CSE 533: Error-Correcting Codes **(Autumn 2006)**

Lecture 14: Tanner Codes

November 19, 2006

Lecturer: Venkatesan Guruswami *Scribe: Widad Machmouchi*

In this lecture, we will discuss Tanner codes: a recursive low complexity approach to code construction. These codes are constructed from an expander graph G and a binary code C^*.

1 Tanner Codes

Fix a $(c, d)-$regular graph G (with left set L of size N and right set R of size M) and a binary linear code C^* of block length d and dimension $d - t$. We define the Tanner code $T(G, C^*)$ as follows:

$$T(G, C^*) = \{x \in \{0, 1\}^N \big| \forall y \in R, x|_{N(y)} \in C^*\}.$$

Since C^* imposes t constraints on its codewords then $T(G, C^*)$ imposes at most Mt constraints. Hence $dim(T(G, C^*)) \geq N - Mt$.

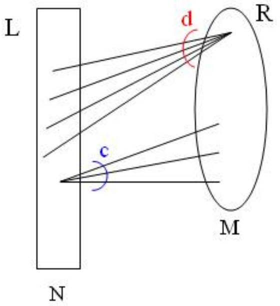

Figure 1: A pictorial view of a Tanner code

Recall the definition of an expander graph:

Definition 1.1. *An $(N, M, c, d, \gamma, \alpha)$-expander graph G is a $(c, d)-$regular graph (with left set L of size N and right set R of size M), such that $\forall S \subseteq L$ such that $|S| \leq \gamma N$, we have $|N(S)| \geq \alpha\, c|S|$.*

The following lemma gives a lower bound on the minimum distance of Tanner codes.

Lemma 1.2. *If G is an $(N, M, c, d, \gamma, \alpha)-$expander and C^* is an $[d, d-t, \Delta]_2$ binary linear code, then $T(G, C^*)$ is a code of rate $\geq 1 - \frac{M}{N}t$ with distance $\geq \gamma N$, provided $\alpha > \frac{1}{\Delta}$.*

Proof Suppose there exists $\tilde{c} \in T(G, C^*)$ with support S such that $|S| \leq \gamma N$. Let $N(S)$ be the neighborhood of S in R and $E(S, N(S))$ the number of edges between S and $N(S)$. Then we have:

$$|S|c \geq E(S, N(S)) \geq |N(S)|\Delta \geq \alpha c|S|\Delta.$$

The second inequality follows from the fact that every check node in $N(S)$ should be connected to at least Δ variable nodes in S (since the minimum distance of C^* is Δ and all the 1's in the codeword appear in S). The third inequality follows from the expansion property of G.
Since $|S|c \geq \alpha c|S|\Delta$, we get a contradiction, provided $\alpha > \frac{1}{\Delta}$. ■
Such expanders can be constructed using edge-vertex incidence graphs of spectral expanders.

2 Spectral Graphs

Definition 2.1. *A $d-$regular graph H on n vertices is said to be an $(n, d, \lambda)-$graph if $\lambda = max\{\lambda_2, |\lambda_n|\}$ where $\lambda_1 = d \geq \lambda_2 \geq \cdots \geq \lambda_n$ are the n eigenvalues of the adjacency matrix of H.*

If $\lambda \ll d$ then the $(n, d, \lambda)-$graph gives a good expander. The best possible λ for an $(n, d, \lambda)-$graph is $\lambda = 2\sqrt{d-1} \approx 2\sqrt{d}$.
Explicit constructions matching exactly the lower bound of $2\sqrt{d-1}$ are known (Ramanujan graphs).

Lemma 2.2 (Pseudorandomness of spectral graphs)**.** *Let $G = (V, E)$ be an $(n, d, \lambda)-$graph. Then $\forall\, S,\, T \subseteq V$*

$$\left| E(S,T) - d|S|\frac{|T|}{n} \right| \leq \lambda\sqrt{|S||T|}.$$

For a complete proof of this lemma, see "The Probabilistic Method" by Alon Spencer.
For $T = S$, we get the following upper bound on the number of edges from S to S.

Corollary 2.3. $\left| 2E(S) - \frac{d|S|^2}{n} \right| \leq \lambda|S|$*, and hence* $E(S) \leq \frac{d|S|}{2}\left(\frac{|S|}{n} + \frac{\lambda}{d}\right)$.

To construct a good expander, we will use the edge-vertex incidence graph of an $(n, d, \lambda)-$graph.

Definition 2.4. *The edge-vertex incidence graph of a $d-$regular graph $G = (V, E)$ is a (2,d)-bipartite graph $G' = (E \cup V, E')$ such that the left set L of G' is E, the right set R is V and $E' = \{(e, v), e \in E, v \in V$ and v is an endpoint of e $\}$.*

The edge-vertex incidence graph of a $d-$regular graph with n vertices is given in Figure 2.
The following corollaries establish the expansion property of the edge-vertex incidence graph of an $(n, d, \lambda)-$graph.

Corollary 2.5. *In the edge-vertex incidence graph of an $(n, d, \lambda)-$graph, any subset of L of size $\frac{\gamma dn}{2}\left(\gamma + \frac{\lambda}{d}\right)$ has at least γn neighbors in R.*

Corollary 2.6. *Let $N = \frac{nd}{2}$ and $M = n$. All left subsets of size $\leq \gamma_0\left(\gamma_0 + \frac{\lambda}{d}\right) N$ expand by $\alpha \geq \frac{1}{d\left(\gamma_0 + \frac{\lambda}{d}\right)}$. Hence, we get an $(N, M, 2, d, \rho, \alpha)-$expander with $\rho = \gamma_0\left(\gamma_0 + \frac{\lambda}{d}\right)$.*

Applying the above corollary to Tanner codes, we get:

Corollary 2.7. *If C^* is an $[d, d{-}t, d' > d\left(\gamma_0 + \frac{\lambda}{d}\right)]_2$ code and G is an $(N, M, 2, d, \rho, \alpha)-$expander, where $\rho = \gamma_0\left(\gamma_0 + \frac{\lambda}{d}\right)$, then $T(G, C^*)$ has rate $1 - \frac{M}{N}t$ and relative distance $\geq \gamma_0\left(\gamma_0 + \frac{\lambda}{d}\right)$.*

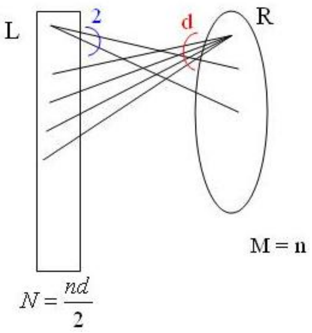

Figure 2: Edge-vertex incidence graph of a $d-$regular graph with n vertices

3 Decoding Tanner Codes

We will now give a decoding algorithm for Tanner codes that decodes up to $\frac{\delta}{4}$ fraction of errors, where δ is the relative distance. This algorithm is due to Zémor, improving on a decoding algorithm given by Sipser and Spielman that decodes up to $\frac{\delta}{48}$ fraction of errors.
The decoding algorithm uses a balanced bipartite graph H. H has degree d and the left and right sets have equal size of $\frac{n}{2}$, so that we get $N = \frac{nd}{2}$ edges. The codeword symbols sit on the edges of the graph.

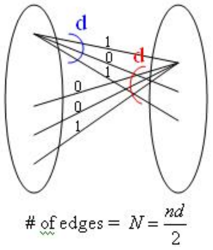

Figure 3: Decoding graph: The codeword sits on the vertices

The decoding goes as follows:
The edges of each vertex are codewords in C^*. At each round, we correct the d symbols neighboring one vertex to the closest codeword in C^*, and we alternate between the left set and right set. After $O(\log n)$ iterations, one can show that the algorithm can correct up to $\frac{\delta}{4}$ fraction of errors. The idea is that if a vertex in one set has too many errors and is decoded incorrectly into a wrong codeword in C^*, hopefully its edges will be connected to many vertices in the other set and will be decoded correctly at a coming round. For a complete proof, the reader is referred to Lecture 5 of the CSE 590VG course, Winter 2003.
One can improve decoding up to $\frac{\delta}{2}$ of errors using GMD decoding ideas (Tal and Roth).

4 Linear time decoding up to half the Singleton bound

One can use expander graphs to get linear time codes with near-optimal rate. We start by a linear code C of rate $1-\sqrt{4\gamma}$ with a linear time decoding algorithm that can correct γ fraction of errors. We block the resulting codeword into blocks of b symbols that are encoded into b' symbols using a RS code of rate $\frac{R}{1-\sqrt{4\gamma}}$. The decoding algorithm of the RS code can decode up to $\frac{1-R}{2}-\varepsilon$ fraction of errors, where $\varepsilon = O(\sqrt{\gamma})$.
The b' symbols are collected into one big symbol that is viewed as a vertex in the left set of the edge-vertex incidence graph of a $(n, b', \lambda)-$graph. Hence the b' symbols sit on the edges of the corresponding vertex.

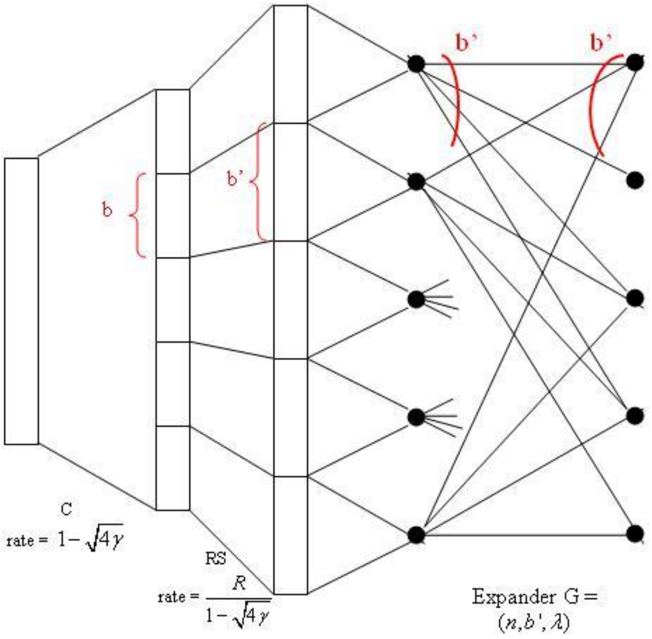
b'
b'
b
b'
C
rate = $1-\sqrt{4\gamma}$
RS
rate = $\frac{R}{1-\sqrt{4\gamma}}$
Expander G =
(n,b',λ)

Figure 4: Linear time code with near-optimal rate

The overall rate of the code is R.The expander graph won't change the overall rate of the resulting code. The purpose of the expander graph is to disperse the errors incurred by the adversary into many blocks of b' symbols. Hence, the received codeword will have symbols in the big alphabet and its symbols will be mapped to symbols in the RS code alphabet.The expansion property of the graph guarantees that these symbols appear in different $b'-$blocks.
The goal is to correct up to $\frac{1-R}{2}-2\varepsilon$ fraction of errors in linear time. The key idea is to use the pseudorandom property of the expander graph. The full analysis of the decoding algorithm is given in the next lecture.