PROOF COMPLEXITY AS A COMPUTATIONAL LENS

LECTURE 9: DEGREE LOWER BOUNDS FOR POLYNOMIAL CALCULUS

Fix field $\mathbb{F}$ variables $\vec{x} = \{x_1, \ldots, x_n\}$

Work in $\mathbb{F}[\vec{x}] / \{x_j^2 - x_j \mid j \in [n]\}$
so all polynomials multilinear

Also think in variables $\bar{x}_j$ when convenient — won't need them today

POLYNOMIAL CALCULUS DERIVATION from $\mathcal{P}$ (sequence of polynomials $\pi = (P_1, P_2, \ldots, P_L)$ such that

P_i is

INPUT POLYNOMIAL $P_i \in \mathcal{P}$

BOOLEAN AXIOM $x_j^2 - x_j$ except we don't need these in multilinear setting

COMPLEMENTARITY AXIOM $x_j + \bar{x}_j - 1$

or derived from $P_j, P_k \in \pi$, $j,k < i$ by

LINEAR COMBINATION $\dfrac{Q \quad R}{\alpha Q + \beta R}$ $\alpha, \beta \in \mathbb{F}$

MULTIPLICATION $\dfrac{Q}{m Q}$ m monomial

A **POLYNOMIAL CALCULUS REFUTATION** of set of polynomials $\mathcal{P}$ is derivation from $\mathcal{P}$ ending in $P_L = 1$

Size of ρ $S(\rho)$ = # monomials in representation of ρ as linear combination of monomials

$S(\pi) = \sum_i S(P_i)$

$\mathrm{Deg}(\pi) =$ max total degree of any polynomial P_i

THM 1 [Impagliazzo, Pudlák, & Sgall '99] | PCDIL

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

Focus on proving degree lower bounds

Build generalized constraint-variable incidence graph (CVIG)

Sets of polynomials P over variables V

Partition $P = Q \cup \bigcup_{i=1}^{m} P_i$

Divide $V = \bigcup_{i=1}^{n} V_i$

OVERLAP $ol(V) = \max_x |\{V_i \mid x \in V_i\}|$

$(U,V)_Q$-graph

Bipartite graph with
- left vertex set $U = \{P_1, P_2, \ldots, P_m\}$
- right vertex set $V = \{V_1, \ldots, V_n\}$
- Edge (P,V) if $Vars(P) \cap V \neq \emptyset$

The edge (P,V) is RESPECTFUL or PC, if Satisfier wins following game on (P,V)

(1) Satisfier commits to $\rho : V \to \{T, \bot\}$ such that if for $q \in Q$ it holds that $Vars(q) \cap V \neq \emptyset$, then ρ satisfies q

(2) Adversary plays α s.t. $\alpha(Q) = T$

(3) Define $\alpha'(x)$ by

$$\alpha'(x) = \begin{cases} \rho(x) & \text{if } x \in V \\ \alpha(x) & \text{otherwise} \end{cases}$$

Satisfier wins if $\alpha'(P \cap Q) = T$

Recall for $G = (U, V, E)$, $U' \subseteq U$

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

BOUNDARY or UNIQUE NEIGHBOURS of U'

PC BOUNDARY of U' in $(U, V)_Q$-graph

$\partial_Q^{PC}(U') = \{ v \in V \mid v \in \partial(U') \text{ and for } P_v \in N(v) \cap U' \}$
(P, v) is a PC edge

$(U, V)_Q$-graph is **(s, δ, ξ, Q)-PC EXPANDER** if $\forall U' \subseteq U$, $|U'| \leq s$ it holds that $|\partial_Q^{PC}(U')| = \delta |U'| - \xi$

with overlap ℓ if $ol(V) \leq \ell$

THEOREM 2 [MN '24]

Suppose $\forall p \in P \quad |Vars(p)| \leq \frac{\delta s - 2\xi}{2\ell}$

$(U, V)_Q$ (s, δ, ξ, Q)-expander with overlap ℓ

$\forall U', |U'| \leq s$ $U' \cup Q$ satisfiable.

Then $\boxed{Deg(P \to \perp) > \frac{\delta s - 2\xi}{2\ell}}$

COROLLARY 3 [MN '24]

Suppose that $\forall p \in P \quad |Vars(p)| \leq \frac{\delta s}{2\ell}$

and $(U, V)_Q$-graph is $(s, \delta, 0, Q)$-PC expander (i.e., $\xi = 0$)

Then $\boxed{Deg(P \to \perp) > \frac{\delta s}{2\ell}}$

How can we use this to prove lower bounds?
Build $(\mathcal{U}, V)_Q$ - graphs and show that they are PC expanders.

THEOREM 4 [Alekhnovich & Razborov '03]
Let F be a CNF formula such that the clause-variable incidence graph $G(F)$ is an (s, δ)-boundary expander for some $\delta > 0$. Then $\boxed{Deg(F \vdash 1) > \delta s/2}$.

COROLLARY 5
Random k-CNF formulas (for $k \geq 3$, with $\Theta(n)$ clauses over n variables) require polynomial calculus proofs of exponential size $\exp(\Omega(n))$ asymptotically almost surely (and linear degree $\Omega(n)$)

Proof of Cor 5 The CVIG of such a random formula is a random k-left-regular bipartite graph, which is an excellent expander a.a.s.

Proof of Thm 4 Axiom clauses/polynomials have $k = O(1)$ variables. Set $Q = \emptyset$, $\mathcal{U}$ = singleton set of clauses, V = singleton sets of variables. All edges (C, x) are PC good - can assign x to fix $C = T$. ☐

GRAPH ORDERING PRINCIPLE GOP(G)

"There exists a totally ordered set on n elements without a minimal element."

Variables $x_{u,v}$ = "element $u \prec$ element v"
$u, v \in [n]$

Bounded-degree graph $G = (V, E)$ $V = [n]$

DEF Non-bipartite boundary expanders

Graph $G=(V,E)$ is an (s,δ)-BOUNDARY EXPANDER if $\forall V' \subseteq V$, $|V'| \leq s$, it holds that $|\partial(V')| \geq \delta |V'|$, where

$$\partial(V') = \{ v \in V \setminus V' : |N(v) \cap V'| = 1 \}$$

$\bar{x}_{u,v} \vee \bar{x}_{v,w} \vee x_{u,w}$	$u,v,w \in V$ $u \neq v \neq w \neq u$	TRANSITIVITY
$\bar{x}_{u,v} \vee \bar{x}_{v,u}$	$u,v \in V$ $u \neq v$	ASYMMETRY
$x_{u,v} \vee x_{v,u}$	$u,v \in V$ $u \neq v$	TOTALITY
$\bigvee_{u \in N(v)} x_{u,v}$	$v \in V$	NON-MINIMALITY

"v is not minimal as witnessed by some neighbour u of v w.r.t. G"

For $G = K_n$, this formula is known as the LINEAR ORDERING PRINCIPLE FORMULA (or LEAST NUMBER PRINCIPLE FORMULA or GRAPH TAUTOLOGY)

THEOREM 6 [Galesi & Lauria '10]
For any non-bipartite (s,δ)-boundary expander G it holds that $\mathrm{Deg}(\mathrm{GOP}(G) \vdash \bot) \geq \frac{\delta s}{4}$.

Remark 1 Result in Galesi-Lauria has slightly better constants — we optimize for simplicity of exposition (GL'10 gets lower bounds for 3-CNF. Here we need 5-CNF)

Remark 2 Random 5-regular graphs are $(\Omega(n), \delta > 0)$-boundary expanders a.a.s. — calculation

Remark 3 Thm 6 yields 5-CNF formulas over $\Theta(n^2)$ variables with refutation degree $\Omega(n)$. [Stålmarck '96] showed that these are short resolution proofs. $O(n^3)$ So these formulas demonstrate that size-width/degree relations in [IPS '99] and [BW '01] are essentially tight. Might look at Stålmarck's resolution proof later in the course.

Proof of Thm 6 Let Q consist of all transitivity, assymmetry, and totality axiom (enforcing that assignments are total orders)

Left vertex sets U = singleton sets with non-minimality axioms

Right vertex sets $V = \{V_v \mid v \in V\}$ where

$$V_v = \{x_{u,w} \mid u = v \text{ or } w = v\}$$

set of all variables that mention v.

Every variable $x_{u,w}$ occurs in V_u and V_w, so overlap = 2.

We claim that all edges (P_v, V_w) are PC-good.

$w \in \{v\} \cup N(v)$

If $w \in N(v)$, then let

$$f_w(x_{w,u}) = \top \quad \text{for all } u \text{ such that } x_{u,w} \text{ or } x_{w,u} \text{ are in } V_w$$
$$f_w(x_{u,w}) = \bot$$

i.e., f_w sets w to be locally smallest element.

$P_v = \{\bigvee_{u \in N(v)} x_{u,v}\}$ is satisfied.

For Q, asymmetry and totality axioms are either untouched or satisfied, since if ρ assigns $x_{u,w}$ it also assigns $x_{w,u}$ and exactly one of the variables is true and the other false.

$\overline{x}_{a,b} \vee \overline{x}_{b,c} \vee x_{a,c}$

For transitivity if $\rho(x_{a,c}) = T$, then we're OK and if $\rho(x_{a,c}) = \bot$ then $c = w$ and we also have $\rho(x_{b,c}) = \bot$

Similarly, if $\rho(x_{ab}) = T$ then $a = w$ and $\rho(x_{a,c}) = T$

if $\rho(x_{b,c}) = T$ then $b = w$ and $\rho(x_{ab}) = \bot$

Consider vertex set $V' \subseteq V(G)$. By discussion above, we have

$$\partial_Q\left(\bigcup_{v' \in V'} \{P_{v'}\}\right) \supseteq \{V_w \mid w \in \partial(V')\}$$

in $(2\ell, V')_Q$-graphs, so the $(2\ell, V')_Q$-graph has at least as good expansion parameters. We get

$$Deg(GOR(G) + \bot) > \frac{\delta S}{2\ell} = \frac{\delta S}{4} \qquad \blacksquare$$

If $w = v$ then let

$$\rho_v(x_{v,u}) = \bot$$
$$\rho_v(x_{u,v}) = T$$

i.e., ρ_v sets v to locally largest element

Exactly same argument shows that Q is OK

GRAPH PIGEONHOLE PRINCIPLE FORMULAS

$G = (U \dot\cup V, E)$ Pigeon u can fly to holes $N(u)$

$\bigvee_{v \in N(u)} x_{u,v}$	$u \in U$	PIGEON AXIOMS
$\bar{x}_{u,v} \vee \bar{x}_{u',v}$	$v \in V$, $u,u' \in N(v)$, $u \neq u'$	HOLE AXIOMS
$\bar{x}_{u,v} \vee \bar{x}_{u,v'}$	$u \in U$, $v \neq v' \in N(u)$	FUNCTIONALITY AXIOMS
$\bigvee_{u \in N(v)} x_{u,v}$	$v \in V$	ONTO AXIOMS

Standard pigeonhole principle formulas for graph $K_{n+1,n}$. Get formula over G by restriction

$$\rho_G(x_{u,v}) = \begin{cases} 0 & \text{if } (u,v) \notin E \\ * & \text{otherwise} \end{cases}$$

So lower bounds for graph PHP formulas imply lower bounds for standard PHP formulas

Let Onto-PHP(G) contain pigeon, hole, and onto axioms
" FPHP(G) " pigeon, hole, and functionality axioms

THEOREM 7 (Essentially [AR'03])
Let $G = (U \dot\cup V, E)$ be an (s,δ)-boundary expander without isolated vertices in V. Then

$$\mathrm{Deg}(\text{Onto-PHP}(G) \vdash 1) > \frac{s\delta}{2}.$$

Proof sketch Let Q = onto & hole axioms
Let U = singleton sets with pigeon axioms.
Let $V_v = \{ x_{u,v} \mid u \in N(v) \}$, i.e. variables are partitioned w.r.t. holes. All edges are PC-good, and the $(U,V)_Q$-graph is isomorphic to G. (Note, though, that pigeons might be sent to several holes to satisfy onto axioms in Q.) ▨

This does not work for FPHP(G), if we try to substitute functionality axioms for onto axioms in Q.

For edge (P_u, V_v), need to set $x_{u,v} = T$

But $(\bar{x}_{u,v} \vee \bar{x}_{u,v'}) \restriction_{x_{u,v}} = \bar{x}_{u,v'}$ — clauses touched but not satisfied

THEOREM 8 [MN '24]
Let $G = (U \dot\cup V, E)$ be a bipartite (s,δ)-boundary expander with left degree $\leq d$. Then

$$\mathrm{Deg}\left(\mathrm{FPHP}(G) \vdash \bot\right) > \frac{\delta s}{2d}$$

Proof Construct $(U,V)_Q$-graph as follows.
Q = hole & functionality axioms
U = singleton sets with pigeon axioms
$V = \{ V_v \mid v \in V \}$ where

$$V_v = \{ x_{u',v'} \mid u' \in N(v) \text{ and } v' \in N(u') \}$$

i.e. – start with hole v
– go to all pigeons u' that can fly to v
– consider all holes v' such pigeons u' can fly to

PCDX

Overlap is $\leq d$, since $x_{u,v}$ can only appear in sets $V_{v'}$ such that $v' \in N(u)$, and $|N(u)| \leq$ left degree d.

G and $(\mathcal{U}, \mathcal{V})_Q$ is same graph
If $(u,v) \in E(G)$, then clearly $\exists$ edge $P_u \leftrightarrow V_v$
Suppose (P_u, V_v) is edge in $(\mathcal{U}, \mathcal{V})_Q$
Then by construction $u \in N(v)$, so $(u,v) \in E(G)$.

Finally, we claim that all edges are PC good.
Consider $P_u = \{ \bigvee_{w \in N(u)} x_{u,w} \}$ and V_v s.t. $v \in N(u)$, i.e., (P_u, V_v) is edge. Choose

$$s_{u,v}(x_{u',v'}) = \begin{cases} \top & \text{if } u'=u \ \& \ v'=v \\ \bot & \text{otherwise} \end{cases}$$

$\bigvee_{w \in N(u)} x_{u,w}$ is satisfied

Hole axioms for v satisfied, since $s(x_{u',v}) = \bot$
All other hole axioms untouched or satisfied, since all other variables in V_v set to $\bot$.
Functionality axioms for u satisfied, since $s(x_{u,v'}) = \bot$
All other functionality axioms either untouched or satisfied, since all other variables in V_v set to $\bot$.

Same graph and all edges good $\Rightarrow$ same expansion
Overlap $\ell \leq d$ yields degree lower bound $\delta s/(2d)$ ∎

COROLLARY 9 [MN'24] — PCD XI

$$S_{PCR}\left(FPHP_n^{n+1} \vdash \bot\right) = \exp(\Omega(n))$$

Proof Apply restriction to $K_{n+1,n}$ to get, say, 5-left-regular $(\Omega(n), \delta > 0)$-boundary expander G.

Theorem 8 $\Rightarrow$ degree lower bound $\Omega(n)$ for $FPHP(G)$

[IPS'99] $\Rightarrow$ exponential size lower bound for $FPHP(G)$

Since $FPHP_n^{n+1}\restriction_G = FPHP(G)$ and restrictions preserve refutations, means that same lower bound applies for $FPHP_n^{n+1}$ ☐

Some questions

Results for resolution in [BIS'07]

(1) Can we get PC lower bounds for graph colouring?
Yes, future lecture

(2) What about clique or vertex cover?

(3) PC lower bounds for Ramsey theory problems?

(4) Degree lower bounds for dense linear ordering formulas
Resolution
[Atserias & Dalmau '08]

Resolution results
[Carlucci, Galesi, Lauria '16]
[Lauria, Pudlák, Rödl, Thapen '17]
[Pudlák '12]

(5) PC size lower bounds for weak pigeonhole principle (WPHP) formulas with $\geq n^2$ pigeons
Understood for resolution Raz & Razborov
Also for graph-WPHP [de Rezende, Nordström, Risse, Sokolov '25]

The lower bound method we have presented works regardless of the field. What about lower bounds that depend on the field?

(6) [Alekhnovich & Razborov '03] have a version of their method that depends on the field. Can it be combined with generalized CVIGs and fibering sets Q?

(7) What about Onto-FPHP formulas in fields F of characteristic p with $n + p^d$ pigeons and n holes? Upper & Lower bounds for Nullstellensatz in [Beame & Riis '98]
Nothing known for PC

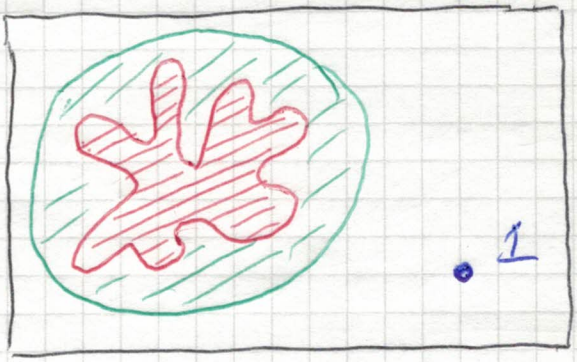
(8) What about perfect matching on sparse non-bipartite graphs G with $|V(G)|$ odd?

[Austrin & Risse '22] Degree lower bound $\Omega\left(\frac{n}{\log n}\right)$ for random d-regular graphs.
Issues: (a) d has to be very large
(b) log factor loss
Proof by reduction to Tseitin formulas.
Direct argument would be desirable

PROOF STRATEGY FOR DEGREE LOWER BOUNDS

Give over-approximation of what can be derived in degree D by defining operator R such that if p derivable from P in degree $\leq D$, then $R(p) = 0$

Then show $R(1) \neq 0$



/// derivable in degree D

/// $\{p \mid R(p) = 0\}$

LEMMA 10 [Razborov '98]

Let P set of multilinear polynomials, $D \in \mathbb{N}^+$

Suppose $\exists$ linear operator R on multilinear polynomials over $Vars(P)$ of degree $\leq D$ such that

(1) $R(f) = 0$ for all axioms $f \in P$

(2) For every term t with $Deg(t) < D$ and every variable x it holds that $R(xt) = R(xR(t))$

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

Then $Deg_{PC}(P \vdash \bot) > D$.

(or $> D/2$ if we want to play it safe)

Proof By forward induction over PC derivation Π.

Change multiplication rule to only multiply one variable at a time.

VARIABLE MULTIPLICATION $\dfrac{p}{xp}$

Modified multiplication rule

Will prove degree lower bound in this setting

Strictly speaking, maybe lose factor 2 for monomial multiplication at get degree LB $> D/2$

Or work slightly harder on property (2) to get it for monomial multiplication. Might be possible. Will not worry about this

DETOUR

What is the issue?

Could have $p = \sum_i \alpha_i m_i$

Multiply by t to get $tp = \sum_i \alpha_i t m_i$

Could have high-degree terms tm_1 & tm_2 that cancel

But maybe we don't have cancellation if have to multiply by $x \in Vars(t)$ one at a time

Variable multiplication can only double the degree

p has degree $D_1 \geq \max\{Deg(m_1), Deg(m_2)\}$

tp has degree $D_2 \geq Deg(t)$

$\forall i \quad Deg(tm_i) \leq D_1 + D_2 \leq 2 \max\{D_1, D_2\}$

By induction over $\pi = (p_1, p_2, \ldots, p_k)$

$R(p_i) = 0$

Base case: $p_i \in P$ $\quad R(p_i) = 0$ by property (1)

Inductive step p_i derived by $\dfrac{q \quad r}{\alpha q + \beta r}$

$$R(\alpha q + \beta r) = \alpha R(q) + \beta R(r) \quad [\text{by linearity}]$$
$$= \alpha \cdot 0 + \beta \cdot 0 \quad [\text{by IH}]$$
$$= 0$$

p_i derived by $\frac{p}{xp}$

$p = \sum_i t_i$ for terms $t_i = \alpha_i \cdot m_i$

$$\begin{aligned} R(xp) &= R(x \textstyle\sum_i t_i) \\ &= R(\textstyle\sum_i x t_i) && \text{[linearity]} \\ &= \textstyle\sum_i R(x t_i) \\ &= \textstyle\sum_i R(x R(t_i)) && \text{[property (2)]} \\ &= \sum R(x R(p)) && \text{[linearity]} \\ &= \sum R(x \cdot 0) && \text{[IH]} \\ &= 0 \end{aligned}$$

So if such operator R exists, all polynomials p derivable in degree $\leq$ Dase $\neq 1$ ▨

How to construct such an R ?

R looks a lot like reduction modulo polynomial ideal I

Ideal $\langle P \rangle$ generated by (input) polynomials P satisfy (1) and (2)

But not (3), since P is unsatisfiable iff $1 \in \langle P \rangle$

Solution Reduce different polynomials modulo different subsets of polynomials of P that are satisfiable. Piece together so that it looks like real polynomial ideal in degree $\leq D$

QUICK RECAP OF ALGEBRA BASICS

Total ordering $\prec$ of multilinear monomials over some fixed set of variables is **ADMISSIBLE** *, if:

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

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

Write $m_1 \preccurlyeq m_2$ 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. deg 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.

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 **REDUCIBLE MODULO I** if $\exists\, g \in I$ s.t. $t = LT(g)$ and **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

$$p = g + r$$

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

Proof p can be written as $p = g + r$ for $g \in I$ 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 $g \in I$ s.t. $LT(g) = LT(p)$ and apply IH to $p' = p - g$.

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

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

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

To argue uniqueness, suppose

$$p = g_1 + r_1 = g_2 + r_2 \quad \text{for } r_1 \neq r_2$$

Rearrange to get

$$r_1 - r_2 = g_2 - g_1 \in I$$

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

The **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

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

for ideal generated by P

In multilinear setting (or with Boolean axioms) we have

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

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

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

$$p' = g' + r' \tag{1}$$

for $g' \in I_2$, r' sum of irreducibles over I_1,

$$p\,R_{I_1}(p') = pr' = g + r \tag{2}$$

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

Then combining (1) and (2) we get

$$pp' = pg' + pr' = pg' + g + r$$

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

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

FACT C If t irreducible mod I and $\rho : \mathrm{Vars}(t) \to \mathbb{F}$ is any partial assignment s.t. $t \restriction \rho \neq 0$, then $t \restriction \rho$ 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 $\mathrm{dom}(\rho)$ and by assumption $\alpha = m_\rho \restriction \rho \neq 0$. Then $t \restriction \rho = \alpha t'$. If $\exists\, g \in I$ s.t. $LT(g) = t \restriction \rho$, then $\alpha^{-1} \cdot m_\rho \cdot g \in I$ and $LT(\alpha^{-1} m_\rho g) = \alpha^{-1} m_\rho \cdot t \restriction \rho = m_\rho \cdot t' = t$, contradicting that t is irreducible ☐