

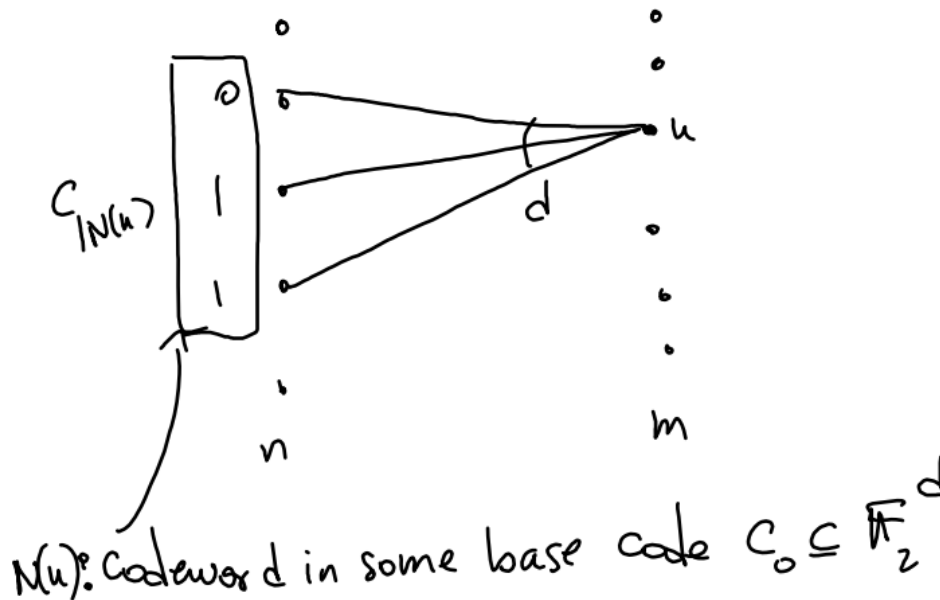
Lecture 13

Lecturer: Elena Grigorescu

Scribe: Kelly Dance

1 Tanner Codes

Like previously introduced expander codes, but instead of merely requiring that $\sum_{i \in N(u)} c_i = 0$ for all $u \in R$, we enforce that our expander graph is d -right regular then require that $c_{|N(u)} \in C_0$ for some fixed smaller code $C_0 \subseteq \mathbb{F}_2^d$.



Definition 1 The Tanner code $X(G, C_0)$ for some d -right regular bipartite graph $G = (L \cup R, E)$ is

$$X(G, C_0) = \{c \in \mathbb{F}_2^n \mid \forall u \in R, c_{|N(u)} \in C_0\}.$$

Where $c_{|N(u)}$ denotes projecting c onto the coordinates in $N(u)$.

Observation 2 If C_0 is the parity check code, i.e. $C_0 = \{c_1 c_2 \dots c_d \mid c_i \in \mathbb{F}_2 \text{ such that } \sum c_i = 0\}$, then $X(G, C_0)$ is a linear code.

Observation 3 If C_0 is linear, then $X(G, C_0)$ is linear

Claim 4 $\dim X(G, C_0) = n - m(d - \dim C_0)$

Proof We have $d - \dim C_0$ constraints per right vertex, so $m(d - \dim C_0)$ total constraints.

■

Corollary 5 The rate of $X(G, C_0)$ is $1 - \frac{m}{n}(d - \dim C_0)$

Theorem 6 If $G = (L \cup R, E)$ is a $(n, m, D, \gamma, \alpha)$ -expander and d -right regular, and C_0 is $[d, l, \Delta]$ (denoting [length of codeword, dimension, distance]) linear code, then $X(G, C_0)$ has distance γn if $\alpha > \frac{D}{\Delta}$.

Proof Assume towards a contradiction that there exists some codeword $c \in X(G, C_0)$ with $wt(c) < \gamma n$. Let $S = \text{supp}(c) \subset L$ be the set of vertices on the left of G corresponding to the locations of 1s in c .

Observe that $|N(u) \cap S| \geq \Delta$ for all $u \in N(S)$, since $u \in N(S)$ we know that $c_{|N(u)}$ is non-zero and C_0 has distance Δ .

Summing $|N(u) \cap S| \geq \Delta$ over all $u \in N(S)$ we see that $D|S| \geq \Delta|N(S)|$ since $D|S|$ is the total number of edges leaving S . However, since G is an $(n, m, D, \gamma, \alpha)$ -expander and $|S| < \gamma n$, we know that $|N(S)| \leq \alpha|S|$. It follows that $\alpha \leq \frac{D}{\Delta}$, contradicting our assumption. ■

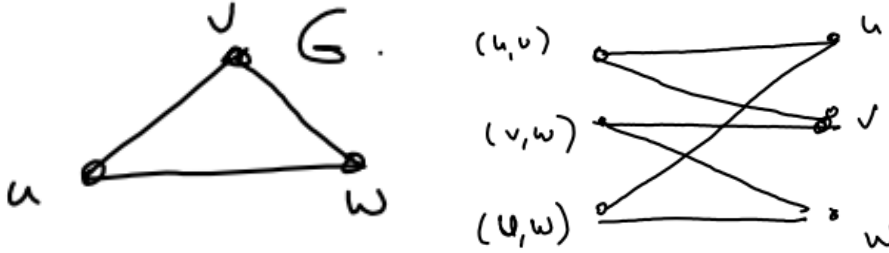
Recall that expander codes for which a set of size $< \gamma n$ expands by a factor of $D(1 - \epsilon)$, achieve a distance of $2\gamma(1 - \epsilon)n$. We will see that with Tanner codes we can achieve this same distance with a much smaller expansion ($D \rightarrow \frac{D}{d_0}$ where d_0 is the distance of C_0).

In order to achieve a high rate, we would like $\frac{m}{n}(d - \dim C_0)$ to be small. So, the number of constraints m should be small, and $\dim C_0$ should be large.

To Achieve this, we will construct Edge Vertex Incidence Graphs.

Definition 7 The Edge Vertex Incidence Graph of a given graph $G = (V, E)$ is a bipartite graph $H_0(G) = (L \cup R, E')$ such that

- $L = E$, each node on the left corresponds to an edge of G .
- $R = V$, each node on the right corresponds to a node from G .
- For each edge $e = (u, v) \in E$, we add the edges (e, u) and (e, v) to E' .



Observation 8 For any graph G , the edge vertex incidence graph $H_0(G)$ is 2-left regular.

Observation 9 If a given graph G is d -regular, then $H_0(G)$ is d -right regular.

Let's construct a Tanner code with this. Start with a d -regular graph G with N nodes and $\frac{Nd}{2}$ edges. Then

$$T(G, C_0) = X(H_0(G), C_0) = \{c \in \mathbb{F}_2^{Nd/2} \mid \forall v \in V, c_{|\Gamma(u)} \in C_0\}.$$

Where $\Gamma(u)$ denotes the set of edges adjacent to u in G .

2 Spectral Expanders

Definition 10 A graph $G = (V, E)$ is an (n, d, λ) -spectral expander if G is d -regular and $\lambda = \max(\lambda_2, |\lambda_n|)$ where $d = \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n \geq -d$ are the eigenvalues of the adjacency matrix of G .

The idea is that all eigenvalues, except for λ_1 , are sufficiently less than d .

Theorem 11 (Expander Mixing Lemma) For a (n, d, λ) -spectral expander graph $G = (V, E)$ and all $S, T \subseteq V$,

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

where $E(S, T)$ denotes the number of edges with one endpoint in each of S and T with double counting for edges that have both endpoints in $S \cap T$.

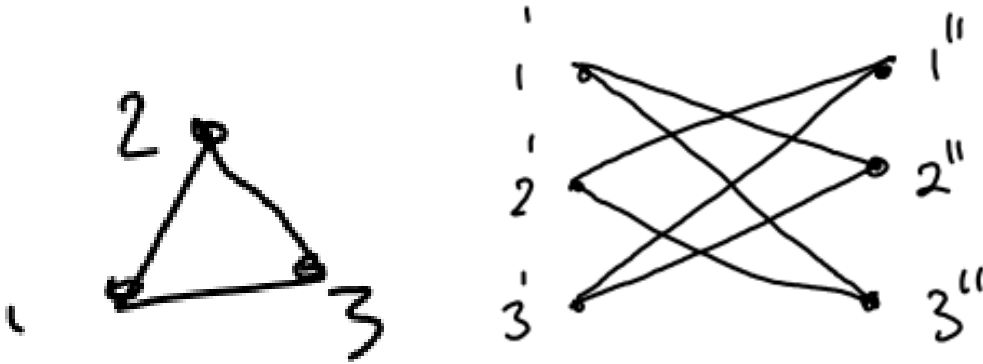
Proof omitted.

2.1 Bipartite Expanders from Spectral Expanders

We will convert spectral expanders with $\lambda = o(d)$ into bipartite expanders with $\alpha > 0$ using the *double cover* of the edge vertex incidence graph.

Definition 12 Given a simple graph $G = (V, E)$, the double cover of G is $DC(G) = (L \cup R, E')$ where

- $L = \{u' \mid u \in V\}$
- $R = \{u'' \mid u \in V\}$
- $E' = \{(u', v''), (u'', v') \mid (u, v) \in E\}$



Observation 13 If $G = (V, E)$ has n vertices and is d -regular, then $DC(G)$ has $2n$ vertices, nd edges, and is still d -regular.

Theorem 14 *Let X be an (n, d, λ) -spectral expander. Let $G = H_0(DC(X))$, that is the edge vertex incidence graph of the double cover of X . Then, for all β such that $\lambda \leq \beta \leq d$, then G is a d -right regular $(N = dn, m = 2n, 2, \frac{\beta(\beta-\lambda)}{d^2}, \frac{2}{\beta})$ -expander.*

Proof omitted.

Theorem 15 *Let $C_0 \subset \mathbb{F}_2^d$ have $\text{dist } \Delta(C_0) \geq \delta_0 d$ and rate $\rho > \frac{1}{2}$. Let G be an (n, d, λ) -spectral expander. Let $H = H_0(DC(G))$ be the edge vertex incidence graph of the double cover of G . Then for large enough d , $X(H, C_0)$ has rate at least $2\rho - 1$ and relative distance at least $\delta_0(\delta_0 - \frac{\lambda}{d})$.*

Proof By Theorem 14 we have that H is a $(N = nd, m = 2n, 2, \gamma = \frac{\beta(\beta-\lambda)}{d^2}, \frac{2}{\beta})$ -expander. So,

$$\begin{aligned} \dim X(H, C_0) &\geq dn - 2n(d - d\rho) \\ &= 2\rho nd - dn \\ &= (2\rho - 1)nd. \end{aligned}$$

So the rate is at least $2\rho - 1$.

Recall that we showed that if G is a d -right regular $(n, m, D, \gamma', \alpha')$ -expander and C_0 is $[d, l, \Delta]_2$ code then $X(G, C_0)$ has distance at least $\gamma'n$ if $\alpha' > \frac{D}{\Delta}$. So if $\frac{2}{\beta} > \frac{2}{\delta_0 d}$ (i.e. $\beta < \delta_0 d$), then the distance is at least $\frac{\beta(\beta-\lambda)}{d^2} dn$ and consequently the relative distance is at least $\frac{\beta}{d}(\frac{\beta}{d} + \frac{\lambda}{d})$. In the limit as $\beta \rightarrow \delta_0 d$, the relative distance $\delta > \delta_0(\delta_0 - \frac{\lambda}{d})$. ■

We can pick $\rho > 1 - h(\delta_0)$ at the GV Bound.

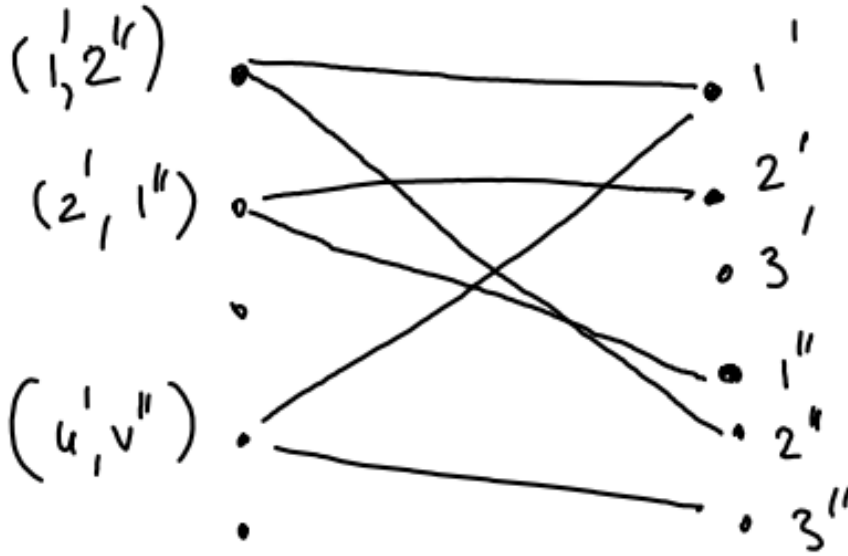
For large d , $\delta(X(H_0(DC(G)), C_0)) = \delta_0^2$ and $R(X(H_0(DC(G)), C_0)) \geq 2(1 - h(\delta_0)) - 1 \geq 1 - 2h(\sqrt{\delta_0}) > 0$ if $\delta < 0.001$.

2.2 Decoding

Sipser-Spielman first found a decoder from $\frac{\delta_0^2}{48}$ fraction of errors. In 2001, Zémor found a decoder from $\frac{\delta_0^2}{4}$ fraction of errors (about $\frac{1}{4}$ of the min distance).

Theorem 16 *We can decode in $O(n)$ time from $(1 - \epsilon)\frac{\delta_0}{2}(\frac{\delta_0}{2} - \frac{\lambda}{d})nd$ errors.*

First, consider the structure of $H' = H_0(DC(G))$.



We can see that each element of our codeword (a node on the right) is a part of exactly 2 constraints (nodes of the left), each part of separate halves of the left corresponding to the different copies of G produced when taking the double cover. Call these halves L and R .

Suppose that we received some codeword $y \in \mathbb{F}_2^{|E(H')|}$. Then for each $v \in L$ in parallel, we can correct $y_{|N(v)}$ to the nearest codeword in C_0 . We can do this in parallel since all $v \in L$ are independent. We then repeat the same process for each $v \in R$. We alternate correcting L and R until no errors remain.

It is possible to prove that we will reduce the number of errors by a constant fraction during each iteration, so the algorithm will terminate after $\theta(\log n)$ many iterations.