Seminário de Métodos Probabilísticos
– Subconjuntos Pseudo-aleatórios do $\mathbb{Z}_n$ –

Jair Donadelli Júnior *

*Referência: F.R.K. Chung and R.L. Graham, *Quasi-Radom Subsets of* $\mathbb{Z}_n$, J. Combin. Theory Ser. A (1992).

0 Aquecimento: Grafos pseudo-aleatórios

Escrevemos $\mathcal{G}(n)$ para a família dos grafos de ordem n e G_n para um grafo arbitrário de ordem n. Em 1989, Chung, Graham e Wilson [2] introduziram uma classe de propriedades de grafos que são equivalentes e satisfeitas por grafos aleatórios *quase-sempre*, isto é, propriedades P tais que

$$\Pr\left[G_n \in \mathcal{G}(n)\colon G_n \text{ satisfaz } P\right] \to 1 \text{ quando } n \to \infty.$$

No Teorema 1 abaixo, listamos essa classe de equivalência de propriedades que são satisfeitas para grafos aleatórios quase sempre, para probabilidade de arestas $1/2$. Resultados análogos podem ser provados para probabilidade de arestas p, para todo $0 < p < 1$ fixo, basicamente pelos mesmos argumentos.

Um grafo que satisfaz alguma (portanto, todas) dessas propriedades é dito *grafo pseudo-aleatório*.

No que segue adotamos as seguintes notações, $N^*_{G_n}(H)$ e $N_{G_n}(H)$ denotam o número de cópias induzidas e não necessariamente induzidas de H em G_n, respectivamente. Denotamos por $\Gamma_{G_n}(x)$ o conjunto dos vértices adjacentes a x em G_n. Usamos C^t para denotar o circuito com t arestas e $A = A(G_n) = (a_{x,y})_{x,y\in V(G_n)}$ é a matriz de adjacências de G_n. Lembramos que A é uma matriz real simétrica, portanto, admite autovalores reais.

Teorema 1 *São equivalentes:*
$\mathbf{P_1}(s)$: *Para todo grafo H de ordem s, $s \geq 4$ inteiro,*

$$N^*_{G_n}(H) = (1+o(1))n^s 2^{-\binom{s}{2}}.$$

$\mathbf{P_2}(t)$: *Para $t \geq 4$ inteiro par,*

$$\mathrm{e}(G_n) \geq (1+o(1))\left(\frac{n}{2}\right)^2 \qquad e \qquad N_{G_n}(C^t) \leq (1+o(1))\left(\frac{n}{2}\right)^t.$$

$\mathbf{P_3}$: *Considere uma ordenação $|\lambda_1| \geq \cdots \geq |\lambda_n|$ dos autovalores λ_i de $A(G_n)$. Então,*

$$\mathrm{e}(G_n) \geq (1+o(1))\left(\frac{n}{2}\right)^2, \qquad \lambda_1 = (1+o(1))\frac{n}{2} \qquad e \qquad \lambda_2 = o(n).$$

$\mathbf{P_4}$: *Para cada $U \subseteq V(G_n)$, temos*

$$\mathrm{e}(U) = \frac{1}{4}|U|^2 + o(n^2).$$

$\mathbf{P_5}$: *Para cada* $U \subseteq V(G_n)$*, com* $|U| = \lfloor n/2 \rfloor$*, temos*

$$\mathrm{e}(U) = \left(\frac{1}{16} + o(1)\right) n^2.$$

$\mathbf{P_6}$: *Para todo* x*,* $y \in V(G_n)$*, se* $S(x,y) = V(G_n) \setminus (\Gamma(x) \triangle \Gamma(y))$*, então*

$$\sum_{x,y \in V} \left| |S(x,y)| - \frac{n}{2} \right| = o(n^3).$$

$\mathbf{P_7}$: *Para todos* x*,* $y \in V(G_n)$

$$\sum_{x,y \in V} \left| |\Gamma(x) \cap \Gamma(y)| - \frac{n}{4} \right| = o(n^3).$$

Note que $\mathbf{P_2}$ vale somente para circuitos pares. O seguinte exemplo mostra a diferença, neste contexto, entre circuitos pares e circuitos ímpares. Sejam G um grafo com $4n$ vértices e V_1, V_2, V_3, V_4 subconjuntos disjuntos de $V(G)$, cada um de tamanho n. Em V_1 e em V_2 colocamos todas arestas, entre V_3 e V_4 colocamos todas as aresta e entre $V_1 \cup V_2$ e $V_3 \cup V_4$ colocamos as arestas com probabilidade $1/2$. Esse grafo não é pseudo-aleatório, entretanto, valem $\mathbf{P_1}(3)$ e $\mathbf{P_2}(2t+1)$ para todo t fixo.

O leitor interessado pode encontrar uma dezena de exemplos de grafos pseudo-aleatórios em Thomason [4]. Vejamos um deles, mas antes do exemplo de grafo pseudo-aleatório, vejamos algumas notações e alguns resultados básicos de álgebra. Dizemos que um inteiro a é um *resíduo quadrático* módulo um primo $p \geq 3$ se p não divide a e

$$a \equiv x^2 \mod p$$

para algum inteiro x. O *símbolo de Legendre*, $(\cdot/p)$, é definido da seguinte forma: se p divide a, então $(a/p) = 0$, senão

$$(a/p) = \begin{cases} +1 & \text{se } a \text{ é resíduo quadrático de } p, \\ -1 & \text{se } a \text{ não é resíduo quadrático de } p. \end{cases}$$

Os seguintes resultados são teoremas básicos de álgebra.

(a) *Metade dos inteiros* a *tais que* $1 \leq a \leq p-1$ *são resíduos quadráticos de* p*.*

(b) *Se d divide $p-1$, então $x^d \equiv 1 \mod p$ tem exatamente d soluções.*

(c) *Para todo primo p vale $a^p \equiv a \mod p$.*

Desses três resultados, temos que o conjunto dos resíduos quadráticos de p é igual ao conjunto das soluções de

$$x^{\frac{p-1}{2}} \equiv 1 \mod p.$$

Portanto, se p não divide a, vale que

$$(a/p) \equiv a^{\frac{p-1}{2}} \mod p, \tag{1}$$

e, se p também não divide b, temos que

$$(a/p)(b/p) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv (ab/p). \tag{2}$$

O *grafo de Paley*, Q_p, é um dos exemplos de grafos pseudo-aleatórios mais conhecidos e usados. Ele é definido para todo primo $p \equiv 1 \mod 4$ (existem infinitos primos dessa forma!) pondo $V(Q_p) = \mathbb{Z}_p$, o corpo finito de ordem p, e as arestas são dadas por $E(Q_p) = \{\{i,j\} \colon (i-j/p) = 1\}$. Note que da escolha de p temos, por (1), que $(-1/p) = (-1)^{(p-1)/2} = 1$ e isso quer dizer que $\{i,j\} \in E(Q_p)$ está bem definido pois

$$(i-j/p) = 1 \Leftrightarrow (i-j/p)(-1/p) = 1 \overset{(2)}{\Leftrightarrow} (j-i/p) = 1.$$

Agora, observe que $k \in V(Q_p)$ é adjacente a i, $j \in V(Q_p)$ distintos, ou não-adjacente a ambos se, e somente se, $\frac{k-i}{k-j}$ é um resíduo quadrático de p. Mas, para quaisquer um dos $1/2(p-1)-1$ resíduos quadráticos a, de p, diferente de 1, existe um único k tal que

$$\frac{k-i}{k-j} = 1 + \frac{j-i}{k-j} = a.$$

Assim, $S(i,j) = 1/2(p-3)$, portanto, $\mathbf{P_6}$ vale.

Terminamos observando que Q_p difere do grafo aleatório $G_{p,1/2}$ no seguinte: S.W. Graham e C. Ringrose [3] provaram que o tamanho do clique máximo de Q_p, que denotamos $\omega(Q_p)$, é tão grande quanto $\log p \log\log\log p$ para infinitos valores de p, enquanto que o valor esperado de $\omega(G_{p,1/2})$ é $(1+o(1))\log p$ (veja Bollobás [1]).

1 Pré-requisitos

O primeiro pré-requisito que veremos é a desigualdade de Cauchy-Schwarz.

Proposição 1 *Sejam $d_1, \ldots, d_n$ reais. Então para todo inteiro não-negativo $m < n$*

$$\sum_{i=1}^{n} {d_i}^2 \geq \frac{1}{n}\left(\sum_{i=1}^{n} d_i\right)^2 + \frac{mn}{n-m}\left(\frac{1}{m}\sum_{i=1}^{m} d_i - \frac{1}{n}\sum_{i=1}^{n} d_i\right)^2. \tag{3}$$

Em particular, se

$$\frac{1}{m}\sum_{i=1}^{m} d_i = \alpha\frac{1}{n}\sum_{i=1}^{n} d_i,$$

então

$$\sum_{i=1}^{n} {d_i}^2 \geq \frac{1}{n}\left(1+(\alpha-1)^2\frac{m}{n-m}\right)\left(\sum_{i=1}^{n} d_i\right)^2. \tag{4}$$

Demonstração. Ponha $S_n = \sum_{i=1}^{n} d_i$ e $Q_n = \sum_{i=1}^{n} {d_i}^2$. Então

$$0 \leq \sum_{i=1}^{n}\left(d_i - \frac{S_n}{n}\right)^2 = \sum_{i=1}^{n}\left({d_i}^2 - 2d_i\frac{S_n}{n} + \frac{{S_n}^2}{n^2}\right) = Q_n - \frac{{S_n}^2}{n}, \tag{5}$$

portanto,

$$Q_n - Q_m = \sum_{i=m+1}^{n} {d_i}^2 \geq \frac{1}{n-m}\left(\sum_{i=m+1}^{n} d_i\right)^2 = \frac{(S_n-S_m)^2}{n-m}.$$

Então

$$\begin{aligned} Q_n = Q_m + (Q_n - Q_m) &\geq \frac{{S_m}^2}{m} + \frac{(S_n-S_m)^2}{n-m} \\ &= \frac{1}{n}{S_n}^2 + \frac{nm}{n-m}\left(\frac{S_n}{n} - \frac{S_m}{m}\right)^2. \end{aligned}$$

e demonstramos (3). Agora, provar (4) é fácil. Observe que (5) é a desigualdade usual de Cauchy-Schwarz. QED

1.1 Notação

Denotamos por $\mathbb{Z}_n$ o anel dos inteiros módulo n. Se S e T são subconjuntos do $\mathbb{Z}_n$ então pomos $|S| = s$ e $|T| = t$.

Definimos a função característica em $S \subseteq \mathbb{Z}_n$ por

$$\chi_S(x) = \begin{cases} 1, & x \in S \\ 0, & x \notin S. \end{cases}$$

Para todos $u, v \in \mathbb{Z}_n$ vamos escrever $u+v$ para $u+v \pmod{n}$. Com isso, definimos $S + x = \{j + x \colon j \in S\}$.

Quase todo $x \in X$ significa todos elementos de X exceto $o(|X|)$ deles, ou seja, a menos de um subconjunto de $m = m(|X|)$ elementos com $m/|X| \to 0$ quando $|X| \to \infty$.

2 Propriedades pseudo-aleatórias do $\mathbb{Z}_n$

Vamos definir propriedades de subconjuntos do $\mathbb{Z}_n$ que provaremos serem equivalentes e que são facilmentes provadas serem satisfeitas para subconjuntos aleatórios do $\mathbb{Z}_n$.

WT: Para quase todo $x \in \mathbb{Z}_n$

$$|S \cap (S + x)| = \frac{s^2}{n} + o(n).$$

ST: Para todo $T \subseteq \mathbb{Z}_n$, onde $|T| = t$, e para quase todo $x \in \mathbb{Z}_n$

$$|S \cap (T + x)| = \frac{st}{n} + o(n).$$

$\mathbf{Q(k)}$: Para quase todos $u_1, \ldots, u_k \in \mathbb{Z}_n$

$$\sum_{x \in \mathbb{Z}_n} \prod_{i=1}^{k} \chi_S(x + u_i) = \frac{s^k}{n^{k-1}} + o(n).$$

$\mathbf{Q(2)}$: Para quase todos $u_1,\, u_2 \in \mathbb{Z}_n$

$$\sum_{x \in \mathbb{Z}_n} \chi_S(x + u_1)\chi_S(x + u_2) = \frac{s^2}{n} + o(n).$$

R(2): Para quase todo $x \in \mathbb{Z}_n$

$$\sum_{u_1+u_2=x} \chi_S(u_1)\chi_S(u_2) = \frac{s^2}{n} + o(n).$$

R(k): Para quase todo $x \in \mathbb{Z}_n$

$$\sum_{u_1+\cdots+u_k=x} \prod_{i=1}^{k} \chi_S(u_i) = \frac{s^k}{n} + o(n^{k-1}).$$

EXP: Para todo $0 \neq j \in \mathbb{Z}_n$

$$\sum_{x\in\mathbb{Z}_n} \chi_S(x)\exp\left(\frac{2\pi ijx}{n}\right) = o(n).$$

Um subconjunto S do $\mathbb{Z}_n$ que satisfaz alguma (e, portanto, todas) dessas propriedades é dito um *subconjunto pseudo-aleatório do* $\mathbb{Z}_n$. Vamos provar a equivalência dessas propriedades em duas etapas.

Lema 1

$$\mathbf{WT} \Rightarrow \mathbf{ST} \Rightarrow \mathbf{Q(k)} \Rightarrow \mathbf{Q(2)} \Rightarrow \mathbf{WT}.$$

Lema 2

$$\mathbf{ST} \Rightarrow \mathbf{R(2)} \Rightarrow \mathbf{R(k)} \Rightarrow \mathbf{EXP} \Rightarrow \mathbf{ST}.$$

2.1 Conexão com grafos pseudo-aleatórios

As propriedades pseudo-aleatórias acima têm conexão com grafos pseudo aleatórios conforme descrevemos abaixo.

Graph: Para $S \subseteq \mathbb{Z}_n$ definimos $G_S = (\mathbb{Z}_n, E)$ por $E = \{\{i,j\} : i+j \in S\}$.

G_S é pseudo-aleatório.

C(2t):

$$\sum_{x_1,\ldots,x_{2t}} \chi_S(x_1+x_2)\chi_S(x_2+x_3)\cdots\chi_S(x_{2t-1}+x_{2t})\chi(x_{2t}+x_1) = s^{2t} + o(n^{2t}).$$

Density: Para todo $T \subseteq \mathbb{Z}_n$

$$\sum_{x,y} \chi_T(x)\chi_T(y)\chi_S(x+y) = \frac{st^2}{n} + o(n^2).$$

E temos o seguinte lema.

Lema 3

$$\mathbf{C(2t)} \Leftrightarrow \mathbf{Graph} \Leftrightarrow \mathbf{Density} \Leftrightarrow \mathbf{Q(2)}.$$

2.2 Demonstrações do Lema 1 e Lema 2

WT $\Rightarrow$ **ST**: Dado $a \in \mathbb{Z}_n$ temos por **WT** que $|(S-a)\cap(S-b)| = s^2/n + o(n)$. Então, temos

$$\begin{aligned}
&\sum_{a\in T}\sum_{b\in T}|(S-a)\cap(S-b)| = \\
&\qquad \sum_{a\in T}\sum_{b\in T}\sum_{x\in\mathbb{Z}_n}\chi_S(x-a)\chi_S(x-b) = \\
&\qquad \sum_{a\in\mathbb{Z}_n}\sum_{\mathbb{Z}_n\in T}\sum_{x\in\mathbb{Z}_n}\chi_S(x-a)\chi_S(x-b)\chi_T(a)\chi_T(b) = \\
&\qquad \sum_{x\in\mathbb{Z}_n}\left(\sum_{c\in\mathbb{Z}_n}\chi_S(x-c)\chi_T(c)\right)^2 = \\
&\qquad \sum_{x\in\mathbb{Z}_n}|(S-x)\cap T|^2.
\end{aligned}$$

Por outro lado,

$$\begin{aligned}
&\sum_{a\in T}\sum_{b\in T}|(S-a)\cap(S-b)| \le \\
&\qquad \sum_{a\in T}\left(\frac{s^2}{n}+o(n)\right)t + no(n) = \\
&\qquad \left(\frac{s^2}{n}+o(n)\right)t^2 + to(n^2) = \\
&\qquad \frac{s^2t^2}{n} + o(n^3).
\end{aligned}$$

Portanto,

$$\sum_{x\in\mathbb{Z}_n}|(S-x)\cap T|^2 = \frac{s^2t^2}{n} + o(n^3). \tag{6}$$

Dado $\varepsilon > 0$ ponha

$$M_\varepsilon = \left\{x\in\mathbb{Z}_n\colon\ \left||(S-x)\cap T| - \frac{st}{n}\right| \ge \varepsilon n\right\},$$

e defina M_ε^+ como os pontos $x \in M_\varepsilon$ tais que $|(S-x)\cap T| \geq st/n + \varepsilon n$ e defina M_ε^- de forma análoga. Devemos mostrar que $|M_\varepsilon| = o(n)$.

Suponha que para algum ε existe δ tal que $|M_\varepsilon| > 2\delta n$. Assim, vamos supor que $m = |M_\varepsilon^+| > \delta n$ (caso contrário, $|M_\varepsilon^-| > \delta n$ e o argumento é análogo).

Na desigualdade de Cauchy-Schwarz (3) pomos

$$\Delta = \frac{1}{m}\sum_{i=1}^{m} d_i - \frac{1}{n}\sum_{i=1}^{n} d_i. \tag{7}$$

Note que $\sum_x |(S-x)\cap T| = st$ então em (3), usando (6), ficamos com

$$\frac{s^2t^2}{n} + o(n^3) \geq \frac{s^2t^2}{n} + \frac{\delta n}{1-\delta}\Delta^2,$$

portanto, $\Delta = o(n)$. Agora,

$$\Delta \geq \frac{1}{m}\left(\frac{st}{n} + \varepsilon n\right) m - \frac{st}{n} = \varepsilon n,$$

uma contradição. QED

ST $\Rightarrow$ **Q(k)**: Provaremos por indução em k. Para $k=2$ temos

$$\sum_{x\in\mathbb{Z}_n} \chi_S(x+u_1)\chi_S(x+u_2) = |(S-u_1)\cap(S-u_2)| = \frac{s^2}{n} + o(n).$$

Sejam $u_1,\ldots,u_k \in \mathbb{Z}_n$, para $k \geq 3$. Então,

$$T = \bigcap_{i=1}^{k-1}(S-u_i) \overset{h.i.}{\Rightarrow} |T| = \frac{s^{k-1}}{n^{k-2}} + o(n).$$

Portanto,

$$\left|\bigcap_{i=1}^{k}(S-u_i)\right| = |T\cap(S-u_k)| = \frac{s(s^{k-1}/n^{k-2}+o(n))}{n} + o(n) = \frac{s^k}{n^{k-1}} + o(n).$$

QED

$\mathbf{Q(k)} \Rightarrow \mathbf{Q(2)}$: De $\mathbf{Q(k)}$ temos que

$$\sum_{u_1,\ldots,u_k} \left(\sum_x \prod_i \chi(x+u_i) \right)^2 =$$

$$n^k \left(\frac{s^k}{n^{k-1}} + o(n) \right)^2 + o(n^k)n^2 =$$

$$\frac{s^k}{n^{k-2}} + o(n^{k+2}),$$

portanto,

$$\sum_{u_1,u_2} \left(\sum_x \chi(x+u_1)\chi(x+u_2) \right)^2 \leq s^4 + o(n^2),$$

pois

$$\sum_{u_1,\ldots,u_k} \left(\sum_x \chi(x+u_1)\cdots\chi(x+u_k) \right)^2 \geq$$

$$\sum_{u_1,u_2} \frac{1}{n^{k-2}} \left(\sum_{u_3,\ldots,u_k} \sum_x \chi(x+u_1)\cdots\chi(x+u_k) \right)^2 =$$

$$\frac{1}{n^{k-2}} \sum_{u_1,u_2} \left(s^{k-2} \sum_x \chi(x+u_1)\chi(x+u_2) \right)^2.$$

Por outro lado,

$$\sum_{u_1,u_2} \sum_x \chi(x+u_1)\chi(x+u_2) = \sum_x \left(\sum_{u_1} \chi(x+u_1) \right) \left(\sum_{u_2} \chi(x+u_2) \right) = s^2 n.$$

Agora, vamos usar a desigualdade de Cauchy-Schwarz (3). Se Δ é como em (7), para todo $1 \leq m \leq n-1$ temos

$$s^4 + o(n^4) \geq \frac{1}{n}(s^2 n)^2 + \frac{m^2 n^2}{n^2 - m^2},$$

ou seja,

$$\frac{m^2 n^2}{n^2 - m^2} \Delta^2 = o(n^4). \tag{8}$$

Definimos os conjuntos $M_\varepsilon = \{u_1, u_2 \in \mathbb{Z}_n \colon\ |\sum_x \chi(x+u_1)\chi(x+u_2) - s^2/n| \geq \varepsilon n\}$ e

$$M_\varepsilon^+ = \left\{u_1, u_2 \in \mathbb{Z}_n \colon\ \sum_x \chi(x+u_1)\chi(x+u_2) \geq s^2/n + \varepsilon n\right\}$$

Queremos provar que para todo $\varepsilon > 0$ e para todo $\delta > 0$ vale que $|M_\varepsilon| \leq \delta n$, para todo $n \geq n_0(\varepsilon, \delta)$. Suponhamos que não e que $|M_\varepsilon^+| > \delta n/2$. Se m é a cardinalidade de M_ε^+ então

$$\frac{m^2 n^2}{n^2 - m^2}\Delta^2 \geq \frac{\delta^2 n^4/4}{n^2}(\varepsilon n)^2 = \left(\frac{\delta\varepsilon}{2}\right)^2 n^4,$$

que contradiz (8). QED

Q(2) ⇒ WT: Temos, para quase todos u_1, $u_2 \in \mathbb{Z}_n$,

$$\frac{s^2}{n} + o(n) = \sum_{x \in \mathbb{Z}_n} \chi_S(x+u_1)\chi_S(x+u_2) = \sum_{y \in \mathbb{Z}_n} \chi_S(y)\chi_S(y+u_2-u_1) = |S \cap (S + u_2 - u_1)|.$$

QED

ST ⇒ R(2): Para quase todo $x \in \mathbb{Z}_n$

$$\frac{st}{n} + o(n) = \sum_{y \in \mathbb{Z}_n} \chi_S(y)\chi_T(y-x) = \sum_{y \in \mathbb{Z}_n} \chi_S(y)\chi_S(x-y),$$

fazendo $T = -S$. QED

$\mathbf{R(2)} \Rightarrow \mathbf{R(k)}$: Vamos provar por indução em k. Assumimos $\mathbf{R(2)}$. Então

$$\sum_x \left(\sum_{u_1+\cdots+u_k} \chi(u_1)\cdots\chi(u_k) \right)^2 =$$

$$\sum_x \left(\sum_{u_1+y=x} \chi(u_1) \sum_{u_2+\cdots+u_k} \chi(u_2)\cdots\chi(u_k) \right)^2 =$$

$$\sum_x \left(\sum_y \chi(x-y) \left(\frac{s^{k-1}}{n} + o(n^{k-2}) \right) + o(n^{k-1}) \right)^2 =$$

$$\sum_x \left(s^2 \left(\frac{s^{2k-2}}{n^2} + o(n^{2k-4}) \right) \right) + o(n^{2k-1}) =$$

$$\frac{s^{2k}}{n} + s^2 o(n^{2k-3}) + o(n^{2k-1}).$$

Agora,

$$\sum_x \sum_{u_1+\cdots+u_k=x} \chi(u_1)\cdots\chi(u_k) =$$

$$\sum_x \sum_{x_1} \cdots \sum_{u_{k-1}} \chi(u_1)\cdots\chi(u_{k-1})\chi(x-u_1-\cdots-u_{k-1}) =$$

$$s^k,$$

e usando Cauchy-Schwarz (3) como temos feito, para todo $m \in [n-1]$ vale que

$$\frac{s^{2k}}{n} + o(n^{2k-1}) \geq \frac{s^{2k}}{n} + \frac{mn}{n-m}\Delta^2,$$

ou seja,

$$\frac{m}{n-m}\Delta^2 = o(n^{2k-2}). \tag{9}$$

Queremos provar que para todo $\varepsilon > 0$ e para todo $\delta > 0$ vale que $|M_\varepsilon| \leq \delta n$, para todo $n \geq n_0(\varepsilon, \delta)$, onde

$$M_\varepsilon = \left\{ x \in \mathbb{Z}_n \colon \left| \sum_{u_1+\cdots+u_k=x} \prod_i \chi(u_i) - s^k/n \right| \geq \varepsilon n^{k-1} \right\}.$$

Definindo M_ε^+ da forma natural como temos feito, suponhamos que não e que $|M_\varepsilon^+| > \delta n/2$. Se m é a cardinalidade de M_ε^+ então

$$\frac{m}{n-m}\Delta^2 \geq \frac{\delta}{2}(\varepsilon n^{k-1})^2 = \frac{\delta\varepsilon^2}{2}n^{2k-2},$$

que contradiz (9). QED

$\mathbf{R(k)} \Rightarrow \mathbf{EXP}$: Seja $M = (m_{i,j})$ a matriz dada por $m_{i,j} = \chi_S(j-i)$. Então M é uma matriz *circulante*, isto é, fixada a i-ésima linha de M obtemos a linha $i+1$ por, para toda coluna j, $m_{j+1,i+1} = m_{i,j}$, ou seja, a linha $i+1$ é um deslocamento circular para a direita da linha i. Assim, M tem autovalores (veja [])

$$(1, \theta^l, \theta^{2l}, \ldots, \theta^{(n-1)l}),\ \theta = \exp\left(\frac{2\pi i}{n}\right),\ l \in \mathbb{Z}_n,$$

com autovetores

$$\lambda_l = \sum_{x\in\mathbb{Z}_n} \chi(x)\theta^{lx}.$$

Observe que do fato de M ser circulante, temos que $M \cdot M^T = M^T \cdot M$. O valor da k-ésima potência de M na linha i e coluna j é dado por

$$\begin{aligned}(M^k)_{i,j} = \sum_{v_1,\ldots,v_{k-1}} m_{i,v_1}m_{v_1,v_2}\cdots m_{v_{k-1},j} = \\ |\{v_1,\ldots,v_k \colon \chi(v_1-i) = \cdots = \chi(j-v_k) = 1\}| = \\ \sum_{u_1+\cdots+u_k=j-i} \chi(u_1)\cdots\chi(u_k),\end{aligned}$$

portanto, para quase todo $x = j-i \in \mathbb{Z}_n$ temos

$$(M^k)_{i,j} = \frac{s^k}{n} + o(n^k - 1).$$

Ponha $A = (M\cdot M^T)^k = M^k \cdot {M^T}^k$. Então,

$$A_{i,j} = \sum_l (M^k)_{i,l}({M^T}^k)_{l,j} \leq n\left(\frac{s^k}{n} + o(n^{k-1})\right)^2 + (n^{k-1})^2 o(n) = \frac{s^{2k}}{n} + o(n^{k-1}),$$

logo,

$$\mathrm{Tr}(A) = s^{2k} + o(n^{2k}) = \sum_{i=0}^{n-1} \lambda_i^{2k}.$$

Como $\lambda_0 = \sum_{x\in\mathbb{Z}_n} \chi(x) = s$ vale $\lambda_0^{2k} = s^{2k}$ donde concluímos que

$$\sum_{i=1}^{n-1} \lambda_i^{2k} = o(n^{2k}),$$

portanto,

$$\lambda_j = \sum_{x\in\mathbb{Z}_n} \chi(x) \exp\left(\frac{2\pi i j x}{n}\right) = o(n),$$

se $j \neq 0$. QED

EXP $\Rightarrow$ ST: Seja $T \subseteq \mathbb{Z}_n$ com cardinalidade $|T| = t$ fixo. Suponha $s, t > \delta n$ para algum $\delta > 0$ e ponha $\lambda = \max_{j\neq 0} |\lambda_j|$.

Considere o vetor característico

$$\overline{\chi_T} = \begin{pmatrix} \chi_T(0) \\ \vdots \\ \chi_T(n-1) \end{pmatrix}.$$

Então, a i-ésima linha do produto $M \cdot \overline{\chi_T}$ é a cardinalidade da intersecção $(S+i) \cap T$. Também $M \cdot \mathbf{1} = s1$.

Ponha $v_T(i) = \frac{1}{n-t}(-1 + \frac{n}{t}\chi_T(i))$. Então $\langle \mathbf{1}, \overline{v_T}\rangle = 0$. Portanto, se $\overline{\chi_T} = \alpha\mathbf{1} + \beta\overline{v_T}$ temos que

$$\overline{\chi_T} = \frac{t(n-t)}{n}\left(\frac{1}{n-t}\mathbf{1} + \overline{v_T}\right),$$

logo

$$M \cdot \overline{\chi_T} = \frac{st}{n}\mathbf{1} + \frac{t(n-t)}{n} M \cdot \overline{v_t}.$$

Suponha existir $\varepsilon > 0$ tal que

$$\sum_x \left| |S \cap (T+x)| - \frac{st}{n} \right| > 3\varepsilon st$$

e ponha

$$W = \left\{ y\colon \left| |S \cap (T+y)| - \frac{st}{n} \right| > \frac{\varepsilon st}{n} \right\}.$$

Observemos que $|W| = w > 2\varepsilon s$: caso contrário, $\sum_{y \in \mathbb{Z}_n} ||S \cap (T+y)| - st/n| \leq 3\varepsilon st$. Ponha

$$W' = \left\{ y \in W\colon |S \cap (T+y)| > \frac{1+\varepsilon}{n} st \right\},$$

e assuma que $|W'| = w' > \varepsilon s$. Assim,

$$\sum_{y \in W'} |S \cap (T+y)| > \frac{1+\varepsilon}{n} stw'.$$

Ponha $W'' = -W'$ e

$$\overline{\chi_{W''}} = \begin{pmatrix} \chi_{W''}(0) \\ \vdots \\ \chi_{W''}(n-1), \end{pmatrix} \qquad \text{e} \qquad \overline{v_{W''}} = \begin{pmatrix} v''_o \\ \vdots \\ v''_{n-1}, \end{pmatrix}$$

onde $v''_i = \frac{1}{n-w'}(-1 + \frac{n}{t}\chi_{W''}(i))$. Dessa forma,

$$\overline{\chi_{W''}} = \frac{w'(n-w')}{n} \left(\frac{1}{n-w'} \mathbf{1} + \overline{v_{W''}} \right).$$

Agora,

$$\langle \overline{\chi_{W''}}, M \cdot \overline{\chi_T} \rangle = \sum_i \chi_{W''}(i) \, |(S+i) \cap T| = \sum_{i \in W''} |(S+i) \cap T| = \sum_{y \in W'} |S \cap (T+y)|,$$

portanto,

$$\langle \overline{\chi_{W''}}, M \cdot \overline{\chi_T} \rangle > \frac{1+\varepsilon}{n} stw'. \tag{10}$$

Por outro lado,

$$\langle \frac{w'}{n}\mathbf{1} + \frac{w'(n-w')}{n}\overline{v_{w''}}, \frac{st}{n}\mathbf{1} + \frac{t(n-t)}{n} M \cdot \overline{v_T} \rangle = \frac{w'st}{n} + \frac{w'(n-w')t(n-t)}{n^2} \langle \overline{v_{W''}}, M \cdot \overline{v_T} \rangle \leq \frac{w'st}{n} + \frac{w'(n-w')t(n-t)}{n^2} \lambda ||\overline{v_{W''}}|| ||\overline{v_T}||.$$

Sabemos calcular $||\overline{v_T}||$

$$||\overline{v_T}|| = \left(\sum_{i=0}^{n-1}\left(\frac{1}{n-t}\left(-1+\frac{n}{t}\chi_T(i)\right)\right)^2\right)^{1/2} =$$
$$\left(\sum_{i\in T}\left(\frac{n-t}{t(n-t)}\right)^2 + \sum_{i\notin T}\frac{1}{(n-t)^2}\right)^{1/2} =$$
$$\left(\frac{1}{t}+\frac{1}{n-t}\right)^{1/2}.$$

Da mesma forma,

$$||\overline{v_{W''}}|| = \left(\frac{1}{w'}+\frac{1}{n-w'}\right)^{1/2}.$$

Assim, ficamos com

$$\langle \frac{w'}{n}\mathbf{1} + \frac{w'(n-w')}{n}\overline{v_{w''}}, \frac{st}{n}\mathbf{1} + \frac{t(n-t)}{n}M\cdot\overline{v_T}\rangle \leq$$
$$\frac{w'st}{n} + \frac{w'(n-w')t(n-t)}{n^2}o(n)\left(\frac{1}{t}+\frac{1}{n-t}\right)^{1/2}\left(\frac{1}{w'}+\frac{1}{n-w'}\right)^{1/2} =$$
$$\frac{w'st}{n} + \frac{(w'(n-w')t(n-t))^{1/2}}{n^2}o(n) =$$
$$\frac{w'st}{n} + o\left(\frac{w'st}{n}\right),$$

contradizendo (10) pois s, $t > \delta n$ e $w' > \varepsilon s$. QED

2.3 Demonstração do Lema 3

Graph $\Leftrightarrow$ $\mathbf{C(2t)}$: A prova de "$\Rightarrow$" é imediata. Para provar o outro lado, temos de $\mathbf{C(2t)}$

$$\mathbf{C(2t)} \Rightarrow \sum_{x_1,\ldots,x_{2t}} \chi(x_1+x_2)\chi(x_2+x_3)\cdots\chi(x_{2t}+x_1) = s^{2t} + o(n^{2t}).$$

Ainda, o número de cópias de C_{2t} em G_S é

$$\sum_{x_1,\ldots,x_{2t}} \chi(x_1+x_2)\chi(x_2+x_3)\cdots\chi(x_{2t}+x_1),$$

onde a soma são sobre as $2t$-uplas sem repetição, que é facilmente provado ser $\Theta(n^{2t})$. QED

Graph $\Leftrightarrow$ **Density**: De **Density** temos que para todo $T \subseteq \mathbb{Z}_n$

$$\sum_{x,y\in\mathbb{Z}_n} \chi_T(x)\chi_T(y)\chi_S(x+y) = \frac{st^2}{n} + o(n^2),$$

portanto, o número de arestas no grafo induzido por T é

$$\mathrm{e}(T) = \frac{1}{2}\sum_{x,y} \chi_T(x)\chi_T(y)\chi_S(x+y) = \frac{st^2}{2n} + o(n^2),$$

logo temos **Graph**.

Por outro lado, de **Graph** temos que para todo $T \subseteq \mathbb{Z}_n$ vale que

$$\mathrm{e}(T) = \frac{s}{2n}t^2 + o(n^2),$$

implicando que

$$\sum_{x,y} \chi_T(x)\chi_T(y)\chi_S(x+y) = \frac{st^2}{n} + o(n^2),$$

ou seja, **Density**. QED

GRAPH $\Leftrightarrow$ $\mathbf{Q(2)}$: De $\mathbf{Q(2)}$ temos que para quase todos u_1, $u_2 \in \mathbb{Z}_n$

$$\sum_{x\in\mathbb{Z}_n} \chi_S(x+u_1)\chi_S(x+u_2) = \frac{s^2}{n} + o(n) \Leftrightarrow$$
$$\left| |\Gamma(u_1)\cap\Gamma(u_2)| - \frac{s^2}{n} \right| = o(n) \leftrightarrow$$
$$\sum_{u_1,u_2} \left| |\Gamma(u_1)\cap\Gamma(u_2)| - \frac{s^2}{n} \right| = o(n^3) \Leftrightarrow \textbf{Graph}.$$

QED

Referências

[1] Béla Bollobás, *Random graphs*, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1985.

[2] F. R. K. Chung, R. L. Graham, and R. M. Wilson, *Quasi-random graphs*, Combinatorica **9** (1989), no. 4, 345–362.

[3] S. W. Graham and C. J. Ringrose, *Lower bounds for least quadratic nonresidues*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 269–309.

[4] Andrew Thomason, *Pseudorandom graphs*, Random graphs '85 (Poznań, 1985), North-Holland Math. Stud., vol. 144, North-Holland, Amsterdam, 1987, pp. 307–331.