Optimal heuristic algorithms for the image of an injective function

E.A. Hirsch[1] D.M. Itsykson[1] V. Nikolaenko[2] A. Smal[1]

[1]Steklov Institute of Mathematics at St. Petersburg

[2]St. Petersburg Academic University

Workshop on post-quantum cryptography, 2011

Outline

Outline

Motivation

- For a computational problem that is not known to be solved in a reasonable (say, polynomial) amount of time, we are still interested to solve it as fast as possible.

Motivation

- For a computational problem that is not known to be solved in a reasonable (say, polynomial) amount of time, we are still interested to solve it as fast as possible.
- Levin's optimal algorithm for $\mathbf{NP}$ *search* problems is known for decades [Lev'73].
- The existence of optimal algorithms is not known for any *decision* problem in $\mathbf{NP} \setminus \mathbf{P}$.

Motivation

- For a computational problem that is not known to be solved in a reasonable (say, polynomial) amount of time, we are still interested to solve it as fast as possible.
- Levin's optimal algorithm for $\mathbf{NP}$ *search* problems is known for decades [Lev'73].
- The existence of optimal algorithms is not known for any *decision* problem in $\mathbf{NP} \setminus \mathbf{P}$.
- For $\mathtt{TAUT}$, the existence of an optimal acceptor is equivalent to the existence of a p-optimal proof system.
- Monroe recently gave a conjecture implying that optimal acceptors for $\mathtt{TAUT}$ do not exist [Mon'11].

Motivation

- For a computational problem that is not known to be solved in a reasonable (say, polynomial) amount of time, we are still interested to solve it as fast as possible.
- Levin's optimal algorithm for $\mathbf{NP}$ *search* problems is known for decades [Lev'73].
- The existence of optimal algorithms is not known for any *decision* problem in $\mathbf{NP} \setminus \mathbf{P}$.
- For $\mathtt{TAUT}$, the existence of an optimal acceptor is equivalent to the existence of a p-optimal proof system.
- Monroe recently gave a conjecture implying that optimal acceptors for $\mathtt{TAUT}$ do not exist [Mon'11].
- Recognizing the image of an injective pseudorandom generator.

- For a probability distribution D, we denote D_n the restriction of D to $\{0, 1\}^n$. U denotes the uniform distributions.

- For a probability distribution D, we denote D_n the restriction of D to $\{0,1\}^n$. U denotes the uniform distributions.
- A *distributional problem* is a pair (L, D) consisting of a language $L \subseteq \{0,1\}^*$ and a distribution D.
- $A(x, d)$ is a *randomized heuristic algorithm* for a distributional problem (L, D) if
  - $A(x, d) \in \{0, 1\}$,
  - $\forall n, \Pr_{x \leftarrow D_n; A}[A(x, d) \neq L(x)] < \frac{1}{d}$, where D_n is over $\{0, 1\}^n$.

Definitions

Acceptors and algorithms

- For a probability distribution D, we denote D_n the restriction of D to $\{0,1\}^n$. U denotes the uniform distributions.
- A *distributional problem* is a pair (L, D) consisting of a language $L \subseteq \{0,1\}^*$ and a distribution D.
- $A(x, d)$ is a *randomized heuristic algorithm* for a distributional problem (L, D) if
  - $A(x, d) \in \{0, 1\}$,
  - $\forall n$, $\Pr_{x \leftarrow D_n; A}[A(x, d) \neq L(x)] < \frac{1}{d}$, where D_n is over $\{0,1\}^n$.
- A *distributional proving problem* is a pair (L, D) consisting of a language $L \subseteq \{0,1\}^*$ and a distribution D, concentrated on $\overline{L}$.
- $A(x, d)$ is a *randomized heuristic acceptor* for a distributional proving problem (L, D),
  - $A(x, d) \in \{1, \perp\}$,
  - $A(x, d) = 1$ for all $x \in L$,
  - $\forall n$, $\Pr_{x \leftarrow D_n; A}[A(x, d) = 1] < \frac{1}{d}$, where D_n is over $\overline{L} \cap \{0,1\}^n$.

- For a probability distribution D, we denote D_n the restriction of D to $\{0,1\}^n$. U denotes the uniform distributions.
- A *distributional problem* is a pair (L, D) consisting of a language $L \subseteq \{0,1\}^*$ and a distribution D.
- $A(x, d)$ is a *randomized heuristic algorithm* for a distributional problem (L, D) if
  - $A(x, d) \in \{0, 1\}$,
  - $\forall n, \Pr_{x \leftarrow D_n; A}[A(x, d) \neq L(x)] < \frac{1}{d}$, where D_n is over $\{0,1\}^n$.
- A *distributional proving problem* is a pair (L, D) consisting of a language $L \subseteq \{0,1\}^*$ and a distribution D, concentrated on $\overline{L}$.
- $A(x, d)$ is a *randomized heuristic acceptor* for a distributional proving problem (L, D),
  - $A(x, d) \in \{1, \perp\}$,
  - $A(x, d) = 1$ for all $x \in L$,
  - $\forall n, \Pr_{x \leftarrow D_n; A}[A(x, d) = 1] < \frac{1}{d}$, where D_n is over $\overline{L} \cap \{0,1\}^n$.

- The *time* spent by a randomized algorithm A on input (x, d)

  $$t_A(x, d) = \min\left\{t \in \mathbb{N} \mid \Pr_A[A(x, d) \text{ stops in time at most } t] \geq \tfrac{1}{2}\right\}.$$

- The *time* spent by a randomized algorithm A on input (x, d)

  $t_A(x, d) = \min\{t \in \mathbb{N} \mid \Pr_A[A(x, d) \text{ stops in time at most } t] \geq \frac{1}{2}\}$.

- For heuristic algorithms (acceptors) A and A' for the same problem (L, D), we say that A *simulates* A' if there are polynomials p and q such that $\forall x \in \operatorname{supp} D$, $\forall d \in \mathbb{N}$,

$$t_A(x, d) \leq \max_{d' \leq q(|x|d)} \{p(t_{A'}(x, d')d|x|)\}.$$

- An *optimal* randomized heuristic algorithm (acceptor) for (L, D) simulates every randomized heuristic algorithm (acceptor) for (L, D).

Outline

Problem statement

Consider the problem of recognizing the image of an polynomial-time computable injective function $f : \{0,1\}^* \to \{0,1\}^*$, such that $|f(x)| = |x| + 1$.

Main question

Is there exists an optimal (randomized) heuristic algorithm for distributional problem $(\mathrm{Im}\, f, U)$.

Problem statement

Consider the problem of recognizing the image of an polynomial-time computable injective function $f : \{0,1\}^* \to \{0,1\}^*$, such that $|f(x)| = |x| + 1$.

Main question

Is there exists an optimal (randomized) heuristic algorithm for distributional problem $(\operatorname{Im} f, U)$.

Remark

If f is an injective pseudorandom generator then there is no *polynomial-time* heuristic randomized algorithm for $(\operatorname{Im} f, U)$ [HIMS10].

Optimal heuristic acceptor for $(\overline{\mathrm{Im} f}, U)$

Algorithm `OptAcc`(x, d)

1. Run $A_{bf}(x, d'), A_1(x, d'), \ldots, A_n(x, d')$ in parallel.
2. Certify every algorithm that stops and outputs 1.
3. If one of the algorithms passes certification test, stop all algorithms and output 1.

Optimal heuristic acceptor for $(\overline{\operatorname{Im} f}, U)$

Algorithm `OptAcc`(x, d)

1. Run $A_{bf}(x, d'), A_1(x, d'), \ldots, A_n(x, d')$ in parallel.
2. Certify every algorithm that stops and outputs 1.
3. If one of the algorithms passes certification test, stop all algorithms and output 1.

Algorithm `CertifyAcc`$(A,\ d)$

1. Test algorithm on many inputs generated from U.
2. If A accepts only a small fraction of inputs, then return ‘‘`PASSED`’’, otherwise ‘‘`FAILED`’’.

Optimal heuristic acceptor for $(\overline{\operatorname{Im} f}, U)$

Algorithm `OptAcc`(x, d)

1. Run $A_{bf}(x, d'), A_1(x, d'), \ldots, A_n(x, d')$ in parallel.
2. Certify every algorithm that stops and outputs 1.
3. If one of the algorithms passes certification test, stop all algorithms and output 1.

Algorithm `CertifyAcc`$(A,\ d)$

1. Test algorithm on many inputs generated from U.
2. If A accepts only a small fraction of inputs, then return "`PASSED`", otherwise "`FAILED`".

Theorem

`OptAcc` *is an optimal randomized heuristic acceptor for* $(\overline{\operatorname{Im} f}, U)$.

General case

Remark

We used only the fact that $\operatorname{Im} f$ is polynomial-time samplable. We neither used the uniformity of U nor the properties of f.

Theorem (HIMS'10)

For every recursively enumerable language L and every polynomial-time samplable D concentrated on $\overline{L}$, there is an optimal heuristic acceptor for distributional proving problem (L, D).

Deterministic case

- A *deterministic* heuristic algorithm (acceptor) is a randomized heuristic algorithm (acceptor) that does not use its randomness.
- The running time t_A is now simply made by the algorithm A.

Deterministic case

- A *deterministic* heuristic algorithm (acceptor) is a randomized heuristic algorithm (acceptor) that does not use its randomness.
- The running time t_A is now simply made by the algorithm A.
- For heuristic algorithms A and A' for a distributional problem (L, D), we say that A *simulates* A', if there are polynomials p and q such that $q(n, d) \geq 2d$ and $\forall n, d \in \mathbb{N}$,

$$\Pr_{x \leftarrow D_n} [t_A(x, d) \leq p(n \cdot d \cdot t_{A'}(x, q(n, d)))] \geq 1 - \frac{1}{2d}.$$

- A deterministic heuristic algorithm (acceptor) for a distributional (proving) problem (L, D) is *optimal on the average* if it simulates every other deterministic heuristic algorithm (acceptor) for (L, D).

Optimal deterministic heuristic acceptor

Theorem (GW'97)

Let n be an integer and $\delta \geq 2^{-\gamma n}$, where γ is some positive constant. Then there exists a family of functions $\mathcal{F}_\delta$, each mapping $\{0,1\}^n$ to itself with good mixing property [GW'97]:

$$\left| \Pr_{x \leftarrow U_n, \phi \leftarrow U(\mathcal{F}_\delta)} [x \in A \wedge \phi(x) \in B] - \rho(A)\rho(B) \right| \leq 2\delta.$$

Family $\mathcal{F}_\delta$ constains a polynomial in $\frac{1}{\delta}$ number of functions, functions in $\mathcal{F}_\delta$ can be efficiently evaluated.

Optimal deterministic heuristic acceptor

Theorem (GW'97)

Let n be an integer and $\delta \geq 2^{-\gamma n}$, where γ is some positive constant. Then there exists a family of functions $\mathcal{F}_\delta$, each mapping $\{0,1\}^n$ to itself with good mixing property [GW'97]:

$$\left| \Pr_{x \leftarrow U_n, \phi \leftarrow U(\mathcal{F}_\delta)} [x \in A \wedge \phi(x) \in B] - \rho(A)\rho(B) \right| \leq 2\delta.$$

Family $\mathcal{F}_\delta$ constains a polynomial in $\frac{1}{\delta}$ number of functions, functions in $\mathcal{F}_\delta$ can be efficiently evaluated.

Algorithm `CertifyDetAcc`(A, x, δ)

1. If $\delta < 2^{-\gamma n}$, then execute $A(y)$ for every $y \in \{0,1\}^n$.
2. If $\delta \geq 2^{-\gamma n}$, then for every $\phi \in \mathcal{F}_\delta$ execute $A(f(\phi(x)))$.
3. If A accepts only a small fraction of inputs, then return "`PASSED`", otherwise "`FAILED`".

Optimal heuristic algorithm

Observation

An optimal heuristic algorithm for $(\mathrm{Im}\, f, U)$ is equivalent to two optimal heuristic acceptors: for $(\overline{\mathrm{Im}\, f}, U)$ and for $(\mathrm{Im}\, f, U)$.

Optimal heuristic algorithm

Observation

An optimal heuristic algorithm for $(\operatorname{Im} f, U)$ is equivalent to two optimal heuristic acceptors: for $(\overline{\operatorname{Im} f}, U)$ and for $(\operatorname{Im} f, U)$.

Obstacle

We don't have a polynomial-time samplable distribution on $\overline{\operatorname{Im} f}$, that is needed for certification procedure.

Optimal heuristic algorithm

Observation

An optimal heuristic algorithm for $(\mathrm{Im}\, f, U)$ is equivalent to two optimal heuristic acceptors: for $(\overline{\mathrm{Im}\, f}, U)$ and for $(\mathrm{Im}\, f, U)$.

Obstacle

We don't have a polynomial-time samplable distribution on $\overline{\mathrm{Im}\, f}$, that is needed for certification procedure.

Key idea

Estimate the probability of wrong answer on $\overline{\mathrm{Im}\, f}$ using distributions $U(\mathrm{Im}\, f)$ and U_{n+1}:

$$\Pr_{x \in \overline{\mathrm{Im}\, f}}[A(x,d) = 1] = 2 \Pr_{x \leftarrow U_{n+1}}[A(x,d) = 1] - \Pr_{x \in \mathrm{Im}\, f}[A(x,d) = 1].$$

Outline

Summary

Let f be an polynomial-time computable injective function $f : \{0,1\}^* \to \{0,1\}^*$, such that $|f(x)| = |x| + 1$.

- There is an optimal randomized heuristic algorithm for recognizing the image of f under the uniform distribution.
- There is an optimal on the average deterministic heuristic algorithm for recognizing the image of f w.r.t the uniform distribution.

Thanks for your attention!