LECTURE 10: PROOF OF DEGREE LOWER BOUNDS

Degree lower bounds $\Rightarrow$ size lower bounds

[IPS '99]

$$\boxed{S_{PC}(\mathcal{P} \vdash \bot) = \exp\left(\Omega\left(\frac{(Deg_{PC}(\mathcal{P} \vdash \bot) - Deg(\mathcal{P}))^2}{|Vars(\mathcal{P})|}\right)\right)}$$

Prove results today for

- multilinear PC (only makes results stronger)
- variable multiplication (degree change $\leq$ factor 2)

[Razborov '98]

DEGREE-D PSEUDO-REDUCTION OPERATOR

If $\exists$ linear operator R such that

(1) $R(f) = 0$ for $f \in \mathcal{P}$

(2) If $deg(t) < D$, then
$R(xt) = R(x \cdot R(t))$

(3) $R(1) \neq 0$

then $\boxed{Deg_{PC}(\mathcal{P} \vdash \bot) > D.}$

Given $\mathcal{P}$ over V, we have

- partitioned $\mathcal{P} = Q \cup \bigcup_{i=1}^{m} P_i$
- divided $V = \bigcup_{i=1}^{n} V_i$
- built bipartite graph $(\mathcal{U}, \mathcal{V})_Q$ for
  $\mathcal{U} = (P_1, \ldots, P_m)$
  $\mathcal{V} = (V_1, \ldots, V_n)$
  Edges (P_i, V_j) if $Vars(P_i) \cap V_j = \emptyset$

QUICK RECAP OF ALGEBRA BASICS

Total ordering $\prec$ of multilinear monomials over some fixed set of variables is $\boxed{\text{ADMISSIBLE}}$ * if:

(a) If $Deg(m_1) < Deg(m_2)$, then $m_1 \prec m_2$

(b) For monomials m_1, m_2, m such that $Vars(m) \cap (Vars(m_1) \cup Vars(m_2)) = \emptyset$ and $m_1 \prec m_2$ it holds that $m m_1 \prec m m_2$

Write $m_1 \preceq m_2$ for $m_1 \prec m_2$ or $m_1 = m_2$

Terms $t_1 = \alpha_1 m_1$ and $t_2 = \alpha_2 m_2$ $(\alpha_i \in \mathbb{F})$ are ordered as underlying monomials m_1 & m_2

*) Tailor-made definition of admissible for our purposes — general definition is, well, more general.

Exact choice of order almost doesn't matter

For concreteness, let us order first w.r.t. degree and then lexicographically $x_1 \prec x_2 \prec x_3 \prec \ldots \prec x_n$

$$x_2 x_3 x_4 \prec x_2 x_3 x_5 \prec x_1 x_2 x_3 x_4$$

In what follows write polynomials $p = \sum_i t_i$ as sums of terms over distinct monomials.

$\boxed{\text{LEADING TERM } LT(p)}$ of $p = \sum_i t_i$ is largest term t_i according to $\prec$.

Let I be ideal in $\mathbb{F}[\vec{x}]/\{x_j^2 - x_j \mid j \in [n]\}$ ring of multilinear polynomials

Term t is $\boxed{\text{REDUCIBLE MODULO } I}$ if $\exists\, g \in I$ s.t. $t = LT(g)$ and $\boxed{\text{IRREDUCIBLE}}$ otherwise.

FACT A Let I ideal over and p polynomial in $\mathbb{F}[\vec{x}]/\{x_j^2 - x_j \mid j \in [n]\}$. Then p can be written uniquely as

$$\boxed{p = q + r}$$

for $q \in I$ and r sum of irreducible terms mod I

Proof p can be written as $p = q + r$ for $q \in I$ and r sum of irreducibles in some way by induction over $LT(p)$.

(i) If $LT(p)$ irreducible, then apply IH to $p' = p - LT(p)$ which has smaller leading term

(ii) If $LT(p)$ reducible, choose $q \in I$ s.t. $LT(q) = LT(p)$ and apply IH to $p' = p - q$.

In both cases $p' = q' + r'$ by induction.

For (i) write $p = q' + (LT(p) + r')$

For (ii) write $p = (q + q') + r'$

To argue uniqueness, suppose

$$p = q_1 + r_1 = q_2 + r_2 \quad \text{for } r_1 \neq r_2$$

Rearrange to get

$$r_1 - r_2 = q_2 - q_1 \in I$$

which shows that leading term in $r_1 - r_2$ is reducible. Contradiction ☒

The $\boxed{\text{REDUCTION OPERATOR}}$ R_I is the operator that when applied to p returns the sum of irreducible terms $R_I(p) = r$ such that $p - r \in I$

Can think of r as representative of equivalence class of polynomials, or as "remainder" when dividing p by I.
(A bit like $17 \bmod 5 = 2$)

For set of (multilinear) polynomials P, write

$$\boxed{\langle P \rangle} = \{ q_i \cdot p_i \mid p_i \in P, \ q_i \text{ polynomial} \}$$

for ideal generated by P

In multilinear setting (or with Boolean axioms) we have

$$\boxed{P \models q \iff q \in \langle P \rangle \iff R_{\langle P \rangle}(q) = 0}$$

We won't prove this, because we don't need it, but it might be helpful for intuition.
Direction $\Leftarrow$ is clear
Direction $\Rightarrow$ needs work and uses Boolean axioms
(Actually, maybe we will need this and might/will give it as exercise)

Let us conclude our algebra recap with two more helpful facts

FACT B For any two polynomials p, p' and ideals $I_1 \subseteq I_2$, it holds that $R_{I_2}(p \cdot R_{I_1}(p')) = R_{I_2}(pp')$.

This is the analogue of saying

$$a \cdot (b \bmod 15) \bmod 5 = ab \bmod 5$$

Proof Write

$$p' = q' + r' \qquad (1)$$

for $q' \in I_1$, r' sum of irreducibles over I_1

$$p R_{I_1}(p') = pr' = q + r \qquad (2)$$

for $q \in I_2$, r sum of irreducibles over I_2

Then combining (1) and (2) we get

$$pp' = pq' + pr' = pq' + q + r$$

where $pq' + q \in I_2$ and r irreducible over I_2. By uniqueness (Fact A), get

$$R_{I_2}(pp') = r = R_{I_2}(p \cdot R_{I_1}(p')) \qquad \square$$

FACT C If t irreducible mod I and $\rho : Vars(t) \to \mathbb{F}$ is any partial assignment s.t. $t\restriction_\rho \neq 0$, then $\boxed{t\restriction_\rho}$ is also irreducible mod I.

Set of irreducible monomials is downward-closed under restrictions.

Proof Let $t = m_\rho \cdot t'$ where m_ρ product of variables in $dom(\rho)$ and by assumption $\alpha = m_\rho\restriction_\rho \neq 0$. Then $t\restriction_\rho = \alpha t'$. If $\exists q \in I$ s.t. $LT(q) = t\restriction_\rho$, then $\alpha^{-1} \cdot m_\rho \cdot q \in I$ and $LT(\alpha^{-1} m_\rho q) = \alpha^{-1} m_\rho \cdot t\restriction_\rho = m_\rho \cdot t' = t$, contradicting that t is irreducible $\square$

High-level idea (will need some polishing)

Define R by reducing modulo polynomial ideals

For every polynomial p, define

$$Sup(p) \subseteq \mathcal{U}$$

and

$$\boxed{R(p) = R_{\langle Sup(p) \cup Q \rangle}(p)}$$

Recall intuition: For multilinear polynomials

$$\boxed{Q \vDash q \iff q \in \langle Q \rangle}$$

Want to prove for polynomials p derivable in not too large degree

(i) $\quad R_{\langle Sup(p) \cup Q \rangle}(p) = 0$

(ii) $\quad Sup(p)$ is not too large

Then can conclude from (ii) that $Sup(p) \cup Q$ satisfiable. But if so p is also satisfiable by (i). So low-degree polynomial calculus derivation cannot derive contradiction

Note that we did this for resolution!

Defined $Sup_S(C)$

Then showed

$$Sup_S(C) \cup Q \vDash C$$

(i.e. $C \in \langle Sup_S(C) \cup Q \rangle$)

Key technical step

If for $S \supseteq Sup_S(C)$, S not too large

$$S \cup Q \vDash C \qquad (C \in \langle S \cup Q \rangle)$$

then

$$Sup_S(C) \cup Q \vDash C \qquad (C \in \langle Sup_S(C) \cup Q \rangle)$$

Axioms outside of $Sup_S(C) \cup Q$ not really relevant for whether C is implied or not

This is kind of an R-operator, but with condition

(2') If $|Vars(p)| < D$, then good things happen.

We need to prove this for $Deg(p)$, not $Vars(p)$

And we need to ensure that R is linear.

So define on monomials, and extend to polynomials by linearity

Fix an $(\mathcal{U}, \mathcal{V})_Q$-graph for P infeasible set of multilinear polynomials.

We will assume that $(\mathcal{U}, \mathcal{V})_Q$ is an (s, δ, ξ, Q)-PC EXPANDER, and will do the proof for $\xi = 0$

We will define support just as for resolution

For term t, $\boxed{\text{NEIGHBOURHOOD}}$ $N(t) = \{ V \in \mathcal{V} \mid Vars(t) \cap V \neq \emptyset \}$
For $p = \sum_i t_i$ $\quad N(p) = \bigcup_i N(t_i)$

$\mathcal{U}' \subseteq \mathcal{U}$ is $\boxed{(s, \mathcal{V}')\text{-CONTAINED}}$ if
- $|\mathcal{U}'| \leq s$
- $\partial_Q(\mathcal{U}') \subseteq \mathcal{V}'$

The $\boxed{\text{SUPPORT}}$ $Sup_s(\mathcal{V}')$ of $\mathcal{V}'$ is the union of all $(s, \mathcal{V}')$-contained subsets $\mathcal{U}' \subseteq \mathcal{U}$

$$\boxed{Sup_s(t)} = Sup_s(N(t))$$

For an $(\mathcal{U}, \mathcal{V})_Q$-graph $\mathcal{G}$, we define

pseudo-reduction operator
$$\boxed{R_{\mathcal{G}}(t) = R_{\langle Sup_s(t) \cup Q \rangle}(t)}$$

and extend to polynomials by linearity

The key technical lemma that we will need is that for $S \supseteq Sup_s(t)$, S not too large

$$\boxed{R_{\langle S \cup Q \rangle}(t) = R_{\langle Sup_s(t) \cup Q \rangle}(t)}$$

HEART OF THE PROOF LEMMA

Let t be any term, and suppose $\mathcal{U}' \subseteq \mathcal{U}$ is such that $\mathcal{U}' \supseteq Sup_S(t)$ and $|\mathcal{U}'| \leq S$. Then

$$\boxed{R_{\langle \mathcal{U}' \cup Q \rangle}(t) = R_{\langle Sup_S(t) \cup Q \rangle}(t) = R(t)}$$

Proof sketch (very sketchy)

Reduce t mod $\langle \mathcal{U}' \cup Q \rangle$ and argue that no polynomials $q_j \in \mathcal{U}' \setminus Sup_S(t)$ is used in unique representation $t = q + r$, $q \in \langle \mathcal{U}' \cup Q \rangle$, r irreducible

Write

$$t = \sum_{i \atop p_i \in Sup_S(t) \cup Q} a_i(\vec{x}) p_i(\vec{x}) + \sum_{j \atop q_j \in \mathcal{U}' \setminus (Sup_S(t) \cup Q)} b_j(\vec{x}) q_j(\vec{x})$$

$$+ \sum_k r_k$$

where r_k are irreducible terms mod $\langle \mathcal{U}' \cup Q \rangle$

For $P' \in \mathcal{U}' \setminus Sup_S(t)$, find PC-good edges (P', V') by peeling argument

Find ρ that satisfies $\sum_j b_j(\vec{x}) q_j(\vec{x})$, i.e., zeroes out these polynomials

All p_i and t are untouched

Basic algebra fact A

Terms r_k maybe touched, but restrictions of irreducible terms are irreducible

Basic algebra fact C

But by uniqueness, this means $\vec{b_j} = 0$ for all j and $\sum_k r_k = R(t)$ ▯

MAIN THEOREM

If $(\mathcal{U}, \mathcal{V})_Q$-graph $\mathcal{G}$ is $(s, \delta, 0, Q)$-PC expander with overlap ℓ, and if $|Vars(p)| \leq \frac{\delta s}{2\ell}$ for all $p \in \mathcal{P}$,

then $R_{\mathcal{G}}$ is a degree-D pseudo-reduction operator for $\mathcal{P}$ with $\boxed{D = \frac{\delta s}{2\ell}}$

Proof sketch

For $f \in \mathcal{P}$ $\quad R(f) = 0$ (*)

Requires more work than for resolution, but is similar. Basically, if $f \in P_i$, then $P_i \in Sup_s(LT(f))$ (though not quite how our proof goes)

Small-degree terms have small support because of expansion

Since $Sup_s(1)$ is small, $Sup_s(1) \cup Q$ is

(**) satisfiable, so $R(1) = R_{\langle Sup_s(1) \cup Q \rangle}(1) \neq 0$

It remains to show that

$$R_{\mathcal{G}}(xt) = R_{\mathcal{G}}(x \cdot R_{\mathcal{G}}(t))$$

This heavily uses the Heart of the Proof Lemma plus some technical lemmas that we will talk about in more detail later.

$$R_g(x R_g(t)) = R_g\Big(x \sum_{t' \in R_g(t)} t'\Big)$$ [expand out]

$$= \sum_{t' \in R_g(t)} R_g(xt')$$ [by linearity of R_g]

$$= \sum_{t' \in R_g(t)} R_{\langle Sups(xt') \cup Q \rangle}(xt')$$ [by definition of R_g]

(***) $$= \sum_{t' \in R_g(t)} R_{\langle Sups(xt) \cup Q \rangle}(xt')$$ [Heart of the proof + some magic]

$$= R_{\langle Sups(xt) \cup Q \rangle}\Big(\sum_{t' \in R_g(t)} xt'\Big)$$ [by linearity of polynomial reduction]

$$= R_{\langle Sups(xt) \cup Q \rangle}(x \cdot R_g(t))$$ [collect terms]

$$= R_{\langle Sups(xt) \cup Q \rangle}\big(x \cdot R_{\langle Sups(t) \cup Q \rangle}(t)\big)$$ [by definition of R_g]

$$= R_{\langle Sups(xt) \cup Q \rangle}(x \cdot t)$$ [Basic algebra fact B]

$$= R_g(xt)$$ ▨

We will spend the rest of today's lecture ironing out (*), (**), and (***) — then we're done!

Let us warm up with two obvious observations

OBSERVATION 1

If $V' \subseteq V''$ and $\mathcal{U}'$ is (s, V')-contained, then $\mathcal{U}'$ is (s, V'')-contained.

OBSERVATION 2

Let t and t' be terms such that $Vars(t) \subseteq Vars(t')$. Then $\boxed{Sup_s(t) \subseteq Sup_s(t')}$.

LEMMA 3

Suppose $(\mathcal{U}, V)_Q$ is an $(s, \delta, 0, Q)$-PC expander and $V' \subseteq V$ is such that $|V'| \leq \delta s/2$. Then every (s, V')-contained subset $\mathcal{U}' \subseteq \mathcal{U}$ is $(s/2, V')$-contained.

Same proof as for resolution. Let us write it down for completeness.

Proof $|\mathcal{U}'| \leq s$, so by expansion

$$|\partial_Q(\mathcal{U}')| \geq \delta |\mathcal{U}'|.$$

By containedness

$$|\partial_Q(\mathcal{U}')| \leq |V'| \leq \delta s/2$$

Hence

$$|\mathcal{U}'| \leq s/2$$

and $\mathcal{U}'$ is $(s/2, V')$-contained as claimed ☒

COROLLARY 4

If $(\mathcal{U},\mathcal{V})_Q$ is $(s,\delta,0,Q)$-expander and $|\mathcal{V}'| \leq \delta s/2$, then $Sups(\mathcal{V}')$ is $(s/2, \mathcal{V}')$-contained.

Again same proof as for resolution.

Proof $Sups(\mathcal{V}') = \bigcup_i \mathcal{U}_i'$ for $(s,\mathcal{V}')$-contained sets. By lemma 3 $|\mathcal{U}_i'| \leq s/2$

$$|\mathcal{U}_1' \cup \mathcal{U}_2'| \leq s \quad \text{and}$$

$$\partial_Q(\mathcal{U}_1' \cup \mathcal{U}_2') \subseteq \partial_Q(\mathcal{U}_1') \cup \partial_Q(\mathcal{U}_2') \subseteq \mathcal{V}'$$

so $\mathcal{U}_1' \cup \mathcal{U}_2'$ is $(s,\mathcal{V}')$-contained and hence $(s/2, \mathcal{V}')$-contained. Now use induction $\boxtimes$

It is now time to do a "peeling lemma" for $(\mathcal{U},\mathcal{V})_Q$-graphs.

LEMMA 5 (PEELING STEP)

Let G be $(\mathcal{U},\mathcal{V})_Q$-graph and t term. Suppose $\mathcal{U}' \subseteq \mathcal{U}$ is such that $\mathcal{U}' \not\subseteq Sups(t)$ and $|\mathcal{U}'| \leq s$. Then $\exists\, P \in \mathcal{U}$ and $V \in \mathcal{V}$ such that

$$P \in \mathcal{U}' \setminus Sups(t)$$

We will be able to play game on (P,V)?

and

$$V \in (\partial_Q(\mathcal{U}') \cap N(P)) \setminus N(t).$$

Proof $\mathcal{U}'$ is not $(s, N(t))$-contained since

$$\mathcal{U}' \not\subseteq Sups(t)$$

But $|\mathcal{U}'| \leq s$, so this means

$$\partial_Q(\mathcal{U}') \not\subseteq N(t)$$

Fix $V \in \partial(\mathcal{U}') \setminus N(t)$ and $P \in \mathcal{U}'$ s.t. $V \in N(P)$.

Since $Sup_s(t)$ is union of $(s, N(t))$-contained sets, we have $\partial_Q(Sup_s(t)) \subseteq N(t)$

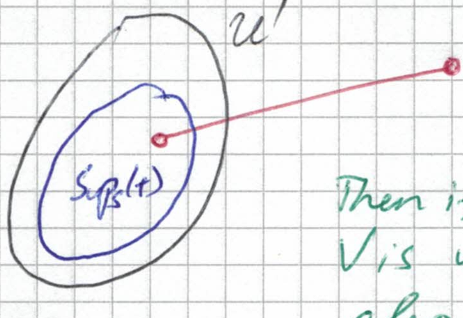
Since $Sup_s(t) \subseteq \mathcal{U}'$, if $P \in Sup_s(t)$ then $V \in \partial_Q(Sup_s(t)) \setminus N(t)$, which is a contradiction. Hence

$$P \in \mathcal{U}' \setminus Sup_s(t)$$

and

$$V \in (\partial_Q(\mathcal{U}') \cap N(P)) \setminus N(t)$$

as required in the lemma.



Then if edge emanates from $Sup_s(t) \subseteq \mathcal{U}'$, V is unique neighbour of $Sup_s(t)$ also — contradiction

LEMMA 6 (Heart of the proof lemma)

Let G be $(\mathcal{U}, \mathcal{V})_Q$-graph

Let t any term

Suppose $\mathcal{U}' \subseteq \mathcal{U}$ is such that $\mathcal{U}' \supseteq Sup_s(t)$ and $|\mathcal{U}'| \leq s$

Then

$$\boxed{R_{\langle \mathcal{U}' \cup Q \rangle}(t) = R_{\langle Sup_s(t) \cup Q \rangle}(t) = R(t)}$$

Up to this point, we only used properties of the graph. Now we need to use algebraic properties of edges!

ARXI

Proof By induction over $\mathcal{U}' \setminus Sup_S(t)$.

If $\mathcal{U}' \not\subseteq Sup_S(t)$, Lemma 5 says that exist

$$P \in \mathcal{U}' \setminus Sup_S(t)$$

and

$$V \in (\theta_Q(\mathcal{U}') \cap N(P)) \setminus N(t).$$

We will show

$$\boxed{R_{\langle \mathcal{U}' \cup Q \rangle}(t) = R_{\langle \mathcal{U}' \setminus \{P\} \cup Q \rangle}(t)} \quad (*)$$

Then lemma follows by induction.

Suppose $R_{\langle \mathcal{U}' \cup Q \rangle}(t) = \sum_k r_k$

for r_k irreducible terms mod $\langle \mathcal{U}' \cup Q \rangle$.

This means that there are polynomials c, u, p, q s.t.

$$\boxed{t = \sum_{p \in P} c_p \cdot p + \sum_{u \in \mathcal{U}' \setminus \{P\}} c_u \cdot u + \sum_{q \in Q} c_q \cdot q + \sum_k r_k} \quad (\dagger)$$

Let ρ be winning assignment for Satisfier on (P, V).

Note that $Vars(u) \cap V = \emptyset$, since V unique neighbours of P. $Vars(t) \cap V = \emptyset$ for same reason. So t and all $u \in \mathcal{U}' \setminus \{P\}$ unaffected by ρ.

Also, since Adversary cannot simultaneously satisfy $\boxed{Q\restriction_\rho \subseteq Q}$ and falsify $P\restriction_\rho$, we have $Q \vDash P\restriction_\rho$ and

USING PROPERTY OF WINNING SATISFIER MOVE ρ

$$P\restriction_\rho = \sum_{q \in Q} c'_q \cdot q$$

Here we are using $\mathcal{P} \vDash p \Leftrightarrow p \in \langle \mathcal{P} \rangle$

Using all this, when we apply ρ to (†) we get

$$t = \underbrace{\sum_{u \in \mathcal{U}' \setminus \{p\}} c_u\restriction_\rho \cdot u + \sum_{\substack{q \in Q\restriction_\rho \\ \subseteq Q}} c_q\restriction_\rho \cdot q + \sum_{q \in Q} c'_q \cdot q}_{\substack{\in \langle \mathcal{U}' \setminus \{p\} \cup Q \rangle \\ \subseteq \langle \mathcal{U}' \cup Q \rangle}} + \underbrace{\sum_k r_k\restriction_\rho}_{\substack{\text{irreducible} \\ \text{mod } \langle \mathcal{U}' \cup Q \rangle \\ \text{by basic algebra fact C}}} \quad (‡)$$

By uniqueness in basic algebra fact A, the right-hand sides in (†) and (‡) must be identical

Since anything irreducible mod $\langle \mathcal{U}' \cup Q \rangle$ is also irreducible mod $\langle \mathcal{U}' \setminus \{p\} \cup Q \rangle$, (‡) shows that

$$R_{\langle \mathcal{U}' \setminus \{p\} \cup Q \rangle}(t) = \sum_k r_k\restriction_\rho = \sum_k r_k =$$

$$= R_{\langle \mathcal{U}' \cup Q \rangle}(t)$$

as claimed in (*), and the lemma follows ☐

Now we just need a few technical lemmas before we can do a non-sketchy proof of the Main Theorem.

In what follows, suppose $(\mathcal{U}, \mathcal{V})_Q$ is an $(s, \delta, 0, Q)$ – PC expander with overlap ℓ.

LEMMA 7

If $Deg(t) \leq \frac{\delta s}{2\ell}$, then $|Sup_S(t)| \leq s/2$

Proof $N(t) \leq Deg(t) \cdot \ell(\mathcal{V}) \leq \frac{\delta s}{2\ell} \cdot \ell \leq \frac{\delta s}{2}$

Now appeal to Lemma 3 ☐

LEMMA 8

For any $\mathcal{U}^* \subseteq \mathcal{U}$ and term t, it holds that

$$\boxed{\mathcal{N}\left(R_{\langle \mathcal{U}^* \cup Q \rangle}(t) \right) \subseteq \mathcal{N}(\mathcal{U}^*) \cup \mathcal{N}(t)}$$

Proof Let $r = R_{\langle \mathcal{U}^* \cup Q \rangle}(t)$, i.e.

$$\boxed{t = q + r} \qquad (*)$$

for $q \in \langle \mathcal{U}^* \cup Q \rangle$ and r sum of irreducibles.

Consider any $V \in \mathcal{V}$ s.t. $V \notin \mathcal{N}(\mathcal{U}^*) \cup \mathcal{N}(t)$.

We will show $V \notin \mathcal{N}(r)$

By assumption $\exists \rho : V \to \{\top, \bot\}$ s.t.

$Q\restriction_\rho \subseteq Q$

Apply ρ to $(*)$. Note that $t\restriction_\rho = t$ since $V \cap Vars(t) = \emptyset$.

Also $q' = q\restriction_\rho \in \langle \mathcal{U}^* \cup Q \rangle$ since $Vars(\mathcal{U}^*) \cap V = \emptyset$ and $Q\restriction_\rho \subseteq Q$

Finally, $r\restriction_\rho$ is still sum of irreducibles

We have

$$\boxed{t = q' + r\restriction_\rho} \qquad (**)$$

By uniqueness, $r\restriction_\rho = r$, so r does not contain any variables in V $\blacksquare$

Now we are very close — just need to get a handle on $R(x \cdot t')$ for $t' \in R(t)$ to do "magic step" in our previous proof sketch of the Main Theorem.

LEMMA 9

Suppose $Deg(t) < \left\lfloor \frac{\delta s}{2\ell} \right\rfloor$

Then for any $t' \in R_{\langle Sup_S(t) \cup Q\rangle}(t)$ and any $x \notin Vars(t)$ it holds that

$$\boxed{R_{\langle Sup_S(xt') \cup Q\rangle}(xt') = R_{\langle Sup(xt) \cup Q\rangle}(xt')}$$

Proof Our plan is to

(a) show $Sup_S(xt') \subseteq Sup_S(xt)$;

(b) show $|Sup_S(xt)| \leq S$;

(c) apply Heart of the Proof Lemma (Lemma 6).

Item (b) follows immediately from Lemma 7.
Item (a) is trickier. We show that

$Sup_S(xt') \cup Sup_S(xt)$

is $(S, N(xt))$ - contained. Then CLAIM α

$Sup_S(xt') \cup Sup_S(xt) \subseteq Sup_S(xt)$

since $Sup_S(xt)$ is the union of all $(S, N(xt))$ - contained sets.

Then apply Lemma 6 with $\mathcal{U}' = Sup_S(xt)$ and t replaced by xt'.

So all that remains is to prove Claim α.

First observe $t' \in R_{\langle Sup(t) \cup Q\rangle}(t)$ implies $t' \preccurlyeq t$ and hence $Deg(t') \leq Deg(t)$

Lemma 7 $\Rightarrow$ $Sup(xt) \leq S/2$

$Sup(xt') \leq S/2$

so

$$| Sup(xt') \cup Sup_S(xt) | \leq S$$

We need to show $\partial_Q(Sup_S(xt') \cup Sup_S(\cancel{xt})) \subseteq N(xt)$

Lemma 8 with $U^* = Sup_S(t) \Longrightarrow$

$$N(t') \subseteq N(Sup_S(t)) \cup N(t) \quad (1)$$

Observation 2 $\Longrightarrow$

$$Sup_S(t) \subseteq Sup_S(xt) \quad (2)$$

Combining (1) & (2) yields

$$\begin{aligned} \underline{N(xt')} &= N(x) \cup N(t') \\ &\subseteq N(x) \cup N(Sup_S(t)) \cup N(t) \\ &\subseteq \underline{N(Sup_S(xt)) \cup N(xt)} \quad (3) \end{aligned}$$

Now we get

$$\begin{aligned} \partial_Q(Sup_S(xt') \cup Sup_S(xt)) &\subseteq \\ &\subseteq \left[\partial_Q(\underline{Sup_S(xt')}) \setminus N(Sup_S(xt))\right] \cup \partial_Q(\underline{Sup_S(xt)}) \\ &\subseteq \left[\underline{N(xt')} \setminus N(Sup_S(xt))\right] \cup \underline{N(xt)} \\ &\subseteq N(xt) \end{aligned}$$

$Sup_S(xt')$ is $(S, N(xt'))$-contained

Use (3)

$Sup_S(xt)$ is $(S, N(xt))$-contained

This concludes the proof of the lemma ∎

Now we can prove the Main Theorem, i.e., that R_g is a degree D pseudo-reduction operator for $D = \frac{\delta s}{2\ell}$

(and so that $Deg_{PC}(P \vdash \bot) > \frac{\delta s}{2\ell}$)

Verify pseudo-reduction properties in reverse order (and note that linearity is by definition)

$\boxed{R_g(1) \neq 0}$ By peeling argument, for $\mathcal{U}' \subseteq \mathcal{U}$, $|\mathcal{U}'| \leq s$, $\mathcal{U}' \cup Q$ is satisfiable (if $\xi = 0$, and otherwise this is an assumption)

$Deg(1) \leq \frac{\delta s}{2\ell}$, so $|Sup_s(1)| \leq s/2$ by Lemma 7 and $1 \notin \langle Sup_s(1) \cup Q \rangle$ since this set is satisfiable.

$\boxed{R_g(xt) = R_g(x \cdot R_g(t))}$ We did the proof for this **except** (***) that

$$R_{\langle Sup_s(xt') \cup Q \rangle}(xt') = R_{\langle Sup_s(\boxed{xt}) \cup Q \rangle}(xt)$$

but this is Lemma 9.

$\boxed{R_g(f) = 0 \text{ for } f \in P}$

If $Q \vDash f$ then $R_g(f) = 0$, so suppose $Q \nvDash f$.

Let $\boxed{t^* = \prod_{x \in Vars(f)} x}$ (i)

Since $|Vars(f)| \leq \frac{\delta s}{2\ell}$, $Deg(t^*) \leq \frac{\delta s}{2\ell}$ and Lemma 7 $\Longrightarrow |Sup_s(t^*)| \leq s/2$

$Sup_s(t^*) \supseteq Sup_s(t)$ $\forall t \in f$. by Observation 2.

Repeated application of Lemma 6 yields

$$R_g(f) = R_{\langle Sup_s(t^*) \cup Q \rangle}(f)$$

We claim $f \in Sup_s(t^*)$, which clearly implies $R_g(f) = 0$

Suppose $f \in P$. For any

$$\boxed{V \in N(P) \setminus N(t^*)} \quad (ii)$$

we claim that (P, V) is not a PC-good edge. If we can show this, then $\{P\}$ is $(s, N(t^*))$-contained and $f \in P \in \mathrm{Sups}_s(t^*)$

By (i) & (ii)

$$\boxed{\mathrm{Vars}(f) \cap V = \emptyset} \quad (iii)$$

Since $Q \nvDash f$, $\exists\, \alpha$ s.t.

$$\alpha(Q) = \top$$
$$\alpha(f) = \bot$$

By (iii) Satisfier cannot play ρ to guarantee that f & P satisfied, so (P, V) is not PC-good edge.

Hence $R_{\mathcal{G}}$ is degree-D pseudo-reduction operator and the Main Theorem follows $\boxed{\Xi}$

We saw last lecture that we can build (s, δ, Q, Q)-PC expanders for many CNF formula families

[Miksa & Nordström '24] provides unified way of proving most field-independent PC lower bounds.

- But not lower bounds that depend on char($\mathbb{F}$)
- Worst-case lower bounds for colouring [Lauria & Nordström '17], but not average-case lower bounds — topic of next lecture!