PROOF COMPLEXITY AS A COMPUTATIONAL LENS

LECTURE 8: NULLSTELLENSATZ AND POLYNOMIAL CALCULUS

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

Input polynomials (axioms) $p_1(\vec{x}), \ldots, p_m(\vec{x})$

Boolean axioms $x_j^2 - x_j \quad \forall j \in [n]$

Hilbert's Nullstellensatz

$\{p_i(\vec{x}) \mid i \in [m]\}$ have no common $\{0,1\}$-valued root iff $\exists\, q_i(\vec{x}), r_j(\vec{x})$ such that

$$\sum_{i=1}^{m} q_i(\vec{x}) p_i(\vec{x}) + \sum_{j=1}^{n} r_j(\vec{x})(x_j^2 - x_j) = 1$$

$\boxed{\text{NULLSTELLENSATZ CERTIFICATE}}$

Can be viewed as algebraic proof system

(a) for CNF formulas: translate clause

$$C = \bigvee_{x \in Pos} x \vee \bigvee_{y \in Neg} \bar{y}$$

Algebraic setting most natural
0 = true
1 = false

to polynomial

$$p_C = \prod_{x \in Pos} x \cdot \prod_{y \in Neg} (1 - y)$$

But the literature is a bit schizophrenic

(b) for general polynomials

Nullstellensatz is sound and implicationally complete (requires a proof that we will skip)

$$\{p_i \mid i \in [m]\} \cup \{x_j^2 - x_j \mid j \in [n]\} \vDash p$$

$$\Updownarrow$$

$\exists\, q_i, r_j$ s.t.

$$\sum_i q_i \cdot p_i + \sum_j r_j (x_j^2 - x_j) = p$$

$\boxed{\text{Monomial } m} = \prod_{i \in I} x_i^{e_i}$ $\quad e_i \in \mathbb{N}^+$ (though we will have $e_i = 1$ – stay tuned)

$\boxed{\text{Term } t} = \alpha \cdot m \quad \alpha \in \mathbb{F}$, m monomial

Represent all polynomials as linear combinations of (distinct) monomials = sums of (distinct) terms

$\boxed{\text{SIZE } S(p)}$ = # monomials in representation of p

(Other size measures also conceivable, like size of arithmetic circuit evaluating polynomial, but
- not as algorithmically relevant
- too hard to prove strong lower bounds)

Let π be Nullstellensatz refutation of sets of polynomials $\mathcal{P}$ (including $x_j^2 - x_j$ for all variables x_j)

$$\boxed{S(\pi)} = \sum_i S(q_i p_i) + \sum_j S(r_j \cdot (x_j^2 - x_j))$$

$\boxed{Deg(\pi)}$ = largest total degree of any monomial

$$\boxed{S_{NS}(\mathcal{P} \vdash \bot)} = \min_{\substack{\pi : \mathcal{P} \vdash \bot \\ \text{NS refutation}}} \left\{ S(\pi) \right\}$$

$$\boxed{Deg_{NS}(\mathcal{P} \vdash \bot)} = \min_{\pi : \mathcal{P} \vdash \bot} \left\{ Deg(\pi) \right\}$$

Nullstellensatz refutation of $\mathcal{P}$ shows that $1 \in \langle \mathcal{P} \rangle$ = ideal generated by $p \in \mathcal{P}$

DEF (IDEAL)

Let R be commutative ring. An IDEAL I of R is a subset such that

1) $p, q \in I \Rightarrow p+q \in I$
2) $p \in I \Rightarrow rp \in I \quad \forall r \in R$

[CEI96]

A POLYNOMIAL CALCULUS DERIVATION of p from $\mathcal{P}$ in $\mathbb{F}[\vec{x}]$ is sequence of polynomials $\pi = (p_1, p_2, \ldots p_L)$ such that

(a) $p_L = p$

(b) For all $p_i \in \pi$ it holds that

$p_i \in \mathcal{P} \setminus \{x_j^2 - x_j\}$ INPUT AXIOM

$p_i = x_j^2 - x_j$ BOOLEAN AXIOM

or p_i derived from $p_j, p_k \in \pi$; $j, k < i$ by

LINEAR COMBINATION $\dfrac{q \qquad r}{\alpha q + \beta r} \quad \alpha, \beta \in \mathbb{F}$

MULTIPLICATION $\dfrac{q}{mq}$ m monomial

A POLYNOMIAL CALCULUS REFUTATION of $\mathcal{P}$ is a derivation of 1 from $\mathcal{P}$

$S(\pi) = \sum_i S(p_i) \qquad S_{PC}(\mathcal{P} \vdash \bot) = \min_{\pi : \mathcal{P} \vdash \bot} \{S(\pi)\}$

$L(\pi) = L \qquad L_{PC}(\mathcal{P} \vdash \bot) = \min_{\pi : \mathcal{P} \vdash \bot} \{L(\pi)\}$

$Deg(\pi) = \max_{p_i \in \pi} \{Deg(p_i)\} \qquad Deg_{PC}(\mathcal{P} \vdash \bot) = \min_{\pi : \mathcal{P} \vdash \bot} \{Deg(\pi)\}$

POLYNOMIAL CALCULUS WITH DUAL VARIABLES

A.K.A. POLYNOMIAL CALCULUS (PCR) [ABRW02]

Annoying problem: Clause $\bigvee_{i=1}^{w} \overline{x}_i$

translated to $\prod_{i=1}^{w} (1 - x_i) = \sum_{S \subseteq [w]} (-1)^{|S|} \prod_{i \in S} x_i$

Exponentially large object! How to deal with this?

(1) $\boxed{\text{Face the problem}}$ This is a real problem for Gröbner basis-based algorithms. So when studying CNF formulas, study only k-CNF formulas for $k = O(1)$, or transform F to "equivalent" 3-CNF formula $\widetilde{F}$ using auxiliary variables

$$x_1 \vee x_2 \vee \cdots \vee x_n \quad \rightsquigarrow \quad \begin{array}{l} \overline{a}_0 \\ a_0 \vee x_1 \vee \overline{a}_1 \\ a_1 \vee x_2 \vee \overline{a}_2 \\ \vdots \\ a_{n-1} \vee x_n \vee \overline{a}_n \\ a_n \end{array}$$

(2) $\boxed{\text{Remove the problem}}$ (at least in theory) by introducing separate variables for positive and negative literals plus polynomial constraints enforcing the meaning of negation

POLYNOMIAL CALCULUS RESOLUTION

Variables $\{x_i \mid i \in [n]\} \cup \{\overline{x}_i \mid i \in [n]\}$

COMPLEMENTARITY or NEGATION AXIOMS $\quad x + \overline{x} - 1$

All other derivation rules and complexity measures are as for polynomial calculus

Translate clause $C = \bigvee_{x \in Pos} x \vee \bigvee_{y \in Neg} \bar{y}$

to monomial $\prod_{x \in Pos} x \cdot \prod_{y \in Neg} \bar{y}$

For a set of polynomials $\mathcal{P}$ over $\{x_i \mid i \in [n]\}$ a PC refutation is a PCR refutation, so

$$\boxed{S_{PCR}(\mathcal{P} \vdash \bot) \leq S_{PC}(\mathcal{P} \vdash \bot)}$$

There are sets of polynomials $\mathcal{P}_n$ for which

$$S_{PCR}(\mathcal{P}_n \vdash \bot) = poly(n) \quad [= n^{O(1)}]$$
$$S_{PC}(\mathcal{P}_n \vdash \bot) = \exp(\Omega(n^{\delta})) \quad \text{[dRLNS21]}$$

Not hard to show

$$\boxed{Deg_{PCR}(\mathcal{P} \vdash \bot) = Deg_{PC}(\mathcal{P} \vdash \bot)}$$

so from now on we will be relaxed with degree subscript

FACT 1 Polynomial calculus is much stronger than Nullstellensatz w.r.t. size
- size $poly(n)$ v.s. $\exp(n^{\delta})$
- degree $O(1)$ v.s. $\Omega(n/\log n)$

FACT 2 Polynomial calculus resolution efficiently simulates resolution

For resolution refutation $\pi_R : F \vdash \bot$

$\exists$ PCR refutation $\pi_{PCR} : \mathcal{F} \vdash \bot$ s.t.

$$S(\pi_{PCR}) = O(L(\pi_R))$$
$$Deg(\pi_{PCR}) \leq W(\pi_R)$$

Proof Simulate resolution refutation line by line.

FACT 3 Polynomial calculus resolution (and also just polynomial calculus) can be exponentially stronger than resolution

Examples: Tseitin formulas for $\mathbb{F} = GF(2)$
Onto-FPHP$_n^{n+1}$ for any field $\mathbb{F}$

THM 4 [CEI 96] "Low degree $\Rightarrow$ small size"
Suppose for $\mathcal{P} \supseteq \{ x_j^2 - x_j \mid j \in [n] \}$ that $Deg(\mathcal{P} \vdash \bot) = d$. Then $S_{PC}(\mathcal{P} \vdash \bot) = n^{O(d)}$

MULTILINEAR POLYNOMIAL CALCULUS

Multilinear monomial: all variables occur with exponent 1 (or 0)

Multilinear polynomial: Has only multilinear monomials

Because of Boolean axioms $x_j^2 - x_j$, can always multilinearize polynomials

So sometimes convenient to define multiplication to yield multilinear result
Work in quotient ring $\mathbb{F}[\vec{x}] / \{ x_j^2 - x_j \mid j \in [n] \}$

All our size lower bounds work for multilinear (ML) polynomial calculus. (Degree is not affected)

All our upper bounds are for (standard) polynomial calculus. Except for length...

PROPOSITION 5 [see, e.g., [MN24]]
For (unsat) k-CNF formula $F = \bigwedge_{i=1}^{m} C_i$,
$\mathcal{L}_{PC}(F \vdash \bot) = O(k \cdot m)$

Proof sketch For $j = 1, \ldots, m$, derive $\boxed{p_j = 1 - \prod_{i=1}^{j} (1 - C_i)}$
(overloading C_i to be polynomial translation of C_i)
Finally get $\boxed{p_m = 1 - \prod_{i=1}^{m} (1 - C_i)}$. Polynomial p_m evaluates to 1 for all $\{0,1\}^n$. But every function $f: \{0,1\}^n \to \mathbb{F}$ has unique representation as multilinear polynomial, so p_m multilinearized must be equal to 1. ∎

This is not expected to be true for non-multilinear polynomial calculus. But shows why proving length lower bounds seems hard, and also algorithmically not so relevant, since multilinearized multiplication is cheap to implement.

THEOREM 6 [IPS '99] "Small size $\Rightarrow$ small degree"
Let $\mathcal{P}$ unsatisfiable polynomial set (including $x_j^2 - x_j$, or just use multilinear setting) over n variables
Then

$$\boxed{Deg(\mathcal{P} \vdash \bot) \leq Deg(\mathcal{P}) + O\left(\sqrt{n \ln S_{PCR}(\mathcal{P} \vdash \bot)}\right)}$$

COROLLARY 7

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

Proof Use same proof as we did for resolution
Use that restrictions can make monomials vanish.

QUESTION $\boxed{\text{What about version for tree-like proofs ?}}$

For resolution: Have seen several lower bound techniques

For polynomial calculus: Degree lower bounds almost only game in town

Since degree doesn't care about PC vs PCR, we will be a bit relaxed going forward. Sufficient to consider polynomial calculus without dual variables.

$\boxed{\text{CHARACTERISTIC}}$ of field $\mathbb{F}$: smallest $p \in \mathbb{N}^+$ such that $p \cdot 1 = 0$
or 0 (zero) if that never happens

How to prove degree lower bounds?

1. For fields of char $\neq 2$, apply affine transformation $\{0,1\} \longrightarrow \{+1,-1\}$
   E.g. [BGIP '01] — we won't cover this

2. Argue in terms of expansion of (some kind of) constraint-variable incidence graph
   [AR '03] [MN '24]

Recall last lecture:

GENERALIZED CLAUSE-VARIABLE INCIDENCE GRAPH (CVIG)

$\mathcal{F}$ CNF formula over variables $\mathcal{V}$

- Left vertex sets $F_1, \ldots, F_m$ for $\mathcal{F} = \mathcal{E} \cup \dot{\bigcup}_{i=1}^{m} F_i$
- Right vertex set $V_1, \ldots, V_n$ for $\mathcal{V} = \bigcup_{j=1}^{n} V_j$

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

- Edge (F_i, V_j) if $Vars(F_i) \cap V_j \neq \emptyset$

An $(\mathcal{F}, \mathcal{V})_{\mathcal{E}}$-graph is an $(s, \delta, \mathcal{E})$-RESOLUTION EXPANDER if

- it is a bipartite (s, δ)-boundary expander, i.e., $\mathcal{F}' \subseteq \mathcal{F}, |\mathcal{F}'| \leq s \Rightarrow |\partial(\mathcal{F}')| \geq \delta |\mathcal{F}'|$
- Satisfier wins the RESOLUTION EDGE GAME on every edge (F_i, V_j)
  1. (1) Adversary plays α s.t. $\alpha(\mathcal{E}) = T$
  2. (2) Satisfier modifies α on V_j to α'
  3. (3) Satisfier wins if $\alpha'(F_i \wedge \mathcal{E}) = T$

THEOREM 8 [BW01] à la [MN24]
If $\mathcal{F}$ admits $(s, \delta, \mathcal{E})$-expander with overlap l, then $W(\mathcal{F} \vdash \bot) > \frac{\delta s}{2l}$

An $(\mathcal{F}, \mathcal{V})_{\mathcal{E}}$-graph is an $(s, \delta, \mathcal{E})$-PC EXPANDER if

- it is a bipartite (s, δ)-boundary expander
- Satisfier wins the PC EDGE GAME on every edge (F_i, V_j)

change of order

(1) Satisfier commits to $\rho : V_j \to \{T, \bot\}$ satisfying any clauses touched in $\mathcal{E}$

(2) Adversary plays α s.t. $\alpha(\mathcal{E}) = T$

(3) Satisfier wins if $\alpha[\rho / V_j](F_i \wedge \mathcal{E}) = T$

What we want to prove in this & next lecture | EG II

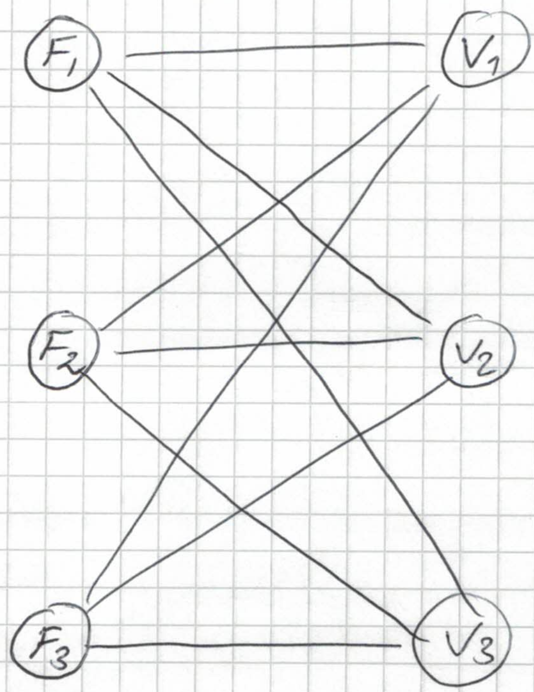
THEOREM 9 [AR03, MN24]
If $\mathcal{F}$ admits $(s, \delta, \mathcal{E})$-PC expander with overlap ℓ, then $\quad \mathrm{Deg}(\mathcal{F} \vdash \bot) > \dfrac{\delta s}{2\ell}$

Recall example

$w \vee x \vee y$
$\bar{u} \vee x$
$u \vee \bar{x}$

$x \vee \bar{y}$
$x \vee \bar{z}$
$\bar{x} \vee y \vee z$

$x \vee y$
$x \vee z$
$\bar{x} \vee \bar{y} \vee \bar{z}$



$\{w, y\}$

$\{x, y\}$

$\{u, w, z\}$

$\mathcal{E} = \{\bar{y} \vee z\}$

Already in resolution edge game, satisfier loses on (F_1, V_1) and (F_1, V_2)
But wins on (F_2, V_2)

In PC game, cannot win on (F_2, V_2)
Filtering set requires $y \mapsto \bot$

$F_2\restriction_{\{y \mapsto \bot\}} = \{x \vee \bar{z}, \bar{x} \vee z\}$

Means we must have $x = z$
But Adversary gets to choose z after Satisfier choose for x.

EGII 1/2

On edge (F_3, V_2) Satisfier has winning strategy

Satisfier chooses $\rho = \{ x \mapsto \top, y \mapsto \bot \}$

then $\rho(E) = \rho(F_3) = \top$

(Less extreme examples are possible)

Prove Thm 9 by first giving second proof of Thm 8

Plus slightly more general setting — what if not possible to win on all edges?

From now on, all polynomials multilinear

ρ satisfies q if q vanishes under ρ (possibly after cancellation if ρ partial assignment)

Let us provide "good edge"-definition for
- resolution $\longleftrightarrow$ semirespectful
- polynomial calculus $\longleftrightarrow$ respectful

ρ RESPECTS polynomial set Q, or is Q-RESPECTFUL, if $\forall q \in Q$ (a) $Vars(q) \cap dom(\rho) = \emptyset$ or

(b) ρ satisfies q

and Q doesn't contain constant non-zero polynomial = contradiction

set of variables V RESPECTS Q if $\exists \rho$, $dom(\rho) = V$ s.t. ρ respects Q

Ex $Q = \{ x_1 x_2,\ x_3 - x_1 x_3,\ x_1 x_4,\ x_5 - x_1 x_5 \}$

$V_1 = \{x_1, x_2\ x_3\}$ $\quad V_2 = \{x_4, x_5\}$

V_2 is Q-respectful by $\rho = \{ x_4 = x_5 = T = 0 \}$

V_1 is not, since assigning x_1 affects but cannot satisfy all polynomials

P, Q sets of polynomials, V set of variables

P is $\boxed{\text{Q-RESPECTFULLY SATISFIABLE}}$ BY V if V respects Q and this is shown by Q-respectful partial assignment ρ to V that satisfies P.

P is $\boxed{\text{Q-SEMIRESPECTFULLY SATISFIABLE}}$ BY V if Q is satisfiable and $\forall \alpha$ satisfying Q $\exists \rho : V \to \{\top, \bot\}$ such that for α' defined by $\alpha'(x) = \boxed{\begin{cases} \rho(x) & \text{if } x \in V \\ \alpha(x) & \text{otherwise} \end{cases}}$ α' satisfies P and Q

Generalized CVIG:

Polynomials $\mathcal{P}$ over variables $\mathcal{V}$

Partition $\mathcal{P} = P_1 \,\dot\cup \cdots \dot\cup\, P_m \,\dot\cup\, Q$

Divide $\mathcal{V} = V_1 \cup \cdots \cup V_n$

Write $\mathcal{U} = \{P_1, \ldots, P_m\}$

Overload $\mathcal{V} = \{V_1, \ldots, V_n\}$

The $\boxed{(\mathcal{U}, \mathcal{V})_Q\text{-graph}}$ has
- left set $\{P_1, P_2, \ldots, P_m\}$
- right set $\{V_1, V_2, \ldots, V_n\}$
- edges (P, V) if $Vars(P) \cap V \neq \emptyset$

(P, V) are $\boxed{\text{Q-RESPECTFUL NEIGHBOURS}}$ if P Q-respectfully satisfiable by V

(P, V) are $\boxed{\text{Q-SEMIRESPECTFUL NEIGHBOURS}}$ if P Q-semirespectfully satisfiable

We also refer to the edges (P, V) as being (semi)-respectful or not.

In our example graph

$F_2 \longleftrightarrow V_2$ $\qquad \mathcal{E}$-semirespectful neighbours

$F_3 \longleftrightarrow V_2$ $\qquad \mathcal{E}$-respectful neighbours

Define boundary expansion by
- first look at boundary / unique neighbours
- only keep (semi) respectful edges (which are those we can win the games on)

$\partial_Q(\mathcal{U}') = \{ V \in \partial(\mathcal{U}') \text{ connected with respectful edge} \}$

$\partial_Q^{SR}(\mathcal{U}') = \{ V \in \partial(\mathcal{U}') \text{ connected with semirespectful edge} \}$

Let $\delta > 0$, $\xi \geq 0$ constant

$(\mathcal{U}, \mathcal{V})_Q$ - graph is (s, δ, ξ, Q) - RESPECTFUL BOUNDARY EXPANDER if $\forall \mathcal{U}' \subseteq \mathcal{U}, |\mathcal{U}'| \leq s$, $|\partial_Q(\mathcal{U}')| \geq \delta|\mathcal{U}'| - \xi$ and every $V \in \mathcal{V}$ is Q-respectful

$(\mathcal{U}, \mathcal{V})_Q$ - graph is (s, δ, ξ, Q) - SEMIRESPECTFUL BOUNDARY EXPANDER if $\forall \mathcal{U}' \subseteq \mathcal{U}, |\mathcal{U}'| \leq s$, $|\partial_Q^{SR}(\mathcal{U}')| \geq \delta|\mathcal{U}'| - \xi$

Twists:
- Only measure respectful part of boundary in expansion
- allow additive slack, so that really small sets might not be expanding

Very rarely useful, so mostly think of $\xi = 0$.

To state main theorems about width and degree, suppose:

F CNF formula that admits (s, δ, ξ, Q)-semirespectful boundary expander with overlap ℓ

$\mathcal{P}$ is set of (multilinear) polynomials that admit (s, δ, ξ, Q)-respectful expander with overlap ℓ

THEOREM 10
Suppose for all $\mathcal{U}' \subseteq \mathcal{U}$, $|\mathcal{U}'| \leq s$ that $\mathcal{U} \wedge Q$ is satisfiable. Then $\boxed{W(F \vdash \bot) > \frac{\delta s - 2\xi}{2\ell}}$

THEOREM 11
Suppose $|Vars(p)| \leq \frac{\delta s - 2\xi}{2\ell}$ $\forall p \in \mathcal{P}$ and $\forall \mathcal{U}' \subseteq \mathcal{U}, |\mathcal{U}'| \leq s$, $\mathcal{U}' \cup Q$ is satisfiable.
Then
$$\boxed{Deg(\mathcal{P} \vdash \bot) > \frac{\delta s - 2\xi}{2\ell}}$$

COROLLARY 12
If $\xi = 0$, then $\boxed{W(F \vdash \bot) > \frac{\delta s}{2\ell}}$

COROLLARY 13
If $|Vars(p)| \leq \frac{\delta s}{2\ell}$ and $\xi = 0$
then $\boxed{Deg(\mathcal{P} \vdash \bot) > \frac{\delta s}{2\ell}}$

Prove Thm 10 (or actually Cor 12 with $\xi = 0$, just for simplicity). We essentially did this last lecture - let us do it again in different way, to prepare us for PC degree lower bounds

Fix $\boxed{F = \bigwedge_{F \in \mathcal{U}} F \wedge Q = \mathcal{U} \wedge Q}$ over $\mathcal{V} = \bigcup_{i=1}^{m} V_i$ represented by $(\mathcal{U}, \mathcal{V})_Q$-graph that is (s, δ, ξ, Q) - semirespectful expander with overlap ℓ.

Set $\xi = 0$ for simplicity — simple, but annoying, to just carry additive ξ around

Want to associate clauses $C \in \pi$ with subset of clauses of F that could have been used to derive C

Last lecture: Minimalist approach - identify smallest such set

This lecture: Maximalist approach - identify largest (but not too large) set

$\boxed{\text{NEIGHBOURHOOD } N(C)} = \{ V \in \mathcal{V} \mid Vars(C) \cap V = \emptyset \}$

"Add ghost vertex $\{C\}$ to left-hand side and see what edges it creates"

$\mathcal{U}' \subseteq \mathcal{U}$ is $\boxed{(s,C)\text{-SEMIRESPECTFULLY}}$ $\boxed{\text{CONTAINED}}$ or just $\boxed{(s,C)\text{-CONTAINED}}$, if

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

$$\partial_Q^{SR}(\mathcal{U}') \subseteq N(C)$$

The clausal $\boxed{\text{SEMIRESPECTFUL } s\text{-SUPPORT } Sup_s^{SR}(C)}$ of C w.r.t. $(\mathcal{U}, \mathcal{V})_Q$ is the union of all (s,C)-contained subsets $\mathcal{U}' \subseteq \mathcal{U}$

Given small-width resolution derivation π from F, show for all $C \in \pi$

(1) $Sup_s^{SR}(C)$ is not too large

(2) $Sup_s^{SR}(C) \cup Q \vDash C$

If so, we're done! (1) means $Sup_s^{SR}(C) \cup Q$ is satisfiable. Then (2) says that C also satisfiable. So small-width π cannot be refutation.

LEMMA 14 Suppose $W(C) \leq \delta s / 2\ell$. Then $Sup_s^{SR}(C)$ is $(s/2, C)$-contained.

Proof $Sup_s^{SR}(C) = \bigcup_i \mathcal{U}_i$ for (s, C)-contained $\mathcal{U}_i$

Fix such $\mathcal{U}_i$. By expansion $[\,|\mathcal{U}_i| \leq s\,]$

$$|\partial_Q^{SR}(\mathcal{U}_i)| \geq \delta |\mathcal{U}_i| \qquad (*)$$

That is, by (s, C)-containedness

$$|\mathcal{U}_i| \leq |\partial_G^{SR}(\mathcal{U}_i)| / \delta \leq \boxed{|N(C)| / \delta} \qquad (**)$$

Furthermore

$$|N(C)| \leq |Vars(C)| \cdot dl(V') \leq W(C) \cdot \ell \leq \boxed{\delta s / 2} \qquad (***)$$

From $(**)$ and $(***)$ conclude

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

Consider any two (s, C)-contained sets $\mathcal{U}_1, \mathcal{U}_2$.

Union $\mathcal{U}_1 \cup \mathcal{U}_2$ is also (s, C)-contained

Just showed $|\mathcal{U}_i| \leq s/2$, so $|\mathcal{U}_1 \cup \mathcal{U}_2| \leq s$

$$\partial_Q^{SR}(\mathcal{U}_1 \cup \mathcal{U}_2) \subseteq \partial_Q^{SR}(\mathcal{U}_1) \cup \partial_Q^{SR}(\mathcal{U}_2) \subseteq N(C)$$

Hence, by induction $\bigcup_i \mathcal{U}_i$ is (s, C)-contained as claimed. $\square$

LEMMA 15 Suppose π resolution derivation from F in width $W(\pi) \leq \frac{\delta s}{2\ell}$. Then $\forall C \in \pi$ $Sup_s^{SR}(C) \cup Q \vDash C$.

Proof By forward induction over derivation π.

Base case $C \in F$. If $C \in Q$ we're good

Suppose $C \in F$ left-hand side vertex. We claim $\{F\}$ is (s, C)-contained, meaning

$C \in F \in Sup_s^{SR}(C)$.

Consider any $V \in N(F)$. If $V \in N(C)$, we're good so suppose not. Then $V \cap Vars(C) = \emptyset$. If $Q \vDash C$ we're still good, so suppose $Q \nvDash C$

Fix total assignment ρ s.t. $\rho(Q) = T$, $\rho(C) = \bot$

Clearly, cannot change ρ on V to satisfy C (and F) so V is not semirespectful neighbour of F, and $V \notin \partial_Q^{SR}(\{F\})$. So $\partial_Q^{SR}(\{F\}) \subseteq N(C)$ and $\{F\}$ is (s, C)-contained as claimed.

Induction step Suppose C derived from C_1 and C_2

By induction $Sup_s^{SR}(C_i) \cup Q \vDash C_i$

Hence

$$\boxed{Sup_s^{SR}(C_1) \cup Sup_s^{SR}(C_2) \cup Q \vDash C}$$

We claim

$$\left(\left(Sup_s^{SR}(C_1) \cup Sup_s^{SR}(C_2)\right) \cap Sup_s^{SR}(C)\right) \cup Q \vDash C$$

For brevity write

$$S = Sup_s^{SR}(C_1) \cup Sup_s^{SR}(C_2)$$

By Lemma 14 $|S| \leq s$. We prove that for any S s.t. $|S| \leq s$ and $S \cup Q \vDash C$, it holds that

$$\left(S \cap Sup_s^{SR}(C)\right) \cup Q \vDash C.$$

To show

$$(\mathcal{S} \cap \mathrm{Sup}_s^{SR}(C)) \cup Q \vDash C$$

show that if $\mathcal{S} \setminus \mathrm{Sup}_s^{SR}(C) \neq \emptyset$, then can decrease size of $\mathcal{S}$ while maintaining implication

$$\mathcal{S} \cup Q \vDash C$$

If $\mathcal{S} \setminus \mathrm{Sup}_s^{SR}(C) \neq \emptyset$, then in particular $\mathcal{S}$ is not (s, C)-contained. Since $|\mathcal{S}| \leq s$, means that $\partial_Q^{SR}(\mathcal{S}) \not\subseteq N(C)$. Fix $V \in \partial_Q^{SR}(\mathcal{S}) \setminus N(C)$ with unique neighbour $F_V \in \mathcal{S}$. Assume towards contradiction that

$$\mathcal{S} \setminus \{F_V\} \cup Q \nvDash C$$

Then $\exists \rho$ s.t. $\rho(\mathcal{S} \setminus \{F_V\}) = T$ $\rho(Q) = T$ $\rho(C) = \bot$ and (by necessity) $\rho(F_V) = \bot$

By semirespectfulness, can modify ρ on V to get ρ' s.t. $\rho'(F_V \wedge Q) = T$

V shares no variables with $\mathcal{S} \setminus \{F_V\}$ so $\rho'(\mathcal{S} \setminus \{F_V\}) = T$. But then ρ' satisfies $\mathcal{S} \cup Q$ but falsifies C. Contradiction.

By induction, can shrink $\mathcal{S}$ until $\mathcal{S} \subseteq \mathrm{Sup}_s^{SR}(C)$ as claimed ∎

Remains to prove that if $|\mathcal{U}'| \leq s$, then $\mathcal{U}' \cup Q$ is satisfiable. This is exactly the same peeling argument as last time if $\xi = 0$

If $\xi > 0$, need satisfiability of $\mathcal{U}' \wedge Q$ as assumption

Questions to think about:

(a) Does the same line of reasoning work for polynomial calculus? Well, yes

(b) If so, why doesn't it yield degree lower bounds?
We use that if a clause C contains many variables, then it has high width
A low-degree polynomial can contain many variables

Next time

Do more complicated proof, following [Alekhnovich-Razborov '03] and [Mikša-Nordström '24], that yields degree lower bounds