TODAY: DISTANCE AMPLIFYING CODES

aka "ABNNR Construction" - Alon Bruck Naor Naor Roth

"AEL Construction" - Alon Edmonds Luby

"GI results" - Guruswami Indyk

- Weekly Reports.
- OH today + Friday (Chining)
- PS 4 next Friday
- PS 3 Due yesterday

Error in PS 4.4

Part (b) omitted

The ABNNR Construction

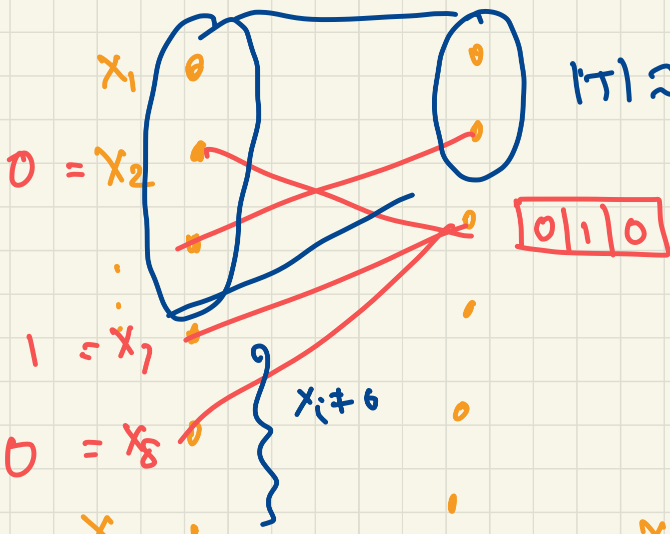
- takes a <u>weak</u> ECC (low distance)

$\Rightarrow$ converts it to a <u>strong</u> one (very high distance)

- Start with a bipartite expander $B = (L, R, E)$

$|L| = |R|$

d- regular



$|T| \approx \frac{n}{d}$

$x = (x_1 \dots x_n) \in \mathbb{F}_2^n$

$\Downarrow$

$y = (y_1 \dots y_n) \in (\mathbb{F}_2^d)^n$

$x \longmapsto y$ <u>not</u> a good error corr. code.

Fix: only use $x = (x_1 \dots x_n) \in C_0 \subseteq \mathbb{F}_2^n$
with C_0 having modest distance.

- Can fix C_0 s.t. $\delta(C_0) = .01$
$R(C_0) = \frac{1}{2}$

- will use d very large (much larger than $\frac{1}{\delta(C_0)}$)

$\Rightarrow$ then encoding of $\underset{\#\,0}{(x_1 \dots x_n)} \longmapsto (y_1 \dots y_n)$

$\exists$ graph B s.t. every subset of left nghbrs of size $\geq .01n$
see at least $(1 - \frac{1}{d})n$ neighbors
on right.

$\Rightarrow \cancel{\#}\ y$ is a code whose distance is $\approx 1 - \frac{1}{d}$

$m \in \mathbb{F}_2^{n/2}$
$\Downarrow C_0$
$x = E(m) \in \mathbb{F}_2^n$
$\Downarrow$ ABNNR
$y = \tilde{E}(E(m)) \in (\mathbb{F}_2^d)^n$

C

$R(C) = ?$ $\delta(C) = ?$

$\text{Rate}(C) = \frac{1}{2}$?

$\boxed{\text{Rate}(C) = \frac{1}{2d}}$

$\delta(C) = 1 - \frac{1}{d}$

By starting with better C_0

$\Rightarrow$ Can push
$\text{Rate}(C) \Rightarrow \frac{1}{d}$

<u>ABNNR Application:</u> Use these codes + concatenation

to get binary codes of distance $\frac{1}{2} - \epsilon$

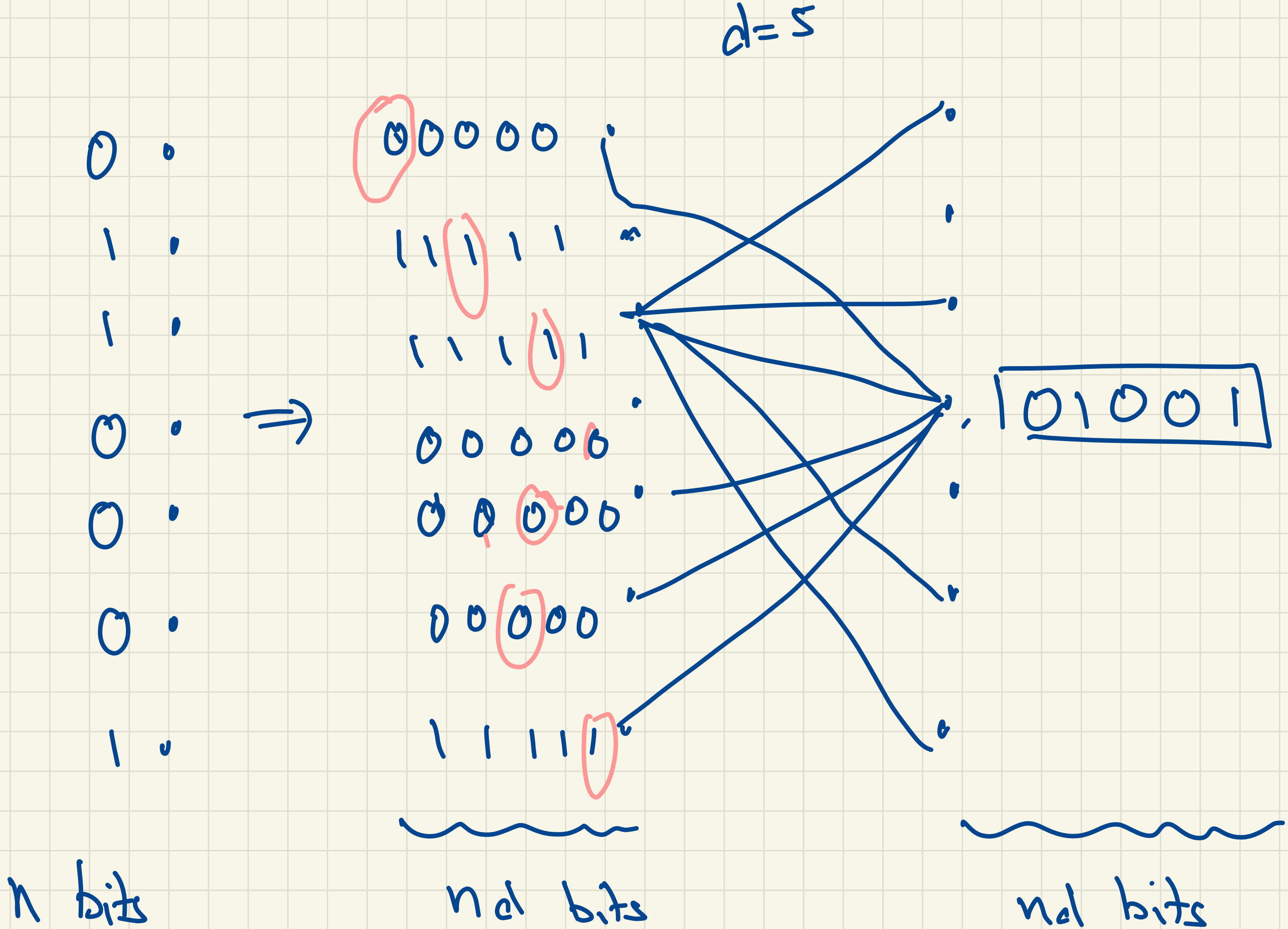
k message bits to $O\left(\frac{k}{\epsilon^3}\right)$ codeword bits

Rate $= \Omega(\epsilon^3)$

Yet ...

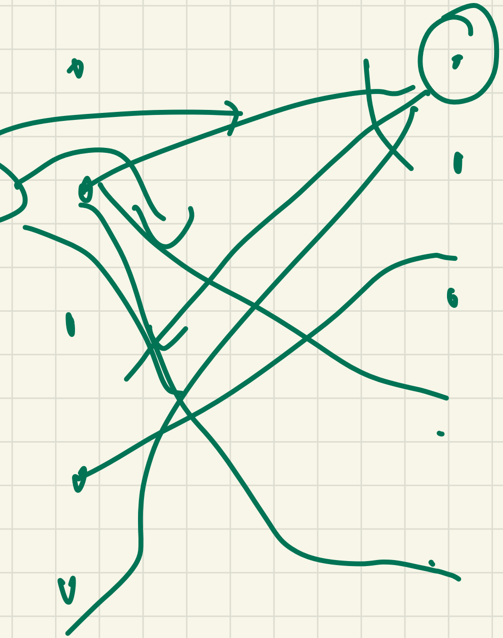
Codes are of small rate

Here is AEL comes in


d=5
0
1
1
0
0
0
1
00000
11111
11111
00000
00000
00000
11111
101001
n bits
nd bits
nd bits

Already precoded

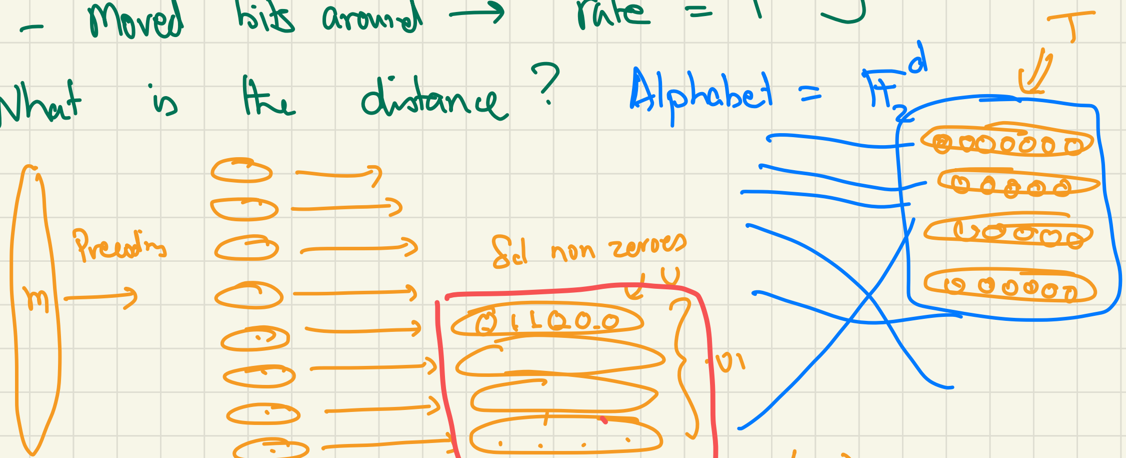
010	$\longrightarrow$	011011
101	$\longrightarrow$	101110
110	$\longrightarrow$	101111
011	$\longrightarrow$	011100
110	$\longrightarrow$	101111
111	$\longrightarrow$	111000
ℓ bits	$\Longrightarrow$	d bits
$\times\, n$		$\times\, n$



- What is the rate of this process?
  - Precoding loss $\to$ $1 - o(1)$
  - ℓ bits $\to$ d bits $\to$ $R = \ell/d$
  - Moved bits around $\to$ rate $= 1$

$$\Rightarrow \frac{\ell}{d} - o(1)$$

- What is the distance? Alphabet $= \mathbb{F}_2^d$



$.01 = \Omega(1)$ fraction non-zeroes

$\delta \cdot d \cdot (.01) \cdot n$ ones

S

$$|\Gamma(U) \cap T| \leq (1-\delta) \cdot d$$

typical vertex on right should see $\approx \frac{|S|}{n} \cdot d$ neighbors in S.

$$(1-\delta)d \ll \frac{|S|}{n} \cdot d$$

$$(1-\delta) \ll \cdot |S|$$

Want from graph B:

size of largest T s.t.

$$\Gamma_{\leq (1-\delta)d}(T) \triangleq \{ u \in L \mid |\Gamma(u) \cap T| \leq (1-\delta)d \}$$

then $|\Gamma_{\leq (1-\delta)d}(T)| \geq (.01)n$

long code of length n

$\exists$ graphs s.t. size of T is small

↑ but over large alphabet

$\Rightarrow$ . . . . codes of $R - o(1)$, distance δ ..., Guruswami - Indyk : - linear-time decoding based on this construction.

- Pick B = random graph - - .

  {will my construction work ?
  " algorithm work ?}

- Extract right graph-theoretic properties that made the proof work & use explicit graphs.

Will attempt in <u>PS5</u> : to use GI idea

to repair PS4.4 (b)

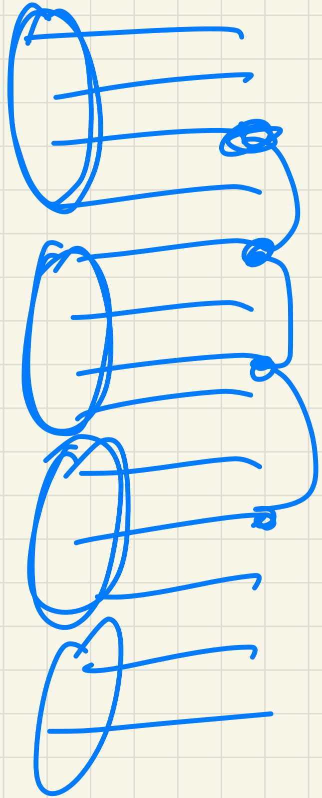
$\Rightarrow$ alphabet-reduction in FRS

& get list-decoding close to capacity

over $O_\epsilon(1)$ alphabets.

<u>Next:</u> Polar Codes : Why ? What ? How ?

set's
of sized



on nd edges