Capítulo 2

Acciones de grupos

En esta lectura, consideramos crecimiento en el contexto de grupos actuando sobre conjuntos. Aquí, $\Omega = \{1, \ldots, n\}$, $\mathrm{Sim}(\Omega) = S_n$ (el *grupo simétrico*) es el conjunto de permutaciones de Ω, y A_n (el *grupo alternante*) es el conjunto de permutaciones pares de Ω.

Recuerde que una *acción* de un grupo G sobre Ω es un homomorfismo $G \to S_n$.[1] Necesitamos alguna terminología:

- Para $\omega \in \Omega$, la *órbita* de ω bajo la acción de G es el conjunto

$$G\omega := \{g\omega \mid g \in G\}.$$

- Para $\omega \in \Omega$, $A \subseteq G$, la *órbita* de ω bajo la acción de A es el conjunto

$$A\omega := \{g\omega \mid g \in A\}.$$

- Para $\omega \in \Omega$, el *estabilizador* de ω in G es el subgrupo

$$G_\omega := \{g \in G \mid g\omega = \omega\}.$$

(La segunda definición es probablemente nueva para usted – es una generalización de la primera, que es estandar.) Recuerde que las órbitas de un grupo G actuando sobre Ω forman una partición de G. Las órbitas de un conjunto A no tienen esta propiedad en general.

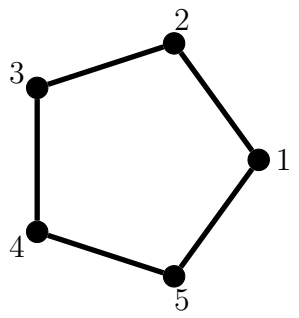
Ejemplo 2.

1. Sea $G = S_n$ y $\omega = 1 \in \Omega$. Entonces la órbita de 1 es Ω, y el estabilizador es

$$G_1 = \{g \in S_n \mid g(1) = 1\} \cong S_{n-1}.$$

2. Sea $\Omega = \{1, \ldots, 5\}$ y $G = D_5$, el grupo dihedral de cardinalidad 10. Es el grupo de automorfismos de un pentágono:

[1] No tengo tiempo en esta lectura discutir la teoría de las acciones de grupos. Para una introducción excellente, recomiendo [6].



Para cada $\omega \in \{1, \ldots, 5\}$, la órbita $G\omega = \Omega$. El estabilizador es de cardinalidad 2 y contiene la identidad y una reflección. Por ejemplo,

$$G_1 = \{(1), (2,5)(3,4)\}.$$

3. Sea $\Omega = \{1, 2, 3, 4, 5\}$ y G el grupo de elementos que preservan la partición $\Omega = \{1, 2\} \cup \{3, 4, 5\}$.
   Entonces $G \cong S_2 \times S_3$ y, por construcción las órbitas de G son $\{1, 2\}$ y $\{3, 4, 5\}$. Hay dos tipos de estabilizadores:

$$G_1 \cong G_2 \cong S_3 \text{ y } G_3 \cong G_4 \cong G_5 \cong S_2 \times S_2.$$

4. Sea V un espacio vectorial de dimensión d sobre un cuerpo $\mathbb{F}$, y sea $G = \mathrm{GL}_d(\mathbb{F})$, el grupo de transformaciones lineales inversibles, un grupo bajo la operación de composición. G actúa sobre el conjunto V y hay dos órbitas:

$$\{\mathbf{0}\} \text{ y } V \setminus \{\mathbf{0}\}.$$

   Otra vez, hay dos tipos de estabilizadores. $G_{\mathbf{0}} = G$, mientras que si $\mathbf{v} \neq \mathbf{0}$, entonces

$$G_{\mathbf{v}} \cong \mathbb{F}^{d-1} \rtimes GL_{d-1}(\mathbb{F}).$$

En todos los ejemplos anteriores, se puede tomar un subconjunto A del grupo G y las órbitas de A seran subconjuntos de las órbitas de G.

Ahora podemos escribir el **teorema de órbita-estabilizador** pero esta versión incluye una proposición para subconjuntos, no solamente para subgrupos.

Teorema 6. *Sea G un grupo actuando sobre un conjunto Ω. Sea $\omega \in \Omega$, y sea $A \subset G$ no vacío. Entonces*

$$|G\omega| = \frac{|G|}{|G_\omega|} \text{ y } |A\omega| \geq \frac{|A|}{|AA^{-1} \cap G_\omega|}$$

Espero que la igualdad sea familiar a ustedes. La desigualdad es en los ejercicios.

Definición 7. La acción de G es *transitiva* si para todo $\omega_1, \omega_2 \in G$ hay un $g \in G$ tal que $g(\omega_1) = (\omega_2)$.

Si $A \subset G$, decimos que A es *transitivo* si para todo $\omega_1, \omega_2 \in G$ hay un $g \in A$ tal que $g(\omega_1) = (\omega_2)$.

A veces, abusaremos terminología y decimos que un grupo G *es transitivo*, si la acción que consideramos es obvia.

Observe que una acción es transitiva si y sólo si la órbita de cada elemento de Ω es el mismo Ω. En Ejemplo 2, (1) y (2) son transitivas; (3) y (4) no son transitivas (son *intransitivas*).

Si tenemos una acción intransitivo, podemos descomponer Ω usando las órbitas de la acción. El grupo actúa sobre cada órbita y, por definición, la acción es transitiva. Por ejemplo, el grupo $\mathrm{GL}_d(\mathbb{F})$ en la cuarta acción actúa transitivamente sobre el conjunto $V \setminus \{\mathbf{0}\}$.

2.1 t-transitividad

Hay otros conceptos do transitividad más fuerte. Sea t un entero tal que $1 \leq t \leq |\Omega|$. Podemos usar la acción de G sobre Ω definir una acción de G sobre $\Omega^t = \underbrace{\Omega \times \cdots \times \Omega}_{t}$: para $(\omega_1, \omega_2, \ldots, \omega_t) \in \Omega^t$ y $g \in G$:

$$g(\omega_1, \omega_2, \ldots, \omega_t) = (g\omega_1, g\omega_2, \ldots, g\omega_t).$$

Debe verificar que esta acción es bien-definida.

Considere un subconjunto importante de Ω^t:

$$\Omega^{(t)} = \{(\omega_1, \ldots, \omega_t) \in \Omega^t \mid \omega_i \neq \omega_j \text{ para todo } i \neq j\}.$$

En otras palabras, $\Omega^{(t)}$ es el conjunto de t-tuplos de elementos *distintos* de Ω. Observe que la acción de G sobre Ω^t se restringe a una acción sobre $\Omega^{(t)}$.

Definición 8. Sea t un entero tal que $1 \leq t \leq |\Omega|$. La acción de G es *t-transitiva* si la acción de G sobre $\Omega^{(t)}$ es transitiva.

Si $A \subseteq G$, decimos que A es t-transitivo si A es transitivo sobre $\Omega^{(t)}$.

En los ejercicios, probaremos que si una acción es t-transitiva para algún $t \geq 2$, entonces es $(t-1)$-transitiva. Observe que una acción es 1-transitiva si y sólo si es transitiva.

Hay dos ejemplos muy importantes de grupos con acciones t-transitivas:

Lema 9. *La acción de S_n sobre Ω es n-transitivo; la acción de A_n sobre Ω es $(n-2)$-transitivo para $n \geq 3$.*

El siguiente es un teorema famoso – es la solucíon a una conjetura de Jordan; su demostración usa la clasificación de grupos finitos simples. Una demostración directa sería un muy gran resultado en la teoría de grupos.

Teorema 10. *Supóngase que G es un grupo finito que actú sobre un conjunto de cardinalidad n, y que esta acción es 6-transitiva. Entonces $G \cong A_n$ o S_n.*

Si reemplazamos 6 con 5, hay dos ejemplos más: $G \cong M_{12}$, M_{24}, S_n o A_n. Sin embargo, si consideramos acciones 2-transitivas o 3-transitiva, hay muchos ejemplos.

Ejemplo 3. Sea $\mathbb{F}_p$, el cuerpo de cardinalidad p, sea $V = \mathbb{F}_p^2$, y sea Ω el conjunto de subespacios 1-dimensionales en V. Entonces $|\Omega| = p + 1$.

Ahora, defina

$$\mathrm{GL}_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, c \in \mathbb{F}_p^*, ad - bc \neq 0 \right\}.$$

Observe que $|G| = p(p-1)^2$ y que G actúa sobre Ω por multiplicación a la izquierda:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left\langle \begin{pmatrix} x \\ y \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \right\rangle$$

En los ejercicios vamos a probar que esta acción es 3-transitiva. Vamos a ver en los ejercicios también que este resultado implica que un estabilizador G_ω de $\omega \in \Omega$ tiene una acción 2-transitiva sobre $\Omega \setminus \{\omega\}$.

Parece que es difícil encontrar grupos con acciones t-transitivas para t grande. Qué pasa para conjuntos? Para responder a esta pregunta, necesito una definición nueva:

Definición 11. Sea A un subconjunto de un grupo G finito. Definimos

$$\langle A\rangle := \{a_1a_2\cdots a_k \mid k \in \mathbb{Z}^+, a_1, \ldots, a_k \in A\}$$

y decimos que $\langle A\rangle$ es *el subgrupo de G generado por A*. Si $G = \langle A\rangle$, decimos que A *genera* G.

Vamos a ver en los ejercicios que $\langle A\rangle$ es, de hecho, un subgrupo de G (entonces, nuestra terminología hace sentido). En los ejercicios ampliaremos la definición que se aplica a grupos infinitos también.

Lema 12. *Supóngase que $A \subseteq G$, un grupo, G actúa sobre un conjunto Ω, y $\omega \in \Omega$. Escribe $H := \langle A\rangle$ y tome $k \in \mathbb{Z}^+$. Si Λ es la órbita de ω bajo A^k y bajo A^{k+1}, entonces Λ es una órbita para H.*

No hemos definido formalmente lo que significa "el crecimiento de una órbita", pero se puede pensar de este resultado como *si una órbita no crece, entonces es lo más grande que se puede.*

Demostración. Ya que Λ es la órbita de ω bajo A^k, luego

$$\Lambda = \{b\omega \mid b \in A^k\}.$$

Ahora, ya que Λ es una órbita para A^{k+1} también,

$$\Lambda = \{ab\omega \mid a \in A, b \in A^k\}.$$

Entonces, si $\lambda \in \Lambda$, entonces $a\lambda \in \Lambda$, y por lo tanto

$$a_1 \cdots a_k\lambda \in \Lambda$$

para todo $a_1, \ldots, a_k \in A$. Es decir que si $\lambda \in \Lambda$, entonces $h\lambda \in \Lambda$ para todo $h \in H$. Entonces Λ es una unión de órbitas de H. Pero Λ es una órbita de A^k implica que Λ es un subconjunto de una órbita de $H \supseteq A^k$, entonces Λ es una órbita de H. □

Corolario 13. *Supóngase que la acción de $H = \langle A\rangle$ sobre Ω sea t-transitiva, y Ω sea finito de cardinalidad n. Entonces el conjunto A^{n^t} es t-transitivo.*

Probaremos este resultado en los ejercicios. Con este resultado, podemos encontrar muchos conjuntos t-transitivos para t grande. Por ejemplo, podemos tomar un conjunto $A \subseteq S_n$ que genera S_n (es decir, no es un subconjunto de un subgrupo de S_n). Entonces A^{n^t} será t-transitivo para todo $1 \leq t \leq n$.

2.2 Ejercicios

(1) Sea G un grupo. Sean $H < G$, $g \in G \backslash H$ y $A = H \cup \{g\}$. Entonces $|A|^2 < 3|A|$, pero $A^3 \supset HgH$, y HgH puede ser mucho más grande que A. Dar un ejemplo (tal vez, con $G = \mathrm{SL}_2(\mathbb{F}_p)$).

(2) Escriba un subconjunto A de S_3 para que las órbitas de los elements de $\Omega = \{1, 2, 3\}$ bajo A no forman una partición de Ω.

(3) Pruebe el teorema de órbita-estabilizador para conjuntos. Use el principio del palomar.

(4) Supóngase que G sea un grupo actuando sobre un conjunto Ω, que $\omega \in \Omega$, y que $2 \leq t \in \mathbb{Z}$. Pruebe que la acción de G es t-transitivo si y sólo si la acción de G es transitivo, y la accíon del establizador G_ω sobre $\Omega \setminus \{\omega\}$ es $(t-1)$-transitivo.

(5) ¿Porqué hemos definido t-transitividad para $t \leq |\Omega|$?

(6) Pruebe Lema 9.

(7) Pruebe que la acción de $\mathrm{GL}_2(\mathbb{F}_p)$ sobre el conjunto en Ejemplo 2 es 3-transitiva. ¿ Cuál es el estabilizador del subespacio $\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle$?

Sugerencia: use Ejercicio (4) .

(8) Sea $A \subseteq G$, un grupo finito. Pruebe que $\langle A \rangle$ es un subgrupo de G. Dé un ejemplo para mostrar que esta conclusión no es verdadera para grupos infinitos. ¿Cómo necesito cambiar la definición para que $\langle A \rangle$ sea un subgrupo en el caso infinito también?

(9) Pruebe que A genera G si y sólo si A no es un subconjunto de un subgrupo proprio de G.

(10) Pruebe Corolario 13.

(11) Tome un grupo G actuando sobre un conjunto Ω. Un *sistema de imprimitividad* para esta acción es una relación de equivalencia R sobre Ω tal que

$$\omega_1 \ R \ \omega_2 \text{ y } g \in G \Longrightarrow \omega_1^g \ R \ \omega_2^g.$$

Hay dos relaciones *triviales*

$$\omega_1 \ R_1 \ \omega_2, \ \forall \omega_1, \omega_2 \in \Omega \text{ tal que } \omega_1 = \omega_2 \qquad\qquad \omega_1 \ R_2 \ \omega_2, \ \forall \omega_1, \omega_2 \in \Omega.$$

Llamamos la acción *imprimitiva* si hay una sistema de imprimitividad no-trivial, y llamamos la acción *primitiva* si no.

(a) Pruebe que, si $|\Omega| > 2$ y la acción es primitiva, entonces la acción es transitiva.

(b) Pruebe que si la acción es 2-transitiva, entonces la acción es primitiva.

(c) Pruebe que la acción del grupo dihedral D_n sobre el n-gono es primitiva para $n = 5$ pero no para $n = 6$.[2]

[2]Este ejercicio con Ejercicio (4) mostran que hay una cadena de implicaciones para acciones de grupos:

$$\cdots \Longrightarrow 3-\text{transitiva} \Longrightarrow 2-\text{transitiva} \Longrightarrow \text{primitiva} \Longrightarrow \text{transitiva}.$$

Capítulo 3

Grafos de Cayley

En esta lectura, $(G, \cdot)$ es un grupo (usualmente finito) y A es un subconjunto (siempre finito) de G.

Definición 14. El *grafo de Cayley* para G con respecto a A es el grafo dirigido (V, E) donde

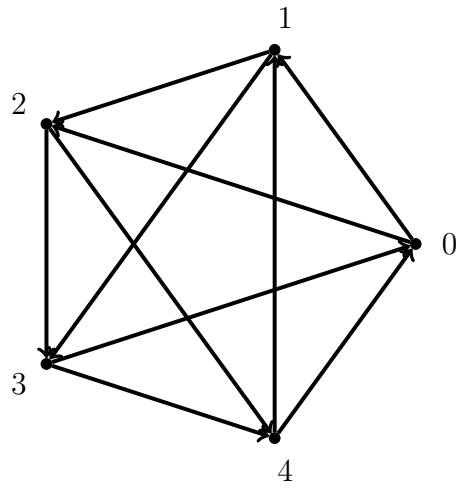
1. el conjunto de vértices, V, es igual al conjunto de elementos de G;
2. si $g, h \in G$, entonces hay una arista de g a h si y sólo si $h = ga$ para algún $a \in A$.

Escribimos $\Gamma(G, A)$ para este grafo.[1]

Si $A = A^{-1}$ hay una arista de g a h, si y sólo si hay una arista de h a g. En este caso, podemos reemplazar las dos aristas dirigidas con una arista sin direccíon, y podemos pensar en $\Gamma(G, A)$ como un grafo no-dirigido.

Ejemplo 4.

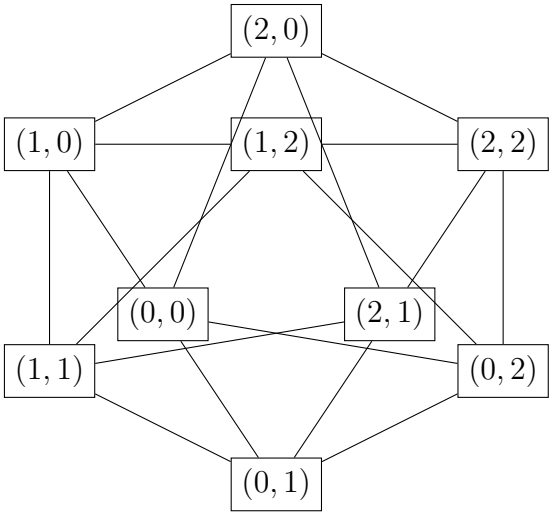
1. Sea $G = (\mathbb{Z}/5\mathbb{Z}, +)$ y $A = \{1, 2\}$. Entonces $\Gamma(G, A)$ es



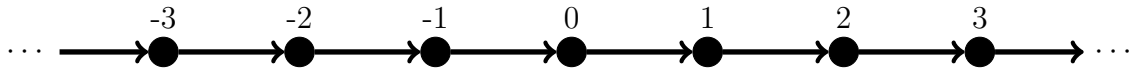
[1]Hay varias convenciones sobre la definición de un grafo de Cayley. En nuestra definición hay una manera natural de nombrar los vértices de $\Gamma(G, A)$ (por los elementos de G). En las diagrámas siguientes, escribiremos estos nombres aunque, de hecho, estamos interesado solamente en la estructura del grafo "abstracto" y, por lo tanto, estos nombres no importan. Por otro lado, algunos autores nombran las aristas también, por los elementos de A. Por ejemplo, si vértices v y w son conectados porque hay $a \in A$ tal que $va = w$, entonces el arista de v a w puede tomar el nombre a (observe que este nombre es único). No haremos esto.

Observe que si agregamos los inversos de los elements de A (para obtener un grafo no-dirigido), entonces $A = G \setminus \{0\}$, y el grafo de Cayley es el grafo completo. Este es verdadero en general: para cualquier grupo G, si A es igual a los elementos de G sin la identidad, entonces $\Gamma(G, A)$ es el grafo completo. ¿Qué pasa si $A = G$?

2. Sea $G = (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$ y $A = \{(1,0), (2,0), (0,1), (0,2)\}$. Observe que, ya que $A = -A$, el grafo es no-dirigido.



3. Sea $G = (\mathbb{Z}, +)$ y $A = \{1\}$. Entonces $\Gamma(G, A)$ es



3.1 La estructura de $\Gamma(G, A)$

Queremos estudiar la estructura de los grafos de Cayley para varios grupos G y conjuntos $A \subseteq G$. Vamos a usar la teoría de acciones: recuerde que un grupo G puede actuar sobre sí mismo por multiplicación. Hay dos posibilidades: primero G actúa *por la izquierda*. La homomorfismo del acción es

$$\begin{aligned} \iota : G &\to \mathrm{Sim}(G), g \mapsto \iota_g, \text{ donde} \\ \iota_g : G &\to G, h \mapsto g \cdot h. \end{aligned}$$

Segundo, G actúa *por la derecha*. La homomorfismo es

$$\begin{aligned} \delta : G &\to \mathrm{Sim}(G), g \mapsto \delta_g, \text{ donde} \\ \delta_g : G &\to G, h \mapsto h \cdot g^{-1}. \end{aligned}$$

Observe que, en ambos casos, si $h \in G$, el estabilizador $G_h = \{1\}$.

Sea $A \subseteq G$. Queremos usar el hecho que G es, sí mismo, el conjunto de vértices en el grafo $\Gamma(G, A)$. El resultado siguiente es obvio.

Lema 15. *Cuando G actua sobre sí mismo por multiplicación por la izquierda, esta acción* preserva las aristas de $\Gamma(G, A)$. *Es decir, si $h_1, h_2 \in G$ son conectados en $\Gamma(G, A)$, entonces gh_1, gh_2 son conectados en $\Gamma(G, A)$.*

Formalmente este lema dice que G es *un grupo de automorfismos* del grafo $\Gamma(G, A)$. La importancia de este es que la estructura del grafo es el mismo del punto de vista de cualquier vértice que escogemos. Por ejemplo, si borramos los nombres de los vértices, es imposible decir cuál fue la identidad: para todo vértice v, hay una manera de nombrar tal que v es la identidad.

3.1.1 Diametro

En el siguiente, vamos a escribir $\overrightarrow{vw}$ para una arista dirigida de un vértice v a un vértice w en un grafo dirigido Γ; similarmente, vamos a escribir $\overline{vw}$ para una arista no-dirigida entre dos vertices v y w en un grafo no-dirigido Γ.

Ahora, en un grafo dirigido un *sendero* de un vértice v a un vertice w es una secuencia de aristas dirigidas de la forma

$$\overrightarrow{vv_1},\ \overrightarrow{v_1v_2},\ \ldots,\ \overrightarrow{v_{k-2}v_{k-1}},\ \overrightarrow{v_{k-1}w}.$$

Este sendero tiene largo k. La *distancia* de v a w es el largo mínimo de un sendero de v a w. Si no hay un sendero de v a w, decimos que la distancia es ∞.

Similarmente, en un grafo no-dirigido un *sendero* de largo k de un vértice v a un vértice w es una secuencia de aristas de la forma

$$\overline{vv_1},\ \overline{v_1v_2},\ \ldots,\ \overline{v_{k-2}v_{k-1}},\ \overline{v_{k-1}w}$$

La *distancia* entre v y w es el largo mínimo de un sendero entre v y w. Otra vez, si no hay un sendero entre v y w, decimos que la distancia es ∞.

En ambos casos, escribimos $d(v, w)$ para la distancia de v a w. Observe que, en un grafo dirigido, es posible que la distancia de v a w es diferente a la distancia de w a v. Por ejemplo en el tercer grafo en Ejemplo 4, $d(1, 2) = 1$ mientras que $d(2, 1) = \infty$.

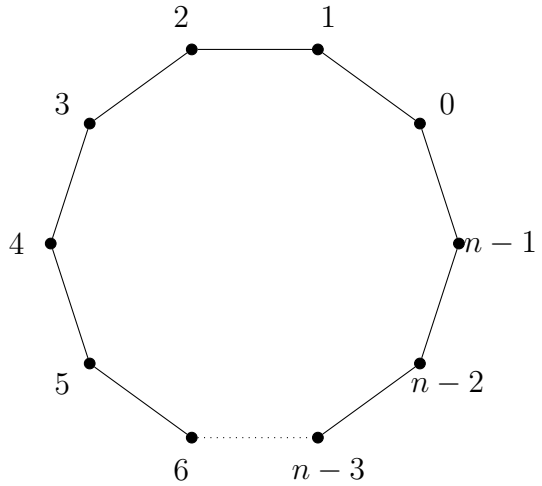
Definición 16. El *diametro* de un grafo Γ, escrito $\mathrm{diam}(\Gamma)$, es definido como

$$\max\{d(v, w) \mid v, w \text{ vértices en } V\},$$

si el máximo exista. Si no, escribimos $\mathrm{diam}(\Gamma) = \infty$.

El ejemplo siguiente será importante más tarde.

Ejemplo 5. Sea G el grupo $(\mathbb{Z}/n\mathbb{Z}, +)$ con $A = \{1, -1\}$. Ya que $A = -A$, podemos dibujar $\Gamma(G, A)$ como un grafo no-dirigido:



El grafo es el n-gono, y es obvio que $\text{diam}(\Gamma(G,A)) = \lfloor \frac{n}{2} \rfloor$. Note que, cuando $n = p$, el grupo $(G,+) = (\mathbb{Z}/p\mathbb{Z},+)$ es simple. Entonces, tenemos una familia de grafos de Cayley de grupos simples para que el diametro crece linealmente como una función de la cardinalidad del grupo.

3.2 Diametro y crecimiento

Si Γ es un grafo de Cayley, i.e. $\Gamma = \Gamma(G,A)$ para algún G y A, entonces podemos usar Lema 15 para ayudarnos en la calculación del diametro de Γ. Ya que el grafo es el mismo del punto de visto de cualquier vértice, el diametro es la distancia máximo de un vértice de la identidad:

$$\text{diam}(\Gamma(G,A)) = \max\{d(1,v) \mid v \text{ un vértice en } V\}.$$

Note que la calculación del diametro de un grafo es, en general un problema difícil. Necesitamos usar la estructura especial de un grafo de Cayley cuando hacemos esta calculación. El resultado siguiente será útil.

Lema 17. *Sea $\Gamma = \Gamma(G,A)$. El conjunto de vértices de distancia 1 de la identidad es igual al conjunto A. Más generalment, el conjunto de vértices de distancia k de la identidad es igual al conjunto A^k.*

Corolario 18. *El diametro* $\text{diam}(\Gamma(G,A))$ *es igual al número mínimo k tal que*

$$\{1\} \cup A \cup A^2 \cup \cdots \cup A^k = G.$$

Si A contiene la identidad de G, entonces el diametro $\text{diam}(\Gamma(G,A))$ *es igual al número mínimo k tal que $A^k = G$.*

Corolario 19. *(a) El diametro de un grafo de Cayley satisface una cota inferior:*

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

(b) Si $\langle A \rangle = G$, tenemos también una cota superior:

$$\text{diam}(\Gamma(G,A)) \leq |G|.$$

Este corolario dice que el diametro de un grafo de Cayley está entre una función logarítmica y una función lineal en la cardinalidad de G. Pensamos de grafos con pequeño diametro como "compacto" en algún sentido, mientras que los grafos con gran diametro son "dispersado" – mire Ejemplo 5 para una familia de tales grafos.

3.3 Ejercicios

(1) Pruebe que si G es finito, $\Gamma(G, A)$ es conectado si y sólo si A genera G.

(2) Sea $A = \{(1, 2, 3)\} \subset S_3$ y $B = \{(1, 2, 3), (1, 2)\} \subset S_3$.
Dibuje $\Gamma(S_3, A)$, $\Gamma(S_3, B)$. ¿A genera S_3? ¿B genera S_3?

(3) Sea D_5, el grupo dihedral de cardinalidad 10. (La definición exacta fue dada en lectura 2.) Sea $A = \{(1, 2, 3, 4, 5), (2, 5)(3, 4)\}$. Dibuje $\Gamma(D_5, A)$.

(4) Sea Γ un grafo dirigido, v un vértice de Γ. La incidencia de v es el número de vertices w tal que hay una arista de v a w. Un grafo es *regular* si para todos vértices v, w, la incidencia de v es igual a la incidencia de w.

Muestre que $\Gamma(G, A)$ es regular. ¿Cuál es la incidencia de un vértice de $\Gamma(G, A)$?

(5) Calcule el diametro de cada grafo en Ejemplo 4, y en los ejercicios (2) y (3) .

(6) Sea G el grupo $(\mathbb{Z}/n\mathbb{Z}, +)$ con $A = \{1\}$. Calcule $\text{diam}(\Gamma(G, A))$.

(7)

(a) Sea $G = S_n$, y A el conjunto de todas transposiciones. Calcule $\text{diam}(\Gamma(G, A))$.

(b) Sea $G = A_n$, y A el conjunto de todos 3-ciclos. Calcule $\text{diam}(\Gamma(G, A))$.

(c) Sea $G = S_n$, y $A = \{(1, 2), (1, 2, 3, \ldots, n)\}$. ¿Puede calcular $\text{diam}(\Gamma(G, A))$? (Este es mucho más difícil.)

(8) Pruebe Lema 17, Corolario 18 y Corolario 19.

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 atribuido 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?

Bibliography

[1] L. Babai, R. Beals, Á. Seress, On the diameter of the symmetric group: polynomial bounds, *Proc. of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, ACM, New York, 2004, 1108–1112.

[2] L. Babai, Á. Seress. On the diameter of Cayley graphs of the symmetric group, *J. Combin. Theory Ser. A*, **49** (1988), 175–179.

[3] L. Babai, Á. Seress, On the diameter of permutation groups, *European J. Combin.* **13** (1992), 231–243.

[4] J. Bamberg, N. Gill, T. Hayes, H. Helfgott, Á. Seress, P. Spiga, Bounds on the diameter of Cayley graphs of the symmetric group, *J. Algeb. Comb.* **40** (2014), no. 1, 1–22.

[5] A. Bochert, Űber die Classe der transitiven Substitutionengruppen (German), *Math. Ann.* **49** (1897), 133144.

[6] J. D. Dixon, B. Mortimer, Permutation groups, Springer, 1996.

[7] H. A. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math. (2)* **167** (2008), 601–623.

[8] H. Helfott, Á. Seress, *On the diameter of permutation groups*, Ann. Math. **179** (2014), no. 2, 611–658.

[9] H. Wielandt, Finite permutation groups, Academic Press, New York, 1964.