$\Pr-\mathsf{ZSUBEXP} \not\subseteq \Pr-\mathsf{RP}$

Gonen Krak * Noam Parzanchevski * Rahul Santhanam † Amnon Ta-Shma *

Abstract

Our main claim in the first version of this archive paper was that unconditionally there exists a promise problem in promise ZSUBEXP that cannot be solved in promise 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* $\Pr-\mathsf{ZTime}(T(n)) \not\subseteq \Pr-\mathsf{ZTime}(O(t(n))$. *Then* $\Pr-\mathsf{ZTime}(T(n)) \not\subseteq \Pr-\mathsf{RTime}(O(t(n))$.

Proof. Suppose $\Pr-\mathsf{ZTime}(T(n)) \subseteq \Pr-\mathsf{RTime}(O(t(n))$. Then also

$$co-\Pr-\mathsf{ZTime}(T(n)) \subseteq co-\Pr-\mathsf{RTime}(O(t(n)).$$

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

$$\Pr-\mathsf{ZTime}(T(n)) \subseteq \Pr-\mathsf{RTime}(O(t(n)) \cap co-\Pr-\mathsf{RTime}(O(t(n)) = \Pr-\mathsf{ZTime}(O(t(n)),$$

in contradiction to the hypothesis of the theorem. □

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

Corollary 2.

- $\Pr-\mathsf{ZTime}(T(n)) \not\subseteq \Pr-\mathsf{RTime}(t(n))$ *and* $\Pr-\mathsf{ZNTime}(T(n)) \not\subseteq \Pr-\mathsf{NTime}(t(n))$ *for any time-constructible T such that $T(n) = w(t(n+1)\log t(n+1))$.*
- $\mathsf{ZTime}(T(n)) \not\subseteq \mathsf{RP}$ *and* $\mathsf{ZNTime}(T(n)) \not\subseteq \mathsf{NP}$ *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* ZSUBEXP $\not\subseteq$ RP *and* ZNSUBEXP $\not\subseteq$ 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

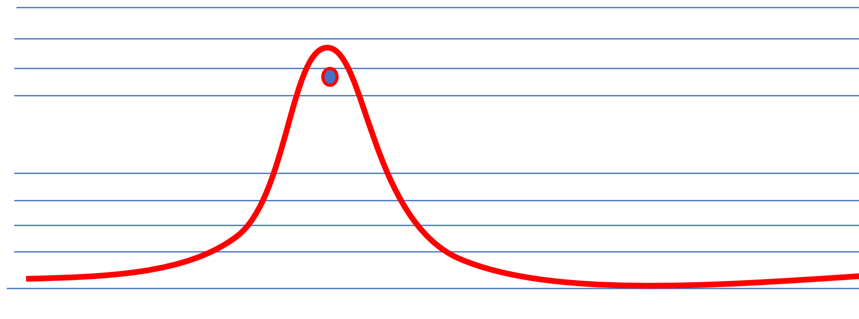

Figure 1: In blue, the $\Pr-\mathsf{ZNTime}$ hierarchy is depicted between $\Pr-\mathsf{ZNP}$ and $\Pr-\mathsf{ZNEXP}$. $\Pr-\mathsf{NP}$ is depicted in red under the assumption that $SAT \notin co\mathsf{NTime}(2^{o(n)})$. SAT appears as the red dot high in the hierarchy. On the other hand by Corollary 2 no full layer of $\Pr-\mathsf{ZNTime}(T)$ is contained in $\Pr-\mathsf{NP}$ for $T = n^{w(1)}$.

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

References

[Bar02] Boaz Barak. A probabilistic-time hierarchy theorem for slightly non-uniform algorithms. In *International Workshop on Randomization and Approximation Techniques in Computer Science*, pages 194–208. Springer, 2002. 1

[IKW02] Russell Impagliazzo, Valentine Kabanets, and Avi Wigderson. In search of an easy witness: Exponential time vs. probabilistic polynomial time. *Journal of Computer and System Sciences*, 65(4):672–694, 2002. 1

[Kab01] Valentine Kabanets. Easiness assumptions and hardness tests: Trading time for zero error. *Journal of Computer and System Sciences*, 63(2):236–252, 2001. 1

[KV87] Marek Karpinski and Rutger Verbeek. Randomness, provability, and the separation of monte carlo time and space. In *Computation Theory and Logic*, pages 189–207. Springer, 1987. 1