AIT Blog

Two Resource Bounded EL Theorems

Samuel Epstein*

October 25, 2022

In my blog on October 9th, I mentioned that one open problem is a resource bounded version of the Sets Have Simple Members Theorem [Eps19, Lev16]. In fact there are two such resource bounded EL theorems that can be derived almost directly from the literature. The first result is a corollary to Theorem 30 in [LOZ22]. The second result is a corollary to Theorem 4.1 in [AF09]. I'll also show how the first result can be applied to derandomization, in the sense of [Eps22b, Eps22a], to produce a resource bounded derandomization. The following definition is known as the probabilistic t-bounded Kolmogorov complexity.

Result One

Definition 1 ([LOZ22])

$$\mathrm{pK}^t(x) = \min\left\{k \;\middle|\; \Pr_{w\sim\{0,1\}^{t(|x|)}}\left[\exists \mathcal{M}\in\{0,1\}^k, \mathcal{M}(w) \text{ outputs } x \text{ within } t(|x|) \text{ steps}\right] \geq \frac{2}{3}\right\}.$$

Using this definition, the following theorem was proven.

Theorem 1 ([LOZ22]) *Suppose there is a randomized algorithm A for sampling strings such that $A(1^n)$ runs in time $T(n)\geq n$ and outputs a string $x\in\{0,1\}^n$ with probability at least $\delta>0$. Then*

$$\mathrm{pK}^t(x) = \log(1/\delta) + O(\log T(n)),$$

where $t(n)=\mathrm{poly}(T(n))$ and the the constant $O(\cdot)$ depends on $|A|$ and is independent of the remaining parameters.

The advantage to the above theorem is that is unconditional, not requiring crypographic assumptions. If $k=\mathrm{pK}^t(x)$, if two parties share a typical random string w, x can be transmitted with k bits and decompressed in time $\mathrm{poly}(|x|)$. The proof of the above theorem can be readily extended to sets of strings. The above definition can be reformulated into the resources bounded complexity of sets.

Definition 2 (Probabilistic t-bounded Kolmogorov complexity(Sets))

$$\mathrm{pK}^t(D) = \min\left\{k : \Pr_{w\sim\{0,1\}^{t(|x|)}}\left[\exists \mathcal{M}\in\{0,1\}^k, \mathcal{M}(w) \text{ outputs } x\in D \text{ within } t(|x|) \text{ steps}\right] \geq \frac{2}{3}\right\}.$$

*JP Theory Group. samepst@jptheorygroup.org

Corollary 1 *Suppose there is a randomized algorithm A for sampling strings such that $A(1^n)$ runs in time $T(n)$ and outputs a string $x \in D \subseteq \{0,1\}^n$ with probability at least $\delta > 0$. Then*

$$\mathrm{pK}^t(D) = \log(1/\delta) + O(\log T(n)),$$

where $t(n) = \mathrm{poly}(T(n))$ and the constants depends on $|A|$ and is independent of the rest of the parameters.

Result Two

Another avenue to explore can be found in [AF09], using the *t-time-bounded Kolmogorov complexity.*

Definition 3

$$\mathrm{K}^t(x) = \min_{\mathrm{TM},\mathcal{M}} \{|\mathcal{M}| + : \mathcal{M} \text{ outputs } x \text{ in at most } t(|x|) \text{ steps.}\}$$

In [AF09], in the proof of Theorem 4,1, a coding theorem was used using resourced bounded complexity. The implications of this was shown in Theorem 20 of [LOZ22]. Let **Crypto** be the assumption that **E** is not contained in $\mathbf{DSPACE}(2^{\epsilon n})$ for some $\epsilon > 0$ and infinitely many n.

Theorem 2 ([AF09]) *Assume **Crypto**. Suppose there is an polynomial time algorithm A such that $A(1^n)$ outputs a string $x \in \{0,1\}^n$ with probability at least $\delta > 0$. Then for some polynomial p dependent on A,*

$$\mathrm{K}^p(x) \leq \log(1/\delta) + O(\log n).$$

To generalize to sets, an extra assumption needs to be made, because otherwise, let $D \subset \{0,1\}^n$ be all random strings of size n. We define the sampler A produce the uniform distribution over $\{0,1\}^n$. Thus $\min_{x \in D} \mathrm{K}^p(x) \leq -\log 1/2 + O(\log n)$, which is incorrect. The assumption made is that there exists a polynommial time algorithm that can test membership to the set D in question. The following corollary follows almost directly from the above theorem. Generally speaking, it states that sets that are efficently decidable and easily sampleable have efficiently compressible members. It remains to be seen if the **Crypto** assumption is needed.

Corollary 2 *Assume **Crypto**. Let $L \in \mathrm{P}$. Suppose there is a polynomial time algorithm A such that $A(1^n)$ outputs a member of L_n with probability $\delta_n > 0$. Then for some polynomial p,*

$$\min_{x \in L_n} \mathrm{K}^p(x) \leq \log(1/\delta_n) + O(\log n).$$

Resource Bounded Derandomization

Corollary 1 is immediately compatible with derandomization, in the sense of [Eps22b, Eps22a]. This proves the existence of a means to succinctly transmit solutions of instances of problems that can be efficiently decompressed.

This property can be described using a protocol between Alice and Bob. They share a typical random string of size poly(n). Alice has access to an instance of the Vertex Coloring, which is the number of colors k and an undirected graph $G = (V, E)$, $|V| = n$, of max degree $d < k/2$. The probability that a random coloring (under uniform randomness) is correct is $\geq (1 - d/k)^n$. Thus Alice gives Bob a string of size $2nd/k + O(\log nk)$, for which Bob can run in time poly(n) and produce a graph coloring with probability $2/3$. Put another way, using G defined earlier,

$$\mathrm{pK}^t(\{x : x \text{ is a } k \text{ coloring of } G\}) = 2nd/k + O(\log nk).$$

References

[AF09] L. Antunes and L. Fortnow. Worst-case running times for average-case algorithms. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 298–303, 2009.

[Eps19] S. Epstein. On the algorithmic probability of sets. *CoRR*, abs/1907.04776, 2019.

[Eps22a] S. Epstein. 22 examples of solution compression via derandomization. *CoRR*, abs/2208.11562, 2022.

[Eps22b] S. Epstein. The outlier theorem revisited. *CoRR*, abs/2203.08733, 2022.

[Lev16] L. A. Levin. Occam bound on lowest complexity of elements. *Annals of Pure and Applied Logic*, 167(10):897–900, 2016.

[LOZ22] Z. Lu, I. Oliveira, and M. Zimand. Optimal coding theorems in time-bounded kolmogorov complexity. *CoRR*, abs/2204.08312, 2022.