

LECTURE 26

Cutting planes proof system

Input: Inconsistent system of 0-1 linear inequalities

Resolution: Denote  $O \geq 1$

Configuration-style proof

At each derivation step

- (1) DOWNLOAD axiom constraint
- (2) apply INFERENCE rule to constraints in memory
- (3) ERASE constraint

Inference rules

Variable axioms

$$\frac{}{x \geq 0} \quad \frac{}{-x \geq -1}$$

Addition

$$\frac{\sum_i a_i x_i \geq A \quad \sum_j b_j x_j \geq B}{\sum_i (a_i + b_i) x_i \geq A + B}$$

Multiplication

$$\frac{\sum_i a_i x_i \geq A}{\sum_i c a_i x_i \geq cA} \quad c \in \mathbb{N}^+$$

Division

$$\frac{\sum_i c a_i x_i \geq A}{\sum_i a_i x_i \geq \lceil A/c \rceil}$$

Complexity measures:

Length = # constraints in derivation

Line space = max # constraints in memory

What about magnitude of coefficients?

[Buss & Clegg '96] building on [Cook, Coullard & Turan '87]

- (a) Cutting planes with division only by fixed  $k \geq 2$   
is as powerful as general cutting planes  
(up to polynomial factors)
- (b) Suppose coefficients and constants have absolute values  $\leq B$  and that cutting planes require input in length  $\lambda$ . Then  $\exists$  representation in length  $O(\lambda^3 \log B)$  with coefficients and constants of absolute value  $O(\lambda^2 \cdot B \cdot 2^k)$ .

So coefficients need not have more than polynomial # bits / exponential magnitude

[Dadush & Tivari '20] proved analogous result for stabbing planes.

OPEN PROBLEM: Possible to bring this down to logarithmic # bits / polynomial magnitude?  
Buss & Clegg state that this was their goal.

Still remains open!

What would separating formulas look like?

Define  $CP^*$  as cutting planes, but on any decision in the coefficients and constant terms should have size at most polynomial in size of input i.e., magnitude = logarithmic # bits

Aside:  $CP^*$  also defined by requiring integers to have magnitude at most polynomial in input size and exponential in # steps of refutation. Same definition if we insist on polynomial-length representations. We will define  $CP^*$  in terms of input.

Can we prove that there is something  $CP$  can do efficiently that  $CP^*$  cannot?

Yes! [dRMNPRV '20]

$$\{F_n\}_{n=1}^{2^\infty}$$

There are families of CNF formulas such that

- Cutting planes refutes  $F_n$  in (roughly) quadratic length and constant line space simultaneously.
- $CP^*$  cannot refute  $F_n$  in subexponential length and subpolynomial line space simultaneously

MAIN TECHNICAL INGREDIENT

Lifing theorem using equality gadget

HIGH-LEVEL IDEA

Take HORN FORMULA: At most 1 positive literal/ clause  
 Can be refuted by deriving unit clauses  $\{z_i\}$   
 in some order in resolution

Make this line-space-efficient in cutting planes  
 by deriving

$$\sum_{i=0}^{n-1} 2^i z_i = \sum_{i=0}^{n-1} 2^i = 2^n - 1$$

(Note that  $\sum_i a_i z_i = A$  is syntactic  
 sugar for

$$\begin{aligned} \sum_i a_i z_i &\geq A \\ \sum_i -a_i z_i &\geq -A \end{aligned} \quad )$$

Lift formula  $C$  with EQUITY GADGET

$$EQ(x,y) = \begin{cases} 1 & \text{if } x=y \\ 0 & \text{o/w} \end{cases} \quad x,y \in \{0,1\}$$

EXAMPLE

$$C = z_1 \vee \overline{z}_2$$

$$\text{Then } C[EQ] = C \circ EQ =$$

$$\begin{aligned} &(x_1 \vee \overline{y}_1 \vee x_2 \vee y_2) \\ \wedge &(x_1 \vee \overline{y}_1 \vee \overline{x}_2 \vee \overline{y}_2) \\ \wedge &(\overline{x}_1 \vee y_1 \vee x_2 \vee y_2) \\ \wedge &(\overline{x}_1 \vee y_1 \vee \overline{x}_2 \vee \overline{y}_2) \end{aligned}$$

(A) Prove that line-space-efficient CP algorithm  
still works for F O EQ if F Horn formula

CP\* V

Derive (n) equalities

$$\sum_{i=0}^n 2^i (x_i - y_i) = 0 \quad (*)$$

Whenever, say,  $z_k$  followed from

$$\begin{array}{c} z_i \\ z_j \\ \hline z_i \vee \overline{z_j} \vee z_k \end{array}$$

"decode"

$$x_i = y_i$$

$$x_j = y_j$$

from (\*) and apply to

$$(\overline{z_i} \vee \overline{z_j} \vee z_k) \circ EQ$$

to derive

$$x_k = y_k$$

and add to (\*). Want to do this length-  
 and space-efficiently

Yields upper bound for general cutting planes.

(B) Suppose there is a short, low-space-efficient refutation  $\pi^*$  in  $CP^*$  of  $F_n \circ EQ$  in length  $L$  and line space  $S$

$CP^* \leq$

Yields deterministic communication protocol for  $\text{Search}(F_n) \circ EQ$  in cost

$$S \leq L \log L$$

Alice & Bob can evaluate the inequalities and send number - logarithmic #bits

Prove lifting theorem relating communication complexity  $D^{cc}$  with decision tree query complexity  $D^{dt}$  by

$$D^{cc}(\text{Search}(F) \circ EQ) \geq D^{dt}(\text{Search}(F))$$

Plug in Horn formulas with large decision tree query complexity - PEBBLING FORMULAS

DONE! Right?

Except [Tziforoff & Mukhopadhyay '19] show that such lifting theorem is NOT TRUE for

- equalizing gadget
- relations/search problems (as opposed to functions)

So instead

- Use equalizing gadget over non-constant # bits
- Lift Nullstellensatz refutation degree (happens to be = query complexity for pebbly formulas)

$$EQ_g : \{0,1\}^g \times \{0,1\}^g \rightarrow \{0,1\}$$

$$EQ_g(x,y) = 1 \text{ iff } x = y$$

MAIN LIFTING THEOREM

Suppose that

- $F$  minimally unsatisfiable CNF formula over  $n$  variables
- $F$  any field
- $g: X \times Y \rightarrow \{0,1\}$  any gadget such that

$$\text{rank}_F(g) \geq \frac{6c n}{\text{Deg}_{NS}(F+1)}$$

Then

$$D^{\text{cc}}(\text{Search}(F) \circ g) \geq \text{Deg}_{NS}^F(F+1)$$

UPPER BOUNDS FOR CP

Suppose that

- $G$  any DAG with constant fan-in & single sink
- $g \in W^+$ ,  $g = O(\log \log n)$

Then the formula  $\text{Peb}_G \circ \text{EQ}_g$  has

- $O(n \log \log n)$  variables
- $\tilde{\Theta}(n)$  clauses of width  $O(\log \log n)$
- cutting planes refutation in simultaneous length  $\tilde{\Theta}(n^2)$  and line space  $O(1)$

$\tilde{O}(f(n))$  means  $O(f(n)(\log(f(n)))^k)$

for some constant  $k$

LOWER BOUND FOR CP\*

Any CP\* refutation of  $\text{Peb}_G \circ \text{EQ}_g$  as above in length  $L$  and line space  $S$  must satisfy

$$S \log L = \Omega(n / \log^2 n)$$

Equality gadget provides a sweet spot!

CP VIII\*

- Hard for deterministic communication  
(which can use CP\* proofs)
- Easy for randomized and real communication (otherwise we would get hardness for general cutting planes)

### SOME OPEN PROBLEMS

- ① Size separation for CP vs CP\*
- ② Line space lower bounds for CP\*
- ③ True length-space trade-offs for CP\* that do not apply for CP
- ④ Direct lower bound proof for parity decision tree query complexity for pebbling formulas

A (TOTAL) SEARCH PROBLEM is a relation  $S \subseteq I \times O$  such that for all  $z \in I$  there exists  $o \in O$  for which  $(z, o) \in S$

Think of this as computational task:

Given  $z$ , find  $o$  s.t.  $(z, o) \in S$

If  $I = I^n$  has product structure, and  $g: X \times Y \rightarrow I$  is a function (a GADGET), then the COMPOSED/LIFTED SEARCH PROBLEM  $S \circ g^n \subseteq (X^n \times Y^n) \times O$  is the task, given  $x \in X^n$  and  $y \in Y^n$  to find  $o$  s.t.  $(g^n(x, y), o) \in S$  where

$$g^n(x, y) = (g(x_1, y_1), g(x_2, y_2), \dots, g(x_n, y_n))$$

Our previous lifting theorems worked for any search problem

Now we have to focus on FALSIFIED CHOICE SEARCH PROBLEM: Given assignment  $\alpha$  to (fixed) unsatisfiable CNF formula  $F$ , find clause  $C$  falsified by  $\alpha$ .

Denote this problem Search( $F$ )

Lifted search problems yield natural communication problems

### DETERMINISTIC COMMUNICATION PROTOCOL

Two players Alice with input  $x \in X^n$   
Bob with input  $y \in Y^n$

Protocol tree  $\Pi$

- Every internal node labelled by function  
 $f^A_r: X^n \rightarrow \{0,1\}$  (Alice speaks) or  
 $f^B_r: Y^n \rightarrow \{0,1\}$  (Bob speaks)
- Every internal node has <sup>two</sup> outgoing edges labelled 0 and 1, respectively
- Input  $x \in X^n \times Y^n$  defines path to leaf  $\ell_x$
- Leaf  $\ell_x$  should be labelled by answer to  $f^A_r g^n$
- Cost of protocol  $\Pi$  = length of longest path  
= max # bits communicated
- For problem  $P$ , write  $D^{cc}(P)$  for minimal cost of any protocol

Given any gadget  $g: \{0,1\}^q \times \{0,1\}^q \rightarrow \{0,1\}$   
and CNF formula  $F$ , can define

### LIFTED FORMULA $F[g]$ or $F \circ g$ by

- replace all literals  $z_i$  by CNF encoding of  $g(x_{i,1}, \dots, x_{i,q}, y_{i,1}, \dots, y_{i,q})$
- replace all literals  $\bar{z}_i$  by CNF encoding of  $\neg g(x_{i,1}, \dots, x_{i,q}, y_{i,1}, \dots, y_{i,q})$
- expand all clauses  $C \in F$  to CNF in canonical way

## OBSERVATION 1

For any unsatisfiable CNF formula  $F$  and any gadget  $g$ ,

$$D^{cc}(\text{Search}(F \cdot g)) \geq D^{cc}(\text{Search}(F)) \cdot \text{rank}_F(g)$$

We will be interested in the RANK of gadgets

For  $g: X \times Y \rightarrow \{0, 1\}$ , the RANK of  $g$  over the field  $\mathbb{F}$ , denoted  $\text{rank}_{\mathbb{F}}(g)$ , is the rank over  $\mathbb{F}$  of the matrix with

- rows indexed by  $x \in X$
- columns indexed by  $y \in Y$
- the cell  $(x, y)$  containing  $g(x, y)$

EXAMPLE The gadget  $\text{EQ}^q: \{0, 1\}^q \times \{0, 1\}^q \rightarrow \{0, 1\}$  defined by

$$\text{EQ}^q(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

has  $\text{rank}_{\mathbb{F}}(\text{EQ}^q) = 2^q$  over any field  $\mathbb{F}$

## LEMMA 2 [HN12]

If there is a cutting planes refinement  $\Pi: F \vdash L$  in length  $L$ , the space  $S$ , and coefficients and constant terms <sup>(absolute values)</sup> bounded by  $B$ , where  $F$  is over  $n$  variables, then

$$D^{cc}(\text{Search}(F)) = O(S \cdot (\log B + \log n) \log L)$$

Given field  $F$

Polynomials  $P = \{p_1, \dots, p_m\}$  over  $x_1, \dots, x_n$

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

a NULLSTELLENSATZ REFUTATION is a sequence of polynomials  $g_1, \dots, g_m, r_1, \dots, r_n$  s.t. the syntactic equality

$$\left[ \sum_{i=1}^m g_i p_i + \sum_{j=1}^n r_j (x_j^2 - x_j) = 1 \right] (*)$$

holds (after cancellations).

Proof system for CNF formulas by translating clauses

$$C = \bigvee_{z \in P} z \vee \bigvee_{z \in N} \bar{z}$$

to

$$p(C) = \prod_{z \in P} (1-z) \circ \prod_{z \in N} z$$

The DEGREE of a Nullstellensatz refutation is the largest total degree of a left-hand side polynomial in  $(*)$

Deg<sub>NS</sub>(F+1) = min NS degree of any refutation of  $F$  over  $F$

Let  $\mathcal{P} \subseteq \mathbb{F}[z]$  be set of polynomials and  $d \in \mathbb{N}^+$ .  
A  $d$ -DESIGN for  $\mathcal{P}$  is a mapping  $D$  of polynomials in  $\mathbb{F}[z]$  of degree  $\leq d$  to  $\mathbb{F}$  such that

- (1)  $D$  is linear
- (2)  $D(1) = 1$
- (3)  $D(qp_i) = 0$  for all  $p_i \in \mathcal{P}$  and all  $q$  such that  $\deg(qp_i) \leq d$
- (4)  $D(z_i^2 q) = D(z_i q)$  for all  $q$  s.t.  $\deg(q) \leq d-1$

THEOREM 3 [Buss '98]

Suppose  $\mathcal{P} \subseteq \mathbb{F}[z]$  is such that  $z_i^2 - z_i \in \mathcal{P}$  for all  $z_i$ . Then  $\boxed{\text{Deg}_{\mathcal{P}}^{\mathbb{F}}(\mathcal{P}+1) > d}$  if and only if  $\mathcal{P}$  has a  $d$ -design.

THEOREM 4 [DRMNRRV '20]

For any single-source DAG  $G$  and any field  $\mathbb{F}$  it holds that  $\boxed{\text{Deg}_{\mathcal{P}_G}^{\mathbb{F}}(\mathcal{P}_G + 1)}$  coincides with the reversible pebbling price of  $G$ .

Proof sketch Let  $V(G) = \{1, 2, \dots, n\}$

Identify  $S \subseteq [n]$  with  $z_S = \prod_{i \in S} z_i$ .

For fixed  $d \in \mathbb{N}^+$ , define

$D(z_S) = 1$  is pebble configuration readable from  $\emptyset$  by reversible pebbling in space  $\leq d$

$D(z_S) = 0$  otherwise

This is a  $d$ -design iff reversible pebbling price of  $G > d$ .

Just for the record,  $P_{\text{BG}}$  is the set of polynomials

- $1 - z_s$  for each source vertex  $s$
  - $(1 - z_v) \prod_{u \in \text{pred}(v)} u$  for non-source vertex  $v$  with immediate predecessors  $\text{pred}(v)$
  - $z_t$  for the sink/target vertex  $t$
  - and also  $z_v^2 - z_v$  for all  $v$
- 

In what remains of this lecture, focus on Nullstellensatz lifting theorem that yields lower bound for  $\text{CP}^*$

### LIFTING THEOREM, FULL VERSION

Suppose

- Unsatisfiable  $k$ -CNF formula over  $n$  variables
- $F$  any field
- $g: X \times Y \rightarrow \{0, 1\}$  with  $R_g = \text{rank}_F(g) \geq 3$
- $D_F = \text{Deg}_{NS}^F(F+1)$

Then

$$D^{cc}(\text{Search}(F) \circ g^n) \geq D_F \log\left(\frac{D_F \cdot R_g}{e^n}\right) - \frac{4n \log e - \log k}{R_g}$$

Earlier version can be shown to follow from this

More non-obvious point: We should have

$\log k \leq k \leq D_F$  if clauses of width  $k$  are needed on NS certificate

Lifting theorem relies (very) heavily on [Pitassi-Robec '18]

Let  $U, V$  be sets

A COMBINATORIAL RECTANGLE  $R$  in  $U \times V$   
is a set  $R = A \times B$  for  $A \subseteq U, B \subseteq V$

A RECTANGLE PARTITION  $\mathcal{P} = \{R_i\}_{i \in [t]}$  of  $U \times V$   
is a set of rectangles such that for all  $(u, v) \in U \times V$   
 $\exists! R_i \in \mathcal{P}$  s.t.  $(u, v) \in R_i$

FACT Deterministic communication protocol  
splits input space into rectangle partition.

A RECTANGLE COVER  $\mathcal{R} = \{R_i\}_{i \in [t]}$  of  $U \times V$   
is a set of rectangles such that  $U \times V \subseteq \bigcup_{i \in [t]} R_i$

Given  $U \times V$  matrix  $A$  and rectangle  $R$  in  $U \times V$ ,  
let  $A|R$  be submatrix of  $A$  induced on  $R$

DEFINITION (Razborov)

Let  $\mathcal{R}$  be rectangle cover of  $U \times V$  and  
A  $U \times V$  matrix over  $\mathbb{F}$ . Then the  
IF-RANK MEASURE of  $\mathcal{R}$  at  $A$  is

$$\mu_{\mathbb{F}}(\mathcal{R}, A) = \frac{\text{rank}_{\mathbb{F}}(A)}{\max_{R \in \mathcal{R}} \text{rank}_{\mathbb{F}}(A|R)}$$

Can be used to show lower bounds for  
deterministic communication (and several  
other computational models — see  
Robere's PhD thesis in 2018)

Notation If  $A \in \mathbb{F}^{n \times m}$  write  $A_j$  /  $A_{\mathcal{J}}$  for  
projection of  $A$  to coordinate  $j$  / coordinates  $\mathcal{J}$

## DEFINITION

Let  $F$  unsatisfiable CNF formula over  $n$  variables  
 $g: X \times Y \rightarrow \{0, 1\}$  gadget

For  $C \in F$ , say that combinatorial rectangle  
 $R \subseteq X^n \times Y^n$  is  $C$ -STRUCTURED if

- (1)  $\underline{g^n(x,y)} \text{ falsifies } C \quad \forall (x,y) \in R$
- (2)  $\forall i \notin \text{Vars}(C) \quad R_i = X \times Y$

A rectangle cover is  $F$ -STRUCTURED if all  
rectangles in it are  $C$ -structured for  $C \in F$

## LEMMA 5

Let

- $F$  unsatisfiable CNF formula over  $n$  variables
- $g: X \times Y \rightarrow \{0, 1\}$  gadget
- $\mathbb{F}$  field

Then

$$\boxed{D^{cc}(\text{Search}(F) \circ g) \geq \max_A \min_R \log_{|\mathbb{F}|} \mu_F(R, A)}$$

where  $A$  ranges over  $X^n \times Y^n$  matrices over  $\mathbb{F}$   
and  $R$  over  $F$ -structured rectangle covers

Proof Let  $\Pi$  be protocol solving  $\text{Search}(F) \circ g$  and  
let  $P$  be induced monochromatic rectangle partition  
Every  $R = A \times B$  in  $P$  labelled by  $C \in F$   
For all  $(x,y) \in R$   $\underline{g^n(x,y)} \text{ falsifies } C$

We have  $A \subseteq X^{\text{Vars}(C)} \times X^{[n] \setminus \text{Vars}(C)}$   
 $B \subseteq Y^{\text{Vars}(C)} \times Y^{[n] \setminus \text{Vars}(C)}$

(overloading  $Z_i$  and index  $i$ )

$$\text{Let } A' = A_{\text{vars}(c)} \times X^{[n] \setminus \text{vars}(c)}$$

$$B' = B_{\text{vars}(c)} \times Y^{[n] \setminus \text{vars}(c)}$$

$$R' = A' \times B'$$

Then  $R' \supseteq R$  and  $R'$  is  $C$ -structured

Let  $R$  be  $F$ -structured rectangle cover obtained in this way.

[Razborov '90] proved that if  $P$  rectangle partition and  $R$  rectangle cover such that  $\forall R \in P \exists R'(R) \in R$  for which  $R \subseteq R'(R)$ , then

$$\text{rank}_F(A) \leq \sum_{R \in P} \text{rank}_F(A|R)$$

$$\leq \sum_{R \in P} \text{rank}_F(A|R'(R))$$

$$\leq |P| \max_{R' \in R} \text{rank}_F(A|R')$$

or, in other words,

$$|P| \geq \frac{\text{rank}_F(A)}{\max_{R' \in R} \text{rank}_F(A|R')} = \mu_F(R, A)$$

Lemma  
A tree with  $T$  leaves has height  $\geq \log T$ , so

$$D^{cc}(\text{Search}(F) \circ g) \geq \log |P| \geq \log \mu_F(R, A)$$

as claimed □

For a clause  $C \in F$  over  $z_1, \dots, z_n$ , the CERTIFICATE of  $C$   $\text{Cert}(C)$  is the smallest partial assignment  $\pi$  falsifying  $C$ .

$$\text{Cert}(F) = \{ \text{Cert}(C) \mid C \in F \}$$

For  $\alpha \in \{0, 1\}^n$ ,  $\alpha$  AGREES with  $\pi \in \text{Cert}(F)$  if  $\pi(z_i) = \alpha_i$  if  $\pi(z_i) \neq *$

If  $F$  is unsatisfiable, every  $\alpha$  agrees with some  $\pi \in \text{Cert}(F)$

### DEFINITION

Let

- $F$  unsatisfiable CNF formula
- $\mathbb{F}$  field
- $p \in \mathbb{F}[z]$  multilinear polynomial

The  $\mathbb{F}$ -ALGEBRAIC GAP COMPLEXITY of  $F$  at  $p$

is

$$\text{gap}_{\mathbb{F}}(F, p) = \deg(p) - \max_{\pi \in \text{Cert}(F)} \deg(p|\pi)$$

The  $\mathbb{F}$ -algebraic gap complexity of  $F$  is

$$\text{gap}_{\mathbb{F}}(F) = \max \{ \text{gap}_{\mathbb{F}}(F, p) \mid \deg(p) = n \}$$

**THEOREM 6** [Pitassi & Robere '18]

For any unsatisfiable formula  $F$  over  $n$  variables and any field  $\mathbb{F}$ , it holds that

$$\text{Deg}_{\text{NS}}^{\mathbb{F}}(F \vdash \perp) = \text{gap}_{\mathbb{F}}(F)$$

This theorem would be worth a separate lecture...

What we want to do now

- ① Take polynomial  $p \in \mathbb{F}[\vec{Z}]$  with very gap complexity
- ② Compose  $[p \circ g^n]$  to get  $X^n \times Y^n$  matrix  $A$
- ③ Argue that  $A$  yields large F-rank measure
- ④ This establishes communication complexity lower bound

Let  $p \in \mathbb{F}[\vec{Z}]$  multilinear polynomial

With notation inspired by Fourier analysis,

write

$$p = \sum_{S \subseteq [n]} \hat{p}(S) \prod_{i \in S} z_i$$

For  $g: X \times Y \rightarrow \{0, 1\}$ , define lifted polynomial

$$p \circ g^n(x, y) = \sum_{S \subseteq [n]} \hat{p}(S) \prod_{i \in S} g(x_i, y_i)$$

Overload notation to view  $p \circ g^n$  as  
 $X^n \times Y^n$  matrix with entry  $(x^*, y^*) \in X^n \times Y^n$   
containing  $p \circ g^n(x^*, y^*)$

### THEOREM 7 [dRMNPRV '20]

For any multilinear  $p \in \mathbb{F}[\vec{Z}]$  and  
any  $g: X \times Y \rightarrow \{0, 1\}$  with  $\text{rank}_F(g) \geq 2$

it holds that

$$\sum_{S: \hat{p}(S) \neq 0} (\text{rank}_F(g) - 2)^{|S|} \leq \text{rank}_F(p \circ g^n) \leq \sum_{S: \hat{p}(S) \neq 0} \text{rank}_F(g)^{|S|}$$

Closely follows ideas in [PR '18] with  
minor but crucial twists

Lemma 5 together with the next theorem yields the main lifting theorem

### THEOREM 18 [dRMNPRV'20]

Let

- F unsatisfiable k-CNF formula over n variables
- F any field
- $g : X \times Y \rightarrow \{0,1\}$  gadget with  $\text{rank}_F(g) \geq 3$

Then there is a  $X^n \times Y^n$  matrix  $A$  over  $F$  such that for any  $F$ -structured rectangle cover  $R$  of  $X^n \times Y^n$  it holds that

$$\mu_F(R, A) \geq \frac{1}{k} \left( \frac{\text{Deg}_{ns}(F+1) \cdot \text{rank}_F(g)}{en} \right)^{\text{Deg}_{ns}(F+1)} \exp\left(\frac{-4n}{\text{rank}_F(g)}\right)$$

Proof sketch

Fix  $P$  s.t.  $\text{gap}_F(F) = \text{gap}_F(F, P)$

Let  $A = P \circ g^n$  and analyze

$$\mu_F(R, P \circ g^n) = \frac{\text{rank}_F(P \circ g^n)}{\max_{R \in R} (\text{rank}_F(P \circ g^n | R))}$$

using Thm 7.

We get numerator  $\geq (\text{rank}_F(g) - 2)^n$  (+)

For denominators, argue that for  $C$ -structured  $R$

$$P \circ g^n | R = \begin{pmatrix} M & \cdots & M \\ \vdots & \ddots & \vdots \\ M & \cdots & M \end{pmatrix}$$

for  $M = (P \cap \pi) \circ g^{[n]} | \text{Vars}(C)$  for  $\pi = \text{Cert}(C)$

But then

$$\text{rank}_F(p \circ g^n | R) = \text{rank}_F((p|_T) \circ g^{\lceil n \rceil \text{Vars}(c)}) \\ \leq \sum_{S: \widehat{p|_T}(S) \neq 0} (\text{rank}_F(g))^{|S|}$$

and  $\widehat{p|_T}(S) \neq 0$  only for  $|S| \leq n - \text{gap}_F(F)$

We can choose  $p$  so that

$$\widehat{p}(S) = 0 \quad \text{for } |S| < n - \text{gap}_F(F)$$

Since monomials of this low degree don't affect the algebraic gap

$\pi = \text{Cert}(c)$  assigns  $\leq k$  variables, so can bring down degree by  $\leq k$

Summing monomials in  $p|_\pi$

- None of degree  $> n - \text{gap}_F(F)$
- At most  $\binom{n}{\text{gap}_F(F)-i}$  of degree  $n - \text{gap}_F(F)$   
for  $i=0, \dots, k$
- None of degree  $< n - \text{gap}_F(F) - k$

So

$$\sum_{S: \widehat{p|_T}(S) \neq 0} (\text{rank}_F(g))^{|S|} \leq \sum_{i=0}^k \binom{n}{\text{gap}_F(F)-i} \text{rank}_F(g)^{n - \text{gap}_F(F) - i} \\ \leq k \binom{n}{\text{gap}_F(F)} \text{rank}_F(g)^{n - \text{gap}_F(F)} \quad (\neq)$$

P~~XIV~~

Work on ( $\dagger$ ) and ( $\ddagger$ ) to get

$$\mu_F(R, \rho \circ g^n) \geq \frac{1}{k} \left( \frac{\text{gap}_F(F) \cdot \text{rank}_F(g)}{e^n} \right)^{\text{gap}_F(F)} \exp\left(-\frac{4n}{\text{rank}_F(g)}\right)$$

and then use that Thm 6 says  
that

$$\text{gap}_F(F) = \text{Deg}_{NS}^F(F+1)$$

◻