

## LECTURE 8: NULLSTELLENSATZ AND POLYNOMIAL CALCULUS

Fix field  $\mathbb{F}$ Variables  $\vec{x} = \{x_1, \dots, x_n\}$ Input polynomials  $P_i(\vec{x})$  (axioms)Boolean coxians  $x_j^2 - x_j \quad \forall j \in [n]$ Hilbert's Nullstellensatz

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

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

NULLSTELLENSATZ CERTIFICATECan be viewed as algebraic proof system(a) for CNF formulas: translate clause

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

to polynomial

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

Algebraic setting  
most natural  
 $0 = \text{true}$   
 $1 = \text{false}$

But the literature  
is a bit  
schizophrenic

(b) for general polynomials

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

$$\{P_i \mid i \in [m]\} \cup \{x_j^2 - x_j \mid j \in [n]\} \vdash P$$

↓

 $\exists g_i, r_j$  s.t.

$$\sum_i g_i \cdot P_i + \sum_j r_j(x_j^2 - x_j) = P$$

$$\text{Monomial } [m] = \prod_{i \in I} x_i^{e_i} \quad e_i \in \mathbb{N}^+ \quad (\text{though we will have } e_i=1-\text{say if needed})$$

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

Represent all polynomials as linear combinations  
<sup>(distinct)</sup> of monomials = sums of (distinct) terms

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

(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  $\pi$  be Nullstellensatz refutation of  
 sets of polynomials  $P$  (including  $x_j^2 - x_j$  for  
 all variables  $x_j$ )

$$[S(\pi)] = \sum_i S(q_i \cdot p_i) + \sum_j S(q_j \cdot (x_j^2 - x_j))$$

$$[\text{Deg}(\pi)] = \text{largest total degree of any monomial}$$

$$[S_{\text{NS}}(P \vdash \perp)] = \min_{\substack{\pi: P \vdash \perp \\ \text{NS refutation}}} \{ S(\pi) \}$$

$$[\text{Deg}_{\text{NS}}(P \vdash \perp)] = \min_{\substack{\pi: P \vdash \perp}} \{ \text{Deg}(\pi) \}$$

Nullstellensatz representation of  $P$  shows that  $1 \in \langle P \rangle$  = ideal generated by  $p \in P$  | PCI

### DEF (IDEAL)

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

$$1) \ p, q \in I \Rightarrow p+q \in I$$

$$2) \ p \in I \Rightarrow rp \in I \quad \forall r \in R$$

in  $\mathbb{F}[x]$

[CEI 96]

### A POLYNOMIAL CALCULUS DERIVATION of $P$

from  $P$  is sequence of polynomials

$\pi = (p_1, p_2, \dots, p_k)$  such that

$$(a) \ p_k = P$$

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

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

$$p_i = x_j^2 - x_j$$

[INPUT AXIOM]

[BOOLEAN AXIOM]

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

[LINEAR COMBINATION]

$$\frac{q}{\alpha q + \beta \sigma} \quad \alpha, \beta \in \mathbb{F}$$

[MULTIPLICATION]

$$\frac{q}{m_q} \quad m \text{ monomial}$$

A POLYNOMIAL CALCULUS REFUTATION of  $P$  is a derivation of 1 from  $P$

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

$$S_{PC}(P_{\perp}) = \min_{\pi: P_{\perp}} \{S(\pi)\}$$

$$L(\pi) = L$$

$$L_{PC}(P_{\perp}) = \min_{\pi: P_{\perp}} \{L(\pi)\}$$

$$\text{Deg}(\pi) = \max_{p_i \in \pi} \{\text{Deg}(p_i)\}$$

$$\text{Deg}_{PC}(P_{\perp}) = \min_{\pi: P_{\perp}} \{\text{Deg}(\pi)\}$$

# POLYNOMIAL CALCULUS WITH DUAL VARIABLES

| PCII

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

Annoying problem: Clause  $\bigvee_{i=1}^w \bar{x}_i$   
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 Face the problem This is a real problem for Gröbner basis-based algorithms. So when studying CNF formulas, study only  $k$ -CNF formulas for  $k=0(1)$ , or transform  $F$  to "equivalent" 3-CNF formula  $\tilde{F}$  with auxiliary variables

$$x_1 \vee x_2 \vee \dots \vee x_n \quad \bar{x}_0 \\ \vdots \quad \bar{x}_0 \vee x_1 \vee \bar{x}_1 \\ x_1 \vee \bar{x}_2 \vee \bar{x}_2 \\ \vdots \\ x_{n-1} \vee x_n \vee \bar{x}_n \\ \bar{x}_n$$

- ② 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  $\{x_i \mid i \in [n]\} \cup \{\bar{x}_i \mid i \in [n]\}$

COMPLEMENTARITY or  
NEGATION AXIOMS

$$x + \bar{x} = 1$$

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

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

PC III

to monomial

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

For a set of polynomials  $P$  over  $\{x_i\}_{i \in [n]}$

a PC refutation is a PCR refutation, so

$$S_{PCR}(P \vdash \perp) = S_{PC}(P \vdash \perp)$$

There are sets of polynomials for which

$$S_{PCR}(P_n \vdash \perp) = \text{poly}(n) \quad [= n^{O(1)}]$$

$$S_{PC}(P_n \vdash \perp) = \exp(-\Omega(n^5)) \quad [\text{dRLNS21}]$$

Not hard to show

$$\text{Deg}_{PCR}(P \vdash \perp) = \text{Deg}_{PC}(P \vdash \perp)$$

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  $\text{poly}(n)$  v.s.  $\exp(n^5)$
- degree  $O(1)$  v.s.  $\Omega(n/\log n)$

FACT 2 Polynomial calculus resolution efficiently simulates resolution

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

$\exists$  PCR refutation  $\pi_{PCR} : P \vdash \perp$  s.t.

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

$$\text{Deg}(\pi_{PCR}) \leq W(\pi_R)$$

Proof Simulate resolution refutation line by line.

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

PCIV

Examples: Tscinh formulas for  $\mathcal{F} = GF(2)$   
One-FPHP<sub>n</sub><sup>n+1</sup> for any field  $\mathcal{F}$

LEM4 [CEI 96] "Low degree  $\Rightarrow$  small size"

Suppose for  $P = \{x_j^2 - x_j \mid j \in [n]\}$  that  $\text{Deg}(P \vdash \perp) = d$ . Then  $S_{PC}(P \vdash \perp) = n^{O(d)}$

## MULTIDIMENSIONAL POLYNOMIAL CALCULUS

Multilinear monomial: all variables occurs 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  $\mathcal{F}[\vec{x}] / \{x_j^2 - x_j \mid j \in [n]\}$

All our <sup>size</sup> lower bounds work for multilinear (Mh) polynomial calculus. (Degree is not affected)

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

PROPOSITION 5 [see, e.g., [MN24]]

PCV

For unsat  $k$ -CNF formula  $F = \bigwedge_{i=1}^m C_i$ ,

$$d_{PC}(F \vdash \perp) = O(k \cdot m)$$

Proof sketch For  $j = 1, \dots, m$ , denote  $P_j = \prod_{i=1}^k (1 - c_i)$

(overloading  $C_i$  to be polynomial translation of  $C_i$ )

Finally get  $P_m = 1 - \prod_{i=1}^m (1 - c_i)$ . Polynomial  $P_m$  evaluates to 1 for all  $\{0, 1\}^n$ . But

every function  $f: \{0, 1\}^n \rightarrow \mathbb{F}$  has unique representation as multilinear polynomial, so  $P_m$  multilinearized must be equal to 1.  $\square$

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  $x_i^2 - x_j$ , or just use multilinear setting) over  $n$  variables

Then

$$\text{Deg}(P \vdash \perp) \leq \text{Deg}(P) + O(\sqrt{n \ln S_{PC}(P \vdash \perp)})$$

COROLLARY 7

$$S_{PC}(P \vdash \perp) = \exp\left(-2 \left( \frac{(\text{Deg}(P \vdash \perp) - \text{Deg}(P))^2}{n} \right)\right)$$

Proof Use same proof as we did for resolution

Use that restrictions can make monomials vanish.

QUESTION

What about version for tree-like proofs?

For resolution: Have seen several lower bound techniques PC VI

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 calculi without dual variables.

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  $\{0, 1\} \rightarrow \{+1, -1\}$   
E.g. [BG10, '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:

| EG I

## GENERALIZED CLAUSE-VARIABLE INCIDENCE

### GRAPH (CVG)

$F$  CNF formula over variables  $V$

- left vertex sets  $F_1, \dots, F_m$  for  $F = \bigcup_{i=1}^m F_i$
- right vertex set  $V_1, \dots, V_n$  for  $V = \bigcup_{j=1}^n V_j$
- OVERLAP of  $(V)$  =  $\max_{\alpha} \{ |V_i| : \alpha \in V_i \}$
- Edge  $(F_i, V_j)$  if  $\text{Vars}(F_i) \cap V_j \neq \emptyset$

An  $(F, V)_E$  - graph is an  $(s, \delta, E)$  - RESOLUTION

EXPANDER if

- it is a bipartite  $(s, \delta)$  - boundary expander,  
i.e.,  $F' \subseteq F$ ,  $|F'| \leq s \Rightarrow |\partial(F')| \geq \delta |F'|$
- Satisfier wins the RESOLUTION EDGE GAME  
on every edge  $(F_i, V_j)$

(1) Adversary plays  $\alpha$  s.t.  $\alpha(E) = T$

(2) Satisfier modifies  $\alpha$  on  $V_j$  to  $\alpha'$

(3) Satisfier wins if  $\alpha'(F_i \cap E) = T$

THEOREM 8 [BWOI] à la [MN24]

If  $F$  admits  $(s, \delta, E)$  - expander with  
overlap  $\ell$ , then  $W(F \vdash \perp) > \frac{\delta s}{2\ell}$

An  $(F, V)_E$  - graph is an  $(s, \delta, E)$  - PC EXPANDER if

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

- change of order ↗ (1) Satisfier commits to  $\varphi: V_j \rightarrow \{T, L\}$  satisfying  
any clauses involved in  $E$
- (2) Adversary plays  $\alpha$  s.t.  $\alpha(E) = T$
- (3) Satisfier wins if  $\alpha[s/V_j](F_i \cap E) = T$

What we want to prove in this & next lecture | EGII

THEOREM 9 [AR03, MN24]

If  $\mathcal{P}$  admits  $(s, \delta, \ell)$ -PC expands with overlap  $\ell$ , then  $\text{Deg}(\mathcal{P} \vdash \perp) > \frac{\delta s}{2\ell}$

Recall example

$w v x v y$

$\bar{u} v \bar{x} c$

$u v \bar{x}$

$x v \bar{y}$

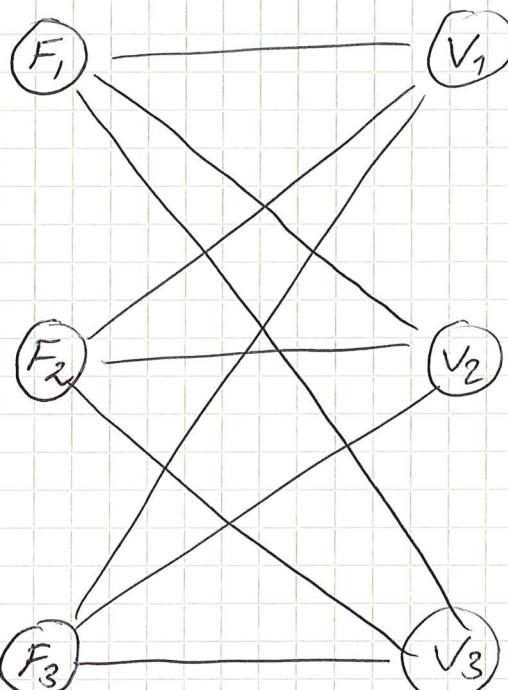
$x v \bar{z}$

$\bar{x} v y v z$

$x v y$

$x v z$

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



$\{w, y\}$

$\{x, y\}$

$\{u, w, z\}$

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

Already in resolution edge game, satisfies  
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  $y \mapsto \perp$

$$F_2 \setminus_{\{y \mapsto \perp\}} = \{x v \bar{z}, \bar{x} v z\}$$

Means we must have  $x = z$

But Adversary gets to choose  $z$  after Satisfier chooses  $x$ .

On edge  $(F_3, V_2)$  Satisfier has

wining strategy

Satisfier chooses  $\rho = \{x \mapsto T, y \mapsto \perp\}$

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

(less extreme examples are possible)

| EGII½

Prove Thm 9 by first giving second proof  
of Thm 8

| EG.III

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

From now on, all polynomials multilinear  
 $\varphi$  satisfies  $g$  if  $g$  vanishes under  $\varphi$   
(possibly after cancellation if  $\varphi$  partial assignment)

let us provide "good edge"-definition for  
- resolution  $\leftrightarrow$  semirespectful  
- polynomial calculus  $\leftrightarrow$  respectful

$\varphi$  RESPECTS polynomial set  $Q$ , or is Q-RESPECTFUL,  
if  $\forall g \in Q$  (a)  $\text{Vars}(g) \cap \text{dom}(\varphi) = \emptyset$  or  
(b)  $\varphi$  satisfies  $g$

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

set of variables  $V$  RESPECTS  $Q$  if  $\exists \varphi$   
 $\text{dom}(\varphi) = V$  s.t.  $\varphi$  respects  $Q$

$V$  SEMIRESPPECTS  $Q$ , or is Q-SEMIRESPPECTFUL,  
if  $\forall \sigma : \text{Vars}(Q) \setminus V \rightarrow \{\top, \perp\} \exists \varphi : V \rightarrow \{\top, \perp\}$   
such that  $\varphi$  satisfies  $Q \upharpoonright \sigma$

Ex  $Q = \{x_1, x_2, x_3 - x_1, x_3, x_1, x_4, x_5 - x_1, x_5\}$   
 $V_1 = \{x_1, x_2, x_3\}$        $V_2 = \{x_4, x_5\}$

$V_2$  is  $Q$ -respectful by  $\varphi = \{x_4 = x_5 = \top = 0\}$   
 $V_1$  is not, since assigning  $x_1$  affects but  
cannot satisfy all polynomials

$P, Q$  sets of polynomials,  $V$  set of variables EG IV

$P$  is  $Q$ -RESPECTFULLY SATISFIABLE BY  $V$  if  
 $V$  respects  $Q$  and this is shown by  $Q$ -respectful  
partial assignment  $\phi$  to  $V$  that satisfies  $P$ .

$P$  is  $Q$ -SEMIREPECTFULLY SATISFIABLE BY  $V$  if  
 $V$  semirespects  $P \cup Q$

Generalized CV16:

Polynomials  $P$  over variables  $V$

Partition  $P = P_1 \cup \dots \cup P_m \cup Q$

Divide  $V = V_1, V_2, \dots, V_n$

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

Overload  $V = \{V_1, \dots, V_n\}$

The  $(\mathcal{U}, V)_Q$ -graph has

- left set  $\{P_1, P_2, \dots, P_m\}$

- right set  $\{V_1, V_2, \dots, V_n\}$

- edges  $(P, V)$  if  $\text{Vars}(P) \cap V \neq \emptyset$

$(P, V)$  are  $Q$ -RESPECTFUL NEIGHBOURS

if  $P$   $Q$ -respectfully satisfiable by  $V$

$(P, V)$  are  $Q$ -SEMIREPECTFUL NEIGHBOURS

if  $P$   $Q$ -semirespectfully satisfiable

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

In our example graph

$F_2 \leftrightarrow V_2$   $\leftarrow$   $E$ -semirespectful neighbours  
 $F_3 \leftrightarrow V_2$   $\leftarrow$   $E$ -respectful neighbours

Define boundary expansion by

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

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

$$\partial_Q^{SR}(U') = \{ V \in \partial(U') \text{ connected with semi-respectful edges} \}$$

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

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

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

Pros:

- 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:

Def VI

F CNF formula that admits  $(s, \delta, \xi, Q)$ -semirespectful boundary expansion with overlap  $\ell$

P is set of (multilinear) polynomials that admit  $(s, \delta, \xi, Q)$ -respectful expansions with overlap  $\ell$

### THEOREM 10

Suppose for all  $\mathcal{U}' \subseteq \mathcal{U}, |\mathcal{U}'| \leq s$  that  $\mathcal{U}' \cup Q$  is satisfiable. Then  $|W(F+1)| > \frac{\sqrt{s} - 2\xi}{2\ell}$

### THEOREM 11

Suppose  $|\text{Vars}(p)| \leq \frac{\sqrt{s} - 2\xi}{2\ell} \quad \forall p \in P$   
and  $\forall \mathcal{U}' \subseteq \mathcal{U}, |\mathcal{U}'| \leq s, \mathcal{U}' \cup Q$  is satisfiable.

Then

$$|\text{Deg}(P+1)| > \frac{\sqrt{s} - 2\xi}{2\ell}$$

### COROLLARY 12

If  $\xi = 0$ , then

$$|W(F+1)| > \frac{\sqrt{s}}{2\ell}$$

### COROLLARY 13

If  $|\text{Vars}(p)| \leq \frac{\sqrt{s}}{2\ell}$  and  $\xi = 0$ ,

then  $|\text{Deg}(P+1)| \geq \frac{\sqrt{s}}{2\ell}$

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  $F = \bigwedge_{F \in U} F \wedge Q = \mathcal{U} \wedge Q$  over  
 $V = \bigcup_{i=1}^m V_i$  represented by  $(\mathcal{U}, V)_Q$ -graph that  
is  $(s, \delta, \xi, Q)$ -semirespectful expander with overlap  $\ell$ .  
Set  $\xi=0$  for simplicity — simple, but annoying,  
to just carry additive  $\xi$  around.

Want to associate clause  $C \in \mathcal{C}$  with subset of  
clauses of  $F$  that could have been used to derive  $C$   
Last because: Minimalist approach — identify smaller  
such set

This because: Maximalist approach — identify larger  
(but not too large) set

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

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

$\mathcal{U}' \subseteq \mathcal{U}$  is (SEMIREPECTFULLY) CONTAINED, or just

$(s, C)$  - contained, if

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

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

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

Given small-width resolution deviation EG VIII  
 from  $F$ , show for all  $C \in \pi$

- (1)  $\text{Sup}_{\pi}^{\text{SR}}(C)$  is not too large
- (2)  $\text{Sup}_{\pi}^{\text{SR}}(C) \cup Q = C$

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

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

Proof  $\text{Sup}_{\pi}^{\text{SR}}(C) = \bigcup_i \mathcal{U}_i$  for  $(s, C)$ -contained  $\mathcal{U}_i$ .  
 Fix such  $\mathcal{U}_i$ . By expansion  $(|\mathcal{U}_i| \leq s)$

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

That is, by  $(s, C)$ -containedness

$$|\mathcal{U}_i| \leq |\partial_Q^{\text{SR}}(\mathcal{U}_i)|/\delta \leq |N(C)|/\delta \quad (**)$$

Furthermore

$$\begin{aligned} |N(C)| &\leq |\text{Vars}(C)| \cdot \text{ol}(V) \leq W(C) \cdot \ell \\ &\leq \boxed{\delta s/2} \end{aligned} \quad (***)$$

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  $(s, C)$ -contained

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

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

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

LEMMA 15 Suppose  $\pi$  resolution derivation from  $F$ , in width  $W(\pi) \leq \frac{\delta s}{2\ell}$ . Then  $\forall C \in \pi \quad \text{Sup}_s^{SR}(C) \cup Q \models C$ .

Proof By forward induction over derivation  $\pi$ .

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

$$C \in F \in \text{Sup}_s^{SR}(C).$$

Consider any  $V \in N(F)$ . If  $V \in N(C)$ , we're good so suppose not. Then  $V \cap \text{Vars}(C) = \emptyset$ . If

$Q \models C$  we're still good, so suppose  $Q \not\models C$

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

Clearly, cannot change  $\rho$  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  $\text{Sup}_s^{SR}(C_1) \cup Q \models C_1$

Hence

$$\boxed{\text{Sup}_s^{SR}(C_1) \cup \text{Sup}_s^{SR}(C_2) \cup Q \models C}$$

We claim

$$\boxed{((\text{Sup}_s^{SR}(C_1) \cup \text{Sup}_s^{SR}(C_2)) \cap \text{Sup}_s^{SR}(C)) \cup Q \models C}$$

For proving write

$$S = \text{Sup}_s^{SR}(C_1) \cup \text{Sup}_s^{SR}(C_2)$$

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

$$\boxed{(S \cap \text{Sup}_s^{SR}(C)) \cup Q \models C}.$$

LEG X

To show

$$(S \cap \text{Sup}^{SR}(C)) \cup Q \models C$$

Show that if  $S \setminus \text{Sup}^{SR}(C) \neq \emptyset$ , then can decrease size of  $S$  while maintaining implication.

$$S \cup Q \models C$$

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

$$S \setminus \{F_V\} \cup Q \not\models C$$

Then  $\exists g$  s.t.  $g(S \setminus \{F_V\}) = T$   $g(Q) = T$

$g(C) = L$  and (by necessity)  $g(F_V) = L$

By semi-respectfulness, can modify  $g$  on  $V$  to get  $g'$  s.t.  $g'(F_V \wedge Q) = T$

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

By induction, can shrink  $S$  until

$$S \subseteq \text{Sup}^{SR}(C) \text{ as claimed}$$



Remains to prove that if  $|U'| \leq s$ , then

$U' \cup Q$  is satisfiable. This is exactly

the same peeling argument as last time if  $\xi = 0$

If  $\xi > 0$ , need satisfiability of  $U' \cup Q$  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  
[Alekhno - Razborov '03] and  
[Miksa - Nordström '24], that  
yields degree lower bounds