Abstract

Our main claim in the first version of this archive paper was that unconditionally there exists a promise problem in promise $\text{ZSUBEXP}$ that cannot be solved in promise $\text{RP}$. We proved this building upon Kabanets’ easy witness method [Kab01] as implemented by Impagliazzo et. al [IKW02], with a separate diagonalization carried out on each of the two alternatives in the win-win argument. Rahul Santhanam showed us a very simple proof that proves a stronger claim. In this revision we give this proof.

1 The simple proof

The following theorem and simple proof were communicated to us by Rahul Santhanam.

**Theorem 1.** Let $T, t : \mathbb{N} \to \mathbb{N}$ be functions such that \( \text{Pr–ZTime}(T(n)) \not\subseteq \text{Pr–ZTime}(O(t(n))) \). Then $\text{Pr–ZTime}(T(n)) \not\subseteq \text{Pr–RTime}(O(t(n)))$.

**Proof.** Suppose $\text{Pr–ZTime}(T(n)) \subseteq \text{Pr–RTime}(O(t(n)))$. Then also

\[ \text{co–Pr–ZTime}(T(n)) \subseteq \text{co–Pr–RTime}(O(t(n))). \]

But $\text{Pr–ZTime}(T(n))$ is closed under complement. Hence,

\[ \text{Pr–ZTime}(T(n)) \subseteq \text{Pr–RTime}(O(t(n)) \cap \text{co–Pr–RTime}(O(t(n))) = \text{Pr–ZTime}(O(t(n))), \]

in contradiction to the hypothesis of the theorem. \hfill \Box

A similar claim holds for $\text{RTime}$ without the promise and for $\text{Pr–ZNTime}(t) = \text{Pr–NTime}(t) \cap \text{Pr–coNTime}(t)$. In particular:

**Corollary 2.**

- $\text{Pr–ZTime}(T(n)) \not\subseteq \text{Pr–RTime}(t(n))$ and $\text{Pr–ZNTime}(T(n)) \not\subseteq \text{Pr–NTime}(t(n))$ for any time-constructible $T$ such that $T(n) = w(t(n + 1) \log t(n + 1))$.

- $\text{ZTime}(T(n)) \not\subseteq \text{RP}$ and $\text{ZNTime}(T(n)) \not\subseteq \text{NP}$ for any time-constructible $T$ such that $T^{(c)}(n) = 2^{w(n)}$, where $T^{(c)}(n)$ is the composition of $T$ with itself $c$ times (see [page 195][Bar02] where it is attributed to [KV87]). In particular $\text{ZSUBEXP} \not\subseteq \text{RP}$ and $\text{ZNSUBEXP} \not\subseteq \text{NP}$.

---

*The Blavatnik School of Computer Science, Tel-Aviv University, Israel 69978. Supported by the Israel Science Foundation grant no. 952/18.
†Department of Computer Science, University of Oxford, Oxford*
Figure 1: In blue, the $\text{Pr-ZNTime}$ hierarchy is depicted between $\text{Pr-ZNP}$ and $\text{Pr-ZNEXP}$. $\text{Pr-NP}$ is depicted in red under the assumption that $\text{SAT} \not\in \text{coNTime}(2^{o(n)})$. $\text{SAT}$ appears as the red dot high in the hierarchy. On the other hand by Corollary 2 no full layer of $\text{Pr-ZNTime}(T)$ is contained in $\text{Pr-NP}$ for $T = n^{\omega(1)}$.

We thank Rahul for communicating the stronger claim and corollaries and the much simpler proofs to us.

References


