S708 LECTURE 19

Note Title 4/16/2008

TODAY: LINEAR-TIME ENCODABLE & DECODABLE CODES [Spielman '94]

Recall: LDPC (Expander) Codes yield $R > 0$ & correct $p > 0$ fraction error in linear time (worst-case)

But what about the "easier" task of encoding. Now it is slower... or is it?

Hope 1: Maybe code defined by LDPC matrix also has an LDG matrix?
(Low Density Generator)

Unfortunately .... This is impossible.

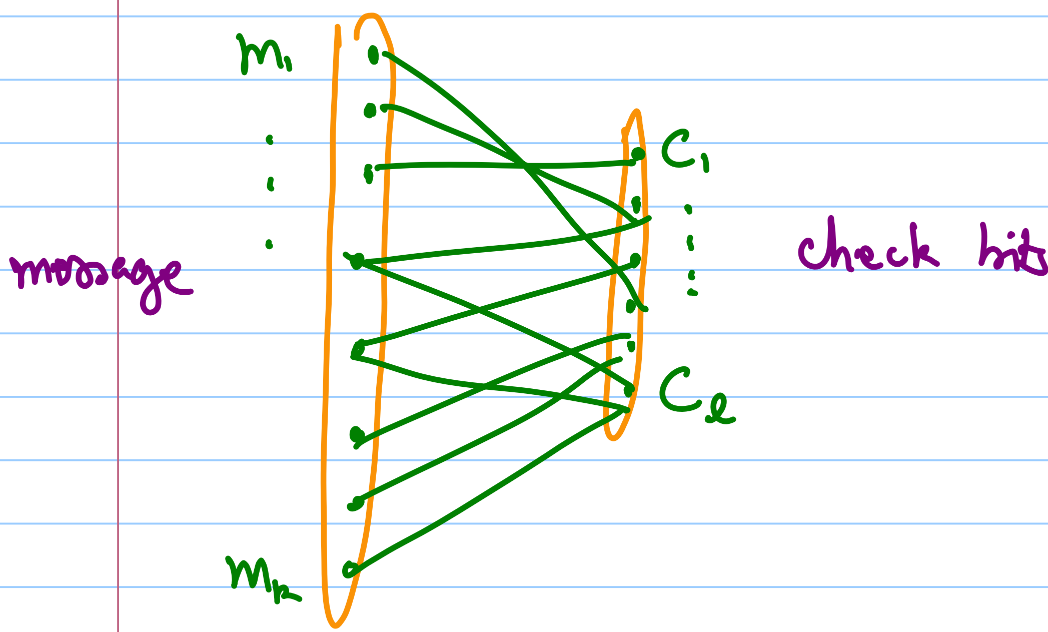
Claim: LDG matrix leads to Low Distance Code.

Proof: Some bits of message affect few bits of codeword. Flipping such a bit leads to codewords that are close to each other. ☒

So ... Hope 1 is shattered.

[Spielman]:

- Use Expander graph to "encode" information anyway.



$$c_j \triangleq \bigoplus_{i \leftrightarrow j} m_i$$

- **Claim:** Given (m', c) s.t. $m' \approx m$ & (m, c) legit codeword of above code, FLIP finds m.

- Conclude : Need to only "protect" c from errors.

- But c is constant factor smaller than m. Smaller problem $\Rightarrow$ Can recurse?

- Er ... Not so simple.

  # message bits has gone down.

  But # errors we are protecting from is still same

- Need to be a bit more careful.

[Spielman]: Two uses of LDG code.

$m \xrightarrow{E} (m,c)$

① Given (m',c) s.t. $\exists\, m \approx m'$

$E(m) = (m,c)$, can compute m.

[if check bits are <u>all</u> correct, can recover message]

② Given (m',c') s.t. $\exists\, m$ s.t.

$E(m) = (m,c)$ & $m \approx m'$, $c \approx c'$

Can find m'' s.t. for $\alpha < 1$.

$\Delta(m,m'') = \alpha \cdot \Delta(c,c')$

[if # check bit errors is <u>small</u> then # message bit errors can be <u>reduced</u>]

Led Spielman to call these ERROR-REDUCTION CODES.

Lemma : (ERROR-REDUCERS)

$\exists\, \rho > 0$ s.t. $\forall k$ $\exists$ Error-Reduction code

$R_k : \{0,1\}^k \to \{0,1\}^{k/2}$ & decoder $FLIP_k$

s.t. the following holds:

Let $c = R_k(m)$ & let (m', c')

be s.t. $\delta((m,c),(m',c')) \leq \rho$

then $\delta(FLIP_k(m',c'), m) \leq \frac{1}{6} \cdot \delta(c,c')$

$\leq \rho/2$

Will defer proof of this Lemma.

Will first see why it suffices.

Theorem: $\exists\, p > 0$ s.t. $\forall k$, $\exists\, E_k, D_k$ (linear time computable) s.t.

$$E_k : \{0,1\}^k \to \{0,1\}^{3k}$$

$$m \mapsto c$$

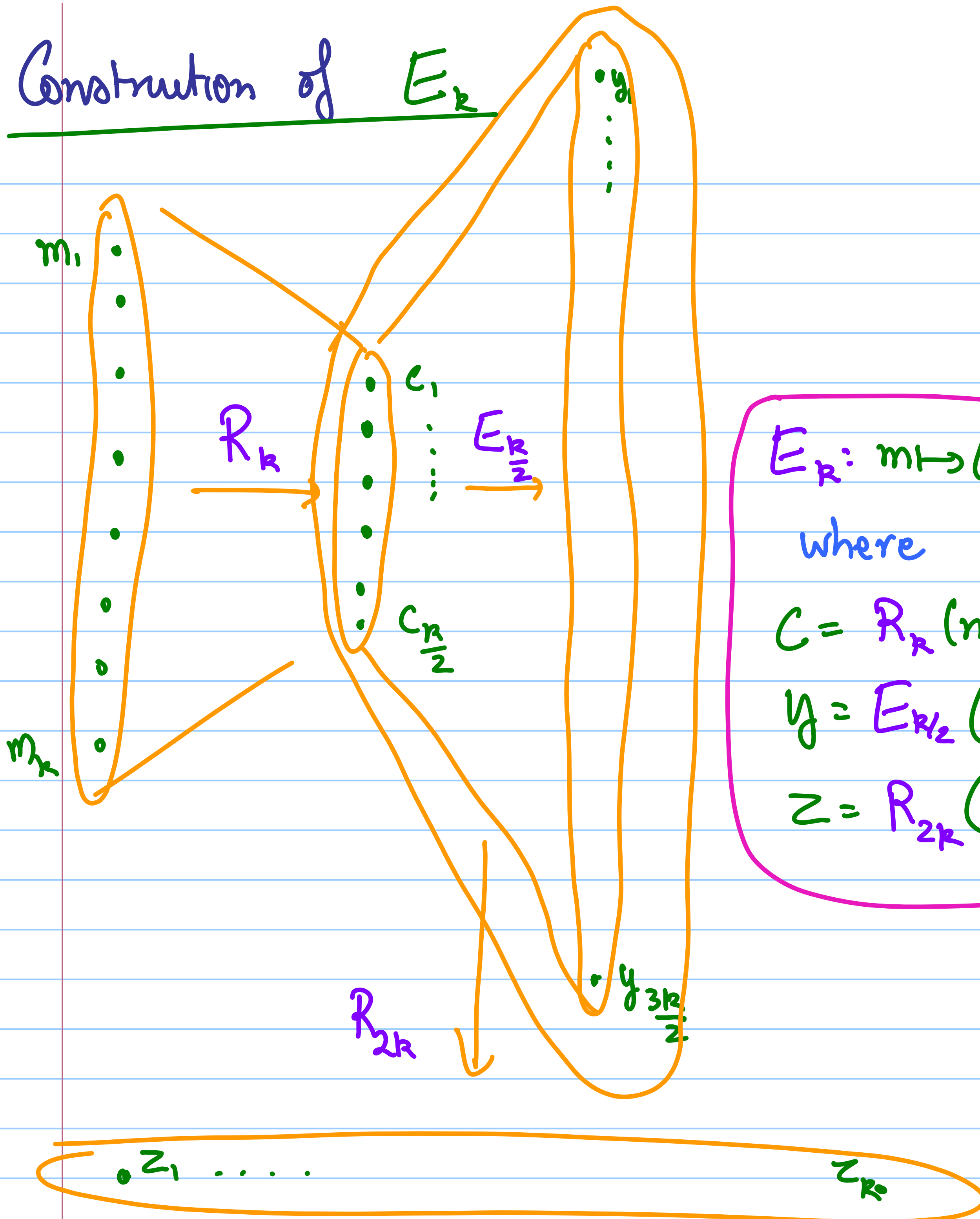
$$D_k : \{0,1\}^{4k} \to \{0,1\}^k$$

$$(m', c') \mapsto m$$

s.t. if $\delta\big((m', c'), (m, E(m))\big) \leq p$

then $D_k(m', c') = m$

Construction of E_k



$E_k : m \mapsto (c, y, z)$

where

$c = R_k(m)$;

$y = E_{k/2}(c)$;

$z = R_{2k}(c, y)$;

Analysis: (Code parameters, Encoding time)

(1) Clearly $k \longmapsto 4k$

$\uparrow$ message   message + check.

(2) Let running time of R_k be $\leq c \cdot k$
$T(k)$

Then running time of E_k is given by

$$T(k) \leq c \cdot k + c \cdot 2k + T(k/2)$$

$$= 6ck = O(k).$$

(six times slower ....)

Decoder $D_k(m', c', y', z')$

① Use $\mathrm{FLIP}_{2k}(c', y', z')$

to get (c'', y'') (with hopefully less error)

② Use $D_{k/2}(c'', y'')$ to get $c^{(3)}$

(hopefully $c^{(3)} = c$)

③ Use $\mathrm{FLIP}(m', c^{(3)})$ to get m''

(hopefully $m'' = m$)

Running Time: Linear ☒

Analysis of Correctness of Decoder:

(for $p = ?$)

- Good to switch to absolute error model.
- Let $e = \Delta\big((m', c', y', z'), (m, c, y, z)\big)$
- Note $e \leq p \cdot (4k)$
- We have $\Delta\big((c', y', z'), (c, y, z)\big) \leq e$

Assume $\frac{e}{3k} \leq \rho \Leftarrow p \cdot \frac{4}{3} \leq \rho$

$\Rightarrow$ (using the Lemma) $FLIP_{2k}$ returns

$$\Delta\big((c'', y''), (c, y)\big) \leq \frac{e}{3k} \cdot \frac{(2k)}{2}$$

$$\leq e/3$$ Step 1

(error has reduced ... but is this good enough)

- Now for step 2 we have

$$\delta\left((c'', y''), (c, y)\right) \leq \frac{e}{3} \leq \frac{4pk}{3}$$

$$< p \cdot (2k)$$

So $D_{\frac{k}{2}}(c'', y'') = c^{(3)} = c$!

Step 2

- Finally for step 3 we have

$$\Delta\left((m', c^{(3)}), (m, c)\right)$$

$$= \Delta\left((m', c), (m, c)\right)$$

$$= \Delta(m', m) \leq e$$

if $e < \rho\left(\frac{3k}{2}\right)$ $\left[\Leftarrow p\,4k \leq \rho \cdot \frac{3k}{2}\right]$

$\Leftarrow p \leq \frac{3}{8}\rho$

~~Thm~~ Lemma

$\Rightarrow \quad \delta(m'', m) \leq \frac{1}{6}\,\delta(c^{(3)}, c)$

$= 0$

$\Rightarrow \quad m'' = m$ as desired.

So theorem holds for $p = \frac{3}{8}\rho$. $\boxtimes$

ERROR-REDUCTION CODES

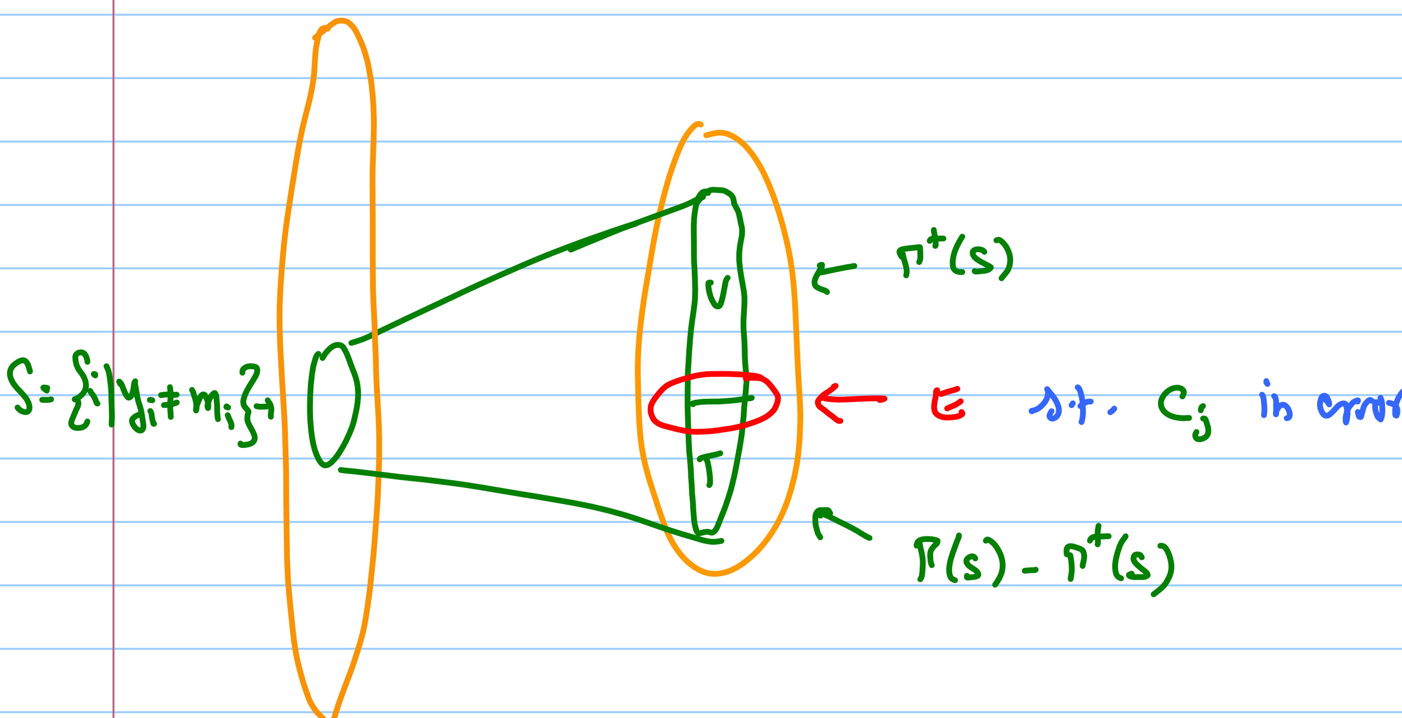
- Pick $(c, 2c)$-bounded (γ, δ)-expander with $\gamma > \frac{7}{8} c$

- Encode using the graph: $E_k(m) = c$ where
$$c_j = \bigoplus_{i \leftrightarrow j} m_i$$

- Decode using FLIP where j^{th} constraint is SAT if $c_j = \bigoplus_{i \leftrightarrow j} y_i$ and $y_1, \dots, y_k$ is current message; Iterate till every message bit is adjacent to more SAT constraints than UNSAT.

Analysis

- Let $t = \Delta((m', c'), (m, E(m)))$
- Initial # UNSAT constraints $\leq c \cdot t$
- So alg. terminates in $c \cdot t$ iterations.
- Total # message errors $(\Delta(y, m))$ is always less than $(c+1) \cdot t$
- Stopping condition = ?



- Note $\Gamma^+(S) - E \subseteq \text{UNSAT} \subseteq \Gamma(S) \cup E$

- $|\Gamma^+(S)| \geq (2\gamma - c) \cdot |S|$

$|\text{UNSAT}| \geq (2\gamma - c) \cdot |S| - |E|$

$|\text{UNSAT} \cap \Gamma(S)| \geq (2\gamma - c)|S| - 2|E|$

- if $\frac{|\text{UNSAT} \cap \Gamma(S)|}{|S|} > \frac{c}{2}$ then not done.

- Stop $\Rightarrow$

$$2\gamma - c - 2\frac{|E|}{|S|} \leq \frac{c}{2}$$

$$\Rightarrow \frac{2|E|}{|S|} \geq 2\gamma - \frac{3c}{2} \geq \frac{c}{4}$$

$$\Rightarrow |S| \leq \frac{8}{c} \cdot |E|$$

Pick c large enough to make this work!