5TO8 LECTURE 18

Note Title 4/14/2008

TODAY :- Tanner Codes

- Sipser - Spielman Decoding

Recall LDPC Codes

Bipartite Graph $\longrightarrow$ Code

$G = (L, R, E) \longrightarrow C_G$

n left vertices $\longrightarrow$ block length n

m right vertices $\longrightarrow k \geq n - m$

Every right vertex v is a constraint ..

Assignment $x_1 \ldots x_n$ to variable (left vertices) must satisfy $\bigoplus_{u \leftrightarrow v} x_u = 0$.

- (c,d)-bounded: left degrees $\le c$
  right degrees $\le d$
- (γ,δ)-expander: $\forall S \subseteq L$ s.t. $|S| \le \delta n$
  $|\Gamma(S)| \ge \gamma \cdot |S|$
- $(\tilde{\gamma},\delta)$-unique expander: $\forall S \subseteq L$ s.t. $|S| \le \delta n$
  $|\Gamma^+(S)| \ge \tilde{\gamma} \cdot |S|$
  - $\Gamma(S) = \{ v \mid \exists u \in S \text{ s.t. } u \leftrightarrow v \}$
  - $\Gamma^+(S) = \{ v \mid \exists!\, u \in S \text{ s.t. } u \leftrightarrow v \}$

<u>Lemma</u>: (c,d) bounded, (γ,δ) expander is also a $(2\gamma - c, \delta)$-unique expander

<u>Theorem</u>: G is (c,d) bounded, (γ,δ) expander & $2\gamma > c \Rightarrow C_G$ has rel. dist. δ.

Decoding Algorithm

FLIP

- Starting with assignment $x_1 \dots x_n$ to variables
- Iteratively maintain assignment $y_1, \dots, y_n$.
  (initially $\bar{y} \leftarrow \bar{x}$)
- In Iteration i
  - Constraint v is sat. if $\bigoplus_{u \leftrightarrow v} x_u = 0$
    & unsat. o.w.
  - if $\exists u$ with more unsat. neighbours than sat. ones then $y_u \leftarrow \bar{y}_u$
    (else STOP; output $\bar{y}$)   flip it.

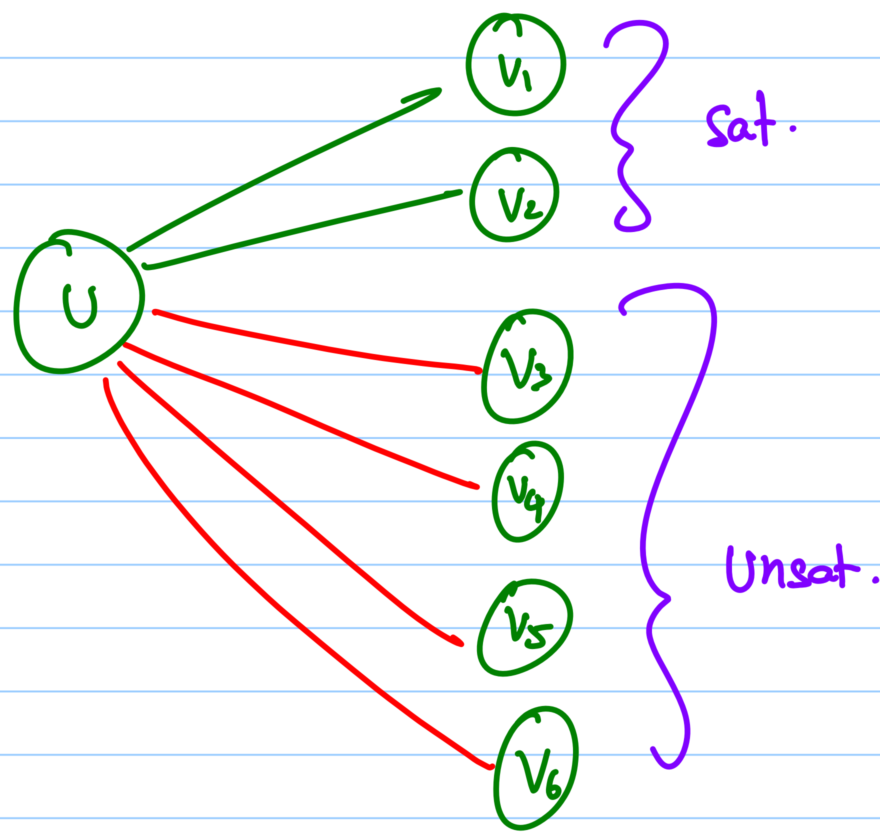
Analysis [Assume $\gamma > \frac{3}{4} \cdot c$]

Claim 1: Algorithm terminates in m iterations

$\Uparrow$

Claim 1': if # errors $= e$ then algorithm terminates in $< c \cdot e$ iterations.

Proof: - Consider a vertex about to be flipped



- Flipping toggles sat vs. unsat status of neighbors of v. Status of all other constraints unchanged

- Conclude: Total # unsat. vertices decreases in each iteration (since v has more unsat ngbrs than sat. ones).

- Initially # unsat ngbrs. $\leq m$ $\boxed{\Rightarrow \text{Claim 1}}$

$$\leq c \cdot e$$

$\Uparrow$

must be neighbor of some corrupted bit.

$\boxed{\Rightarrow \text{Claim 1}'}$

$\boxtimes$

- So we know algorithm terminates quickly.
- But does it terminate in right codeword?

Claim 2: if $e = \Delta(\underset{\text{codeword}}{\bar{c}}, \underset{\text{received word}}{\bar{x}}) < \frac{\delta n}{c+1}$

then alg. terminates with all constraints sat.

Claim 2.1: if $e = \Delta(\bar{c}, \bar{x}) < \frac{\delta n}{c+1}$

then throughout $\Delta(c, y) < (c+1) \cdot e$

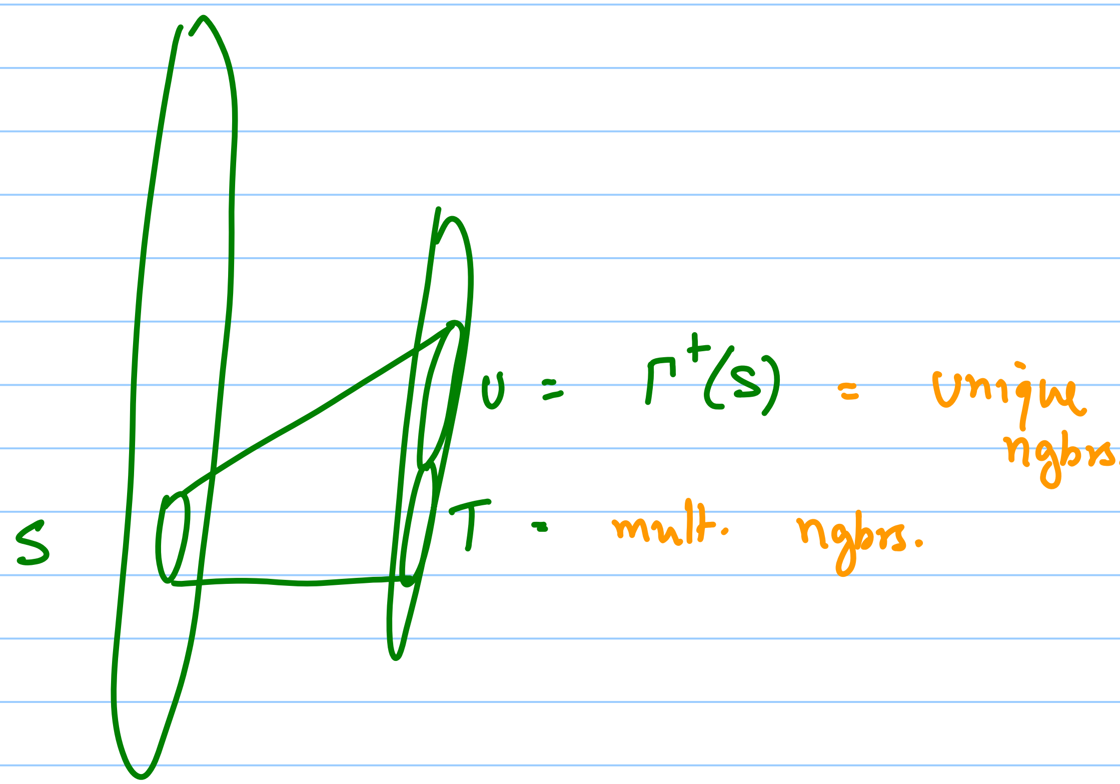
Proof of Claim 2.1: In each iteration $\Delta(c, y)$ increases by at most 1. Initially $\Delta(c, y) = \Delta(c, x) = e$. # Iterations is at most $c \cdot e$ (Claim 1').

$\boxtimes$

Proof of Claim 2: At beginning of iteration i (in particular, in final iteration) ...,

let $S = \{ v \mid y_v \neq c_v \} \neq \phi$

$\uparrow$ erroneous locations. $\qquad \uparrow$ for contradiction



$|S| \leq (c+1)e < \delta n$

$\Rightarrow |\Gamma^+(S)| \geq (2\gamma - c) \cdot |S|$

$> \frac{c}{2} \cdot |S|$

- But this implies some vertex $v \in S$ must have $> \frac{c}{2}$ neighbours in $\Gamma^+(S)$
- For this vertex v every nghr in $\Gamma^+(S)$ is unsat & those are more than # other vertices.

Conclude: $|S| \neq \phi \Rightarrow \exists$ flippable vertex v. $\boxtimes$

Claim 3: If $\Delta(c, x) = e < \frac{\delta n}{c+1}$ then algorithm terminates with c

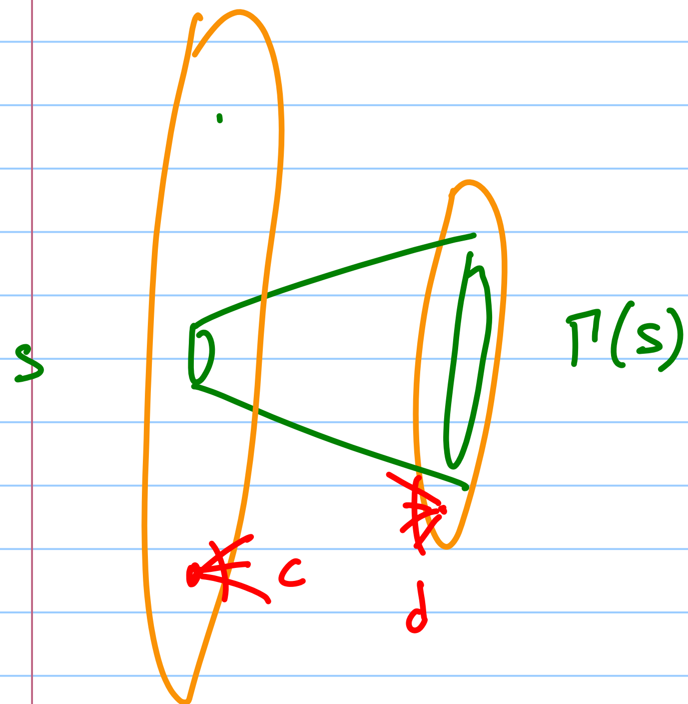
Proof: Else alg outputs $\bar{c} \in C_G$ with

$$\Delta(c, \bar{c}) \leq (c+1) e < \delta n$$

$\uparrow$

contradiction $\boxtimes$

Expander Graphs & Explicit Constructions



What kind of expanders exist?

Any $c, d = O(1)$; $n \to \infty$

$\gamma \to c$ & $\delta < \frac{1}{c} \cdot \frac{m}{n}$

achievable existentially ...

but what about constructive stuff?

History

[Gabber-Galil] - first constructive results

$\gamma > 0$, $\frac{c}{d} < 1$

[Margulis]

[Tanner '84]

⋮

[Lubotsky, Phillips, Sarnak]
[Margulis]
$\Big\}$ $\frac{\gamma}{c} \to \frac{1}{2}$

↑

just short of being useful!

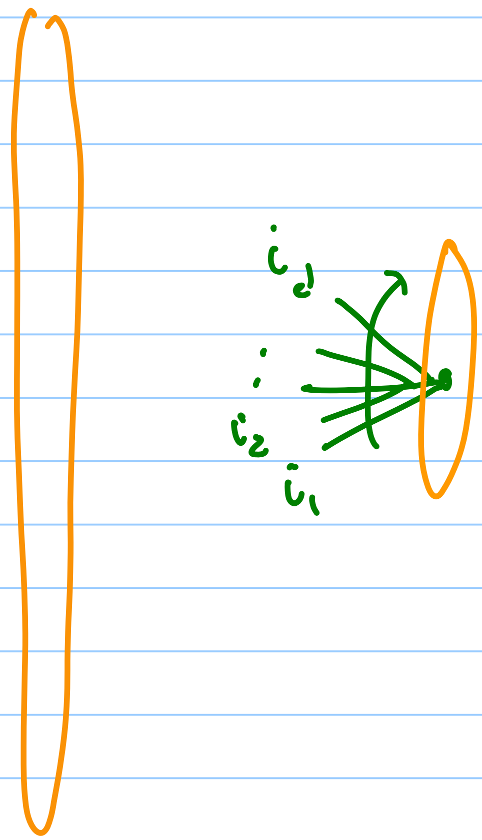
(What can you do with above?)

[2001] [Capalbo, Reingold, Vadhan, Wigderson]: Can get $\frac{\gamma}{c} \to 1$.

[Inner]: Recursive construction: $G \oplus C_{small}$

G: graph with ordering on edges

C_{small}: tiny code



$(x_{i_1}, x_{i_2} \cdots x_{i_d}) \in C_{small}$

Variables   Constraint

<u>Lemma</u>: $C_{small} = [d, \ell, \Delta]$ - code

G is (c,d) regular, (γ, δ)-expander

then $C = G \oplus C_{small}$ has rate $R \geq 1 - \frac{c(d-\ell)}{d}$

& dist δ, provided $\gamma > \frac{c}{\Delta}$.

Proof: # linear constraints $\leq (d-\ell)\cdot m$

$$\Rightarrow \text{rate} \geq \frac{n-(d-\ell)m}{n}$$

$$= \frac{n-(d-\ell)\frac{cn}{d}}{n}$$

$$= 1 - \frac{c(d-\ell)}{d}$$

Distance: Usual arguments (see notes of last lecture). $\boxtimes$

Issue: Can we C_{small} of large Δ but this increases $d-\ell$ which reduces rate. Will this technique ever be successful in

Abstraction of Expander technology in 90's

Specify $\frac{\gamma}{c} < \frac{1}{2}$; Can find c s.t.

$\forall d \;\; \exists\, \delta, n_0$ s.t. $\forall n \geq n_0$

n-vertex expanders could be constructed.

... Now can verify that good codes can be constructed this way.

Decoding = ?

- Usual decoding doesn't seem to work
- But parallelized variant does.

Parallel-FLIP (parameter : $t < \Delta$)

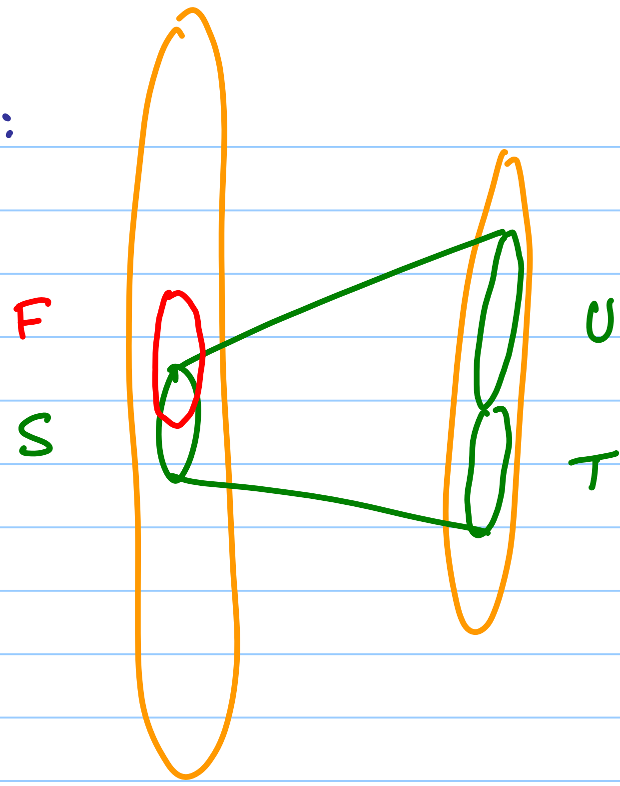
In Iteration i

- All constraints that are within distance t from codeword of C_{small} send FLIP message to neighbors in ERROR
- In parallel all variables that receive FLIP messages flip their assignment

Stop when all constraints satisfied.

Analysis: Will argue that in each iteration # bits in error, $\Delta(y, c)$, goes down (by constant fraction).

Sketch:



Let S = variables in error $= \{ v \mid c_v \neq y_v \}$

$U = \{ v \mid \# \{ u \in S \text{ s.t. } v \leftrightarrow u \} \in \{1 \ldots t\} \}$

$T = \Gamma(S) - U$

F = variables that receive FLIP message.

Claim: Constraint in U sends FLIP message to (and only to) neighbors in S.

Proof: Note U vertices are within distance t of C_{small} & errors are from vertices in S. $\boxtimes$

Lower bound on $|F \cap S|$:

$$|F \cap S| \geq \frac{|U|}{c} \geq \frac{1}{c} \cdot \frac{1}{t-1} (t \cdot \gamma - c) \cdot |S|$$

Upper bound on $|F - S|$:

$$|F - S| \leq \left(\frac{c \cdot |S|}{\Delta - t} \right) \cdot t$$

vertex must have Δ-t neighbours in S to send wrong FLIP messages

Which is greater?

$$\frac{1}{c}\cdot\frac{1}{t-1}\cdot(t\cdot\gamma-c) \quad \text{vs.} \quad \frac{c\cdot t}{\Delta-t}$$

<u>Setup</u>: Fix $\frac{\gamma}{c}$; c;

Let $t\to\infty$; Fix t;

Let $\Delta\to\infty$; Fix Δ;

Let $d\to\infty$; (so code has +ve rate)

<u>Then</u> $\frac{1}{c}\cdot\frac{1}{t-1}(t\cdot\gamma-c)$

$$\to \frac{1}{t-1}\left(t\cdot\frac{\gamma}{c}-1\right) \to \frac{\gamma}{c} > 0$$

<u>While</u> $\frac{c\cdot t}{\Delta-t} \to \frac{c\cdot t}{\Delta} \to 0$

$\boxtimes$

Conclusions

- Can design codes of $R > 0$ correcting $\rho > 0$ fraction of error in linear time
- But R vs. ρ relationship not great! (much worse than algebraic constructions).
- Some extremal settings.
  - Can let $R \to 1$ with $\rho > 0$
  - Can't see $\rho \to \frac{1}{2}$ with $R > 0$ (needs list decoding...)