Proof Complexity

Jan Krajíček

Charles University

References:

can be found in a draft of my forthcoming book

Proof Complexity

available at:

`http://www.karlin.mff.cuni.cz/~krajicek`

The final complete manuscript will be there by the end of May.

Proof:

- mathematical
- in propositional logic
- formal

Complexity:

- How hard it is to verify the proof?
- Who is the verifier?

Verifier:

- no creative input
- modelled by a *Turing machine* Q
- inputs: α (the formula) and π (the proof)
- output $Q(\alpha, \pi)$: 1 (accept) or 0 (reject)

The complexity of π:

- *the time Q needs to compute $V(\alpha, \pi)$*

- mathematical set-up:
  formulas, proofs, ... are all represented by strings over a finite alphabet

  - $\{0,1\}^*$: the set of finite binary strings

  - $|\alpha|$ = the size of α = the length of the string representing α

  - atom p_n represented e.g. by string $p1\ldots1$

A useful technical shift:

- *demand that Q runs in polynomial time* (i.e. the number of steps is $poly(|\alpha|, |\pi|)$)

- if the original Q runs in time t then we can pad the original proof π to

$$\pi' \ := \ \pi \ b \ldots b$$

b is t-times, and define new p-time Q' operating as follows:

read from π' just π and then work as Q

I.e.: time becomes proof length.

Definition: [Cook-Reckhow]

A propositional proof system
is a binary relation $Q(x, y)$ such that:

- Q is p-time decidable
- $\forall \alpha \in$ TAUT $\exists \pi \; Q(\alpha, \pi) = 1$
  [the *completeness*]
- $\forall \alpha, \pi \; Q(\alpha, \pi) = 1 \rightarrow \alpha \in$ TAUT
  [the *soundness*]

Example: a Frege system

- *the language:* $\{\neg, \rightarrow\}$

- *one inference rule:* modus ponens

- *three axiom schemes*:

  - $p \rightarrow (q \rightarrow p)$,

  - $[p \rightarrow (q \rightarrow r)] \rightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$,

  - $(\neg p \rightarrow \neg q) \rightarrow [(\neg p \rightarrow q) \rightarrow p]$.

Main problem:

Is there a proof system in which all tautologies have polynomial size proofs?

- p-size: $|\pi| \leq poly(|\alpha|)$
- a p-bounded proof system

Complexity classes:

$\mathcal{P}$: *p-time decidable problems*

Ex.: Is α a formula?

$\mathcal{NP}$: *properties easy to prove* (in p-size)

Ex.: Is α satisfiable?

$co\mathcal{NP}$: *properties easy to refute*

Ex.: Is α a tautology?

Fundamental problem:

$$\mathcal{P} = \mathcal{NP} \ ?$$

Hilbert's **Entscheidungsproblem**:

Can the logical validity of a first-order formula be decided by an algorithm?

[Church and Turing : NO]

Replacing *first-order* by propositional and asking for p-time algorithm the problem becomes equivalent to the $\mathcal{P} =_? \mathcal{NP}$ problem.

Theorem [Cook-Reckhow]

There exists a p-bounded proof system iff the class $\mathcal{NP}$ is closed under complementation.

Corollary

If no p-bounded proof system exists then $\mathcal{P} \neq \mathcal{NP}$.

Hence we want to show that no p-bounded proof system exists.

- a literal: p or $\neg p$

- a clause: a disjunction of literals

$$C : \ell_1 \wedge \ldots \wedge \ell_w$$

- a term: a conjunction of literals

$$D : \ell_1 \wedge \ldots \wedge \ell_w$$

CNF formulas: $C_1 \wedge \ldots \wedge C_t$

limited extension: a way how to attach to a formula β a CNF formula $CNF(\beta)$ such that:

$$\beta \in \mathsf{SAT} \Leftrightarrow CNF(\beta) \in \mathsf{SAT}$$

Observation: $\alpha \in \mathsf{TAUT} \Leftrightarrow \neg\alpha \notin \mathsf{SAT}$

A technical maneuver:

- *instead of proving that α is a tautology we shall prove that $\neg\alpha$ is not satisfiable*, and

- *for that we shall refute the set of clauses $C_1, \ldots, C_t$ forming $CNF(\neg\alpha)$.*

We look at the system

$$C_i = \text{true} \ , \quad \text{for all } i \leq t$$

as a system of logical equations and we want to show it has no solution.

Algebraic proof systems:

- atom p_i is though of as a variable p_i,
- literal $\neg p_i$ by $1 - p_i$,
- replace *logical equation*

$$C \ : \ \ell_1 \vee \ldots \vee \ell_w = \text{true}$$

by *polynomial equation*

$$f \ : \ (1 - \ell_1) \cdot \ldots \cdot (1 - \ell_w) = 0$$

axioms:

- Boolean: $x_i^2 - x_i = 0$, for all $i \leq n$

- initial equations from clauses:

$$f_i = 0 \ , \quad \text{for all} \quad i \leq t$$

rules:

$$\frac{g_1 \quad g_2}{g_1 + g_2}$$

$$\frac{g}{gh} \ , \ h \text{ any polynomial}$$

Hilbert's Nullstellensatz:

The system $f_i = 0$, $i \leq t$, *has no* 0-1 *solution iff one can derive the constant* 1.

A technical issue:
how to represent polynomials so that their equality can be feasibly recognized?

Geometric proof systems:

represent the logical equation

$$C \ : \ \ell_1 \vee \ldots \vee \ell_w = \text{true}$$

by *integer linear inequality*

$$L \ : \ \ell_1 + \ldots + \ell_w \geq 1$$

axioms:

- Boolean: $x_i \geq 0$ and $-x_i \geq -1$, for all $i \leq n$

- initial inequalities from clauses:

$$L_i \geq 1 \ , \quad \text{for all } i \leq t$$

rules:

$$\frac{L_1 \geq a_1 \quad L_2 \geq a_2}{L_1 + L_2 \geq a_1 + a_2}$$

$$\frac{L \geq b}{cL \geq cb} \ , \ c \geq 1 \text{ integer}$$

$$\frac{L \geq b}{\frac{L}{c} \geq \lceil b/c \rceil}$$

$c \geq 1$ integer dividing all coefficients in L

This is the cutting planes proof system.

Completeness: Chvátal - Gomory cuts

Another algorithm for integer linear programming is by Lovász - Schrijver.

A logical refutation system: resolution

Only one rule:

$$\frac{E \vee p \qquad F \vee \neg p}{E \vee F}$$

Theorem:
Resolution is sound and complete.

[It is the basis of many SAT solving algorithms.]

A SAT solving algorithm M:

- *input*: a set of clauses

- *output*: either a satisfying assignment or the declaration UNSAT

Interpret M is a proof system Q by:

$Q(\alpha, \pi) = 1$ *holds iff* π *is the run of* M *on* $CNF(\neg\alpha)$ *ending with UNSAT*.

Ex. hard formula: the pigeon-hole principle

- fix $n \geq 1$ and the set $[n] := \{1, \ldots, n\}$

- atoms p_{ij}, for $i \in [n+1]$ and $j \in [n]$

- meaning: $p_{ij} = 1$ iff *pigeon i sits in hole j*

- $\neg PHP_n$ is the set of clauses:

  - $\bigvee_j p_{ij}$, for all i

  - $\neg p_{iu} \vee \neg p_{iv}$, for all i and all $u \neq v$

  - $\neg p_{aj} \vee \neg p_{bj}$, for all $a \neq b$ and j

Feasible interpolation:

- two sets of clauses $A_i(\overline{p}, \overline{q})$ and $B_j(\overline{p}, \overline{r})$ together unsatisfiable

- $\overline{p} = (p_1, \ldots, p_n)$ and the three tuples of atoms are disjoint

Two subsets $U, V \subseteq \{0,1\}^n$:

$$U := \{\overline{a} \in \{0,1\}^n \mid \bigwedge_i A_i(\overline{a}, \overline{q}) \in \mathsf{SAT}\}$$

$$V := \{\overline{a} \in \{0,1\}^n \mid \bigwedge_j B_j(\overline{a}, \overline{r}) \in \mathsf{SAT}\}$$

A_i, B_j unsatisfiable

$$\Updownarrow$$

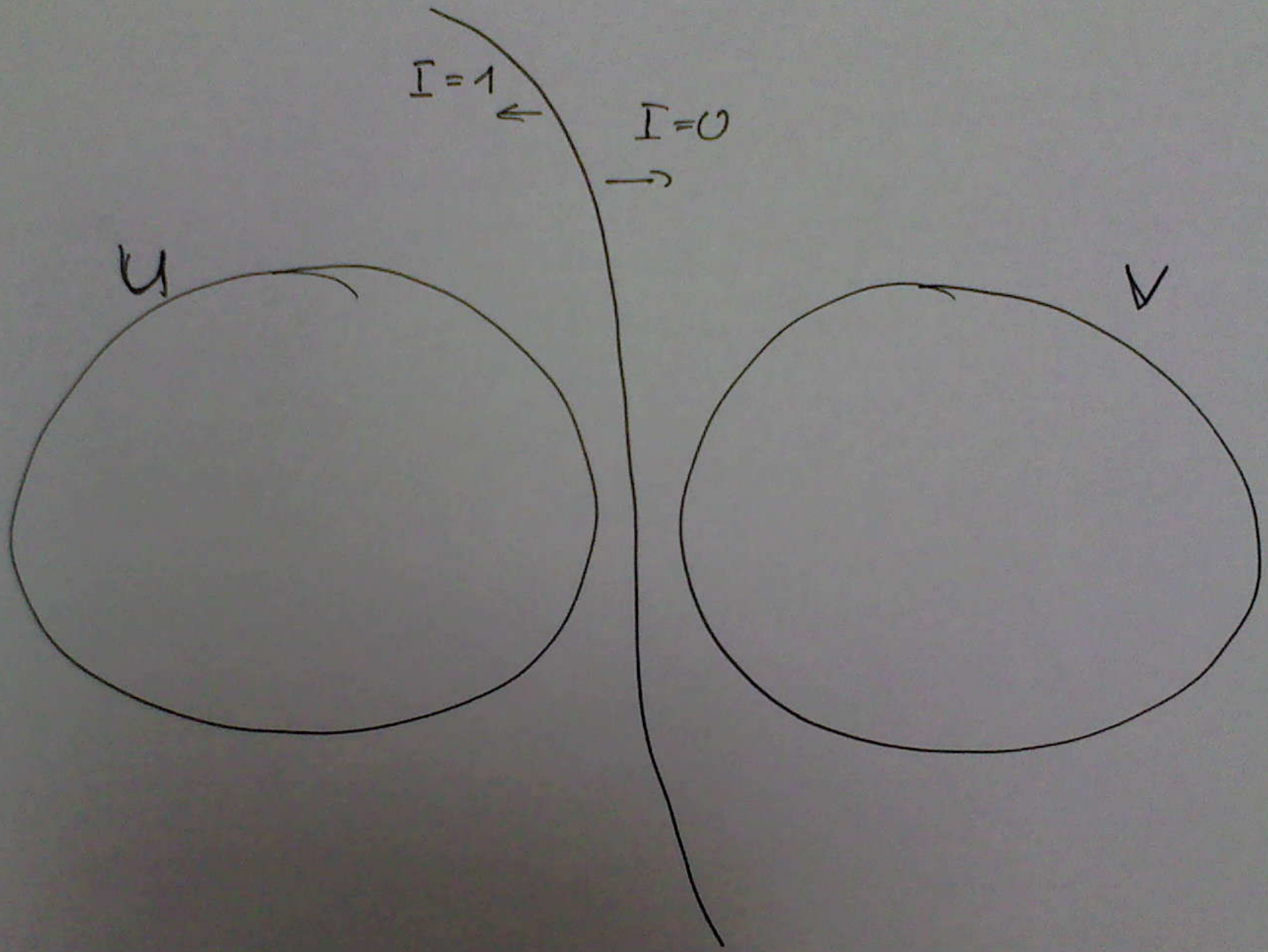
(1) $\quad \bigwedge_i A_i(\overline{p}, \overline{q}) \;\rightarrow\; \neg \bigwedge_j B_j(\overline{p}, \overline{r}) \in \mathsf{TAUT}$

$$\Updownarrow$$

$$U \cap V = \emptyset$$

$$\Updownarrow$$

any interpolant $I(\overline{p})$ of (1) defines a set $\{\overline{a} \mid I(\overline{a}) = 1\}$ separating U from V


I = 1
I = 0
U
V

Definition

A proof system Q has feasible interpolation iff whenever A_i, B_j can be refuted in Q in size s then there is a Boolean circuit $C(\overline{p})$ of size $\leq poly(s)$ separating U from V.

A Boolean circuit with inputs $x_1, \ldots, x_n$ is a sequence of instructions:

$$y_1, y_2, \ldots, y_t$$

where each y_k is computed from

$$0, 1, x_1, \ldots, x_n, y_1, \ldots, y_{k-1}$$

by $\neg, \vee$ or $\wedge$.

Applications:

If U/V are hard to separate then A_i, B_j are hard to refute in Q.

Monotone version:

- U closed upwards
- C is monotone (no $\neg$)

We have no non-trivial lower bounds for general circuits but for monotone circuits strong lower bounds are known.

RSA pair

RSA encryption method

$$E \ : \ \overline{b} \in \{0,1\}^n \to E(\overline{b}) \in \{0,1\}^n$$

$$U := \{\overline{a} \in \{0,1\}^n \mid \exists \overline{b} \ E(\overline{b}) = \overline{a} \wedge b_n = 0\}$$

$$V := \{\overline{a} \in \{0,1\}^n \mid \exists \overline{b} \ E(\overline{b}) = \overline{a} \wedge b_n = 1\}$$

Fact: If RSA is secure then U/V are hard to separate.

$Clique$ - $Color$ pair

$Clique$:
the set of graphs on $[n]$ *which have a clique of size* k

It is closed upwards: adding more edges does not destroy a clique

$Color$:
the set of graphs on $[n]$ *which are* $(k-1)$*-colorable*

Win-win situation:

- If Q has feasible interpolation
  then we got lower bounds (unconditional or conditional).

- If Q does not have feasible interpolation
  then it is possible to derive a time lower bound for any algorithm searching for Q-proofs.

Key word: *automatizability*.

Remark:

It is possible (but unlikely) that a Frege system is p-bounded: we have only quadratic lower bound at present.

But **assuming** that no p-bounded proof system exists (i.e. that $\mathcal{NP} \neq co\mathcal{NP}$) we may ask if there is an optimal proof system P:

- *no other proof system Q has more than a polynomial speed-up over P:*

$$\text{minsize}_P(\alpha) \ \leq \ poly(\text{minsize}_Q(\alpha))$$

Quantitative Gödel's theorem:

S: a finite consistent extension of Robinson's arithmetic

$Con_S(x)$: formalizes that *"there is no proof of contradiction in S of size $\leq x$"*

dyadic numerals $\underline{n}$:

$$\underline{0} := 0 \quad \text{and} \quad \underline{1} := 1$$

$$\underline{2n} := (1+1) \cdot \underline{n} \quad \text{and} \quad \underline{2n+1} := \underline{2n} + 1$$

Note: the size of $Con_S(\underline{n})$ is $\approx \log n$.

Theorem [H.Friedman, P.Pudlák]

There are $\epsilon > 0$ *and* $c \geq 1$ *such that:*

- $S \not\vdash_{n^{\epsilon}} Con_S(\underline{n})$.
- $S \vdash_{n^{c}} Con_S(\underline{n})$.

Problem:

Is there a fixed theory S_0 such that for all S it holds:

$$S_0 \vdash_{n^{c}} Con_S(\underline{n}) \ ?$$

Theorem [J.K. - P.Pudlák]

An optimal proof system exists iff there is a theory S_0 proving statements $Con_S(\underline{n})$ for all S in size $poly(n)$.

In order to use this to disprove the existence of an optimal proof system we would need, it seems, a new proof of Gödel's theorem.

Problem:

Can we prove that Robinson's arithmetic does not prove Con_{GB} by a proof that is significantly different from the proof that GB does not prove it?

Hilbert's canceled 24th problem:

The 24th problem in my Paris lecture was to be:
Criteria of simplicity, or proof of the greatest simplicity of certain proofs. Develop a theory of the method of proof in mathematics in general. Under a given set of conditions there can be but one simplest proof. Quite generally, if there are two proofs for a theorem, you must keep going until you have derived each from the other, or until it becomes quite evident what variant conditions (and aids) have been used in the two proofs. Given two routes, it is not right to take either of these two or to look for a third; it is necessary to investigate the area lying between the two routes.

Hilbert's Twenty-Fourth Problem

Rüdiger Thiele

1. INTRODUCTION. For geometers, Hilbert's influential work on the foundations of geometry is important. For analysts, Hilbert's theory of integral equations is just as important. But the address "Mathematische Probleme" [**37**] that David Hilbert (1862–1943) delivered at the second International Congress of Mathematicians (ICM) in Paris has tremendous importance for all mathematicians. Moreover, a substantial part of Hilbert's fame rests on this address from 1900 (the year after the American Mathematical Society began to publish its *Transactions*). It was by the rapid publication of Hilbert's paper [**37**] that the importance of the problems became quite clear, and it was the American Mathematical Society that very quickly supplied English-language readers with both a report on and a translation of Hilbert's address. (In Paris, the United States and England were represented by seventeen and seven participants, respectively.)

Indeed, this collection of twenty-three unsolved problems, in which Hilbert tried "to lift the veil behind which the future lies hidden" [**37**, p. 437] has occupied much attention since that time, with many mathematicians watching each contribution attentively and directing their research accordingly. Hermann Weyl (1885–1955) once remarked that "We mathematicians have often measured our progress by checking which of Hilbert's questions had been settled in the meantime" [**110**, p. 525]. (See also [**31**] and [**115**].)

Hilbert and his twenty-three problems have become proverbial. As a matter of fact, however, because of time constraints Hilbert presented *only* ten of the problems at the Congress. Charlotte Angas Scott (1858–1931) reported on the Congress and Hilbert's presentation of ten problems in the *Bulletin of the American Mathematical Society* [**91**]. The complete list of twenty-three problems only appeared in the journal *Göttinger Nachrichten* in the fall of 1900 [**37**], and Mary Winston Newson (1869–1959) translated the paper into English for the *Bulletin* in 1901 [**37**]. Already by September 1900, George Bruce Halsted (1853–1922) had written in this MONTHLY that Hilbert's beautiful paper on the problems of mathematics "is epoch-making for the history of mathematics" [**34**, p. 188]. In his report on the International Congress, Halsted devoted about forty of the article's eighty lines to the problems. As to the actual speech, no manuscript was preserved, nor was the text itself ever published.

Recently, Ivor Grattan-Guinness presented an interesting overview of Hilbert's problems in the *Notices of the American Mathematical Society*, discussing the form in which each of the twenty-three problems was published [**30**]. Yet, in dealing with the celebrated problems from this viewpoint, he failed to mention the most interesting problem of Hilbert's collection: the canceled twenty-fourth. Hilbert included it neither in his address nor in any printed version, nor did he communicate it to his friends Adolf Hurwitz (1859–1919) and Hermann Minkowski (1864–1909), who were proofreaders of the paper submitted to the *Göttinger Nachrichten* and, more significantly, were direct participants in the developments surrounding Hilbert's ICM lecture.

So, for a century now, the twenty-fourth problem has been a Sleeping Beauty. This article will try to awaken it, thus giving the reader the chance to be the latter-day Prince (or Princess) Charming who can take it home and solve it. This paper also aims to convince the reader of the utility of the history of mathematics in the sense to which