Model Theory and Proof Complexity

Jan Krajíček

Charles University

Complexity theory: fundamental problems open

P vs. NP

Propositional Entscheidungsproblem: Is there a p-time algorithm recognizing propositional tautologies?
[Conj.: NO]

P vs. BPP

Universal derandomization: Can randomization be removed from p-time algorithms?
[Conj.: YES]

One-way functions

Is factoring (discrete log, ...) hard? Does there exist a pseudo-random number generator?
[Conj.: YES]

Proof complexity

NP vs. coNP

Length of propositional proofs: Is there a proof system in which every tautology has a p-size proof?

Proof system [Cook-Reckhow]:

- $Q(x, y)$ p-time relation
- $\varphi \in TAUT$ iff $\exists w\ Q(\varphi, w)$
- p-size proofs: $|w| \leq |\varphi|^{const}$

[Conj.: NO $>$ YES]

Finite structures

Corollary of Fagin's thm

NP $=$ coNP iff $\Sigma^1_1 = \Pi^1_1$ on finite structures.

- generally: relational language with constants,
- for simplicity of notation: just one relation $([n], R)$, $R \subseteq [n]^c$,
- $[n] := \{1, \ldots, n\}$.

Want:
An infinite class $\mathcal{C}$ of structures definable by a Π^1_1 sentence $\forall X \alpha(X)$ that is not definable by any Σ^1_1 condition $\exists Y \beta(Y)$.

- X, Y are variables for relations of different arities.

Candidate classes

Non-3-colorability

Graphs $\mathbf{G} = ([n], E)$ that cannot be colored by 3 colors.

CSP

Pair of structures $\mathbf{A}$ and $\mathbf{B}$ such that $\mathbf{A}$ cannot be homomorphically mapped into $\mathbf{B}$. ($\mathbf{B}$ can be suitably fixed.)

TAUT

Structures $\mathbf{A} = ([n], R)$ encoding formulas (e.g. in DNF) that are tautologies.

Ex.: Systems of equations

Unsolvable polynomial systems

A system of polynomial equations EQ over the 2-element field $\mathbf{F}_2$ that has no solution in the field.

Set-up:

- constant c and parameter $n \geq 1$,
- variables x_i indexed by $\leq c$-tuples i from $[n]$,
- degree $\leq c$ polynomials f_j over $\mathbf{F}_2$ indexed by $\leq c$-tuples j from $[n]$,
- monomials represented by $\leq c^2$ tuples and the whole system EQ_n by a $\leq c^3$-ary relation.

Π^1_1-definition

Base structure: $\mathbf{A}_n = ([n], R_n)$, with R_n including EQ_n (and maybe some other structure).

- 0-1 assignment to variables $\Leftrightarrow$ subsets $U \subseteq [n]^c$,
- a witness to U solving all $f_j = 0$: $V \subseteq [n]^c \times ([n]^{c^2} \times [n]^{c^2})$ such that
  - for all j, $V(j, \_)$ is a total 2-partition of the monomials of f_j that are non-zero under U.

A suitable Π^1_1-definition $\forall X \alpha(X)$ over $\mathbf{A}_n$ says:

for no U, no V is a witness that U solves EQ_n.

(with $X = (U, V)$).

Pseudofinite structure

Starting with a sequence for $n \geq 1$:

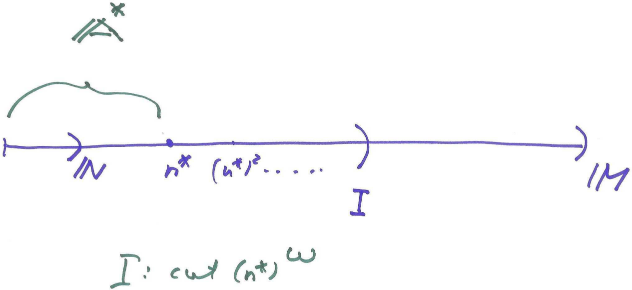
$$\ldots \ , \ \mathbf{A}_n \ , \ \ldots$$

$\downarrow\downarrow\downarrow$ ultraproduct, overspill in a non-standard model, ... $\downarrow\downarrow\downarrow$

pseudofinite $\mathbf{A}^* = ([n^*], R^*)$

- n^* is a non-standard element of a model $\mathbf{M}$ of true arithmetic,
- in $\mathbf{M}$ it holds that $\mathbf{A}^* \models \forall X \alpha(X)$.

Basic picture



Basic question

Assume we expand $\mathbf{A}^*$ by a witness W to $\neg\alpha$:

$$\mathbf{B} = (\mathbf{A}^*, W) \models \neg\alpha(W) ,$$

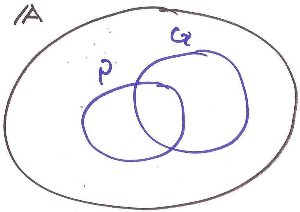
where

- W encodes an assignment U and a witness V that it solves all $f_j = 0$.

Question

What else must $\mathbf{B}$ satisfy in order to imply that a specific Σ^1_1 condition $\exists Y \beta(Y)$ does not define the class of all $\mathbf{A}_n$, $n \geq 1$?

PHP example



$0 < |P| < |Q|$

$\Updownarrow$

no $f: Q \to P$ is 1-to-1

$\Updownarrow$

$\exists g: P \xrightarrow[\text{1-to-1}]{} \mathrm{rng}(P) \subsetneq Q$

D

Assuming 1-to-1 f $\Rightarrow$ violating $\boxed{PHP}$ by $g \circ f$

soundness of

Soundness

We want to keep the soundness of $\exists Y \beta(Y)$:

$$\mathbf{B} \models \forall X, Y\ \beta(Y) \to \alpha(X)\ .$$

An argument:
Assume that $\exists Y \beta(Y)$ holds in all $\mathbf{A}_n$, $n \geq 1$, and that a witness to that is a part of R_n. Then it is also a part of R^* and

$$\mathbf{A}^* \models \exists Y \beta(Y) \text{ and thus also } \mathbf{B} \models \exists Y \beta(Y)$$

($\mathbf{A}^* \preceq_R \mathbf{B}$ suffices if a witness for Y is a part of R^*). But if

$$\mathbf{B} \models \neg\alpha(W)$$

we contradict the soundness.

Ex.: Nullstellensatz

NS proofs

System EQ_n is unsolvable iff there are polynomials g_j, h_i over $\mathbf{F}_2$ such that

$$\sum_j g_j f_j \; + \; \sum_i h_i(x_i^2 - x_i) \; = \; 1 \; .$$

- If the degree of all g_j, h_i is bounded by a constant d then the whole tuple of these polynomials can be encoded by a relation S_n (a part of R_n),
- and R^* contains S^*, an NS proof over $[n^*]$.

Arranging soundness of degree $\leq d$ NS-proofs:

- Expand $\mathbf{A}^*$ by a solution U, V to EQ^* such that $\mathbf{B}$ allows to count consistently parities of definable sets - an abstract Euler characteristic.

Ex.: propositional proof

Propositional proofs

$$Y \ : \ \varphi_1 \ , \varphi_2 \ \ \ldots \ , \ \varphi_i \ , \ \ldots \ , \ \varphi_k$$

- φ_k is a propositional formula with atoms for atomic formulas involving X and expressing that $\forall X \alpha(X)$ is true (e.g. EQ_n is unsolvable),
- $\beta(Y)$ says that Y is a correct proof in *propositional calculus*.

Arranging soundness of Y:

- The expansion **B** ought to satisfy the Least Number Principle for statements:

$$\neg Sat(\varphi_i, W) \ .$$

Such first φ_i not satisfied by W violates the soundness of rules or axioms.

Sat formula

- φ_i are of a bounded depth in the DeMorgan language.

  Sat is FO-definable. This case was solved (Ajtai, ...)

- φ_i are arbitrary formulas or even circuits.

  Sat is $\Delta^1_1 := \Sigma^1_1 \cap \Pi^1_1$ -definable. This is a pivotal open problem of proof complexity to establish a lower bound for ordinary propositional calculus: (Extended) Frege system.

- φ_i are of bounded depth but in a language properly extending the DeMorgan one by the parity connective $\bigoplus$.

  Sat is FO definable in logic with the parity quantifier Q_2. This is an enigmatic frontline open problem: Everything seems to be in place for its solution which is elusive (thirty years now!).

Problem summary

Want B such that:

1. $\mathbf{A}^* \preceq \mathbf{B}$
2. $\mathbf{B} \models \neg\alpha(W)$
3. **B** satisfies the LNP for as large class of formulas as possible.

The construction:

B (to be denoted $K(F,G)$)

- will be Boolean-valued, and
- the three condition will be satisfied in the *maximum Boolean value sense*.

Set-up: sample space

$\mathbf{M}$: ambient non-standard $\aleph_1$-saturated model of true arithmetic

Ω: a non-standard finite set, $\Omega \in \mathbf{M}$

$\mathcal{A}$: Boolean algebra of subsets of Ω in $\mathbf{M}$ ($\mathcal{A} \in \mathbf{M}$)

μ: (weighted) counting measure on $\mathcal{A}$

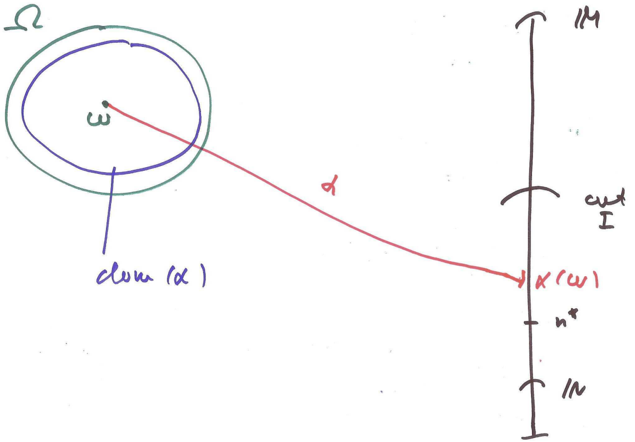
Inf: ideal in $\mathcal{A}$ of sets of infinitesimal μ measure (not definable)

$\mathcal{B}$: the quotient algebra $\mathcal{A}/\mathit{Inf}$

Key fact

$\mathcal{B}$ is complete.

Family F - the FO part of $K(F, G)$



- $[\![\alpha = \beta]\!] := \{\omega \in \Omega \mid \alpha(\omega) = \beta(\omega)\} \ / \ \mathit{Inf}.$

Family G - the SO part of $K(F,G)$

Elements of G (SO objects) are (some) *unary* maps

$$\Gamma \ : \ F \to F$$

(not necessarily definable) satisfying equality axioms: for all $\alpha, \beta \in F$

$$[\![\alpha = \beta]\!] \ \leq \ [\![\Gamma(\alpha) = \Gamma(\beta)]\!] \ .$$

Define

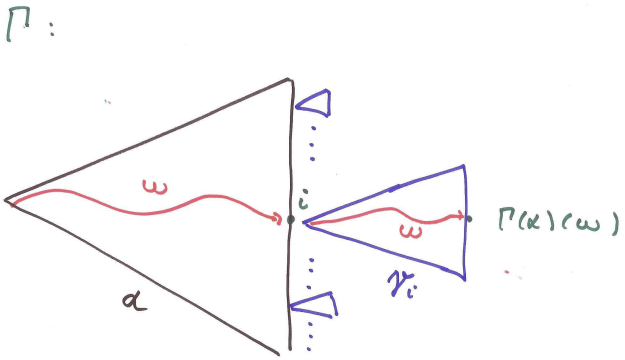
$$[\![\Gamma = \Delta]\!] \ := \ \bigwedge_{\alpha \in F} [\![\Gamma(\alpha) = \Delta(\alpha)]\!] \ .$$

Ex. of G

Γ is given by $(\gamma_i)_{i<m} \in \mathbf{M}$, all $\gamma_i \in F$ and $m \in I$, and

$$\Gamma(\alpha)(\omega) \ := \ \gamma_i(\omega) \ , \quad \text{for} \quad i := \alpha(\omega)$$

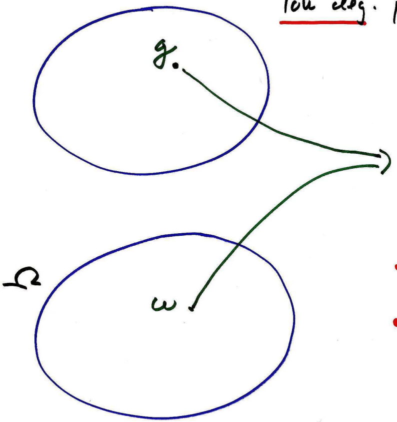
or 0, if $i \geq m$.



Partial evaluations

low deg. poly's : deg $\leq n^{o(1)}$

infinit.



$\omega(g) \in \{0, 1, *\}$

- respects $+, \cdot$
- $\omega(EQ^*) \in \{0, *\}$

F_{alg} and G_{alg}

- α: queries $n^{o(1)}$-times for values of low degree polynomials,
- Γ: as before $(\gamma_0, \ldots, \gamma_{m-1})$.

Key requirement

Every $\alpha \in F$ is defined almost everywhere:

$$\text{Prob}_{\omega \in \Omega}[\alpha(\omega) \ \text{ undefined }] < o(1) \ . \tag{1}$$

Remark: Under a much weaker requirement that the probability is bounded by

$$1 \ - \ \exp((n^*)^{o(1)}) \tag{2}$$

we can choose suitable subfamilies $F' \subseteq F_{alg}$ and $G' \subseteq G_{alg}$ and construct a nonstandard hardcore $\Omega' \subseteq \Omega$ such that (1) holds for $K(F', G')$ and Ω'.

Properties of the model

Lemma

Any $K(F_{alg}, G_{alg})$ satisfies:

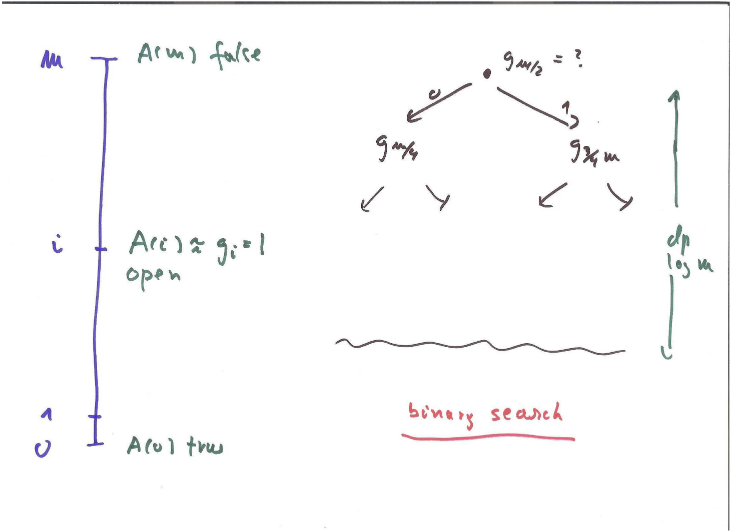
1. *open comprehension,*
2. *open induction,*
3. *interprets the parity quantifier Q_2 in front of open formulas,*
4. *(crucially) quantifier elimination for FO formulas (with parameters).*

Hence 1. - 3. hold for all FO formulas with Q_2, as well as does the LNP.

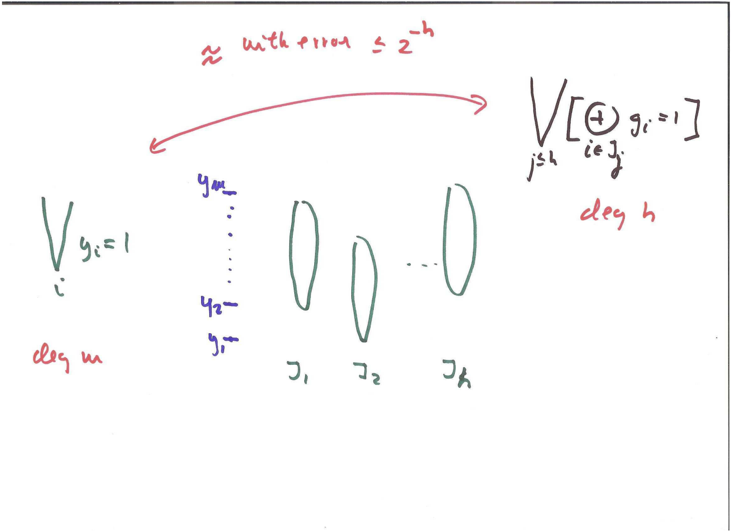
Any $\Leftrightarrow$ *For any partial evaluation satisfying the key requirement ...*

Corollary: Propositional proofs that use bounded depth formulas in the DeMorgan language augmented by $\bigoplus$ are sound in the model.

Induction


m
A(m) false
i
A(i) ≈ g_i = 1
open
1
0
A(0) true
g_{m/2} = ?
0
1
g_{m/4}
g_{3/4 m}
dp
log m
binary search

Q.E.



$\approx$ with error $\le 2^{-h}$
$\bigvee_{j \le h} [\bigoplus_{i \in J_j} y_i = 1]$
deg h
$\bigvee_i y_i = 1$
deg m
y_m
y_2
y_1
J_1
J_2
J_h

A surprising property

Theorem

Any $K(F_{alg}, G_{alg})$ actually satisfies all Π^1_1 consequences of Σ^1_1-induction. In particular, propositional proofs using arbitrary formulas (or even circuits) are sound in the model.

Corollary: If EQ^* can be solved in any $K(F_{alg}, G_{alg})$ then proofs of the unsolvability of EQ_n, $n \geq 1$, in Extended Frege systems require super-polynomial size.

Finitary consequence: If EQ_n and Ω_n are such that no low degree / low depth algebraic trees find with too high probability where $\omega \in \Omega_n$ is undefined then proving unsolvability of EQ_n in EF requires super-poly (exponential, in fact) size.

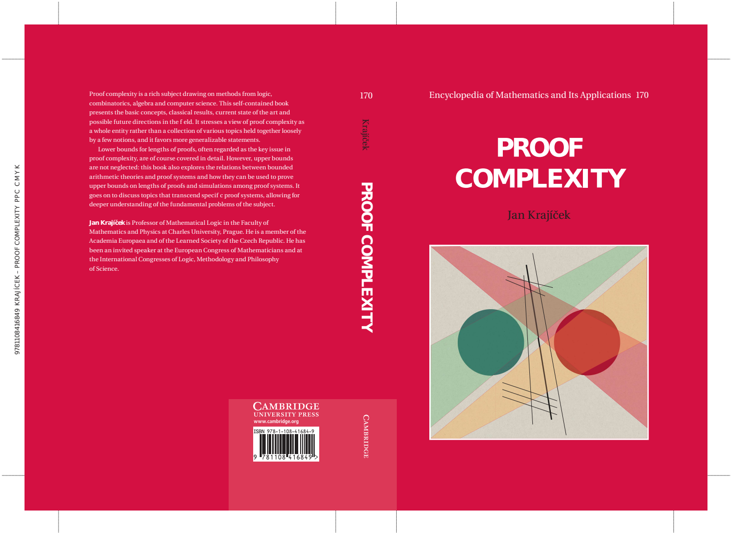
Concluding remarks

1. The statement that each α is defined a.e. says that no low degree/low depth algebraic decision tree can find g for which $\omega(g) = *$ with a large probability.
   This is a computational statement and it would be interesting to find systems EQ_n and partial evaluations Ω_n for which it follows from some *established computational hypothesis*.

   [Candidate systems EQ_n are offered by the theory of proof complexity generators.]

2. Model theory plays a conceptual role: it offers a framework for thinking about lower bounds for strong (or all) proof systems. One can expect that in all applications yielding finitary statements these can be likely proved using finitary means. E.g. the previous *Finitary consequence* has a finitary proof.

General reference



Proof complexity is a rich subject drawing on methods from logic, combinatorics, algebra and computer science. This self-contained book presents the basic concepts, classical results, current state of the art and possible future directions in the f eld. It stresses a view of proof complexity as a whole entity rather than a collection of various topics held together loosely by a few notions, and it favors more generalizable statements.

Lower bounds for lengths of proofs, often regarded as the key issue in proof complexity, are of course covered in detail. However, upper bounds are not neglected: this book also explores the relations between bounded arithmetic theories and proof systems and how they can be used to prove upper bounds on lengths of proofs and simulations among proof systems. It goes on to discuss topics that transcend specif c proof systems, allowing for deeper understanding of the fundamental problems of the subject.

Jan Krajíček is Professor of Mathematical Logic in the Faculty of Mathematics and Physics at Charles University, Prague. He is a member of the Academia Europaea and of the Learned Society of the Czech Republic. He has been an invited speaker at the European Congress of Mathematicians and at the International Congresses of Logic, Methodology and Philosophy of Science.

CAMBRIDGE UNIVERSITY PRESS
www.cambridge.org
ISBN 978-1-108-41684-9

170 Krajíček PROOF COMPLEXITY CAMBRIDGE

Encyclopedia of Mathematics and Its Applications 170

PROOF COMPLEXITY

Jan Krajíček

9781108416849 KRAJÍCEK - PROOF COMPLEXITY PPC C M Y K

Specific reference