Error Correcting Codes: Combinatorics, Algorithms and Applications (Spring 2009)

Lecture 35: Expander codes

4-15-09

Lecturer: Atri Rudra *Scribe: Jeff Hazel*

1 Last Lecture:

Recall:

Definition 1.1. *we have: (n , m , a , β, a(1-ε)) : a (lossless) expander*

$\rightarrow$ with the following:
(i) 0 < m/n < 1
(ii) a = O(1)
(iii) ε as a constant (e.g. < 1/4)

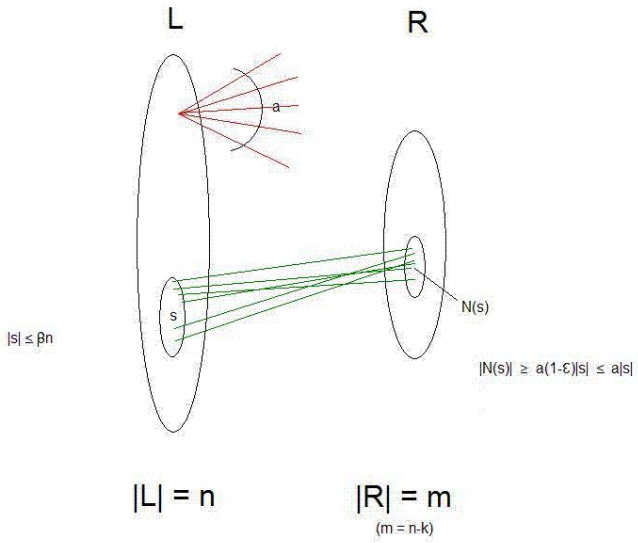

Figure 1: bipartite mapping from L to R

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 , β, a(1-ε)) : 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:

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

let U(S) = set of unique neghbors
a unique neghbor is the right node on a 1-ary edge from the left.

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

$$\text{(B): } \forall S \subseteq L\,, \qquad |\,S\,| < \delta n\,, \qquad |\,U(S)| > 0$$

To prove (B) we need the following:
Lemma :

$$\forall S \subseteq L\,, \qquad |\,S\,| \leq \beta n$$
$$a|S| \quad \geq \quad |N(S)| \quad \geq \quad |U(S)| \quad \geq \quad a(1\text{-}2\varepsilon)|S|$$
$$\text{**(>0 if } \varepsilon < 1/2)$$

Proof :
Consider only S and N(S):
$|S| \leq \beta n$
the number of x $\geq$ a(1-ε)|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-ε)|S|
can we show that the number of vertices in N(S) with 1 distinct edge $\geq$ a(1-2ε)|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-ε) $\geq$ a(1-ε)|S| - aε|S| a out of S, at least 1 back is distinct
a(1-ε)|S| is now accounted for, simply distribute the remaining $\leq a\varepsilon|S|$ as necessary

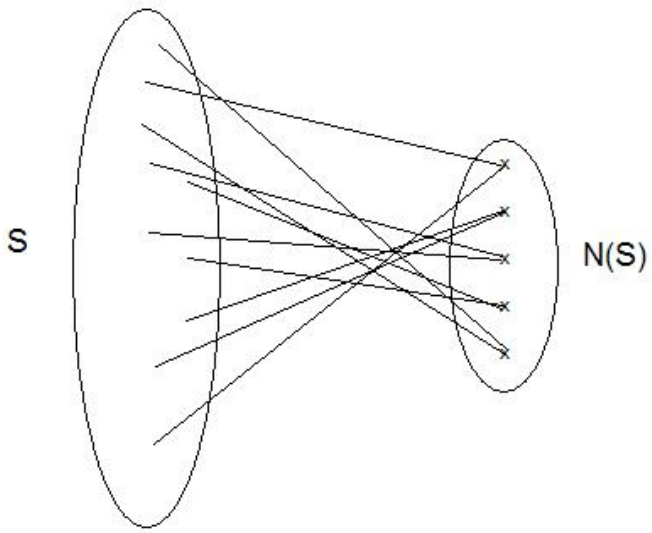

Figure 2: S to N(S) mapping

$\underline{corollary}$:
if $\varepsilon < 1/4$ (as we defined it to be earlier),
$|U(S)| > (a|S|)/2$

Decoding :

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

- *uptoβ(1-epsilon) fraction of errors*

MessagePassingAlgorithm :

Once a message is recieved we consider 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 recieved all of this feedback, if a bit, b_i recieves 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.

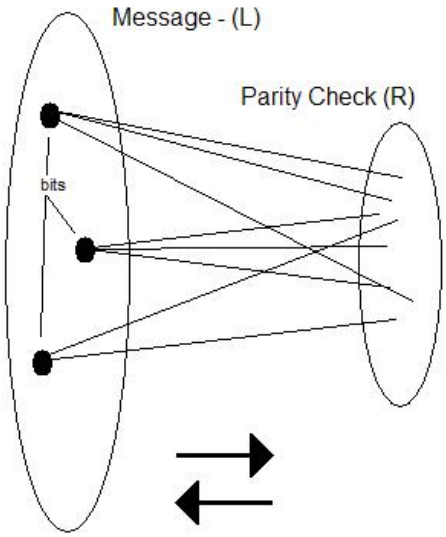

Figure 3: decode by message passing algorithm

$\underline{whythisworks}$:
the number of parity errors is monotone decreasing
this means we converge to a valid codeword
(hopefully the correct one)

$\underline{Lemma}$:
if the nunmber of errors $\leq \beta n$*, a "flippable" vertex exists*

$\underline{ProofIdea}$:
L flips a given bit b_i *iff* $>$ *a/2,* pr_i *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_i *responses this time which is* $>$ *a/2 and so as we had hoped, we have improved.*