1 Last Lecture:

Recall:

**Definition 1.1.** we have: $(n, m, a, \beta, a(1-\varepsilon))$ : a (lossless) expander

\[ \rightarrow \text{with the following:} \]
(i) $0 < m/n < 1$
(ii) $a = O(1)$
(iii) $\varepsilon$ as a constant (e.g. < 1/4)

**Figure 1:** bipartite mapping from L to R

mapping:

codeword position $[L] \rightarrow [R]$ parity check matrix row

**a is the degree of vertices from L $\rightarrow$ R**
2 Rate, Relative Distance of Expanders:

**Proposition 2.1.** \((n, m, a, \beta, a(1-\varepsilon))\) : an expander, is a linear code of rate \(\geq (1 - m/n)\)

due to each parity check on the right side representing 1 constraint (not necessarily unique)
we can show:

\[(A): \delta > \beta \quad (\{ \delta > 2\beta(1-\varepsilon) \} \text{ is actually provable})\]

let \(U(S) = \text{set of unique neighbors}\)
a unique neighbor is the right node on a 1-ary edge from the left.

to prove (A), it is sufficient to show:

\[(B): \forall S \subseteq L, \quad |S| < \delta n, \quad |U(S)| > 0\]

To prove (B) we need the following:

**Lemma:**

\[
a|S| \geq |N(S)| \geq |U(S)| \geq a(1-2\varepsilon)|S| \quad \text{**(>0 if } \varepsilon < 1/2\text{)**}
\]

**Proof:**

Consider only \(S\) and \(N(S)\):

\(|S| \leq \beta n\)

the number of \(x \geq a(1-\varepsilon)|S|\)

trivially, there are \(a|S|\) edges from \(S\) to \(N(S)\)

each \(x\) is at the end of at least 1 edge

the number of distinct edges \(\geq a(1-\varepsilon)|S|\)

can we show that the number of vertices in \(N(S)\) with 1 distinct edge \(\geq a(1-2\varepsilon)|S|\) ?

\[\downarrow\]

the number of non-distinct edges \(\leq a\varepsilon|S|\)

\(w \notin U(S)\) iff \(w\) has no non-distinct edge incident on it

\[\downarrow\]

\(|U(S)| \geq |N(S)| - a\varepsilon|S|\)

\(a(1-\varepsilon) \geq a(1-\varepsilon)|S| - a\varepsilon|S|\) \(a\) out of \(S\), at least 1 back is distinct

\(a(1-\varepsilon)|S|\) is now accounted for, simply distribute the remaining \(\leq a\varepsilon|S|\) as necessary
Figure 2: S to N(S) mapping

corollary:
if ε < 1/4 (as we defined it to be earlier),
|U(S)| > (a|S|)/2
Decoding:

linear time decoding (actually error correction) algorithm for expander codes

- up to $\beta (1 - \epsilon)$ fraction of errors

Message Passing Algorithm:

Once a message is received we consider the case where there are 2 sides to decoding (similar but not the same as the bipartite graph of 1.1)

- each left value sends its bits to the corresponding neighbors on the right
- the right then computes the parity of the bits

If the result is 0, we are done as the parity check has succeeded ($b_j = 0 \ \forall j$)... no errors

Next:

If an error in parity occurs, the right side sends this error back to the corresponding bit on the left side

Once the left side has received all of this feedback, if a bit, $b_i$ receives more error parity than correct, it is flipped (e.g. $1 = 0, 0 = 1$)

And the process starts again. 1 and only 1 bit is flipped at a time, then everything is re-sent to the right.

Figure 3: decode by message passing algorithm
why this works:
the number of parity errors is monotone decreasing
this means we converge to a valid codeword
(hopefully the correct one)

Lemma:
if the number of errors \( \leq \beta n \), a "flippable" vertex exists

Proof Idea:
\( L \) flips a given bit \( b_i \) iff \( > \alpha/2 \), pr; parity responses come back as negative
this means that if only 1 bit is flipped at a time before the process is repeated, then the round will result in
\( a-pr \) responses this time which is \( > \alpha/2 \) and so as we had hoped, we have improved.