Information efficiency of proof systems

Jan Krajíček

Charles University

Simons Institute seminar, 25.March 2021

basics 1

Cook-Reckhow's definition

A propositional proof system (abbreviated pps) is a p-time function whose range is exactly TAUT, the set of propositional tautologies:

$$P \ : \ \{0,1\}^* \rightarrow_{onto} \ \mathrm{TAUT} \ .$$

Fundamental problem

Is NP closed under complementation? Equivalently, is there a pps P such that the length-of-proofs function

$$s_P(\tau) \ := \ \min\{|w| \mid P(w) = \tau\}$$

is bounded by $|\tau|^{O(1)}$?

basics 2

Two pps P and Q can be compared by their proof lengths:

$$P \geq Q \;\Leftrightarrow\; s_P(\tau) \leq s_Q(\tau)^{O(1)}$$

or by the possibility to efficiently translate proofs:

$$P \geq_p Q \;\Leftrightarrow\; \exists \text{ p-time } f \text{ s.t. } \forall w, P(f(w)) = Q(w)\ .$$

(f is a p-simulation of Q by P.)

The optimality problem

Is there a maximal pps w.r.t. $\geq$ or $\geq_p$?
(The former would be called optimal, the latter p-optimal.)

basics 3

NO $\Rightarrow$ NP $\neq$ coNP or P $\neq$ NP, resp.
(in fact, $\Rightarrow$ NE $\neq$ coNE or E $\neq$ NE)

The Optimality problem relates to a number of questions in surprisingly varied areas: structural complexity th. (disjoint NP sets, sparse complete sets, ...), finite model th., quantitative Gödel's thms, games on graphs, etc., and quite a results characterizing the existence of optimal systems are known.

In particular, relative to a theory there is an optimal pps ($\geq$-max w.r.t. to all pps that are provably sound in the theory) and uniformity of pps may be important (there is an optimal pps among pps with advice).

proof search alg's

What about the complexity of searching for propositional proofs?

Proof search problem (informal)

Is there an optimal way to search for propositional proofs?

Definition

A proof search algorithm is a pair (A, P) where P is a pps and A is a deterministic algorithm that stops on all inputs and finds P-proofs for all tautologies:

$$P(A(\tau)) \ = \ \tau$$

for all $\tau \in TAUT$.

no new problem

A natural quasi-ordering:

$$(A, P) \geq_t (B, Q) \;\Leftrightarrow_{df}\; time_A(\tau) \;\leq\; time_B(\tau)^{O(1)} \;.$$

Lemma

For any fixed pps P there is A such that (A, P) is time-optimal among all (B, P), i.e. $\geq_t$-maximal.

Let (A_p, P) denote a proof search algorithm time-optimal for all (B, P).

Theorem

For any sufficiently strong (essentially just containing resolution R) pps P: P is p-optimal iff (A_P, P) is time-optimal among all proof search algorithms (B, Q).

doubts about $\geq_t$

- Is there a way to define a quasi-ordering $\succeq$ of proof search alg's differently so that the problem of optimality *does not reduce* to the p-optimality problem?

- It should be that $\geq_t \subseteq \succeq$, i.e. the comparison by time is the finest.

- But $(A, P) >_t (B, Q)$ may hold just because A remembers one p-time sequence of tautologies (and their P-proofs) that are hard for Q but easy for P.
  Perhaps one ought to compare alg's only on inputs on which *they do something non-trivial*?

- In general, could it be that in some *natural* quasi-ordering $\succeq$ there is an optimal proof search algorithm?

These and other informal questions lead me to the following notion.

information efficiency

Definition

For a pps P, the information efficiency function is defined as:

$$i_P(\tau) \;:=\; \min\{Kt(\pi|\tau) \mid P(\pi) = \tau\} \;.$$

Here Kt is Levin's time-bounded Kolmogorov complexity:

$$Kt(w|u) \;:=\; \min\{|e| + \log t \mid \text{machine } e \text{ computes } w \text{ from } u \text{ in time} \leq t\}$$

For τ, $|\tau| = m$, and for P whose proofs are not shorter than the formula being proved and which allows to simulate efficiently the truth-table proof:

$$\log m \leq \log s_P(\tau) \leq i_P(\tau) \leq m \;.$$

information and time

Lemma 1

Let (A, P) be any proof search algorithm. Then for all $\tau \in TAUT$:

$$i_P(\tau) \leq Kt(A(\tau)|\tau) \leq |A| + \log(time_A(\tau)) \ .$$

In particular, $time_A(\tau) \geq \Omega(2^{i_P(\tau)})$.

Lemma 2 (i-automatizability)

For every proof system P there is an algorithm B such that for all $\tau \in TAUT$:

$$Kt(B(\tau)|\tau) = i_P(\tau)$$

and

$$time_B(\tau) \leq 2^{O(i_P(\tau))} \ .$$

information vs. size

- *Can $i_P(\tau)$ give a better time lower bound than $s_P(\tau)$?*

That is, can we have that

$$i_P(\tau) \;\geq\; \omega(\log s_P(\tau)) \tag{1}$$

holds for infinite set of tautologies of unbounded size?

Observation

(1) can happen for a given pps P iff P is not automatizable.

calculation 1

Denote $m := |\tau|$ and call a quantity

- small or large iff it is $O(\log m)$ or $\omega(\log m)$, resp.,
- and a string simple or complex iff its Kt-complexity is small or large, resp.

Formulas τ that witness (1) must necessarily have only complex P-proofs as

$$i_P(\tau) \leq Kt(\pi|\tau) \leq Kt(\pi)$$

and must have some short proofs, w.l.o.g.

$$s_P(\tau) \leq m^{O(1)} .$$

calculation 2

A convenient way then how to express that τ witnesses (1) is to say that

A criterion

For all P-proofs π of τ:

$$It(\tau : \pi) \ := \ Kt(\pi) - Kt(\pi|\tau) \ \text{ is small } \ .$$

[This quantity, defined by Kolmogorov, was by him interpreted as information that τ conveys about π.]

If we find formulas τ that have short proofs but only complex proofs that are themselves simple then we are done:

$$It(\tau : \pi) \leq Kt(\tau) + \log - \text{terms}$$

and hence it is small.

example

If formulas τ are complex then this inequality does not help. Examples of these formulas can be constructed as follows.

Take $h : \{0,1\}^* \to \{0,1\}^*$ a OWP and $B(x)$ its hard bit predicate.
For $b \in \{0,1\}^m$ and $x = (x_1, \dots, x_m)$ define formula η_b by:

$$h_m(x) = b \to B(x) = B(h^{(-1)}(b)) \ .$$

Theorem (ess. K.-Pudlák'95)

Assume P admits p-size proofs of the injectivity of each h_m. Then formulas η_b have p-size P-proofs and, if h is one-way, $i_P(\eta_b)$ cannot be bounded by $O(\log |\eta_b|) = O(\log m)$.

uses of size lower bounds

A separation of information from size implies that P $\neq$ NP and hence analysis of such flas must necessarily by asymptotic and use some strong hypothesis.

- *Can we treat lower bound for information $i_P(\tau)$ individually for some τ, similarly as size lower bounds are (often) individual?*

Size lower bounds for P are used in proof complexity primarily for three things:

1. No $Q \leq P$ is p-bounded: an instance of NP $\neq$ coNP.
2. It implies time lower bounds for all SAT alg's that are simulated by P; in particular, for all whose soundness has p-size P-proofs: an instance of P $\neq$ NP.
3. It implies independence results for the FO theory T_P attached to P. In particular, P $\neq$ NP is then consistent with T_P.

information is just as useful

But having *only* information lower bounds:

$$i_P(\tau) \;\geq\; \omega(\log |\tau|) \tag{2}$$

is just as good:

1. It implies for all $Q \leq_p P$ that either Q is not p-bounded or P $\neq$ NP. (Uses that $P \geq_p Q \Rightarrow i_P(\tau) \leq O(i_Q(\tau).)$

2. It also implies time lower bounds for SAT alg's (Lemma 1).

3. It also implies independence from T_P (propositional translations are performed by p-time alg's.)

a problem

Hence it makes a good sense to try the following

Problem

Prove an *unconditional* lower bound

$$i_P(\tau) \geq \omega(\log|\tau|))$$

for some proof system P for which no super-polynomial *size lower bounds* are known.

Maybe try first to prove the lower bound for P which we know (unconditionally) is not p-bounded but for formulas τ for which no super-polynomial lower bound for $s_P(\tau)$ is known.

Expect that the i-hard formulas will have long P-proofs.

uniform candidates

reflection formulas:

$$\langle Ref_Q \rangle_m$$

expressing that

- *all formulas with a Q-proof of size $\leq m$ are tautologies.*

- Probably too general to be useful for *unconditional* lower bound.

- A version expressing the soundness of Q-proofs π with

$$Kt(\pi | Q(\pi)) \leq \log m$$

may be useful.

non-uniform candidates

Generators of proof complexity: given

$$g : \{0,1\}^n \to \{0,1\}^m \ , \ n < m$$

computable in time $m^{O(1)}$, take for any $b \in \{0,1\}^m \setminus Rng(g)$ the formula

$$\tau(g)_b(x,y) \ := \ g(x) \neq b \ .$$

Observation

If g is a PRNG then for no P can $i_P(\tau(g)_b)$ be bounded by $O(\log m)$.

Specific functions g for which $s_P(\tau(g)_b)$ is conjectured to be super-polynomial for strong (or all) pps were proposed.
Whenever we know that P is not p-bounded it can be demonstrated using some such g.

related topics in proof complexity

- proof complexity generators
- implicit proof systems
- proof systems with advice
- diagonalization
- random formulas
- complexity of finding hard tautologies
- ...

references

- *Information in propositional proofs and algorithmic proof search*

  [a preliminary version available at my web page]

- *Proof Complexity*, (2019), CUP

  [for a proof complexity background]