On optimal heuristic randomized semidecision procedures, with applications to proof complexity and cryptography*

Edward A. Hirsch Dmitry Itsykson Ivan Monakhov
Alexander Smal
Steklov Institute of Mathematics at St. Petersburg

5th July 2010

Abstract

The existence of a (p-)optimal propositional proof system is a major open question in (proof) complexity; many people conjecture that such systems do not exist. Krajíček and Pudlák [KP89] show that this question is equivalent to the existence of an algorithm that is optimal[1] on all propositional tautologies. Monroe [Mon09] recently gave a conjecture implying that such algorithm does not exist.

We show that in the presence of errors such optimal algorithms *do* exist. The concept is motivated by the notion of heuristic algorithms. Namely, we allow the algorithm (called *heuristic acceptor*) to claim a small number of false "theorems" (according to any polynomial-time samplable distribution on non-tautologies) and err with bounded probability on other inputs. Our result remains valid for all recursively enumerable languages and can also be viewed as the existence of an optimal weakly automatizable heuristic proof system.

We also note that the existence of a **co-NP**-language L with polynomial-time samplable distribution on $\overline{L}$ that has no polynomial-time heuristic acceptors is equivalent to the existence of infinitely-often one-way function.

1 Introduction

Given a specific problem, does there exist the "fastest" algorithm for it? Does there exist a proof system possessing the "shortest" proofs of the positive solutions to the problem?

*Supported by Federal Target Programme "Scientific and scientific-pedagogical personnel of the innovative Russia" 2009-2013 (contracts П265 and 2010-1.5-503-007-009) and RFBR (grants 08-01-00640 and 09-01-12066) and the president grants NSh-5282.2010.1 and MK-4089.2010.1. Work was done while the third author was a master student in St. Petersburg Academic University supported by Yandex Fellowship.

[1]Recent papers [Mon09] call such algorithms *p-optimal* while traditionally Levin's algorithm was called *optimal*. We follow the older tradition. Also there is some mess in terminology here, thus please see formal definitions in Sect. 2 below.

Although the first result in this direction was obtained by Levin [Lev73] in 1970s, these important questions are still open for most interesting languages, for example, the language of propositional tautologies.

Classical version of the problem. According to Cook and Reckhow [CR79], a proof system is a polynomial-time mapping of all strings ("proofs") onto "theorems" (elements of certain language L; if L is the language of all propositional tautologies, the system is called a *propositional* proof system). The existence of a *polynomially bounded* propositional proof system (that is, a system that has a polynomial-size proof for every tautology) is equivalent to $\mathbf{NP} = \mathbf{co\text{-}NP}$. In the context of polynomial boundedness a proof system can be equivalently viewed as a function that given a formula and a "proof", verifies in polynomial time that a formula is a tautology: it must accept at least one "proof" for each tautology (*completeness*) and reject all proofs for non-tautologies (*soundness*).

One proof system Π_w is *simulated* by another one Π_s if the shortest proofs for every tautology in Π_s are at most polynomially longer than the shortest proofs in Π_w. The notion of *p-simulation* is similar, but requires also a polynomial-time computable function for translating the proofs from Π_w to Π_s. A *(p-)optimal* propositional proof system is one that (p-)simulates all other propositional proof systems.

The existence of an optimal (or p-optimal) propositional proof system is a major open question. If one would exist, it would allow to reduce the **NP** vs **co-NP** question to proving proof size bounds for just one proof system. It would also imply the existence of a complete disjoint **NP** pair [Raz94, Pud03]. Krajíček and Pudlák [KP89] show that the existence of a p-optimal system is equivalent to the existence of an algorithm that is optimal on all propositional tautologies, namely, it always solves the problem correctly and it takes for it at most polynomially longer to stop on every tautology than for any other correct algorithm *on the same tautology*. Then Sadowski [Sad99] proved a similar equivalence for `SAT`. Finally, Messner [Mes99] gave a different proof of these equivalences extending them to many other languages. He also coined in the term "optimal acceptors" for such algorithms. Monroe [Mon09] recently gave a conjecture implying that optimal acceptors for `TAUT` do not exist. Note that Levin [Lev73] showed that an optimal algorithm does exist for finding witnesses to non-tautologies; however, (1) its behaviour on tautologies is not restricted; (2) after translating to the decision problem by self-reducibility the running time in the optimality condition is compared to the running time for *all shorter formulas as well*.

An *automatizable* proof system is one that has an automatization procedure that given a tautology, outputs its proof of length polynomially bounded by the length of the shortest proof in time bounded by a polynomial in the output length. The automatizability of a proof system Π implies polynomial separability of its canonical **NP** pair [Pud03], the latter implies the automatizability of a system that p-simulates Π and thus the weak automatizability of Π (system Π is *weakly automatizable* if there is an automatization procedure that outputs proofs in a system that p-simulates Π). This, however, does not imply the existence of (p-)optimal propositional proof systems in the class of (weakly) automatizable proof systems. To the best of our knowledge, no such system is known to the date.

Proving propositional tautologies heuristically. An obvious obstacle to constructing an optimal proof system by enumeration is that no efficient procedure is known for enumerating the set of all complete and sound proof systems. Recently a number of papers overcome similar obstacles in other settings by considering either computations with non-uniform advice (see [FS06] for survey) or *heuristic* algorithms [FS04, Per07, Its09]. In particular, optimal propositional proof systems with advice do exist [CK07]. We try to follow the approach of heuristic computations to obtain a "heuristic" proof system. While our work is motivated by propositional proof complexity, i.e., the language of propositional tautologies, our results apply to algorithms and proof systems for any recursively enumerable language.

We introduce a notion of a (randomized) *heuristic acceptor* (a randomized semidecision procedure that may have false positives) and a corresponding notion of a *simulation*. Its particular case, a deterministic acceptor (making no errors) for language L, along with deterministic simulations, can be viewed in two ways:

- as an automatizable proof system for L (note that such proof system can be identified with its automatization procedure; however, it may not be the case for randomized algorithms, whose running time may depend on the random coins), where simulations are p-simulations of proof systems;
- as an algorithm for L, where simulations are simulations of algorithms for L in the sense of [KP89].

Given $x \in L$, an acceptor must return 1 and stop. The question (handled by simulations) is how fast it does the job. For $x \notin L$, the running time does *not* matter. Given $x \notin L$, a deterministic acceptor simply must *not* return 1. A randomized heuristic acceptor may erroneously return 1; however, for "most" inputs it may do it only with bounded probability ("good" inputs). The precise notion of "most" inputs is: given an integer parameter d and a sampler for $\overline{L}$, "bad" inputs must have probability less than $1/d$ according to the sampler. The parameter d is handled by simulations in the way such that no heuristic acceptor can stop in time polynomial in d and the length of input unless an optimal heuristic acceptor can do that. A pair (D, L) where D is a polynomial-time samplable distribution on $\overline{L}$ is called a *distributional proving problem*.

Polynomially bounded heuristic acceptors. Similarly to the classical case, the notion of optimal heuristic acceptor has sense only for the languages and samplers that have no polynomially bounded heuristic acceptors. It turns out that such polynomial-time samplers and languages in **co-NP** correspond roughly to pseudo-random generators and the complements of their images, respectively (recall the suggestion of [ABSRW00, Kra01a, Kra01b] to consider such problems for proving lower bounds for classical proof systems). More precisely, there is such an intractible pair if and only if there is an infinitely-often one-way function.

Relation to proof systems. We also define randomized heuristic proof systems as the systems that have proofs of "theorems" (these proofs are accepted with probability at least

$\frac{1}{2}$), have no proofs (even those accepted with probability $\frac{1}{8}$) of most "non-theorems" except of a $1/d$ fraction according to a sampler of "non-theorems".

As said above, in the classical case optimal acceptors exist if and only if optimal proof systems exist. We are currently unable to prove such equivalence in the heuristic case. It is not even immediately obvious that the equivalence to (weakly) automatizable heuristic proof systems, trivial in the classical case, holds for heuristic acceptors. We prove that it is indeed the case that heuristic acceptors are equivalent to weakly automatizable heuristic proof systems, which gives an optimal weakly automatizable heuristic proof system. It is clear from the proof that one could omit the word "weakly" from this statement if the automatizing procedure is allowed to output not only proofs but also "almost proofs" (accepted by the proof system with probability $\frac{1}{4}$).

In Sect. 2 we give precise definitions. In Sect. 3 we construct an optimal randomized heuristic acceptor. In Sect. 4 we give a notion of (randomized) heuristic proof system and show that weakly automatizable heuristic proof systems are equivalent to heuristic acceptors. In Sec. 5 we show that the existence of problems intractible for heuristic acceptors is equivalent to the existence of infinitely-often one-way functions. We also provide a complete distributional proving problem. Finally, in Sect. 6 we list possible directions for further research.

2 Preliminaries

2.1 Distributional proving problems

In this paper we consider algorithms and proof systems *that allow small errors*, i.e., claim a small amount of wrong theorems. Formally, we have a probability distribution concentrated on non-theorems and require that the probability of sampling a non-theorem accepted by an algorithm or validated by the system is small.

Definition 2.1. We call a pair (D, L) a *distributional proving problem* if D is a collection of probability distributions D_n concentrated on $\overline{L} \cap \{0,1\}^n$. In this paper we assume that D is polynomial-time samplable, i.e., there is a polynomial-time randomized Turing machine (*sampler*) that given 1^n on input outputs x with probability $D_n(x)$ for every $x \in \{0,1\}^n$.

In what follows we write $\Pr_{x \leftarrow D_n}$ to denote the probability taken over x from such distribution, while $\Pr_A$ denotes the probability taken over internal random coins used by algorithm A (sometimes A is omitted).

2.2 Heuristic acceptors

Definition 2.2. A *heuristic acceptor* for distributional proving problem (D, L) is a randomized algorithm A with two inputs $x \in \{0,1\}^*$ and $d \in \mathbb{N}$ that satisfies the following conditions:

1. A either accepts, i.e., outputs 1 (denoted $A(\ldots) = 1$) or does not halt at all;
2. For every $x \in L$ and $d \in \mathbb{N}$, $A(x, d) = 1$.

3. For every $n, d \in \mathbb{N}$,
$$\Pr_{r \leftarrow D_n} \left\{ \Pr_A\{A(r,d) = 1\} \geq \frac{1}{8} \right\} < \frac{1}{d}.$$

A *normalized heuristic acceptor* is defined similarly, but condition (3) is replaced by

3′. For every $n, d \in \mathbb{N}$,
$$\Pr_{r \leftarrow D_n;\ A}\{A(r,d) = 1\} < \frac{1}{d}.$$

Remark 2.1. A normalized heuristic acceptor is *not* necessarily a heuristic acceptor for the same input. However, it is a heuristic acceptor for a different value of d as we will show below.

Remark 2.2. A semidecision procedure for every recursively enumerable language L is a (heuristic) acceptor for arbitrary D.

The time spent by a heuristic acceptor may depend on its random coins. Therefore the main complexity characteristic of a heuristic acceptor is its median time.

Definition 2.3. The median running time of algorithm A on input z is
$$t_A(z) = \min\{t \mid \Pr_A\{A(z) \text{ stops in at most } t \text{ steps}\} \geq \frac{1}{2}\}.$$

We will also use a similar notation for "probability p time":
$$t_A^{(p)}(z) = \min\{t \mid \Pr_A\{A(z) \text{ stops in at most } t \text{ steps}\} \geq p\}.$$

Definition 2.4. Function $f : \{0,1\}^* \times \mathbb{N} \to \mathbb{N}$ is *polynomially bounded on language* L if there is a polynomial p such that for all $x \in L$ and $d \in \mathbb{N}$, $f(x,d) \leq p(|x|d)$.

Definition 2.5. Function $f : \{0,1\}^* \times \mathbb{N} \to \mathbb{N}$ *dominates* function $g : \{0,1\}^* \times \mathbb{N} \to \mathbb{N}$ on language L (denoted $f \succeq g$), if there are polynomials p and q such that for all $x \in L$ and $d \in \mathbb{N}$,
$$g(x,d) \leq \max_{d' \leq q(|x|d)} \{p(f(x,d')d|x|)\}.$$

Remark 2.3.

1. If $f \succeq g$ on L and f is polynomially bounded on L, then so is g.
2. $\succeq$ is transitive.

Definition 2.6. Heuristic acceptor A for distributional proving problem (D, L) is *polynomially bounded* if $t_A(x,d)$ is polynomially bounded on L.

Definition 2.7. For heuristic acceptors A and A' for the same language L, heuristic acceptor A *simulates* A' if $t_{A'} \succeq t_A$ on L.

Heuristic acceptor A *strongly simulates* A' if $t_{A'} \succeq t_A^{(3/4)}$ on L.

Proposition 2.1 (Chernoff-Hoefding bound [McD98]). For independent random variables $X_i \in \{0,1\}$ with $\mathbf{E}\, X_i = \mu$ where $1 \le i \le N$, for every $\epsilon > 0$,

$$\Pr\left\{\left|\frac{\sum_{i=1}^{N} X_i}{N} - \mu\right| \ge \epsilon\right\} \le 2e^{-2\epsilon^2 N}.$$

Proposition 2.2. For heuristic acceptor A for (D, L), there is a normalized heuristic acceptor B that strongly simulates A.

Proof. The new algorithm $B(x,d)$ runs ℓ instances of $A(x,2d)$ independently in parallel (where ℓ is to be defined later) and stops (answering 1) as soon as at least $\frac{5}{16}\ell$ instances of A stop. That many instances must stop in time at most $t_A(x,2d)$ with probability at least $1 - 2e^{-\frac{9\ell}{128}}$ by Chernoff-Hoefding bound. Thus for every $x \in L$ and ℓ big enough, $t_B^{(3/4)}(x,d) \le \mathrm{poly}(\ell, t_A(x,2d))$.

Let $x \in \operatorname{supp} D_n$. Split $\operatorname{supp} D_n$ into $S_1 = \{x \in \operatorname{supp} D_n \mid \Pr_A\{A(x,2d) = 1\} < \frac{1}{8}\}$ and $S_2 = \operatorname{supp} D_n \setminus S_1$. Since A is a heuristic acceptor, $D_n(S_2) < \frac{1}{2d}$. For $x \in S_1$, Chernoff-Hoefding bound yields exponentially small probability $2e^{-\frac{9\ell}{128}}$ of B accepting x. Choose ℓ such that $2e^{-\frac{9\ell}{128}} < \frac{1}{4d}$. Then $\Pr_{x\leftarrow D_n;\ B}\{B(x,d) = 1\} = \Pr_{x\leftarrow D_n;\ B}\{B(x,d) = 1 \mid x \in S_1\} D_n(S_1) + \Pr_{x\leftarrow D_n}\{B(x,d) = 1 \mid x \in S_2\} D_n(S_2) \le \Pr_{x\leftarrow D_n;\ B}\{B(x,d) = 1 \mid x \in S_1\} + D_n(S_2) < \frac{1}{4d} + \frac{1}{2d} < \frac{1}{d}$. □

Proposition 2.3. If $\Pr_{x\leftarrow D_n;\ A}\{A(x,d) = 1\} < \frac{1}{d}$ holds for every d, then for every $\lambda > 0$, $\Pr_{x\leftarrow D_n}\{\Pr_A\{A(x,\lambda d) = 1\} \ge \frac{1}{\lambda}\} < \frac{1}{d}$.

Proof. $\frac{1}{\lambda d} > \Pr_{x\leftarrow D_n;A}\{A(x,\lambda d) = 1\} \ge \Pr_{x\leftarrow D_n;A}\{A(x,\lambda d) = 1 \mid \Pr_A\{A(x,\lambda d) = 1\} \ge \frac{1}{\lambda}\}$ $\cdot \Pr_{x\leftarrow D_n}\{\Pr_A\{A(x,\lambda d) = 1\} \ge \frac{1}{\lambda}\} \ge \frac{1}{\lambda} \Pr_{x\leftarrow D_n}\{\Pr_A\{A(x,\lambda d) = 1\} \ge \frac{1}{\lambda}\}$. □

Corollary 2.1. If A is a normalized heuristic acceptor, then $B(x,d) = A(x,8d)$ is a heuristic acceptor simulating A.

Propositions 2.2 and 2.3 imply that every heuristic acceptor is simulated by a normalized heuristic acceptor, and vice versa.

3 Optimal heuristic acceptor

In this section, we construct an optimal heuristic acceptor, i.e., one that simulates every other heuristic acceptor. By Prop. 2.2 and 2.3 it suffices to construct an optimal normalized heuristic acceptor. Throughout the section, L is a recursively enumerable language.

The algorithm that we construct runs all heuristic acceptors in parallel and stops when the first of them stops (recall Levin's optimal algorithm for SAT [Lev73]). A major obstacle to this simple plan is the fact that it is unclear how to enumerate all heuristic acceptors efficiently (put another way, how to check whether a given algorithm is a correct heuristic acceptor). The plan of overcoming this obstacle (similar to constructing a complete public-key cryptosystem [HKN+05] (see also [GHP09])) is as follows:

- Prove that w.l.o.g. a correct heuristic acceptor is very good: in particular, amplify its probability of success.
- Devise a "certification" procedure that distinguishes very good heuristic acceptors from incorrect acceptors with overwhelming probability.
- Run all candidate heuristic acceptors in parallel, try to certify heuristic acceptors that stop, and halt when the first of them passes the check.

The certification procedure is as follows.

Algorithm 3.1 (Procedure Certify$(A, d', n, T, \ell, \delta)$).

- Do ℓ times:
  - Sample $x \in D_n$.
  - Run $A(x, d')$ for at most T steps.
- Output 1, if there were at most $\delta\ell$ accepting computations that accepted (out of ℓ).

Proposition 3.1. Let $A^{\leq T}$ denote A with T-bounded alarm clock which interrupts A after T steps and makes it output $\perp$ if A has not finished itself. Then

- If $\Pr_{x \leftarrow D_n;\ A}\{A^{\leq T}(x, d') = 1\} < \frac{\delta}{2}$, then $\Pr\{\textsc{Certify}(A, d', n, T, \ell, \delta) = 1\} \geq 1 - 2e^{-\delta^2\ell/2}$.
- If $\Pr_{x \leftarrow D_n;\ A}\{A^{\leq T}(x, d') = 1\} > 2\delta$, then $\Pr\{\textsc{Certify}\{A, d', n, T, \ell, \delta) = 1\} \leq 2e^{-2\delta^2\ell}$.

Proof. Follows from Chernoff-Hoefding bounds. □

We now construct an optimal normalized acceptor U.

Algorithm 3.2 (Algorithm $U(x, d)$).

1. Run $A_1(x, 4dn), A_2(x, 4dn), \ldots, A_{\lfloor \frac{n}{2} \rfloor}(x, 4dn)$, and a semidecision procedure for L on input x in parallel, where $n = |x|$ and A_i is the algorithm with Goedel number i.
2. If A_i accepts in T_i steps, then run $\textsc{Certify}(A_i, 4dn, T_i, 2n^3d^3, \frac{1}{2dn})$ and accept if Certify accepts (otherwise continue).
3. If the semidecision procedure accepts, then accept.

(If one of the parallel threads accepts, all other processes are terminated.)

Lemma 3.1. $U(x, d)$ is a normalized heuristic acceptor.

Proof. By construction U either accepts or does not stop. For $x \in L$, it does stop because of the semidecision procedure for L.

Let τ_i denote $\max_T\{\Pr_{x\leftarrow D_n;\ A_i}\{A_i^{\le T}(x, 4dn) = 1\} \le \frac{1}{nd}\}$. Let $X_i(x)$ be a random variable that denotes the number of steps that $A_i(x, 4dn)$ makes before it accepts. If $A_i(x, 4dn)$ doesn't accept, then $X_i(x) = \infty$. Let $C_i(T)$ denote the event $\textsc{Certify}(A_i, 4dn, T, 2n^3d^3, \frac{1}{2dn}) = 1$.

For every i,

$$\Pr_{x\leftarrow D_n;\ A_i;\ \textsc{Certify}}\{\bigcup_{T=1}^{\infty} X_i(x) = T \wedge C_i(T)\} = \sum_{T=1}^{\infty} \Pr_{x\leftarrow D_n;\ A_i;\ \textsc{Certify}}\{X_i(x) = T \wedge C_i(T)\}$$

$$= \sum_{T=1}^{\tau_i} \Pr_{x\leftarrow D_n;\ A_i}\{X_i(x) = T\} \Pr_{\textsc{Certify}}\{C_i(T)\} + \sum_{T>\tau_i} \Pr_{x\leftarrow D_n;\ A_i}\{X_i(x) = T\} \Pr_{\textsc{Certify}}\{C_i(T)\} \quad (1)$$

Lets estimate the first sum of (1):

$$\sum_{T=1}^{\tau_i} \Pr_{x\leftarrow D_n;\ A_i}\{X_i(x) = T\} \Pr_{\textsc{Certify}}\{C_i(T)\} \le \sum_{T=1}^{\tau_i} \Pr_{x\leftarrow D_n;\ A_i}\{X_i(x) = T\}$$

$$= \Pr_{x\leftarrow D_n;\ A_i}\{1 \le X_i(x) \le \tau_i\} \le \frac{1}{nd}.$$

And now we estimate the second sum of (1):

$$\sum_{T>\tau_i} \Pr_{x\leftarrow D_n;\ A_i}\{X_i(x) = T\} \Pr_{\textsc{Certify}}\{C_i(T)\} \le \Pr_{x\leftarrow D_n;\ A_i}\{\tau_i < X_i(x)\} \Pr_{\textsc{Certify}}\{C_i(\tau_i + 1)\}$$

$$\le \Pr_{\textsc{Certify}}\{C_i(\tau_i + 1)\} \overset{\text{Prop. 3.1}}{\le} 2e^{-nd} < \frac{1}{nd}.$$

Therefore, the whole sum (1) is less than $\frac{2}{dn}$. The D-measure of inputs that force U to erroneously output 1 is

$$\Pr_{x\leftarrow D_n;\ U}\{U(x, d) = 1\} \le \sum_{i=1}^{\lfloor n/2\rfloor} \Pr_{x\leftarrow D_n;\ A_i;\ \textsc{Certify}}\{\bigcup_{T=1}^{\infty} X_i(x) = T \wedge C_i(T)\} < \frac{n}{2} \cdot \frac{2}{nd} = \frac{1}{d}.$$

□

Lemma 3.2. Normalized heuristic acceptor U simulates every other normalized heuristic acceptor.

Proof. Let A be a heuristic acceptor. Then Prop. 2.2 yields a normalized heuristic acceptor B that strongly simulates A. Assume that B has Goedel number b. Then for $\lfloor \frac{n}{2} \rfloor > b$, it is run by U. By Prop. 3.1, CERTIFY accepts it with probability at least $1 - 2e^{-dn/2}$. Therefore, for $\lfloor \frac{n}{2} \rfloor > b$, with probability at least $\frac{1}{2}$ the running time of $U(x, d)$ is at most $p_1(dn \cdot t_B^{(3/4)}(x, 4dn))$ for some polynomial p_1, hence $t_U \preceq t_B^{(3/4)}$. Since B strongly simulates A, $t_B^{(3/4)} \preceq t_A$. Thus $t_U \preceq t_A$. □

Theorem 3.1. $U'(x,d) = U(x, 8d)$ is a heuristic acceptor that simulates every other heuristic acceptor.

Proof. It is a heuristic acceptor by Lemma 3.1 and Cor. 2.1. It simulates every other heuristic acceptor by Lemma 3.2, Prop. 2.2, and the fact that $U(x, 8d)$ simulates $U(x, d)$. □

4 Weakly automatizable heuristic proof systems

In this section we define heuristic proof systems and show that weakly automatizable heuristic proof systems are essentially equivalent to heuristic acceptors (hence, there is an optimal one).

Definition 4.1. Randomized Turing machine Π is a *heuristic proof system* for distributional proving problem (D, L) if it satisfies the following conditions.

1. The running time of $\Pi(x, w, d)$ is bounded by a polynomial in d, $|x|$, and $|w|$.
2. (Completeness) For every $x \in L$ and every $d \in \mathbb{N}$, there exists a string w such that $\Pr_\Pi\{\Pi(x, w, d) = 1\} \geq \frac{1}{2}$. Every such string w is called a *correct* $\Pi^{(d)}$*-proof of* x.
3. (Soundness) $\Pr_{x \leftarrow D_n}\{\exists w : \Pr_\Pi\{\Pi(x, w, d) = 1\} \geq \frac{1}{8}\} < \frac{1}{d}$.

The main complexity characteristic of a heuristic proof system is the length of the shortest (correct) proof. For heuristic proof system Π, we denote $l_\Pi(x, d) = \min\{|w| \mid \Pr_\Pi\{\Pi(x, w, d) = 1\} \geq \frac{1}{2}\}$.

We now define the notion of weakly automatizable proof system similarly to the classical case. Namely, a system is weakly automatizable if there is an algorithm that given $x \in L$, finds efficiently a proof of x in *another* heuristic proof system and this proof is at most polynomially longer than the length of the shortest proof in Π.

Definition 4.2. Heuristic proof system Π is *weakly automatizable* if there is a randomized Turing machine A, heuristic proof system $\hat{\Pi}$, and polynomial p satisfying the following conditions:

1. For every $x \in L$ and every $d \in \mathbb{N}$,
$$\Pr_{w \leftarrow A(x,d)}\left\{|w| \leq p(d \cdot |x| \cdot l_\Pi(x, d)) \wedge w \text{ is a correct } \hat{\Pi}^{(d)}\text{-proof of } x\right\} \geq \tfrac{1}{4}. \qquad (2)$$
2. The running time of $A(x, d)$ is bounded by a polynomial in $|x|$, d, and the size of its own output.

Heuristic proof system Π is *automatizable* if it is weakly automatizable and $\hat{\Pi} = \Pi$.

Definition 4.3. We say that heuristic proof system Π_1 *simulates* heuristic proof system Π_2 if l_{Π_2} dominates l_{Π_1} on L.

Note that this definition essentially ignores proof systems that have much shorter proofs for some inputs than the inputs themselves. We state it this way for its similarity to the acceptors case.

Definition 4.4. Heuristic proof system Π is *polynomially bounded* if l_Π is polynomially bounded on L.

Proposition 4.1. If heuristic proof system Π_1 simulates system Π_2 and Π_2 is polynomially bounded, then Π_1 is also polynomially bounded.

Consider weakly automatizable proof system $(\Pi, A, \hat{\Pi})$ for distributional proving problem (D, L) with recursively enumerable language L. Let us consider the following algorithm.

Algorithm 4.1 (Algorithm $U_\Pi(x, d)$).

- Execute 1000 copies of $A(x, d)$ and a semidecision procedure for L in parallel.
- For each copy of $A(x, d)$,
  - if it stops with result w, then
    - execute $\hat{\Pi}(x, w, d)$ 60000 times;
    - if there were at least 10000 accepts of $\hat{\Pi}$ (out of 60000), accept.
- If the semidecision procedure for L accepts, then accept.

Lemma 4.1. If $(\Pi, A, \hat{\Pi})$ is a (correct) heuristic weakly automatizable proof system for recursively enumerable language L, then U_Π is a heuristic acceptor for L and $l_\Pi(x, d)$ dominates $t_{U_\Pi}(x, d)$.

Proof. Soundness (condition 3 in Def. 2.2). Let $\Delta_n = \{x \in \overline{L} \mid \exists w : \Pr\{\hat{\Pi}(x, w, d) = 1\} \geq \frac{1}{8}\}$. By definition, $D_n(\Delta_n) < \frac{1}{d}$. For $x \in \overline{L} \setminus \Delta_n$ and specific w, Chernoff bounds imply that $\hat{\Pi}(x, w, d)$ accepts in at least $\frac{1}{6}$ fraction of the 60000 executions with exponentially small probability, which remains much smaller than $\frac{1}{8}$ even after multiplying by 1000.

Completeness (conditions 2 and 1 in Def. 2.2) is guaranteed by the execution of the semidecision procedure for L.

Simulation. For $x \in L$, the probability that the event in (2) does not hold all 1000 times is negligible (at most $(\frac{3}{4})^{1000} < 10^{-120}$). Thus with high probability at least one of the parallel executions of $A(x, d)$ outputs a correct $\hat{\Pi}^{(d)}$-proof of size bounded by a polynomial in $l_\Pi(x, d)$, $|x|$ and d. For $x \in L$ and correct $\hat{\Pi}^{(d)}$-proof w, Chernoff bounds imply that $\hat{\Pi}(x, w, d)$ accepts in at least $\frac{1}{6}$ fraction of the 60000 executions with probability close to 1. Therefore, $t_{U_\Pi}(x, d)$ is bounded by a polynomial in $|x|$, d, and $l_\Pi(x, d)$. □

Lemma 4.2. Let C be a heuristic acceptor for (D, L). Then there is a weakly automatizable heuristic proof system Π_C for (D, L) such that t_C dominates l_{Π_C}.

Proof. The system Π_C will have unary words 1^T as proofs. Namely, $\Pi_C(x, 1^T, d)$ accepts if $C(x, d)$ accepts in at most T steps. The median time $t_C(x, d)$ written in unary is the shortest $\Pi_C^{(d)}$-proof of x. The correctness of Π_C follows from the correctness of C.

The weakly automatizing procedure for Π_C will output proofs that are accepted by this system with slightly smaller probability than the required $\frac{1}{2}$. Thus we construct another system $\hat{\Pi}$ that accepts these proofs. More precisely, $\hat{\Pi}(x, 1^T, d)$ executes ℓ parallel instances of $C(x, d)$ for at most T steps and stops as soon as at least $\frac{3}{16}\ell$ instances accept. For $x \in L$, Chernoff bounds imply that for $T \geq t_C^{(1/4)}(x, d)$ and ℓ big enough, $\hat{\Pi}(x, 1^T, d)$ accepts with probability at least $\frac{1}{2}$.

For those inputs x for which $\Pr\{C(x, d) = 1\} < \frac{1}{8}$, Chernoff bounds imply that $\Pr\{\hat{\Pi}(x, 1^T, d) = 1\}$ with exponentially small (in particular, less than $\frac{1}{8}$) probability. The D-probability of other inputs is at most $\frac{1}{d}$, which implies the correctness of $\hat{\Pi}$.

The automatizing procedure executes $C(x, d)$ and, if it accepts, outputs 1^T where T is the number of steps made by C. With probability at least $\frac{1}{4}$ the resulting proof 1^T has $T \in [t_C^{(1/4)}(x, d); t_C^{(1/2)}(x, d)]$. Every such proof is a correct $\hat{\Pi}^{(d)}$-proof of length not exceeding $l_{\Pi_C}(x, d) = t_C^{(1/2)}(x, d)$. □

Theorem 4.1. For recursively enumerable L and polynomial-time samplable D, there is an optimal weakly automatizable heuristic proof system (i.e., one that simulates every other weakly automatizable heuristic proof system for (D, L)).

Proof. By Lemma 4.1 each weakly automatizable heuristic proof system Π yields a heuristic acceptor A with $w_\Pi \succeq t_A$. Then A is simulated by the universal heuristic acceptor U' (Theorem 3.1, i.e., $t_A \succeq t_{U'}$. By Lemma 4.2 heuristic acceptor U' can be transformed into a weakly automatizable heuristic proof system $\Pi_{U'}$ with $t_{U'} \succeq w_{\Pi_{U'}}$. By transitivity, $\Pi_{U'}$ simulates Π. □

5 Hard problems for heuristic acceptors

In this section, we show that the existence of one-way functions implies the existence of distributional proving problems that have no polynomially bounded heuristic acceptors. More precisely, the existence of such problems is equivalent to the existence of *infinitely-often* one-way functions, i.e., ones that are hard to invert for infinitely many input lengths. The logic of the equivalence is as follows: $\exists$ i.o. one-way functions $\Rightarrow$ $\exists$ i.o. pseudorandom generators $\Rightarrow$ $\exists$ intractable distributional proving problems $\Rightarrow$ $\exists$ average-case one-way functions $\Rightarrow$ $\exists$ i.o. one-way functions.

Definition 5.1. Let $f\colon \{0,1\}^* \to \{0,1\}^*$ be a length-preserving polynomial-time computable function. We call it *i.o. one-way* if for every polynomial-time randomized algorithm A and every polynomial p,

$$\forall n_0\ \exists n > n_0\ \Pr_{x \leftarrow \mathbf{U}_n}\{A(x) \in f^{-1}(f(x))\} < \frac{1}{p(n)}.$$

Similarly to the classical case, the existence of i.o. one-way functions implies the existence of i.o. pseudorandom generators.

Definition 5.2. Let $G : \{0,1\}^* \to \{0,1\}^*$ be a polynomial-time computable function such that $\forall r\ |G(r)| = |r|+1$. We call it i.o. pseudorandom generator if for every polynomial-time randomized algorithm A and every polynomial p,

$$\forall n_0\ \exists n > n_0 \mid \Pr_{x\leftarrow \mathbf{U}_n}\{A(G(x)) = 1\} - \Pr_{x\leftarrow \mathbf{U}_{n+1}}\{A(x) = 1\}| < \frac{1}{p(n)}.$$

Theorem 5.1 (cf. [HILL99]). If there is an i.o. one-way function, then there is an i.o. pseudorandom generator.

Proof. The construction repeats that of [HILL99]. In the latter the lengths of inputs where the one-way function is hard to invert are mapped to the lengths of inputs where the pseudorandom generator is hard to break. □

Assume there exists an i.o. pseudorandom generator. We now show how to transform it into a distributional proving problem that has no polynomially bounded heuristic acceptors.

Theorem 5.2. If there is an i.o. pseudorandom generator G, then there is a distributional proving problem (D, L) with polynomial-time samplable D and language $L \in$ **co-NP** such that there is no polynomially bounded heuristic acceptor for (D, L).

Proof. Define $D_{n+1}(x) = \Pr_{y\leftarrow \mathbf{U}_n}\{G(y) = x\}$ and $L = \bigcup_n(\{0,1\}^{n+1} \setminus G(\{0,1\}^n))$.

Suppose that there is a normalized heuristic acceptor A for (D, L) such that $t_A(x, d) \le q(|x|d)$ for a polynomial q. We then construct algorithm $B(x)$ as follows: It executes $A(x, \frac{1}{10})$ for $q(10|x|)$ steps and outputs 1 iff A accepts (otherwise B outputs 0).

We now show that B breaks G. Indeed, $\Pr_{x\leftarrow \mathbf{U}_{n+1}}\{B(x) = 1\} \ge \frac{1}{2} \cdot \frac{|\{0,1\}^{n+1}\setminus G(\{0,1\}^n)|}{2^{n+1}} \ge \frac{1}{2}(1 - \frac{1}{2}) = \frac{1}{4}$. However, $\Pr_{x\leftarrow \mathbf{U}_n}\{B(G(x)) = 1\} < \frac{1}{10}$. Contradiction. □

Following [HI10], we define average-case one-way functions.

Definition 5.3. Length-preserving polynomial-time computable function $f\colon \{0,1\}^* \to \{0,1\}^*$ is *average-case one-way* if for every poly$(|x|d)$-time randomized algorithm $A(x, d)$,

$$\forall n_0\ \exists n > n_0\ \Pr_{x\leftarrow \mathbf{U}_n}[\Pr_A\{f(A(f(x), d)) \ne f(x)\} \ge \frac{1}{4}] \ge \frac{1}{d}.$$

Remark 5.1. Using the argument that similar to one used in propositions 2.2 and 2.3 it is possible to show that the condition

$$\Pr_{x\leftarrow \mathbf{U}_n}\{\Pr_A\{f(A(f(x), d)) \ne f(x)\} \ge \frac{1}{4}\} \ge \frac{1}{d}$$

can be equivalently replaced by

$$\Pr_{x\leftarrow \mathbf{U}_n}\{f(A(f(x), d)) \ne f(x)\} \ge \frac{1}{d}.$$

Theorem 5.3 ([HI10]). The existence of average-case one-way functions implies the existence of i.o. one-way functions.

Theorem 5.4. Assume that (D, L) has no polynomially bounded heuristic acceptors. Then there exists an average-case one-way function.

Proof. Assume that D has a polynomial-time sampler g using $p(n)$ random bits for inputs of length n, i.e., $|g(x)| = n$ whenever $|x| = p(n)$. Define function f as follows:

$$f(x) = \begin{cases} g(x)0^{p(n)-n}, & \text{if } \exists n\ |x| = p(n), \\ x, & \text{otherwise.} \end{cases}$$

We now show that f is average-case one-way. Let $B(x, d)$ be a $q(|x|d)$-time algorithm (where q is a polynomial) and for every n big enough, $\Pr_{x \leftarrow \mathbf{U}_{p(n)};\ B}\{f(B(f(x), d)) \neq f(x)\} < \frac{1}{d}$. Define algorithm $A(x, d)$ as follows: Compute $y = B(x0^{p(|x|)-|x|}, d)$; if $f(y) = x0^{p(|x|)-|x|}$, then output 0, otherwise 1.

The running time of $A(x, d)$ is poly$(|x|d)$. For $x \in L$, there is no preimage, i.e., $A(x, d) = 1$. For $x \notin L$, $\Pr_{x \leftarrow D_n;\ A}\{A(x, d) = 1\} = \Pr_{x \leftarrow \mathbf{U}_{p(n)};\ B}\{f(B(f(x), d)) \neq f(x)\} < \frac{1}{d}$, which gives a polynomially bounded normalized heuristic acceptor and thus a polynomially bounded heuristic acceptor for (D, L). □

Corollary 5.1. The following objects exist (or do not exist) simultaneously:

- Distributional proving problem that has no polynomially bounded heuristic acceptors.
- Infinitely often one-way function.
- Average-case one-way function.
- Infinitely often pseudorandom generator.

Similarly to Levin's universal one-way function [Lev87] one can construct a universal distributional proving problem which is complete under reductions that preserve tractability for heuristic acceptors. Such reductions resemble reductions used in average-case complexity (see [BT06]).

Definition 5.4. Distributional proving problem (D_1, L_1) reduces to distributional proving problem (D_2, L_2) if there is an injective polynomial-time computable $f : \{0,1\}^* \to \{0,1\}^*$ mapping inputs of equal length to inputs of equal length such that

- $x \in L_1 \iff f(x) \in L_2$;
- there is a polynomial p such that for for every input x, $p(|x|)D_2(f(x)) \geq D_1(x)$.

Proposition 5.1. If (D, L) reduces to (D', L') and (D', L') has a polynomially bounded heuristic acceptor, then so has (D', L').

Proof. Assume the reduction is given by function f mapping words of length t into words of length $\varphi(t)$, and p is as in the definition above. Let $A(x,d)$ be a heuristic acceptor for (D',L'). Then $B(x,d)=A(f(x),p(|x|)d)$ is a heuristic acceptor for (D,L):

$$\Pr_{x\leftarrow D_n}\{\Pr_A\{A(f(x),p(|x|)d)=1\}\geq\tfrac{1}{8}\}=\textstyle\sum_{x\in\operatorname{supp}D_n:\Pr\{A(f(x),p(n)d)=1\}\geq\frac{1}{8}}D(x)$$

$$\leq\sum_{x\in\operatorname{supp}D_n:\Pr\{A(f(x),p(n)d)=1\}\geq\frac{1}{8}}p(n)D'(f(x))\leq\sum_{y\in\operatorname{supp}D'_{\varphi(n)}:\Pr\{A(y,p(n)d)=1\}\geq\frac{1}{8}}p(n)D'(y)$$

$$=p(n)\cdot\Pr_{y\leftarrow D'_{\varphi(n)}}\{\Pr\{A(y,p(n)d)=1\}\geq\tfrac{1}{8}\}<p(n)/(dp(n))=1/d.$$

□

Lemma 5.1. There is a constant C such that every problem (D,L) reduces to some (D',L') where D' has a sampler running in time at most Cn^2.

Proof. We use padding. Assume that sampler g for D runs in at most cn^c steps and uses at least n random bits. The new sampler h, asked to produce a sample of length n, pads g's sample by outputting $h(r)=0^{cn^c}1g(r)$. Let $L'=\{0^{c|x|^c}1x\mid x\in L\}$. The reduction is given by $f(y)=0^{c|y|^c}1y$. □

We now construct a universal distributional proving problem (R,X). The language X contains only inputs of even lengths. The distribution R is uniform on odd lengths and defined on length $2n$ as follows: with probability $1/2^i$ (where $1\leq i\leq n-1$), its sampler $g(r)$ outputs the concatenation $s_iA_i(r)$, where where s_i is a word of length n that contains zeroes except for the position i where it has 1 and A_i is the algorithm with Goedel number i equipped with quadratic alarm clock as in Lemma 5.1; with probability $1/2^{n-1}$ it outputs $s_nA_n(r)$. Let $X=\{0,1\}^*\setminus\operatorname{supp}R$.

Theorem 5.5. Every distributional proving problem (D,L) reduces to (R,X).

Proof. By Lemma 5.1 the problem (D,L) reduces to a quadratic-time samplable (D',L'). Assume that the sampler for D' has Goedel number k, then (D',L') reduces to (R,X) by $f(x)=s_kx$, where s_k is as in the definition of R (for $|x|<k$, f computes the answer itself and maps to an appropriate fixed string, which takes a constant time). The domination condition $2^kR(x)\geq D'(x)$ is satisfied since k is a constant. □

6 Further research

- For weakly automatizable heuristic proof system equivalent to a heuristic acceptor, show that its automatizing procedure can output a correct proof in the same proof system. (That is, the system is automatizable in the classical sense.)
- Devise an optimal heuristic proof system.
- Give a nice conjecture implying the existence of distributional proving problems that have no polynomially bounded heuristic proof systems.
- Consider a version of the notion of heuristic proof systems related to trapdoor functions.

Acknowledgements

The authors are grateful to Dima Antipov and Dima Grigoriev for helpful discussions.

References

[ABSRW00] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Pseudorandom generators in propositional proof complexity. Technical Report 00-023, Electronic Colloquium on Computational Complexity, 2000. Extended abstract appears in Proceedings of FOCS-2000.

[BT06] Andrej Bogdanov and Luca Trevisan. Average-case complexity. *Foundation and Trends in Theoretical Computer Science*, 2(1):1–106, 2006.

[CK07] Stephen A. Cook and Jan Krajíček. Consequences of the provability of $NP \subseteq P/poly$. *The Journal of Symbolic Logic*, 72(4):1353–1371, 2007.

[CR79] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, March 1979.

[FS04] Lance Fortnow and Rahul Santhanam. Hierarchy theorems for probabilistic polynomial time. In *Proceedings of the 45th IEEE Symposium on Foundations of Computer Science*, pages 316–324, 2004.

[FS06] Lance Fortnow and Rahul Santhanam. Recent work on hierarchies for semantic classes. *SIGACT News*, 37(3):36–54, 2006.

[GHP09] Dima Grigoriev, Edward A. Hirsch, and Konstantin Pervyshev. A complete public-key cryptosystem. *Groups, Complexity, Cryptology*, 1(1):1–12, 2009.

[HI10] E.A. Hirsch and D.M. Itsykson. An infinetely often one-way function based on an average-case assumption. *St. Petersburg Math. J.*, 21(3):459–468, 2010.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[HKN+05] Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold, and Alon Rosen. On robust combiners for oblivious transfer and other primitives. In *Proc. of EUROCRYPT-2005*, 2005.

[Its09] Dmitry M. Itsykson. Structural complexity of AvgBPP. In *Proceedings of 4th International Computer Science Symposium in Russia*, volume 5675 of *Lecture Notes in Computer Science*, pages 155–166, 2009.

[KP89] Jan Krajíček and Pavel Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54(3):1063–1079, September 1989.

[Kra01a] Jan Krajíček. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170(1–3):123–140, 2001.

[Kra01b] Jan Krajíček. Tautologies from pseudorandom generators. *Bulletin of Symbolic Logic*, 7(2):197–212, 2001.

[Lev73] Leonid A. Levin. Universal sequential search problems. *Problems of Information Transmission*, 9:265–266, 1973.

[Lev87] Leonid A. Levin. One-way functions and pseudorandom generators. *Combinatorica*, 7, 1987.

[McD98] C. McDiarmid. *Concentration*, volume 16 of *Algorithms and Combinatorics*, pages 195–248. Springer-Verlag, 1998.

[Mes99] Jochen Messner. On optimal algorithms and optimal proof systems. In *Proceedings of the 16th Symposium on Theoretical Aspects of Computer Science*, volume 1563 of *Lecture Notes in Computer Science*, pages 361–372, 1999.

[Mon09] Hunter Monroe. Speedup for natural problems and coNP?=NP. Technical Report 09-056, Electronic Colloquium on Computational Complexity, 2009.

[Per07] Konstantin Pervyshev. On heuristic time hierarchies. In *Proceedings of the 22nd IEEE Conference on Computational Complexity*, pages 347–358, 2007.

[Pud03] Pavel Pudlák. On reducibility and symmetry of disjoint NP pairs. *Theoretical Computer Science*, 295(1–3):323–339, 2003.

[Raz94] Alexander A. Razborov. On provably disjoint NP-pairs. Technical Report 94-006, Electronic Colloquium on Computational Complexity, 1994.

[Sad99] Zenon Sadowski. On an optimal deterministic algorithm for SAT. In *Proceedings of CSL'98*, volume 1584 of *Lecture Notes in Computer Science*, pages 179–187. Springer, 1999.