Lecture 16

Lecturer: Madhu Sudan *Scribe: Reina Riemann*

1 TOPICS

- Tanner Products and Sipser-Spielman codes.
- Linear time encodable & decodable codes.
- Decoding in linear time (Data structure exercise).

2 Tanner product generalization

Remember that for a (γ, δ) expander graph, $|S| \leq \delta \cdot n$ and the neighborhood of S, $\Gamma(S) \geq \gamma|S|$. This implies that for a c-left regular graph with $\gamma > c/2$, the corresponding code has minimum distance$\geq \delta \cdot n$.

We'll look at Tanner's construction in order to go past the $\frac{c}{2}$ barrier. Tanner's generalization uses a $d-right$ regular bipartite graph, together with a small code $B = [d, l, \Delta]$. An assignment to the left is a codeword of $C = C(G, B)$ if every right vertex sees a codeword of B. This imposes $d-l$ new constrains, so the total number of constrains is $n - m(d-l)$ where n is the number of vertices on the left of the bipartite graph and m is the number of vertices on the right. We also have that $c \cdot n = d \cdot m$. Therefore $n - m(d-l) = n(1 - (c/d)(d-l))$.

Consider the following partition of $\Gamma(S) = A \cup B$, where A has$\leq (\Delta - 1)$ neighbours and B has $\geq \Delta$in S. It follows that:

$$\begin{aligned} |A| + |B| &\geq \gamma \cdot |S| \\ |A| + \Delta|B| &\leq \#\,of\,edges\,of\,S \leq c \cdot |S| \\ (\Delta - 1)|A| &\leq (\triangle\gamma - c)|S| \end{aligned}$$

Construction yields code $C(B, G)$ of minimum distance $\delta \cdot n$ provided $\gamma > \frac{c}{\Delta}$.

- First, pick c,γ, then we can build $\forall d\, \exists \delta > 0, \forall n$,$(c, d)$ regular graphs that are (γ, δ) expanders.
- Set $\Delta > \left\lceil \frac{c}{\gamma} \right\rceil$
- Pick (d, l) such that $d > c(d-l)$, $\exists [d, l, \Delta]_2$code (so that $d > \Delta log(d)$) guaranteed.
- $\exists \delta$ such that $\exists (c, d)$ regular (γ, δ) expander that we can construct.

3 Parallel-flip algorithm

In parallel, every right vertex acts as follows:

- If neighbors form codeword of B, then ok
- If neighbors are at a distance $\leq \varepsilon\Delta$, then send a flip message to these neighbors.
- If neighbors are at a distance $\geq \varepsilon\Delta$, then do nothing

Note that at each iteration the number of bits in error reduces by a constant fraction.

4 Spielman codes

With the Sipser-Spielman codes, the n^2 encoding time takes more than the linear decoding. The Spielman codes have both linear time encoding and decoding. The main idea is to use error-reduction codes. Expanders are used in the spielman construction, but this time the expander is associated with the generator matrix rather than the parity-check matrix. These codes are systematic, i.e. the encoding contains the message bits followed by the check bits. These codes are called "Cascade codes" because of their recursive structure. The encoding is determined by a graph G with $log(k)$layers, where k is the number of bits in the message, and each of the layers of G is low density.

Error-reduction codes

- R_k: message→$(message, check-bits)$
- k message bits →3·k/2 codeword bits
- m'→(m',c')

Property: If the distance$\triangle(c', c) \leq t \leq\delta \cdot k\Rightarrow \Delta(m', m) \leq t/2$

Spielman Codes $C_k : m \rightarrow (m,\ x)$ where $|x| = 3k$ that is, k message bits get encoded into $4k$ codeword bits

Encoding C_k

- Apply $R_k(m) = (m, c)$, where $|c| = k/2$
- Apply $C_{k/2}(c) = (c, y)$, where $|y| = 3 \cdot k/2$
- Apply $R_{2k}(c, y) = ((c, y),\ z)$,where $|z| = k$
- All of the above imply that $C_k(m) = (m,(c, y, z))$, where $|c, y, z| = 3k$

Distance of C_k

$\Delta(m,(c, y, z)),(m',(c', y', z'))) < \delta k$

then$\Delta(z, z') < \delta k$

By R_{2k}, $\Delta((c', y'),(c, y)) < \delta k/2$

By $C_{k/2}$, $(c', y') = (c, y)$

By R_k, $c' = c$

Next time we'll cover the error-reduction algorithm.