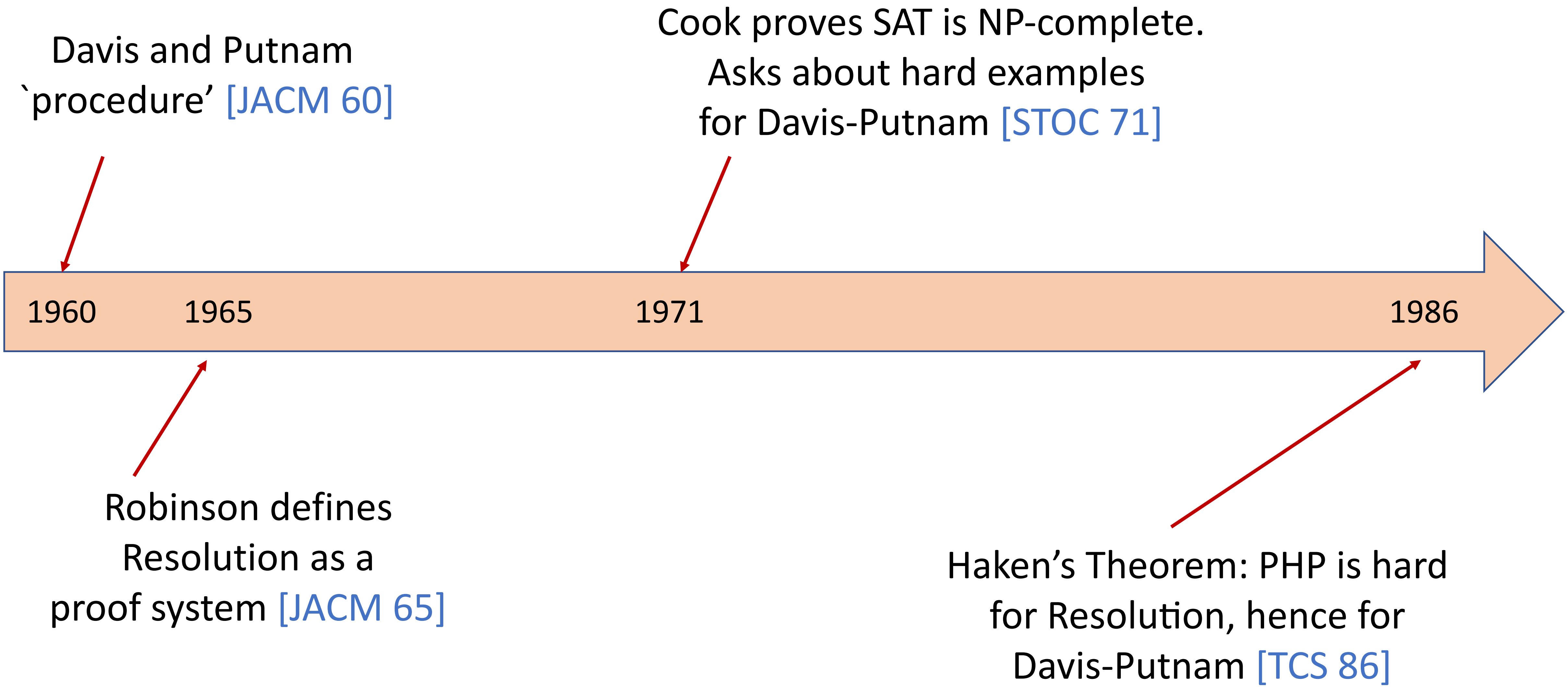
AUTOMATING RESOLUTION IS NP-HARD

Albert Atserias Moritz Müller

Universitat Politècnica de Catalunya
Barcelona

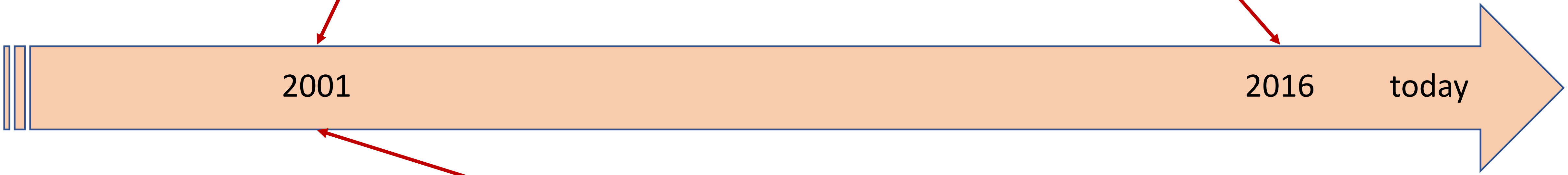
Satisfiability Problem and Resolution : Timeline 1960-1986



Satisfiability Problem and Resolution : Timeline 1987-today

CHAFF implementation.
First “evidence”
that proof-search
is “easy”. [CAD 01]

Boolean Pytagorean Triple Problem:
200 TB Resolution proof! [Nature 16]



Alekhnovich-Razborov.
First “evidence”
that proof-search
is “hard” [FOCS 01]

DEFINITIONS AND STATEMENT OF THE MAIN RESULT

Variables, Literals, Clauses, and CNF Formulas

$$\left.x_1, x_2, \ldots, x_n \quad \text{and} \quad \neg x_1, \neg x_2, \ldots, \neg x_n\right\} \text{literals}$$

$$\overbrace{(l_1 \vee \cdots \vee l_k)}^{\text{a clause}} \qquad \overbrace{C_1 \wedge \cdots \wedge C_m}^{\text{a CNF formula}}$$

literals of the clause

clauses of the CNF

$$F = (x_1 \vee \neg x_3 \vee x_5) \wedge (x_2 \vee x_4) \wedge (\neg x_2 \vee x_5 \vee x_3)$$

an example

Resolution Rule: Derives New Clauses From Old

given $C \vee x$ and $D \vee \neg x$ infer $C \vee D$

left premise

right premise

resolvent

Resolution Refutations, a.k.a. Proofs of Unsatisfiability

the refuted CNF formula

a refutation of F

$$\overbrace{C_1, \dots, C_i, \dots, C_m}^{F} : \quad \overbrace{D_1, \dots, D_j, \dots, D_k, \dots, D_l, \dots, D_s}^{P} = \emptyset$$

Hypothesis

Left Right

the proof-graph of P

$\text{Length}(P) \quad := \quad s$

$\text{Res}(F) \quad := \quad \inf \{ \text{Length}(P) \; : \; P \text{ is a Resolution refutation of } F \}$

Note: $Res(F) \leq 2^n$ **or** $Res(F) = \infty$

Proof Search Problem for Resolution

Given an unsatisfiable CNF formula F

find a Resolution refutation of F

by Haken's Theorem,
the complexity is necessarily
exponential in the size of F

Proof Search Problem for Resolution

Q1: Could we find short proofs under the promise that they exist?

alternative formulations of the same question

Q2: Could the problem be solved in reasonable time as a function of n, m, and $s = \text{Res}(F)$?

We would say that Resolution is AUTOMATABLE in poly time, quasipoly time, etc.
[Bonet, Pitassi, Raz 97]

Main Result

Theorem:

Resolution is not automatable
in polynomial-time unless P = NP

Main Result

Theorem:

Resolution is not automatable
in polynomial-time unless P = NP
nor in subexponential-time unless ETH fails

Main Result (contd)

We find a map that takes CNFs into CNFs:

$$F \xrightarrow{\text{polytime}} G$$

SMALL

F is satisfiable $\Longrightarrow$ $\text{Res}(G) \leq |G|^{1+\varepsilon}$

F is unsatisfiable $\Longrightarrow$ $\text{Res}(G) \geq \exp(|G|^{\frac{1}{2}-\varepsilon})$

BIG

Main Result (contd)

Corollary:

Minimum Resolution proof-length
is not approximable
within subexponential error
in polynomial-time
unless P = NP

HISTORY OF THE PROBLEM

History of the problem

- Some partial POSITIVE results.

- Some partial NEGATIVE results.

Stronger and Weaker Proof Systems

arbitrary formulas, circuits, etc.

given $C \vee A$ and $D \vee \neg A$ infer $C \vee D$

Stronger and Weaker Proof Systems

Extended Frege	circuits
Frege	formulas
TC^0-Frege	threshold formulas of bdd depth
AC^0-Frege	formulas of bdd depth
k-DNF-Frege $\equiv$ Res(k)	k-DNFs
Resolution	**clauses**
regular Resolution	clauses, but read-once proof-graphs
tree-like Resolution	clauses, but tree-like proof-graphs

Partial POSITIVE Result 1: Tree-like Resolution in quasi-poly time

Theorem [Beame-Pitassi 98]

Tree-like Resolution is automatable in time $n^{O(\log s)}$

- Intuitively: tree-like proofs $\equiv$ decision trees, and divide & conquer works.
- It says: upper bound $\mathrm{Res}(G) \leq$ **SMALL** cannot be tree-like (unless ETH fails).

Partial POSITIVE Result 2: Resolution in subexponential time

Theorem [Ben-Sasson-Wigderson 99]

Resolution is automatable in time $n^{O(\sqrt{n \log s}+k)}$

- For $s = \mathrm{poly}(n)$, this is $\exp(n^{1/2} \log(n)^{3/2})$.
- Puts limits on the efficiency of our reduction (unless ETH fails).

Partial NEGATIVE Result 1: Stronger Proof Systems

Theorem [Krajicek-Pudlak 98]

Extended Frege is not automatable in poly time

unless RSA is broken by poly-size circuits

- Assumption is crypto, and far from optimal.
- Later improved to Frege, TC^0-Frege and AC^0-Frege [Bonet et al. 97, 99]
- Still crypto and very far from Resolution.

Partial NEGATIVE Result 2: Weaker Hardness, Stronger Assumption

Theorem [Alekhnovich-Razborov 01]

Resolution is not automatable

in polynomial time unless W[P] is tractable

- Says nothing about automatability in, say, quasipoly-time.
- Best lower bound: time $n^{\log\log(n)^{0.14}}$, under ETH [Mertz-Pitassi-Wei 19]
- Applies to tree-like Resolution!

THE NEW CONSTRUCTION

$$F \xrightarrow{\text{polytime}} G$$

F is satisfiable $\Longrightarrow$ $\mathrm{Res}(G) \leq$ **SMALL**

F is unsatisfiable $\Longrightarrow$ $\mathrm{Res}(G) \geq$ **BIG**

Reflection Principle for Resolution

[Cook 75, Razborov 96, Pudlak 01]

X encodes a CNF formula

$$SAT(X, Y) \wedge REF(X, Z)$$

Y encodes a truth-assignment

Z encodes a Resolution refutation (of length $\leq |Z|$)

Reflection Principle for Resolution (cntd)

$$\overbrace{C_1, \dots, C_i, \dots, C_m}^{F}: \qquad \overbrace{D_1, \dots, D_j, \dots, D_k, \dots, D_l, \dots, D_s}^{P} = \emptyset$$

Left Right

$$SAT(X, Y) \wedge REF(X, Z)$$

$X(i, q, b)$: clause C_i contains variable x_q with sign b

$Y(q)$: variable x_q evaluates to 1 under the truth assignment

$\mathrm{Z}(i, j, k, q)$: clause D_i is inferred from D_j and D_k by resolving on x_q

$\mathrm{Z}(i, q, b)$: clause D_i contains variable x_q with sign b

Reflection Principle for Resolution (cntd)

building on
[Pudlak 01]

Theorem [Atserias-Bonet 02]

$SAT(X, Y) \wedge REF(X, Z)$ has poly-size 2-DNF Frege refs.

Reflection Principle for Resolution (cntd)

Proof (idea):

$$\underbrace{D_1, \dots, D_j, \dots, D_k, \dots, D_l, \dots, D_s = \emptyset}$$

$SAT(X, Y)$

$REF(X, Z)$

s

$\bigvee_{q=1}^{n}\big(Y(q) \wedge Z(1, q, 1)\big) \vee \bigvee_{q=1}^{n}\big(\neg Y(q) \wedge Z(1, q, 0)\big).$

$\dots$

$\bigvee_{q=1}^{n}\big(Y(q) \wedge Z(s, q, 1)\big) \vee \bigvee_{q=1}^{n}\big(\neg Y(q) \wedge Z(s, q, 0)\big).$

But REF says that this last one is empty!

2-DNF formulas

First Half of the Main Result

Corollary

F is satisfiable $\implies$ $\text{Res}(\underbrace{REF(F,Z)}_{G}) \leq$ **SMALL**

Proof (idea):

- Suppose Y satisfies F
- $SAT(F,Y) \wedge REF(F,Z) \equiv \overbrace{REF(F,Z)}^{G}$
- $\bigvee_{q=1}^{n}\big(Y(q) \wedge Z(i,q,1)\big) \vee \bigvee_{q=1}^{n}\big(\neg Y(q) \wedge Z(i,q,0)\big)$ is a clause!

Status

F is satisfiable $\Longrightarrow$ $\text{Res}(\overbrace{REF(F, Z)}^{G}) \leq$ **SMALL** !

F is unsatisfiable $\Longrightarrow$ $\text{Res}(REF(F, Z)) \geq$ **BIG** ? ?

for poly length Z

Towards a Lower Bound

want this to be **HARD** to refute

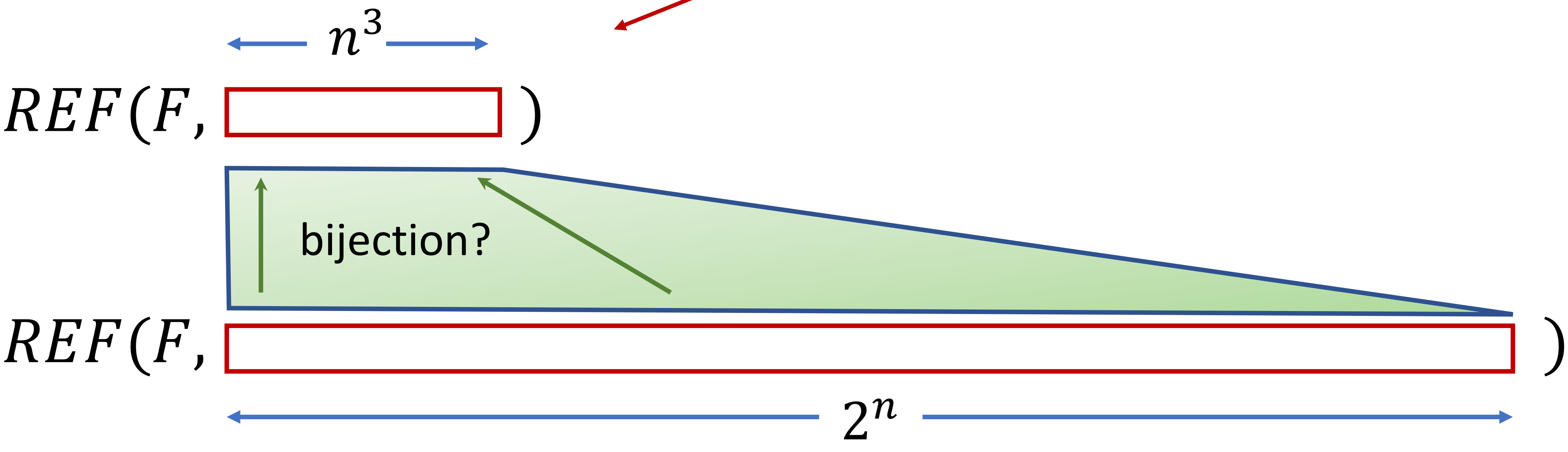
$$REF(F, \underbrace{\boxed{\qquad\qquad}}_{n^3})$$

$$REF(F, \underbrace{\boxed{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}}_{2^n})$$

know this is **IMPOSSIBLE** to refute
(since, F being unsat, $REF(F, 2^n)$ is sat)

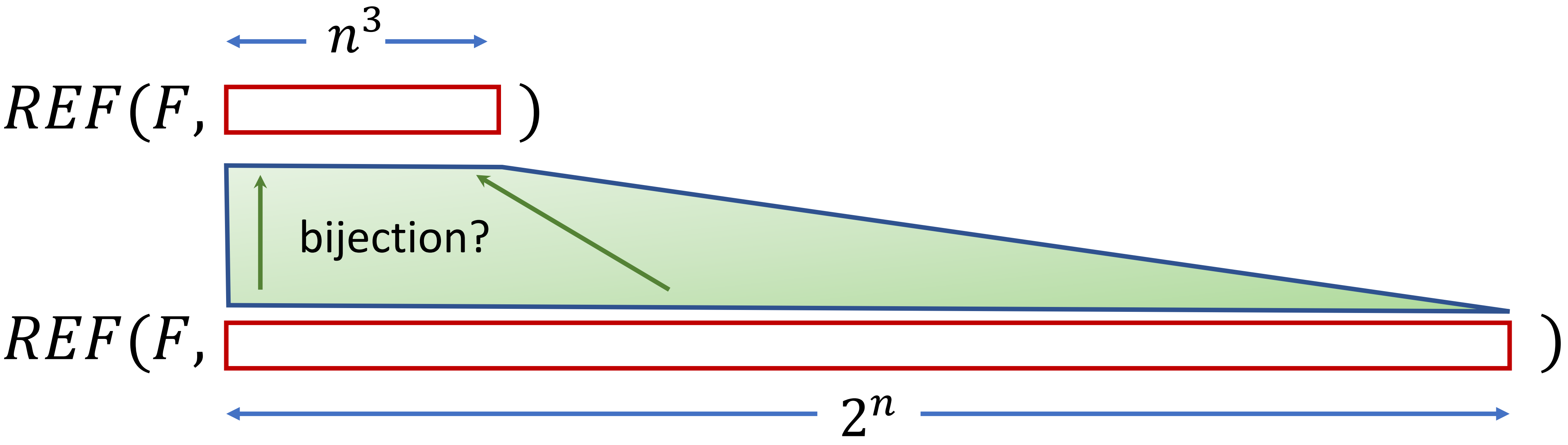
Towards a Lower Bound

want this to be **HARD** to refute



know this is **IMPOSSIBLE** to refute
(since, F being unsat, $REF(F, 2^n)$ is sat)

Towards a Lower Bound



Q1: Could we TRANSPORT the sat assignment?
Q2: Could we also PRESERVE its local structure?

(cf. [Razborov 98],[Krajicek 01])

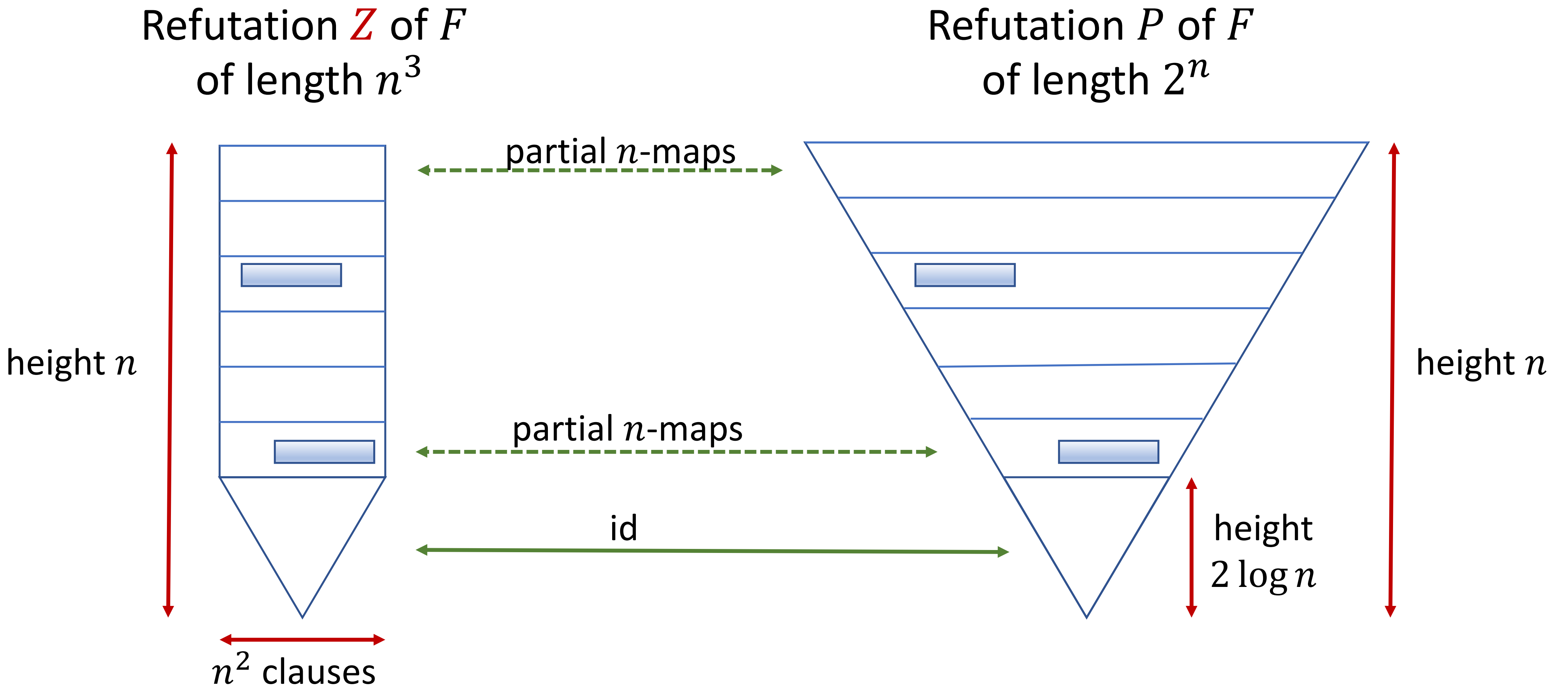
Towards a Lower Bound

Alas! Not known!

$\Bigg($ **Since** $bijectivePHP(n^3, 2^n)$ is PRESUMABLY HARD for 2-DNF Frege $\Bigg)$

F is unsatisfiable $\quad \Longrightarrow \quad$ $\text{Res}(REF(F, n^3)) \geq$ **BIG**

Towards a Lower Bound: Width



$$REF(F, n^3) \equiv_n REF(F, 2^n) \equiv 1$$

width-n
local views:

Towards a Lower Bound: Width

Alas! Not enough for
Ben-Sasson-Wigderson to apply!

Theorem

F is unsatisfiable $\implies$ Resolution refs of $REF(F, Z)$
require (index-)width $\geq$ n

for Z of length n^3

Relativization

[Krajicek 01]

$$REF(X, Z)$$

$$\boldsymbol{R}REF(X, Z)$$

new variables

$\mathrm{Z}(i)$: clause D_i is active

$\mathrm{Z}(i, j, k, q)$: $\boxed{\text{if active,}}$ clause D_i is inferred from D_j and D_k by resolving on x_q

$\mathrm{Z}(i, q, b)$: $\boxed{\text{if active,}}$ clause D_i contains variable x_q with sign b

Relativization (cntd)

$$\boldsymbol{R}REF(X, Z)$$

A few representative clauses of $RREF$:

$\neg Z(i) \vee \neg Z(i,j,k,q) \vee Z(j)$ activity propagates upwards

$\neg Z(i) \vee \neg Z(i,j,k,q) \vee Z(j,q,0)$ proof shape is required on active clauses (only)

$Z(s)$ last clause is active

etc ...

Lower Bound: Apply a Random Restriction

[Dantchev-Riis 03]

Refutation of $\boldsymbol{R}REF(F, n^3)$

small length

Refutation of $REF(F, n^3)$

w/ prob. $\geq 1 - 2^{-cn}$
index-width $< n$

$Z(s)$	:= 1		
$Z(i)$	:= 1 or 0	w/ prob. 1/2	**if** $i \neq s$
$Z(i, q, b)$	:= 1 or 0	w/ prob. 1/2	**if** $Z(i) = 0$
$Z(i, j, k, q)$	:= 1 or 0	w/ prob. 1/2	**if** $Z(i) = 0$
$Z(i, j, k, q)$	:= 0		**if** $Z(i) = 1$ and not $Z(j) = Z(k) = 1$

Upper Bound Revisited

active

$$\boldsymbol{D_1}, D_2, \dots, D_j, \dots, \boldsymbol{D_k}, \dots, D_i, \dots, \boldsymbol{D_l}, \dots, \boldsymbol{D_s}$$

$$SAT(X, Y) \wedge \boldsymbol{R}REF(X, Z)$$

$$SAT(X, Y)$$

$$RREF(X, Z)$$

$$\neg Z(1) \vee \bigvee_{q=1}^{n} \big(Y(q) \wedge Z(1, q, 1)\big) \vee \bigvee_{q=1}^{n} \big(\neg Y(q) \wedge Z(1, q, 0)\big).$$

s $\dots$

$$\neg Z(s) \vee \bigvee_{q=1}^{n} \big(Y(q) \wedge Z(s, q, 1)\big) \vee \bigvee_{q=1}^{n} \big(\neg Y(q) \wedge Z(s, q, 0)\big).$$

But $RREF$ says that s is active **and** empty!

still 2-DNF formulas

All Together

F is satisfiable $\implies$ $\text{Res}(RREF(F, n^3)) \leq$ **SMALL**

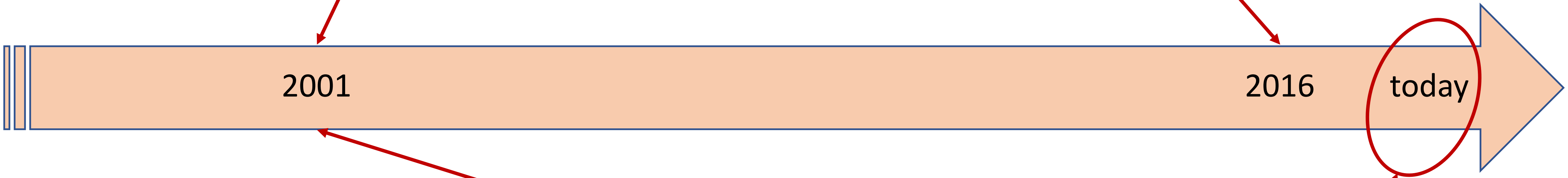
F is unsatisfiable $\implies$ $\text{Res}(RREF(F, n^3)) \geq$ **BIG**

TO CONCLUDE

Satisfiability Problem and Resolution

CHAFF implementation.
First “evidence”
that proof-search
is “easy”. [CAD 01]

Boolean Pytagorean Triple Problem:
200 TB Resolution proof! [Nature 16]



Alekhnovich-Razborov.
First “evidence”
that proof-search
is “hard” [FOCS 01]

Proof-search
is as hard
as it can be

Buffer

$$\frac{C \vee x \qquad\qquad D \vee \neg x}{C \vee D}$$

F is satisfiable $\implies$ min Resolution refutation size of G is $\leq |G|^{1+\varepsilon}$

F is unsatisfiable $\implies$ min Resolution refutation size of G is $\geq \exp(|G|^{\frac{1}{2}-\varepsilon})$

The Resolution rule:

$$\text{given} \quad \underbrace{C \vee x}_{\text{the left premise}} \quad \text{and} \quad \underbrace{D \vee \neg x}_{\text{the right premise}} \quad \text{infer} \quad \underbrace{C \vee D}_{\text{the resolvent}}$$

A Resolution refutation of F (a.k.a. proof of unsatisfiability):

$$\overbrace{C_1, \dots, C_i, \dots, C_m}^{F}: \qquad \overbrace{D_1, \dots, D_j, \dots, D_k, \dots, D_l, \dots, D_t = \emptyset}^{P}$$

Hypothesis

Left

Right

History of the problem

- Some partial positive automatability results:
  - for tree-like Resolution in quasipoly-time,
  - for general Resolution in non-trivial time.

- Some partial negative automatability results:
  - for stronger proof systems,
  - for weak approximation
  - under stronger (non-optimal) assumptions.

Partial negative automatability results:

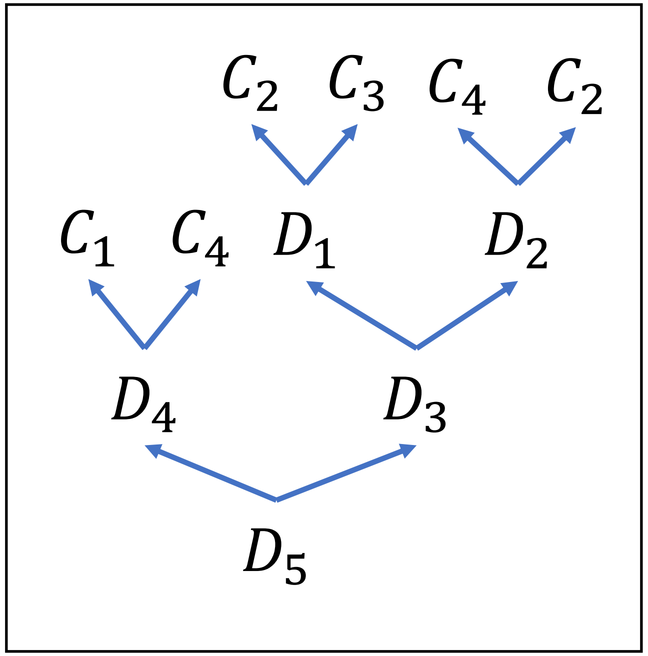
- for stronger proof systems under stronger assumptions
- for Resolution under stronger assumptions
- very weak hardness of approximation of min-proof-length

Partial positive automatability results:

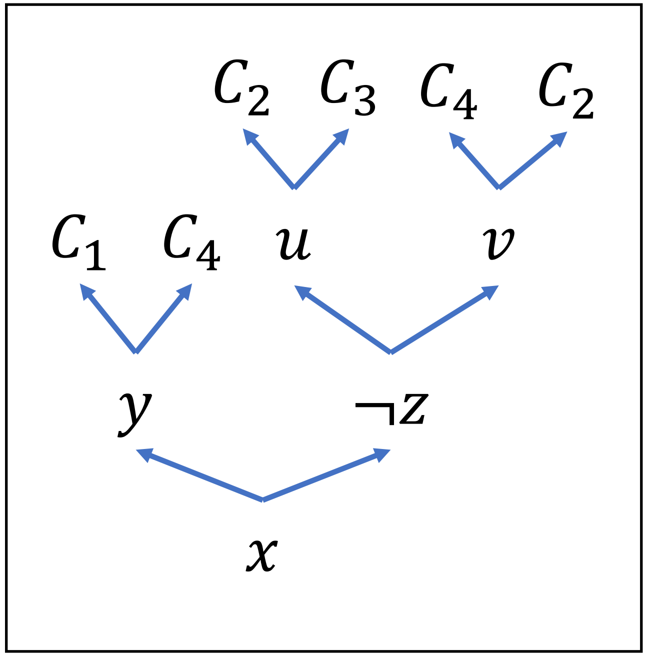
- for tree-Resolution in quasi-polynomial time
- for Resolution in non-trivial exponential time

Tree-like Resolution Proof Search

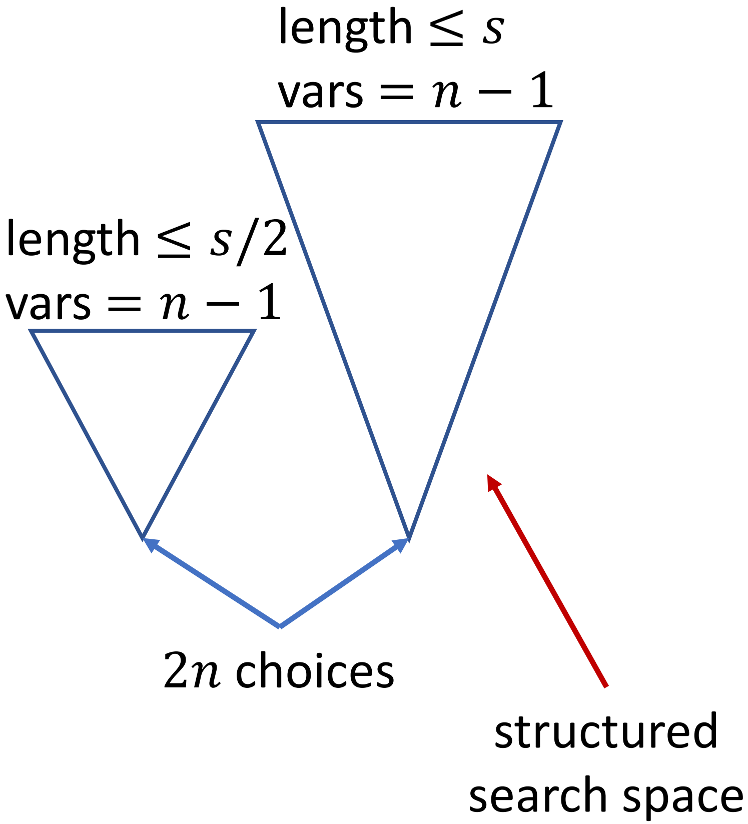
$$\overbrace{C_1, \dots, C_i, \dots, C_m}^{F}: \qquad \overbrace{D_1, \dots, D_j, \dots, D_k, \dots, D_l, \dots, D_s}^{P} = \emptyset$$



tree-like proof view



decision tree view



Stronger Proof Systems (cntd)

Extended Frege not automatable in polynomial time

assuming RSA secure against poly-size circuits

[Krajicek-Pudlak 1998]

Frege and TC^0-Frege not automatable in polynomial time

assuming Diffie-Helman secure against poly-size circuits

[Bonet-Pitassi-Raz 2000]

AC^0-Frege not automatable in polynomial time

assuming Diffie-Helman secure against subexponential circuits

[Bonet-Domingo-Gavalda-Maciel-Pitassi 2004]

Proof idea:

Let F : {0,1}^n -> {0,1}^n be a one-way permutation.
Let WITNESS_b(X,Y) say “Y is a witness that hard bit of F(X) is b.”
Then

WITNESS_0(X,Y) & WITNESS_1(X,Z)

has a short Extended Frege refutation. QED

Resolution Refutations, a.k.a. Proofs of Unsatisfiability

the refuted CNF formula

the refutation of F

$$\overbrace{C_1, \dots, C_i, \dots, C_m}^{F} : \qquad \overbrace{D_1, \dots, D_j, \dots, D_k, \dots, D_l, \dots, D_s = \emptyset}^{P}$$

Hypothesis

Left

Right

$$\begin{aligned}
\text{Length}(P) &:= s &&\leq 2^{n+1} \\
\text{Width}(P) &:= \max_i |D_i| &&\leq n \\
\text{Size}(P) &:= \textstyle\sum_i |D_i| &&\leq \text{Length}(P) \cdot \text{Width}(P)
\end{aligned}$$

$$\text{Res}(F) := \min \{ \text{Length}(P) : P \text{ is a Resolution refutation of } F \}$$

Stronger Proof Systems (cntd)

Theorem [Bonet-Pitassi-Raz 97]

Frege and TC^0-Frege are not automatable in poly time

unless Diffie-Helman is broken by poly size circuits

Theorem [Bonet-Domingo-Gavalda-Maciel-Pitassi 99]

AC^0-Frege is not automatable in poly time

unless Diffie-Helman is broken by subexp size circuits

Partial NEGATIVE Result 1: Stronger Proof Systems

[Bonet-Pitassi-Raz 97]

[Bonet-Domingo-Gavalda-Maciel-Pitassi 99]

Non-automatability of Frege, TC^0-Frege and AC^0-Frege unless different (still crypto) assumptions fail

Reflection Principle for Resolution (cntd)

Proof (idea):

$$\underbrace{D_1, \dots, D_j, \dots, D_k, \dots, D_l, \dots, D_s = \emptyset}$$

$$SAT(X, Y) \wedge REF(X, Z)$$

Each clause D_i in Z is made *true* by Y!

$$\bigvee_{q=1}^{n} \big(Y(q) \wedge Z(i, q, 1)\big) \vee \bigvee_{q=1}^{n} (\neg Y(q) \wedge Z(i, q, 0))$$

But for $i = s$ this is the empty clause!

2-DNF formulas