LECTURE 7

Now we want to prove the theorem we stated but did not have time to prove last time

THEOREM 5 [IPS '99]

$$Deg_{PCR}(F \vdash \perp) \leq W(F) + O\left(\sqrt{n \ln S_{PCR}(F \vdash \perp)}\right)$$

where n = #vars in F

COROLLARY 6 For F unsat k-CNF over n variables, $k = O(1)$

$$S_{PCR}(F \vdash \perp) = \exp\left(\Omega\left(\frac{Deg_{PCR}(F \vdash \perp)^2}{n}\right)\right)$$

Same theorems hold for PC
[In fact, originally proved for PC but we will use them for PCR]

QUESTION: If degree is the analogue of width, do we also have connections between degree and monomial space in PC/PCR?

Excellent question. No idea. Don't even know if anyone thought about this.

Before proving Thm 5 we take care of a couple of technicalities

PROPOSITION 7
Always $\mathrm{Deg}_{PC}(F \vdash \Phi) = \mathrm{Deg}_{PCR}(F \vdash \Phi)$
straightforward
Left as an exercise.

PROPOSITION 8
If $\pi : F \vdash \Phi$ is a PC- or PCR-refutation and ρ is a restriction, then $\pi|_\rho$ is a refutation of $F|_\rho$ in at most the same size, length, and mon space, and degree.

x true $x = 0$, all polys for clauses C s.t. $x \in Lit(C)$ are satisfied & disappear

x false $x = 1$, so literals x just disappear from clauses C s.t. $x \in Lit(C)$

Proof of Thm 5 is by induction

Given unsatisfiable F

$k = W(F)$

n = #vars in F

$S = S_{PCR}(F \vdash 0)$

$d = \sqrt{2n \ln S}$

Compare $S < \exp(2n)$ by doing good enough simulation of resolution, so $d < 2n$ and $a > 1$

$$a = \left(1 - \frac{d}{2n}\right)^{-1}$$

$fat(\pi)$ = # monomials of degree $\geq d$ in π

LEMMA 9 Let G k-CNF over $m \leq n$ vars

Suppose $\exists$ PCR-refutation $\pi^A : G \vdash 1$

s.t. $fat(\pi^A) < a^b$

Then $\exists$ PCR-ref π' s.t.

$$Deg(\pi') \leq k + d + b - 1$$

Lemma 9 is sufficient to prove Thm 5.

Not all monomials in π are fat (e.g. contradiction 1) so

$$fat(\pi) < S \leq a^{\lceil \log_a S \rceil} \leq a^{\log_a S + 1}$$

Set $b = \log_a S + 1$

$k = W(F)$

$d = \sqrt{2n \ln S}$ has right size

Need to look closer at b

$$\sigma = \log_a S + 1 = 1 + \frac{\ln S}{\ln a}$$

since $\log_a x = \frac{\ln x}{\ln a}$

$$\ln a = \ln\left(\left(1 - \frac{d}{2n}\right)^{-1}\right)$$

$$= -\ln\left(1 - \frac{d}{2n}\right)$$

$$\geq \frac{d}{2n}$$

since $\ln(1+x) \leq x$ (for $x > -1$)

so $-\ln(1-x) \geq x$

$d = \sqrt{2n \ln S}$ gives that

$$\frac{d}{2n} = \sqrt{\frac{\ln S}{2n}}$$

Putting all of this together gives

$$\sigma = 1 + \frac{\ln S}{\ln a}$$

$$\leq 1 + \ln S \cdot \sqrt{\frac{2n}{\ln S}} = 1 + \sqrt{2n \ln S}$$

So $\mathrm{Deg}(\pi') \leq k + d + \sigma - 1$

$$\leq W(F) + 2\sqrt{2n \ln S}$$

Proof of Lem 9 by induction over G and # variables $m \le n$.

Base cases

$G = 0 \Rightarrow$ No fat monomials of degree $d \le d + (k + G - 1)$

$S = 1 \Rightarrow$ empty clause OK

$m = 1$ or $k = 1$ or $S \le 3 \Rightarrow$

G contains $x \wedge \bar{x}$

~~Subtracting~~ $x + \bar{x} - 1$ clauses $\bot$

$m \le k$ $\quad S > 3 \Rightarrow d > 1$

Degree $\le$ # vars $\le$

$m \le k \le k + (d + G - 1)$

Induction step

Consider $\pi : G \vdash \bot$; $\mathrm{fat}(\pi) < a^G$

$2m$ distinct literals

At least $d \cdot \mathrm{fat}(\pi)$ literals in fat monomials

By counting $\exists$ literal in $\frac{d}{2m}\mathrm{fat}(\pi) \ge \frac{d}{2n}\mathrm{fat}(\pi)$ monomials.

Set this monomial w/log x to true

$\pi|_x : G|_x \vdash \bot$

$\pi|_x$ has less than $\left(1 - \frac{d}{2n}\right) \cdot a^b \le a^{b-1}$ fat monomials

By ihyp

$$Deg(G|_x \vdash \bot) \leq k + d + 6 - 2$$ ← π_x

$G|_{\bar{x}}$ has one less variable, so by ihyp

$$Deg(G|_{\bar{x}} \vdash \bot) \leq k + d + 6 - 1$$ ← $\pi_{\bar{x}}$

Take π_x and multiply by $\bar{x}$ everywhere

Yields derivation $\pi: G \vdash \bar{x}$
in degree $\leq k + d + 6 - 1$

Using $\bar{x}$, can derive $G|_{\bar{x}}$ from G
without increasing degree.

Then do $\pi_{\bar{x}}$

Lemma follows by induction principle

Suppose we have $C \vee x \longleftrightarrow npa(C) \cdot x$ (1)

and $\bar{x}$ (2)

Axiom $x + \bar{x} - 1$ (3)

(3) - (2) yields $x - 1$ (4)

Multiply by $pi(C)$ to get $m(C)\,x - m(C)$ (5)

(1) - (5) yields $m(C) \longleftrightarrow$ clause C without x

LECTURE 7 CONTINUED

Now we want to prove lower bounds on PCR size for a new formula family.

DEF F is a *random k-CNF formula* with Δn clauses over n variables, denoted $F \sim \mathcal{F}_k^{n,\Delta}$, if F is constructed by picking Δn clauses independently and uniformly ~~at~~ random with replacements from the set of all $\binom{n}{k}2^k$ k-clauses over n variables.

Δ is called the clause density.
We will focus on *constant* clause density, although in general Δ can grow as a function of n.

FACT For any k, if we pick $\Delta = O(1)$ large enough (depending on k) it holds for $F \sim \mathcal{F}_k^{n,\Delta}$ that F is almost surely unsatisfiable (i.e. with prob $1 - o(1)$, i.e., approaching 1 as $n \to \infty$).

For instance, for $k = 3$ $\Delta = 4.6$ is enough.
It is believed that there is a sharp threshold Δ_k s.t. for any $\varepsilon > 0$

$F \sim \mathcal{F}_k^{n,\Delta_k - \varepsilon}$ is almost surely satisfiable as $n \to \infty$

$F \sim \mathcal{F}_k^{n,\Delta_k + \varepsilon}$ — " — unsatisfiable — " —

For $k=3$, Δ_3 is believed to be ≈ 4.2 7:2

But there is no formal proof that this threshold Δ_k exists (except for Δ_2, which is $= 1$), only fairly strong indications. What is known formally is that

$F \sim \mathcal{F}_3^{n,\Delta}$ is a.s. sat if $\Delta \leq 3.5$

$F \sim \mathcal{F}_3^{n,\Delta}$ is a.s. unsat if $\Delta \geq 4.6$

(and there is a whole industry improving these bounds by ingenious methods, not seldom in the third decimal place or so — in particular, the bounds stated above are <u>not</u> optimal)

Random k-CNFs of small (but sufficiently large) constant density are plausible candidates to be hard for pretty much <u>any</u> proof system. No structure, so hard to refute. Unfortunately, therefore also hard to prove lower bounds.

Known to be hard for resolution [CS88]

— " — PC, first in journal version characteristic $\neq 2$ [IB99] [AR03] ↙ then in any char including 2 [AR01]

<u>Not</u> known to be hard for CP — great open problem

We want to do LB proof in [AR01] for PC/PCR

Recall

$G = (U \dot\cup V, E)$ is a (d, s, e)-unique-neighbour expander or boundary expander if

1) constant left-degree $\leq r$
2) $\forall U' \subseteq U$ s.t. $|U'| \leq s$ it holds that $|\partial U'| \geq e \cdot |U'|$

where the boundary $\partial U'$ is

$$\partial U' = \{ v \in N(U') \mid |N(v) \cap U'| = 1 \}$$

(In [AROL], this is called an (r', s', c')-expander matrix for rows U columns V
s' = degree d
r' = max size s of expanding set
e' = expansion constant e.)

For a CNF formula F, we can construct bipartite graph $G(F)$ with

U = clauses C

V = variables x

E ~~edges~~ = (C, x) edge if x occurs in C

LEMMA [CS88] Let $F \sim \mathcal{F}_k^{n,\Delta}$ for $\Delta = O(1)$ ~~large enough~~, and let $G(F)$ be the corresponding bipartite graph. Then there are constants $K_1, K_2 > 0$ such that almost surely $G(F)$ is a $(k, K_1 \cdot n, K_2)$ – boundary expander.

This is very similar in spirit to a problem on the first problem set, and we will just accept it as true. We remark that [AR01] states a more general version for non-constant Δ, but we focus on $\Delta = O(1)$.

[AR01] proves that good boundary expansion properties ~~for~~ of $G(F)$ is enough to prove degree lower bounds for F in PC

THEOREM [AR01] If $G(F)$ is a (d, s, e)-boundary expander, then $\mathrm{Deg}_{PC}(F \vdash \perp) \geq se/2$ over any field $\mathbb{F}$.

Combining this with the LB on size in terms of degree, we get

COROLLARY [AR01]
If $F \sim \mathcal{F}_k^{n,\Delta}$ for $k \geq 3$ and $\Delta = O(1)$ large enough, then almost surely F is unsatisfiable and $S_{PCR}(F \vdash \perp) = \exp(\Omega(n))$ (and hence also $S_{PC}(F \vdash \perp) = \exp(\Omega(n))$).

CNF formula $F = \underbrace{C_1 \wedge \cdots \wedge C_m}_{\text{over } x_1, \ldots, x_n}$ translated to polynomials $f_1, \ldots, f_m$ in $\mathbb{F}[x_1, \ldots, x_n]$

PC-derivation: generate new elements in the ideal in $\mathbb{F}[x_1, \ldots x_n]$ spanned by $f_1, \ldots, f_m$

Notation: $\mathrm{Span}(f_1, \ldots, f_m)$

PC-refutation: Derivation showing that $1 \in \mathrm{Span}(f_1, \ldots, f_m)$

T_n = set of all (multilinear) monomials or terms

$\mathrm{Deg}(m)$ = degree of monomial/term = # variables

$T_{n,d} = \{ t \in T_n \mid \mathrm{Deg}(t) \leq d \}$

Note that we will assume that Boolean axioms $x_i^2 - x_i$ are always applied (implicitly) to get multilinearity. If we wanted to be formal, we could / should say that we are working in the polynomial ring $\mathbb{F}[x_1, \ldots x_n]$ factored by ideal I generated by $\{ x_i^2 - x_i \mid i = 1, \ldots, n \}$, which is an $\mathbb{F}$-algebra denoted $S_n(\mathbb{F})$ in [AR01]

[An *algebra* is a vector space V over a field $\mathbb{F}$ with multiplication
- multiplication is distributive
- $\forall\ f \in \mathbb{F},\ x, y \in V \quad f(xy) = (fx)y = x(fy)$]

But we *don't* want to get too formal, so we will just think about all polynomials appearing as being "magically" multilinear.

Write $S_n(\mathbb{F})$ to denote all multilinear polynomials

Write $S_{n,d}(\mathbb{F})$ to be the linear space of all multilinear polynomials of degree $\leq d$.

Want to have a way of comparing/ordering monomials=terms

An (total) ordering $\preceq$ of T_n is *admissible* if

(1) $\deg(t_1) < \deg(t_2) \Rightarrow t_1 \prec t_2$

(2) If $t_1 \preceq t_2$ and $t \in T_n$ does not contain any variables from t_1, t_2, then $t t_1 \preceq t t_2$

Example Order first wrt degree and then lexicographically.

For any $f \in S_n(\mathbb{F})$, let $LT(f)$ be the *leading term* of f wrt $\preceq$

Note that $\deg(LT(f)) = \deg(f)$.