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

Lecture 34: Expander Codes

April 13, 2009

Lecturer: Atri Rudra *Scribe: Jesper Dybdahl Hede*

In the last lecture we examined explicit linear codes that achieve BSC_p capacity, polynomial time decoding and exponentially small decoding error probability. We saw decoding time:

$$poly(N) + N \cdot 2^{O(k)}, \text{ where } k = \theta\left(\frac{\log \frac{1}{\gamma}}{\varepsilon^2}\right) \text{ and } \gamma = \varepsilon^3$$

A question to motivate this lecture is whether we can achieve BSC_p capacity with $poly(N, \frac{1}{\varepsilon})$ decoding. The answer is still open.

In this lecture we will examine if we can achieve BEC_α capacity with $N \cdot poly(\frac{1}{\varepsilon})$ decoding.

Theorem 1. *For small enough $\beta > 0$, there exist an explicit binary linear code of rate $\frac{1}{1+\beta}$, and can correct $\Omega(\frac{\beta^2}{(\log \frac{1}{\beta})^2})$ fraction of worst-case errors with $O(N)$ encoding and decoding.*

These codes are called *expander codes*. Note that they are optimal in running time (linear). Using expander codes is the only other way to get asymptotically good binary codes besides code concatenation.

1 Factor Graphs (for linear binary codes)

We examine a $[n, k]_2$-code C.
The factor graph for C is the bipartite graph corresponding to C's parity check matrix (when thought of as an adjacency matrix).

As an example we regard the $[7, 4]_2$-Hamming code:

$$H_{HAM} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{matrix} p_1 \\ p_2 \\ p_3 \end{matrix}$$
$$\begin{matrix} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 \end{matrix}$$

The parity check matrix is displayed as a factor graph in figure 1. In the parity check matrix the columns are named c_1 to c_7 and the rows are named p_1 to p_3. For a given row and column in the matrix, if there is a 1 then there is a line between the row and column points in the graph.

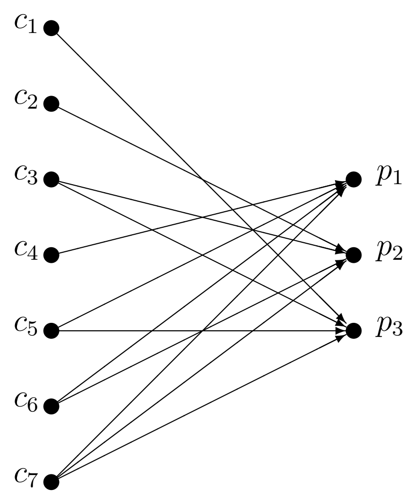

Figure 1: Parity check matrix for $[7,4]_2$-Hamming code as a factor graph.

Note that the parity check is done by calculating

$$\sum_{i=1}^{l} c_{j_i} = 0 \textit{ (over } \mathbb{F}_2).$$

In other words, if the parities sum to zero then the given symbol's parity checks out. In a factor graph this can be illustrated as figure 2. So to check the parity of an entire codeword we have that all the parities must sum to zero:

$$(c_1, ...c_n) \in C \textit{ iff } \forall p_j, \sum_{i=1}^{l} c_{j_i} = 0$$

1.1 Linear Density Parity Check (LDPC) codes

A LDPC code is a linear binary code whose factor graph has $O(n)$ edges, where the maximum possible amount for any factor graph is $O(n(n-k))$.

2 Expander Codes

Expander codes are a specific form of general expanders. Factor graphs as we previously examined is another kind of ”expander”.

See figure 2 for a graphical example of an expander graph. Every element c on the left has exactly a number of neighbors on the right

$$\forall v \in L, deg(v) = a.$$

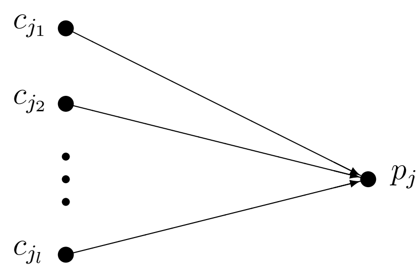

Figure 2: Example of single parity check.

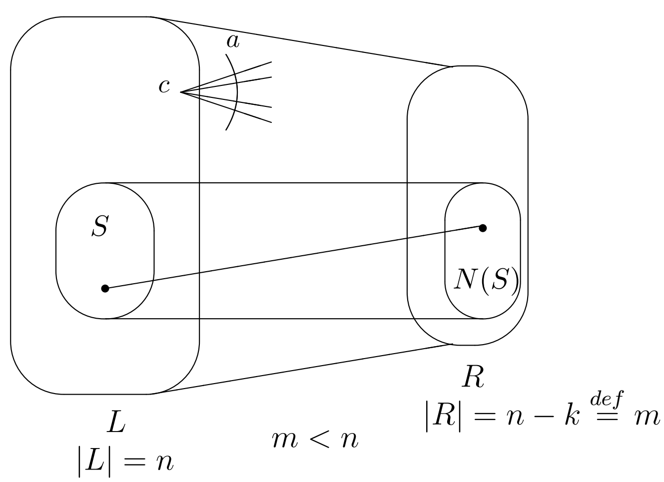

Figure 3: Expander as a factor graph.

So the number of elements in $N(S)$ is at most a times the length of S. Now, the factor graph is only said to be an expander if the number of elements in $N(S)$ is at least as high as the number of elements in S:

$$\Omega(|S|) \leq |N(S)|.$$

Definition 1. *A* (n, m, a, β, α)*-expander is an* (L, R, E) *left a-regular bipartite graph such that* $\forall S \subseteq L, |S| \leq \beta \cdot n, |N(S)| \geq \alpha \cdot |S|$

For all expanders we have

$$\alpha \leq a$$

and

$$a\beta n \leq m.$$

A special kind of expander is a loss less expanders, for which it holds

$$\alpha \geq a(1 - \varepsilon), \varepsilon > 0.$$

In other words, with a loss less expander α is very close to a.

Theorem 2. *(Existence)* $\forall \varepsilon > 0, m \leq n, \exists \beta > 0$ *such that there is an* $(n, m, a, \beta, a(1 - \varepsilon))$*-expander for which it holds* $a = \theta(\frac{\log \frac{2n}{m}}{\varepsilon})$, $\beta = \theta(\frac{\varepsilon}{a} \cdot \frac{m}{n})$.

By probabilistic method as well as knowing that $0 < \frac{n}{m} < 1, \varepsilon = \theta(1)$ we see that a is in the order of $\frac{1}{\varepsilon}$ and β is in the order of ε^2:

$$a = \theta(\frac{1}{\varepsilon})$$

$$\beta = \theta(\varepsilon^2)$$

Theorem 3. *For* $0 < \frac{m}{n} < 1, \varepsilon = \theta(1)$, *there exist a polynomial time construction of* $(n, m, O(1), \Omega(1), a(1-\varepsilon))$*-expander.*