On optimal heuristic randomized semidecision procedures, with application to proof complexity

Edward A. Hirsch and Dmitry Itsykson

Steklov Institute of Mathematics at St. Petersburg

STACS
March 4, 2010

Acceptors and proof systems

- $\mathcal{A}$ is an acceptor for language L if
  - $\forall x \in L\ \mathcal{A}(x) = 1$,
  - $\forall x \notin L\ \mathcal{A}(x)$ does not stop.
- [Cook, Reckhow, 70s] A proof system for language L is a polynomial-time surjective mapping $\Pi\colon \{0,1\}^* \to L$.
  - w is called a Π-proof of $f(w)$.
- Proof system from acceptor:
  - $\Pi_{\mathcal{A}}$: [protocol of $\mathcal{A}(x)$] $\mapsto x$.
- An automatizable proof system is a pair $(\Pi, \mathcal{B})$:
  - $\forall x \in L\ \mathcal{B}(x)$ outputs a Π-proof of x in time $\leq \mathrm{poly}$(size of the shortest Π-proof of x).
  - $\forall x \notin L\ \mathcal{B}(x)$ does not stop.
- $(\Pi_{\mathcal{A}}, \widetilde{\mathcal{A}})$ is an automatizable proof system.

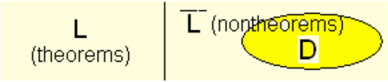
Propositional proof systems

- Propositional proof systems: proof systems for the language of Boolean tautologies **TAUT**.
- Every algorithm for **TAUT** yields a proof system, but not vice versa.
- $\mathbf{NP} = \mathbf{coNP}$ iff there is a proof system that has a polynomial-size proof for every tautology.
- $\mathbf{P} = \mathbf{NP}$ iff there is an automatizable proof system that has a polynomial-size proof for every tautology.

Simulation and Optimality

- A proof system Π_1 p-simulates a proof system Π_2 if $\exists$ polynomial-time computable function f that maps Π_2-proofs to Π_1-proofs.
- An acceptor $\mathcal{A}_1$ simulates an acceptor $\mathcal{A}_2$ if $\forall x \in L$ running time of $\mathcal{A}_1(x) \leq poly(\text{running time of } \mathcal{A}_2(x))$.
- [Krajíček, Pudlák, 1989] $\exists$ p-optimal proof system for **TAUT** $\iff$ $\exists$ optimal acceptor for **TAUT**.
- [Messner, 1999] For every paddable language L, $\exists$ p-optimal proof system for $L \iff \exists$ optimal acceptor for L.
- [Cook, Krajíček, 2007] $\exists$ p-optimal proof system with 1 bit of nonuniform advice.

Heuristic proof systems and acceptors



- Distributional proving problem: (L, D) where D is polynomial-time samplable distribution on $\overline{L}$.
- Heuristic proof system for (L, D) is a randomized algorithm $\Pi(x, w, d)$:
  - Running time of $\Pi(x, w, d)$ is $poly(|x|, |w|, d)$.
  - (Completeness) $\forall x \in L \; \forall d \in \mathbb{N} \; \exists w \;\; \Pr\{\Pi(x, w, d) = 1\} > \frac{1}{2}$.
  - (Soundness) $\Pr_{x \leftarrow D_n}\{\exists w \;\; \Pr\{\Pi(x, w, d) = 1\} > \frac{1}{4}\} < \frac{1}{d}$.
- Heuristic acceptor for (L, D) is a randomized algorithm $\mathcal{A}(x, d)$:
  - $\forall x \in L \; \forall d \in \mathbb{N} \; \mathcal{A}(x, d) = 1$.
  - $\Pr_{x \leftarrow D_n}\{\Pr\{\mathcal{A}(x, d) \text{ stops}\} > \frac{1}{4}\} < \frac{1}{d}\}$.
- Median running time:
  - $\min\{t \mid \Pr\{A(x, d) \text{ runs in} \leq t \text{ steps}\} \geq \frac{1}{2}\}$.

Optimal heuristic acceptor

Theorem. For every r.e. language L and p-samplable D with support in $\overline{L}$ there exists an acceptor $U(x, d)$ for (L, D) that has optimal (up to $poly(|x|, d)$) median time.

Construction (sketch):

Optimal heuristic acceptor $U(x, d)$:

- In parallel for all $1 \leq i \leq \log_* n$:
  1. Execute $A_i(x, d')$; Let T_i be its running time.
  2. Verify the correctness of A_i:
     Repeat for many times:
     - $r \leftarrow D_n$,
     - If $A_i^{\leq T_i}(r, d') = 1$ too often,
       then put a black point;

     and verify that the number of black points is small.
  3. Return "1".
- Execute the semidecision procedure for r.e. language L.

Further research

- Some recent observations (unpublished)
  - An optimal heuristic automatizable proof system (under weak enough notion of automatizability).
  - $\exists$ one-way functions $\implies$ $\exists$ p-samplable distribution D on $\overline{\textbf{TAUT}}$ such that every heuristic acceptor for $(\textbf{TAUT}, D)$ is not polynomial bounded.
  - A universal distribution on $\overline{\textbf{TAUT}}$ that dominates distributions on $\overline{\textbf{TAUT}}$ that are provably correct or certify their results.
- Open questions
  - Construct an optimal heuristic proof system.
  - Extend the equivalence between p-optimal proof systems and optimal acceptors to the heuristic case.