

Pseudo-Random Generators for All Hardnesses *

Christopher Umans
Microsoft Research
One Microsoft Way
Redmond, WA 98052
umans@microsoft.com

1. Abstract

A *pseudo-random generator* (PRG) is a function that “stretches” a short random seed into a longer *pseudo-random* output string that “fools” small circuits:

Definition 1 (ϵ -PRG) An ϵ -PRG for size s is a function $G : \{0, 1\}^t \rightarrow \{0, 1\}^m$ such that for all circuits C of size at most s :

$$|\Pr_z[C(G(z)) = 1] - \Pr_x[C(x) = 1]| \leq \epsilon.$$

PRGs entail hard functions, so (in the absence of strong circuit lower bounds) they are constructed using the assumption that hard functions exist. They can therefore be seen as objects that convert computational hardness into pseudo-randomness. We construct the first pseudo-random generators with logarithmic seed length that convert s bits of hardness into $s^{\Omega(1)}$ bits of 2-sided pseudo-randomness for any s . Specifically, we prove the following theorem:

Theorem 1 (main) Given a function

$$f : \{0, 1\}^{\log n} \rightarrow \{0, 1\}$$

with circuit complexity at least s , one can construct a $1/m$ -PRG $G : \{0, 1\}^{O(\log n)} \rightarrow \{0, 1\}^m$ for size m circuits with $m = s^{\Omega(1)}$; moreover, G can be computed in $n^{O(1)}$ time with oracle access to f .

This improves [1] (in which $m = s^{\Omega(1/\log \log \log n)}$) and gives a direct proof of the optimal hardness vs. randomness tradeoff in [2], which can be stated as follows:

Theorem 2 ([2]) If there exists a function family $f = \{f_n\}$ in E with circuit complexity at least $s(n)$, then

$$BPTIME(\ell) \subseteq DTIME(2^{O(s^{-1}(\ell^{O(1)}))}).$$

*The conference version of this abstract appears in the *Proceedings of STOC 2002*, May 19–21, 2002, Montreal, Quebec, Canada.

Theorem 1 also shows in a precise sense the *equivalence* (up to a polynomial) between computational hardness and 2-sided pseudo-randomness, something that was not known previously.

A key element in our construction is an augmentation of the standard low-degree extension encoding that exploits the field structure of the underlying space in a new way. This builds on ideas used in the new algebraic PRG construction of [2], and it is possible that some of the algebraic structure that we exploit may be helpful in improving the extractor constructions in that paper, which use the same framework. Indeed, the PRG construction in this paper yields extractors via the connection between extractors and certain PRGs noticed by Trevisan [4]. It remains an open problem to construct optimal extractors, and the new techniques of [3] and [2] may be able to be pushed further with additional insight into the algebraic structure of these constructions; we hope some of the ideas in this paper can be useful to this end.

References

- [1] R. Impagliazzo, R. Shaltiel, and A. Wigderson. Extractors and pseudo-random generators with optimal seed-length. In *Proceedings of the Thirty-second Annual ACM Symposium on the Theory of Computing*, 21–23 May 2000.
- [2] R. Shaltiel and C. Umans. Simple extractors for all min-entropies and a new pseudo-random generator. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, 2001.
- [3] A. Ta-Shma, D. Zuckerman, and S. Safra. Extractors from Reed-Muller codes. In *Proceedings of the 42th Annual IEEE Symposium on Foundations of Computer Science*, 2001.
- [4] L. Trevisan. Construction of extractors using pseudorandom generators. In *Proceedings of the 31st ACM Symposium on Theory of Computing*, 1999.