Quantum Coding Theory **(UC Berkeley CS294, Spring 2024)**

Lecture 17: Tanner Codes

March 20, 2024

Lecturer: John Wright *Scribe: Sergio Escobar*

1 Tanner Codes

Quantum Tanner codes are based off of classical Tanner codes. A Tanner code is a classical code based off a graph G. A Tanner code can be defined on a generic graph or on a bipartite graph. We will use the bipartite graph approach. Let $G = (V, E)$, where $V = L \sqcup R$ and all edges in G are between L and R, i.e. $(u, v) \in E$ implies $u \in L, v \in R$ or vice-versa. We shall also assume that $|L| = n|R|$ and that G is r-regular.

The number of edges in G is $|E| = n \cdot r = |L| \cdot r = m$. We define $E(u)$ to be the set of edges incident to u. To each edge we shall associate a bit. Codewords are defined by the bit string attained from the bits associated to each edge. So, the codewords have length m.

Definition 1.1. Let $G = (L, R, E)$ be an r-regular bipartite graph. Let $C_0 \subset \{0, 1\}^r$ be a 'base' code. Then, a Tanner code is

$$TC(G, C_0) = \{c \in \{0, 1\}^{|E|} : \forall v \in L \cup R, c\big|_{E(v)} \in C_0\}.$$

That is, the Tanner code is the set of $|E|$-bit strings such that for each vertex, the bits associated to the edges incident to that vertex are in the base code C_0. It is implied that for each vertex there is a known ordering of the edges that decides the order of the bits.

Fact 1.2. *If C_0 is linear, then $TC(G, C_0)$ is linear.*

Proof. Let $c, c' \in TC(G, C_0)$. Note that for any v, we have $(c + c')\big|_{E(v)} = c\big|_{E(v)} + c'\big|_{E(v)} \in C_0$. □

Another way to see that the Tanner code is linear is by writing down its parity checks. Since C_0 is linear, there are $r - \dim(C_0)$ linearly independent parity checks. So, to check if a given string is a code word in the Tanner code, we just need to check that the edges on each vertex satisfy the parity checks. Since there are $2n$ vertices, there are at most $2n(r - \dim(C_0))$ linearly independent parity checks (we say at most, since it may turn out that some parity checks are implied by others).

Fact 1.3. *We have*

$$\dim(TC(G, C_0)) = \#\text{bits} - \#\text{linearly independent parity checks} \geq m - 2n(r - \dim(C_0)).$$

Write $\dim(C_0) = r \cdot R_0$ for $0 \leq R_0 \leq 1$. The bigger R_0 is, the better a code C_0 is since this means it encodes more bits. Then,

$$m-2n(r-\dim(C_0)) = nr-2n(r-\dim(C_0)) = nr(1-2(1-R_0)) = nr(2R_0-1) = m(2R_0-1).$$

So, if we want $\dim(TC(G, C_0)) \in \Omega(m)$, then we need $R_0 \in (\frac{1}{2}, 1]$.

We want the code to not only have good dimension but also good distance. Getting good dimension is fairly easy, as we just showed; getting good distance is harder. We have to be careful about what graphs we use. Suppose C_0 has good distance $\Delta_0 \cdot r$ and let $c \in TC(G, C_0)$ be nonzero. We want to argue that c has high (Hamming) weight, since this implies that the Tanner code has good distance.

Since c is nonzero, at least one edge e in the graph is assigned a 1. Let $e = (u, v) \in L \times R$ and note that since $c\big|_{E(u)} \in C_0$, we have $|c\big|_{E(u)}| \geq \Delta_0 \cdot r$. So, knowing that at least one edge incident to $u \in L$ is assigned a 1 implies that many edges are assigned 1. Each outgoing edge with a 1 on it meets a vertex $v_i \in R$, $i = 1, \ldots, \Delta_0 \cdot r$. Applying the same argument to the vertices v_i shows that c must have very high weight, however this only holds if most of the edges with a 1 incident to each v_i all meet different vertices in L. That is, it may be the case that the graph has two sets of vertices $S \subset L$ and $T \subset R$ that only share edges with each other.

So, the idea is to look for graphs such that for small sets $S \subset L, T \subset R$, most edges from S go outside of T, i.e. $E(S, T) = \{\text{edges between } S \text{ and } T\}$ is small. This will prevent the bad situation from before where all edges with weight 1 are shared between two small sets. A good place to start is to look at random graphs.

Let G be a random r-regular bipartite graph. We calculate

$$\mathbf{E}[|E(S, T)|] = |S| \cdot r \cdot \frac{|T|}{n},$$

this follows since $|S| \cdot r$ is the number of edges coming out of S, and $|T|/n$ is the average fraction of those edges that go into T.

Definition 1.4. We say that a graph $G = (L, R, E)$ is ε-pseudorandom if $\forall S \subset L, \forall T \subset R$, we have

$$\left| |E(S, T)| - |S| \cdot r \cdot \frac{|T|}{n} \right| \leq \varepsilon r \sqrt{|S| \cdot |T|}.$$

Observe that we allow the 'error' to be larger if $r, |S|$, or $|T|$ is large.

Assuming that G is ε-pseudorandom, we show that the Tanner code $TC(G, C_0)$ has good distance. Set $S = \{u \in L : c\big|_{E(u)} \neq 0\}$ and $T = \{v \in R : c\big|_{E(v) \neq 0}\}$. Observe that $|c| \geq \max\{|S| \cdot \Delta_0 \cdot r, |T| \cdot \Delta_0 \cdot r\}$, so in particular, $|c| \geq \sqrt{|S| \cdot |T|}\Delta_0 \cdot r$. We show that most edges with a 1 go between S and T and hence $\sqrt{|S| \cdot |T|}\Delta_0 \cdot r \leq |c| \leq |E(S, T)|$.

By the ε-psuedorandomness, we have

$$\begin{aligned}&\Delta_0 r\sqrt{|S|\cdot|T|} \le |c| \le |E(S,T)| \le \frac{r}{n}|S|\cdot|T| + \varepsilon r\sqrt{|S|\cdot|T|}\\ &\Rightarrow (\Delta_0-\varepsilon)r\sqrt{|S|\cdot|T|} \le \frac{r}{n}|S|\cdot|T|\\ &\Rightarrow (\Delta_0-\varepsilon)n \le \sqrt{|S|\cdot|T|}.\end{aligned}$$

So, either $|S|$ or $|T|$ is very large. Also, observe that this implies

$$|c| \ge \Delta_0 r\sqrt{|S|\cdot|T|} \ge \Delta_0 r(\Delta_0-\varepsilon)n = \Delta_0(\Delta_0-\varepsilon)m.$$

So, if the base code has constant distance Δ_0 and the underlying graph is ε-pseudorandom with $\varepsilon < \Delta_0$, then the distance of the Tanner code = const$\cdot m$.

2 Expander Graphs

Intuitively, an expander graph is a graph in which any small set of vertices has a large neighborhood.

Fact 2.1. *Let $G = (V, E)$ be a graph. Its adjacency matrix is given by*

$$A(G) = \begin{cases} 1 & \textit{if } (u,v) \in E) \\ 0 & \textit{otherwise,} \end{cases}$$

where the rows and columns are indexed by the vertices in V. We observe that $A(G)$ is an $n \times n$ real, symmetric matrix and therefore has eigenvalues $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_n$.

Fact 2.2. *If G is r-regular, the vector $v = [1\ 1\ \dots\ 1]^T$ is an eigenvector with eigenvalue $\lambda_1 = r$.*

Proof. Since G is r-regular, each row has exactly r entries equal to 1 and the rest are 0. So, $A(G)v = rv$. □

Definition 2.3. A graph G is a λ-spectral expander if $\lambda = \max\{\lambda_2, |\lambda_n|\}$ is small.

Example 2.4. *Consider a graph G with k connected components $V_1, \dots, V_k$. Then, there are k eigenvectors of the form $v_j = [a_1\ \dots\ a_n]^T$ where $a_i = 1$ if and only if $i \in V_j$, i.e. the vector which is 1 only on the vertices in V_j. The associated eigenvalues are $|V_j|$. So, if there are at least two large connected components, the largest two eigenvalues are not small and so G is not an expander.*

Definition 2.5. The double cover of a graph $G = (V, E)$ is a bipartite graph $G' = (V_L, V_R, E')$ where $|V_L| = |V| = |V_R|$. To each edge $v \in V$, we associate a vertex $v_L \in V_L$ and a vertex $v_R \in V_R$. We have that $(u_L, v_R) \in E' \subset V_L \times V_R$ if and only if $(u, v) \in E$. The bipartite adjacency matrix of the double cover has its rows indexed by vertices in V_L and the columns indexed by the vertices in V_R, with a 1 entry if and only if $(v_L, v_R) \in E'$. In particular the bipartite adjacency matrix of G' is just the adjacency matrix $A(G)$ of G.

Fact 2.6. *If $G = (V, E)$ is a λ-spectral expander, then its double cover is $(\frac{\lambda}{r})$-pseudorandom.*

Proof. Let $A(G)$ be the adjacency matrix of G and expand it in an eigenbasis.

$$A(G) = \sum_{i=1}^{n} \lambda_i \left|v_i\right\rangle \left\langle v_i\right| ,$$

where we know that $\lambda_1 = r$ and we normalize $\left|v_1\right\rangle = \frac{1}{\sqrt{n}}[1 \ \ldots \ 1]^T = \frac{1}{\sqrt{n}}(\left|1\right\rangle + \cdots + \left|n\right\rangle)$. Let $S, T \subset V$ and define

$$\left|S\right\rangle = \sum_{i \in S} \left|i\right\rangle .$$

Then,

$$\begin{aligned}
|E(S,T)| = \left\langle S\right| A(G) \left|T\right\rangle &= \sum_{i=1}^{n} \lambda_i \left\langle S|v_i\right\rangle \left\langle v_i|T\right\rangle \\
&= \lambda_1 \left\langle S|v_1\right\rangle \left\langle v_i|T\right\rangle + \sum_{i\geq 2} \lambda_i \left\langle S|v_i\right\rangle \left\langle v_i|T\right\rangle \\
&= \frac{r}{n}|S| \cdot |T| + \sum_{i\geq 2} \lambda \left\langle S|v_i\right\rangle \left\langle v_i|T\right\rangle
\end{aligned}$$

Therefore,

$$\begin{aligned}
\left| |E(S,T)| - \frac{r}{n}|S| \cdot |T| \right| &= \left| \sum_{i\geq 2} \lambda_i \left\langle S|v_i\right\rangle \left\langle v_i|T\right\rangle \right| \\
&\leq \sum_{i\geq 2} |\lambda_i| \cdot | \left\langle S|v_i\right\rangle | \cdot | \left\langle v_i|T\right\rangle | \\
&\leq \lambda \sum_{i\geq 1} | \left\langle S|v_i\right\rangle | \cdot | \left\langle v_i|T\right\rangle | \\
&\leq \lambda \sqrt{\sum_{i\geq 1} | \left\langle S|v_i\right\rangle |^2} \sqrt{\sum_{i\geq 1} | \left\langle v_i|T\right\rangle |^2} \\
&= \lambda \sqrt{\sum_{i\geq 1} \left\langle S|v_i\right\rangle \left\langle v_i|S\right\rangle} \sqrt{\sum_{i\geq 1} \left\langle T|v_i\right\rangle \left\langle v_i|T\right\rangle} \\
&= \lambda \sqrt{\left\langle S|S\right\rangle} \sqrt{\left\langle T|T\right\rangle} \\
&= \lambda \sqrt{|S| \cdot |T|} \\
&= \frac{\lambda}{r} r \sqrt{|S| \cdot |T|}.
\end{aligned}$$

□

Example 2.7. *Another example of a graph which is not an expander graph is any r-regular bipartite graph. By regularity, $|L| = |R|$, so the vector $v = [1\ 1\ \ldots\ -1\ -1]^T$ (the 1's are in positions indexed by vertices in L and the -1's are in positions indexed by vertices in R) is an eigenvector with eigenvalue $-r$.*

We care about expander graphs since there are known efficient algorithms for generating expander graphs. Recall the distance of the Tanner code is given by $\Delta_0(\Delta_0 - \varepsilon)m$, while the dimension is $m(2R_0 - 1)$. So, if the inner code has good distance Δ_0 and rate R_0, our work above shows that we can efficiently generate a good Tanner code.