Today

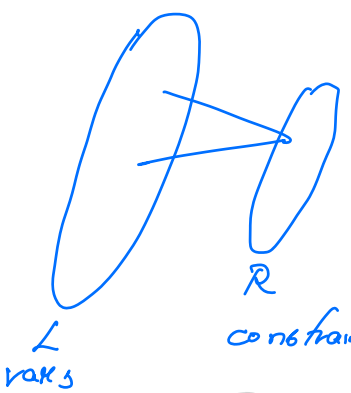
- Expander-based codes
  - * Sipser-Spielman
  - * Distance Amplification

CSS.318.1
Coding Theory
Lecture (2022-10-17)
Instructor: Prahladh Harsha.

Expander Codes (Sipser-Spielman)

Linear-time unique decoding of expander codes

① Codes based on unique-expanders



$G = (L, R, E)$, $|L| = n$; $|R| = m$

(c, d)-regular

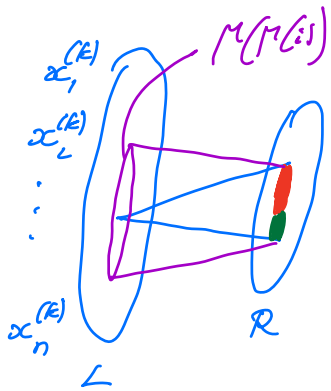
$(\delta, c(1-\varepsilon))$ expander for some $\varepsilon \in (0, 1/2)$

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

Thm [Sipser-Spielman]

① $\varepsilon \in (0, 1/2) \Rightarrow \delta(C(G)) \geq 2\delta(1-\varepsilon)$

② $\varepsilon \in (0, 1/4) \Rightarrow C(G)$ is linear-time decodable from $\delta(1-2\varepsilon)n$ errors.



Linear-time Decoder

Input: $x = (x_1 \dots x_n) \in \{0,1\}^n$

w/ promise $\delta(x, C(G)) < \delta(1-2\varepsilon)$.

Algorithm

I. Initialization Phase

$k \leftarrow 0$

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

For each $j \in R$

if $\sum_{i \in \Gamma(j)} x_i = 0$, label j as 'sat'

else label j as 'unsat'

For each $i \in L$

$SAT_i^{(k)} = \{j \in \Gamma(i) \mid j \text{ labeled sat}\}$

$UNSAT_i^{(k)} = \{j \in \Gamma(i) \mid j \text{ labeled unsat}\}$

Maintain list Q of vars s.t $|UNSAT_i| > |SAT_i|$

II While $\exists i \in L$, s.t $|UNSAT_i^{(k)}| > |SAT_i^{(k)}|$

$k \leftarrow k+1$

$$x_{i'}^{(k)} = \begin{cases} x_{i'}^{(k-1)} & \text{if } i' \neq i \\ 1 - x_{i'}^{(k-1)} & \text{if } i' = i \end{cases}$$

Update $SAT_{i'}^{(k)}$, $UNSAT_{i'}^{(k)}$ for all $i' \in L$ s.t $\Delta(i,i') \leq 2$.

Update list Q.

III Return $x^{(k)}$.

$SAT^{(k)} = \bigcup_{i \in L} SAT_i^{(k)}$; similarly $UNSAT^{(k)}$

Since $\delta(1-2\varepsilon) < \frac{1}{2} 2\delta(1-\varepsilon)$, there is atmost one $c \in C(G)$ s.t $\delta(x, C(G)) < \delta(1-2\varepsilon)$.

$$S^{(k)} = \{ c \in L / x_i^{(k)} \neq c_i \}$$

Claim 0: (i) $0 \leq |S^{(0)}| < \delta(1-2\varepsilon)n$

$\forall k, \quad |S^{(k)} - S^{(k-1)}| = 1$

(ii) $0 \leq |UNSAT^{(k+1)}| < |UNSAT^{(k)}| \ldots |UNSAT^{(0)}| \leq m$

Claim 1: If $\varepsilon \in (0, 1/4)$ & $0 < |S^{(k)}| < \delta n$

$\Downarrow$

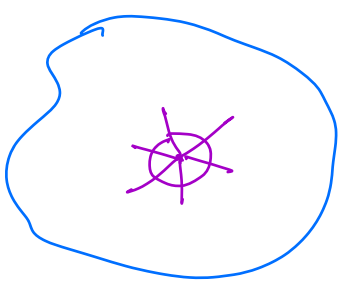
$\exists i \in L$ such that $|UNSAT_i^{(k)}| > |SAT_i^{(k)}|$

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

(Proofs from last lecture)

(2) Codes based on expanders

(not necessarily unique-expanders)



$G = (V, E)$

d- regular

λ-spectral expander.

(ie, $1 = \lambda_1 \geq \lambda \geq \lambda_2 \ldots \geq \lambda_n \geq -\lambda \geq -1$

where $\lambda_1 \ldots \lambda_n$ are eigen values of normalized adj matrix.

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

(w.l.) $R_0 > 1/2$. $\delta_0 > \lambda$

$$C(G, C_0) = \{x \in \{0,1\}^E \mid \forall v \in V,\ (x_e)_{e \ni i} \in C_0\}$$

Thm [Sipser-Spielman]

$$R(C(G, C_0)) \geq 2R_0 - 1$$
$$\delta(C(G, C_0)) \geq \delta_0(\delta_0 - \lambda)$$

Informally, the expanders 'lifts' the goodness of constant-size code to large code.

Expander Mixing Lemma

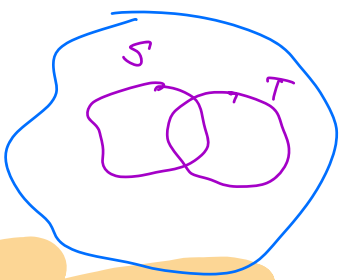
$G = (V, E)$ - graph

λ - spectral expander

$\forall S, T \subseteq V$

$$\left| \Pr_{\substack{e \sim_R V \\ e \sim_R i}} [(e, j) \in S \times T] - \mu(S)\mu(T) \right| < \lambda \sqrt{\mu(S)\mu(T)(1-\mu(S))(1-\mu(T))}$$

where $\mu(S) = |S|/n$.



What about decoding complexity of these expander-codes?

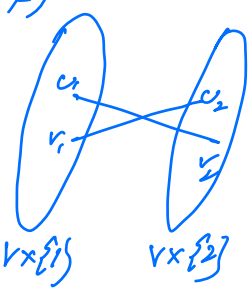
[Sipser-Spielman] linear time decoding, if # errors $< \frac{\delta_0^2}{48} n$

[Zemor] (slight variant of above construction)
linear time decoding of # errors $< \frac{\delta_0^2 n}{4}$

Double-Cover of a graph:

$G = (V, E)$

Double-cover is a bipartite graph (L, R, F)



a) $L = V \times \{1\}$

$R = V \times \{2\}$

$\forall (u,v) \in E$

$((u,1),(v,2)) \in F$

$((v,1),(u,2)) \in F$

Zemor's Construction:

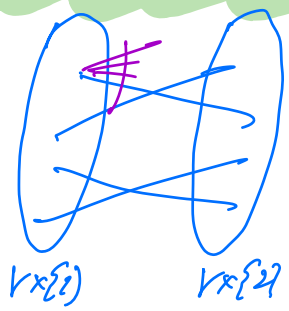
$G = (V, E)$ - λ-spectral expander, d-regular

$C_0 = [d, R_0 d, \delta_0 d]_2$ - code a) $R_0 > 1/2$

$\delta_0 > \lambda$

$Z(G, C_0) = C(H, C_0)$ where H is double-cover of G.

Thm: $R(Z(G,C_0)) \geq 2R_0 - 1$; $\delta(Z(G,C_0)) \geq \delta_0(\delta_0 - \lambda)$



Left-phase

$\forall v \in L$, modify $(xc)|_{E \sim v}$ to the closest codeword $c \in C_0$ that minimizes $\Delta((xc)|_{E \sim v}, c)$.

Right-phase: Defined similarly.

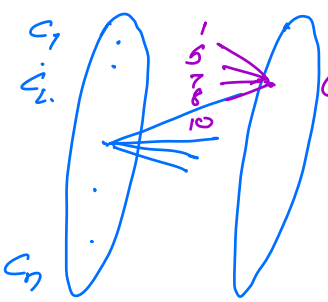
Formal Decoder

For $A \log |V|$ times (A - large universal const)
{ Run left-phase
  right phase

Output word.

Distance-Amplification

Two constructions using bipartite expanders
- Alon, Bruck, Naor, Naor, Roth [ABNNR]
- Alon, Edmonds, Luby [AEL]



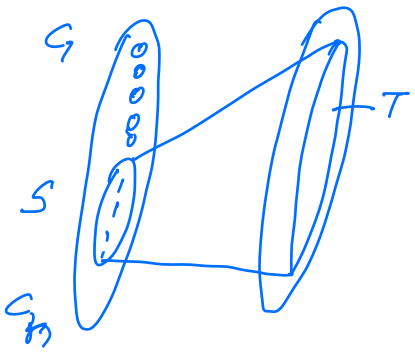
$G = ([n], [n], E)$
λ-spectral expander, d-regular

C - $[n, Rn, \delta n]_2$-code

$ABNRR(G, C)$
$= \{ x \in (\{0,1\}^d)^n \mid \exists\, c = (c_1, \ldots, c_n) \in C$
$s.t.\ (x_j)_i = c_{\Gamma_i(j)} \}$

- Rate of ABNNR code: R/d.

Distance of ABNNR code:



$c \in C$ be a non-zero codeword

$S = \{i : c_i \neq 0\}$

$|S| \geq \delta n$ (distance of C)

Dispersor Property: (δ, β)-disperser

If every set $S \subseteq [n]$, $|S| \geq \delta n$ satisfies $|\Gamma(S)| \geq \beta n$

G is (δ, β)-disperser & C is $(n, Rn, \delta n)_2$-code

$\Downarrow$

$ABNNR(G, C)$ is a $[n, Rn/d, \beta n]_{2^d}$-code.

$T = \Gamma(S)$; $|T| = \beta n$

Apply Expander mixing Lemma to $S \times T$

$$\left| \Pr_{\substack{c \sim_R L \\ j \sim_R i}} [(c_j) \in S \times T] - \mu(S) \cdot \mu(T) \right| < \lambda$$

$$|\delta - \delta \cdot \rho| < \lambda$$

$$(1 - \rho) < \lambda / \delta$$

$\Rightarrow$ Distance of ABNNR code $\geq 1 - \lambda/\delta$

Thm: If G is a λ-spectral expander & $\lambda < \delta$.

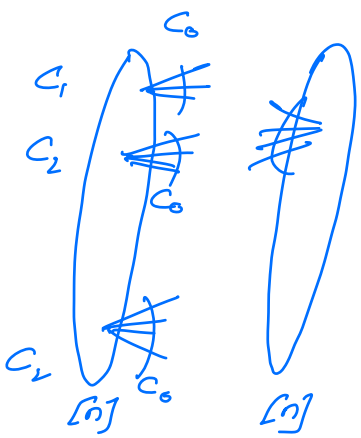
then $\delta(ABNNR(G,C)) \geq 1-\lambda/\delta$.

Alon-Edmonds-Luby Modification

ABNNR Construction.

- Code concatenation of C w/ $Rep^{(d)}$ to move from vertices to edges
- Use a better code than $Rep^{(d)}$

$C_0 : \quad \to \Sigma$



G - d-regular
λ-spectral expander

C - $[n, R_0 n, \delta_0 n]_{2^\alpha}$-code. $\quad q=\{0,1\}^\alpha$

$C_0 : \{0,1\}^\alpha \to \{0,1\}^d \quad (\alpha = R_0 d)$

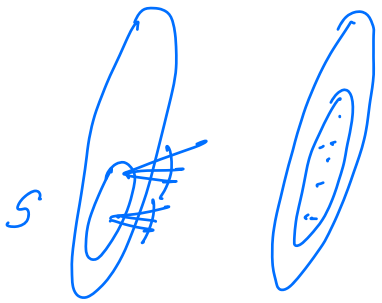
$(d, R_0 d, \delta_0 d)_2$-code.

$$AEL(G, C, C_0) = \{x \in (\{0,1\}^d)^n \mid \ldots\}$$

Rate: RR_0

Distance: Thm [AEL] $\delta(AEL) \geq \delta_0 - \lambda/\delta$

Pf:



$c \in C$ be a nonzero codeword

c' be the corresponding AEL codeword.

$S = \{i \in [n] \mid c_i \neq \bar{0}\}$

$T = \{j \in [n] \mid c'_j \neq \bar{0}\}$

$|S| = \delta n; \quad |T| = \rho n$

$|\delta\delta_0 - \delta\rho| < \lambda$

$\Rightarrow (\delta_0 - \rho) < \lambda/\delta$

$\boxtimes$