

# AIT Blog

## On Creating Pairs of Derandomization Theorems

Samuel Epstein\*

November 14, 2022

I've uploaded a new paper to my site, with the intention of eventually uploading it to arXiv and submission for publication. The main contribution is a resource bounded EL Theorem and a general formula for resource bounded randomization, in the sense of [Eps22]. In this blog, I show an example of taking theorem produced from non-constructive probabilistic proof and producing a pair of derandomization theorems, one that is resource free and one that is resource bounded.

A *hypergraph* is a pair  $J = (V, E)$  of vertices  $V$  and edges  $E \subseteq \mathcal{P}(V)$ . Thus each edge can connect  $\geq 2$  vertices. A hypergraph is *k-uniform* if the size  $|e| = k$  for all edges  $e \in E$ . A 2-uniform hypergraph is just a simple graph. A valid *C-coloring* of a hypergraph  $(V, E)$  is a mapping  $f : V \rightarrow \{1, \dots, C\}$  where every edge  $e \in E$  is not *monochromatic*  $|\{f(v) : v \in e\}| > 1$ . The following classic result uses Lovasz Local Lemma.

**Theorem. [Probabilistic Method]** *Let  $G = (V, E)$  be a  $k$ -regular hypergraph. If for each edge  $f$ , there are at most  $2^{k-1}/e - 1$  edges  $h \in E$  such that  $h \cap f \neq \emptyset$ , then there exists a valid 2-coloring of  $G$ .*

We can now use derandomization, in the sense of [Eps22], to produce bounds on the Kolmogorov complexity of the simplest such 2-coloring of  $G$ .

**Theorem. [Derandomization]** *Let  $G = (V, E)$  be a  $k$ -regular hypergraph. If, for each edge  $f$ , there are at most  $2^{k-1}/e - 1$  edges  $h \in E$  such that  $h \cap f \neq \emptyset$ , then there exists a valid 2-coloring  $x$  of  $G$  with*

$$\mathbf{K}(x) <^{\log} \mathbf{K}(n, k) + ne/2^{k-1} + \mathbf{I}(G; \mathcal{H}).$$

The function  $\mathbf{K}$  is the prefix free Kolmogorov complexity.  $\mathbf{I}(G; \mathcal{H}) = \mathbf{K}(G) - \mathbf{K}(G|\mathcal{H})$  is the amount of asymmetric information the halting sequence  $\mathcal{H} \in \{0, 1\}^\infty$  has about the graph  $G$ . We can now use resource derandomization, introduced in <http://www.jptheorygroup.org/doc/Resource.pdf>, to achieve bounds for the smallest time-bounded Kolmogorov complexity  $\mathbf{K}^t(x) = \min\{p : U(p) = x \text{ in } t(\|x\|) \text{ steps}\}$  of a 2-coloring of  $G$ . **Crypto** is the assumption that there exists a language in  $\mathbf{DTIME}(2^{O(n)})$  that does not have size  $2^{o(n)}$  circuits with  $\Sigma_2^p$  gates.

---

\*JP Theory Group. samepst@jptheorygroup.org

**Theorem.** [Resource Bounded Derandomization] Assume *Crypto*. Let  $G_n = (V, E)$  be a  $k$ -regular hypergraph where  $\|V\| = n$ , uniformly polynomial time computable in  $n$ . Furthermore, for each edge  $f$  in  $G_n$  there are at most  $2^{k-1}/e - 1$  edges  $h \in E$  such that  $h \cap f \neq \emptyset$ . Then there is a polynomial  $p$ , and a valid 2-coloring  $x$  of  $G_n$  with

$$\mathbf{K}^p(x) < ne/2^{k-1} + O(\log n).$$

## References

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