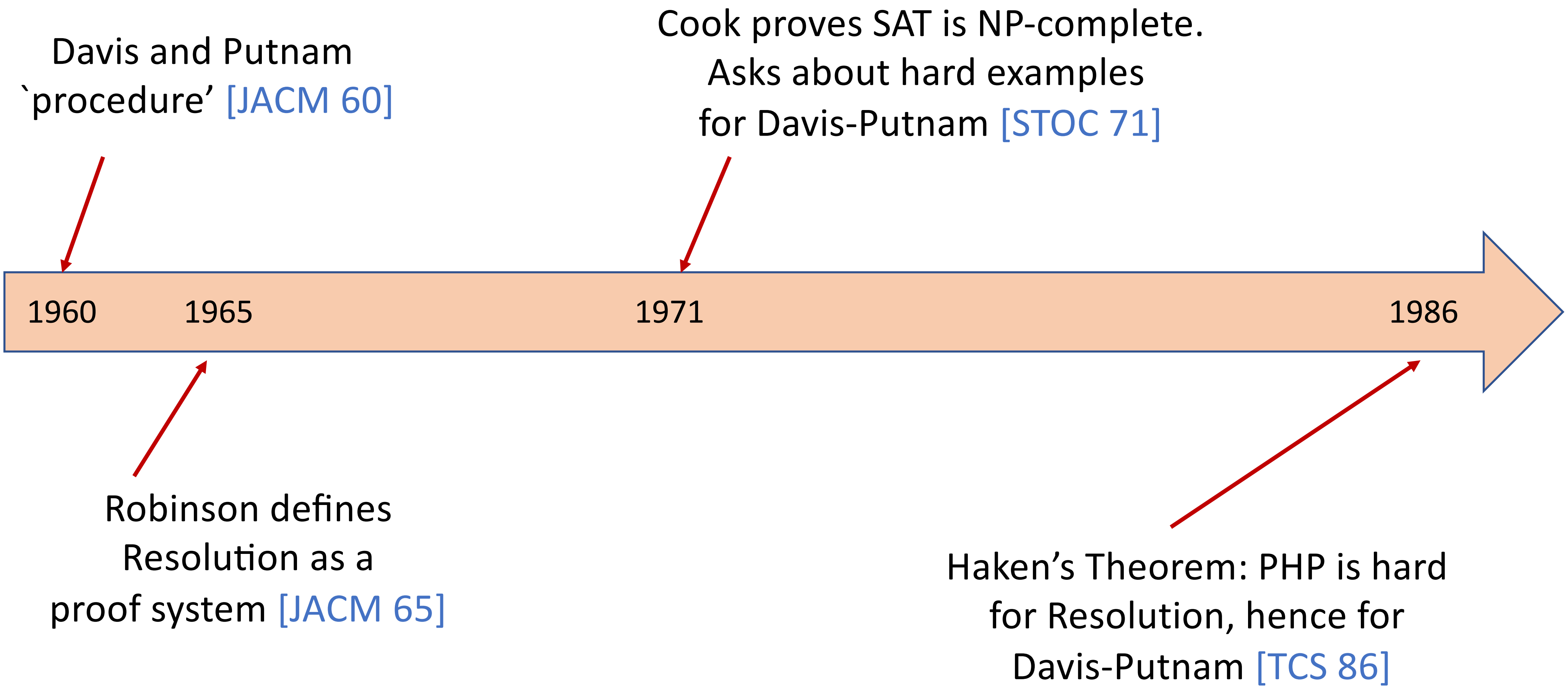
AUTOMATING RESOLUTION IS NP-HARD

Albert Atserias

Moritz Müller

Universitat Politècnica de Catalunya

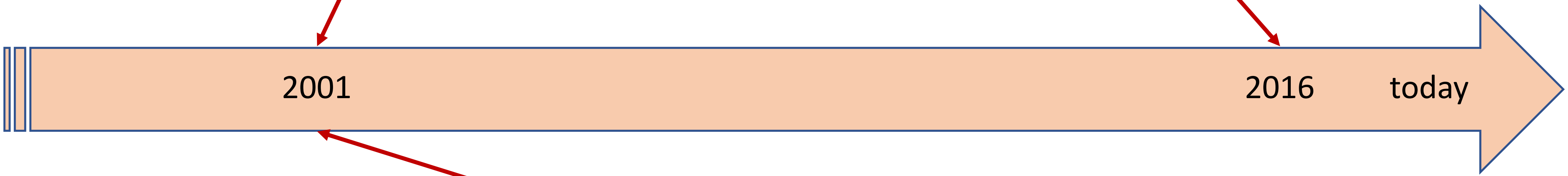
Satisfiability Problem and Resolution : Timeline 1960-1986



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

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

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

literals of the clause

clauses of the CNF

an example

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

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

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

Hypothesis

Left

Right

the proof-graph of P

Length(P) := s

Res(F) := $\min \{$ Length(P) : P is a Resolution refutation of F $\} \leq 2^{n+1}$

Proof Search Problem for Resolution

$\boxed{\text{Given an unsatisfiable CNF formula } F \text{ find a Resolution refutation of } F}$

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 solvable
in time polynomial 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)

Indeed, we find a map from CNFs to CNFs:

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

SMALL

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

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

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 $C \vee D$

⋮

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

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 $\exp(n^{1/2} \log(n)^{3/2})$.
- It puts some 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]

X encodes a CNF formula

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

Y encodes a truth-assignment

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

(Our G will be $REF(F, Z)$, essentially)

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

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

$X(i, q, b)$	: variable x_q appears in clause C_i with sign b
$Y(q)$	: variable x_q evaluates to 1 under the truth assignment
$\mathrm{Z}(l, j, k, q)$	: clause D_l is inferred from D_j and D_k by resolving on x_q
$\mathrm{Z}(i, q, b)$	: variable x_q appears in clause D_i 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):

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

clauses of $SAT(X, Y)$

clauses of $REF(X, Z)$

s

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

...

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

But REF says that this last one is $\emptyset$!

2-DNF formulas

First Half of the New Construction

Corollary

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

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!

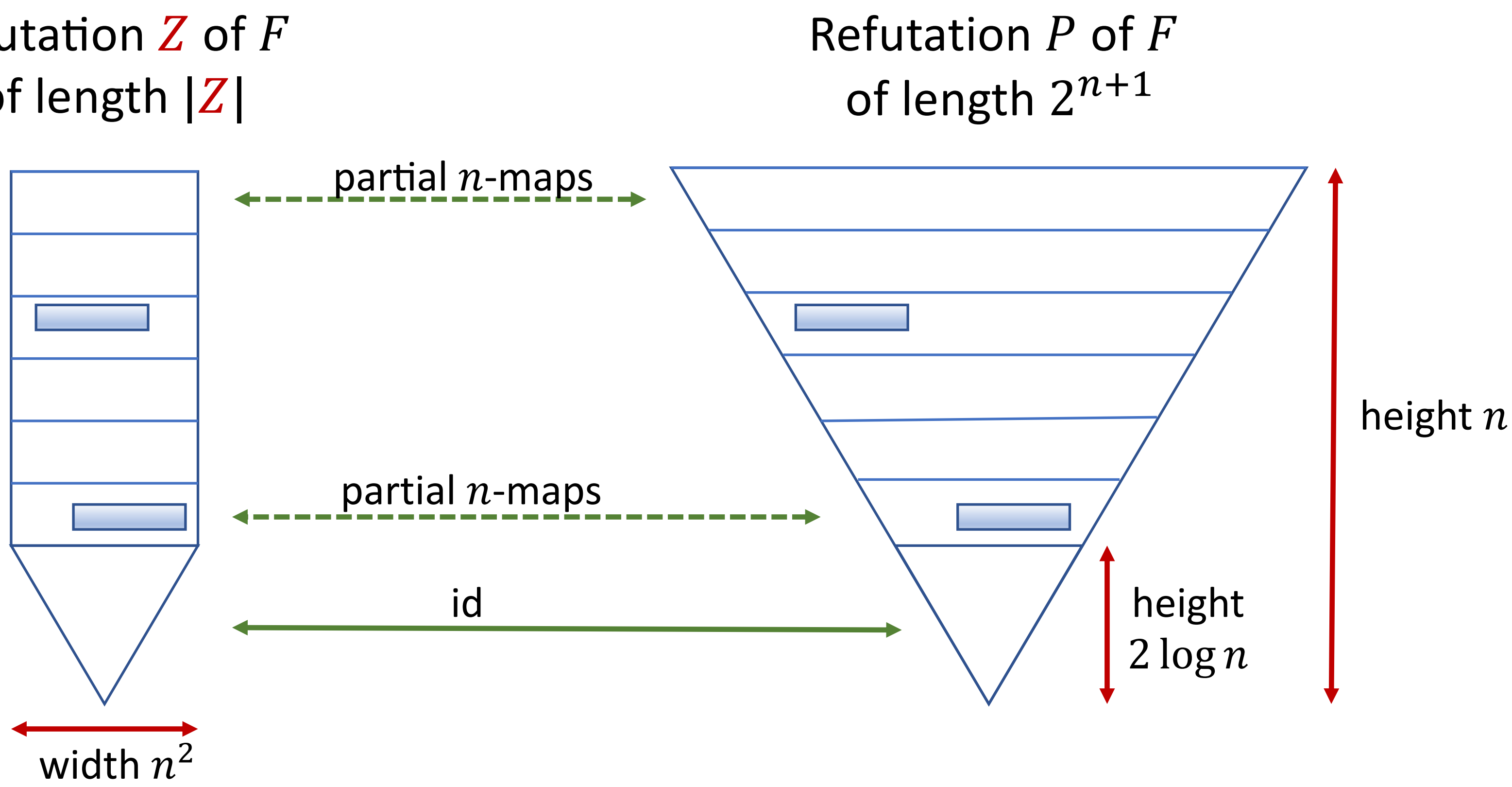
Status

F is satisfiable $\implies$ $\mathrm{Res}(\overbrace{REF(F, Z)}^{G}) \leq$ **SMALL** ❗

F is unsatisfiable $\implies$ $\mathrm{Res}(REF(F, Z)) \geq$ **BIG** ❓

for poly length Z

Indistinguishability Argument for Unsatisfiable F



$$REF(F, Z) \equiv_n REF(F, P) \equiv 1$$

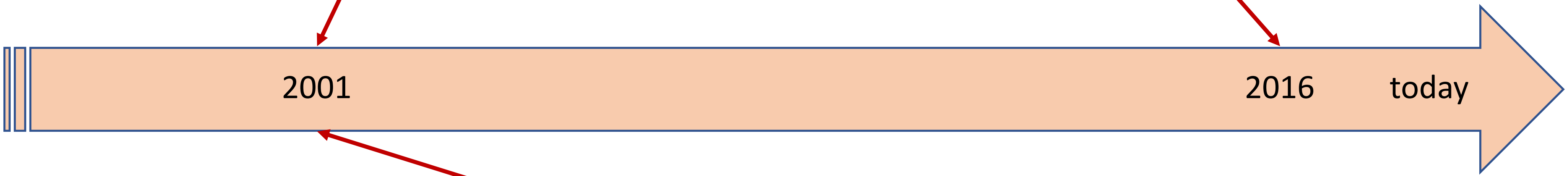
width-n
local views:

TO CONCLUDE

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]

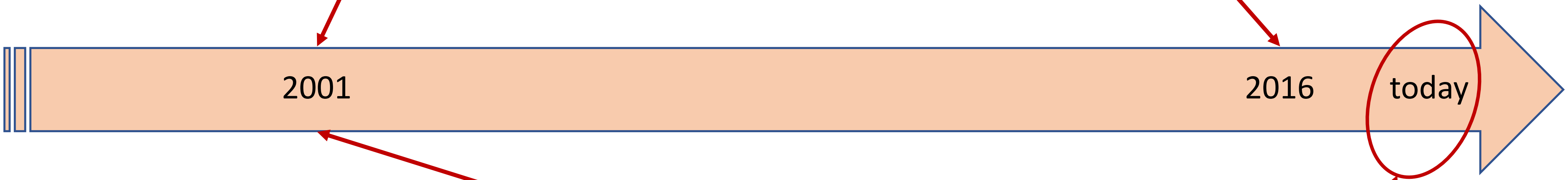


Alekhnovich-Razborov.
First “evidence”
that proof-search
is “hard” [FOCS 01]

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]

AUTOMATING RESOLUTION IS NP-HARD