Heuristic time hierarchies via hierarchies for sampling distributions

Authors:

Dmitry Itsykson, Alexander Knop, Dmitry Sokolov

Institute:

St. Petersburg Department of V.A. Steklov Institute of Mathematics of the Russian Academy of Sciences

First steps

HARTMANIS AND STEARNS, 1965

For any $k > 0$ we have that

$$\mathbf{P} \not\subseteq \mathbf{DTime}(n^k).$$

COOK, 1973; ZAK, 1983

For any $k > 0$ holds

$$\mathbf{NP} \not\subseteq \mathbf{NTime}(n^k).$$

First steps

HARTMANIS AND STEARNS, 1965

For any $k > 0$ we have that

$$\mathbf{P} \not\subseteq \mathbf{DTime}(n^k).$$

COOK, 1973; ZAK, 1983

For any $k > 0$ holds

$$\mathbf{NP} \not\subseteq \mathbf{NTime}(n^k).$$

Probabilistic algorithms

BOUNDED PROBABILISTIC ALGORITHMS

Language $L \in \mathbf{BPTime}(n^k)$ iff there is randomized $O(n^k)$-time algorithm A such that

$$\forall x \in \{0,1\}^* \Pr[A(x) = L(x)] > \frac{3}{4}.$$

We also denote $\mathbf{BPP} = \bigcup_k \mathbf{BPTime}(n^k)$.

OPEN QUESTION

Is it true that for any $k > 0$ holds that

$$\mathbf{BPP} \not\subseteq \mathbf{BPTime}(n^k).$$

Probabilistic algorithms

BOUNDED PROBABILISTIC ALGORITHMS

Language $L \in \mathbf{BPTime}(n^k)$ iff there is randomized $O(n^k)$-time algorithm A such that

$$\forall x \in \{0,1\}^* \Pr[A(x) = L(x)] > \frac{3}{4}.$$

We also denote $\mathbf{BPP} = \bigcup_k \mathbf{BPTime}(n^k)$.

OPEN QUESTION

Is it true that for any $k > 0$ holds that

$$\mathbf{BPP} \not\subseteq \mathbf{BPTime}(n^k).$$

Derandomization

FOLKLORE

If there is pseudorandom generator that maps $\log(n)$ bits to $\mathrm{poly}(n)$ then $\mathbf{BPP} \not\subseteq \mathbf{BPTime}(n^k)$.

ITSYKSON, KNOP, SOKOLOV, 2015

If there is pseudorandom generator that maps n bits to $\mathrm{poly}(n)$ then $\mathbf{BPP} \not\subseteq \mathbf{BPTime}(n^k)$.

Derandomization

FOLKLORE

If there is pseudorandom generator that maps $\log(n)$ bits to $\mathrm{poly}(n)$ then **BPP** $\not\subseteq$ **BPTime**(n^k).

ITSYKSON, KNOP, SOKOLOV, 2015

If there is pseudorandom generator that maps n bits to $\mathrm{poly}(n)$ then **BPP** $\not\subseteq$ **BPTime**(n^k).

Deterministic algorithms

HEURISTIC DETERMINISTIC ALGORITHM

Language $L \in \mathsf{Heur}_\delta\mathbf{DTime}(n^k)$ iff there is $O(n^k)$-time algorithm A such that

$$\forall n \in \mathbb{N} \Pr_{x \in \{0,1\}^n}[A(x) = L(x)] > 1 - \delta.$$

FOLKLORE

For every $k > 0$ and $\epsilon > 0$ holds that

$$\mathbf{P} \not\subseteq \mathsf{Heur}_{1-\epsilon}\mathbf{DTime}(n^k).$$

Deterministic algorithms

HEURISTIC DETERMINISTIC ALGORITHM

Language $L \in \mathrm{Heur}_\delta\mathbf{DTime}(n^k)$ iff there is $O(n^k)$-time algorithm A such that

$$\forall n \in \mathbb{N} \Pr_{x\in\{0,1\}^n}[A(x) = L(x)] > 1 - \delta.$$

FOLKLORE

For every $k > 0$ and $\epsilon > 0$ holds that

$$\mathbf{P} \not\subseteq \mathrm{Heur}_{1-\epsilon}\mathbf{DTime}(n^k).$$

Bounded probabilistic algorithms

HEURISTIC BOUNDED PROBABILISTIC ALGORITHMS

Language $L \in \text{Heur}_\delta\mathbf{BPTime}(n^k)$ iff there is randomized $O(n^k)$-time algorithm A such that

$$\forall n \in \mathbb{N} \Pr_{x \in \{0,1\}^n}[\Pr[A(x) = L(x)] > \frac{3}{4}] > 1 - \delta.$$

We also denote $\text{Heur}_\delta\mathbf{BPP} = \bigcup_k \text{Heur}_\delta\mathbf{BPTime}(n^k)$

FORTNOW AND SANTHANAM, 2004

For each $k > 0$ there is $\epsilon > 0$ such that

$$\text{Heur}_\epsilon\mathbf{BPP} \not\subseteq \text{Heur}_\epsilon\mathbf{BPTime}(n^k).$$

Bounded probabilistic algorithms

HEURISTIC BOUNDED PROBABILISTIC ALGORITHMS

Language $L \in \text{Heur}_\delta\mathbf{BPTime}(n^k)$ iff there is randomized $O(n^k)$-time algorithm A such that

$$\forall n \in \mathbb{N} \Pr_{x \in \{0,1\}^n}[\Pr[A(x) = L(x)] > \frac{3}{4}] > 1 - \delta.$$

We also denote $\text{Heur}_\delta\mathbf{BPP} = \bigcup_k \text{Heur}_\delta\mathbf{BPTime}(n^k)$

FORTNOW AND SANTHANAM, 2004

For each $k > 0$ there is $\epsilon > 0$ such that

$$\text{Heur}_\epsilon\mathbf{BPP} \not\subseteq \text{Heur}_\epsilon\mathbf{BPTime}(n^k).$$

Bounded probabilistic algorithms

HEURISTIC BOUNDED PROBABILISTIC ALGORITHMS

Language $L \in \text{Heur}_\delta\textbf{BPTime}(n^k)$ iff there is randomized $O(n^k)$-time algorithm A such that

$$\forall n \in \mathbb{N} \Pr_{x \in \{0,1\}^n}[\Pr[A(x) = L(x)] > \frac{3}{4}] > 1 - \delta.$$

We also denote $\text{Heur}_\delta\textbf{BPP} = \bigcup_k \text{Heur}_\delta\textbf{BPTime}(n^k)$

PERVYSHEV, 2006

For each $k > 0$ and $\epsilon > 0$ holds that

$$\text{Heur}_\epsilon\textbf{BPP} \not\subseteq \text{Heur}_{\frac{1}{2}-\epsilon}\textbf{BPTime}(n^k).$$

Nondetermenistic algorithms

HEURISTIC NONDETERMENISTIC ALGORITHMS

Language $L \in \mathsf{Heur}_\delta\mathbf{NTime}(n^k)$ iff there is nondetermenistic $O(n^k)$-time algorithm A such that

$$\forall n \in \mathbb{N} \Pr_{x \in \{0,1\}^n}[A(x) = L(x)] > 1 - \delta.$$

PERVYSHEV, 2006

For each $k > 0$ and $\epsilon > 0$ holds that

$$\mathbf{NP} \not\subseteq \mathsf{Heur}_{\frac{1}{2}-\epsilon}\mathbf{NTime}(n^k).$$

Nondetermenistic algorithms

HEURISTIC NONDETERMENISTIC ALGORITHMS

Language $L \in \mathrm{Heur}_\delta\mathbf{NTime}(n^k)$ iff there is nondetermenistic $O(n^k)$-time algorithm A such that

$$\forall n \in \mathbb{N} \Pr_{x \in \{0,1\}^n}[A(x) = L(x)] > 1 - \delta.$$

PERVYSHEV, 2006

For each $k > 0$ and $\epsilon > 0$ holds that

$$\mathbf{NP} \not\subseteq \mathrm{Heur}_{\frac{1}{2}-\epsilon}\mathbf{NTime}(n^k).$$

State of art for heuristic hierarchies

FOLKLORE

For any $k > 0$ and $\epsilon > 0$ holds

$$\mathbf{P} \not\subseteq \mathrm{Heur}_{1-\epsilon}\mathbf{DTime}(n^k).$$

PERVYSHEV, 2006

For any $k > 0$ and $\epsilon > 0$ holds

$$\mathrm{Heur}_{\epsilon}\mathbf{BPP} \not\subseteq \mathrm{Heur}_{\frac{1}{2}-\epsilon}\mathbf{BPTime}(n^k) \text{ and}$$

$$\mathbf{NP} \not\subseteq \mathrm{Heur}_{\frac{1}{2}-\epsilon}\mathbf{NTime}(n^k).$$

Generalized hierarchy

ITSYKSON, KNOP, SOKOLOV, 2015

For any $k > 0$, $\epsilon > 0$ and $a > 1$ holds that

$$\mathsf{Heur}_{\epsilon}\mathbf{FBPP} \not\subseteq \mathsf{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{FBPTime}(n^k).$$

Moreover there is $F : \{0,1\}^n \to \{0,\ldots,b-1\}$ such that $F \in \mathsf{Heur}_{\epsilon}\mathbf{FBPP}$ and $F \notin \mathsf{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{FBPTime}(n^k)$.

Generalized hierarchy

ITSYKSON, KNOP, SOKOLOV, 2015

For any $k > 0$, $\epsilon > 0$ and $a > 1$ holds that

$$\mathsf{Heur}_\epsilon\mathbf{FBPP} \not\subseteq \mathsf{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{FBPTime}(n^k).$$

Moreover there is $F : \{0,1\}^n \to \{0,\dots,b-1\}$ such that $F \in \mathsf{Heur}_\epsilon\mathbf{FBPP}$ and $F \notin \mathsf{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{FBPTime}(n^k)$.

Samplable random variables

SAMPLABLE RANDOM VARIABLES

Ensemble of random variables $\gamma \in \mathbf{DSamp}(n^k)$ iff there is a randomized $O(n^k)$-time algorithm A such that γ_n and $A(1^n)$ are equally distributed. We also denote $\mathbf{PSamp} = \bigcup_k \mathbf{DSamp}(n^k)$.

WATSON, 2014

For any $k > 0$, $\epsilon > 0$ and $a > 1$ there is an ensemble of random variables $\gamma \in \mathbf{PSamp}$ such that for every $\beta \in \mathbf{DSamp}(n^k)$ holds $\Delta(\gamma, \delta) > 1 - \frac{1}{a} - \epsilon$ and $\mathrm{supp}(\gamma) = \{0, \ldots, a-1\}$.

Samplable random variables

SAMPLABLE RANDOM VARIABLES

Ensemble of random variables $\gamma \in \mathbf{DSamp}(n^k)$ iff there is a randomized $O(n^k)$-time algorithm A such that γ_n and $A(1^n)$ are equally distributed. We also denote $\mathbf{PSamp} = \bigcup\limits_k \mathbf{DSamp}(n^k)$.

WATSON, 2014

For any $k > 0$, $\epsilon > 0$ and $a > 1$ there is an ensemble of random variables $\gamma \in \mathbf{PSamp}$ such that for every $\beta \in \mathbf{DSamp}(n^k)$ holds $\Delta(\gamma, \delta) > 1 - \frac{1}{a} - \epsilon$ and $\mathrm{supp}(\gamma) = \{0, \ldots, a-1\}$.

Proof for $a = 2$

1. Consider the language $L = \{r \mid 0.r > \Pr[\gamma_n = 1]\}$.
2. Note that $L \in \text{Heur}_\epsilon\textbf{BPP}$.
   Consider the following algorithm:
   - Sample r_1, ..., r_m from γ_n;
   - Return 1 if $0.r \geq \frac{1}{m}\sum_{i=0}^{m} r_i$;
   - Return 0 in other case.
3. Note that $L \notin \text{Heur}_{1-\frac{1}{a}-\epsilon}\textbf{BPTime}(n^k)$.
   Let us assume the opposite that L are decidable by algorithm D and consider the following algorithm:
   - sample random $r \in \{0, 1\}^n$;
   - return 1 if $D(r) = 1$ else return 0.

Proof for $a = 2$

1. Consider the language $L = \{r \mid 0.r > \Pr[\gamma_n = 1]\}$.
2. Note that $L \in \mathsf{Heur}_\epsilon\mathbf{BPP}$.
   Consider the following algorithm:
   - Sample r_1, ..., r_m from γ_n;
   - Return 1 if $0.r \geq \frac{1}{m}\sum_{i=0}^{m} r_i$;
   - Return 0 in other case.
3. Note that $L \notin \mathsf{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{BPTime}(n^k)$.
   Let us assume the opposite that L are decidable by algorithm D and consider the following algorithm:
   - sample random $r \in \{0, 1\}^n$;
   - return 1 if $D(r) = 1$ else return 0.

Proof for $a = 2$

1. Consider the language $L = \{r \mid 0.r > \Pr[\gamma_n = 1]\}$.
2. Note that $L \in \text{Heur}_\epsilon\mathbf{BPP}$.
   Consider the following algorithm:
   - Sample r_1, ..., r_m from γ_n;
   - Return 1 if $0.r \geq \frac{1}{m}\sum_{i=0}^{m} r_i$;
   - Return 0 in other case.
3. Note that $L \notin \text{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{BPTime}(n^k)$.
   Let us assume the opposite that L are decidable by algorithm D and consider the following algorithm:
   - sample random $r \in \{0,1\}^n$;
   - return 1 if $D(r) = 1$ else return 0.

Proof for $a = 2$

1. Consider the language $L = \{r \mid 0.r > \Pr[\gamma_n = 1]\}$.
2. Note that $L \in \mathsf{Heur}_\epsilon\mathbf{BPP}$.
   Consider the following algorithm:
   - Sample r_1, ..., r_m from γ_n;
   - Return 1 if $0.r \geq \frac{1}{m}\sum_{i=0}^{m} r_i$;
   - Return 0 in other case.
3. Note that $L \notin \mathsf{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{BPTime}(n^k)$.
   Let us assume the opposite that L are decidable by algorithm D and consider the following algorithm:
   - sample random $r \in \{0,1\}^n$;
   - return 1 if $D(r) = 1$ else return 0.

Proof for $a = 2$

1. Consider the language $L = \{r \mid 0.r > \Pr[\gamma_n = 1]\}$.
2. Note that $L \in \mathrm{Heur}_{\epsilon}\mathbf{BPP}$.
   Consider the following algorithm:
   - Sample r_1, ..., r_m from γ_n;
   - Return 1 if $0.r \geq \frac{1}{m}\sum_{i=0}^{m} r_i$;
   - Return 0 in other case.
3. Note that $L \notin \mathrm{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{BPTime}(n^k)$.
   Let us assume the opposite that L are decidable by algorithm D and consider the following algorithm:
   - sample random $r \in \{0,1\}^n$;
   - return 1 if $D(r) = 1$ else return 0.

Proof for $a = 2$

1. Consider the language $L = \{r \mid 0.r > \Pr[\gamma_n = 1]\}$.
2. Note that $L \in \text{Heur}_\epsilon\textbf{BPP}$.
   Consider the following algorithm:
   - Sample r_1, ..., r_m from γ_n;
   - Return 1 if $0.r \geq \frac{1}{m}\sum\limits_{i=0}^{m} r_i$;
   - Return 0 in other case.
3. Note that $L \notin \text{Heur}_{1-\frac{1}{a}-\epsilon}\textbf{BPTime}(n^k)$.
   Let us assume the opposite that L are decidable by algorithm D and consider the following algorithm:
   - sample random $r \in \{0, 1\}^n$;
   - return 1 if $D(r) = 1$ else return 0.

Proof for $a = 2$

1. Consider the language $L = \{r \mid 0.r > \Pr[\gamma_n = 1]\}$.
2. Note that $L \in \mathrm{Heur}_\epsilon\mathbf{BPP}$.
   Consider the following algorithm:
   - Sample r_1, ..., r_m from γ_n;
   - Return 1 if $0.r \geq \frac{1}{m}\sum_{i=0}^{m} r_i$;
   - Return 0 in other case.
3. Note that $L \notin \mathrm{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{BPTime}(n^k)$.
   Let us assume the opposite that L are decidable by algorithm D and consider the following algorithm:
   - sample random $r \in \{0,1\}^n$;
   - return 1 if $D(r) = 1$ else return 0.

Proof for $a = 2$

1. Consider the language $L = \{r \mid 0.r > \Pr[\gamma_n = 1]\}$.
2. Note that $L \in \text{Heur}_\epsilon\mathbf{BPP}$.
   Consider the following algorithm:
   - Sample r_1, ..., r_m from γ_n;
   - Return 1 if $0.r \geq \frac{1}{m}\sum_{i=0}^{m} r_i$;
   - Return 0 in other case.
3. Note that $L \notin \text{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{BPTime}(n^k)$.
   Let us assume the opposite that L are decidable by algorithm D and consider the following algorithm:
   - sample random $r \in \{0, 1\}^n$;
   - return 1 if $D(r) = 1$ else return 0.

Proof for $a = 2$

1. Consider the language $L = \{r \mid 0.r > \Pr[\gamma_n = 1]\}$.
2. Note that $L \in \mathrm{Heur}_{\epsilon}\mathbf{BPP}$.
   Consider the following algorithm:
   - Sample r_1, ..., r_m from γ_n;
   - Return 1 if $0.r \geq \frac{1}{m}\sum_{i=0}^{m} r_i$;
   - Return 0 in other case.
3. Note that $L \notin \mathrm{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{BPTime}(n^k)$.
   Let us assume the opposite that L are decidable by algorithm D and consider the following algorithm:
   - sample random $r \in \{0, 1\}^n$;
   - return 1 if $D(r) = 1$ else return 0.

Open questions

- Hierarchy theorem for **BPTime**(n^k) or **RTime**(n^k);
- Hierarchy theorem for heuristic version of **RTime**(n^k);
- Prove hierarchy for heuristic version of **BPTime**(n^k) for bigger confidence parameter.

Open questions

- Hierarchy theorem for **BPTime**(n^k) or **RTime**(n^k);
- Hierarchy theorem for heuristic version of **RTime**(n^k);
- Prove hierarchy for heuristic version of **BPTime**(n^k) for bigger confidence parameter.

Open questions

- Hierarchy theorem for **BPTime**(n^k) or **RTime**(n^k);
- Hierarchy theorem for heuristic version of **RTime**(n^k);
- Prove hierarchy for heuristic version of **BPTime**(n^k) for bigger confidence parameter.