Lecture 14 Expander Graphs & Sipser-Spielman Codes

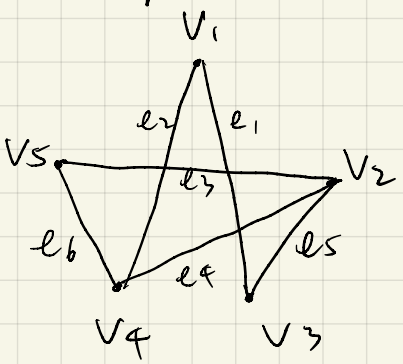
Basics of Graphs

Graph $G=(V,E)$ $|V|=n$, $|E|=e$

Adjacency Matrix $A \in \mathbb{F}_2^{n\times n}$ $A_{i,j}=1$ iff. $(v_i,v_j)\in E$.

Incidence Matrix $B \in \mathbb{F}_2^{n\times e}$ $B_{i,j}=1$ iff. v_i is a node of edge e_j.

Examples



$$A=\begin{bmatrix} 0&0&1&1&0\\ 0&0&1&1&1\\ 1&1&0&0&0\\ 1&1&0&0&1\\ 0&1&0&1&0 \end{bmatrix} \qquad B=\begin{bmatrix} 1&1&0&0&0&0\\ 0&0&1&1&1&0\\ 1&0&0&0&1&0\\ 0&1&0&1&0&1\\ 0&0&1&0&0&1 \end{bmatrix}$$

① $\operatorname{tr} A = 0$

② $\operatorname{tr} A^2 = 2e$

Eigenvalues of k-regular graphs.

$$k=\lambda_0(A)\geq\lambda_1(A)\geq\cdots\geq\lambda_{n-1}(A)\geq -k$$

① $\lambda_0(A)=k$: $A\,1_n = k\,1_n$

② $|\lambda_i(A)|\leq k$, $\forall\ i=0,\cdots,n-1$:

$$Ax=\lambda_i x, \quad |x_t|=\max_i |x_i|$$

$$|\lambda_i x_t| = \Big|\sum_{(v_t,v_j)\in E} x_j\Big| \leq \sum_{0\leq i<n,\ (v_t,v_j)\in E} |x_j| \leq k|x_t|$$

$\Rightarrow |\lambda_i|\leq k$. equality only holds for

③ Let $\Delta = \max_{|\lambda_i| \neq k} |\lambda_i|$, then

$\Delta \geq c\sqrt{k}$ $\quad n \to \infty, c \to 1$.

$tr(A^2) = kn$

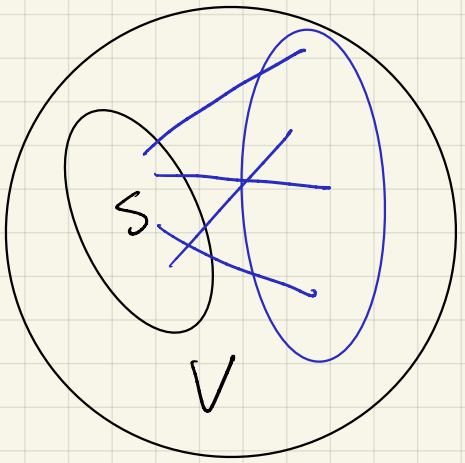
$tr(A^2) = \sum_{i=0}^{n-1} \lambda_i^2(A) \leq k^2 + (n-1)\Delta^2$ ↗ should.

$\Rightarrow \Delta \geq \sqrt{\frac{n-k}{n-1}} \cdot \sqrt{k}$.

Alon-Bopanna Theorem

$$\liminf_{n \to \infty} \lambda(X) \geq 2\sqrt{k-1}$$

Expander Graphs



$$h(G) = \min_{|S| \leq n/2} \frac{e(S, \bar{S})}{|S|} = \partial S$$

(d, ε) – expander graph:

① d-regular

② $h(G) \geq \varepsilon$.

③ $h(G) \leq d$

$$\frac{1}{2}(d - \lambda_2) \leq h(G) \leq \sqrt{2d(d-\lambda_2)}$$

① ↑

Smaller λ_2 leads to better expansion

Extreme (Optimal): $\lambda_2 \sim 2\sqrt{k-1}$. Ramanujan Graph.

① $\lambda_1(X) = \max_{\substack{x \neq 0 \\ x \perp 1_n}} \frac{|x^T A x|}{|x^T x|}$

Let $x_i = \begin{cases} n-|S|, & v_i \in S \\ -|S|, & v_i \in \bar{S} \end{cases} \Rightarrow x \perp 1_n$. ($|S| = s$)

$$x^T x = (n-s)^2 s + s^2 (n-s) = s(n-s)n$$

$$x^T A x = 2 \sum_{(v_i, v_j) \in E} x_i x_j = d \sum_{v_i \in V} x_i^2 - \sum_{(v_i, v_j) \in E} (x_i - x_j)^2$$

$$= d\, x^T x - e(S, \bar{S})\, n^2$$

$$\Rightarrow \lambda_1(X) \geq \frac{|x^T A x|}{|x^T x|} = d - \frac{n\, e(S, \bar{S})}{s(n-s)}$$

$$\Rightarrow \forall\, |S| \leq n/2, \quad \frac{e(S, \bar{S})}{|S|} \geq \frac{n-s}{n}(d - \lambda_1) \geq \frac{1}{2}(d - \lambda_1)$$

$$\Rightarrow h(G) \geq \frac{1}{2}(d - \lambda_1)$$

② Let $S = \gamma n$. $\gamma \leq 1/2$, then ① becomes

$$e(S, \bar{S}) \geq \frac{s(n-s)}{n}(d - \lambda_1)$$

$$= \gamma(1-\gamma)\, n (d - \lambda_1)$$

$$ds = 2e(S) + e(S, \bar{S})$$

$$\Rightarrow e(S) \leq \frac{d\gamma n}{2} - \frac{1}{2}\gamma(1-\gamma)\, n (d - \lambda_1)$$

$$= \frac{dn}{2}\left(\gamma - \gamma(1-\gamma) + \frac{\lambda_1}{d}\gamma(1-\gamma)\right)$$

$$= \frac{dn}{2}\left(\gamma^2 + \frac{\lambda_1}{d}\gamma(1-\gamma)\right).$$

Alon-Chung

$$\boxed{e(S) \leq \frac{dn}{2}\left(\gamma^2 + \frac{\lambda_1}{d}\gamma(1-\gamma)\right)}$$

(Expansion of Incidence graph)

Construction of Ramanujan Graph

Margulis

Lubotzky, Phillips, Sarnak.

$q(q^2-1)/2$ vertices

$(p+1)$-regular

$\lambda_2 \le 2\sqrt{p}$

Primes $p, q \equiv 1 \pmod 4$

Solution $u^2 \equiv -1 \pmod q$

Solutions (a,b,c,d), $a>0$, $2 \mid b,c,d$.

to $a^2+b^2+c^2+d^2 = p$.

↑ $p+1$ solution

$$S = \left\{ \begin{pmatrix} a+ub & c+ud \\ -c+ud & a-ub \end{pmatrix} \;\middle|\; \begin{matrix} a^2+b^2+c^2+d^2=p \\ a>0,\ 2 \nmid b,c,d \end{matrix} \right\}, \quad |S| = p+1$$

Cayley graph

$$X^{p,q} = \begin{cases} X(PGL_2(\mathbb{F}_q), S) & \left(\frac{p}{q}\right) = -1 \\ X(PSL_2(\mathbb{F}_q), S) & \left(\frac{p}{q}\right) = 1. \end{cases}$$

↑ $\exists x$ s.t. $p \equiv x^2 \bmod q$

Example

$p=5$, $q=13$, $\left(\frac{p}{q}\right) = -1$.

$u = 5$. $a^2+b^2+c^2+d^2 = 5$.

$(a,b,c,d) = (1,0,0,2), (1,0,2,0), (1,2,0,0)$

$(1,0,0,-2), (1,0,-2,0), (1,-2,0,0)$

$$S = \left\{ \begin{bmatrix} 1 & 10 \\ 10 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -10 \\ -10 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} 11 & 0 \\ 0 & -9 \end{bmatrix}, \begin{bmatrix} -9 & 0 \\ 0 & 11 \end{bmatrix} \right\}$$

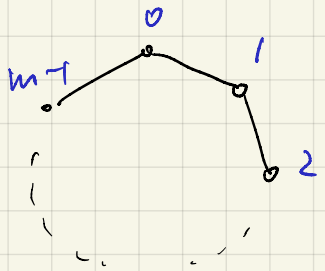
Cayley Graph

$X(G, S)$ G group, $S \subseteq G$.

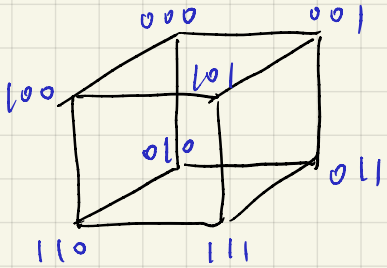
$g \in V$, $(g, gs) \in E$, $\forall\ g \in G, s \in S$

Examples

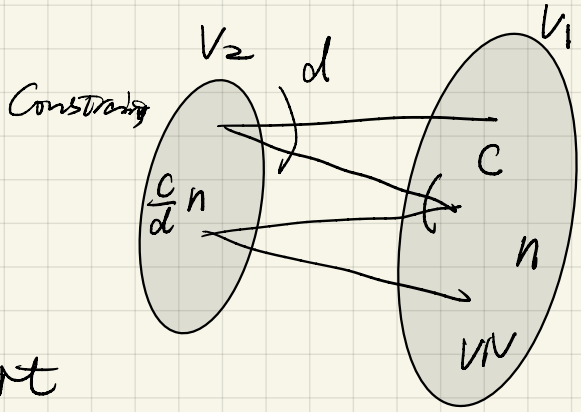
G: $\mathbb{Z}_m$. S: 1.



G: $\mathbb{F}_2^3$. S: $\{(001), (010), (100)\}$.



Sipser–Spielman Codes



$(c, d, \varepsilon, \delta)$–Expander

① bipartite

② c, d: degrees of each part

③ $\forall\ S \subseteq V_1$, $|S| \le \varepsilon n$, $|N(S)| > \delta |S|$

Construction 1:

① $B: (c, d, \alpha, \frac{c}{d\varepsilon})$– expander

② S: $[d, rd, \ge \varepsilon d]$ – code, $r > \frac{c-1}{c} d$

③ $C(B, S)$: neighborhood of each constraint form a codeword $\in S$.

$\Rightarrow$ $C(B,S)$: $[n, Rn, \geq \alpha n]$ - code.

Rate: $R > (cr-(c-1))$

Each constraint node $\rightarrow$ $< (1-r)d$ constraint.

Totally $< (1-r)d\left(\frac{c}{d}n\right) = c(1-r)n$ constraint.

$k > n - c(1-r)n = n[cr-(c-1)]$

$\Rightarrow R > cr-(c-1)$.

Distance: Any $S \subseteq V_1$ s.t. $|S| \leq \alpha n$, (d_{min} ↑)

$\Rightarrow c|S| = |\partial S| = \sum_{C \in N(S)} \deg(C) \geq \left(\min_{C \in N(S)} \deg(C)\right) \cdot N(S)$

$> d_{min} \cdot \frac{c}{d\varepsilon}|S|$.

$\Rightarrow d_{min} < d\varepsilon$.

$\Rightarrow$ Not a local code.

Example

① $S = \{(x_1 x_2 \cdots x_d) \mid \sum x_i = 0 \text{ on } \mathbb{F}_2\}$.

$\rightarrow$ LDPC code with Tanner graph B.

Constructions of B $\quad |V| = \frac{dn}{2} \quad |C| = n$.

Incidence Matrix of of d-regular graph with λ_2.

Incidence graph of d-regular G.

If $|V| = \frac{dn}{2}\left(\gamma^2 + \frac{\lambda_2}{d}\gamma(1-\gamma)\right)$, then $|N(V)| \geq \gamma n$.

Edges in G

$$\Rightarrow \max_{c \in N(v)} \deg \le \frac{dn\left(\gamma^2 + \frac{\lambda_2}{d}\gamma(1-\gamma)\right)}{\gamma n} = d\left(\gamma + \frac{\lambda_2}{d}(1-\gamma)\right)$$

If $d\left(\gamma + \frac{\lambda_2}{d}(1-\gamma)\right) < \varepsilon d$. $\Rightarrow$ Not a codeword

$$\Leftrightarrow \quad \gamma < \frac{\varepsilon - \frac{\lambda_2}{d}}{1-\frac{\lambda_2}{d}} = \gamma_0$$

relative weight $\ge \gamma_0^2 + \frac{\lambda_2}{d}\gamma_0(1-\gamma_0)$

$$\ge \gamma_0\left(\gamma_0 + \frac{\lambda_2}{d}(1-\gamma_0)\right)$$

$$= \left(\frac{\varepsilon - \frac{\lambda_2}{d}}{1-\frac{\lambda_2}{d}}\right)\cdot\left(\frac{\varepsilon - \frac{\lambda_2}{d}}{1-\frac{\lambda_2}{d}}\left(1-\frac{\lambda_2}{d}\right) + \frac{\lambda_2}{d}\right)$$

$$= \left(\frac{\varepsilon - \lambda_2/d}{1-\lambda_2/d}\right)\varepsilon.$$

Sequential Decoding

Flip an VN if it is in more unsatisfied constraints than satisfied constraints.

$$\begin{cases} B: (c, d, \alpha, 3c/4) - \text{Expander} \\ S: \left\{(x_i) \mid \sum x_i \equiv 0 \mod 2\right\}. \end{cases}$$

The Decoder can always decode $\le \alpha n/2$ errors.

Proof. $(V, u, s) \leftarrow$ # satisfied constrained.

$\uparrow$ $\quad\uparrow \longleftarrow$ # unsatisfied constraints

erroneous bits

① If $v \le \alpha n$, decoder can proceed

$$\begin{cases} u+s > (3c/4)v & \text{(Expansion)} \\ u+2s \le cv \end{cases}$$

$$\Rightarrow u > \frac{cv}{2} \Rightarrow \text{At least one node connects to } > \frac{c}{2} \text{ unsatisfied constraints}$$

② $v \le \alpha n$ is always satisfied

$u \le (\alpha n/2)c$ initially and strictly decreases through the decoding steps. From ①. $v \le \alpha n$.

Parallel Decoding.

Construction 1:

① $B : (c, d, \alpha, \frac{c}{d\varepsilon})$ - expander

② $S : [d, rd, \ge \varepsilon d]$ - code, $r > \frac{c-1}{c} d$

③ $C(B, S)$: neighborhood of each constraint form a codeword $\in S$.

① For each constraint, if the local view defers from a codeword in S by $\le \frac{d\varepsilon}{4}$ nodes $\longrightarrow$ send flip to the nodes

$\frac{1}{2}d\varepsilon$

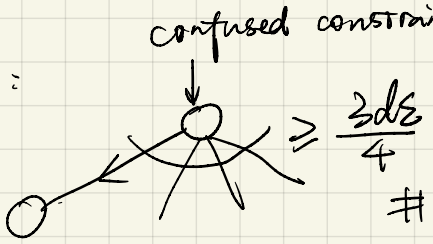
② Flip all nodes that receive ≥ 1 flip messages

The decoder transform an input of relative distance α to an output of relative distance $\alpha\left(\frac{2}{3} + \frac{16\alpha}{\varepsilon^2} + \frac{4\lambda}{d\varepsilon}\right)$

Proof: Difference from the output to a codeword

} nodes flipped but are not erroneous N_1

nodes unflipped but are erroneous. N_2

N_1: 

$(1-\delta)\,d\varepsilon$

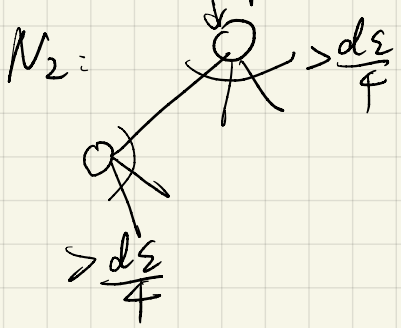
$$\#\text{ confused constraints} \leq \frac{2\cdot\frac{\alpha dn}{2}}{(1-\delta)\frac{3d\varepsilon}{4}} = \frac{4\alpha n}{3\varepsilon}$$

$\frac{\alpha n}{(1-\delta)\varepsilon}\cdot\delta d\varepsilon$

$N_1 \leq \#$ flips sent from confused constraints

$$\leq \frac{4\alpha n}{3\varepsilon}\cdot\frac{d\varepsilon}{4} = \frac{dn}{2}\cdot\frac{2\alpha}{3}$$

$\frac{dn}{2}\cdot\left(\frac{2\delta}{1-\delta}\alpha\right)$

N_2: 

$$\#\text{ unhelpful constraints} \leq \frac{2\cdot\frac{\alpha dn}{2}}{\frac{d\varepsilon}{4}} = \frac{4\alpha n}{\varepsilon}$$

$\delta d\varepsilon$

$\frac{\alpha n}{\delta\varepsilon}$

$\Downarrow$ expansion

$$N_2 \leq \frac{dn}{2}\left(\left(\frac{4\alpha}{\varepsilon}\right)^2 + \frac{\lambda}{d}\left(\frac{4\alpha}{\varepsilon}\right)\right)$$

$\left(\frac{\alpha}{\delta\varepsilon}\right)^2 + \frac{\lambda}{d}\left(\frac{\alpha}{\delta\varepsilon}\right)$

$\Rightarrow$ output relative distance

$$\leq \frac{N_1+N_2}{dn/2} \leq \frac{2\alpha}{3} + \left(\frac{4\alpha}{\varepsilon}\right)^2 + \frac{\lambda}{d}\left(\frac{4\alpha}{\varepsilon}\right)$$

$\frac{2\delta}{1-\delta}\alpha + \left(\frac{\alpha}{\delta\varepsilon}\right)^2 + \frac{\lambda}{d}\left(\frac{\alpha}{\delta\varepsilon}\right)$

$$= \alpha\left(\frac{2}{3} + \frac{16\alpha}{\varepsilon^2} + \frac{4\lambda}{d\varepsilon}\right) = \beta$$

$\alpha\left(\frac{2\delta}{1-\delta} + \frac{\alpha}{\delta^2\varepsilon^2} + \frac{\lambda}{\delta d\varepsilon}\right)$

If $\frac{2}{3} + \frac{16\alpha}{\varepsilon^2} + \frac{4\lambda}{d\varepsilon} < 1 \Leftarrow \alpha < \left(\frac{1}{3} - \frac{4\lambda}{d\varepsilon}\right)\frac{\varepsilon^2}{16}$

$\beta < 1$

$2\sqrt{d-1}$, if $\alpha < \frac{\varepsilon^2}{48}$, always exists such d.

After $\leq \log_{1/\beta} \alpha n$ rounds, decoder succeeds.

$$\alpha < \delta^2\varepsilon^2\left(\frac{1-3\delta}{1-\delta} - \frac{\lambda}{\delta d\varepsilon}\right)$$