LECTURE 8: RECAP WHERE WE ARE

Recall

For a CNF formula F, can define bipartite graph $G(F)$ with clauses on left, variables on right, and edges when variables occur in clauses.

$G(F)$ is a unique-neighbor expander or boundary expander if all moderately large vertex sets on left side have many unique neighbors on right side.

A random graph is a good expander almost surely (for the right parameters)

Random k-CNF $F \sim \mathcal{F}_k^{n,\Delta}$

Δn randomly chosen k-clauses over n variables

Unsat almost surely if $\Delta = O(1)$ large enough. $G(F)$ will be good boundary expander a.s.

To get exponential lower bounds on $R(R)$ refutation size of random k-CNFs, sufficient to prove

THEOREM 1 [ARO1 / ARO3] [Thm 3.13 in ARO3] If $G(F)$ is a (d,s,e)-boundary expander, then $\mathrm{Deg}_{PC}(F \vdash 1) \geq se/2$ over any field $\mathbb{F}$.

LECTURE 8 RECAP NOTATION

Formula $F = C_1 \wedge \dots \wedge C_m$ over $x_1, \dots, x_n$ translated to polynomials $f_1, \dots, f_m$ in $\mathbb{F}[x_1, \dots, x_n]$

T_n = set of all multilinear monomials/terms

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

[Assume that Boolean axioms $x_i^2 - x_i$ are always applied implicitly so that we automatically have multilinearity.]

$S_n(\mathbb{F})$ = set of all multilinear polynomials (formally an $\mathbb{F}$-algebra — vector space with multiplication)

$S_{n,d}(\mathbb{F})$ = set of all multilinear polynomials of degree $\leq d$ (vector space)

Order all monomials so that

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 or t_2, then $t t_1 \preceq t t_2$.

E.g. first w.r.t degree and then lexicographically

For any $f \in S_n(\mathbb{F})$, let $LT(f)$ denote the <u>leading term</u> of f w.r.t $\preceq$.

(Note that $Deg(LT(f)) = Deg(f)$

Ideal subring that in addition is closed under multiplication by any element of larger ring.

Span $(f_1, \ldots, f_m)$ = ideal generated by these polynomials.

Concrete example

Consider ring $\mathbb{Z}$

Take subring $I_k = \{ kn \mid n \in \mathbb{Z} \}$ for some $k > 1$.

This is an ideal.

Can write any $m \in \mathbb{Z}$ as a sum of

$q \in I$

r minimal irreducible term in $\Delta = \{0, 1, \ldots, k-1\}$

$$m = r + q$$

Just a fancy way of describing modular arithmetic

$$m \equiv r \pmod{k}$$

Continuing our fancy terminology, we can say that the reduction operator

R_{I_k} maps m to $R_{I_k}(m) = r$.

This works in general as well.

Some standard algebra stuff

V ideal, t term

t is **reducible mod V** if $\exists f \in V$ s.t. $LT(f) = t$

Let Δ = set of irreducible terms

Fact any polynomial $p \in S_n(\mathbb{F})$ can be written uniquely as $p = g + r$

$g \in V$ ← linear independence connection

$r \in$ linear subspace over Δ (Diagram a DIRECT SUM)

The reduction operator R_V maps term t to polynomial $R_V(t)$ s.t. $t - R_V(t) \in V$

Adaptation to our setting

[CEI 96] proposed using same ideas when V is not tome ideal

Let $V_{n,d}(f_1, \ldots, f_m)$ [or just $V_{n,d}$ for short] be all polynomials in $S_{n,d}(\mathbb{F})$ derivable in degree $\leq d$.

Not closed under multiplication ⇒ "pseudoideal"

Addition rule in PC ⇒ $V_{n,d}$ linear subspace

$t \in T_{n,d}$ is **reducible** if $t = LT(f)$ for some $f \in V_{n,d}$.

$\Delta_{n,d}$ = set of irreducible terms.

Again can write any $p \in S_{n,d}(\mathbb{F})$ uniquely as $p = g + r$ $g \in V_{n,d}$ $r \in$ lin space over $\Delta_{n,d}$

~~7.8~~ 8:V

Let $R_{n,d}$ be projection of p onto 2nd ~~first~~ coordinate ~~of~~ r.

We want to prove lower bound on degree d

$\Updownarrow$

Prove that if d too small, then $1 \notin V_{n,d}$

$\Updownarrow$

$R_{n,d}(1) \neq 0$

or in fancy notation $1 \notin \ker(R_{n,d})$

or equivalently $\ker(R_{n,d}) \neq S_{n,d}(\mathbb{F})$

Might be hard to get a handle on $R_{n,d}$ — but we don't necessarily need to

Can define stronger R, in the sense that

$$\ker(R_{n,d}) \subseteq \ker(R)$$

and then show $\ker(R) \neq S_{n,d}(\mathbb{F})$

Want to do the following — Lem 2.10 in [IKO3] "Lower bounds for the PC" Comp Cplx, 7: 291–324, 1998

LEMMA 2 [Razborov '98]

Suppose $f_1, \ldots, f_m$ axioms, $d < n$. If $\exists$ linear operator R on $S_{n,d}(\mathbb{F})$ s.t. $R \neq 0$ and

(1) $\forall i \quad R(f_i) = 0$

(2) $\forall t, x_j \quad \deg(t) < d \Rightarrow R(x_j \cdot t) = R(x_j \cdot R(t))$

then there is no PC-refutation of $\{f_1, \ldots, f_m\}$ in degree $\leq d$

~~Proof For any PC-derivation in degree $< d$, R sends~~

Proof

~~7.9~~ 8.VI

For any PC-derivation in degree d, R sends anything derived to 0

- True for axioms
- True for addition by linearity
- True for multiplication by (2)

Hence true by induction.

But $R(1) \neq 0$ by assumption, for if ~~so~~ not R would send everything in $Span(\mathcal{F})$ to 0. But $R \not\equiv 0$ by assumption, so $R(1) \neq 0$

So we want to construct such R!

But pseudo-ideals not nice to work with.

So construct $R(t)$ by

- finding set of axioms on which t depends
- Look at ordinary ideal $V(t)$ generated by these axioms
- Define $R(t) = R_{V(t)}(t)$

Standard reduction operator for ideal — nicer to work with

Hope that ideal doesn't get too large so that still (have) $1 \notin V(t)$

Lem 3.14 in

LEMMA 3 [ARO3]

Suppose $\vec{y}, \vec{v}, \vec{z}$ partition of $\vec{x} = \{x_1, \ldots, x_n\}$

$\vec{P} = \vec{P}(\vec{y}, \vec{v})$ set of polynomials over $\vec{y} \cup \vec{v}$

$Q = Q(\vec{v}, \vec{z})$ polynomial over $\vec{v} \cup \vec{z}$

s.t. $(z - b)$ divides Q for some $z \in \vec{z}$, $b \in \{0, 1\}$.

Suppose term $t(\vec{y}, \vec{v})$ free of $\vec{z}$-variables is reducible mod $\mathrm{span}(\vec{P}, Q)$ wrt $\prec$

THEN t is reducible mod $\mathrm{span}(\vec{P})$

Proof By assumption, $\exists$ poly $f \in \mathrm{span}(\vec{P}, Q)$ s.t. $t = LT(f)$.

In general $f \in \mathrm{span}(p_1, \ldots, p_k) \iff \{p_1, \ldots, p_k\} \models f$

i.e. if for every α s.t. $\forall i\ p_i(\alpha) = 0$ it holds that $f(\alpha) = 0$.

So $\vec{P}, Q \models f$ Apply restriction setting $z = b$

$\vec{P}|_{z=b}, Q|_{z=b} \models f|_{z=b}$

$\vec{P}$ does not contain z. $Q|_{z=b} = 0$ by assumption

Hence $\vec{P} \models f|_{z=b}$ or $f|_{z=b} \in \mathrm{span}(\vec{P})$

But t does not contain z either, and so

$LT(f) = t = LT(f|_{z=b})$ so t is reducible mod $\mathrm{span}(\vec{P})$ as claimed

Now construct reduction operator R.

Let CNF F be encoded as $f_1, \ldots, f_m$ | polynomials

Let $N(f_i)$ neighbours on right-hand side in $G(F)$ of f_i = clause C_i

By a little abuse of notation, let
$N(t)$ = vertices on RHS in $G(F)$ corresponding to variables in term/monomial t.

Let I, I_1 denote subsets in $[m]$ correspondig to subsets of the f_i
Want to define with subsets of axioms/polys in $f_1, \ldots, f_m$ should be used to generate the ideal we will use for R

DEF 4 [Support of term t] — Def 3.15 in TCS3

Say that we can t-infer I_1 from I, denoted $I \vdash_t I_1$, if

(a) $|I_1| \leq s/2$

(b) $\partial(I_1) \subseteq N(I) \cup N(t)$

write ∂I, without parantheses for consistency?

OR MAYBE NOT

where we identify $\partial(I_1)$ and $\partial(\{f_i \mid i \in I_1\})$
∂I_1
$N(I)$ " $N(\{f_i \mid i \in I\})$

(a): I_1 is not too large

(b): Any new boundary variables in I_1 were represented in term t

Let the support of the term t, denoted $\mathrm{Sup}(t)$, be the largest set of $[i,m]$ that can be t-inferred by repeated application starting from $\emptyset$

$$\begin{aligned} \emptyset &\vdash_t I_1 \\ I_1 &\vdash_t I_2 \\ I_1 \cup I_2 &\vdash_t I_3 \qquad \text{etc} \end{aligned}$$

Let $V(t) = \mathrm{Span}(\{ f_i \mid i \in \mathrm{Sup}(t) \})$

Let $R(t) = R_{V(t)}(t)$.

We want to prove that this R is a linear operator as in Lem 2.

LEM 5 [Lem 3.16 in TR03]
If $\mathrm{Deg}(t) \le se/2$, then $|\mathrm{Sup}(t)| \le s/2$

Proof By contradiction. Suppose $\exists$ sequence $I_0 = \emptyset, I_1, I_2, \ldots, I_\tau$ s.t.

$$\bigcup_{j=1}^{r-1} I_j \vdash_t I_r$$

and

$$\left| \bigcup_{j=1}^{\tau} I_j \right| > s/2$$

Fix $\tau^* \le \tau$ to be smallest index s.t. $\left| \bigcup_{j=1}^{\tau^*} I_j \right| > s/2$

Then $\left| \bigcup_{j=1}^{\tau^*} I_j \right| \le s$ (since $|I_{\tau^*}| \le s/2$ by Def 4(a)).

By expansion $\left| \partial \left(\bigcup_{j=1}^{\tau^*} I_j \right) \right| > se/2$

By Def 4.6 every new boundary element at each step belongs to $N(t)$, and

$\partial(\bigcup_{j=1}^{t} I_j)$ is a conservative estimate of all these elements. This means that # variables in t = $Deg(t) > se/2$. Contradiction ☐

~~We can~~ Now we can intuitively see that we are in good shape. If $G(F)$ is an ordinary expander with expansion rate $e \geq 1$ then any subset of $\leq se$ clauses is satisfiable. Hence, in this case we have $1 \notin V(t)$ for every ideal $V(t)$.

[This is not the way the proof in AR03 goes, and they don't require this good expansion, but for random k-CNFs maybe we could do (parts of) the rest of the argument this way.]

LEMMA 6 [Lemma 3.17, in AR03]

Assume that t term, $I \supseteq Sup(t)$, $|I| \leq s/2$

Then $R_{Span(I)}(t) = R_{Span(Sup(t))}(t) = R_{V(t)}(t)$

[where we overload notation so that

$Span(I) = Span(\{f_i \mid i \in I\})$.]

Proof

By assumption $Sup(e) \not\subseteq_t I \setminus Sup(t)$

Hence by Def 4(6) $\exists\, j \in I \setminus Sup(t)$ s.t. f_j contains a variable $z \in \partial I$ that does not occur in t.

Use Lemma 3 and set

$$\vec{P} = \{ f_i \mid i \in I \setminus \{j\} \}$$

$$Q = f_j \quad \text{divisible by } (z-b)$$

Then if t is reducible mod (span $(\vec{P}, Q)$) t is also reducible mod (span $(\vec{P})$).

[That is t reducible mod (span (I)) $\Rightarrow$
t " mod (span $(I \setminus \{j\})$]

Farthermore $R_{span(\vec{P})}(t) = R_{span(\vec{P},Q)}(t)$, i.e. all irreducible terms in $R_{span(\vec{P})}(t)$ are irreducible also mod (Span $(\vec{P}, Q)$).
This follows from repeated application of Lemma 3 if we can prove that none of these terms contains variable z.
But that must be one
Because

$$t = R_{span(\vec{P})}(t) + q \quad , q \in Span(\vec{P})$$

Now ① t does not contain z (by assumption)
② q does not contain z (by assumption)
③ $R_{span(\vec{P})}(t)$ and q linearly independent

So if $R_{span(\vec{P})}(t)$ contained any z-stuff, it would not cancel and t would also contain z.

This means that we have proven

$$R_{span(I)}(t) = R_{span(I \setminus \{j\})}(t)$$

for $j \in I \setminus Sup(t)$

By induction, eliminate all $j \in I \setminus Sup(t)$ one by one. The ~~Lemma~~ follows.

Now we can verify that our R satisfies the conditions in Lemma 2

(1) R is linear simply since we define it on monomials in $S_{n,d}(\mathbb{F})$ and extend it by linearity

(2) For any axiom f_i it holds that $R(f_i) = 0$

Consider $t_i = \prod_{x_j \in Vars(f_i)} x_j$

For all terms $t \in f_i$ $Vars(t) \subseteq Vars(t_i)$.

By Lemma 5 $|Sup(t_i)| \leq s/2$

Clearly for each $t \in f_i$ $Sup(t) \subseteq Sup(t_i)$

Since $i \in Sup(t_i)$, ~~for all~~ $R_{span(Sup(t_i))}(f_i) = 0$

($f_i \in Span(f_i)$ so "the remainder" is 0)

By Lemma 6, $R(f_i) = 0$

(since R will agree with $R_{span(Sup(t))}$ on each $t \in f_i$)

(3) $\forall t, x_i \quad Deg(t) < se/2 \Rightarrow R(x_i, t) = R(x_i, R(t))$ 8: XIII

By Lemma 5, $|Sup(x_i, t)| \leq s/2$ (†)

By Lemma 6, $R_{span(Sup(t))}(t) = R_{span(Sup(xt))}(t)$

For any term $t' \in R_{span(Sup(t))}(t)$ it holds that

$Sup(xt') \subseteq Sup(xt)$ This is so since

$N(t') \subseteq \bigcup_{i \in Sup(t)} N(t_i) \cup N(t)$ (*)

(that is, all variables in t' must come from somewhere on LHS in (*)).

By Lemma 6 again

$$R_{span(Sup(xt'))}(xt') = R_{span(Sup(xt))}(xt') \quad (\dagger)$$

and since $x\, R_{span(Sup(xt))}(t)$ is equal to xt modulo the ideal $span(Sup(xt))$, we get

$$R(x\,R(t)) \overset{\text{by def}}{=} R_{span(Sup(xt))}(x\, R_{span(Sup(xt))}(t)) \overset{\text{by (†)}}{=}$$

$$\overset{\text{by what was just said}}{=} R_{span(Sup(xt))}(xt) \overset{\text{by def}}{=} R(xt)$$

④ $R \neq 0$, i.e. in particular

$R(1) \neq 0$

Consider Def 4 with $t = 1$ and initial $I = \emptyset$. Then

$N(t) = \emptyset$ and $N(I) = \emptyset$

and by expansion for any

I_1 s.t. $|I_1| \leq s/2$

we have $\partial I_1 \neq \emptyset$.

Hence we cannot t_I-derive anything and $Sup(1) = \emptyset$

Thus $R(1) = R_{span(Sup(1))}(1)$

$= R_{span(\emptyset)}(1) = 1.$

We have verified the conditions in Lemma 2, and Theorem 1 follows.

Hence for $F \in \mathcal{F}_k^{n,\Delta}$ with $\Delta = O(1)$ large enough, F is unsat and requires linear refutation degree, and thus exponential refutation size in both PC and PCR.