# AIT Blog

## Certificates and Inverting Hash Functions

Samuel Epstein*

November 6, 2022

This blog entry covers applications of a resource bounded version of the Sets Have Simple Members Theorem. Sufficient conditions for the efficient compression of proofs is given. We show that the pre-image of a simple element with respect to a hash function contains an element that is simple with respect to resource bounded Kolmogorov complexity. For my survey, I've decided to change it to a paper, focusing on the Sets Have Simple Members Theorem and its applications. More specifically, the application is derandomization in the context of bounded and unbounded resources. The contents are as followed.

1. New Proof to Sets Have Simple Members Theorem
2. Resource Bounded EL Theorem (From [AF09])
3. Resource Free Derandomization - Codebook Compression Size vs. Capacity Tradeoff
4. Resource Bounded Derandomization - Certificate Compression

In my October 25th blog, I stated the following result, which follows almost directly from the proof of Theorem 4.1 in [AF09]. Let **Crypto** be the assumption that **E** is not contained in **DSPACE**$(2^{\epsilon n})$ for some $\epsilon > 0$ and infinitely many $n$. There are several variants of resouce bounded complexity. In the following definition, the running time of universal Turing machine is taken into account.

**Definition 1** *For function $t$, the time-bounded Kolmogorov complexity is* $\mathbf{K}^t(x) = \min\{\|p\| : U(p) = x \text{ in } t(\|x\|) \text{ steps}\}$.

**Theorem 1** *Assume **Crypto**. Let $L \in$ 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 $p$,* $\min_{x \in L_n} \mathbf{K}^p(x) < \log(1/\delta_n) + O(\log n)$.

Generally speaking, the following corollary states that if an efficiently generatable string has a good change of producing a random certificate with respect to an NP language, then the string has a simple proof.

**Corollary 1** *Assume **Crypto**. Let $\{x_n\}$ be uniformly computable in polynomial time, where $\|x_n\| = n$. Fix a language in* NP. *There is a polynomial $p$ where if a random proof for $x_n$ has success rate $\gamma_n$,*

$$\min_{y \in \text{Proofs}(x_n)} \mathbf{K}^p(y) < -\log \gamma_n + O(\log \|y\|).$$

*JP Theory Group. samepst@jptheorygroup.org

The following corollary shows that every efficiently computable sequence of strings have hash function pre-images that contain an efficiently compressible member.

**Corollary 2** *Assume **Crypto**. Let $\{x_n\}$ be a uniformly polynomial time sequence and $\|x_n\| = n$. Let $f$ be a polynomial time hash function, where $\|f(x)\| = \|x\| - k$. There is a polynomial $p$ where for $D = f^{-1}(x_n)$,*

$$\min_{y \in D} \mathbf{K}^p(y) = n + k - \log |D| + O(\log(n+k)).$$

It would be of interest to see if the generatable sequence requirement in the above corollary could be removed. This would entail revisiting Theorem 4.1 in [AF09], and changing the sampling function to a hash function. If it is true it means that to invert $x$ with $f$, one can find a secret key $\pi$ of size approximately equal to $x$ that efficiently expands to an element in $f^{-1}(x)$.

**Corollary 3** *Assume **Crypto**. Let $f$ be a polynomial time function, where $f(\{0,1\}^n) \subseteq \{0,1\}^{n-k}$. There is a polynomial $p$ where for $\{0,1\}^n \supseteq D = f^{-1}(x)$,*

$$\min_{y \in D} \mathbf{K}^p(y) = n - \log |D| + O(\log n).$$

The following corollary is a resource bounded version of SAT derandomization, which is Theorem 4 in [Eps22]. This Theorem 4 uses Lovasz Local Lemma to achieve its bounds. The following corollary states that if simple SAT formulas have variables that do not appear in too many clauses, then they will admit efficiently compressible solutions.

**Corollary 4** *Assume **Crypto**. Let $\Phi_n$ be a $k(n)$-SAT formula, using $n$ variables, $m(n)$ clauses, uniformly polynomial time computable in $n$. Furthermore, each variable occurs in at most $2^{k(n)}/e-1$ clauses. There is a polynomial $p$ where*

$$\min_{x \text{ satisfies } \Phi_n} \mathbf{K}^p(x) < 2m(n)e2^{-k(n)} + O(\log n).$$

In fact many of the derandomization examples in [Eps22] can be converted to resource bounded versions, however in some cases, the result is trivial. So far, resource bounded games only derandomize to trivial examples. Thus it is an open question if given a non-trivial polynomial time environment, there is a player with low resource bounded Kolmogorov complexity that could do well against it. We show one more example of resource bounded derandomization.

**Corollary 5** *Assume **Crypto.** Let $\{G_n\}$ be a uniformly polynomial time computable sequence of $k$-regular graphs. There is a polynomial $p$ where for each $G_n$, there is a partition $x$ of $\lfloor \frac{k}{3 \ln k} \rfloor$ components each containing a cycle with complexity*

$$\mathbf{K}^p(x) < 2n/k^2 + O(\log n).$$

## 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.

[Eps22] S. Epstein. 22 examples of solution compression via derandomization. *CoRR*, abs/2208.11562, 2022.