In this lecture we will construct asymptotically good codes without having to use code concatenation. We will do so by constructing codes from a smaller local code, and using the properties of the local code to prove global properties of the code we construct.

1 Tanner codes

Recall that any linear code C has a parity check matrix H_C, and that every row of H_C represents a parity check that a codeword in C must satisfy. The main idea behind Tanner codes is that we can replace (not necessarily contigious) blocks of check bits with a short local code, resulting in a global code in which the checks or constraints that codewords must satisfy depend solely on properties of our local code.

Definition 8.1. Given a r-right regular bipartite graph $G = (L, R, E)$ where $|L| = n$ and $|R| = m$, and a code $C_0 \subseteq \mathbb{F}_2^r$, we define the **Tanner code** of G and C_0 as

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

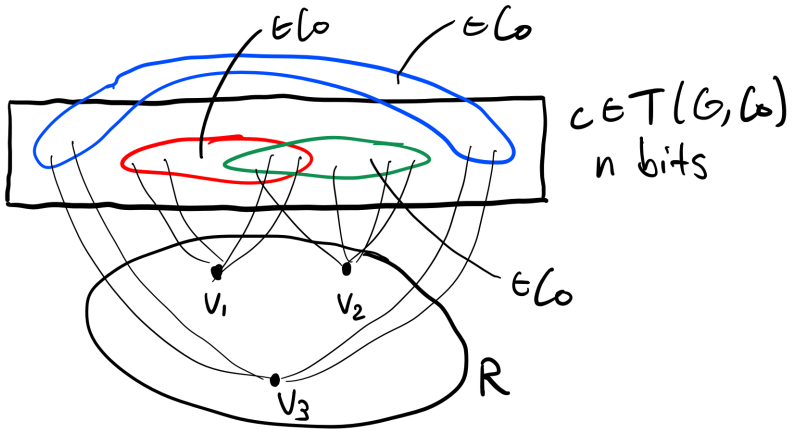

Figure 8.1: Visualization of a Tanner code.

We see that the Tanner code, when restricted to a small subset of indicies chosen according to its graph, is also an element of a smaller code.

Remark 8.2. If the local code C_0 is a parity check code then $T(G, C_0)$ has parity check matrix $M(G)$, the adjacency matrix of G.

Lemma 8.3. *If the local code C_0 is linear, then $T(G, C_0)$ is linear and we have*

$$\dim T(G, C_0) \geq n - m(r - dim(C_0)).$$

Proof. Given any set S, we have, for any $c_1, c_2 \in \mathbb{F}_2^n$, $(c_1 \restriction_S) + (c_2 \restriction_S) = (c_1 + c_2) \restriction_S$, so if $c_1, c_2 \in T(G, C_0)$, then $c_1 + c_2 \in T(G, C_0)$ as $c_1 + c_2$ will satisfy all local constraints given by any $u \in R$, so $T(G, C_0)$ is linear.

For any codeword $c \in T(G, C_0)$, the constraint $c \restriction_{N(u)} \in C_0$ can be written as $r - \dim(C_0)$ total linear constraints, where $r = \frac{m}{n}$. Since $|R| = m$, this means that we can have at most $m(r - \dim(C_0))$ linear constraints total, so the result follows. □

To construct Tanner codes from local code C_0, we must construct graphs with needed properties. One way to look at this is to take a r-regular graph G, and construct a factor graph G' defined to be the edge-vertex incidence graph of G.

Definition 8.4. Given a r-regular graph $G = (V, E)$ with $|V| = v$ and $|E| = \frac{vr}{2}$ the **edge-vertex incidence graph** of G is the bipartite graph $G' = (L, R, E')$ where $|L| = |E|, |R| = |V|$, and each vertex in L corresponds to an edge in E, and each vertex in R corresponds to a vertex in V. For any $e = (a, b) \in L = E$, we have $(e, a), (e, b) \in E'$.

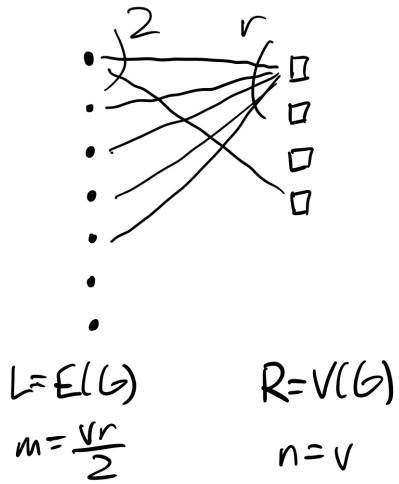

Figure 8.2: Edge-vertex incidence graph for a r-regular graph. Note that it is $(2, r)$-biregular.

We can view the bits of codewords of a Tanner code as edges on the edge-vertex incidence graph, where each vertex of G is a check/constraint on all edges (codeword bits) incident to that vertex. Then we have an equivalent definition of a Tanner code using this formulation:

Definition 8.5. Given an edge-vertex incidence graph G', we define the Tanner code as

$$X(G', C_0) = \{\mathbb{F}_2^E | \forall v \in V(G') : c \restriction_{N(v)} \in C_0\}.$$

Let R_0 and δ_0 be the rate and dimension, respectively, of C_0. We wish $X(G, C_0)$ to have rate $R(X(G, C_0))$ and relative distance $\delta(X(G, C_0))$ bounded away from zero.

By our previous lemma, we see that

$$\dim X(G, C_0) \geq \frac{vr}{2} - c(r - \dim C_0) = \frac{vr}{2} - c(r - R_0 r) \geq \frac{vr}{2}(2R_0 - 1)$$

so $X(G, C_0)$ is a linear code with block length $\frac{vr}{2}$ and rate $R(X(G, C_0)) \geq 2R_0 - 1$. So for the Tanner code we construct to have positive rate, we simply pick C_0 to be a linear code with $R_0 \in (\frac{1}{2}, 1]$.

Constructing a code with large relative distance ($\delta = \Omega(vr)$) is more difficult, and this requires us to pick an appropriate family of r-regular graphs to do our construction. Note that since the Tanner code is linear given linear C_0, bounding relative distance of $X(G, C_0)$ is equivalent to lower bounding the weight of all nonzero codewords $c \in X(G, C_0)$.

Suppose we pick a nonzero codeword $c \in \mathbb{F}_2^E$. Let $S = \{v | c \restriction_{E(v)} \neq 0\}$ be the set of all vertices touched by nonzero bits of c, and consider the subgraph $F = (S, \{f | c_f = 1\}$ of G. Observe that the minimum degree of F is at least $\delta_0 r$, and $wt(c) = |E(F)| \geq \frac{\delta_0 r |S|}{2}$. So for us to have $wt(c) \geq \delta = \Omega(vr)$, we require $|S| = \Omega(v)$.

Therefore, we want a graph G such that any small set S in $V(G)$ is not too isolated with respect to the rest of the graph, in that S has a large number of incident edges leaving the subgraph induced by S. Such a graph is called an expander graph, which we will formally define later on.

Notice that a random r-regular graph G on v vertices satisfies these properties: the expected number of edges from $|S|$ to itself is

$$\mathbb{E}[(S, S)] = \frac{r|S| \cdot |S|}{v} \geq \frac{\delta_0 r |S|}{2},$$

so we have

$$|S| \geq \frac{\delta_0 v}{2}.$$

As it is difficult to construct a random graph efficiently, we will show that pseudorandom graphs can be used to generate Tanner codes with distance bounded away from zero. Pseudorandom graphs are graphs whose edges are roughly randomly distributed, where the number of edges between any two (possibly equal) subsets of its vertices is approximately equal to the expected number of such edges,

$$\mathbb{E}[|E(S, T)|] = \frac{r|S||T|}{v}.$$

Definition 8.6. A graph $G = (V, E)$ with $|V| = v$ is **ϵ-almost random** if for all $S, T \subseteq V$,

$$\left| E(S, T) - \frac{r|S||T|}{v} \right| \leq \epsilon r \sqrt{|S||T|}.$$

Now suppose that we have a $\epsilon-$almost random graph G and consider the same set S from above. From the definition above, we have

$$\delta_0 r |S| \leq |E(S, S)| \leq \frac{r|S|^2}{v} + \epsilon r |S|.$$

Rearranging gives

$$\frac{r|S|}{v} \geq (\delta_0 - \epsilon) r,$$

or equivalently,

$$|S| \geq (\delta_0 - \epsilon) v.$$

Therefore we have

$$d(X(H, C_0)) = \min \widetilde{(c)} \geq \frac{\delta_0 r |S|}{2} \geq \delta_0 (\delta_0 - \epsilon) \frac{vr}{2},$$

so $\delta \geq \delta_0(\delta_0 - \epsilon)$.

2 Expander Graphs

Now that we have shown that $\epsilon-$almost random graphs generate Tanner codes with a large relative distance, we now desire to construct one. We will show that expander graphs, for which efficient constructions are known, are $\epsilon-$almost random.

Definition 8.7. Given a graph G with adjacency matrix $A(G)$, the **spectrum** of G is the set of real eigenvalues $\lambda_1, \cdots \lambda_v$ of $A(G)$.

Remark 8.8. Note that if G is a connected graph, then $\lambda_2 < \lambda_1$. If G is $r-$regular, then $\lambda_1 = r$.

Definition 8.9. A graph $G = (V, E)$ with $|V| = v$ is a $\lambda-$**spectral expander** if $\lambda = \max\{\lambda_2, |\lambda_v|\}$.

It turns out that spectral expanders and pseudorandom graphs are closely related, as shown by the following lemma:

Lemma 8.10. *(Expander Mixing Lemma)[AC88] If a r-regular graph G is a $\lambda-$spectral expander, then it is $\frac{\lambda}{r}-$almost random.*

Proof. Let A be the adjacency matrix of G and let $\lambda_1, \cdots \lambda_v$ be its eigenvalues with corresponding eigenvectors $u_1, \cdots u_v$. Since A is symmetric, we have $A = \sum_{i=1}^{v} \lambda_i u_i u_i^T$. Consider any two vertex sets $S, T \subseteq V$, with corresponding indicator vectors 1_S and 1_T for S and T, respectively. We see that

$$|E(S,T)| = 1_S^T A 1^T = \sum_{i=1}^{v} \lambda_i \langle 1_S, u_i\rangle\langle u_i, 1_T\rangle = \lambda_1\langle 1_S, u_1\rangle\langle u_1, 1_T\rangle + \sum_{i=2}^{v} \lambda_i \langle 1_S, u_i\rangle\langle u_i, 1_T\rangle.$$

We can write $1_S = \sum_{i=1}^{v} \alpha_i u_i = \frac{\alpha_1}{\sqrt{v}} 1^v + \sum_{i=2}^{v} \alpha_i u_i$ and $1_T = \sum_{i=1}^{v} \beta_i u_i = \frac{\beta_1}{\sqrt{v}} 1^v + \sum_{i=2}^{v} \beta_i u_i$ as linear combinations of eigenvectors of A. We have $\alpha_1 = \langle 1_S, u_1\rangle = \frac{|S|}{\sqrt{v}}$ and $\beta_1 = \langle 1_T, u_1\rangle = \frac{|T|}{\sqrt{v}}$, from which we get

$$|E(S,T)| = \lambda_1 \frac{|S||T|}{v} + \sum_{i=2}^{v} \lambda_i \langle 1_S, u_i\rangle\langle u_i, 1_T\rangle = \frac{r|S||T|}{v} + \sum_{i=2}^{v} \lambda_i \alpha_i \beta_i \leq \frac{r|S||T|}{v} + \lambda \sum_{i=2}^{v} \alpha_i \beta_i,$$

so by Cauchy Schwarz,

$$\left| |E(S,T)| - \frac{r|S||T|}{v} \right| \leq \lambda \sum_{i=2}^{v} \alpha_i \beta_i \leq \lambda \sqrt{\sum_{i=2}^{v} \alpha_i^2} \sqrt{\sum_{i=2}^{v} \beta_i^2} \leq \lambda \|1_S\| \|1_T\| = \lambda \sqrt{|S||T|}$$

and thus G is a $\frac{\lambda}{r}$-pseudorandom graph. □

Remark 8.11. The term *mixing* in the Expander Mixing Lemma refers to a property of random walks starting at an arbitrary vertex of a graph. The mixing time of a graph denotes the minimum number of steps it takes for the distribution of a random walk on that graph to be $\epsilon-$close to the uniform distribution. By showing that a r-regular $\lambda-$spectral expander mixes is a pseudorandom graph, we can see that expander graphs mix quickly (taking $O\left(\frac{\log v}{1-\frac{\lambda}{r}}\right)$ iterations to do so). Many known results in proving certain objects mix in a small number of iterations have been done by proving the object is an expander graph.

Since the relative distance is inversely to $\epsilon = \frac{\lambda}{r}$, we wish to find a graph where λ is significantly smaller than r. Note that λ cannot be arbitrarily small:

Theorem 8.12. *(Alon-Boppana Bound) [AHL02] For an r-regular graph G, $\lambda_2 \geq 2\sqrt{r-1} - o(1)$.*

Graphs that meet the Alon-Boppana Bound up to an $o(1)$ term are known as Ramanujan graphs:

Definition 8.13. A r-regular graph is **Ramanujan** if $\lambda_2 \leq 2\sqrt{r-1}$, and is $\epsilon-$**near Ramanujan** if $\lambda_2 \leq 2\sqrt{r-1} + \epsilon$.

It is known that near-Ramanujan graphs of any degree can be constructed efficiently [MOP20] so we can use them to construct Tanner codes. We showed above that $R(X(G, C_0)) \geq 2R_0 - 1$ and $\delta(X(G, C_0)) \geq \delta_0(\delta_0 - \epsilon)$, so we require local code C_0 to have rate $R_0 > \frac{1}{2}$ and relative distance $\delta_0 > \epsilon = \Omega(\frac{1}{\sqrt{r}})$. Note that given we have a code meeting the Gilbert-Varshamov Bound, this lower bound on δ_0 combined with $\delta_0 \approx h^{-1}(1 - R_0)$ requires R_0 to be sufficiently distant from 1.

3 Decoding Expander Codes

This will be covered in more detail in the next lecture. A high level overview of the decoding algorithm is that given some possibly corrupted message $y \in \mathbb{F}_2^E$, we decode according to the LHS of the factor graph by picking, for all $u \in L$, the local code c minimizing $d(c, y \restriction_{N(u)})$, correcting any errors that occur during this process, then repeating the same for all $v \in R$. This algorithm will converge in $O(\log n)$ given the number of errors is not too large.

References

[AC88] Noga Alon and F.R.K. Chung. Explicit construction of linear sized tolerant networks. *Discrete Mathematics*, 72(1):15–19, 1988. 8.10

[AHL02] Noga Alon, Shlomo Hoory, and Nathan Linial. The moore bound for irregular graphs. *Graphs and Combinatorics*, 18(1):53–57, 2002. 8.12

[MOP20] Sidhanth Mohanty, Ryan O'Donnell, and Pedro Paredes. Explicit near-ramanujan graphs of every degree. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 510–523, 2020. 2