6.440 Essential Coding Theory April 14, 2008

Lecture 18

Lecturer: Madhu Sudan *Scribe: Elena Grigorescu*

In the previous lecture we introduced expander codes and showed some general existential results, and discussed the rate and distance of such objects. Today's lecture will detail the Sipser-Spielman decoding algorithm for Tanner codes, which are generalizations of the Gallager type expander codes.

1 Notations and main results from last lecture

Let $G = L \cup R$ be a bipartite graph with n left vertices and m right vertices. Then G corresponds to a binary code C_G with block length n, and dimension $k \geq n - m$, where the left vertices correspond to variables $x_1, \ldots, x_n \in \{0, 1\}$, while the right vertices $c_1, \ldots, c_m$ correspond to constraints, such that c_i is *satisfied* iff $\sum_{u \leftrightarrow c_i} x_u = 0$. Let SAT be the set of satisfied constraints, and UNSAT be its complement in R. For $u \in L$ let $sat(u)$ be the number of satisfied constraints that u is adjacent to, and let $unsat(u)$ be the number of unsatisfied such constraints.

The graph G is (c, d)-*bounded* if the left degrees are at most c and the right degrees are at most d. Let $\Gamma(S) = \{v \in R \mid \exists\, u \in S,\ u \leftrightarrow v\}$. G is a (γ, δ)-*expander* if: $\forall S \subseteq L$ s.t. $|S| < \delta n$, it is the case that $|\Gamma(S)| > \gamma|S|$. We assume $\gamma > 1$. We also needed a special subset of $\Gamma(S)$ namely, the set of vertices with unique neighbors in S, denoted $\Gamma^+(S) = \{v \in R \mid \exists\,!\ u \in S,\ u \leftrightarrow v\}$. As before, G is a $(\tilde{\gamma}, \delta)$- *unique neighbor expander* if: $\forall S \subseteq L$ s.t. $|S| < \delta n$, it is the case that $|\Gamma^+(S)| > \tilde{\gamma}|S|$.

We showed last time the existence of such expander codes and exhibited a relation between the expansion parameters of the underlying graph G and the relative distance $\delta(C_G)$ of the resulting Gallager code. We could thus obtain binary codes with rate > 0 and relative minimum distance > 0, which is a non-trivial task.

Theorem 1 *Let c, d be constants, and let $\gamma < c$ and $\delta = \Omega(1) > 0$. Then there exists (c, d)- bounded (γ, δ) expanders.*

Theorem 2 *If G is a (c, d)- bounded, (γ, δ) - expander then $\delta(C_G) \geq \delta$.*

The proof used the following key lemma.

Lemma 3 *If G is a (c, d)-bounded (γ, δ)- expander, then G is also a $(2\gamma - c, \delta)$- unique neighbor expander, provided that $\gamma > c/2$.*

2 Decoding in linear time

In his initial paper, Gallager (1964) gave a decoding algorithm for LDPC codes, but his algorithm was difficult to analyze. Later on, Sipser and Spielman (1994) showed a much simpler and easier to analyze decoding algorithm for Tanner codes, which can be viewed as generalization of LDPC codes. We will start with their algorithm applied to LDPC codes and later on we will sketch its analysis for Tanner codes.

Given: a received vector $x = x_1 \ x_2 \ \ldots \ x_n$
Goal: find the transmitted codeword $w = w_1 w_2 \ldots w_n \in C_G$ s.t. $\Delta(w, x) \leq pn$, for some $p = O(1)$ to be chosen later.

```
FLIP :
1.Initialize :   $y \leftarrow x$
2.Iterate :      while there exists $u \in L$ s.t. $unsat(u) > sat(u)$, flip $u$.
3.Output :       $y$.
```

Theorem 4 *If the number of errors $\Delta(w, x) < \alpha n$, for some constant $0 < \alpha < 1$, then on input x, the FLIP algorithm terminates in time $O(n)$, and outputs the correct codeword w (under some constraints on α, and on the expansion parameters of G).*

Proof

Suppose the received word x is within e errors of some codeword w, so $e = \Delta(w, x)$. Further suppose $\gamma > \frac{3}{4}c$.

Claim 5 *FLIP terminates in ce iterations.*

Proof It is easy to notice that FLIP terminates in m iterations. Indeed, at each iteration, by flipping a left bit we must increase the number of satisfied constraints by at least 1 To show the stronger result of the claim, let $S = \{i \mid x_i \neq w_i\}$. Notice that only the vertices in $\Gamma(S)$ are initially possibly unsatisfied. Thus, initially $UNSAT \subseteq \Gamma(S)$ which implies that $|UNSAT| \leq |\Gamma(S)| \leq ce$, concluding that the algorithm terminates in at most ce iterations. ■

Claim 6 *If x is within $e = \Delta(x, w)$ from w and $e < \frac{\delta}{c+1}n$, then FLIP terminates in the codeword w.*

Proof First notice that since at each step at most 1 bit of y is being flipped, in the final step ec we must have that $\Delta(y, w) \leq \Delta(x, w) + ce < (c+1)e < \delta n$.

At the beginning of the final iteration step let $S_f = \{i \mid y_i \neq w_i\}$. Suppose for a contradiction that $S_f \neq \emptyset$. By Lemma 3 our (c, d)-bounded, (γ, δ)- expander is also a $(2\gamma - c, \delta)$-unique-neighbor-expander. Since $|S_f| = \Delta(y, w) < \delta n$, we obtain that $|\Gamma^+(S_f)| \geq (2\gamma - c)|S_f| \geq \frac{c}{2}|S_f|$. Since $\Gamma^+(S_f) \subseteq UNSAT \subseteq \Gamma(S_f)$, on average, a vertex in S_f has more than $\frac{c}{2}$ unsatisfied neighbors in $\Gamma(S_f)$. This implies that there is a vertex $v \in S_f$ with more than $\frac{c}{2}$ neighbors in $\Gamma(S_f)$, and since v has at most c neighbors, v must have more unsatisfied constraints than satisfied ones, and therefore it must be flipped. This contradicts the fact that we were in the final step of the algorithm, and implies that $|S_f| = 0$ and that the output is the correct codeword w. ■

■

3 A short history of expanders

We know that existentially, the following parameters are achievable: $c, d = O(1)$, $\gamma < c$ and $\delta < \frac{1}{c}\frac{m}{n}$. A line of research has focused on explicit constructions of good expanders, starting with Grabber and Garil (1980), and independently Margulis, whose constructions achieved $\gamma > 0$ and $\frac{c}{d} < 1$. Tanner (1984) improved some of the parameters, and later Lubotsky, Phillips and Sarnak, and independently Margulis, obtained constructions for any c, d, and for $\frac{\gamma}{c} \to \frac{1}{2}$, with $\delta = O(1) > 0$. In a major breakthrough, Capalbo, Reingold, Vadhan and Wigderson (2001) obtained results of the type: $\forall \frac{\gamma}{c} < 1, \exists c$, s.t. $\forall d$, $\exists \delta, n_0$ s.t. $\forall n > n_0$ one can construct a (c, d)-bounded, (γ, δ)-expander on n vertices. Notice that our previous analysis for FLIP can only be applied to expanders satisfying $\gamma > \frac{3}{4}c$ and therefore, those obtained by the latter authors. The original Sipser-Spielman algorithm used Tanner type codes, which can be viewed as generalizations of LDPC codes. In the following section we introduce Tanner codes and a decoding algorithm for expanders with $\frac{\gamma}{c} < \frac{1}{2}$.

4 Tanner codes and their decoding

Let $G = L \cup R$, with $|L| = n$ and $|R| = m$, be (c, d)-bounded, (γ, δ)-expander and let $C_{small} = [d, l, \Delta]$ be a small code, where $d = O(1)$, $l \leq d$. Denote by $\mathcal{C} \times C_{small}$ the following graph (code). For each vertex $v \in R$ its outgoing edges to the variables are given in a fixed order, say $(x_{i_1}, x_{i_2}, \ldots, x_{i_d})$. An assignment $(x_1, x_2, \ldots, x_n)$ is a codeword of $\mathcal{C}$ iff, for each constraint $v \in R$ we have that its corresponding ordered variables satisfy $(x_{i_1}, x_{i_2}, \ldots, x_{i_d}) \in C_{small}$.

Lemma 7 *$\mathcal{C} = G \times C_{small}$ has Rate $> 1 - (d - l)\frac{c}{d}$ and Distance $\geq \delta$, provided $\gamma > \frac{c}{\Delta}$.*

Proof We count the number of unconstrained coordinates of L. Each vertex on the right can constrain at most $d - l$ coordinates. Thus Rate $> 1 - (d-l)\frac{m}{n} \geq 1 - (d - l)\frac{(cn/d)}{n}$. The distance statement can be obtain in the same way as in the previous lectures and we omit it here. ■

In the '90s, as described before, explicit expanders were known for the following setting of parameters: given $\frac{\gamma}{c} < \frac{1}{2}$, $\exists c$ s.t. $\forall d, \exists \delta, n_0$ s.t. $\forall n, n_0$ one could build a n-vertex expander. To decode these codes Sipser and Spielman proposed a parallel variant of FLIP.

```
Parallel FLIP   ( parameter $t \ll \Delta$) :
1.Initialize :  $y \leftarrow x$
2.Iterate :     (a) Every constraint that is at distance $\leq t$ from a codeword of $C_{small}$
                 sends flip messages to the variables in error.
                 (b) In parallel, every variable that received a flip message flips.
3.Output :      $y$, when all constraints are satisfied.
```

Lemma 8 *The number of variables in error reduces by a constant factor in each iteration.*

Proof Sketch:

Let $S = \{v \in L \mid y_v \neq c_v\}$ be the set of variables in error. Let $U = \{u \in R \mid |\{v \in S, v \leftrightarrow u\}| \leq t\}$. Let $F = \{v \in L \mid v \text{ receives flip message}\}$.

Claim 9 *Each constraint in U sends flip messages only to variables in S.*

Proof The vertices in U are at distance $\leq t$ from C_{small} and thus they must send flip messages exactly to those vertices in S that are in error. ■

The vertices in U send correct flip messages, and we have that the set of variables receiving correct flip messages has size $|S \cap F| \geq \frac{|U|}{c} \geq \frac{1}{c}\frac{t\gamma - c}{t-1}|S|$ which tends to $\frac{\gamma}{c}|S|$ for fixed γ, c, and fixed large t, Δ, d.

We now bound the number of incorrect flip messages received. Notice that a constraint v will send a flip message to a vertex outside S only if it sees too many vertices in S. Since such a constraint is at distance t from some codeword of C_{small} it follows that v is adjacent to at least $\Delta - t$ bad vertices of S. Then $|F - S| \leq \frac{c|S|}{\Delta - t}t$, which tends to 0 under the same settings of the parameters as above.

This concludes that at each iteration, the number of vertices in error decreases by a factor of $\frac{\gamma}{c}$.