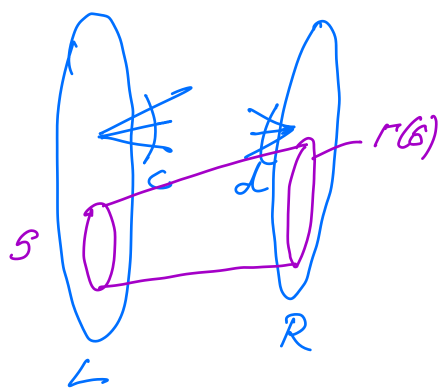
Today
- Expander Codes

CS5.318.1
Coding Theory
Lecture 13 (2022-10-12)
Instructor: Prahladh Harsha.

Expander Codes

$G = (L, R, E)$.



$|L| = n$ (variables)

$|R| = m$ (constraints)

(c,d)-degree bounded
left degree $\le c$
right degree $\le d$.

(c,d)-regular.

Neighborhoods $(S \subseteq L)$

$\Gamma(S) = \{ j \in R \mid \exists i \in S, (i,j) \in E \}$

$\Gamma^{odd}(S) = \{ j \in R \mid |\Gamma(j) \cap S| = \text{odd} \}$,

$\Gamma^{+}(S) = \{ j \in R \mid |\Gamma(j) \cap S| = 1 \}$.

Given graph $G = (L, R, E)$. defined the

$$\mathcal{C}(G) = \{ x \in \{0,1\}^n \mid \forall j \in R, \sum_{i \in \Gamma(j)} x_i = 0 \pmod 2 \}$$

Fact: $\mathrm{Dim}(\mathcal{C}(G)) \geq n - m$

$$= n - \frac{cn}{d} = n\left(1 - \frac{c}{d}\right)$$

$cn = dm$ if (c,d)-regular

$\mathrm{Rate}(\mathcal{C}(G)) \geq 1 - \frac{c}{d}.$

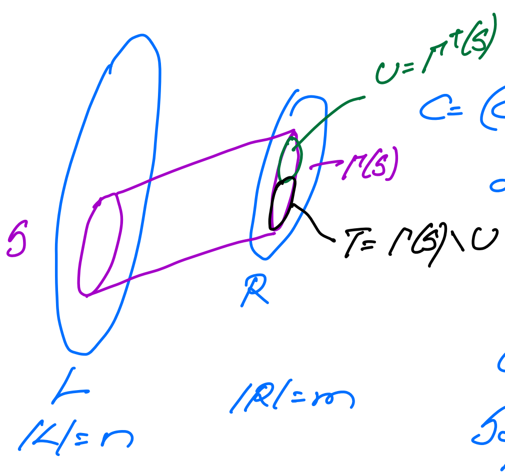
G is (δ, A)-expander if

$\forall S \subseteq L, \quad |S| \leq \delta n \Rightarrow |\Gamma(S)| \geq A|S|.$

Lemma: [Sipser-Spielman] If $G = (L, R, E)$ is a (c,d)-regular bipartite graph that is a (δ, A)-expander for some $A > c/2$, then

$$\delta(\mathcal{C}(G)) > \delta.$$

Proof:



$c = (c_1, c_2 \ldots c_n) \in \mathcal{C}(G)$ be a non-zero codeword of min weight.

Claim: $wt(c) > \delta n$

Suppose not, i.e. $wt(c) < \delta n$

$S = \{i \in L \mid c_i = 1\}$

By expansion

$$|U| + |T| \geq A \cdot |S|$$

$$|U| + 2|T| \leq c|S|$$

Hence, $|U| \geq (2A - c)|S|$

> 0 if $2A > c$.

Every constraint in $U = \Gamma^+(S)$ is a violated constraint

$\Rightarrow\Leftarrow$ c is a codeword.

Hence, $wt(c) > \delta n$. $\boxtimes$

Cor: G is (c,d)-regular $(\delta, c(1-\varepsilon))$ for some $\varepsilon \in (0, 1/2)$, then

$$\delta(\mathcal{C}(G)) > \delta.$$

Distance is even better.

Claim: $\delta(\mathcal{C}(G)) \geq 2\delta(1-\varepsilon)$

Pf: c - min wt non-zero codeword.

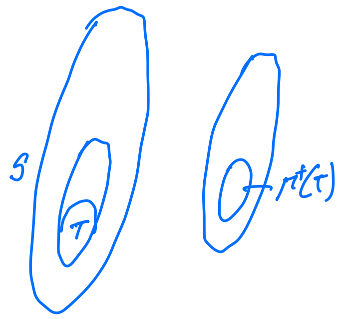
$S = \{ i \in L \mid c_i = 1 \}$.

From before, $|S| > \delta n$

Suppose $|S| < 2\delta(1-\varepsilon) n$. for contradiction.

We have $\delta n < |S| < 2\delta(1-\varepsilon)n$.

Fix any subset $T \subseteq S$, st $|T| = \delta n$.



$$|\Gamma^{odd}(S)| \geq |\Gamma^+(S)|$$
$$\geq |\Gamma^+(T)| - |\Gamma(S \setminus T)|$$
$$\geq (c(1-2\varepsilon)\delta n)$$
$$- c\,|S \setminus T|$$
$$> (c(1-2\varepsilon)\delta n) - c(\delta(1-2\varepsilon))n$$
$$= 0$$

$\boxtimes$

—

Qn: Do such bipartite expanders w/ expansion as large as $c(1-\varepsilon)$ for $\varepsilon \in (0, \frac{1}{2})$ exist?

Probabilistic Construction.

Thm: $\forall\, c \geq 3$, $d \geq 1$, $\varepsilon \geq \frac{\log(d/c)}{c}$, & sufficiently large n.

there exist a (c,d)-regular bipartite graph $G = (L, R, E)$ satisfying

- $|L| = n$; $|R| = m = cn/d$.
- $\left(\frac{\varepsilon}{d}, c(1-\varepsilon)\right)$-expander.

At the time of Sipser-Spielman's work in 94 explicit construction of expanders w/ expansion $> c/2$ were not known.

[2002] Capalbo-Reingold-Vadhan-Wigderson gave explicit construction of lop-sided bipartite expanders w/ expansion $A = c(1-\varepsilon)$ for small ε.

$\left(\frac{\varepsilon^2}{d_r}, c(1-\varepsilon)\right)$-expanders

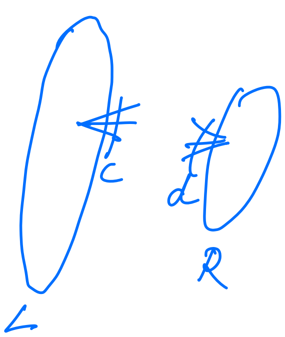
Can bipartite expanders w/ expansion $< c/2$ yield "good" codes?

YES, using Tanner's construction of graph based codes [Sipser-Spielman].

Tanner Code:

Ingredients: ① $G = (L, R, E)$ (c,d)-regular

② C_0 - $[d, R_0 d, \delta_0 d]_2$-code.



$\mathcal{C}(G, C_0)$

$= \{x \in \{0,1\}^L \mid \forall j \in R,\ x|_{\Gamma(j)} \in C_0\}$.

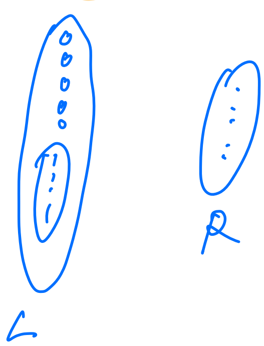
Sipser-Spielman:
Expansion lets you lift the "good" properties of constant-sized code C_0 to the large code $\mathcal{C}(G, C_0)$.

Rate of $\mathcal{C}(G, C_0)$:

$$\dim(\mathcal{C}(G,C_0)) \geq n - m[d(1-R_0)]$$
$$= n - \frac{cn}{d}[d(1-R_0)]$$
$$= n[1 - c(1-R_0)]$$
$$= n[cR_0 - (c-1)].$$

As long as $R_0 > \frac{c-1}{c}$, the $R > cR_0 - (c-1)$.

Distance of $\mathcal{C}(G, C_0)$:



Let $c \in \{0,1\}^n$ be a min wt non-zero codeword of $\mathcal{C}(G, C_0)$.

$S = \{i \in L \mid z_i = 1\}$

$\Delta = \delta_0 d$ (distance of C_0).

$U_\Delta = \{j \in R \mid |\Gamma(j) \cap S| < \Delta\}$.

$T_\Delta = \Gamma(S) \setminus U_\Delta$

$$|U_\Delta| + |T_\Delta| \geq A \cdot |S| \quad \text{(by expansion)}$$

$$|U_\Delta| + \Delta |T_\Delta| \leq c|S| \quad \text{(by counting edges)}$$

Hence, $|U| \geq (\Delta A - c)|S|$

> 0 if $A > \frac{c}{\Delta}$

$= \frac{c}{\delta_0 d}$.

As long as we chose C_0 such that:

$[d, R_0 d, \delta_0 d]_2$-code.

- $R_0 > \frac{c-1}{c}$.
- $\delta_0 > c/d$.

the "lifted" Tanner code has rate, distance

$R > cR_0 - (c-1)$.

$\delta > \delta$ (upto expansion factor)

An alternate (non-bipartite description) of the above Tanner lift is the following [Sipser-Spielman].

Let $G = (V, E)$ (not-bipartite) be a

d-regular.

λ-spectral expander.

C Normalized adjacency matrix.

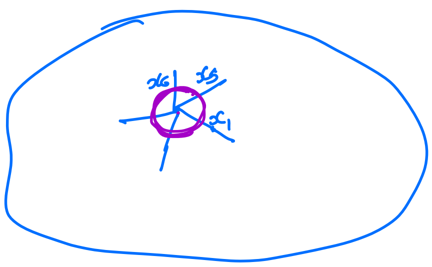
$$1 = \lambda_1 \geq \lambda_2 \dots \geq \lambda_n \geq -1$$

$$\max\{\lambda_2, |\lambda_n|\} \leq \lambda$$

& C_0 - $[d, R_0 d, \delta_0 d]_2$ - code.

$$R_0 > 1/2$$
$$\delta_0 > \lambda$$

then $\mathcal{C}(G, C_0) = \{x \in \{0,1\}^E \mid \forall v \in V,\ x|_{N(v)} \in C_0\}$



then

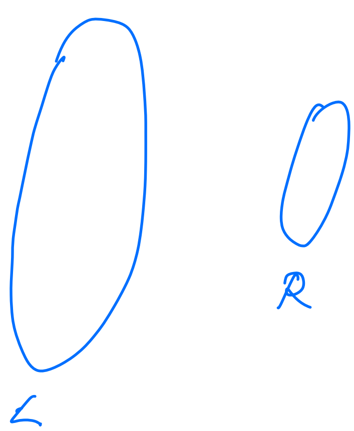
$\mathcal{C}(G, C_0)$ has

rate $R \geq 2R_0 - 1$

distance $\delta_0(\delta_0 - \lambda)$.

$\boxtimes$

Linear-time Decoding Algorithm for Expander Codes



$G = (L, R, E)$

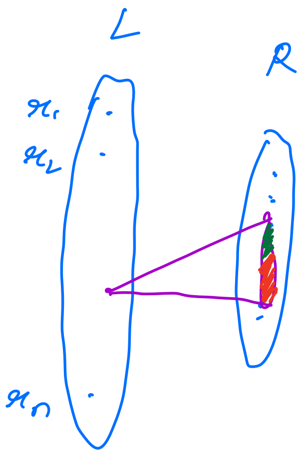
(c, d)-regular.

$(\delta, c(1-\varepsilon))$ - expander for some $\varepsilon \in (0, 1/4)$

Thm [SS] $\mathcal{C}(G)$ is linear time uniquely decodable if # errors $< \delta(1-2\varepsilon)n$.

(Recall $\delta(\mathcal{C}(G)) \geq 2\delta(1-\varepsilon)$

For small ε, this is decoding all the way to nearly half the known bound on distance of code.



Decoder:

Input: $x = (x_1, \ldots x_n)$ of promise

$$\delta(x, \mathcal{C}(G)) < \delta(1-\varepsilon)$$

① Initialization phase:

$k \leftarrow 0$

$x^{(k)} \leftarrow x$

Label vertices in R as sat/unsat depending on whether the constraint is satisfied

② While $\exists\, i \in L$, s.t. $UNSAT_i > SAT_i$

$x_i^{(k+1)} \leftarrow 1 - x_i^{(k)}$

$x_{i'}^{(k+1)} \leftarrow x_{i'}^{(k)}$ for all $i' \neq i$

$k \leftarrow k+1$

③ Output $x^{(k)}$.

Analysis : Let $c \in \mathcal{C}(G)$ be the unique codeword st

$$\delta(x, c) < \delta(1-2\varepsilon)n$$

$$S^{(k)} = \{ i \in L \mid x_i^{(k)} \neq c_i \}$$
$$|S^{(0)}| < \delta(1-2\varepsilon)n$$

Claim 1: If $\varepsilon \in (0, 1/4)$ & $0 < |S^{(k)}| \leq \delta n$, then $\exists\, i \in L$, st $|UNSAT_i| > |SAT_i|$

Pf: Observe that all unique neighbours of $S^{(k)}$ are unsatisfied at k-th iteration

$$|UNSAT^{(k)}| \geq c(1-2\varepsilon) \cdot |S^{(k)}|$$
$$> \frac{c}{2} |S^{(k)}| \quad \text{if } \varepsilon < 1/4.$$

Hence, $\exists\, i \in S^{(k)}$ st $|UNSAT_i^{(k)}| > \frac{c}{2}$

deg $= c$.

Hence $|UNSAT_i^{(k)}| > |SAT_i^{(k)}|$.

Claim 2: $|S^{(0)}| < \delta(1-2\varepsilon)n \Rightarrow |S^{(k)}| < \delta n$.

Pf: Obs: ① # unsat right constraints is always decreasing

② $|S^{(k)} - S^{(k+1)}| = 1$

$$|UNSAT^{(0)}| \leq |\Gamma(S^{(0)})| \leq c\,|S^{(0)}| < c\,\delta\,(1-2\varepsilon)\,n$$

Suppose for contradiction there exist a k', s.t. $|S^{(k')}| \geq \delta n$.

By ② $\exists\, k$, $|S^{(k)}| = \delta n$

$$|UNSAT^{(k)}| \geq |\Gamma^{+}(S^{(k)})| \geq \delta n \cdot c\,(1-2\varepsilon)$$

contradiction to (1).

Hence done $\boxtimes$.