Notas das reuniões do PICME
Segundo semestre de 2014

Leonardo Nagami Coregliano
Henrique Stagni

26 de dezembro de 2014

Sumário

1 Transformada Rápida de Fourier e Multiplicação de Polinômios

1.1 Conceitos Básicos de Grupos e a Transformada de Fourier

26/08/2014 – Fernando Mário de Oliveira Filho

Iniciaremos relembrando alguns conceitos básicos de grupos.

Definição 1.1.1. Um *grupo* é uma tripla $(G, e, +)$, onde G é um conjunto, $e \in G$ é um elemento de G chamado *identidade* e $+\colon G \times G \to G$ é uma operação que satisfaz as seguintes propriedades.

i. (Associatividade) Para todos $x, y, z \in G$, temos $(x + y) + z = x + (y + z)$;

ii. (Elemento neutro) Para todo $x \in G$, temos $e + x = x$;

iii. (Elemento oposto) Para todo $x \in G$, existe $y \in G$ tal que $y + x = e$.

O elemento y do Item iii é chamado de *oposto* de x e é denotado por $-x$. Muitas vezes abusaremos da notação denotando por $x-y$ a fórmula $x+(-y)$. Também abusaremos da notação falando apenas que G é um grupo, em vez de mencionar a tripla inteira e, salvo menção explícita ao contrário, a operação será sempre $+$ e a identidade será sempre e.

Um grupo G que também satisfaz a propriedade abaixo é chamado de *grupo abeliano*.

v. (Comutatividade) Para todos $x, y \in G$, temos $x + y = y + x$.

Alguns exemplos clássicos de grupos abelianos são $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ com a operação de soma módulo n e o toro $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ com a operação de multiplicação (nesse último caso manteremos a notação multiplicativa para evitar confusões).

Exemplos simples de grupos não abelianos são o grupo $M_{n\times n}(\mathbb{R})$ das matrizes inversíveis de ordem $n \times n$ munidas da operação de multiplicação de matrizes e o grupo $\mathfrak{S}_n$ das permutações de tamanho n (funções bijetoras de $[n]$ em $[n]$) munidas da composição de funções.

Deixamos algumas propriedades básicas de grupos como exercício.

Exercício resolvido 1.1.2. Suponha que G é um grupo com identidade e. Valem as seguintes asserções.

1. (Caracterização do neutro) Para todo $x \in G$, temos $x + x = x$ se e só se $x = e$;

2. (Elemento oposto à direita) Para todo $x \in G$, temos $x + (-x) = e$;

3. (Elemento neutro à direita) Para todo $x \in G$, temos $x + e = x$;

4. (Unicidade do elemento neutro) Se $x, y \in G$ são tais que $x + y = y$, então $x = e$;

5. (Unicidade do elemento oposto) Se $x, y, z \in G$ são tais que $y + x = z + x = e$, então $y = z$;

6. (Bijeção através da operação) Para todo $y \in G$, a função $g_y\colon G \ni x \mapsto x + y \in G$ é bijetora.

Lembramos agora a definição de homomorfismos e isomorfismos de grupos.

Definição 1.1.3. Um *homomorfismo de grupos* do grupo G no grupo H é uma função $f\colon G \to H$ que preserva a operação, isto é, uma função tal que $f(x + y) = f(x) + f(y)$, para todos $x, y \in G$.

Um *isomorfismo de grupos* é um homomorfismo de grupos que é também bijetor.

Dizemos que um grupo G é *isomorfo* a um grupo H (e denotamos por $G \cong H$) se existe um isomorfismo de grupos de G em H.

O exercício abaixo diz que homomorfismos também preservam identidade.

Exercício resolvido 1.1.4. Se f é um homomorfismo de grupos do grupo G no grupo H, então temos $f(e_G) = e_H$, onde e_G e e_H são as identidades de G e H respectivamente.

Um tipo particular de homomorfismos merece atenção especial.

Definição 1.1.5. Um *caracter* de um grupo G é um homomorfismo de grupos de G para o grupo $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ (munido da multiplicação usual), isto é, um caracter é um homomorfismo $\chi\colon G \to \mathbb{T}$.

Denotamos o conjunto dos caracteres de G por $\widehat{G}$.

É fácil ver que, dado um grupo G, o conjunto dos caracteres de G munido do produto ponto-a-ponto de funções é um grupo abeliano e, dado um caractere χ, seu elemento oposto (denotado χ^{-1} devido à notação multiplicativa) é exatamente seu conjugado complexo ponto-a-ponto (i.e., para todo $g \in G$, temos $\chi^{-1}(g) = \overline{\chi(g)}$).

Muitas vezes veremos caracteres como elementos do espaço vetorial $\mathbb{C}^G$ das funções de G a $\mathbb{C}$. O teorema abaixo nos diz quanto é o produto interno entre dois caracteres.

Teorema 1.1.6. Se χ e ψ são caracteres de um grupo abeliano finito G, então

$$\chi^*\psi = \langle \psi, \chi \rangle = \sum_{x \in G} \overline{\chi(x)}\psi(x) = \begin{cases} |G|, & \text{se } \chi = \psi; \\ 0, & \text{se } \chi \neq \psi. \end{cases}$$

Demonstração. Se $\chi = \psi$, então temos

$$\sum_{x \in G} \overline{\chi(x)}\psi(x) = \sum_{x \in G} |\chi(x)|^2 = \sum_{x \in G} 1 = |G|.$$

Suponha agora que $\chi \neq \psi$, então existe $y \in G$ tal que $\psi(y) \neq \chi(y)$, logo temos $\overline{\chi(y)}\psi(y) \neq 1$.

Por outro lado, temos

$$\overline{\chi(y)}\psi(y) \sum_{x \in G} \overline{\chi(x)}\psi(x) = \sum_{x \in G} \overline{\chi(x)\chi(y)}\psi(x)\psi(y) = \sum_{x \in G} \overline{\chi(x+y)}\psi(x+y) = \sum_{z \in G} \overline{\chi(z)}\psi(z),$$

donde segue que

$$(1 - \overline{\chi(y)}\psi(y))\chi^*\psi = 0,$$

e, portanto $\chi^*\psi = 0$. ∎

Corolário 1.1.7. Para o grupo $\mathbb{Z}_n$, cada $u \in \mathbb{Z}_n$ define um caracter

$$\begin{array}{rccc} \chi_u\colon & \mathbb{Z}_n & \longrightarrow & \mathbb{T} \\ & x & \longmapsto & e^{2\pi i u x/n}. \end{array}$$

Ademais a função $\mathbb{Z}_n \ni u \mapsto \chi_u \in \widehat{\mathbb{Z}_n}$ é um isomorfismo de grupos.
Demonstração. Sejam $u, x, y \in \mathbb{Z}_n$ arbitrários e observe que

$$\begin{aligned} \chi_u(x+y) &= \exp\left(\frac{2\pi i u((x+y) \bmod n)}{n}\right) = \exp\left(\frac{2\pi i u(x+y)}{n}\right) \\ &= \exp\left(\frac{2\pi i u x}{n}\right)\exp\left(\frac{2\pi i u y}{n}\right) = \chi_u(x)\chi_u(y), \end{aligned}$$

logo χ_u de fato é caracter de $\mathbb{Z}_n$ (também temos trivialmente que $|\chi_u(x)| = 1$ para todo $x \in \mathbb{Z}_n$).

Observe agora que

$$\chi_{x+y}(u) = \exp\left(\frac{2\pi i((x+y) \bmod n)u}{n}\right) = \chi_x(u)\chi_y(u),$$

logo a função $g\colon \mathbb{Z}_n \ni u \mapsto \chi_u \in \widehat{\mathbb{Z}_n}$ é um homomorfismo de grupos, resta provar apenas que essa função é bijetora.

Suponha que $x \neq y$ e observe que

$$\chi_x(1) = e^{2\pi i x/n} \neq e^{2\pi i y/n} = \chi_y(1),$$

logo a função g é injetora.

Porém, o Teorema 1.1.6 nos diz que o conjunto $\widehat{\mathbb{Z}_n}$ é ortogonal no espaço vetorial $\mathbb{C}^G$, isso significa que

$$|\widehat{\mathbb{Z}_n}| \leqslant \dim \mathbb{C}^G = |G|,$$

e como g é injetora temos que a imagem de g possui cardinalidade maior ou igual a $|G|$. Portanto g é bijetora (pois seu domínio é finito). ■

Lembramos agora a definição de produto direto de grupos.

Definição 1.1.8. O *produto direto* dos grupos G e H é o grupo $G \times H$ munido da operação definida por

$$(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2),$$

para todos $g_1, g_2 \in G$ e $h_1, h_2 \in H$.

A identidade de $G \times H$ é o elemento (e_G, e_H), onde e_G é a identidade de G e e_H é a identidade de H.

O exercício abaixo caracteriza os caracteres de um produto direto.

Exercício resolvido 1.1.9. Se χ é caracter de G e ψ é caracter de H, então

$$\begin{array}{rccc} \chi \otimes \psi\colon & G \times H & \longrightarrow & \mathbb{T} \\ & (g, h) & \longmapsto & \chi(g)\psi(h) \end{array}$$

é caracter de $G \times H$.

Ademais, se φ é caracter de $G \times H$, então existem χ caracter de G e ψ caracter de H tais que $\varphi = \chi \otimes \psi$.

Lembramos do seguinte fato de álgebra.

Fato 1.1.10. Se G é um grupo abeliano finito, então existem $k_1, k_2, \ldots, k_n \in \mathbb{N}^*$ tais que

$$G \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n}.$$

Finalmente definimos a Transformada de Fourier.

Definição 1.1.11. Seja G um grupo abeliano finito e considere o espaço vetorial $\mathbb{C}^G$ munido do produto interno

$$\langle f, g \rangle = \sum_{x \in G} f(x)\overline{g(x)},$$

para todos $f, g \in \mathbb{C}^G$.

Considere também fixada uma decomposição de G como produto direto de $\mathbb{Z}_k$'s como no Fato 1.1.10.

A *Base Canônica* de $\mathbb{C}^G$ é a base $(e_u)_{u \in G}$, onde

$$e_u(x) = \begin{cases} 1, & \text{se } x = u; \\ 0, & \text{se } x \neq u; \end{cases}$$

para todos $u, x \in G$.

A *Base de Fourier* de $\mathbb{C}^G$ é a base $(\chi_u)_{u\in G}$, onde χ_u é o caractere associado a u conforme o Corolário 1.1.7 e o Exercício 1.1.9.

A *Transformada de Fourier* (ou *Transformada Direta de Fourier*) de um elemento $f \in \mathbb{C}^G$ é a função

$$\begin{aligned} \widehat{f}\colon G &\longrightarrow \mathbb{C} \\ u &\longmapsto \langle f, \chi_u \rangle . \end{aligned}$$

Da definição da Transformada de Fourier e do Teorema 1.1.6, segue que

$$f = \frac{1}{|G|} \sum_{u\in G} \widehat{f}(u)\chi_u,$$

que é comumente dita *Transformada Inversa de Fourier* do elemento $\widehat{f}$.

Para o caso em que $G = \mathbb{Z}_n$, temos

$$\begin{aligned} \widehat{f}(u) &= \sum_{x\in\mathbb{Z}_n} f(x)e^{-2\pi iux/n} \quad \text{para todo } u \in \mathbb{Z}_n; \\ f(x) &= \frac{1}{n} \sum_{u\in\mathbb{Z}_n} \widehat{f}(u)e^{2\pi iux/n} \quad \text{para todo } x \in \mathbb{Z}_n. \end{aligned}$$

Como G é abeliano, segue também que $\chi_u(x) = \chi_x(u)$, para todos $u, x \in G$.

A proposição abaixo mostra a relação entre a Transformada Direta e a Transformada Inversa de Fourier.

Proposição 1.1.12. Se $f \in \mathbb{C}^G$ e $g = \overline{\widehat{f}}$, então temos

$$\overline{\widehat{g}(x)} = |G|f(x),$$

para todo $x \in G$.

Demonstração. Segue direto de

$$\begin{aligned} \overline{\widehat{g}(x)} = \overline{\langle g, \chi_x \rangle} &= \overline{\sum_{u\in G} g(u)\overline{\chi_x(u)}} \\ &= \sum_{u\in G} \overline{g(u)}\chi_x(u) = \sum_{u\in G} \widehat{f}(u)\chi_u(x) \\ &= |G|f(x). \end{aligned}$$

■

02/09/2014 – Fernando Mário de Oliveira Filho

Definição 1.1.13 (convolução)**.** A *convolução* de duas funções $f, g \in \mathbb{C}^{\mathbb{Z}_n}$ é a função $f * g \in \mathbb{C}^{\mathbb{Z}_n}$ dada por

$$(f * g)(x) = \sum_{y\in\mathbb{Z}^n} f(y)g(x - y),$$

para todo $x \in \mathbb{Z}_n$.

Proposição 1.1.14.

$$\widehat{(f * g)}(u) = \widehat{f}(u)\widehat{g}(u)$$

Demonstração.

$$\begin{aligned}
\widehat{(f*g)}(u) &= \sum_{x\in\mathbb{Z}_n} (f*g)(x)\overline{\chi_u(x)} \\
&= \sum_{x\in\mathbb{Z}_n}\sum_{y\in\mathbb{Z}_n} f(y)g(x-y)\overline{\chi_u(x)} \\
&= \sum_{y\in\mathbb{Z}_n} f(y)\sum_{x\in\mathbb{Z}_n} g(x-y)\overline{\chi_u(x)} \\
&= \sum_{y\in\mathbb{Z}_n} f(y)\sum_{z\in\mathbb{Z}_n} g(z)\overline{\chi_u(z+y)} && \text{fazendo } z = x-y \\
&= \sum_{y\in\mathbb{Z}_n} f(y)\overline{\chi_u(y)}\sum_{z\in\mathbb{Z}_n} g(z)\overline{\chi_u(z)}, && \text{pois } \chi_u \text{ é homomorfismo} \\
&= \widehat{f}(u)\widehat{g}(u).
\end{aligned}$$

■

1.2 Aplicação da Transformada de Fourier para o problema da multiplicação de polinômios

Notação 1.2.1. Seja $\mathbb{C}[x]$ o conjunto dos polinômios com coeficientes complexos e indeterminada x. Dado um polinômio $p \in \mathbb{C}[x]$ denotamos:

- o grau de p por $g(p)$.
- o coeficiente do monômio x^k em p por $[x^k]p$. Por exemplo, se $p = x^4 + 8x^2$, $[x^2]p = 8$ e $[x^3]p = 0$.

Pergunta 1.2.2. Dados polinômios $p, q \in \mathbb{C}[x]$, como calcular o produto $pq \in \mathbb{C}[x]$ de p e q de maneira eficiente?

O algoritmo trivial para esse problema consiste em calcular (todos) os produtos de monômios de p por monômios de q e somá-los. Seja $n = \max\{g(p), g(q)\} + 1$. Não é difícil ver que esse algoritmo tem complexidade $O(n^2)$, no pior caso. Veremos como obter um algoritmo mais eficiente para esse problema, com o auxílio da transformada de Fourier.

Seja $N = 2n$ e considere funções $f, g : \mathbb{Z}_N \to \mathbb{C}$ que fornecem os coeficientes dos polinômios p, q respectivamente, isto é, $f(k) = [x^k]p$ e $g(k) = [x^k]q$. Podemos escrever o coeficiente de pq em x^k como

$$[x^k](pq) = \sum_{l\in\mathbb{Z}_N} f(l)g(k-l) = (f*g)(k).$$

Na expressão acima note que se $k - l < 0$ então $g(k-l) = 0$, uma vez que estamos trabalhando em $\mathbb{Z}_N$ (a expressão não seria verdadeira se f, g fossem polinômios sobre $\mathbb{Z}_n$).

Concluímos que calcular pq se resume a calcular o convolução $f * g$. Isso dá origem ao seguinte algoritmo:

1. Calcular $\widehat{f}$ e $\widehat{g}$.
2. Tomar $h(k) = \widehat{f}(u)\widehat{g}(u)$, para todo $k \in \mathbb{Z}_N$.
3. Calcular $\widehat{h}$.
4. Para todo $0 \leqslant k \leqslant N-2$, $[x^k](pq) = \frac{1}{N}\overline{\widehat{h}(k)}$.

É fácil ver que os passos acima calculam corretamente os coeficientes de (pq). De fato, pela Proposição 1.1.14, $h(k) = \widehat{(f*g)}(k)$ e, portanto, $\frac{1}{N}\overline{\widehat{h}(k)} = (f*g)(k)$, pela Proposição 1.1.12.

Os passos 2 e 4 acima fazem $O(n)$ operações aritméticas. Veremos, a seguir, como calcular a transformada de Fourier (usada nos passos 1 e 3) fazendo apenas $O(n \lg n)$ operações aritméticas, o que implicará que o algoritmo acima faz um total de $O(n \lg n)$ operações.

Teorema 1.2.3 (*Transformada Rápida de Fourier* – Gauss 1805, Cooley-Turkey 1965)**.** Existe um algoritmo que calcula a transformada de Fourier de uma função $f : \mathbb{Z}_n \to \mathbb{C}$ e consome tempo $O(n \lg n)$.

Demonstração. Até o final da prova, assumiremos que n é uma potência de 2 (se esse não for o caso, basta aplicar o algoritmo à função $f' : \mathbb{Z}_{n'} \to \mathbb{C}$, onde n' é a menor potência de 2 maior do que n e $f'(k) = f(k)$, para $0 \leqslant k \leqslant n$, e $f'(k) = 0$, para $n < k \leqslant n'$).

Temos que:

$$\begin{aligned}
\widehat{f}(u) &= \sum_{k=0}^{n-1} f(k) e^{-2\pi i k u/n} \\
&= \sum_{k=0}^{n/2-1} f(2k) e^{-2\pi i 2ku/n} + \sum_{k=0}^{n/2-1} f(2k+1) e^{-2\pi i (2k+1)u/n} \\
&= \underbrace{\sum_{k=0}^{n/2-1} f(2k) e^{-2\pi i k u/(n/2)}}_{A_u} + e^{2\pi i u/n} \underbrace{\sum_{k=0}^{n/2-1} f(2k+1) e^{-2\pi i k u/(n/2)}}_{B_u}
\end{aligned}$$

Defina f_0 como a soma dos monômios de ordem par de f e f_1 como a soma dos monômios de ordem ímpar ($f = f_0 + f_1$). Se $0 \leqslant u < \frac{n}{2}$, vale que $A_u = \widehat{f_0}$ e $B_u = \widehat{f_1}$. Se $\frac{n}{2} \leqslant u < n$, temos

$$\begin{aligned}
A_u &= \sum_{k=0}^{n/2-1} f(2k) e^{-2\pi i k (u-\frac{n}{2})/\frac{n}{2}} \underbrace{e^{-2\pi i k}}_{1} = A_{u-\frac{n}{2}}, \\
B_u &= \sum_{k=0}^{n/2-1} f(2k+1) e^{-2\pi i k (u-\frac{n}{2})/\frac{n}{2}} \underbrace{e^{-2\pi i k}}_{1} = B_{u-\frac{n}{2}}.
\end{aligned}$$

Concluímos que $\widehat{f}$ pode ser escrita como

$$\widehat{f}(u) = \begin{cases} \widehat{f_0}(u) + e^{-2\pi i u/n} \widehat{f_1}(u), & \text{se } 0 \leqslant u < \frac{n}{2} \\ \widehat{f_0}(u - \frac{n}{2}) + e^{-2\pi i u/n} \widehat{f_1}(u - \frac{n}{2}), & \text{se } \frac{n}{2} \leqslant u < n \end{cases}.$$

Uma vez calculadas as funções $\widehat{f_0}$ e $\widehat{f_1}$, a expressão acima pode ser computada por meio de $O(n)$ operações aritméticas. Isso dá origem a um algoritmo recursivo cujo número de operações $T(n)$ é dado pela recorrência

$$\begin{aligned}
T(1) &= 1 \\
T(n) &= 2T(\frac{n}{2}) + O(n),
\end{aligned}$$

da onde concluímos que $T(n) = O(n \lg n)$, como desejado. ■

Observação 1.2.4. O algoritmo trivial para multiplicação de polinômios pode ser mais eficiente que o apresentado nesta seção para *polinômios esparsos*, isto é, polinômios de grau alto mas com poucos coeficientes diferentes de zero.

Além disso, o algoritmo que usa a transformada de Fourier tem a desvantagem de introduzir erros de precisão numérica, mesmo para polinômios com coeficientes inteiros.

2 Alguns tópicos sobre aleatoriedade, pseudo-aleatoriedade e análise de Fourier

2.1 Grafos aleatórios e pseudoaleatórios

16/09/2014 – Yoshiharu Kohayakawa

Definição 2.1.1 (Modelo Erdős-Rényi de grafo aleatório)**.** O grafo $G_{n,p}$ é um grafo aleatório de n vértices em que cada uma das possíveis $\binom{n}{2}$ arestas é incluída independentemente com probabilidade p.

Observação 2.1.2. No estudo de grafos aleatórios $G(n,p)$ permite-se, em geral, que p seja uma função de n (por exemplo, é possível estudar o grafo $G_{n,1/\sqrt{n}}$). Contudo vamos nos restringir aqui ao caso que $0 < p < 1$ é uma *constante*.

usaremos superíndices para denotar o tamanho de um grafo

Seja $J = J^n$ um grafo com n vértices . Estamos interessados na seguinte pergunta: J ***parece*** **um grafo aleatório** $G_{n,p}$**?** A princípio essa pergunta é um pouco vaga, uma vez que todo grafo pode ser uma instância de $G_{n,p}$ com probabilidade positiva. Mais especificamente, temos

$$\mathbb{P}(G_{n,p} = J) = p^{e(J)}(1-p)^{\binom{n}{2}-e(J)}.$$

$e(G)$ denota o número de arestas de um grafo G

Entretanto, existem propriedades que são *tipicamente válidas* para grafos aleatórios $G_{n,p}$. Por exemplo, esperamos que as arestas de um grafo aleatório estejam bem distribuídas, isto é, a probabilidade de um grafo aleatório ter conjuntos grandes muito esparsos (ou muito densos) é baixa.

Podemos então reinterpretar a pergunta acima como: J satisfaz propriedades que são tipicamente válidas para grafos $G_{n,p}$? A seguir definimos mais precisamente o que é uma propriedade "tipicamente válida" de $G_{n,p}$.

Definição 2.1.3. Dizemos que uma propriedade $\mathcal{P}$ vale para $G_{n,p}$ *assintoticamente quase certamente* (*a.q.c*) se

$$\lim_{n\to\infty} \mathbb{P}(G_{n,p} \text{ satisfaz } \mathcal{P}) = 1.$$

Vamos listar agora uma série de propriedades que valem a.q.c para $G_{n,p}$.

◇ **Propriedade** $U_p(\varepsilon)$**:**
Um grafo $\Gamma = \Gamma^n$ satisfaz $U_p(\varepsilon)$ se para qualquer $S \subseteq V(\Gamma)$, com $|S| \geqslant \varepsilon n$,

$$e(\Gamma[S]) = (1 \pm \varepsilon)p\binom{|S|}{2}.$$

Fato 2.1.4. Para quaisquer $0 < p < 1$ e $0 < \varepsilon < 1$, $G_{n,p}$ satisfaz $\mathcal{U}_p(\varepsilon)$ a.q.c.
Demonstração (esboço). A variável aleatória $X_S = e(G_{n,p}[S])$, que conta o número de arestas do grafo induzido por um conjunto S de tamanho m segue uma distribuição binomial de média $p\binom{m}{2}$ e variância $(1-p)p\binom{m}{2}$. A desigualdade de Chebyschev já seria suficiente para mostrar que $\mathbb{P}(|X_S - \mu| > \varepsilon\mu) \to 0$ quando $n \to \infty$, para um conjunto *fixo* S, $|S| \geqslant \varepsilon n$. No entanto, para provar que isso vale para *todo* conjunto S, $|S| \geqslant \varepsilon n$, é preciso usar uma cota de Chernoff que afirma que $\mathbb{P}(|X_S - \mu| \geqslant \varepsilon\mu) \leqslant 2e^{-\frac{1}{3}\varepsilon^2\mu}$. Como há menos que 2^n conjuntos S como no enunciado, usamos a cota da união para mostrar que

$$\mathbb{P}(\forall S, |S| \leqslant \varepsilon n : |X_S - \mu| > \varepsilon\mu) < 2^n 2e^{-\frac{1}{3}\varepsilon^3 n} \to 0, \text{quando } n \to \infty.$$

■

◇ **Propriedade** $C_p^4(\varepsilon)$**:**
Um grafo $\Gamma = \Gamma^n$ satisfaz $C_p^4(\varepsilon)$ se

$$\#\{C^4 \to \Gamma\} = (1 \pm \varepsilon)(pn)^4,$$

onde

$$\#\{H \to G\} = \#\{f : \text{é um } \textit{homomorfismo} \text{ de } H \text{ para } G\}$$

(um *homomorfismo* de H em G é uma função $f : V(H) \to V(G)$ que preserva adjacências, isto é, tal que $xy \in E(H)$ implica $f(x)f(y) \in E(G)$).

Fato 2.1.5. Para quaisquer $0 < p < 1$ e $0 < \varepsilon < 1$, $G_{n,p}$ satisfaz $C_p^4(\varepsilon)$ a.q.c.

◇ **Propriedade $H_p(\varepsilon)$ (para um grafo H):**
Um grafo $\Gamma = \Gamma^n$ satisfaz $H_p(\varepsilon)$ se $\#\{H \to \Gamma\} = (1 \pm \varepsilon)p^{e(H)}n^{v(H)}$.

$v(G)$ é o número de vértices de um grafo G

◇ **Propriedade $Subgr_p^h(\varepsilon)$:**
$Subgr_p^h(\varepsilon) = \bigcap_{\{H:v(H)=h\}} H_p(\varepsilon)$, ou seja a propriedade $Subgr_p^h(\varepsilon)$ vale para um grafo Γ se Γ satisfaz $H_p(\varepsilon)$ para todo grafo H com h vértices.

Fato 2.1.6. Para quaisquer h, p, ε fixos, $G_{n,p}$ satisfaz $Subgr_p^h(\varepsilon)$ a.q.c.

◇ **Propriedade $Spec_p(\varepsilon)$:**
Para um grafo $\Gamma = \Gamma^n$, seja A a matriz de adjacência de Γ. Como A a simétrica os seus autovalores $\lambda_1 \geqslant \cdots \geqslant \lambda_n$ são todos reais. Dizemos que Γ satisfaz $Spec_p(\varepsilon)$ se

$$\begin{aligned} \lambda_1 &= (1 \pm \varepsilon)pn, \\ |\lambda_k| &\leqslant \varepsilon pn, \text{ para todo } k = 2, 3, \dots n. \end{aligned}$$

Fato 2.1.7. Para quaisquer p, ε fixos, $G_{n,p}$ satisfaz $Spec_p(\varepsilon)$ a.q.c.

Teorema 2.1.8 (Chung,Graham,Wilson)**.** Seja $0 < p < 1$ uma constante fixa e suponha que $\Gamma = \Gamma^n$ é um grafo com $e(\Gamma)\binom{n}{2}^{-1} = (1 + o(1))p$. Então as propriedades $U_p(o(1))$, $C_p^4(o(1))$, $Subgr_p^h(o(1))(h = 4, 5, \dots)$ e $Spec_p(o(1))$ são todas *equivalentes*.

Observação 2.1.9. Dizer que, por exemplo, que $U_p(o(1))$ *implica* $C_p^4(o(1))$ significa dizer que: para qualquer $\varepsilon > 0$, existem $\delta > 0$ e $n_0 > 0$ tais que todo grafo $\Gamma = \Gamma^n$ (com $n \geqslant n_0$) que satisfaz $U_p(\delta)$ também satisfaz $C_p^4(\varepsilon)$.

2.2 Aleatoriedade e pseudo-aleatoriedade em grupos finitos

22/09/2014 – Yoshiharu Kohayakawa

A partir daqui, vamos trabalhar com um *grupo abeliano finito* fixo Z. Tipicamente, estamos interessados nos casos $Z = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ ou $Z = \mathbb{Z}_p^n$ (em resultados assintóticos, se $Z = \mathbb{Z}_p^n$, fixamos p e fazemos $n \to \infty$).

Também fixaremos uma *forma bilinear* (não-degenerada) denotada pelo operador $\cdot$.

$$\begin{aligned} Z \times Z &\to \mathbb{R}/\mathbb{Z} \\ (\xi, x) &\mapsto \xi \cdot x \end{aligned}$$

Exemplo 2.2.1.
1. Para $Z = \mathbb{Z}_n$, podemos tomar $\xi \cdot x = (\xi \cdot x)/n$.
2. Para $Z = \mathbb{Z}_p^n$, podemos tomar $\xi \cdot x = (\sum_{i=1}^n \xi_i x_i)/p$, onde $\xi = (\xi_1, \dots, \xi_n)$ e $x = (x_1, \dots, x_n)$.

Definição 2.2.2. Para todo $\xi \in Z$, definimos o elemento $e_\xi \in \mathbb{C}^Z$ da seguinte forma.

$$\begin{aligned} e_\xi : Z &\to \mathbb{C} \\ x &\mapsto e(\xi \cdot x), \end{aligned}$$

onde $e : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ é a função tal que $e(\theta) = e^{2\pi i\theta}$.

Estamos interessados em estudar funções $f : Z \to \mathbb{C}$. Em particular, para conjuntos $A \subset Z$, estamos interessados na função $\mathbb{1}_A : Z \to \mathbb{C}$ indicadora de A ($\mathbb{1}_A(x) = 1$ se $x \in A$ e $\mathbb{1}_A(x) = 0$, caso contrário).

Definição 2.2.3. Dadas duas funções $f, g \in \mathbb{C}^Z$, definimos o seu produto interno como

$$\langle f, g \rangle_{\mathbb{C}^Z} = \frac{1}{|Z|} \sum_{x \in Z} f(x)\overline{g(x)} = \mathbb{E}_{x \in Z} f(x)\overline{g(x)} = \mathbb{E}_Z(f\overline{g}).$$

Lema 2.2.4. $(e_\xi)_{\xi \in Z}$ é uma base ortonormal de $(\mathbb{C}^Z, \langle \cdot, \cdot \rangle_{\mathbb{C}^Z})$. ■

Definição 2.2.5. Dada uma função $f \in \mathbb{C}^Z$, podemos expressá-la na base formada pelos (e_ξ):

$$f = \sum_{\xi \in Z} \langle f, e_\xi \rangle_{\mathbb{C}^Z} e_\xi.$$

Os escalares $\langle f, e_\xi \rangle_{\mathbb{C}^Z}$ da expressão acima são chamados de *coeficientes de Fourier* de f e são denotados por $\widehat{f}(\xi)$.

O coeficiente de Fourier associado ao elemento 0 está associado à média dos valores que a função em questão assume. De fato,

$$\widehat{f}(0) = \langle f, e_0 \rangle_{\mathbb{C}^Z} = \langle f, (1, \ldots, 1) \rangle_{\mathbb{C}^Z} = \frac{1}{|Z|} \sum_{x \in Z} f(x) = \mathbb{E}_Z(f).$$

Lema 2.2.6 (Parseval)**.** Sejam $f, g \in \mathbb{C}^Z$ e $\widehat{f} = (\widehat{f}(\xi))_\xi$ e $\widehat{g} = (\widehat{g}(\xi))_\xi$. Como consequência de $(e_\xi)_{\xi \in Z}$ ser uma base ortonormal, valem as seguintes indentidadades:

i. $\|f\|_{\mathbb{C}^Z} = \sqrt{\langle f, f \rangle_{\mathbb{C}^Z}} = \sqrt{\sum_\xi |\widehat{f}(\xi)|^2} =: \|\widehat{f}\|_{l^2_Z}$.

ii. $\langle f, g \rangle_{\mathbb{C}^Z} = \sum_\xi \widehat{f}(\xi)\overline{\widehat{g}(\xi)} =: \langle \widehat{f}, \widehat{g} \rangle_{l^2_Z}$,

onde $\langle \cdot, \cdot \rangle_{l^2_Z}$ e $\|\cdot\|_{l^2_Z}$ são, respectivamente, o produto interno usual e a norma euclidiana em $\mathbb{C}^Z$.

Definição 2.2.7. Dizemos que um conjunto $A \subset Z$ é *livre de somas* se

$$a + a' \notin A, \forall a, a' \in A.$$

Qual o tamanho máximo de um conjunto $A \subset Z$ livre de somas? Se $A \subseteq Z$ é tal que $|A| > |Z|/2$, então A não pode ser livre de somas. De fato, A é livre de somas se, e somente se, $A \cap (A + A') \neq \emptyset$ (onde $A + A' = \{a + a' : a, a' \in A\}$). Como $|A + A'| \geqslant |A|$ se $|A| > |Z|/2$, essa interseção nunca será vazia.

Definição 2.2.8 (convolução)**.**

$$(f * g)(x) = \mathbb{E}_{y \in Z} f(x - y)g(y) = \mathbb{E}_{y \in Z} f(y)g(x - y).$$

A convolução está diretamente relacionada com o conjunto da soma de dois conjuntos. Dados $A, B \subseteq Z$, temos

$$\begin{aligned}
(\mathbb{1}_A * \mathbb{1}_B)(x) &= \mathbb{E}_{y \in Z} \mathbb{1}_A(x - y)\mathbb{1}_B(y) \\
&= \frac{1}{|Z|} \sum_{y \in Z} \underbrace{\mathbb{1}_A(x - y)\mathbb{1}_B(y)}_{[=1 \Leftrightarrow y \in (x - A) \cap B]} \\
&= \mathbb{P}_{y \in Z}(y \in (x - A) \cap B) \\
&= \mathbb{P}_Z((x - A) \cap B).
\end{aligned}$$

Então $supp(\mathbb{1}_A * \mathbb{1}_B) = A + B$.

Como vimos anteriormente o coeficiente de Fourier associado associado ao elemento 0 é a média da função em questão. Em particular, $\widehat{\mathbb{1}}_A(0)$ é a densidade de A. Veremos que os demais coeficientes medem, em algum sentido, a "aleatoriedade" de A.

Definição 2.2.9. O *viés de Fourier* de um conjunto $A \subseteq Z$ é

$$\|A\|_u = \max_{\xi \neq 0} |\widehat{\mathbb{1}}_A(\xi)|.$$

Definição 2.2.10. A é *α-pseudo aleatório* se $\|A\|_u \leqslant \alpha$.

Sejam $A_1, \ldots, A_k \subseteq Z$ e $\sigma : A_1 \times \cdots \times A_k$ a função soma, isto é, $\sigma(a_1, \ldots, a_k) = a_1 + \cdots + a_k$. Se $A_1, \ldots, A_k$ são conjuntos escolhidos uniformemente ao acaso, o valor esperado de $|\sigma^{-1}(x)|$ (isto é, o valor esperado do número de k-uplas $(a_1, \ldots, a_k)$ que somam x) é $|Z|^{k-1}\mathbb{P}(A_1)\ldots\mathbb{P}(A_k)$, para $x \in Z$. O resultado a seguir mostra que mesmo no caso não aleatório, $\sigma^{-1}(x)$ está próximo do valor esperado, contanto que $A_1, \ldots, A_k$ tenham viés baixo.

Proposição 2.2.11. Se $k \geqslant 3$, então para qualquer $x \in Z$,

$$\left| \frac{|\sigma^{-1}(x)|}{|Z|^{k-1}} - \mathbb{P}(A_1)\ldots\mathbb{P}(A_k) \right| \leqslant \|A_1\|_u \ldots \|A_{k-2}\|_u \mathbb{P}(A_{k-1})^{\frac{1}{2}}\mathbb{P}(A_{k-1})^{\frac{1}{2}}.$$

Demonstração.

30/09/2014 – Yoshiharu Kohayakawa

Por um lado, temos

$$\begin{aligned}
\frac{1}{|Z|^{k-1}}|\sigma^{-1}(x)| &= \sum_{\substack{(a_1,\ldots,a_k)\in A_1\times\cdots\times A_k \\ \sum_i a_i = x}} \mathbb{1}_{A_1}(a_1)\cdots\mathbb{1}_{A_k}(a_k) \\
&= (\mathbb{1}_{A_1} * \cdots * \mathbb{1}_{A_k})(x) \\
&= Re(\sum_{\xi}(\widehat{\mathbb{1}}_{A_1}(\xi)\cdots\widehat{\mathbb{1}}_{A_k}(\xi))e_\xi(x)) \\
&\geqslant \mathbb{P}_Z(A_1)\cdots\mathbb{P}(A_k) - \sum_{\xi\neq 0}|\widehat{\mathbb{1}}_{A_1}(\xi)|\cdots|\widehat{\mathbb{1}}_{A_k}(\xi)| && \textit{(desigualdade triangular)} \\
&\geqslant \mathbb{P}_Z(A_1)\cdots\mathbb{P}(A_k) - \|A_1\|_u\cdots\|A_{k-2}\|_u \sum_{\xi\neq 0}|\widehat{\mathbb{1}}_{A_{k-1}}(\xi)||\widehat{\mathbb{1}}_{A_k}(\xi)| \\
&\geqslant \mathbb{P}_Z(A_1)\cdots\mathbb{P}(A_k) - \|A_1\|_u\cdots\|A_{k-2}\|_u \|\widehat{\mathbb{1}}_{A_{k-1}}(\xi)\|_{l^2_Z}\|\widehat{\mathbb{1}}_{A_k}(\xi)\|_{l^2_Z} && \textit{(Cauchy-Schwarz)} \\
&= \mathbb{P}_Z(A_1)\cdots\mathbb{P}(A_k) - \|A_1\|_u\cdots\|A_{k-2}\|_u \mathbb{P}_Z(A_{k-1})^{\frac{1}{2}}\mathbb{P}_Z(A_k)^{\frac{1}{2}}.
\end{aligned}$$

$\|\cdot\|_{l^2_Z}$ é a norma euclidiana

A desigualdade no sentido oposto

$$\frac{1}{|Z|^{k-1}}|\sigma^{-1}(x)| \leqslant \mathbb{P}_Z(A_1)\cdots\mathbb{P}_Z(A_k) + \|A_1\|_u\cdots\|A_{k-2}\|_u\mathbb{P}_Z(A_{k-1})^{\frac{1}{2}}\mathbb{P}_Z(A_k)^{\frac{1}{2}}$$

pode ser obtida de maneira completamente análoga. ■

Observação 2.2.12. Em particular, se $\|A_1\|_u\cdots\|A_{k-2}\|_u < \mathbb{P}(A_1)\cdots\mathbb{P}(A_{k-2})\mathbb{P}(A_{k-1})^{\frac{1}{2}}\mathbb{P}(A_k)^{\frac{1}{2}}$, então o resultado acima implica $A_1 + \cdots + A_k = Z$.

Lema 2.2.13 (Soma de Gauss)**.** Seja F um corpo de ordem ímpar e $A = \{a^2 : a \in F\}$. Então

$$\|A\|_u \leqslant \frac{1}{2|F|^{\frac{1}{2}}} + \frac{1}{2|F|}.$$

Demonstração. Como todo elemento não nulo de A é o quadrado de exatamente dois elementos de

F ($a \neq -a$, uma vez que o corpo tem ordem ímpar), temos

$$\begin{aligned}\widehat{\mathbb{1}}_A &= \frac{1}{|F|}\sum_{a\in A} e(-\xi\cdot a)\\ &= \frac{1}{|F|} + \frac{1}{2|F|}\sum_{\substack{a\in F\\ a\neq 0}} e(\xi\cdot a^2)\\ &= \frac{1}{2|F|} + \frac{1}{2|F|}\sum_{a\in F}\sum_{a\in F} e(-\xi\cdot a^2).\end{aligned}$$

Por outro lado,

$$\begin{aligned}|\sum_{a\in F} e(-\xi\cdot a^2)|^2 &= |\sum_{a\in F} e(\xi\cdot a^2)|^2\\ &= \sum_{a,b\in F} e(\xi\cdot(a^2-b^2))\\ &= \sum_{a,h\in F} e(\xi\cdot(a^2-(a+h)^2))\\ &= \sum_{h\in F} \underbrace{e(-\xi\cdot h^2)}_{\text{1 se } h=0}\underbrace{\sum_{a\in F} e(\xi\cdot 2ah)}_{\substack{|F| \text{ se } h=0\\ 0 \text{ se } h\neq 0}}\\ &= |F|.\end{aligned}$$

O resultado segue da substituição desta identidade na anterior. ■

Corolário 2.2.14. Sejam A e F como no lema anterior. Então $A+A+A = F$.
Demonstração. Basta aplicar os últimos dois resultados, lembrando que $\mathbb{P}_Z(A) > \frac{1}{2}$. ■

3 Polinômios estáveis e desigualdade de Gurvits

3.1 Permanente de uma matriz

14/10/2014 – Marcel K. de Carli Silva

Seja $A \in \mathbb{R}^{n\times n}$ uma matriz. O determinante de A pode ser expresso como

$$\det A = \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \prod_{i=1}^{n} A_{i\sigma(i)},$$

onde S_n é o grupo das permutações de n elementos.

O *permanente* de A é definido de maneira semelhante como

$$\operatorname{perm} A = \sum_{\sigma\in S_n}\prod_{i=1}^{n} A_{i\sigma(i)}.$$

Apesar do determinante de uma matriz poder ser computado em tempo polinomial, não se conhece um algoritmo polinomial para o cálculo do permanente. Mais do que isso, o problema de se calcular o permanente de uma matriz é #P-completo. Um dos melhores algoritmos conhecidos para esse problema se baseia no princípio da inclusão-e-exclusão e tem consumo de tempo $O(n2^n)$.

Podemos dar uma interpretação combinatória para o permanente da seguinte maneira: se $A \in \mathbb{Z}_+^{n\times n}$ é a matriz de biadjacência de um (multi-)grafo bipartido G (isto é, A_{ij} conta o número de arestas

entre u_i e v_j, onde $\{u_1, \ldots, u_n\}$ e $\{v_1, \ldots, v_n\}$ são as partes da bipartição), então é fácil de ver que $\operatorname{perm} A$ conta o número de emparelhamentos perfeitos de G.

A seguir apresentamos algumas conjecturas que envolvem o permanente de uma matriz.

Conjectura 3.1.1 (Erdős-Renyi)**.** Para todo $k \geqslant 3$, se $A \in \mathbb{Z}_+^{n\times n}$ satisfaz $A\mathbb{1} = A^t\mathbb{1} = k\mathbb{1}$, então $\operatorname{perm} A \geqslant \alpha_k^n$, para algum $\alpha_k > 1$.

Conjectura 3.1.2 (van der Waerden '26)**.** Seja $A \in \mathbb{R}_+^{n\times n}$ uma matriz duplamente estocástica, isto é, uma matriz satisfazendo $A\mathbb{1} = A^T\mathbb{1} = \mathbb{1}$. Então $\operatorname{perm} A \geqslant \frac{n!}{n^n}$. A igualdade vale se, e só se, $A_{ij} = \frac{1}{n}$ para todo i, j.

Não é difícil ver que esta conjectura implica a primeira. De fato, se A é uma matriz como na conjectura de Erdős-Renyi, então temos

$$\operatorname{perm} A = k^n \operatorname{perm}(\frac{A}{k}) \underset{(3.1.2)}{\geqslant} k^n \frac{n!}{n^n} \geqslant \underbrace{\left(\frac{k}{e}\right)^n}_{=:\alpha_k}.$$

Conjectura 3.1.3 (Schiver?, Valiant?)**.** O maior valor que podemos tomar para a constante a_k da conjectura anterior é

$$a_k = \frac{(k-1)^{k-1}}{k^{k-2}}.$$

Seja $\underline{A} = (A_1, \ldots, A_n)$, com $A_j \in \mathbb{R}^{n\times n}$, $A_j \succeq 0$, $\operatorname{Tr} A_j = 1$ para todo j e $\sum_{j=1}^n A_j = I$. O *descriminante misto* de $\underline{A}$ é dado por

$$D(\underline{A}) = [x_1 \ldots x_n] \det(\sum_{j=1}^n x_j A_j).$$

$[x_1 \ldots x_n]p$ denota o coeficiente do monômio $x_1 \ldots x_n$ de um polinômio $p \in \mathbb{C}[x_1, \ldots, x_n]$.

Em particular se para todo j, $A_j = \operatorname{diag}(Be_j)$, para uma certa matriz $B \in \mathbb{R}^{n\times n}$, então $D(\underline{A}) = \operatorname{perm} B$.

Conjectura 3.1.4 (Bapat)**.** Se $\underline{A}$ é como acima, então $D(\underline{A}) \geqslant \frac{n!}{n^n}$. Ademais, vale a igualdade se, e somente se, $A_j = \frac{1}{n}I$ para todo $j \in [n]$.

Todas as conjecturas apresentadas acima já foram provadas por diferentes autores. Recentemente, Gurvits (2007) deu uma prova curta, unificada e mais geral para todos esses resultados. Essa prova faz uso de *polinômios estáveis* e *hiperbólicos*.

3.2 Polinômios estáveis

Um polinômio $p \in \mathbb{C}[x_1, \ldots, x_n]$ é *estável* se não possui raízes em $\mathcal{H}^n$, onde $\mathcal{H} = \{z \in \mathbb{C} : Im(z) > 0\}$.

Proposição 3.2.1. Um polinômio $p \in \mathbb{R}[x]$ é estável se, e somente se, p possui apenas raízes reais.
Demonstração. Se r é raiz de p, então $\overline{r}$ também é raiz de p. ■

Proposição 3.2.2. Sejam $p \in \mathbb{C}[x_1, \ldots, x_n]$ estável e $a \in \overline{\mathcal{H}} = \{z \in \mathbb{C} : Im(z) \geqslant 0\}$. Então $p|_{x_i=a}$ é estável.
Demonstração. A afirmação é trivial se $a \in H$. Se $a \in \partial\mathcal{H}$, o resultado segue por um lema de preservação (da estabilidade) sobre limites, dado a seguir. ■

o *limite* considerado aqui é por cada coeficiente

Lema 3.2.3. Se $0 \not\equiv p \in \mathbb{C}[x_1, \ldots, x_n]$ é limite de uma sequência de polinômios estáveis, então p é estável.

Teorema 3.2.4 (Gauss-Lucas)**.** Seja $p \in \mathbb{C}[x]$ um polinômio não constante com raízes $r_1, \ldots, r_m$. Então cada raiz de p' está em $\operatorname{conv}\{r_1, \ldots, r_m\}$.

Demonstração. Como $p(x) = \alpha \prod_{i=1}^{m}(x - r_j)$, temos

$$\frac{p'(x)}{p(x)} = \frac{d \log p(x)}{dx} = \sum_{j=1}^{m} \frac{1}{x - r_j}, \text{ se } x \neq r_1, \ldots, r_m.$$

Suponha $p'(x) = 0$. Então

$$\sum_{j=1}^{m} \frac{1}{x - r_j} = \sum_{j=1}^{m} \frac{x - r_j}{|x - r_j|^2} = 0$$

$$\left(\sum_{j=1}^{m} \frac{1}{|x - r_j|^2} \right) x = \sum_{j=1}^{m} \frac{1}{|x - r_j|^2} r_j$$

■

Corolário 3.2.5. Se $0 \not\equiv p \in \mathbb{C}[x_1, \ldots, x_n]$ é estável, então $\frac{\partial p}{\partial x_i}$ é estável.
Demonstração. Podemos supor sem perda de generalidade que $i = 1$. Fixe $z_2, \ldots, z_n \in \mathcal{H}$. O polinômio $q(x) = p(x, z_2, \ldots, z_n)$ deve ser, portanto, estável. Aplicando o Teorema 3.2.4 concluímos que $q'(x)$ também não tem raízes em $\mathcal{H}$, isto é, $\frac{\partial p}{\partial x_i}$ é estável. ■

$\underline{x} = (x_1, \ldots, x_n)$

Exemplo 3.2.6. Se $A \in \mathbb{R}_+^{n \times n}$ é estável, então

$$\text{prod}_A(\underline{x}) := \prod_{j=1}^{n} (A\underline{x})_j \text{ é estável.}$$

A

Proposição 3.2.7. Sejam $B \in CC^{m \times m}$ uma matriz hermitiana e $A_j \in \mathbb{C}^{m \times m}$, $A_j \succeq 0$, para todo $j \in [n]$. Então

$$p(\underline{x}) := \det(\sum_{i=1}^{n} A_j + B)$$

é estável.
Demonstração. Aplicando o Lema 3.2.3, podemos assumir que $A_j \succ 0$. Seja

$$\underline{z} = \underbrace{\underline{a}}_{\in \mathbb{R}^n} + \underline{b}i, \underline{b} > 0,$$

tal que

$$\sum_{i=1}^{n} z_j A_j + B = H + iC,$$

onde

$$C = \sum_{j=1}^{n} b_j A_j \succ 0$$

e H é hermitiana. Temos

$$H + iC = C^{\frac{1}{2}}(C^{-\frac{1}{2}} H C^{-\frac{1}{2}} + iI) C^{\frac{1}{2}},$$

da onde segue que

$$p(Z) = \underbrace{\det C}_{>0} \underbrace{\det(\overbrace{C^{-\frac{1}{2}} H C^{-\frac{1}{2}}}^{\text{hermitiana}} + iI)}_{\neq 0}.$$

■

3.3 Polinômios duplamente estocásticos

21/10/2014 – Marcel K. de Carli Silva

um polinômio é *homogêneo* se os monômios não nulos têm todos o mesmo grau

Um polinômio homogêneo $p \in \mathbb{R}_+[x_1, \ldots, x_n]$ de grau n é *duplamente estocástico* se $\frac{\partial p}{\partial x_j}(\mathbb{1}) = 1$ para todo $j \in [n]$.

Exemplo 3.3.1. Se $A \in \mathbb{R}^{n\times n}$ é duplamente estocástico, então prod_A é duplamento estocástico.
Demonstração.

$$\frac{\partial}{\partial x_j}\operatorname{prod}(\mathbb{1}) = \frac{\partial}{\partial x_j}\prod (A\underline{x})_k\Big|_{x=1} = \sum_{k=1}^{n}\frac{\partial}{\partial x_j}(A\underline{x})_k\Big|_{x=1} = \prod_{l\in[n]-\{j\}}(A\mathbb{1})_l = 1.$$

■

Seja $p \in \mathbb{R}_+[x_1, \ldots, x_n]$ um polinômio homogêneo de grau n. A *capacidade* de p é dada por

$$\operatorname{cap}(p) = \inf_{\underline{x}\in\mathbb{R}^n_{>0}} \frac{p(\underline{x})}{x_1\cdots x_n}.$$

Proposição 3.3.2. Se $p \in \mathbb{R}_+[x_1, \ldots, x_n]$ é duplamente estocástico, então $p(\mathbb{1}) = 1$.

Proposição 3.3.3. Se $p \in \mathbb{R}_+[x_1, \ldots, x_n]$ é duplamente estocástico, então $\operatorname{cap}(p) = 1$.
Demonstração. Escreva $p(\underline{x})$ como

$$p(\underline{x}) = \sum_{\alpha\in\mathbb{N}^n} p_\alpha \underline{x}^\alpha,$$

onde $\underline{x}^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$. Sabemos, pela proposição anterior, que $p(\mathbb{1}) = 1$, isto é, que $\sum_\alpha p_\alpha = 1$. Para qualquer $\underline{y} \in \mathbb{R}^n_{>0}$, temos

$$\log p(\underline{y}) = \log\sum_{\alpha\in\mathbb{N}^n} p_\alpha \underline{y}^\alpha \underset{Jensen}{\geqslant} \sum_{\alpha\in\mathbb{N}^n} p_\alpha \log(\underline{y}^\alpha) = \sum_{j=1}^{n}\log(y_j)\underbrace{\sum_{\alpha\in\mathbb{N}^n}\alpha_j p_\alpha}_{\frac{\partial p}{\partial x_j}(\mathbb{1})=1} = \log(y_1\cdots y_n).$$

■

3.4 Desigualdade de Gurvits

Teorema 3.4.1 (Gurvits 2008)**.** Sejam $p \in \mathbb{R}_+[x_1, \ldots, x_n]$ um polinômio homogêneo de grau n e $G : \mathbb{N}_+ \to \mathbb{R}$ uma função com $G(0) = 1$ e $G(k) = \frac{h(k)}{h(k-1)}$, para $k \geqslant 1$, onde $h(k) = \frac{k!}{k^k}$. Então

$$[x_1 \ldots x_n]p = \frac{\partial^n}{\partial x_1\cdots\partial x_n}p(\underline{0}) \geqslant cap(p)\prod_{i=1}^{n} G(\min\{i, \deg_i(p)\}).$$

Ademais, vale a igualdade se, e só se, $p(\underline{x}) = (a^T x)^n$, para algum $a \in \mathbb{R}^n_+$.

Mostraremos a seguir como a Desigualdade de Gurvits fornece demonstrações simples para algumas das conjecturas apresentadas anteriormente.

Demonstração da Conjectura 3.1.2. A função G é não-crescente e, portanto, temos

$$\prod_{1}^{n} G(\min\{i, \deg_i(p)\}) \geqslant \prod_{i=1}^{n} G(i) = h(n) = \frac{n!}{n^n}.$$

Assim, se $A \in \mathbb{R}^{n\times n}$ é uma matriz duplamente estocástica, então

$$\operatorname{perm} A \underset{ex.}{=} [x_1 \ldots x_n]\operatorname{prod}_A \underset{D.G.}{\geqslant} \underbrace{\operatorname{cap}(p)}_{1}\frac{n!}{n^n}.$$

■

Demonstração da Conjectura 3.1.4. Seja $\underline{A}$ como na conjectura. Então

$$D(\underline{A}) = [x_1 \dots x_n] \det(\sum_{j=1}^{n} x_j A_j) \geqslant \operatorname{cap}(\sum_{j=1}^{n} x_j A_j) \frac{n!}{n^n} = \frac{n!}{n^n}.$$

■

Para provar a Desigualdade de Bapat, vamos primeiro provar os dois seguintes lemas.

Lema 3.4.2. Seja $p \in \mathbb{R}_+[x]$ um polinômio com grau $m \geqslant 1$, $p = \sum_{i=1}^{m} p_i x^i$. Se p é estável, então $p'(0) \geqslant \operatorname{cap}(p) G(m)$.

Demonstração. Vamos assumir $\operatorname{cap}(p) > 0$, uma vez que a desigualdade é trivialmente verdadeira caso contrário. Se $m = 1$, então $p'(0) = p_1 = \operatorname{cap}(p) G(1) = \operatorname{cap}(p)$. Assuma então $m > 1$. Se $p_0 = 0$, então

$$p'(0) = \lim_{t \downarrow 0} \frac{p(t)}{t} \geqslant \operatorname{cap}(p) \underbrace{G(m)}_{\leqslant 1}.$$

Se $p_0 > 0$, então podemos assumir $p_0 = 1$ (divida tudo por p_0). Neste caso podemos escrever

$$p(x) = \prod_{i=1}^{m} (1 + a_i x),$$

para certos $a_i > 0$, uma vez que as raízes de p são todas reais (pois p é estável) e negativas (pois os coeficientes de p são todos positivos). Temos $p'(0) = p_1 = a_1 + \dots + a_m$.

Para todo $x > 0$, vale que

$$\frac{\log(\operatorname{cap}(p) x)}{m} \leqslant \frac{\log p(x)}{m} = \frac{1}{m} \sum_{i=1}^{m} \log(1 + a_i x) \underset{Jensen}{\leqslant} \log\left(1 + \frac{a_1 + \dots + a_m}{m} x\right),$$

da onde segue que

$$\operatorname{cap}(p) x \leqslant \left(1 + \frac{p_1 x}{m}\right)^m =: q(x).$$

Como a inequação acima vale para todo $x > 0$, concluímos que

$$\operatorname{cap}(p) \leqslant \operatorname{cap}(q) \underset{fato}{=} \frac{p_1}{G(m)}.$$

(o x^* que atinge o ótimo em $\operatorname{cap}(q)$ é $x^* = \frac{m}{(m-1)p_1}$) ■

Lema 3.4.3. Seja $p \in \mathbb{R}_+[x_1 \dots x_n]$ um polinômio estável e homogêneo de grau n, $n \geqslant 1$. Então

$$\operatorname{cap} \underbrace{\left(\frac{\partial}{\partial x_n} p \Big|_{x_n = 0} \right)}_{:= q} \geqslant G(\deg_n(p)) \operatorname{cap}(p).$$

Demonstração. Seja $m = \deg_n(p) \geqslant 1$, sem perda de generalidade. Se $n = 1$, a afirmação segue do lema anterior. Suponha $n \geqslant 2$. Para qualquer $\underline{y} \in \mathbb{R}_{>0}^{n-1}$, defina $r_{\underline{y}}(x) = p(y_1, \dots, y_{n-1}, x)$. Então

$$\begin{aligned} \frac{q(\underline{y})}{y_1 \dots y_{n-1}} &= q(\alpha \underline{y}) && (\text{para } \alpha = (y_1 \dots y_{n-1})^{-\frac{1}{n-1}}) \\ &= r'_{\alpha y}(0) \\ &\geqslant G(m) \operatorname{cap}(r_{ay}). && (\text{usando o lema anterior}) \end{aligned}$$

■

Demonstração da Desigualdade de Gurvits. Seja $q_n = p$ e defina, indutivamente

$$q_{i-1} = \frac{\partial}{\partial x_i} q_i \Big|_{x_i=0},$$

para todo $i \in [n]$. Observe que todos os polinômios definidos são estáveis.

Temos

$$\begin{aligned}
\frac{\partial^n}{\partial x_1 \dots \partial x_n} p(\underline{0}) = q_0 = \operatorname{cap}(q_0) &\geqslant \operatorname{cap}(q_1) G(\deg_1(q_1)) \\
&\geqslant \operatorname{cap}(q_2) G(\deg_1(q_1)) G(\deg_2(q_2)) \\
&\geqslant \cdots \\
&\geqslant \operatorname{cap}(q_n) \prod_{i=1}^{n} G(\deg_i(q_i)) \\
&\geqslant \operatorname{cap}(q_n) \prod_{i=1}^{n} G(\underbrace{\min\{i, \deg_i(p)\}}_{\geqslant \deg_i(q_i)}).
\end{aligned}$$

■

3.5 Número de caminhos hamiltonianos em um torneio

04/11/2014 – Yoshiharu Kohayakawa

Um *torneio* é um grafo completo em que todas as arestas recebem uma orientação. Por exemplo:

(figura)

Um *caminho hamiltoniano* em um torneio é um caminho orientado que percorre todos os vértices do torneio. Para todo torneio T defina

$$P(T) = \text{número de caminhos hamiltonianos em } T.$$

Exercício 3.5.1. Para todo torneio T, $P(T) > 0$.

Exercício 3.5.2. Para todo torneio T, $P(T) \equiv 1 \pmod 2$.

Estamos interessados no número máximo de caminhos hamiltonianos que um torneio de tamanho n pode ter.

$$P(n) = \max\{P(T) : \ T \text{ é um torneio com } n \text{ vértices}\}.$$

O resultado a seguir, que fornece uma cota inferior para $P(n)$, é considerado a primeira aplicação do método probabilístico.

Teorema 3.5.3 (Szele '43)**.** $P(n) \geqslant n! 2^{n-1}$.

Demonstração. Considere um torneio T em que orientamos as $\binom{n}{2}$ arestas de K^n aleatória e independentemente. Seja X o número de caminhos hamiltonianos em T. Temos

$$X = \sum_{\sigma} \mathbb{1}_{\{\sigma \text{ é caminho hamiltoniano}\}},$$

onde o somatório é sobre todas as permutações σ de $V(T)$. Assim,

$$\begin{aligned}\mathbb{E}(X) &= \sum_{\sigma} \mathbb{E}(\mathbb{1}_{\{\sigma \text{ é caminho hamiltoniano}\}}) \\ &= \sum_{\sigma} \mathbb{P}(\mathbb{1}_{\{\sigma \text{ é caminho hamiltoniano}\}}) \\ &= \sum_{\sigma} \left(\frac{1}{2}\right)^{n-1} = n!2^{n-1}.\end{aligned}$$

■

Szele também mostrou que $P(n) \leqslant cn!/2^{\frac{3}{4}n}$, para alguma constante $c > 0$. Ademais, Szele provou que

$$\lim_{n\to\infty} \left(\frac{P(n)}{n!}\right)^{\frac{1}{n}}$$

existe e conjecturou que é igual a $\frac{1}{2}$.

Alon mostrou que

$$P(n) \leqslant cn^{\frac{3}{2}} \frac{n!}{2^{n-1}},$$

confirmando a conjectura de Szele. Para isso, Alon usa a cota de Brégman para permanentes, exposta a seguir.

A desigualdade de Brégman.

Sabemos que o permanente de matrizes estocásticas é no máximo 1 (esse máximo é atingido, por exemplo, pela matriz identidade). Considere agora uma matriz $A \in \mathbb{R}_{\geqslant 0}^{n\times n}$ cuja soma dos elementos de cada linha é k. Neste caso, $\max \operatorname{perm}(A) = k^n$ (a matriz kI atinge esse máximo). Suponha ainda que A tem entradas somente em $\{0, 1\}$. Se $k|n$, temos $\max \operatorname{perm}(A) \geqslant (k!)^{\frac{n}{k}}$ (esse valor é atingido por uma matriz diagonal por blocos de tamanho $k \times k$).

Conjectura 3.5.4 (Minc '63)**.** Seja $A \in \{0, 1\}^{n\times n}$ uma matriz tal que a i-ésima linha soma $r_i > 0$, para $1 \leqslant i \leqslant n$. Então

$$\operatorname{perm}(A) \leqslant \prod_{i=1}^{n} r_i!^{\frac{1}{r_i}}.$$

Teorema 3.5.5 (Brégman '73)**.** A conjectura de Minc vale.

Dizemos que um arco (x, y) tem *cauda* x e *cabeça* y.

Voltando para torneios: Um 1-fator em um torneio é uma coleção de arcos F tal que todo vértice é *cabeça* de exatamente 1 arco em F e *cauda* de exatamente 1 arco em F. Em particular, se F é conexo então, F determina um *circuito hamiltoniano*. Definimos

$$F(T) = \text{número de 1-fatores em } T$$

e

$$C(T) = \text{número de circuitos hamiltonianos em } T.$$

Temos $C(T) \leqslant F(T)$. Ademais, vale que $P(T) = nC(T)$ para torneios de tamanho n.

Dado T, $V(T) = [n]$, definimos a *matriz de adjacência* $A = (a_{ij})$ fazendo

$$a_{ij} = \begin{cases} 1 & \text{se } (i, j) \in E(T), \\ 0 & \text{caso contrário.} \end{cases}$$

O permanente da matriz acima está relacionado com o número de 1-fatores de T. De fato, cada parcela não-nula da soma que define $\operatorname{perm}(A)$ corresponde a um 1-fator de T. Isto é, temos

$F(T) \leqslant \mathrm{perm}(A)$. Suponha o vértice i de T tem grau de saída $r_i > 0$, para todo $i \in [n]$ (note que $\sum_i r_i = \binom{n}{2}$). Então segue do Teorema de Brégman que

$$F(T) \leqslant \mathrm{perm}(A) \leqslant \prod_{i=1}^{n} r_i!^{\frac{1}{r_i}}.$$

Lema 3.5.6. O valor de

$$\begin{aligned} &\max \prod_{i=1}^{n} r_i!^{\frac{1}{r_i}} \\ \text{sujeito a } &\sum_{i=1}^{n} r_i = S, \\ &0 < r_i \in \mathbb{N} \end{aligned}$$

é atingindo quando $r_1, \ldots, r_n$ são o mais iguais possíveis, isto é, quando $|r_i - r_j| \leqslant 1$, para todo $1 \leqslant i, j \leqslant n$.

Demonstração. Exercício. (mostrar que se existe i, j tais que $r_i \geqslant r_j + 2$, então podemos substituir r_i por $r_i + 1$ e r_j por $r_j + 1$ e aumentar o valor da função objetivo) ■

Usando o resultado acima e a fórmula de Stirling obtemos

Stirling: $n! = \left(\frac{n}{e}\right)^n \sqrt{2\pi n}(1 + o(1))$

$$\max\left\{\prod_{i=1}^{n} r_i!^{\frac{1}{r_i}} : \sum_{i=1}^{n} r_i = \binom{n}{2}, r_i > 0\right\} = (1 + o(1))\sqrt{\frac{\pi}{2e}} n^{\frac{3}{2}} \frac{(n-1)!}{2^n}.$$

Ponha

$$F(n) = \max\{F(T) : T \text{ é um torneio de tamanho } n\}$$

e

$$C(n) = \max\{C(T) : T \text{ é um torneio de tamanho } n\}.$$

Temos

$$C(n) \leqslant F(n) \leqslant (1 + o(1))\sqrt{\pi} 2e n^{\frac{3}{2}} \frac{(n-1)!}{2^n}.$$

Para obter uma cota para $P(n)$ a partir da desigualdade acima, procedemos da seguinte forma. Seja T um torneio qualquer. Construa um torneio aleatório $T' = T + x$, adicionando um vértice x a T e orientando as arestas incidentes a x de forma uniforme e independente. Cada caminho hamiltoniano de T tem probabilidade $\frac{1}{4}$ de dar origem a um circuito hamiltoniano de T'. Então

$$\mathbb{E}(C(T')) = \frac{1}{4} P(T),$$

o que implica que existe T' com pelo menos $\frac{1}{4}P(T)$ circuitos hamiltonianos. Então devemos ter

$$P(T) \leqslant c n^{\frac{3}{2}} \frac{n!}{2^{n-1}}.$$

3.6 Uma prova do Teorema de Brégman via entropia

18/11/2014 – Yoshiharu Kohayakawa

Veremos uma demonstração do Teorema 3.5.5 via entropia, feita por Radhakrishna (1996).

Seja X uma variável aleatória com $\mathrm{supp}(X)$ finito . Definimos a *entropia* de X como

$\mathrm{supp}\, X = \{x : \mathbb{P}(X = x) > 0\}$

$$H(X) = \sum_{x \in \mathrm{supp}(X)} \mathbb{P}(X = x) \log \frac{1}{\mathbb{P}(X = x)},$$

onde a função $\log(x)$ denotará, a partir daqui, o logaritmo na base 2. A entropia de uma variável aleatória pode ser interpretada como uma média da quantidade de informação (em *bits*) que cada evento $[X = x]$ carrega.

Seja (X, Y) um par de variáveis aleatórias e $x \in \operatorname{supp}(X)$. Definimos uma variável aleatória Y_x tal que para todo $y \in \operatorname{supp}(Y)$

$$\mathbb{P}(Y_x = y) = \mathbb{P}(Y = y \mid X = x).$$

A *entropia condicional* de Y dado X é dada por

$$H(Y \mid X) = \mathbb{E}_{x \in \operatorname{supp}(X)}(H(Y_x)).$$

Proposição 3.6.1. $H(X) \leqslant \log |\operatorname{supp}(X)|$.
Demonstração.

$$\begin{aligned} H(X) &= \sum_{x \in \operatorname{supp}(X)} \mathbb{P}(X = x) \log \frac{1}{\mathbb{P}(X = x)} \\ &\leqslant \log \sum_{x \in \operatorname{supp}(X)} \mathbb{P}(X = x)(\mathbb{P}(X = x))^{-1} \\ &= \log |\operatorname{supp}(X)|, \end{aligned}$$

onde a desigualdade segue do fato da função log ser côncava (Jensen). ■

$\sqcup$ denota união disjunta

Suponha que $\operatorname{supp}(X) = A_1 \sqcup \cdots \sqcup A_r$ e $|\operatorname{supp}(Y_x)| \leqslant i$, para todo $1 \leqslant i \leqslant r$ e $x \in A_i$. Então segue da proposição acima que

$$H(Y|X) \leqslant \sum_{i=1}^{r} \mathbb{P}(X \in A_i) \log i. \tag{1}$$

Também usaremos o seguinte fato.

Proposição 3.6.2. $H(X, Y) = H(X) + H(Y \mid X)$.
Demonstração.

$$\begin{aligned} H(X) + H(Y \mid X) &= \sum_{x \in \operatorname{supp}(X)} \mathbb{P}(X = x) \log \frac{1}{\mathbb{P}(X = x)} \\ &\quad + \sum_{x \in \operatorname{supp}(X)} \mathbb{P}(X = x) \sum_{y \in \operatorname{supp}(Y_x)} \mathbb{P}(Y = y \mid X = x) \log \frac{1}{\mathbb{P}(Y = y \mid X = x)} \\ &= \sum_{x \in \operatorname{supp}(X)} \sum_{y \in \operatorname{supp}(Y_x)} \mathbb{P}(X = x)\mathbb{P}(Y = y \mid X = x) \log \frac{1}{\mathbb{P}(X = x)\mathbb{P}(Y = y \mid X = x)} \\ &= \sum_{(x,y) \in \operatorname{supp}(X,Y)} \mathbb{P}(X = x, Y = y) \log \frac{1}{\mathbb{P}(X = x, Y = y)} \\ &= H(X, Y). \end{aligned}$$

■

Seja $A = (a_{i,j})$ uma matriz em $\{0, 1\}^{n \times n}$ com exatamente r_i 1s na linha i, para todo $i \in [n]$. Seja $S = \{\sigma : a_{i,\sigma(i)} = 1, \forall i \in [n]\}$. Temos $\operatorname{perm}(A) = |S|$. Vamos considerar σ como uma permutação uniformemente sorteada em S. Temos

$$H(\sigma) = \log |\operatorname{supp} \sigma| = \log |S| = \log \operatorname{perm}(A).$$

Queremos provar que

$$H(\sigma) \leqslant \log \prod_{i=1}^{n} (r_i!)^{\frac{1}{r_i}} = \sum_{i=1}^{n} \frac{1}{r_i} \log r_i! = \sum_{i=1}^{n} \sum_{j=1}^{r_i} \frac{1}{r_i} \log j. \tag{2}$$

Vamos revelar σ em n etapas usando uma permutação τ das linhas de A, isto é, consideramos $\tau \in S_n$ como uma permutação escolhida uniformemente ao acaso e examinamos

$$\sigma(\tau(1)), \sigma(\tau(2)), \dots \sigma(\tau(n)).$$

Fixe i e seja $k = \sigma^{-1}(i)$, isto é, $\sigma(i)$ é o k-ésimo elemento da sequência acima. Ao examinar $\sigma(i)$ já vimos $\sigma(\tau(1)), \dots, \sigma(\tau(k-1))$. Seja

$$R_i(\sigma, \tau) = \{j : a_{i,j} = 1 \text{ e } j \neq \sigma(\tau(1)), \dots, \sigma(\tau(k-1))\}.$$

Em particular, temos $\sigma(i) \in R_i(\sigma, \tau)$ (pois σ é uma permutação em S).

Lema 3.6.3. Para qualquer σ e $j \in \{1, 2 \dots, r_i\}$

$$\mathbb{P}_\tau(|R_i(\sigma, \tau)| = j) = \frac{1}{r_i}.$$

Demonstração. Fixe σ e seja $T = \{j : a_{i,j} = 1\}$. Note que $i \in \tau^{-1}(T)$. O conjunto $R_i(\sigma, \tau)$ depende apenas de como as linhas $\sigma^{-1}(T)$ aparecem em τ (as colunas de T que não estão em $R_i(\sigma, \tau)$ são justamente as da forma $\sigma(i')$, para todo i' que precede i na ordem dada por τ). Isto é, se i é o l-ésimo elemento (dentro das linhas em $\sigma^{-1}(T)$) da ordem dada por τ, então

$$|R_i(\sigma, \tau)| = r_i - l + 1.$$

Mas como τ é uma permutação escolhida de forma uniforme, l tem distribuição uniforme em $\{1, \dots, r_i\}$ aquelas que aparecem antes de i. ■

Para todo τ fixo temos

$$H(\sigma) = H(\sigma(\tau(1)), \sigma(\tau(2)), \dots, \sigma(\tau(n))) = \sum_{i=1}^{n} H(\sigma(\tau(i))|\sigma(\tau(1)), \dots, \sigma(\tau(i-1))),$$

onde a última desigualdade segue da aplicação da Proposição 3.6.2 n vezes. Fixado i, seja $Y = \sigma(\tau(i))$ e $X = (\sigma(\tau(1)), \dots, \sigma(\tau(i-1)))$. Particione o $\operatorname{supp} X$ em classes $A_1, \dots, A_{r_i}$ de forma que $|R_i(\sigma, \tau)| = j$ para todo $\sigma \in A_j$. Então, segue da equação (1) que

$$H(\sigma) \leqslant \sum_{i=1}^{n} \sum_{j=1}^{r_i} \mathbb{P}_\sigma(|R_i(\sigma, \tau)| = j) \log j).$$

Tiramos a média sobre todo τ, obtemos

$$\begin{aligned}
\mathbb{E}_\tau(H(\sigma)) = H(\sigma) &= \mathbb{E}_\tau \sum_{i=1}^{n} \sum_{j=1}^{r_i} \mathbb{P}_\sigma(|R_i(\sigma, \tau)| = j) \log j \\
&= \sum_{i=1}^{n} \sum_{j-1}^{r_i} \mathbb{E}_\tau \left(\mathbb{P}_\sigma(|R_i(\sigma, \tau)| = j)\right) \log j \\
&= \sum_{i=1}^{n} \sum_{j-1}^{r_i} \left(\mathbb{P}_{\sigma,\tau}(|R_i(\sigma, \tau)| = j)\right) \log j \\
&= \sum_{i=1}^{n} \sum_{j-1}^{r_i} \frac{1}{r_i} \log j,
\end{aligned}$$

da onde segue o Teorema de Brégman (ver equação (2)).

4 Casamentos e Integração Invariante

4.1 Grupos topológicos e integração

Trabalharemos com grupos G em um espaço topológico, isto é, grupos munidos de uma topologia e tais que a operação do grupo e a operação de tomar inversos de elementos são, ambas, funções contínuas, tais como:

- Grupos finitos como $\mathbb{Z}_n$.
- Grupos topológicos não compactos, como $\mathbb{R}^n$ e $\mathbb{C}^n$ (onde a operação do grupo é a soma).
- O grupo ortogonal $O(\mathbb{R}^n) = \{A \in \mathbb{R}^{n\times n} : A^T A = I\}$, em que a operação considerada é a multiplicação.

A partir daqui vamos supor que G é *compacto*. Também definimos $\mathcal{C}(G) = \{f : G \to \mathbb{R} : f \text{ é contínua}\}$.

Definição 4.1.1 (integração)**.** Uma *integração* de um grupo G é um funcional $I : \mathcal{C}(G) \to \mathbb{R}$ satisfazendo

1. $I(\alpha f + \beta g) = \alpha I(f) + \beta I(g)$. *[linearidade]*
2. $I(f) \geqslant 0$, se $f \geqslant 0$. *[monotonicidade]*
3. Se $\mathbb{1}$ é a função constante de valor 1, então $I(\mathbb{1}) = 1$ *[normalização]*
4. $\forall s, t \in G$, se $g(x) = f(sxt) \forall x \in G$, então $I(f) = I(g)$. *[invariância]*

Teorema 4.1.2 (Haar 1933)**.** Para todo grupo topológico compacto G, existe uma (única) integração de G.

Notamos que para grupos G finitos podemos simplesmente tomar a seguinte integração

$$I : \mathcal{C}(G) \to \mathbb{R}$$
$$I : f \mapsto \frac{1}{|G|} \sum_{x\in G} f(x).$$

4.2 Aplicação do Teorema de Haar: integração na esfera

$S^{n-1} = \{x \in \mathbb{R}^n : \|x\| = 1\}$

Seja $f : S^{n-1} \to \mathbb{R}$ contínua e

$$\int_{S^{n-1}} f(x)dx := \int_{O(\mathbb{R}^n)} f(Ax_0)dA \text{ para todo } x_0 \in S^{n-1} \text{ fixo.}$$

Aqui, estamos usando a notação de integral para definir uma integração de S^{n-1} (em função de uma integração de $O(\mathbb{R}^n)$). Essa integração está bem-definida pois para qualquer x_0', existe $B \in O(\mathbb{R}^n)$ tal que $Bx_0 = x_0'$ — logo, pela propriedade de *invariância*, a definição acima independe da escolha de x_0.

Se $A \subseteq S^{n-1}$ é "mensurável", defina a *densidade* de A por $\delta(A) = \int_{S^{n-1}} \mathbb{1}_A(x)dx$, onde $\mathbb{1}_A$ é a função característica[1] de A.

Para todo $t_0 \in [-1, 1)$ fixo, defina

$$m_{t_0}(S^{n-1}) = \sup\{\delta(A) : A \subseteq S^{n-1}, \langle x, y\rangle \neq t_0 \forall x, y \in A\}.$$

Teorema 4.2.1. Seja $V \subseteq S^{n-1}$ finito e

$$\alpha(V) = \max\{|A| : A \subseteq V \text{ e } \langle x, y\rangle \neq t_0, \forall x, y \in A\}.$$

Então $m_{t_0} \leqslant \frac{\alpha(V)}{|V|}$.

[1] a rigor, não podemos fazer essa definição pois $\mathbb{1}_A$ não é contínua, mas é possível contornar essa limitação.

Demonstração. Seja $A \subseteq S^{n-1}$ um conjunto que "evita" t_0, isto é, que não contém elementos cujo produto interno é t_0. Então

$$\begin{aligned}
\delta(A)|V| &= \sum_{v\in V} \int_{O(\mathbb{R}^n)} |A \cap \{Tv\}| dT \\
&= \int_{O(\mathbb{R}^n)} \sum_{v\in V} |A \cap \{Tv\}| dT && \textit{[linearidade]} \\
&= \int_{O(\mathbb{R}^n)} |A \cap TV| dT \\
&\leqslant \int \alpha(V) dT \\
&= \alpha(V). && \textit{[normalização]}
\end{aligned}$$

■

O resultado acima nos permite afirmar, por exemplo, que para $t_0 = \cos 2\pi/3$ e $n = 2$, temos $m_{t_0} = \frac{1}{3}$, uma vez que o conjunto $A = \{(\cos(\theta), \sin(\theta))\}_{0\leqslant\theta\leqslant\pi/3}$ atinge esse valor e qualquer conjunto $V \in S^{n-1}$ formado pelos três vértices de um triângulo equilátero atesta que $m_{t_0} \leqslant \frac{1}{3}$.

4.3 Demonstração do Teorema de Haar

Faremos uso de dois resultados de topologia, enunciados a seguir.

Topologia

Definição 4.3.1 (U-rede)**.** Seja $U \subseteq G$ aberto. Um conjunto $A \subseteq G$ é uma *U-rede* se $A \cap sUt \neq \emptyset$, $\forall s, t \in G$.

Na definição acima, U geralmente será um conjunto "pequeno", isto é, com densidade próxima de 0.

Proposição 4.3.2. Se G é compacto, então existe uma U-rede finita para todo $U \subseteq G$.

Definição 4.3.3 (medida)**.** A *medida* da rede $U \subseteq G$ abeliano é dada por

$$\delta(U) = \delta_f(U) = \sup\{|f(x) - f(y)| : x, y \in sUt \text{ para algum } s, t \in G\}.$$

Proposição 4.3.4. Para todo $\varepsilon > 0$, existe $U \neq \emptyset$ aberto tal que $\delta(U) < \varepsilon$. ■

Lema 4.3.5. Seja $U \subseteq G$ um conjunto aberto e A, B U-redes de cardinalidade mínima. Então

$$|f(A) - f(B)| < \delta(U).$$

Demonstração. Considere um grafo bipartido $H = (A \sqcup B, E)$, cujas partes são os conjuntos A e B respectivamente, e tal que para todo $x \in A$ e $y \in B$. Suponha que H admita um emparelhamento perfeito $a_1b_1, \ldots, a_nb_n$ (com $a_i \in A$, $b_i \in B$). Nesse caso, temos

$$|f(A) - f(B)| \leqslant \frac{1}{n}\sum_{i=1}^{n} |f(a_i) - f(b_i)| \leqslant \frac{1}{n}\sum_{i=1}^{n} \delta(U) = \delta(U),$$

como desejado.

Resta, portanto, mostrar que H de fato possui um emparelhamento perfeito. Primeiro, note que como A e B são de cardinalidade mínima, devemos ter $|A| = |B|$. Assim, pelo Teorema de Hall, é suficiente mostrar que $\forall X \subseteq A$, X possui pelo menos $|X|$ vizinhos em B. Fixe $X \in A$ e seja $Y = \Gamma(X)$ o conjunto formado pelos vértices adjacentes a pelo menos um vértice de X.

Afirmamos que $T = Y \cup (A \setminus X)$ é U-rede. De fato, como A é U-rede, existe $x \in A \cap sUt$. Se $x \in T$ não há nada a fazer. Se que $x \notin T$, então $x \in X$. Mas como B também é U-rede, sabemos que existe $y \in B \cap sUt$. Logo x é adjacente a y, o que implica que $y \in Y$ e, em particular, que $y \in T$.

Como T é U-rede, devemos ter $|T| \geqslant |A|$. Mas $|T|-|Y|+|A|-|X| \geqslant 0$, da onde segue que $|Y| \geqslant |X|$, como desejado.

■

Lema 4.3.6. Se A é U-rede mínima e B é V-rede mínima, então $|f(A) - f(B)| \leqslant \delta(U) - \delta(V)$.
Demonstração. Para qualquer $b \in B$, Ab também é U-rede mínima.Segue do lema anterior que $|f(A) - f(Ab)| \leqslant \delta(U)$. Assim

$$|f(A) - f(AB)| = \left\| f(A) - \frac{1}{|B|} f(A, b) \right\| \leqslant \frac{1}{|B|} \sum |f(A) - f(Ab)| \leqslant \frac{1}{|B|} \delta(U)|B| = \delta(U).$$

Similarmente temos $|f(B) - f(AB)| \leqslant \delta(V)$. O resultado segue, portanto, da desigualdade triangular. ■

Pela Proposição 4.3.4, existem $\{U_n\}_{n \geqslant 0}$ abertos tais que $\delta(U_n) \to 0$. Para todo $n \geqslant 0$, considere uma U_n-rede mínima A_n, cuja existência é garantida pela Proposicao 4.3.2. Fixe $f \in \mathcal{C}(G)$. Pelo Lema 4.3.6, a sequência $\{f(A_n)\}_{n \geqslant 0}$ é de Cauchy e, portanto, converge para um certo valor $I(f)$. Afirmamos que o funcional $f \mapsto I(f)$ é uma integração de G. De fato, não é difícil verificar as três primeiras condições da Definição 4.1.1. Para verificar a condição de *invariância*, note que também segue do Lema 4.3.6 que o limite $I(f)$ *não depende* da escolha de $\{U_n\}$. Em particular, fixados $s, t \in G$, podemos repetir o argumento a partir da sequência $\{sU_nt\}_{n \geqslant 0}$ para concluir que $I(f) = I(g)$ (onde $g : x \mapsto sf(x)t$).

A Soluções dos exercícios resolvidos

Exercício resolvido. (1.1.2) Suponha que G é um grupo com identidade e. Valem as seguintes asserções.

1. (Caracterização do neutro) Para todo $x \in G$, temos $x + x = x$ se e só se $x = e$;

2. (Elemento oposto à direita) Para todo $x \in G$, temos $x + (-x) = e$;

3. (Elemento neutro à direita) Para todo $x \in G$, temos $x + e = x$;

4. (Unicidade do elemento neutro) Se $x, y \in G$ são tais que $x + y = y$, então $x = e$;

5. (Unicidade do elemento oposto) Se $x, y, z \in G$ são tais que $y + x = z + x = e$, então $y = z$;

6. (Bijeção através da operação) Para todo $y \in G$, a função $g_y \colon G \ni x \mapsto x + y \in G$ é bijetora.

Demonstração. Para a asserção da caracterização do elemento neutro, temos

$$x + x = x \Longrightarrow (-x) + (x + x) = (-x) + x \Longrightarrow e + x = e \Longrightarrow x = e.$$

Por outro lado, se $x = e$, então trivialmente $x + x = e + e = e$.

Para a asserção do elemento oposto à direita, observe que se $x \in G$, temos que

$$(x + (-x)) + (x + (-x)) = x + e + (-x) = x + (-x),$$

logo, da caracterização do elemento neutro, segue que $x + (-x) = e$.

Para a asserção do elemento neutro à direita, observe que se $x \in G$, temos que

$$x + e = x + ((-x) + x) = e + x = x.$$

Para a asserção da unicidade do elemento neutro, basta observar que $x + y = y$ implica que $x + y + (-y) = y + (-y)$, logo temos $x = e$.

Para a asserção da unicidade do elemento oposto, basta observar que $y + x = z + x$ implica que $y + x + (-x) = z + x + (-x)$ e pelas asserções do elemento oposto à direita e elemento neutro à direita, segue que $y = z$.

Finalmente, para a asserção da bijeção através da operação, observe que se $g_y(x) = g_y(z)$, então $y + x = y + z$, logo $x = z$. Por outro lado, para todo $x \in G$, temos que $g_y((-y) + x) = y + (-y) + x = x$. ■

Exercício resolvido. (1.1.4) Se f é um homomorfismo de grupos do grupo G no grupo H, então temos $f(e_G) = e_H$, onde e_G e e_H são as identidades de G e H respectivamente.

Demonstração. Basta observar que

$$f(e_G) = f(e_G + e_G) = f(e_G) + f(e_G),$$

logo, da caracterização da identidade (Exercício 1.1.2), segue que $f(e_G) = e_H$. ■

Exercício resolvido. (1.1.9) Se χ é caracter de G e ψ é caracter de H, então

$$\begin{array}{rccc} \chi \otimes \psi \colon & G \times H & \longrightarrow & \mathbb{T} \\ & (g, h) & \longmapsto & \chi(g)\psi(h) \end{array}$$

é caracter de $G \times H$.

Ademais, se φ é caracter de $G \times H$, então existem χ caracter de G e ψ caracter de H tais que $\varphi = \chi \otimes \psi$.

Demonstração. Observe primeiramente que se $(g_1, h_1), (g_2, h_2) \in G \times H$, então temos

$$\begin{aligned}\chi \otimes \psi((g_1, h_1) + (g_2, h_2)) &= \chi \otimes \psi((g_1 + g_2, h_1 + h_2)) = \chi(g_1 + g_2)\psi(h_1 + h_2) \\ &= \chi(g_1)\chi(g_2)\psi(h_1)\psi(h_2) = \chi(g_1)\psi(h_1)\chi(g_2)\psi(h_2) \\ &= \chi \otimes \psi((g_1, h_1))\chi \otimes \psi((g_2, h_2)).\end{aligned}$$

Portanto $\chi \otimes \psi$ é caracter de $G \times H$.

Seja agora φ um caracter qualquer de $G \times H$. Sejam e_G e e_H as identidades de G e H respectivamente e defina $\chi(g) = \varphi(g, e_H)$ para todo $g \in G$ e $\psi(h) = \varphi(e_G, h)$ para todo $h \in H$.

Observe que, para todos $g_1, g_2 \in G$, temos

$$\chi(g_1 + g_2) = \varphi((g_1 + g_2, e_H)) = \varphi((g_1, e_H) + (g_2, e_H)) = \varphi((g_1, e_H))\varphi((g_2, e_H)) = \chi(g_1)\chi(g_2).$$

Analogamente, para todos $h_1, h_2 \in H$, temos

$$\psi(h_1 + h_2) = \varphi((e_G, h_1 + h_2)) = \varphi((e_G, h_1) + (e_G, h_2)) = \varphi((e_G, h_1))\varphi((e_G, h_2)) = \psi(h_1)\psi(h_2).$$

Portanto χ é caracter de G e ψ é caracter de H.

Observe agora que para todo $(g, h) \in G \times H$, temos

$$\chi \otimes \psi((g, h)) = \chi(g)\psi(h) = \varphi((g, e_H))\varphi((e_G, h)) = \varphi((g + e_G, e_H + h)) = \varphi((g, h)).$$

Portanto $\varphi = \chi \otimes \psi$. ■

B Notação

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$
$$\mathbb{N}^* = \mathbb{N} \setminus \{0\}$$
$$\mathbb{R}_+ = \{x \in \mathbb{R} : x \geqslant 0\}$$
$$[n] = \{1, 2, \ldots, n\}, \text{ para } n \in \mathbb{N}^*$$
$$\mathbb{J}_n \text{ denota a matriz } n \times n \text{ com todas as entradas 1}$$
$$f(n) \sim g(n) \text{ significa } \lim_{n\to+\infty} \frac{f(n)}{g(n)} = 1$$
$$f(n) = O(g(n)) \text{ significa } \limsup_{n\to+\infty} \left|\frac{f(n)}{g(n)}\right| < +\infty$$
$$f(n) = \Omega(g(n)) \text{ significa } g(n) = O(f(n))$$
$$f(n) = \Theta(g(n)) \text{ significa } f(n) = O(g(n)) \text{ e } f(n) = \Omega(g(n))$$
$$f(n) \asymp g(n) \text{ significa } f(n) = \Theta(g(n))$$
$$f(n) = o(g(n)) \text{ significa } \limsup_{n\to+\infty} \left|\frac{f(n)}{g(n)}\right| = 0$$
$$f(n) = \omega(g(n)) \text{ significa } g(n) = o(f(n))$$
$$\pi(n) = |\{a \in [n] : a \text{ é primo}\}|, \text{ para } n \in \mathbb{N}$$
$$\lfloor x \rfloor \text{ denota o maior inteiro menor ou igual a } x, \text{ para } x \in \mathbb{R}$$
$$\lceil x \rceil = -\lfloor -x \rfloor$$
$$\binom{A}{k} = \{B \subset A : |B| = k\}, \text{ para } A \text{ um conjunto}$$
$$\binom{A}{\leqslant k} = \{B \subset A : |B| \leqslant k\}, \text{ para } A \text{ um conjunto}$$
$$n \mid m \text{ significa } n \text{ divide } m, \text{ para } n, m \in \mathbb{Z}, m \neq 0$$
$$N_G(v) = \{w \in V(G) : vw \in E(G)\}, \text{ para } G \text{ um grafo e } v \in V(G)$$
$$d_G(v) = |N_G(v)|, \text{ para } G \text{ um grafo e } v \in V(G)$$
$$N_G(X) = \bigcup_{x\in X} N_G(x), \text{ para } G \text{ um grafo e } X \subset V(G)$$
$$\delta_G(X) = \{xy \in E(G) : x \in X\}, \text{ para } G \text{ um grafo e } X, Y \subset V(G)$$
$$\delta_G(X, Y) = \{xy \in E(G) : x \in X \text{ e } y \in Y\}, \text{ para } G \text{ um grafo e } X, Y \subset V(G)$$
$$\delta(G) = \min\{d_G(v) : v \in V(G)\}, \text{ para } G \text{ um grafo}$$
$$\Delta(G) = \sup\{d_G(v) : v \in V(G)\}, \text{ para } G \text{ um grafo}$$

Índice de palestrantes

Índice de nomes

Referências