COMPSCI 690T Coding Theory and Applications	Feb 27, 2017

Lecture 9

Instructor: Arya Mazumdar *Scribe: Names Redacted*

1 Review

Family of Codes [n,k,d]:

$$k = Rn, d = \delta n \tag{1}$$

R is rate, δ is relative distance

The best achievable parameters are Gilbert-Varshamov bound:

$$R = 1 - h(\delta) \tag{2}$$

$$\delta = h^{-1}(1 - R) \tag{3}$$

The number of errors that can be corrected by this code is approximately $\frac{h^{-1}(1-R)}{2}n$ – which is linearly growing with n. However there is not polynomial time algorithms guaranteed for this correction. We then planned to study a family of codes called LDPC (Low Density Parity Check Matrix) codes, that has polynomial time decoding and correct a linearly growing number of errors.

LDPC codes are defined by a sparse parity-check matrix. In the parity check matrix number of 1s in each row and column grows slowly $O(\log n)$ or is a constant. This sparse matrix is often randomly generated (Gallager 1963).

2 Spectral Expanders

For a D-regular graph $G(V, E)$ the $n \times n$ adjacency matrix A has D 1s in every row and column. The maximum eigenvalue of this matrix is D. Because $A \times \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = D \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$.

For this matrix it is known that the 2nd largest eigenvalue λ must follow:

$$\lambda \geq 2\sqrt{D-1}(1 - o(1)). \tag{4}$$

Spectral Gap. Absolute difference between the two largest eigenvalues of the graph.

When $\lambda = 2\sqrt{D-1}$, we have largest spectral gap. Such graph exists and are called Ramanujan graph. Explicit construction of Ramanujan Graphs are possible due to Margoulis.

3 Expander Mixing Lemma

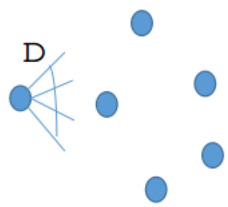
Let $G = (V, E)$ be a D-regular graph on n vertices with $\lambda \in (0, D)$ the second-largest eigenvalue (in absolute value) of the adjacency matrix. For any two subsets $S, T \subseteq V$, let $E(S, T) = |\{(x, y) \in S \times T : (x, y) \in E\}|$ be the number of edges between S and T.

$$|E(S,T) - \frac{D|S||T|}{n}| \leq \lambda\sqrt{|S||T|}. \tag{5}$$

3.1 Tanner Codes

Tanner 1981(http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1056404).

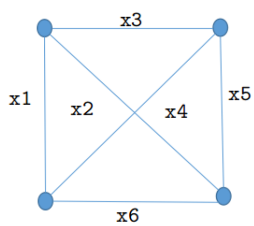
Small Code of length D, Local code C_0



n=number of edges $|E|$. m=number of vertices and each vertex has degree D.

Example: $C_0[3,2,2], D = 3$. The codewords of C_0 are listed here as the rows: $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$.

Consider the graph below:



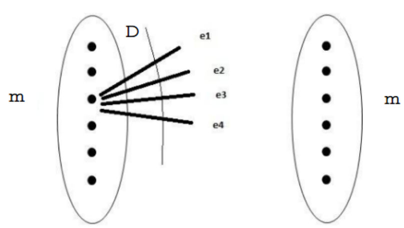
.

The Parity Check Matrix of this graph is:

$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$.

3.2 Zemor's Algorithm for decoding

Zemor's decoding algorithm for Tanner code:



Let U be the set of all vertices on the left and V be the set of all vertices on the right.

The first iteration of the algorithm consists of applying the complete decoding for the code induced by E_v for every $v \in U$. This means that for replacing, for every $v \in S$, the vector$(w_{v(1)}, w_{v(2)}, \ldots, w_{v(D)}$ by the closest codewords of C_0. Since the subsets of edges E_v are disjoint for $v \in S$, the decoding of these m subvectors of w may be done in parallel.

The iteration will yield a new vector z. The next iteration consists of applying the preceding procedure to z but with U replaced by V. In other words, it consists of decoding all the subvectors induced by the vertices of V. The coming iterations repeat those two steps alternately applying parallel decoding to the subvectors induced by the vertices of U and to the subvectors induced by the vertices of V.

Theorem 1 *For local code $C_0[D, R_0, \delta D]$, Rate of code C is $R \geq 2R_0 - 1$.*

Proof Local code has $D - R_0 D$ linear constraints, we have $2m$ vertices so the number of total linear constraints is $2m(R - R_0 D) = 2\frac{n}{D}(D - R_0 D)$ So for code C we have $R \geq n - 2\frac{n}{D}(D - R_0 D)$. So $R \geq 1 - (2 - 2R_0) = 2R_0 - 1$. ■