## TODAY

- Linear time Encodable & Decodable codes
- (if time) Distance Amplifying codes

---

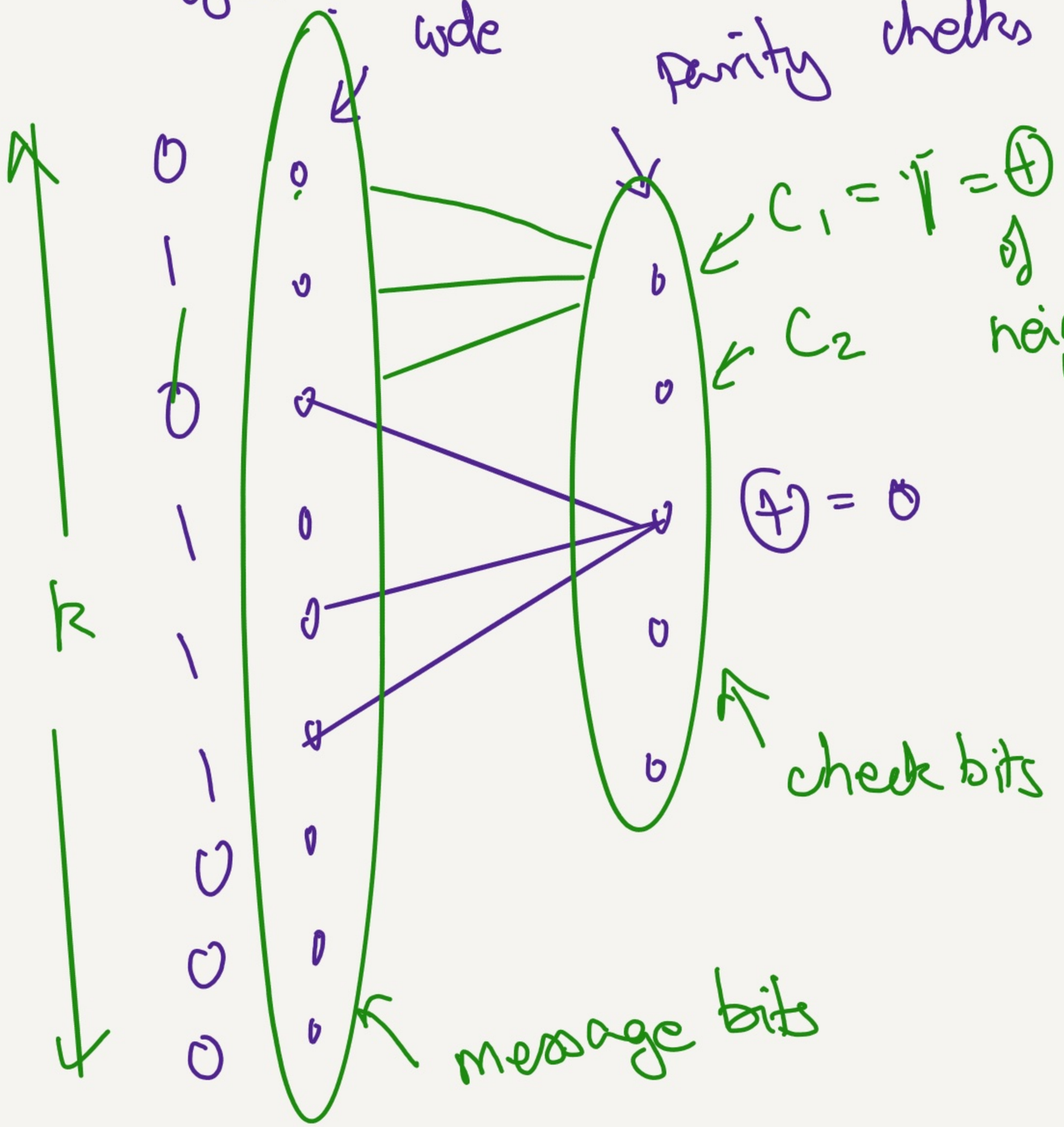
## Admin

- Zoom Questionnaire
- Zoom Protocol
- How are you?

---

- PS3 tomorrow
- P/NP/SAT/USAT

Suppose we take the bipartite graph from last lecture & used it encode - what do we get?




$m \in \mathbb{F}_2^k$

neighbors

Encoding

$(m, c)$

Rate $\geq 1/2$

[Spielman]

- Is this a good error correcting code?

(is $\delta = \Omega(1)$?)

- # right nodes $= l \leq$ # left nodes $= k$
- $(c,d)$-regular (left degree $= c$, right degree $= d$)
- $(\gamma, \delta)$-expander ($S \subseteq L$, $|S| \leq \delta k$ then $|\Gamma(S)| \geq \gamma \cdot c \cdot |S|$)

"Systematic" where message appears in its encoding

$m = 0 \Rightarrow x = 0$

$m = 0^{k-1}1 \Rightarrow x$ has $\leq c$ 1's $\Rightarrow$

$m \longmapsto (m, x)$

encoding has at most $c+1$ 1's.

# Defn: $\epsilon$- Error reduction Code

$E: m \longmapsto (m, x)$ is an $\epsilon$- error reduction code if

$\exists$ Decoder $D: (\hat{m}, \hat{x}) \longmapsto \tilde{m}$ s.t. the following holds

- if $\delta(m, \hat{m}) \leq \epsilon$ AND $\delta(x, \hat{x}) \leq \epsilon$

linear time?

then $\delta(m, \tilde{m}) \leq \dfrac{\delta(x, \hat{x})}{2}$

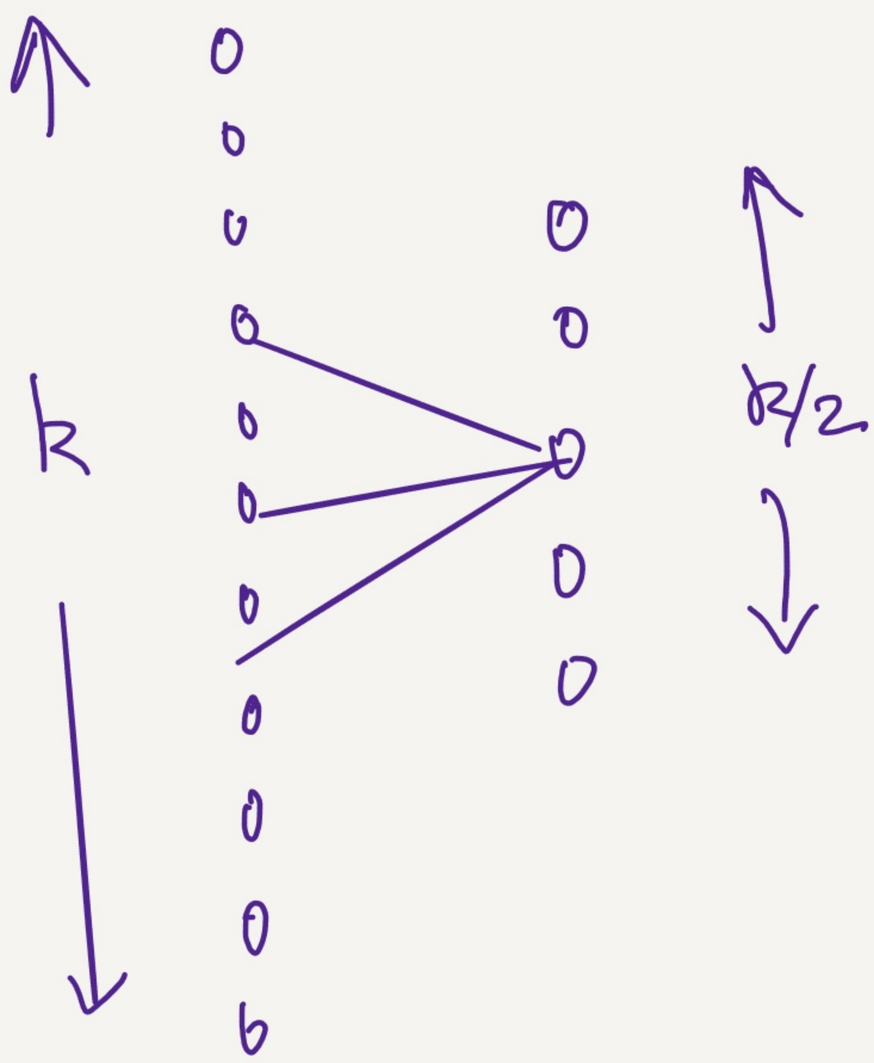
---

① if $\delta(x, \hat{x}) = 0 \Rightarrow \delta(m, \tilde{m}) = 0 \Rightarrow$ perfect error-recti.

② otherwise if $\delta(m, \hat{m}) = \delta(x, \hat{x}) = \epsilon$

then $\delta(m, \tilde{m}) \leq \dfrac{\epsilon}{2}$ $\Leftarrow$ still reducing error.

**Theorem:** if $\gamma = 1/8$, $\delta > 0$, $d = 2c = O(1)$ then $\exists \epsilon > 0$ s.t. "Spielman-Construction" is an $\epsilon$-error-reducing code, with linear time decoder.




$$x_j = \bigoplus_{i \leftrightarrow j} m_i$$

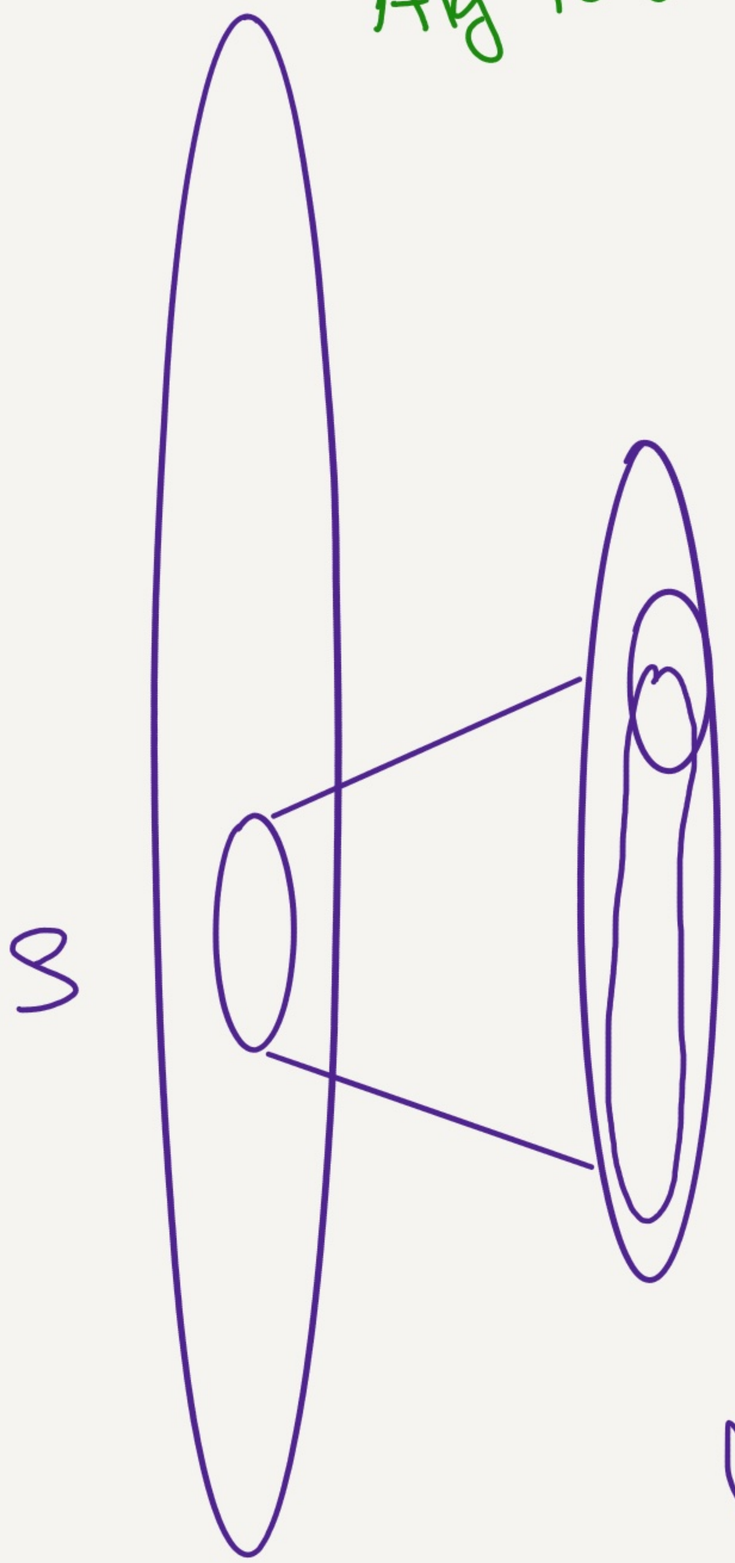
"Spielman-construction"

**Proof:** Exercise

Alg to decode = FLIP

$$S = \{i \mid m_i \neq \hat{m}_i\}$$

$$T = \{j \mid x_j \neq \hat{x}_j\}$$




$\Gamma(S)$ = neighbors of $S$

$$\Gamma(S) = U \cup V$$

$U$: unique neighbors

$V$: other neighbors

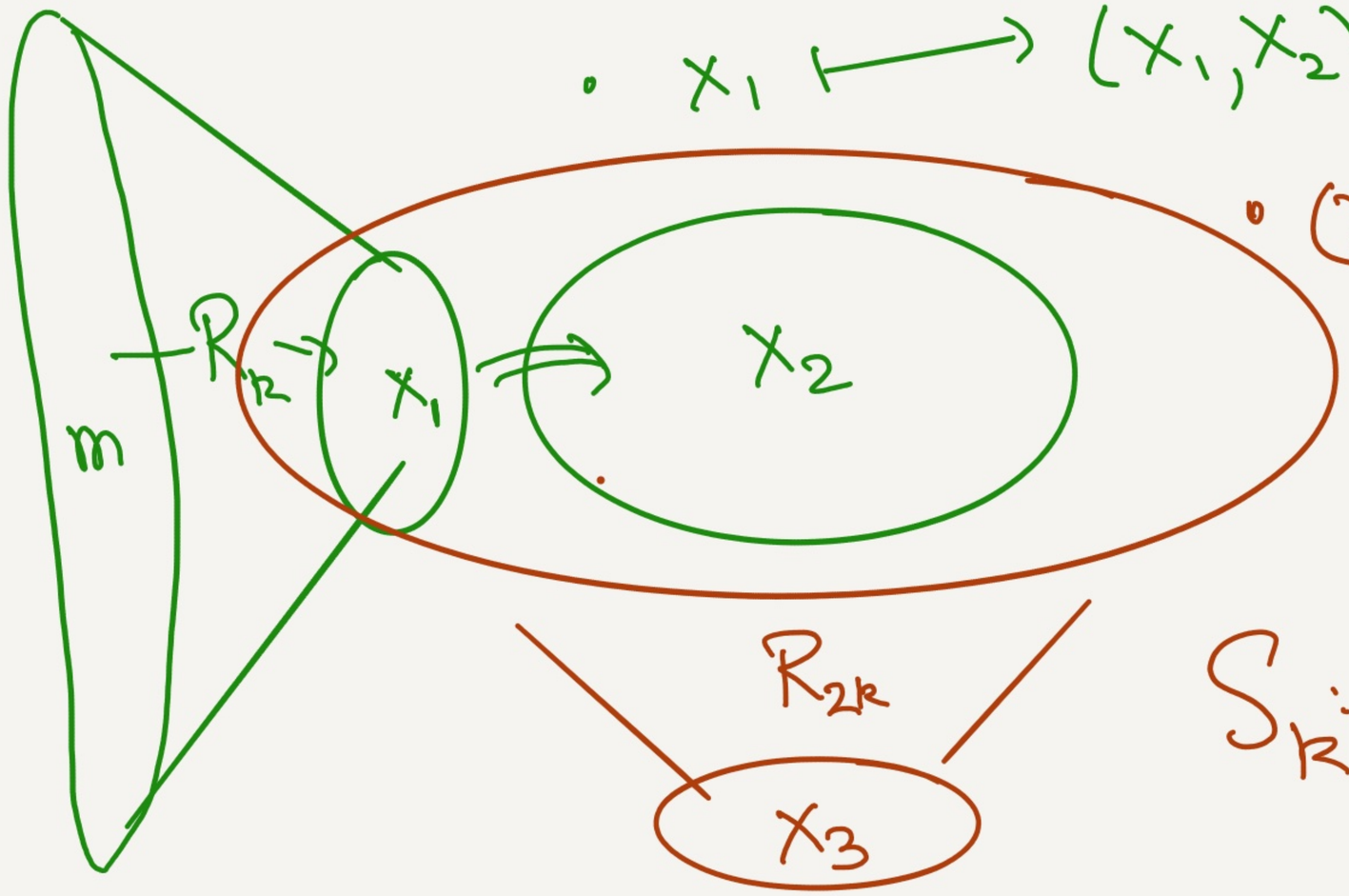
$U - T$ has unsat check nodes

"FLIP" Algorithm will find a vertex on left with more UNSAT than SAT neighbors.

# Spielman - Code

$$S_k : \mathbb{F}_2^k \to \mathbb{F}_2^{4k}$$

- $m \longmapsto (m, x_1)$ : Use $R_k$
- $x_1 \longmapsto (x_1, x_2)$ : Using $S_{k/2}$
- $(x_1, x_2) \longmapsto ((x_1, x_2), x_3)$ using $R_{2k}$




$$S_k : m \to (m, x_1, x_2, x_3)$$

$m \in \mathbb{F}_2^k$

$x_1 \in \mathbb{F}_2^{k/2}$

$x_2 \in \mathbb{F}_2^{3k/2}$

$x_3 \in \mathbb{F}_2^k$

① Start with $k$ message bits

② Apply error-reduction to get $k/2$ check bits

**Inductive Claim:** $S_k$ correct $\epsilon k$ errors.

- Say we have $\Delta\left((\hat{m}, \hat{x}_1, \hat{x}_2, \hat{x}_3), (m, x_1, x_2, x_3)\right) \leq \epsilon k$

$\Rightarrow \Delta(\hat{m}, m) \leq \epsilon k$ ; $\Delta((\hat{x}_1, \hat{x}_2), (x_1, x_2)) \leq \epsilon k$ ;

$\Delta(\hat{x}_3, x_3) \leq \epsilon k$

- $R_{2k}$ - error reduction step $\Rightarrow D(\hat{x}_1, \hat{x}_2, \hat{x}_3) = \tilde{x}_1, \tilde{x}_2$

s.t. $\Delta\left((\tilde{x}_1, \tilde{x}_2), (x_1, x_2)\right) \leq \frac{\epsilon k}{2}$

- $S_{k/2}$ can correct $\epsilon k/2$ errors in $\tilde{x}_1, \tilde{x}_2$

$\Rightarrow$ can recover $\bar{x}_1 = x_1$

- $R_k$ will output $\tilde{m}$ s.t.

$\delta(m, \tilde{m}) \leq \frac{\delta(\bar{x}_1, x_1)}{2} = 0$

Verify rate ✓

Verify linear time encoding ✓

# Decoding Algorithm for $S_{1R}$

$D^S(\hat{m}, \hat{x}_1, \hat{x}_2, \hat{x}_3)$

: ① $(\tilde{x}_1, \tilde{x}_2) = D^R_{2R}(\hat{x}_1, \hat{x}_2, \hat{x}_3)$

② $\bar{x}_1 = D^S_{R/2}(\tilde{x}_1, \tilde{x}_2)$

③ $\tilde{m} = D^R_R(\hat{m}, \bar{x}_1)$

Output $\tilde{m}$

- So for Codes using graphs are using the expansion to check for errors.

[Sipser - Spielman] last lecture

[Spielman] today

- To come next lecture.
  - Use graph + expansion to "spread errors".
  - Very nice collection of codes of high distance
  - The challenge in coding theory is mostly at high rate
  - Also linear time decodable.