Improved Pseudorandom Generators for Depth 2 Circuits

Anindya De1,⋆; Omid Etesami1,⋆⋆, Luca Trevisan2,⋆⋆⋆, and Madhur Tulsiani3,†

1 University of California at Berkeley
{anindya,etesami}@cs.berkeley.edu
2 University of California at Berkeley and Stanford University
luca@cs.berkeley.edu
3 Institute for Advanced Study, Princeton
madhurt@math.ias.edu

Abstract. We prove the existence of a poly(n, m)-time computable pseudorandom generator which “1/poly(n, m)-fools” DNFs with n variables and m terms, and has seed length O(log² nm · log log nm). Previously, the best pseudorandom generator for depth-2 circuits had seed length O(log³ nm), and was due to Bazzi (FOCS 2007).

It follows from our proof that a 1/m^{O(log mn)}-biased distribution 1/poly(nm)-fools DNFs with m terms and n variables. For inverse polynomial distinguishing probability this is nearly tight because we show that for every m, δ there is a 1/m^{Ω(log 1/δ)}-biased distribution X and a DNF φ with m terms such that φ is not δ-fooled by X.

For the case of read-once DNFs, we show that seed length O(log mn · log 1/δ) suffices, which is an improvement for large δ.

It also follows from our proof that a 1/m^{O(log 1/δ)}-biased distribution δ-fools all read-once DNF with m terms. We show that this result too is nearly tight, by constructing a 1/m^{Ω(log 1/δ)}-biased distribution that does not δ-fooled a certain m-term read-once DNF.

Keywords: DNF, pseudorandom generators, small bias spaces.

1 Introduction

One of the main open questions in unconditional pseudorandomness and derandomization is to construct logarithmic-seed pseudorandom generators that “fool”...
bounded-depth circuits. Ajtai and Wigderson first considered the problem of pseudorandomness against bounded-depth circuits, and constructed a pseudorandom generator against $AC^0$ with a seed of length $O(n^\varepsilon)$ for any $\varepsilon > 0$. This was substantially improved by Nisan, who used the hardness of parity against $AC^0$ to construct a pseudorandom generator against depth $d$ circuits with a seed of length $O(\log^{2d+6} n)$. This remains the best known result for $AC^0$.

Even for depth-2 circuits, the construction of optimal pseudorandom generators remains a challenging open question. A depth-2 circuit is either a CNF or a DNF formula, and a pseudorandom generator that fools DNFs must also fool CNFs with the same distinguishing probability, so from now on we will focus without loss of generality on DNFs, and denote by $n$ the number of variables and $m$ the number of terms.

Nisan’s result quoted above gives a pseudorandom generator for DNFs with seed length $O(\log^{10} nm)$. Luby, Velickovic and Wigderson reduced the seed length to $O(\log^4 nm)$ via various optimizations. For the simpler task of approximating the number of satisfying assignments to a DNF formula, Luby and Velickovic provide a deterministic algorithm running in time $(m \log n)^{\exp(O(\sqrt{\log \log m}))}$. The current best pseudorandom generator for DNFs is due to Bazzi. In 1990, Linial and Nisan conjectured that depth-$d$ circuits are fooled by every distribution that is $(\log nm)^{O_d(1)}$-wise independent. Bazzi proved the depth-2 case of the Linial-Nisan conjecture, and showed that every $O(\log^2 (m/\delta))$-wise independent distribution $\delta$-fools DNFs. This result gives two approaches to constructing a pseudorandom generator for DNFs of seed length $O(\log n \cdot \log^{2w} (m/\delta))$, which is $O(\log^3 nm)$ when $\delta = 1/poly(n, m)$. One is to use one of the known constructions of $k$-wise independent generators of seed length $O(k \log n)$. The other is to use a result of Alon, Goldreich and Mansour showing that every $\epsilon$-biased distribution, in the sense of Naor and Naor, over $n$ bits is $\epsilon n^k$-close to a $k$-wise independent distribution. This means that, because of Bazzi’s theorem, every $\exp(-O(\log n \cdot \log^2 (m/\delta)))$-biased distribution fools DNFs; Naor and Naor prove that an $\epsilon$-biased distribution over $n$ bits can be sampled using a seed of $O(\log(n/\epsilon))$ random bits, and so a $\exp(-O(\log n \cdot \log^2 (m/\delta)))$-biased distribution can be sampled using $O(\log n \cdot \log^2 (m/\delta))$ random bits.

Razborov considerably simplified Bazzi’s proof (retaining the same quantitative bounds). In a recent breakthrough, building on Razborov’s argument, Braverman has proved the full Linial-Nisan conjecture.

For width-$w$ DNF formulas, better bounds are known for small $w$. Luby and Velickovic prove the existence of a generator with seed length $O(\log n + w^2 \log 1/\delta)$ which $\delta$-fools all width-$w$ DNFs. It follows from their proof that

---

1. We say that a random variable $X$, ranging over $\{0, 1\}^n$, “$\delta$-fools” a function $f : \{0, 1\}^n \to \mathbb{R}$ if

$$|E_X f(X) - E_{U_n} f(U_n)| \leq \delta,$$

where $U_n$ is uniformly distributed over $\{0, 1\}^n$. If $\mathcal{C}$ is a class of functions, then we say that $X$ $\delta$-fools $\mathcal{C}$ if $X$ $\delta$-fools every function $f \in \mathcal{C}$.  

2. Each term involves at most $w$ variables.