

# CAN A NATURAL NUMBER BE NEGATIVE?

Iddo Tzameret

*Joint work with*

Yaroslav Alekseev, Dima Grigoriev and Edward Hirsch

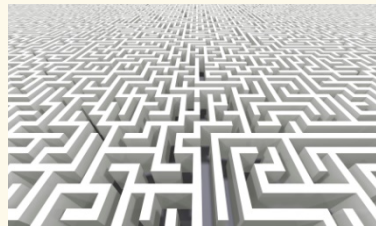


# CAN A NATURAL NUMBER BE NEGATIVE?

Iddo Tzameret

*Joint work with*

Yaroslav Alekseev, Dima Grigoriev and Edward Hirsch



yes

# The Conceptual Framework

## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .



## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \dots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

## The Binary Value Principle

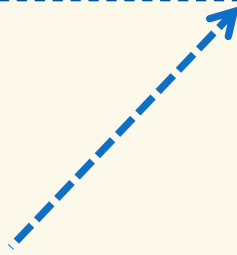
$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

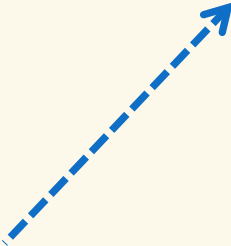
for  $x_i \in \{0,1\}$ , all  $i$ .



## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .



Algebraic and  
Semi-Algebraic proofs

## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

Algebraic and  
Semi-Algebraic proofs



## The Binary Value Principle

$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

Algebraic and  
Semi-Algebraic proofs

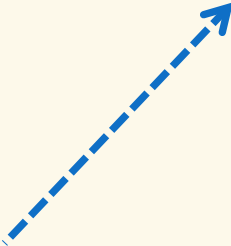
Algebraic  
Circuit  
Complexity

## The Binary Value Principle

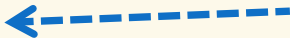
$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

Algebraic and  
Semi-Algebraic proofs



Algebraic  
Circuit  
Complexity



## The Binary Value Principle

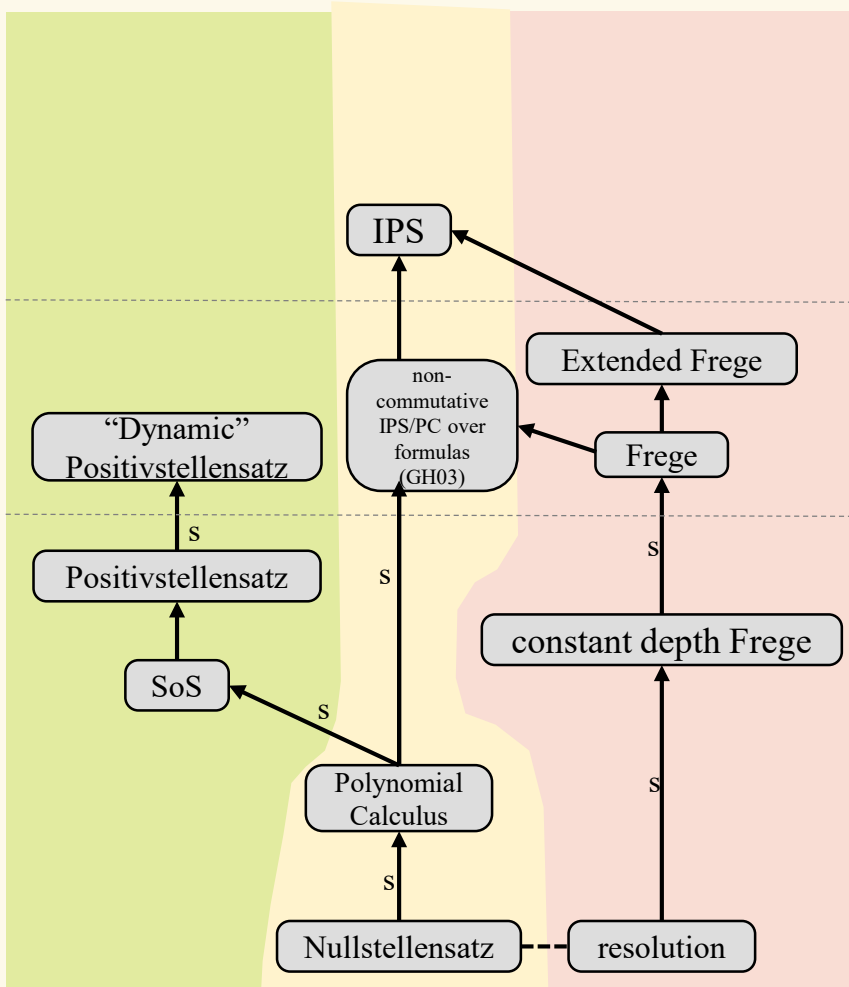
$$x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$$

for  $x_i \in \{0,1\}$ , all  $i$ .

Algebraic and  
Semi-Algebraic proofs

Algebraic  
Circuit  
Complexity

# The Context: Proof Complexity



- Proof systems:
  - A way to analyse algorithms run-time:
    - Each proof-line is a step in the algorithm
  - A way to approach **NP** vs **coNP** (hence **P** vs **NP**) problem:
    - Size lower bounds against proofs of UNSAT rule out that certain kind of witnesses can establish **NP=coNP**.
  - **IPS**: circuit representation of algebraic proofs (like circuit vs sparsity measure)

# Motivation 1

- Are semi-algebraic proofs **stronger** than algebraic ones?

# Algebraic Proofs

- Inference in a **polynomial ideal** over a field:

if  $p, q \in \langle f_1(\bar{x}), \dots, f_m(\bar{x}) \rangle$

then

$h \cdot p \in \langle f_1(\bar{x}), \dots, f_m(\bar{x}) \rangle$ , for any polynomial  $h$

and

$p + q \in \langle f_1(\bar{x}), \dots, f_m(\bar{x}) \rangle$

Observe: preserves **equalities** with 0:

**if**  $f_1(\bar{a}) = \dots = f_m(\bar{a}) = 0$  (for  $\bar{a}$  field assignment)

**then** all inferred polynomials = 0 (under assignment).

# Semi-Algebraic Proofs

Inference in the **cone** over reals  $\mathbb{R}$ :

1) If  $p, q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$   
then

$p \cdot q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$  and  
 $p + q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$ ,

2) and for any polynomial  $s$

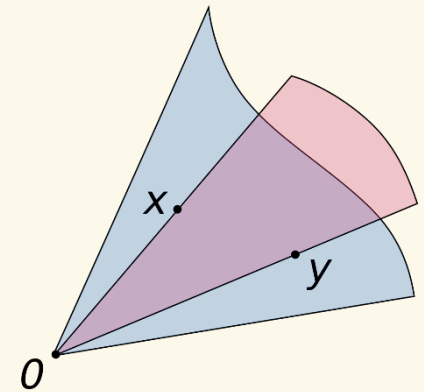
$s^2 \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$ , and

3) if  $c \geq 0$  then  $c \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$

0:

if  $f_1(\bar{a}) \geq 0, \dots, f_m(\bar{a}) \geq 0$  (for  $\bar{a}$  field assignment)

**then** all inferred polynomials  $\geq 0$  (under assignment).



# Semi-Algebraic Proofs

0:

Inference in the **cone** over reals  $\mathbb{R}$ :

1) If  $p, q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$

then

$p \cdot q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$  and

$p + q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$ ,

2) and for any polynomial  $s$

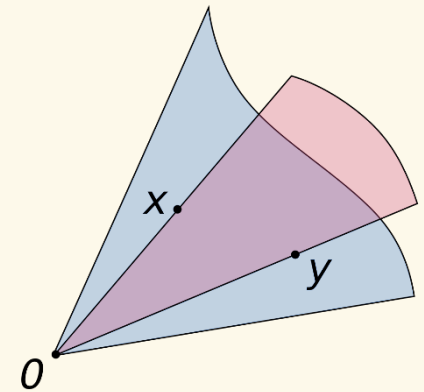
$s^2 \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$ , and

3) if  $c \geq 0$  then  $c \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$

Observe: preserves **inequalities**  $\geq 0$ :

if  $f_1(\bar{a}) \geq 0, \dots, f_m(\bar{a}) \geq 0$  (for  $\bar{a}$  field assignment)

**then** all inferred polynomials  $\geq 0$  (under assignment).





# Semi-Algebraic Proofs

$f_1(\bar{a}) \geq 0, \dots, f_m(\bar{a}) \geq 0$  (for  $\bar{a}$  field assignment)

0:

Inference in the **cone** over reals  $\mathbb{R}$ :

1) If  $p, q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$

then

$p \cdot q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$  and

$p + q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x})),$

2) and for any polynomial  $s$

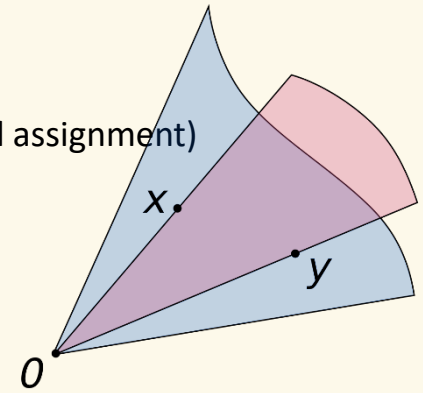
$s^2 \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x})),$  and

3) if  $c \geq 0$  then  $c \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$

**if**  $f_1(\bar{a}) \geq 0, \dots, f_m(\bar{a}) \geq 0$  (for  $\bar{a}$  field assignment)

**if**  $f_1(\bar{a}) \geq 0, \dots, f_m(\bar{a}) \geq 0$  (for  $\bar{a}$  field assignment)

**then** all inferred polynomials  $\geq 0$  (under assignment).



# Semi-Algebraic Proofs

0 (under assignment).

$f_1(\bar{a}) \geq 0, \dots, f_m(\bar{a}) \geq 0$  (for  $\bar{a}$  field assignment)

0:

Inference in the **cone** over reals  $\mathbb{R}$ :

1) If  $p, q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$

then

$p \cdot q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$  and

$p + q \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$ ,

2) and for any polynomial  $s$

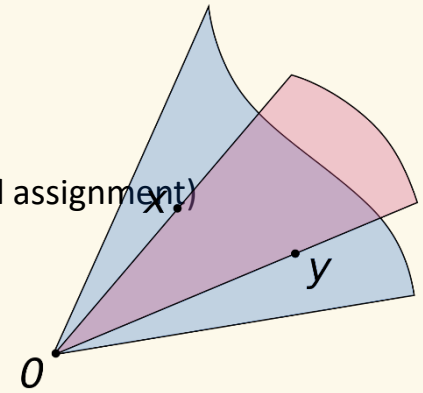
$s^2 \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$ , and

3) if  $c \geq 0$  then  $c \in \text{cone}(f_1(\bar{x}), \dots, f_m(\bar{x}))$

**then** all inferred polynomials  $\geq 0$  (under assignment).

**if**  $f_1(\bar{a}) \geq 0, \dots, f_m(\bar{a}) \geq 0$  (for  $\bar{a}$  field assignment)

**then** all inferred polynomials  $\geq 0$  (under assignment).



# What's Stronger: Algebraic or Semi-Algebraic Proofs?

algebraic proofs:

2)  $\langle p, -p \rangle \ni 0$  ( $p \geq 0$ ):

- $\langle p, -p \rangle = 0$  as a pair of inequalities:  $p \geq 0$  and  $-p \geq 0$ .
- $\langle p, -p \rangle \ni \langle p \rangle$ : to derive  $h \cdot p$  in  $\text{cone}(p, -p)$ , for any polynomial  $h$
- $\langle p, -p \rangle = \text{cone}(p, -p)$  = "some sos" – "some sos"

# What's Stronger: Algebraic or Semi-Algebraic Proofs?

- algebraic proofs:
- In our setting we freely have semi-algebraic  $\geq$  algebraic proofs:

2)  $\geq 0$ ):

- $p \geq 0$  as a pair of inequalities:  $p \geq 0$   
and  $-p \geq 0$ .
- $\text{cone}(p, -p) \supseteq \langle p \rangle$ : to derive  $h \cdot p$  in  $\text{cone}(p, -p)$ , for any polynomial  $h$
- $h \cdot p = \text{"some sos"} - \text{"some sos"}$

# What's Stronger: Algebraic or Semi-Algebraic Proofs?

- algebraic proofs:
  - 1) Semi-algebraic proofs refute both unsatisfiable sets of ***equalities and inequalities***:

2)  $\langle p, -p \rangle \ni 0$  ( $p \geq 0$ ):

- $\langle p, -p \rangle \ni 0$  as a pair of inequalities:  $p \geq 0$  and  $-p \geq 0$ .
- $\langle p, -p \rangle \ni 0$ : to derive  $h \cdot p$  in  $\text{cone}(p, -p)$ , for any polynomial  $h$
- $\langle p, -p \rangle \ni 0$  = "some sos" – "some sos"

# What's Stronger: Algebraic or Semi-Algebraic Proofs?

- algebraic proofs:
  - 1) Semi-algebraic proofs refute both unsatisfiable sets of ***equalities and inequalities***:

For equalities we will be working in the ideal (e.g., in PC):

2)  $\langle p \rangle \subseteq \langle p, -p \rangle$  ( $p \geq 0$ ):

-  $\langle p, -p \rangle = 0$  as a pair of inequalities:  $p \geq 0$   
and  $-p \geq 0$ .

-  $\text{cone}(p, -p) \supseteq \langle p \rangle$ : to derive  $h \cdot p$  in  $\text{cone}(p, -p)$ , for any polynomial  $h$

-  $\text{cone}(p, -p) = \text{some sos} - \text{some sos}$

# What's Stronger: Algebraic or Semi-Algebraic Proofs?

- algebraic proofs:
  - 1) Semi-algebraic proofs refute both unsatisfiable sets of ***equalities and inequalities***:

For equalities we will be working in the ideal (e.g., in PC):

2)  $\langle p \rangle \subseteq \langle p \rangle + \langle q \rangle$  ( $p \geq 0$ ):

-  $\langle p \rangle \subseteq \langle p \rangle + \langle q \rangle$  as a pair of inequalities:  $p \geq 0$   
and  $-p \geq 0$ .

-  $\langle p \rangle \subseteq \langle p \rangle + \langle q \rangle$ : to derive  $h \cdot p$  in  $\text{cone}(p, -p)$ , for any polynomial  $h$

-  $\langle p \rangle \subseteq \langle p \rangle + \langle q \rangle$  = "some sos" – "some sos"

# What's Stronger: Algebraic or Semi-Algebraic Proofs?

- algebraic proofs:
  - 1) Semi-algebraic proofs refute both unsatisfiable sets of ***equalities and inequalities***:

For equalities we will be working in the ideal (e.g., in PC):

$$\boxed{\text{polynomials in the ideal of equalities}} + \boxed{\text{polynomials in the cone of inequalities}}$$

2)  $\geq 0$ ):

-  $p = 0$  as a pair of inequalities:  $p \geq 0$   
and  $-p \geq 0$ .

-  $\text{cone}(p, -p) \supseteq \langle p \rangle$ : to derive  $h \cdot p$  in  $\text{cone}(p, -p)$ , for any polynomial  $h$

-  $h \cdot p = \text{"some sos"} - \text{"some sos"}$



# What's Stronger: Algebraic or Semi-Algebraic Proofs?

- 0):
- algebraic proofs:
  - 1) Semi-algebraic proofs refute both unsatisfiable sets of ***equalities and inequalities***:

For equalities we will be working in the ideal (e.g., in

$$\text{PC} \left( \boxed{\text{polynomials in the ideal of equalities}} + \boxed{\text{polynomials in the cone of inequalities}} \right)$$

- 2) Otherwise (even without the boolean axioms  $x_i^2 \geq 0$ ):

- 3)  $\geq 0$ ):

- $p = 0$  as a pair of inequalities:  $p \geq 0$  and  $-p \geq 0$ .

- $\text{cone}(p, -p) \supseteq \langle p \rangle$ : to derive  $h \cdot p$  in  $\text{cone}(p, -p)$ , for any polynomial  $h$

# What's Stronger: Algebraic or Semi-Algebraic Proofs?

- $0$  as a pair of inequalities:  $p \geq 0$  and  $-p \geq 0$ .
- $0$ ):
- algebraic proofs:
  - 1) Semi-algebraic proofs refute both unsatisfiable sets of ***equalities and inequalities***:

For  $\{p_i\} \subseteq \mathbb{R}[x]$ ,  $\{q_j\} \subseteq \mathbb{R}[x]$ , in PCP,  $\{p_i\} \cup \{q_j\} \neq \emptyset$

- Can treat equalities:  $p = 0$  as a pair of inequalities:  $p \geq 0$  and  $-p \geq 0$ .

2)  $\{p_i\} \cup \{q_j\} \neq \emptyset$  ( $p_i \geq 0$ ):

- $\{p_i\} \cup \{q_j\} \neq \emptyset$  as a pair of inequalities:  $p \geq 0$  and  $-p \geq 0$ .

$\text{cone}(n, n) \supseteq \{n\}$ ; to derive  $h = n$  in  $\text{cone}(n, n)$  for

# What's Stronger: Algebraic or Semi-Algebraic Proofs?

- one  $p, -p$   $\text{cone}(p, -p) \supseteq \langle p \rangle$ : to derive  $h \cdot p$  in  $\text{cone}(p, -p)$ , for any polynomial  $h$
- $0$  as a pair of inequalities:  $p \geq 0$  and  $-p \geq 0$ .
- $0$ ):
- algebraic proofs:

- 1) Separate sets of equalities and inequalities:
 

polynomials in the ideal of equalities	polynomials in the cone of inequalities
--	---

For equalities we will be working in the ideal (e.g., in PC):

- Then  $\text{cone}(p, -p) \supseteq \langle p \rangle$ : to derive  $h \cdot p$  in  $\text{cone}(p, -p)$ , for any polynomial  $h$

- 2)  $p \geq 0$ :

# What's Stronger: Algebraic or Semi-Algebraic Proofs?

- = "some sos" – "some sos"
- $one p, -p p p, -p p p, -p p p, -p p p \supseteq p p p p$ : to derive  $h \cdot p p$  in cone  $p, -p p p, -p p p, -p p p$ , for any polynomial  $h$
- $0$  as a pair of inequalities:  $p p \geq 0$  and  $-p p \geq 0$ .
- $0$ ):

- algebraic  $\left[ \begin{array}{c} \text{polynomials in the ideal} \\ \text{of equalities} \end{array} \right] + \left[ \begin{array}{c} \text{polynomials in the cone} \\ \text{of inequalities} \end{array} \right]$  sets of ***equalities and inequalities:***

For equalities we will be working in the ideal (e.g., in PC):

- Nice trick: every poly  $h =$  "some sos" – "some sos"
- 2)  $\geq 0$ ):

# What's Stronger: Algebraic or Semi-Algebraic Proofs?

- = "some sos" – "some *sos*"
- $one\ p, -p\ pp, -pp\ p, -p \supseteq p\ pp\ p$ : to derive  $h \cdot pp$  in cone  $p, -p\ pp, -pp\ p, -p$ , for any polynomial  $h$
- $0$  as a pair of inequalities:  $pp \geq 0$  and  $-pp \geq 0$ .
- $0$ ):

- algebraic  $\left[ \begin{array}{c} \text{polynomials in the ideal} \\ \text{of equalities} \end{array} \right] + \left[ \begin{array}{c} \text{polynomials in the cone} \\ \text{of inequalities} \end{array} \right]$  sets of

## ***equalities and inequalities:***

For equalities we will be working in the ideal (e.g., in PC):

- Example:  $x = \frac{1}{4}(1+x)^2 - \frac{1}{4}(1-x)^2$

- 2)  $\geq 0$ ):

# Motivation 2

- (Conditional) lower bounds on strong proof systems.
- Unknown for e.g. Frege and beyond.

# Our Results

# Our Results

## 1. Algebraic proofs weaker than semi-algebraic ones (under complexity assumptions)

- Formulate the **Cone Proof System (CPS)**
  - A proof system that characterises very strong semi-algebraic reasoning
  - Cone Proof System = Positivstellensatz over algebraic circuits
    - Semi-algebraic analogue of IPS (GP14)
- **CPS is strictly stronger than IPS** (under complexity assumptions)
  - Even the strongest algebraic proof system (IPS) cannot simulate the “weakest” semi-algebraic proof system (under complexity assumptions)



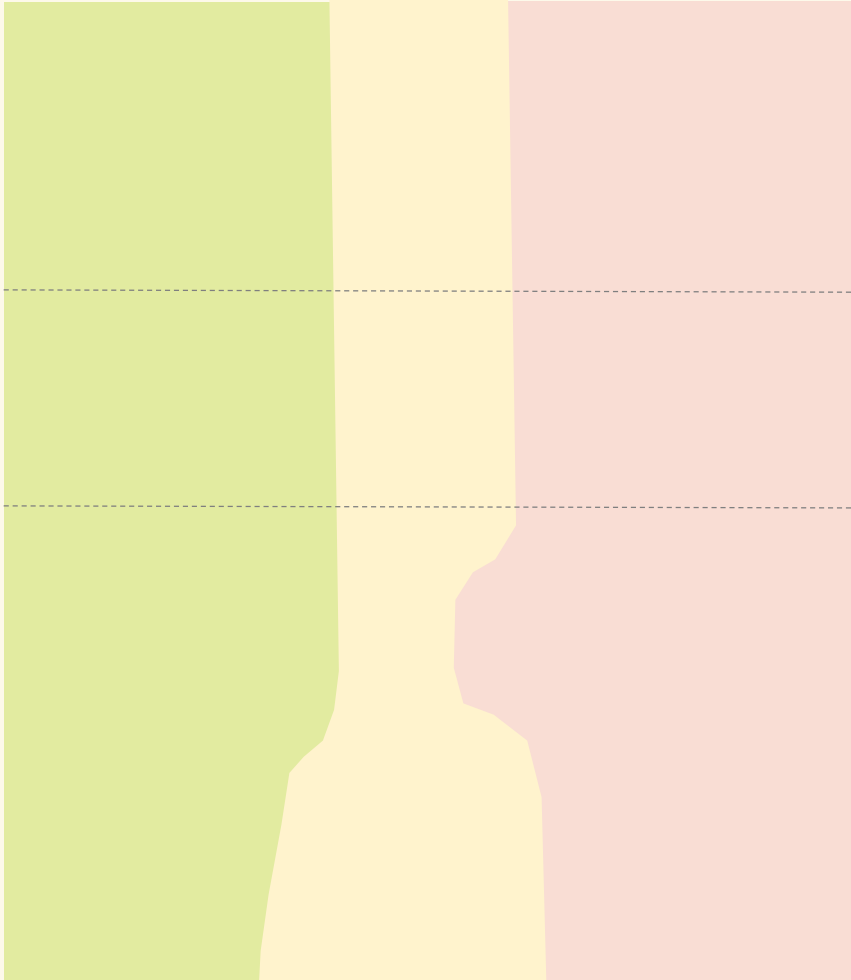
# Expressivity



**Semi-Algebraic Proofs**  
Systems for sets of polynomial equations and inequalities over a field with 0-1 variables

**Algebraic Proofs**  
Systems for sets of polynomial equations over a field with 0-1 variables

Systems for **propositional logic**



Very Strong Systems

Strong Systems

Weak to Medium Strength Systems



Proof Complexity Strength

# Expressivity



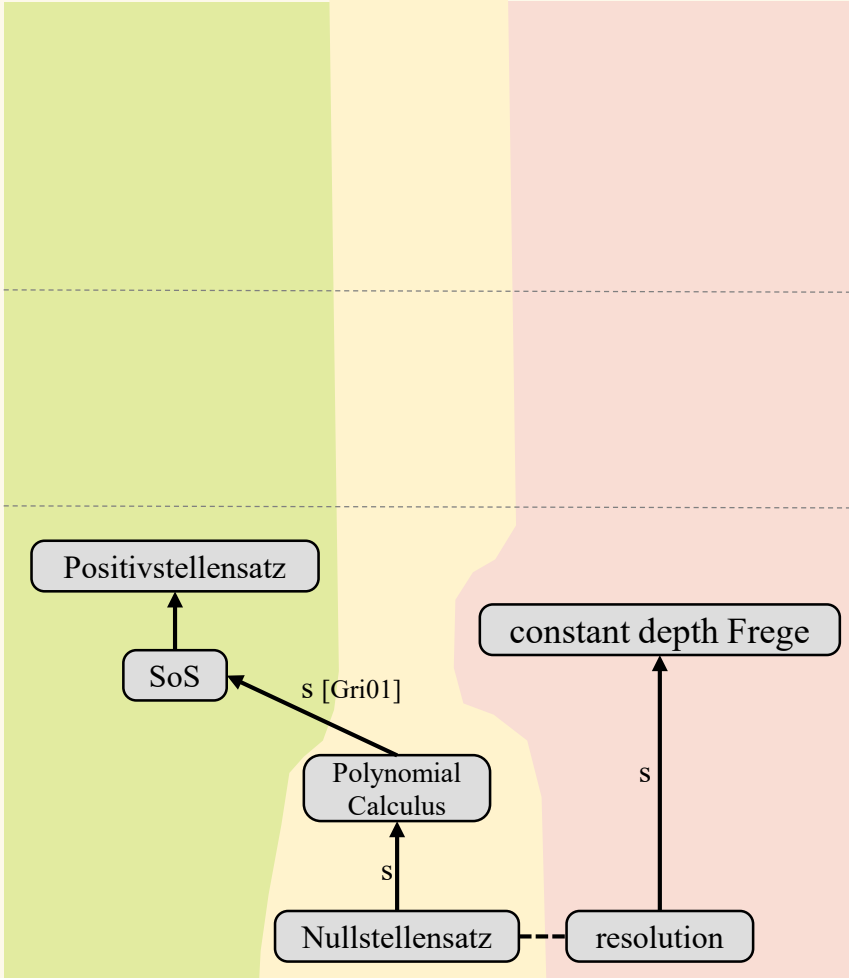
## Semi-Algebraic Proofs

Systems for sets of polynomial equations and inequalities over a field with 0-1 variables

## Algebraic Proofs

Systems for sets of polynomial equations over a field with 0-1 variables

## Systems for propositional logic



Very Strong Systems

Strong Systems

Weak to Medium Strength Systems

Proof Complexity Strength



# Expressivity



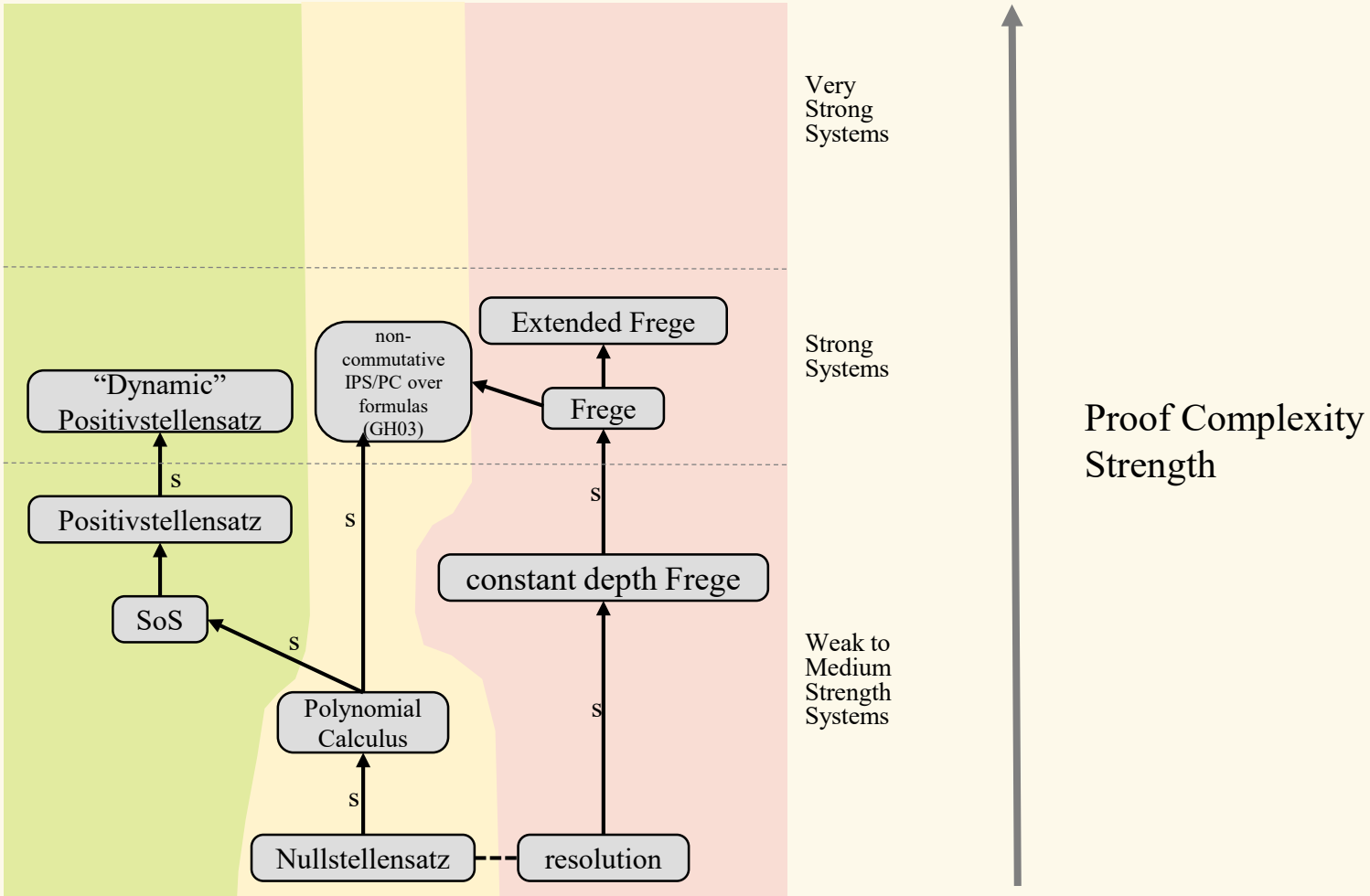
## Semi-Algebraic Proofs

Systems for sets of polynomial equations and inequalities over a field with 0-1 variables

## Algebraic Proofs

Systems for sets of polynomial equations over a field with 0-1 variables

## Systems for propositional logic

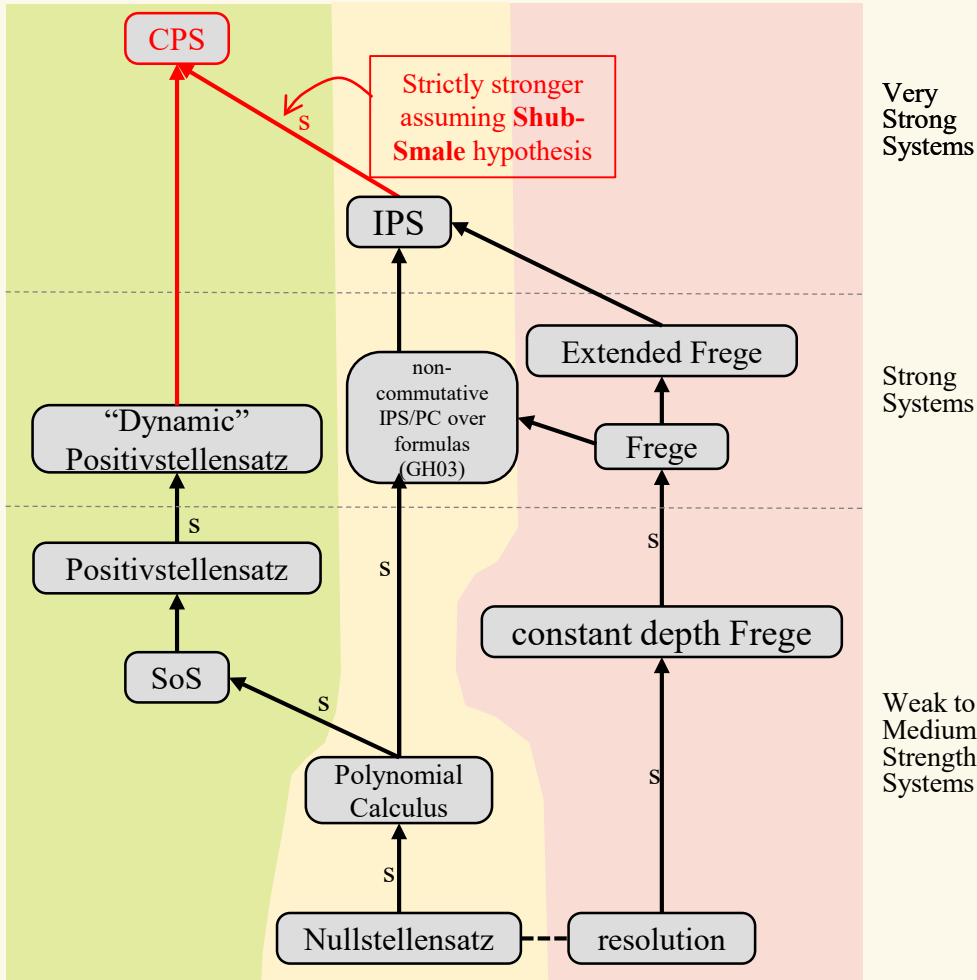


# Expressivity

**Semi-Algebraic Proofs**  
Systems for sets of polynomial equations and inequalities over a field with 0-1 variables

**Algebraic Proofs**  
Systems for sets of polynomial equations over a field with 0-1 variables

Systems for **propositional logic**



# Our Results

- Formulate the **Cone Proof System (CPS)**  
A proof system that characterises very strong semi-algebraic reasoning
- CPS is strictly stronger than IPS (under complexity assumptions)

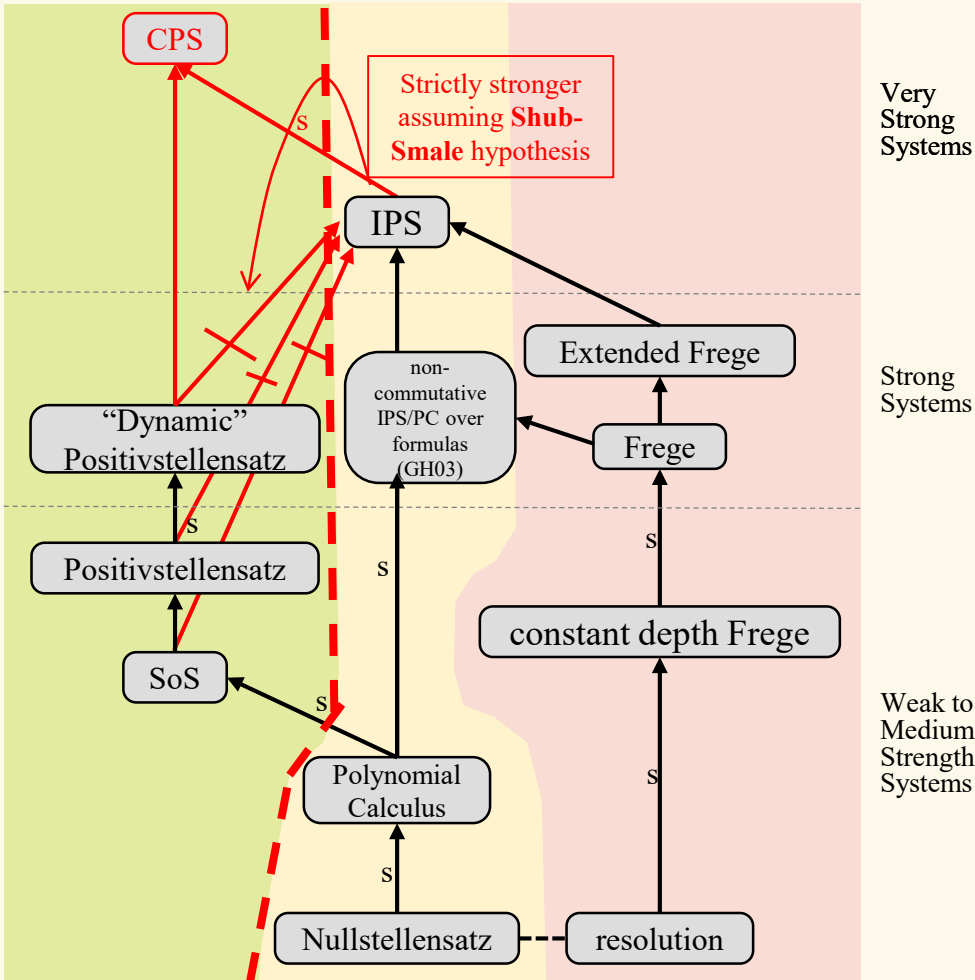
# Expressivity

←

**Semi-Algebraic Proofs**  
Systems for sets of polynomial equations and inequalities over a field with 0-1 variables

**Algebraic Proofs**  
Systems for sets of polynomial equations over a field with 0-1 variables

Systems for **propositional logic**



# Our Results

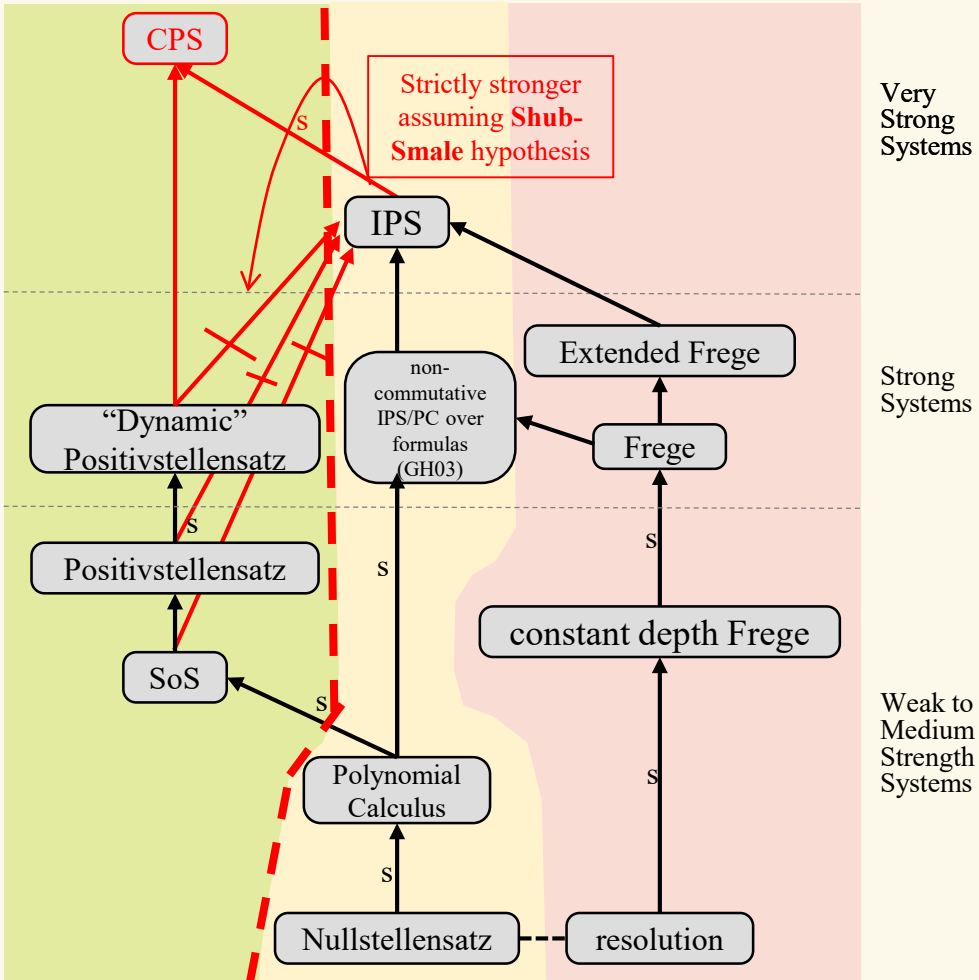
- Even the strongest algebraic proof system (IPS) **cannot** simulate the "weakest" semi-algebraic proof system (under complexity assumptions)

# Expressivity

**Semi-Algebraic Proofs**  
Systems for sets of polynomial equations and inequalities over a field with 0-1 variables

**Algebraic Proofs**  
Systems for sets of polynomial equations over a field with 0-1 variables

Systems for **propositional logic**



# Our Results

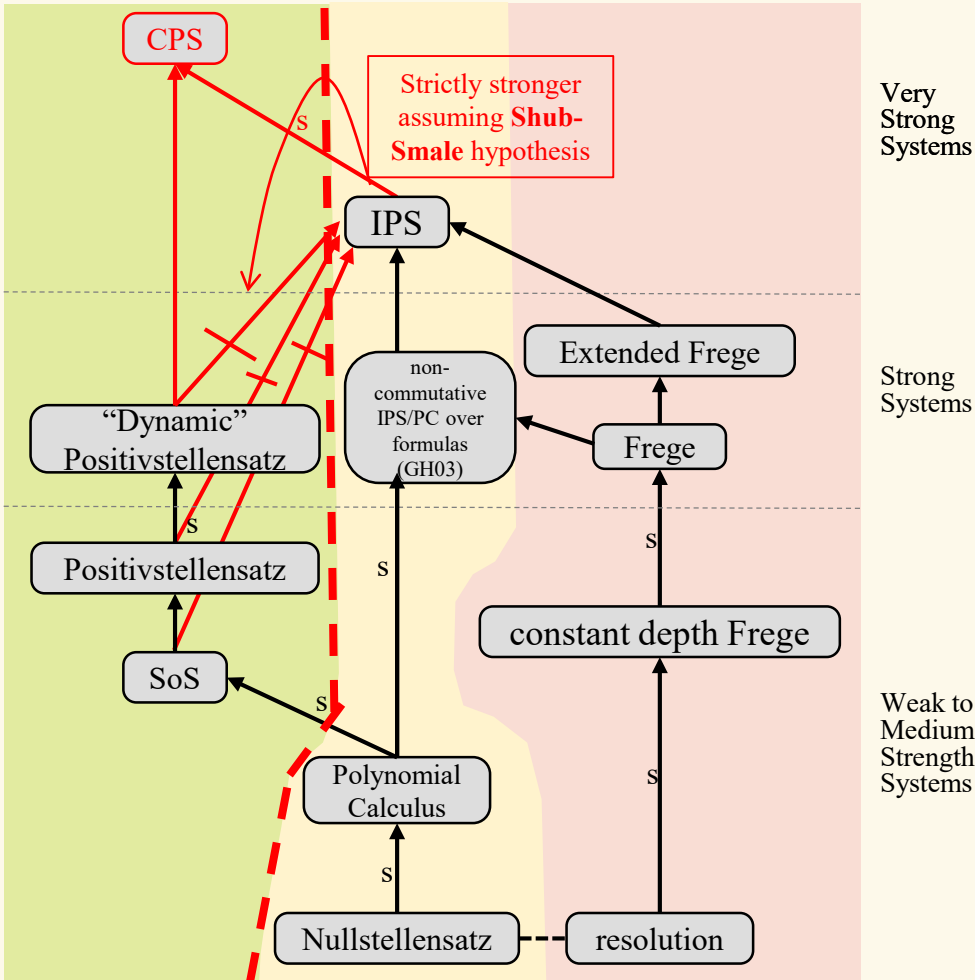
- Even the strongest algebraic proof system (IPS) **cannot** simulate the "weakest" semi-algebraic proof system (under complexity assumptions)

# Expressivity

**Semi-Algebraic Proofs**  
Systems for sets of polynomial equations and inequalities over a field with 0-1 variables

**Algebraic Proofs**  
Systems for sets of polynomial equations over a field with 0-1 variables

Systems for **propositional logic**



# Our Results

- Even the strongest algebraic proof system (IPS) **cannot** simulate the "weakest" semi-algebraic proof system (under complexity assumptions)

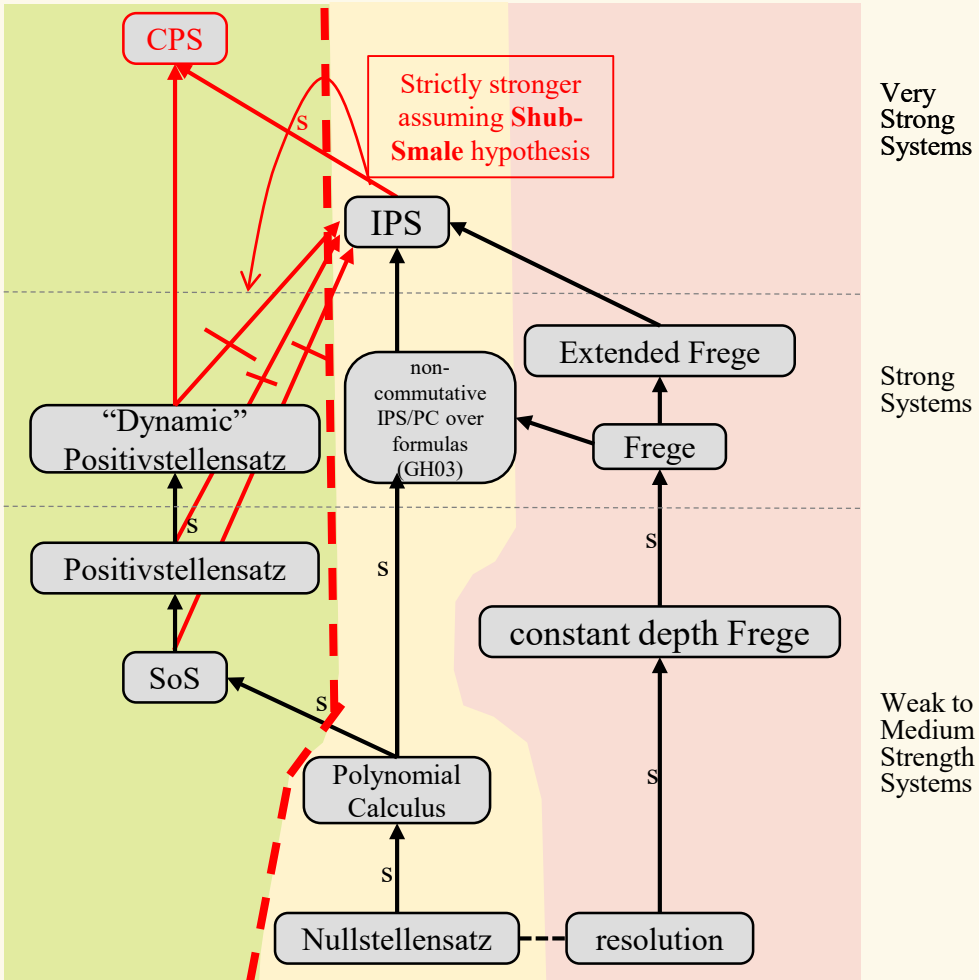
# Expressivity

←

**Semi-Algebraic Proofs**  
Systems for sets of polynomial equations and inequalities over a field with 0-1 variables

**Algebraic Proofs**  
Systems for sets of polynomial equations over a field with 0-1 variables

Systems for **propositional logic**



# Our Results

- Even the strongest algebraic proof system (IPS) **cannot** simulate the "weakest" semi-algebraic proof system (under complexity assumptions)



# Our Results

## **2. Conditional I**

# Our Results

## 2. Conditional I

- **BVP hard for IPS**

# Our Results

## 2. Conditional I

- **BVP hard** for IPS
- **BVP is very easy** for CPS (or any semi-algebraic proof system from SoS and beyond)

# Our Results

## 2. Conditional I

- **BVP hard** for IPS
- **BVP is very easy** for CPS (or any semi-algebraic proof system from SoS and beyond)
  - Hardness under complexity assumption:

# Our Results

## 2. Conditional I

- **BVP hard** for IPS
- **BVP is very easy** for CPS (or any semi-algebraic proof system from SoS and beyond)
  - Hardness under complexity assumption:
- **Hardness assumptions:** computing factorials with constant-free algebraic circuits is hard:

# Our Results

**2. Conditional I**  $k_m m! \ m=1 \ \infty$  for any nonzero integers  $k_m$  in at most  $(\log m)^c$  operations.

**og m ) c og m og m m (log m ) c**

- **BVP hard for IPS**
- **BVP is very easy for CPS** (or any semi-algebraic proof system from SoS and beyond)
  - Hardness under complexity assumption:
- **Hardness assumptions:** computing factorials with constant-free algebraic circuits is hard:
  - cannot compute  $k m m! \ m = 1 \ \infty$  for any nonzero integers  $k_m$  in at most  $(\log m)^c$  operations.

# Our Results

## **2. Conditional lower bounds against strong proof systems (cnt.)**

# Our Results

## **2. Conditional lower bounds against strong proof systems (cnt.)**

- Recall IPS refutation is “a single circuit that computes the algebraic refutation”.



# Our Results

## 2. Conditional lower bounds against strong proof systems (cnt.)

- Recall IPS refutation is “a single circuit that computes the algebraic refutation”.
- Our lower bound extends (Forbes, Shpilka, T., Wigderson 2016) functional lower bounds approach to IPS

# Our Results

## 2. Conditional lower bounds against strong proof systems (cnt.)

- Recall IPS refutation is “a single circuit that computes the algebraic refutation”.
- Our lower bound extends (Forbes, Shpilka, T., Wigderson 2016) functional lower bounds approach to IPS
  - Can't get better without actually showing  $VP \neq VNP$

# Our Results

## **3. Characterising the advantage of semi-algebraic proofs over algebraic ones**

# Our Results

## **3. Characterising the advantage of semi-algebraic proofs over algebraic ones**

- **BVP characterises semi-algebraic proofs:**

# Our Results

## 3. Characterising the advantage of semi-algebraic proofs over algebraic ones

- BVP characterises semi-algebraic proofs:

$$\mathbf{IPS + BVP = CPS}$$

# Our Results

## 3. Characterising the advantage of semi-algebraic proofs over algebraic ones

- **BVP characterises semi-algebraic proofs:**

$$\mathbf{IPS + BVP = CPS}$$

- Assume an algebraic proof system  $P$  is strong enough to do efficient bit-arithmetic. Then,  $P$  simulates semi-algebraic proofs (of the “corresponding complexity”) iff it refutes BVP efficiently.

-

# Our Results

## 3. Characterising the advantage of semi-algebraic proofs over algebraic ones

- **BVP characterises semi-algebraic proofs:**

$$\mathbf{IPS + BVP = CPS}$$

- Assume an algebraic proof system  $P$  is strong enough to do efficient bit-arithmetic. Then,  $P$  simulates semi-algebraic proofs (of the “corresponding complexity”) iff it refutes BVP efficiently.

# Our Results

## 3. Characterising the advantage of semi-algebraic proofs over algebraic ones

- **BVP characterises semi-algebraic proofs:**

$$\mathbf{IPS + BVP = CPS}$$

- Assume an algebraic proof system  $P$  is strong enough to do efficient bit-arithmetic. Then,  $P$  simulates semi-algebraic proofs (of the “corresponding complexity”) iff it refutes BVP efficiently.



# Moral

- One can do interesting things with coefficients of relatively large magnitudes (though their size is still polynomial!)

# Moral

Algebraic proofs **can do** efficiently basic bit-arithmetic (we show this).

- But assuming Shub-Smale Hypothesis, algebraic proofs **cannot** prove basic properties about the bits of polynomials, given a polynomial equation; e.g., that

$$+ \cdots + x_n = 0 \vdash \text{Bit}_i(x_1 + \cdots + x_n) = 0$$

# Moral

$$x_1 + \dots + x_n = 0 \vdash \text{Bit}_i(x_1 + \dots + x_n) = 0$$

*Algebraic* proofs **can do** efficiently basic bit-arithmetic (we show this).

- But assuming Shub-Smale Hypothesis, algebraic proofs **cannot** prove basic properties about the bits of polynomials, given a polynomial equation; e.g., that

$$x_1 + \dots + x_n = 0 \vdash \text{Bit}_i(x_1 + \dots + x_n) = 0$$

# The Technical Part

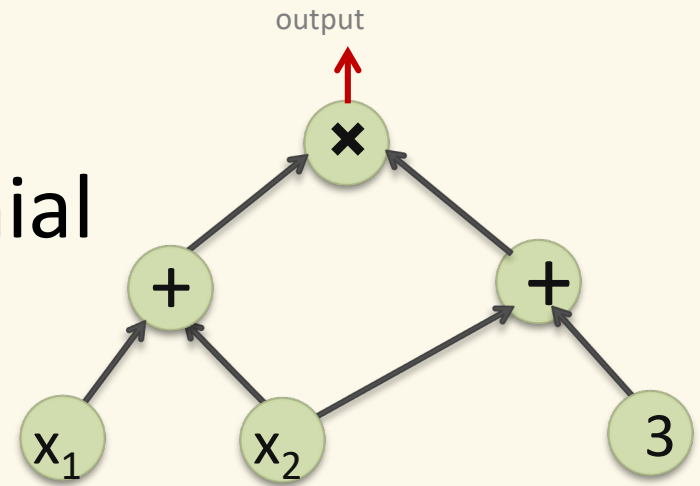
# Algebraic circuits

Fix a field  $\mathbb{F}$

An **algebraic circuit** over  $\mathbb{F}$   
computes a formal polynomial  
over  $\mathbb{F}$

**Size** = # of nodes

$$(x_1 + x_2) \cdot (x_2 + 3) = x_1x_2 + x_2^2 + 3x_1 + 3x_2$$



# Shub-Smale Hypothesis

- A **constant-free** circuit is an algebraic circuit that uses  $1, 0, -1$  as the only constants available on leaves.
- For integer  $m$ ,  $\tau(m)$  is the smallest constant-free circuit that computes  $m$ .
- **Shub-Smale Hypothesis:** no constant-free circuit of size at most  $(\log m)^c$ , for a constant  $c$ , computes  $(k_m m!)_{m=1}^{\infty}$ , for any nonzero integers  $k_m$ .

# Ideal Proof System (IPS)

- A refutation of  $f_1(\bar{x}) = \dots = f_m(\bar{x}) = 0$  for polynomials  $f_i(\bar{x})$  in  $\mathbb{F}[\bar{x}]$  is a constant-free algebraic circuit  $C(\bar{x}, \bar{y}, \bar{z})$  such that:
  1.  $C(\bar{x}, \bar{0}, \bar{0}) = 0$ ;
  2.  $C(\bar{x}, f_1(\bar{x}), \dots, f_m(\bar{x}), x_1^2 - x_1, \dots, x_n^2 - x_n) = 1$   
(equality as formal polynomials).
- The **size** of the IPS proof is the size of the circuit  $C$ .

# IPS Conditional Lower Bounds

**Thm:** Assuming Shub-Smale Hypothesis there are no  $\text{poly}(n)$ -size (constant-free) IPS refutations over  $\mathbb{Q}$  of the  $\text{BVP}_n: x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n = -1$ .

*Proof Sketch.*

**Step 1:** FSTW16: IPS = NS over circuits. Hence, consider by way of contradiction:

$$g \cdot (x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1}x_n + 1) + \sum_{i=1}^n h_i \cdot (x_i^2 - x_i) = 1$$

with  $g$  of  $\text{poly}(n)$  algebraic circuit.



# IPS Conditional Lower Bounds

**Thm:** Assuming Shub-Smale Hypothesis there are no  $\text{poly}(n)$ -size (constant-free) IPS refutations over  $\mathbb{Q}$  of the  $\text{BVP}_n: x_1 + 2x_2 + 4x_3 + \dots + 2^{n-1}x_n = -1$ .

*Proof Sketch (cnt.).*

**Step 2:** Show that it is enough to prove lower bounds for IPS refutations over  $\mathbb{Z}$  of

$$g \cdot (x_1 + 2x_2 + 4x_3 + \dots + 2^{n-1}x_n + 1) + \sum_{i=1}^n h_i \cdot (x_i^2 - x_i) = M$$

for all nonzero integers  $M$  with  $\tau(M)$  is  $\text{poly}(n)$ .

**Idea:** Multiply the  $\text{IPS}_{\mathbb{Q}}$  enough times to get all constants integers ( $\tau(M)$  remains  $\text{poly}(n)$ ).

# IPS Conditional Lower Bounds

*Proof Sketch (cnt.).*

**Step 3:** Consider the refutation over  $\mathbb{Z}$

$$g \cdot (x_1 + 2x_2 + 4x_3 + \dots + 2^{n-1}x_n + 1) + \sum_{i=1}^n h_i \cdot (x_i^2 - x_i) = M$$

for  $M$  with  $\tau(M) = \text{poly}(n)$ .

- **Restriction:** For every number  $b$  in  $[0, 2^n - 1]$  with bit-vector  $\bar{b} = (b_1 \dots b_n)$

$$g \upharpoonright \bar{b} \cdot (b_1 + 2b_2 + 4b_3 + \dots + 2^{n-1}b_n + 1) + 0 = M \upharpoonright \bar{b}$$

$$\mathbf{A} \cdot (b_1 + 2b_2 + 4b_3 + \dots + 2^{n-1}b_n + 1) = \mathbf{M}$$

where  $\mathbf{A}$  is some integer dependent on  $b$ .

**Corollary:**  $M$  is an integer of  $\tau(M) = \text{poly}(n)$  and is divisible by every number in  $[1, 2^n]$

# IPS Conditional Lower Bounds

*Proof Sketch (cnt.).*

**Step 3:** Consider the refutation over  $\mathbb{Z}$

$$g \cdot (x_1 + 2x_2 + 4x_3 + \dots + 2^{n-1}x_n + 1) + \sum_{i=1}^n h_i \cdot (x_i^2 - x_i) = M$$

for  $M$  with  $\tau(M) = \text{poly}(n)$ .

- **Restriction:** For every number  $b$  in  $[0, 2^n - 1]$  with bit-vector  $\bar{b} = (b_1 \dots b_n)$

$$g \upharpoonright \bar{b} \cdot (b_1 + 2b_2 + 4b_3 + \dots + 2^{n-1}b_n + 1) + 0 = M \upharpoonright \bar{b}$$

$$A \cdot (b_1 + 2b_2 + 4b_3 + \dots + 2^{n-1}b_n + 1) = M$$

where  $A$  is some integer dependent on  $b$ .

**Corollary:**  $M$  is an integer of  $\tau(M) = \text{poly}(n)$  and is divisible by every number in  $[1, 2^n]$

# IPS Conditional Lower Bounds

*Proof Sketch (cnt.).*

## Step 4:

**Lemma:** If  $M$  is an integer of  $\tau(M)=\text{poly}(n)$  and is divisible by every number in  $[1,2^n]$  then Shub-Smale Hypothesis is false!

*Proof sketch.* We show there exists a  $\text{poly}(n)$ -size constant-free circuit that computes  $2^n!$  (hence,  $\tau(m!)=\log^c m$ , for  $m$  a power of 2; almost what we need).

- By repeated squaring:  $\tau(M^{2^n}) = \text{poly}(n)$
- **Fact:** Consider the prime factorization of  $2^n!$ 
  - $2^n! = p_1^{r_1} \cdots p_k^{r_k}$
  - $p_i$  is at most  $2^n$  (hence, it's a factor of  $M$ ), and
  - $r_i$  is at most  $2^n$ .
- Hence, every  $p_i^{r_i}$  is a factor of  $M^{2^n}$ . QED

# $\tau$ -conjecture based lower bounds

- Under the  **$\tau$ -conjecture** we can establish IPS lower bounds over the field of rational functions in the indeterminate single variable  $y$ .

# The Cone Proof System

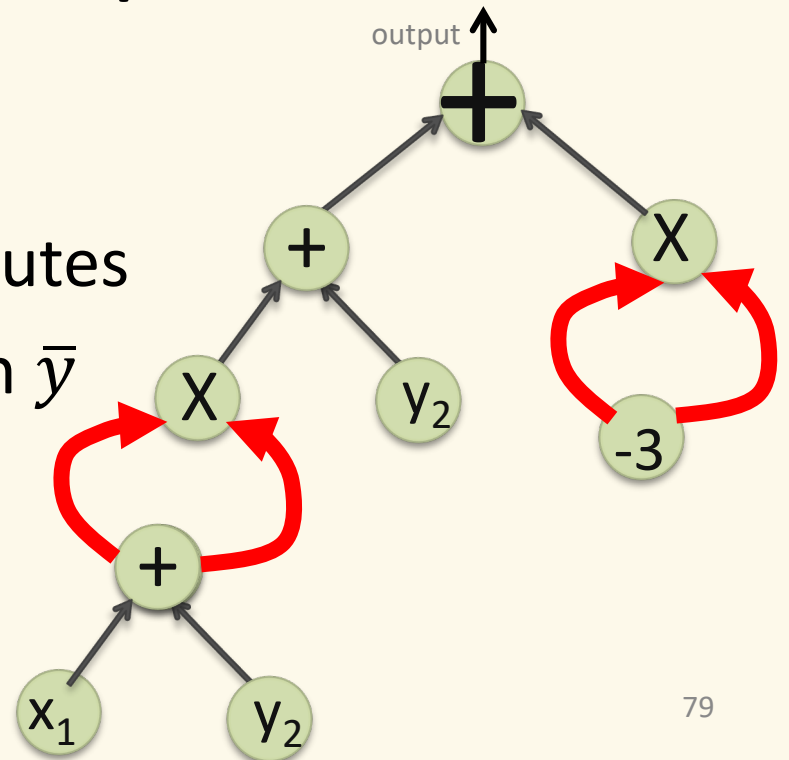
# Cone Proof System (CPS)

A  $\bar{y}$ -**conic circuit** is a circuit  $C(\bar{x}, \bar{y})$  in which

- $\bar{y}$ -variables are assumed to be nonnegative;
- $\bar{x}$  variables or negative constants (that may be negative) must be **part of a squared sub-circuit**.

Fact:

A  $\bar{y}$ -**conic circuit**  $C(\bar{x}, \bar{y})$  computes only non-negative values when  $\bar{y}$  are non-negative; i.e., polynomials in  $\text{cone}(\bar{y})$



# Cone Proof System (CPS)

A **CPS** refutation of  $f_1(\bar{x}) = \dots = f_m(\bar{x}) = 0$  and  $h_1(\bar{x}) \geq 0, \dots, h_k(\bar{x}) \geq 0$ , for polynomials in  $\mathbb{R}[\bar{x}]$  is a constant-free algebraic circuit  $C(\bar{x}, \bar{y})$  such that:

1.  $C(\bar{x}, \bar{y})$  is a  $\bar{y}$ -conic circuit;
2.  $C(\bar{x}, \bar{H}) = -1$

where

$$\bar{H} = \{f_i(\bar{x}), -f_i(\bar{x}), h_i(\bar{x}), x_j^2 - x_j, -(x_j^2 - x_j), x_j, 1 - x_j\}_{i,j}$$

- The **size** of the IPS proof is the size of the circuit  $C$ .



# Cone Proof System (CPS)

A **CPS** refutation of  $f_1(\bar{x}) = \dots = f_m(\bar{x}) = 0$  and  $h_1(\bar{x}) \geq 0, \dots, h_k(\bar{x}) \geq 0$ , for polynomials in  $\mathbb{R}[\bar{x}]$  is a constant-free algebraic circuit  $C(\bar{x}, \bar{y})$  such that:

1.  $C(\bar{x}, \bar{y})$  is a  $\bar{y}$ -conic circuit;
2.  $C(\bar{x}, \bar{H}) = -1$

where

$$\bar{H} = \{f_i(\bar{x}), -f_i(\bar{x}), h_i(\bar{x}), x_j^2 - x_j, -(x_j^2 - x_j), x_j, 1 - x_j\}_{i,j}$$

- The **size** of the IPS proof is the size of the circuit  $C$ .

**Thm:** CPS simulates all known (to us) proof systems (e.g., IPS, SoS, Positivstellensatz, EF).

# CPS Upper Bounds

**Proposition:** CPS admits *linear size* refutations of the binary value principle  $BVP_n$ .

*Proof.* Idea: because we have the boolean axioms for the  $\bar{x}$  variables

$$S := \sum_{i=1}^n 2^{i-1} \cdot x_i + 1.$$

$$\overline{\mathcal{H}} := \{x_1 \geq 0, \dots, x_n \geq 0, -S \geq 0, S \geq 0, x_1^2 - x_1 \geq 0, \dots, x_n^2 - x_n \geq 0, \\ -(x_1^2 - x_1) \geq 0, \dots, -(x_n^2 - x_n) \geq 0, 1 - x_1 \geq 0, \dots, 1 - x_n \geq 0\}$$

$$C(\overline{x}, \overline{y}) := \left( \sum_{i=1}^n 2^{i-1} \cdot y_i \right) + y_{n+1}$$

$$C(\overline{x}, \overline{\mathcal{H}}) = C(\overline{x}, x_1, \dots, x_n, -S, \dots) = \left( \sum_{i=1}^n 2^{i-1} \cdot x_i \right) + (-S) =$$

# CPS Upper Bounds

**Proposition:** CPS admits *linear size* refutations of the binary value principle  $BVP_n$ .

*Proof.* Idea: because we have the boolean axioms for the  $\bar{x}$  variables

$$S := \sum_{i=1}^n 2^{i-1} \cdot x_i + 1.$$

$$\overline{\mathcal{H}} := \left\{ \underbrace{x_1 \geq 0, \dots, x_n \geq 0}, -S \geq 0, S \geq 0, x_1^2 - x_1 \geq 0, \dots, x_n^2 - x_n \geq 0, \right. \\ \left. -(x_1^2 - x_1) \geq 0, \dots, -(x_n^2 - x_n) \geq 0, 1 - x_1 \geq 0, \dots, 1 - x_n \geq 0 \right\}$$

$$C(\overline{x}, \overline{y}) := \left( \sum_{i=1}^n 2^{i-1} \cdot y_i \right) + y_{n+1}$$

$$C(\overline{x}, \overline{\mathcal{H}}) = C(\overline{x}, x_1, \dots, x_n, -S, \dots) = \left( \sum_{i=1}^n 2^{i-1} \cdot x_i \right) + (-S) =$$

83 -1.

# CPS Upper Bounds

**Proposition:** CPS admits *linear size* refutations of the binary value principle  $BVP_n$ .

*Proof.* Idea: because we have the boolean axioms for the  $\bar{x}$  variables

$$S := \sum_{i=1}^n 2^{i-1} \cdot x_i + 1.$$

$$\overline{\mathcal{H}} := \{ \underbrace{x_1 \geq 0, \dots, x_n \geq 0}_{\text{red bracket}}, -S \geq 0, S \geq 0, x_1^2 - x_1 \geq 0, \dots, x_n^2 - x_n \geq 0, \\ -(x_1^2 - x_1) \geq 0, \dots, -(x_n^2 - x_n) \geq 0, 1 - x_1 \geq 0, \dots, 1 - x_n \geq 0 \}$$

$$C(\overline{x}, \overline{y}) := \left( \sum_{i=1}^n 2^{i-1} \cdot y_i \right) + y_{n+1}$$

$$C(\overline{x}, \overline{\mathcal{H}}) = C(\overline{x}, x_1, \dots, x_n, -S, \dots) = \left( \sum_{i=1}^n 2^{i-1} \cdot x_i \right) + (-S) =$$

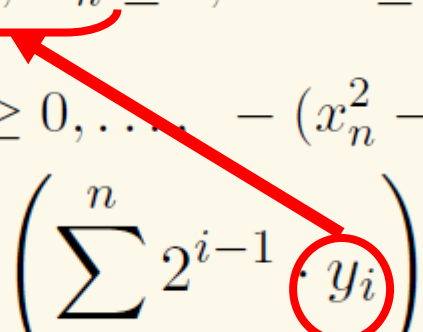
# CPS Upper Bounds

**Proposition:** CPS admits *linear size* refutations of the binary value principle  $BVP_n$ .

*Proof.* Idea: because we have the boolean axioms for the  $\bar{x}$  variables

$$S := \sum_{i=1}^n 2^{i-1} \cdot x_i + 1.$$

$$\overline{\mathcal{H}} := \{ \underbrace{x_1 \geq 0, \dots, x_n \geq 0}_{\text{red bracket}}, -S \geq 0, S \geq 0, x_1^2 - x_1 \geq 0, \dots, x_n^2 - x_n \geq 0, \\ -(x_1^2 - x_1) \geq 0, \dots, -(x_n^2 - x_n) \geq 0, 1 - x_1 \geq 0, \dots, 1 - x_n \geq 0 \}$$

$$C(\overline{x}, \overline{y}) := \left( \sum_{i=1}^n 2^{i-1} \cdot y_i \right) + y_{n+1}$$


$$C(\overline{x}, \overline{\mathcal{H}}) = C(\overline{x}, x_1, \dots, x_n, -S, \dots) = \left( \sum_{i=1}^n 2^{i-1} \cdot x_i \right) + (-S) =$$

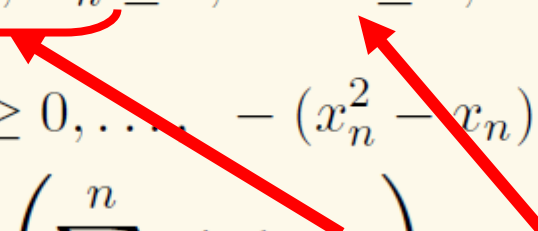
# CPS Upper Bounds

**Proposition:** CPS admits *linear size* refutations of the binary value principle  $BVP_n$ .

*Proof.* Idea: because we have the boolean axioms for the  $\bar{x}$  variables

$$S := \sum_{i=1}^n 2^{i-1} \cdot x_i + 1.$$

$$\overline{\mathcal{H}} := \{ \underbrace{x_1 \geq 0, \dots, x_n \geq 0}_{\text{red bracket}}, -S \geq 0, S \geq 0, x_1^2 - x_1 \geq 0, \dots, x_n^2 - x_n \geq 0, \\ -(x_1^2 - x_1) \geq 0, \dots, -(x_n^2 - x_n) \geq 0, 1 - x_1 \geq 0, \dots, 1 - x_n \geq 0 \}$$

$$C(\overline{x}, \overline{y}) := \left( \sum_{i=1}^n 2^{i-1} \cdot y_i \right) + y_{n+1}$$


$$C(\overline{x}, \overline{\mathcal{H}}) = C(\overline{x}, x_1, \dots, x_n, -S, \dots) = \left( \sum_{i=1}^n 2^{i-1} \cdot x_i \right) + (-S) =$$

# CPS Upper Bounds

**Proposition:** CPS admits *linear size* refutations of the binary value principle  $BVP_n$ .

*Proof.* Idea: because we have the boolean axioms for the  $\bar{x}$  variables

$$S := \sum_{i=1}^n 2^{i-1} \cdot x_i + 1.$$

$$\bar{\mathcal{H}} := \{ \underbrace{x_1 \geq 0, \dots, x_n \geq 0}_{\text{red bracket}}, -S \geq 0, S \geq 0, x_1^2 - x_1 \geq 0, \dots, x_n^2 - x_n \geq 0, \\ -(x_1^2 - x_1) \geq 0, \dots, -(x_n^2 - x_n) \geq 0, 1 - x_1 \geq 0, \dots, 1 - x_n \geq 0 \}$$

$$C(\bar{x}, \bar{y}) := \left( \sum_{i=1}^n 2^{i-1} \cdot y_i \right) + y_{n+1}$$

$$C(\bar{x}, \bar{\mathcal{H}}) = C(\bar{x}, x_1, \dots, x_n, -S, \dots) = \left( \sum_{i=1}^n 2^{i-1} \cdot x_i \right) + (-S) =$$

# CPS = IPS+Binary Value Principle

- IPS\* and CPS\*:

IPS and CPS over  $\mathbb{Q}$ , where: possible values that are computed along the IPS or CPS proofs (as circuits) are *not super-exponential* (for 0-1 input variables).

**Theorem:**  $\text{IPS}^* = \text{CPS}^*$  iff  $\text{IPS}^*$  admits  $\text{poly}(n)$ -size refutations of the Binary Value Principle.



**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

$$\text{VAL} (\text{BIT}_1(f) \cdots \text{BIT}_n(f)) = f$$

**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

$$\text{VAL}(\text{BIT}_1(f) \cdots \text{BIT}_n(f)) = f$$

**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

$$\text{VAL}(\text{BIT}_1(f) \cdots \text{BIT}_n(f)) = f$$

Thanks for listening!

# Appendix

**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

**Proof sketch:** Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- $(\bar{x}, \bar{F}) = -1$  is freely provable in  $\text{IPS}^*$ :  
 $C(\bar{x}, \bar{F}) + 1 = 0$  (this is still not a refutation of  $\bar{F}$ !)
- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value of an integer number given by the  $n$  boolean bits  $w$  in two's complement.

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

where  $\text{BIT}_i(f)$  is the polynomial that computes the  $i$ th bit of the number computed by  $f$  as a function of the variables  $x$  to  $f$  that range over  $\{0, 1\}$  values.

**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

$C(x, F) = -1$  is freely provable in  $\text{IPS}^*$ :  $C(x, F) + 1 = 0$  (this is still not a refutation of  $C(x, F)$  !)

Proof **sketch:** Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- As a polynomial identity  $C(x, F) = -1$  is freely provable in  $\text{IPS}^*$ :

$C(\bar{x}, \bar{F}) + 1 = 0$  (this is still not a refutation of  $\bar{F}$  !)

- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value of an integer number given by the  $n$  boolean bits  $w$  in two's complement.

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

where  $\text{BIT}_i(f)$  is the polynomial that computes the  $i$ th bit of the number computed by  $f$  as a function of the variables  $x$  to  $f$  that range over  $\{0, 1\}$  values.

**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

$C(x, F) = -1$  is freely provable in  $\text{IPS}^*$ :  $C(x, F) + 1 = 0$  (this is still not a refutation of  $C(x, F)$  !)

Proof **sketch:** Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- As a polynomial identity  $C(x, F) = -1$  is freely provable in  $\text{IPS}^*$ ,  $C(\bar{x}, \bar{F}) + 1 = 0$  (this is still not a refutation of  $\bar{F}$ !)

IPS proofs  $A=B$  means:  
from boolean axioms we  
can prove  $A=B$

- IPS can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value of an integer number given by the  $n$  boolean bits  $w$  in two's complement.

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

where  $\text{BIT}_i(f)$  is the polynomial that computes the  $i$ th bit of the number computed by  $f$  as a function of the variables  $x$  to  $f$  that range over  $\{0, 1\}$  values.



**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

$\text{CPS}^* \text{ refutation of } F \text{ is } C(x, F) = -1$  is freely provable in  $\text{IPS}^*$ :  $C(x, F) = -1$  (this is still not a refutation of  $F$  !)

Proof **sketch:** Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value of an integer number given by the  $n$  boolean bits  $w$  in two's complement.

IPS proofs A=B means:  
from boolean axioms we  
can prove A-B

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

where  $\text{BIT}_i(f)$  is the polynomial that computes the  $i$ th bit of the number computed by  $f$  as a function of the variables  $x$  to  $f$  that range over  $\{0, 1\}$  values.

**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

$F F F F \ x, F = -1$  is freely provable in  $\text{IPS}^*$ :  $C C \ x, F \ x x x x, F F F F \ x, F + 1 = 0$  (this is still not a refutation of  $F F F F$  !)

Proof **sketch:** Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value of an integer number given by the  $n$  boolean bits  $w$  in two's complement.
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value of an integer number given by the  $n$  boolean bits  $w$  in two's complement.

IPS proofs  $A=B$  means:  
from boolean axioms we  
can prove  $A=B$

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

where  $\text{BIT}_i(f)$  is the polynomial that computes the  $i$ th bit of the number computed by  $f$  as a function of the variables  $x$  to  $f$  that range over  $\{0, 1\}$  values.

# Thm: $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$ (over $\mathbb{Z}$ , for simplicity)

$\text{CPS}^*$  refutation of  $F = -1$  is freely provable in  $\text{IPS}^*$ :  $\text{CPS}^* \text{ refutation of } F = -1$   
 (this is still not a refutation of  $F = 0$  !)

Proof **sketch**: Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value number given by the  $n$  boolean bits  $w$  in two's complement.

IPS proofs  $A=B$  means:  
 from boolean axioms we  
 can prove  $A=B$

**Lemma**: For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

**Lemma**: For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

where  $\text{BIT}_i(f)$  is the polynomial that computes the  $i$ th bit of the number computed by  $f$  as a function of the variables  $x$  to  $f$  that range over  $\{0, 1\}$  values.

**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

$\sum_{i=1}^n x_i^2 - 1$  is freely provable in  $\text{IPS}^*$ :  $\sum_{i=1}^n x_i^2 - 1 = 0$   
 (this is still not a refutation of  $\sum_{i=1}^n x_i^2 - 1$  !)

Proof **sketch:** Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value number given by the  $n$  boolean bits  $w$  in two's complement.

IPS proofs  $A=B$  means:  
 from boolean axioms we  
 can prove  $A=B$

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

where  $\text{BIT}_i(f)$  is the polynomial that computes the  $i$ th bit of the number computed by  $f$  as a function of the variables  $x$  to  $f$  that range over  $\{0, 1\}$  values.

**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

$\text{CPS}^* \text{ refutation of } F \text{ is } -1$  is freely provable in  $\text{IPS}^*$ :  $\text{CPS}^* \text{ refutation of } F \text{ is } -1$   
 (this is still not a refutation of  $F$  !)

**Proof sketch:** Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value number given by the  $n$  boolean bits  $w$  in two's complement.

IPS proofs A=B means:  
 from boolean axioms we  
 can prove A-B

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

$$\text{VAL}(\text{BIT}_1(f) \cdots \text{BIT}_n(f)) = f$$

where  $\text{BIT}_i(f)$  is the polynomial that computes the  $i$ th bit of the number computed by  $f$  as a function of the variables  $x$  to  $f$  that range over  $\{0, 1\}$  values.

**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

$\text{CPS}^*$  refutation of  $F$  is freely provable in  $\text{IPS}^*$ :  $\text{CPS}^* \text{ refutation of } F \text{ is freely provable in } \text{IPS}^*$   
 (this is still not a refutation of  $F$  !)

**Proof sketch:** Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value number given by the  $n$  boolean bits  $w$  in two's complement.

IPS proofs A=B means:  
 from boolean axioms we  
 can prove A=B

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

$$\text{VAL}(\text{BIT}_1(f) \cdots \text{BIT}_n(f)) = f$$

where  $\text{BIT}_i(f)$  is the polynomial that computes the  $i$ th bit of the number computed by  $f$  as a function of the variables  $x$  to  $f$  that range over  $\{0, 1\}$  values.

Thm:  $CPS^* = IPS^* + BVP_n$  (over  $\mathbb{Z}$ , for simplicity)

$FFFF \ x, F = -1$  is freely provable in  $IPS^*$ :  $CC \ x, F \ x \ x \ x, F \ F \ F \ x, F + 1 = 0$   
 (this is still not a refutation of  $FFFF$  !)

Proof sketch: Let  $C(\bar{x}, \bar{F}) = -1$  be a  $CPS^*$  refutation of  $\bar{F}$ .

- $IPS$  can do efficient bit-arithmetic as follows:
- Define  $VAL(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value number given by the  $n$  boolean bits  $w$  in two's complement.

IPS proofs A=B means:  
 from boolean axioms we  
 can prove A-B

**Lemma:** For any circuit  $f$ ,  $IPS^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

**Lemma:** For any circuit  $f$ ,  $IPS^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

$$\text{VAL}(\text{BIT}_1(f) \cdots \text{BIT}_n(f)) = f$$

where  $\text{BIT}_i(f)$  is the polynomial that computes the  $i$ th bit of

the number computed by  $f$  as a function of the variables  $x$  to  $f$  that range over  $\{0, 1\}$  values.

# Thm: $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$ (over $\mathbb{Z}$ , for simplicity)

$F F F F \ x, F = -1$  is freely provable in  $\text{IPS}^*$ :  $CC \ x, F \ x \ x \ x \ x, F F F F \ x, F + 1 = 0$   
 (this is still not a refutation of  $F F F F$  !)

Proof **sketch**: Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value of the integer number given by the  $n$  boolean bits  $w$  in two's complement.

IPS proofs A=B means:  
 from boolean axioms we  
 can prove A-B

**Lemma**: For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

**Lemma**: For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

where  $\text{BIT}_i(f)$  is the polynomial  $\text{VAL}(\text{BIT}_1(f) \cdots \text{BIT}_n(f)) = f$

the number computed by  $f$  as a function of the variables  $x$

the number computed by  $f$  as a function of the variables  $x$

to  $f$  that range over  $\{0, 1\}$  values.



**Thm:**  $\text{CPS}^* = \text{IPS}^* + \text{BVP}_n$  (over  $\mathbb{Z}$ , for simplicity)

$\text{CPS}^*$  refutation of  $F$  is freely provable in  $\text{IPS}^*$ :  $\text{CPS}^* \text{ refutation of } F \text{ is freely provable in } \text{IPS}^*$   
 (this is still not a refutation of  $F$  !)

**Proof sketch:** Let  $C(\bar{x}, \bar{F}) = -1$  be a  $\text{CPS}^*$  refutation of  $\bar{F}$ .

- $\text{IPS}$  can do efficient bit-arithmetic as follows:
- Define  $\text{VAL}(w) := w_1 + 2w_2 + \dots + 2^{n-2}w_{n-1} - 2^{n-1}w_n$  to be the value number given by the  $n$  boolean bits  $w$  in two's complement.

IPS proofs A=B means:  
 from boolean axioms we  
 can prove A=B

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

**Lemma:** For any circuit  $f$ ,  $\text{IPS}^*$  has a  $\text{poly}(|f|)$ -size proof (from boolean axioms) of

$$\text{VAL}(\text{BIT}_1(f) \cdots \text{BIT}_n(f)) = f$$

where  $\text{BIT}_i(f)$  is the polynomial

$$\text{VAL}(\text{BIT}_1(f) \cdots \text{BIT}_n(f)) = f$$

the number computed by  $f$  as a function of the variables  $x$

to  $f$  that range over  $\{0, 1\}$  values.

to  $f$  that range over  $\{0, 1\}$  values.

# Proof (cnt.)

- We have IPS\* proof from boolean axioms of

$$C(\bar{x}, \bar{F}) = \text{VAL}(\text{BIT}_1(C) \cdots \text{BIT}_n(C)) = -1.$$

- Since C is a conic circuit and thus preserves non-negative signs we can prove:

$$\text{the sign-bit } \text{BIT}_n(C) = 0.$$

- We are left with the need to refute

$$\text{VAL}(\text{BIT}_1(C) \cdots \text{BIT}_{n-1}(C)) = -1$$

which is precisely  $\text{BVP}_n$ .

QED

$$\text{IPS}_{\mathbb{Z}} \geq_p \text{IPS}_{\mathbb{Q}}$$

**Prop:** Size- $s$  constant-free  $\text{IPS}_{\mathbb{Q}}$  from  $F$  of  $H$ , for  $F$  a set of assumptions ( $F, H$  written as constant-free algebraic circuits over  $\mathbb{Z}$ ) then there exists a size  $\leq 4s$  constant-free boolean  $\text{IPS}_{\mathbb{Z}}$  proof of  $M \cdot H$ , for some  $M$  in  $\mathbb{Z} \setminus \{0\}$ , such that  $\tau(M) \leq 4s$ .

*Proof.* Multiply the  $\text{IPS}_{\mathbb{Q}}$  enough times to get all constants integers.