Proof Complexity
Part A: Introduction, Frege proofs, Abstract proof systems and Resolution

Sam Buss

Satisfiability Boot Camp
Simons Institute, Berkeley, California
January–May 2021

Part A. discusses:

- Frege proofs
- Abstract proof systems
  p-simulation
- Resolution
- Extended resolution / extended Frege

Propositional logic, satisfiability, tautologies

Propositional formulas:

- Variables: Range over *True/False*.
  Variables are denoted $x, y, z, \ldots$ or $p, q, \ldots$.
- Literals: Variables and negated variables.
  Negation of x sometimes denoted $\overline{x}$. Then $\overline{\overline{x}}$ is x.
- Formulas: Formed from variables/literals, and propositional connectives, such as $\wedge$, $\vee$, $\rightarrow$, $\neg$.
  Formulas are denoted $\varphi, \psi, \ldots$
- CNF, DNF - Conjunctive/Disjunctive Normal Form Formulas.

Satisfiability and Validity:

- A formula φ is a **tautology** iff every truth assignment makes φ true. We also say φ is **valid**.
- A formula φ is **satisfiable** iff some truth assignment makes φ true.
- φ is unsatisfiable iff $\neg\varphi$ is a tautology.
- It is NP-hard to determine satisfiability/validity of a formula φ.
- It is NP-hard to determine satisfiability of a CNF formula φ.
- It is NP-hard to determine validity of a DNF formula φ.
- One way to establish satisfiability is to give a **satisfying assignment** for φ.
- One way to establish unsatisfiability is to give a **proof** of $\neg\varphi$.

First example of a proof system (Frege system)

The **Frege proof system** $\mathcal{F}$ is a "textbook-style" propositional proof system with Modus Ponens as its only rule of inference.

Variables: x, y, z, ... range over *True*/*False*.
Connectives: $\neg$, $\wedge$, $\vee$, $\rightarrow$.

Modus Ponens: $$\frac{\varphi \qquad \varphi \rightarrow \psi}{\psi}.$$

Axiom Schemes:
$$\varphi \rightarrow \psi \rightarrow \varphi$$
$$(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \psi \rightarrow \chi) \rightarrow (\varphi \rightarrow \chi)$$
$$\varphi \rightarrow \psi \rightarrow \varphi \wedge \psi$$
$$\varphi \wedge \psi \rightarrow \varphi$$
$$\varphi \wedge \psi \rightarrow \psi$$

and 5 more axiom schemes.

Thm: $\mathcal{F}$ is sound and complete.
In fact: $\mathcal{F}$ is implicationally sound and implicationally complete.

Completeness and Soundness:
A formula φ has an $\mathcal{F}$ proof iff it is valid.

Implicational Soundness and Completeness:
There is an $\mathcal{F}$-proof of φ from hypotheses Γ iff $\Gamma \models \varphi$.
In particular, every tautology has an $\mathcal{F}$-proof.

Pf idea:
Soundness: Inferences preserve truth.
Completeness: Formalize the method of truth tables; i.e., try all truth assignments.

More generally, a **Frege system** is specified by any finite complete set of Boolean connectives and finite set of axiom schemes and rule schemes, provided it is implicationally sound and implicationally complete.

Defn: The **size** of a Frege proof is the number of symbols in the proof. $\mathcal{F} \vdash^{m} \varphi$ means φ has an $\mathcal{F}$ proof of size m.
The **size** $|\varphi|$ of a formula φ is the number of symbols in φ.

By completeness, every tautology has an $\mathcal{F}$-proof.
However, the method of truth tables gives exponential size proofs.

Open problem: Is there a polynomial $p(n)$ such that every tautology φ has an $\mathcal{F}$-proof of size $\leq p(n)$, where n is the size of φ.
That is, is $\mathcal{F}$ polynomially bounded?

The answer is the same for all Frege systems, in that any two Frege systems "p-simulate" each other.
[Reckhow'76; Cook-Reckhow'79]

Abstract Proof Systems

Defn: An **abstract proof system** is a polynomial time function f mapping $\{0,1\}^*$ *onto* the set of tautologies.
w is an f-**proof** of φ iff $f(w) = \varphi$.
The **size** of w is $|w|$, i.e. the length of w.

Example: The Frege system $\mathcal{F}$ as an abstract proof system:

$$f_{\mathcal{F}}(w) = \begin{cases} \text{the last line of } w & \text{if } w \text{ is an } \mathcal{F}\text{-proof} \\ (x \vee \neg x) & \text{otherwise} \end{cases}$$

Similar constructions allow very strong systems, e.g. ZF set theory, to be abstract proof systems.

Thm. [Cook-Reckhow'79] There is a polynomially bounded abstract proof system iff $\mathrm{NP} = \mathrm{coNP}$.

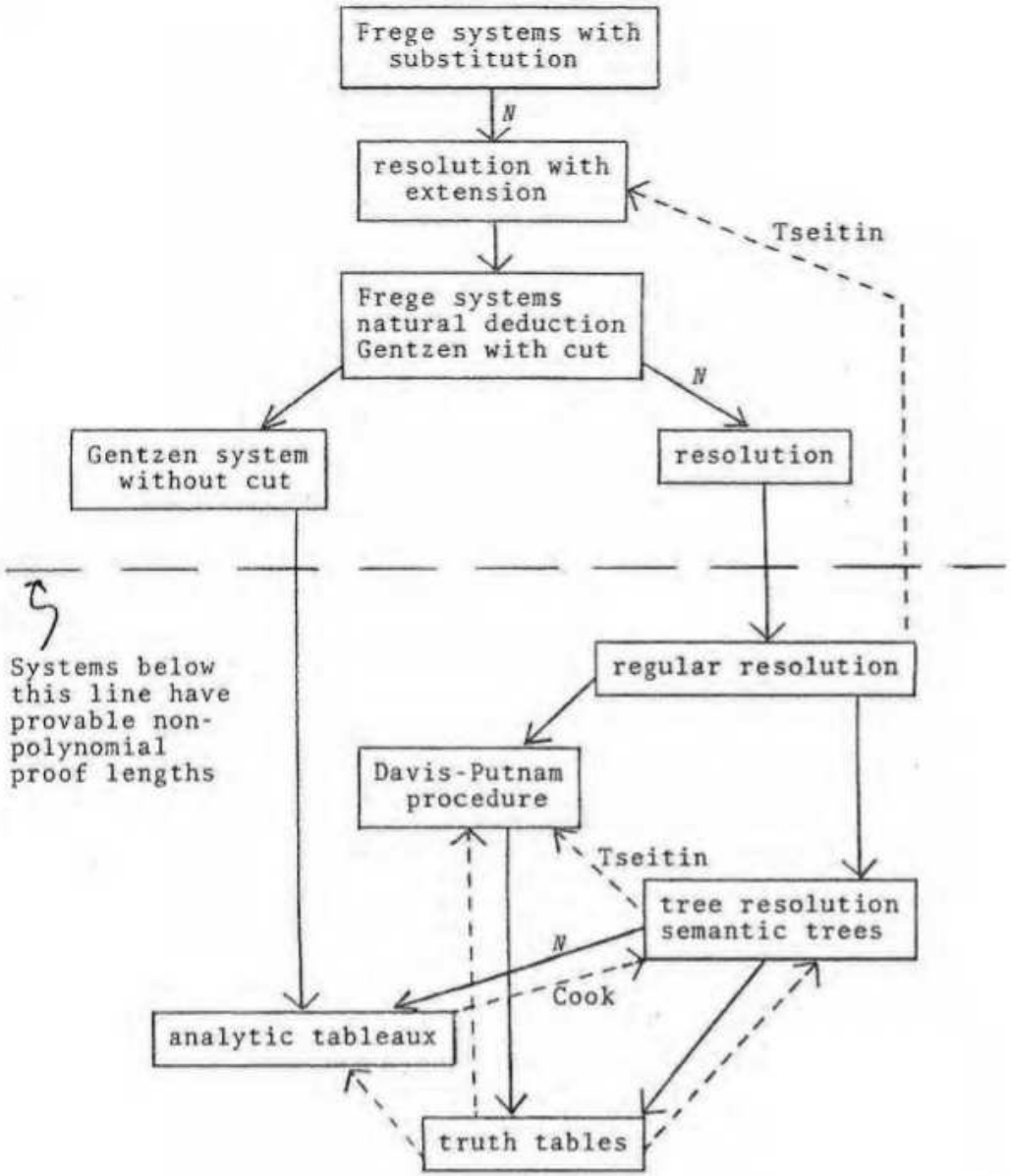
Proof idea: The set of tautologies is coNP-complete.

Defn: Let f, g be abstract proof systems.
f **simulates** g if there is a polynomial $q(n)$ s.t., whenever $g(w) = \varphi$, there is a v, $|v| \leq q(|w|)$ such that $f(v) = \varphi$.
f **p-simulates** g if there is a polynomial-time computable $h(w)$, such that, whenever $g(w) = \varphi$, we have $f(h(w)) = \varphi$.
f is **polynomially bounded** if, for some polynomial $q(n)$, every tautology φ has an f-proof w of size $\leq q(|\varphi|)$.

1. Any two Frege systems p-simulate each other.
2. It is open whether there is an abstract proof system which (p-)simulates all abstract proof systems.

Thm: [Krajíček-Pudlák'98]

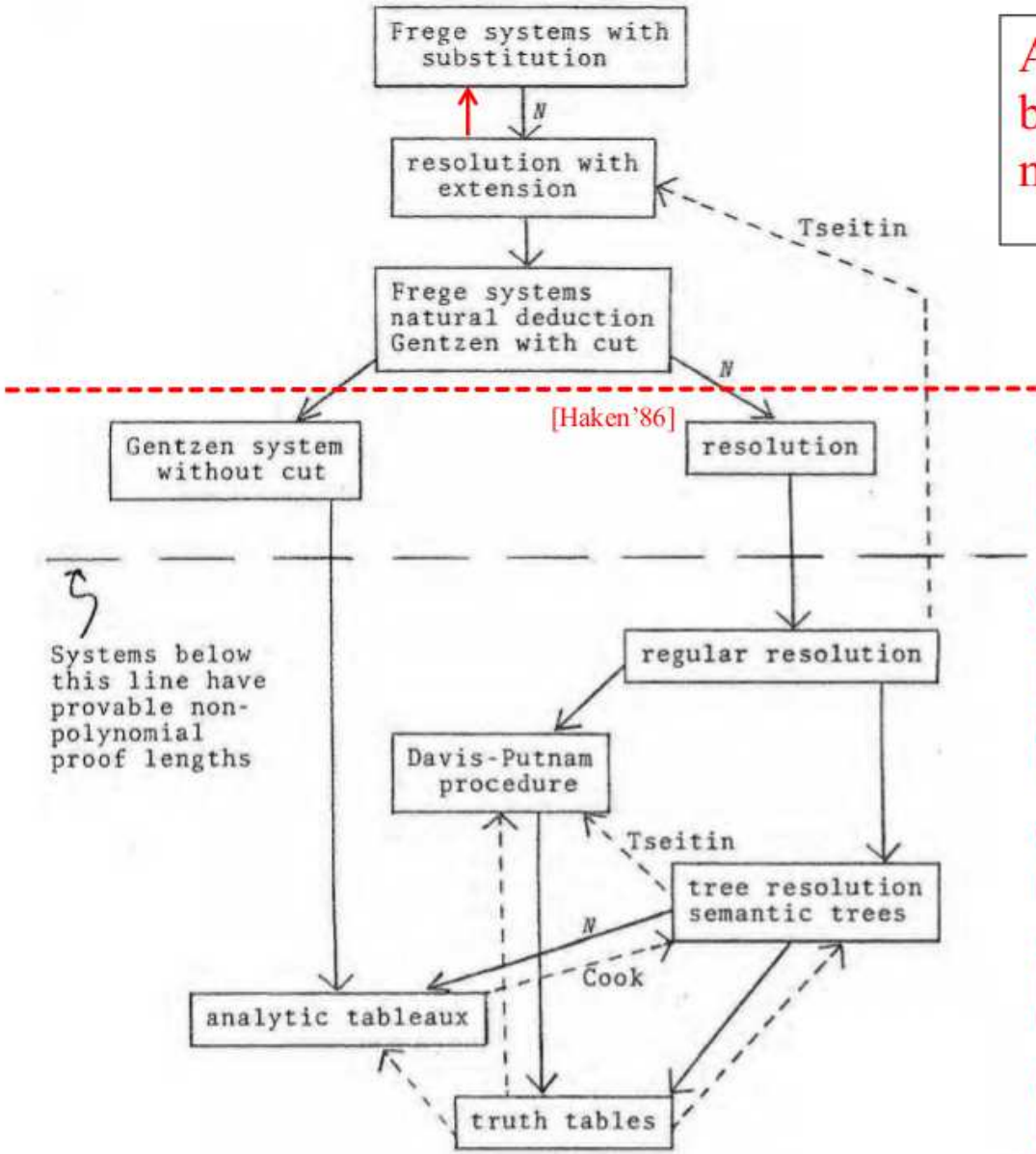
- If EXP=NEXP, there is an abstract proof system which p-simulates every abstract proof system.
- if NEXP=coNEXP, there is a abstract proof system which simulates every abstract proof system.



R.A. Reckhow, PhD thesis, 1975

Cook's Program: Prove NP≠coNP by proving there is no polynomially bounded propositional proof system.

As of 1975: Systems above the line were not known to not be polynomially bounded.



R.A. Reckhow, PhD thesis, 1975

As of 2015, proof systems below the line are known to not be polynomially bounded:

Constant-depth (AC^0) Frege
[Ajtai'88; Pitassi-Beame-Impagliazzo'93; Krajicek-Pudlak-Woods'95]

Constant-depth Frege with counting mod m axioms
[Ajtai'94; Beame-Impagliazzo-Krajicek-Pitassi-Pudlak'96; B-Impagliazzo-Krajicek-Pudlak-Razborov-Sgall'96; Grigoriev'98]

Cutting Planes
[Pudlak'97]

Nullstellensatz
[B-Impagliazzo-Krajicek-Pudlak-Razborov-Sgall'96; Grigoriev'98]

Polynomial calculus
[Razborov'98; Impagliazzo-Pudlak-Sgall'99; Ben-Sasson-Impagliazzo'99; B-Grigoriev-Impagliazzo-Pitassi'96; B-Impagliazzo-Krajicek-Pudlak-Razborov-Sgall'96; Alekhnovich-Razborov'01]

Critique of "simulation" between proof systems

Notions such as "p-simulate" and "simulate" can compare the strength of proof systems, but suffer from the fact they do not account for the difficulty of searching for proofs.

- The difficulty of **proof search** often turns out to be more important than lengths of proofs.
- It is often preferable to search for proofs in a weaker system that admits effective search procedures.

A prime example of this is resolution, and its subsystems, which we discuss next.

Resolution

Resolution is a refutation system, refuting sets of clauses. Thus, resolution is a system for refuting CNF formulas, equivalently, a system for proving DNF formulas are tautologies.

- A literal is a variable x or a negated variable $\overline{x}$.
- A *clause* is a set of literals, interpreted as their disjunction
- A set Γ of clauses is a CNF formula
- Resolution rule: $$\frac{x, C \qquad \overline{x}, D}{C \cup D}$$
- A **resolution refutation** of Γ is a derivation of the empty clause from clauses in Γ.
- This allows resolution to be a proof system for DNF formulas.

Thm: Resolution is sound and complete (for CNF refutations)

Proof idea: (For completeness.) Use the Davis-Putnam ['60] procedure. Choose one variable x, do all possible resolution inferences using x and $\overline{x}$; discard the clauses containing x and $\overline{x}$; and iterate.

Thm: (Completeness for resolution derivations.) If $\Gamma \models C$, there is a clause $D \subseteq C$ such that there is a resolution derivation of D from Γ.

This is can also be proved via the Davis-Putnam procedure.

Regular resolution

A resolution derivation can be viewed as a sequence of clauses, each clause is either

- A hypothesis (an "input clause"), or
- Inferred by resolution from earlier clauses.

Defn: [Tseitin'68] A resolution refutation is **regular** if, viewing the refutation as a dag, there is no path in the dag on which the same variable is resolved on more than once.

Thm: Regular resolution is complete.

Pf: The Davis-Putnam procedure yields a regular refutation.

Thm: [Alekhnovich, Johannsen, Pitassi, Urquhart'02]
Regular resolution does not simulate resolution.

Resolution as an abstract proof system — extension

Defn: Extension rule for resolution ([Tseitin '68]): For x and y literals, and letting z be a *new* variable, introduce $z \leftrightarrow (x \wedge y)$ by adding the clauses:

$$\{\overline{x}, \overline{y}, z\} \qquad \{\overline{z}, x\} \qquad \{\overline{z}, y\}.$$

(A similar construction works for $x \vee y$.)

Resolution as an abstract proof system: Given φ, introduce clauses Γ for the extension variables z_ψ for all subformulas ψ of φ.

The set of clauses $\overline{z}_\varphi, \Gamma$ expresses the *negation* of φ.

A **resolution proof** of φ is a **resolution refutation** of $\overline{z}_\varphi, \Gamma$.

Extended resolution and Extended Frege systems

Defn: The proof system **extended resolution** is resolution augmented with unrestricted use of the extension rule (not just extension for subformulas of the formula φ to be proved).

Defn: Extension for the Frege system $\mathcal{F}$ allows introduction of new variables for formulas; namely the **extension rule**:

$$z \leftrightarrow \varphi$$

where z is a "new" variable, i.e., not appearing in earlier lines the proof, in φ, or in the last line of the proof.
The **extended Frege system ($e\mathcal{F}$)** is Frege ($\mathcal{F}$) plus the extension rule.

Thm: Extended resolution and extended Frege p-simulate each other.

Recall proof size $\vdash^{m}$ is measured in terms of symbols.
We can also measure proof size in terms of numbers of inference steps, denoted $\vdash^{m \text{ steps}}$.

Thm. [Statman'77] If $\mathcal{F} \vdash^{m \text{ steps}} \varphi$, then φ has a $e\mathcal{F}$-proof of size $O(m + |\varphi|^2)$, that is $e\mathcal{F} \vdash^{O(m+|\varphi|^2)} \varphi$.

In other words: the *size* of extended Frege proofs is essentially the same as the *number of lines* in Frege proofs.

Proof idea: Introduce extension variables for the formulas in the Frege proof; thereby reduce all lines to constant size with only a linear increase in the number of lines in the $e\mathcal{F}$-proof. □

Using extension allows succinct representation of Boolean circuits C, by introducing an extension variable for each gate in C. Thus, in effect:

- A Frege proof is a proof in which each line is a Boolean *formula*.
- An extended Frege proof is a proof in which each line is a Boolean *circuit*.

It is widely conjectured that Boolean circuits cannot be converted into polynomial size equivalent Boolean formulas; the analogous conjecture for proof systems is that $\mathcal{F}$ does not (p-)simulate $e\mathcal{F}$. [Cook-Reckhow'79]

There is no known direct connection between these conjectures:

- Formulas might polynomially represent circuits, yet this might not be provable with $\mathcal{F}$ proofs.
- Conversely, $\mathcal{F}$ might simulate $e\mathcal{F}$ by some other means.

State of the art:

1. Any two Frege systems p-simulate each other.
2. Any two $e\mathcal{F}$ systems p-simulate each other.
3. Extended Frege systems p-simulate Frege systems.
4. It is open whether $\mathcal{F}$ simulates $e\mathcal{F}$.
5. It is open whether $\mathcal{F}$ or even $e\mathcal{F}$ is polynomially bounded.
6. Extended resolution and $e\mathcal{F}$ systems p-simulate each other.
7. Frege systems p-simulate resolution.
8. Resolution does not simulate $\mathcal{F}$.
9. Regular resolution does not simulate resolution.

Part B. of these talks will discuss what is known about separating resolution, Frege and extended Frege systems.
Part C. will discuss resolution and CDCL proof search.
Part D. will discuss cutting planes, algebraic proofs, and automatizability (proof search).

End of part A!

Some survey articles:

- S. Buss, J. Nordström, "Proof Complexity", In Handbook of Satisfiability, 2021.
- S. Buss, "Towards NP-P via Proof Complexity and Search", Annals of Pure and Applied Logic 163, 7 (2012) 906-917.
- S. Buss, "Propositional Proof Complexity: An Introduction", In Computational Logic, edited by U. Berger and H. Schwichtenberg, Springer-Verlag, Berlin, 1999, pp. 127-178.
- P. Beame and T. Pitassi, "Propositional Proof Complexity: Past, Present and Future", In Current Trends in Theoretical Computer Science Entering the 21st Century, World Scientific, 2001, pp. 42-70.
- P. Beame with A. Sabharwal, "Propositional Proof Complexity", In Computational Complexity Theory, IAS/Park City Clay Mathematics Series 10, 2000, pp. 199-246.
- P. Pudlák, "Twelve problems in proof complexity", In Proc. 3rd International Computer Science Symposium in Russia, CSR 2008, pp.13-27
- N.Segerlind, "The Complexity of Propositional Proofs", Bulletin of Symbolic Logic 13 (2007) 417-481.