A $\qquad\qquad\qquad\qquad$ B

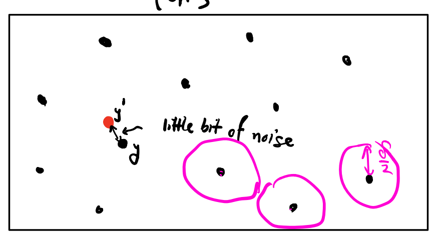
$x \in \{0,1\}^k \xrightarrow{\cancel{\text{noise}}} x + err \in \{0,1\}^k$

$y = \underline{E}(x) \in \{0,1\}^n \xrightarrow{\text{noise}} y' = y + \underset{\sim}{err} \in \{0,1\}^n$

$\Downarrow$ decode

y

$\{0,1\}^n$



$dist(x,y) = \frac{1}{n} \# \{ i \mid x_i \neq y_i \}$

An encoding $E : \{0,1\}^k \to \{0,1\}^n$ has distance δ

$\forall \; x, y \in \{0,1\}^k \quad x \neq y \qquad dist\big(E(x), E(y)\big) \geq \delta$

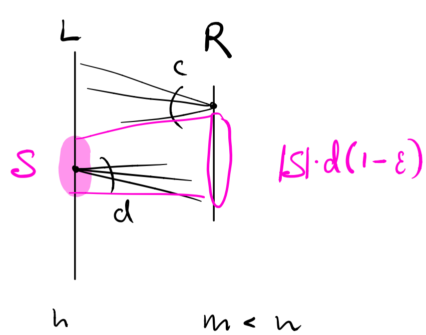
$C = Im(E)$

Rate of C is $r = \frac{\dim(C)}{n}$

tradeoff $\quad \delta$ vs $r \qquad r + h(\frac{\delta}{2}) \leq 1$

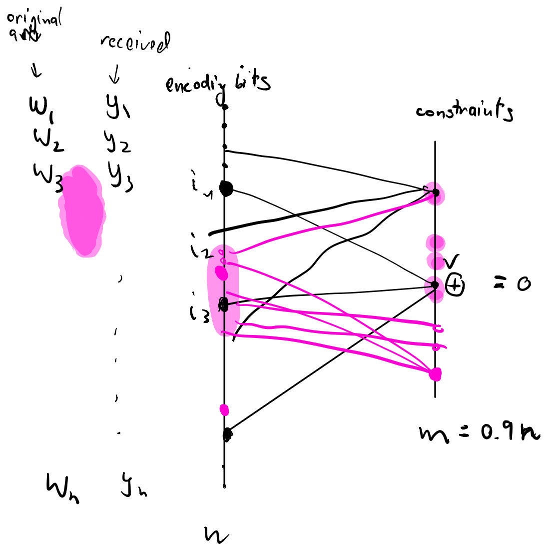
<u>ECCs from expanders</u> $\quad$ (Sipser & Spielman)

1. <u>unique nbr</u> expanders
2. Tanner code (based on spectral expanders)



A bip. graph is an excellent expander $\forall \, S \subseteq L \quad |S| \leq \gamma n$

$|\underbrace{\Gamma(S)}_{\text{nbrs of } S}| \geq d \cdot |S| \cdot (1 - \varepsilon)$



$$C = \left\{ y \in \{0,1\}^n \;\middle|\; \forall v \in R \quad \bigoplus_{i \sim v} y_i = 0 \right\}$$

Claim: C has const rate, const dist. & decodable

$\dim C \geq n - m \rightarrow$ rate ✓

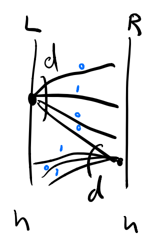
$\text{dist}\, C \geq \gamma$

$$\forall\, x \neq y \in C \quad \left|\{ i \mid x_i \neq y_i \}\right| \geq \gamma n$$

Tanner Codes

Let G be an $(n, d, \overset{\text{normalized}}{\lambda})$ - graph.

$$G' = (\overbrace{L \cup R}^{V}, E)$$



Let G' be double cover

Let $C_0 \subseteq \{0,1\}^d$ $\quad r_0 > \frac{1}{2} + \varepsilon$

$\dim C_0 = r_0 \cdot d$ $\quad \delta_0 > 3\lambda$

Define

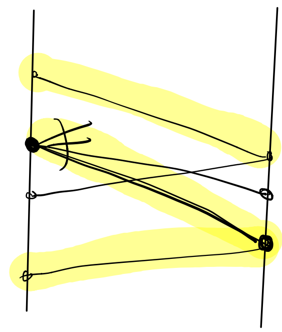
$$C = \left\{ y \in \{0,1\}^E \;\middle|\; \forall v \in V \quad y|_{\underbrace{\Gamma(v)}_{\text{edges touching } v}} \in C_0 \right\}$$

rate: count constraints. $2nd(1 - r_0)$ $\quad n \cdot d$

rate $\geq \frac{1}{nd}\left(nd - nd(2(1-r_0))\right) \geq 2\varepsilon$

dist:

all left verts touching F — T



S - right vertices touching F

$x - y \neq 0$ $\quad x \neq y \in C$

$F = \{ e \in E \mid x_e \neq y_e \}$

Every vertex touching F must touch $\geq \delta_0 \cdot d$ edges of F.

EML: $\left| E(S,T) - d|S| \cdot \frac{|T|}{n} \right| \leq \lambda d \sqrt{|S| \cdot |T|}$

$$\sqrt{|S| \cdot |T|} \cdot \delta_0 \cdot d \leq |F| \leq E(S,T) \leq \frac{d}{n} |S| \cdot |T| + \lambda d \sqrt{|S|\,|T|}$$

$$\Rightarrow \quad n \cdot \delta_0 \cdot (\delta_0 - \lambda) \leq |F|$$

$$\text{dist}(C) \geq \delta_0 \cdot (\delta_0 - \lambda)$$

---

input $y \in \{0,1\}^E$ $\quad w$ - closest codeword.

Assume $\text{dist}(y, w) \leq (1-\varepsilon) \frac{\delta_0}{2} \cdot \left(\frac{\delta_0}{2} - \lambda \right)$.

Let $F = \{ e \in E \mid y_e \neq w_e \}$

$S_1 = \{ v \in L \mid v \text{ sees an error after the first left-decoding} \}$

each $v \in S_1$ has $\geq \frac{\delta_0 d}{2}$ nbrs in F.

1. Claim: $|S_1| \leq (1-\varepsilon)\left(\frac{\delta_0}{2} - \lambda \right) \cdot n$

2. claim: Let $T_1 = \{ v \in R \mid v \text{ sees an error after the first right-decoding} \}$

$$|T_1| \leq \frac{|S_1|}{1+\varepsilon}$$

3. Let $S \subseteq \{0,1\}^k$ $|S| = n$.

Prove that the following are equivalent

1. Let A be the n-by-k matrix whose <u>rows</u> are the elements of S.
   Let C be the subspace generated by the <u>columns</u> of A.

   $$\forall \; x, y \in C \;\; x \neq y, \;\; \frac{1-\varepsilon}{2} \leq \frac{1}{n}\mathrm{dist}(x,y) \leq \frac{1+\varepsilon}{2}$$

2. For every $\alpha \in \{0,1\}^k \setminus \{\bar{0}\}$

   $$\left| \mathop{\mathbb{E}}_{s \in S}\left[(-1)^{\sum_{i=1}^{k} \alpha_i s_i} \right] \right| \leq \varepsilon$$

   (such an S is called an ε-biased set)