Electronic Colloquium on Computational Complexity, Report No. 94 (2026)

Seven observations about weighted pseudorandom generators

Dean Doron* Oded Goldreich†

June 4, 2026

Abstract

Weighted pseudorandom generators (wPRGs) were suggested by Braverman, Cohen, and Garg (*STOC*, 2018) as a relaxation of pseudorandom generator (PRG) used for derandomization. We present proofs of several observations regarding wPRGs, where some of these observations are well known.

Preface

In the context of "derandomization-oriented" pseudorandom generators, the verdict of a randomized decision procedure D is emulated by a deterministic algorithm that invokes a "pseudorandom generator" on all possible seeds, and rules according to the average value of D on the corresponding pseudorandom outcomes. When using this strategy for derandomizing a randomized-time (resp., randomized-space) complexity class it is reasonable to allow the generator, called a "canonical derandomizer" in [5, Sec. 8.3], to run in exponential-time (resp., linear-space).

As observed by Braverman, Cohen, and Garg [1], in the context of using this derandomization strategy, using a weighted average (rather than a standard (unweighted) average) is just as good. Furthermore, it seems that this relaxation is beneficial [8, 2, 3], provided that one also uses negative weights. In contrast, it is known that non-negative weights give no benefit.

In this memo, we present a proof of the foregoing folklore as well as present a few other observations about wPRGs.

Preliminaries

A weighted pseudorandom generator (wPRG), denoted (G, ω), is obtained by augmenting a standard pseudorandom generator (PRG) $G : \{0,1\}^k \to \{0,1\}^n$, where $k < n$, with a weight function $\omega : \{0,1\}^k \to \mathbb{R}$. We say that a wPRG (G, ω) fools (or ϵ-fools) the distinguisher D if

$$\mathrm{E}_{s\in\{0,1\}^k}[\omega(s) \cdot D(G(s))] = \mathrm{E}_{u\in\{0,1\}^n}[D(u)] \pm \epsilon. \tag{1}$$

In particular, if (G, ω) fools (i.e., ϵ-fools) a class of distinguishers that contains the all-1 function, then $\mathrm{E}_s[\omega(s)] \approx 1$ (i.e., $\mathrm{E}_s[\omega(s)] = 1 \pm \epsilon$). Actually, recalling that wPRGs are used for derandomization and so scanning all seeds is feasible, we may assume (w.l.o.g.) that the average weight is exactly 1 (because we can compute $\nu \leftarrow \mathrm{E}_s[\omega(s)]$ and normalize the original weights by ν).

*Stein Faculty of Computer and Information Science, Ben-Gurion University of the Negev, Israel.
†Department of Computer Science, Weizmann Institute of Science, Rehovot, Israel.

ISSN 1433-8092

In general, when making "w.l.o.g assertions" about wPRGs, we allow for (1) increasing the seed length (i.e., k) by a constant factor, (2) increasing the deviation (i.e., ϵ) by raising it to a (positive) constant power, (3) increasing the space complexity (of computing the wPRG) by an additive amount that is linear in the seed-length, and (4) increasing the time complexity by a factor that is exponential in the seed-length. We shall also assume that $\epsilon \geq 2^{-k}$, and that ϵ is at most a sufficiently small constant.

In the context of derandomization, the standard definition of a distinguisher is that it is a function (computable within some complexity class) that outputs a verdict in $\{0,1\}$. In other contexts, randomized processes with Boolean output may also be considered, and when considering their expected value one gets a function that ranges over $[0,1]$. Since all observations hold also for the latter case, we define a class of distinguishers as a set of functions from strings to $[0,1]$. (We note that some of the observations hold also for arbitrary functions from strings to $\mathbb{R}$.)[1]

Observations

All observations are quite oblivious of the class of distinguishers, with the exception that some of them require this class to contain the all-1 function. We first recall the observation made in the previous section.

Observation 1 (the average weight approximately equals 1): *Suppose that (G,ω) is a wPRG that ϵ-fools a class of distinguishers $\mathcal{D}$ that contains the all-1 function. Then, $\mathrm{E}_{s\in\{0,1\}^k}[\omega(s)] = 1 \pm \epsilon$.*

The following observation is well-known (at least to experts).

Observation 2 (non-negative weights are useless): *Let $\omega : \{0,1\}^k \to \mathbb{R}^+$ (i.e., $\omega(s) \geq 0$ for every s) and suppose that (G,ω) fools a class of distinguishers $\mathcal{D}$ that contains the all-1 function. Then, $\mathcal{D}$ can be fooled by a standard PRG of the same complexity.*

Proof: We first assume (w.l.o.g.) that the weight function ω takes values that are multiples of $1/F$ such that $F = O(2^k/\epsilon)$. (This can be justified by rounding the weights to the closest multiple of $1/F$, incurring a deviation of less than $2^k/F \leq \epsilon/2$.) Recall that, by Observation 1, the weights sum-up to approximately 2^k. By moving weights among seeds, we can also assume (w.l.o.g.) that there are no zero weights and that the weights sum-up to $K \stackrel{\text{def}}{=} 2^k$. (Note that these simplifying assumptions hold also when there are negative weights.)

Next, letting $m(s) = F \cdot \omega(s) \in \mathbb{N}$ (equiv., $\omega(s) = m(s)/F$), we have for every $D : \{0,1\}^n \to \mathbb{R}$

$$\begin{aligned}
\mathrm{E}_{s\in\{0,1\}^k}[\omega(s)\cdot D(G(s))] &= \frac{1}{FK}\cdot \sum_{s\in\{0,1\}^k} m(s)\cdot D(G(s)) \\
&= \frac{1}{FK}\cdot \sum_{s\in\{0,1\}^k}\sum_{i\in[m(s)]} D(G(s))
\end{aligned}$$

[1] The distinction is hinted in the proofs (i.e., by the way we refer to D). We note that functions from strings to $\mathbb{R}$, even when having low computational complexity, are not a reasonable notion of a class of distinguishers. Consider, for example, the function $f : \{0,1\}^n \to \mathbb{R}$ such that $f(1^n) = 2^{n-1}$ and $f(x) = 0$ otherwise. Then, no $G : \{0,1\}^k \to \{0,1\}^n$ (with $k < n$) can fool f, because $\mathrm{E}_{u\in\{0,1\}^n}[f(u)] = 2^{-n}\cdot 2^{n-1} = 1/2$, whereas $\mathrm{E}_{s\in\{0,1\}^k}[f(G(s))]$ is either 0 or at least $2^{-k}\cdot 2^{n-1} \geq 1$.

$$= \frac{|S|}{FK} \cdot \mathrm{E}_{(s,i)\in S}[D(G'(s,i))]$$

where $S = \{(s,i) : s \in \{0,1\}^k \ \& \ i \in [m(s)]\}$ and $G'(s,i) = G(s)$. Recalling that $\sum_{s\in\{0,1\}^k} \frac{m(i)}{F} = K$, we have $|S| = FK$ and the claim follows (since $\mathrm{E}_{s'\in S}[D(G'(s'))] = \mathrm{E}_{s\in\{0,1\}^k}[\omega(s) \cdot D(G(s))]$). ■

Observation 3 (extremely bounded weights are useless): *Suppose that $\omega : \{0,1\}^k \to \mathbb{R}$ is upper-bounded by 1* (i.e., $\omega(s) \leq 1$ for every s) *and suppose that (G,ω) fools a class of distinguishers $\mathcal{D}$ that contains the all-1 function. Then, $\mathcal{D}$ can be fooled by a standard PRG of the same complexity. Specifically, if the wPRG ϵ-fools $\mathcal{D}$, then the standard PRG 2ϵ-fools $\mathcal{D}$.*

This observation is implicit in the proof of [3, Lem. 5.6], which is reproduced next.[2]

Proof: On the one hand, using $\omega(s) \leq 1$ for every s, we have, for every $D \in \mathcal{D}$

$$\begin{aligned} \mathrm{E}_s[D(G(s))] &\geq \mathrm{E}_s[\omega(s) \cdot D(G(s))] \\ &\geq \mathrm{E}_u[D(u)] - \epsilon. \end{aligned}$$

On the other hand, using $1 - \omega(s) \geq 0$, for every $D \in \mathcal{D}$, we have

$$\begin{aligned} \mathrm{E}_s[D(G(s))] &= \mathrm{E}_s[\omega(s) \cdot D(G(s))] + \mathrm{E}_s[(1-\omega(s)) \cdot D(G(s))] \\ &\leq (\mathrm{E}_u[D(u)] + \epsilon) + \mathrm{E}_s[(1-\omega(s))] \\ &\leq \mathrm{E}_u[D(u)] + 2\epsilon, \end{aligned}$$

where the last inequality uses $\mathrm{E}_s[\omega(s)] \geq 1 - \epsilon$ (which holds by Observation 1). It follows that the standard PRG G 2ϵ-fools $\mathcal{D}$. ■

Observation 4 (weights in intervals vs at the extremes): *Suppose that for $B : \mathbb{N} \to \mathbb{R}$ such that $B(k) \in [1, \exp(O(k))]$ it holds that $\omega : \{0,1\}^k \to [-B(k), +B(k)]$ and suppose that (G,ω) fools a class of distinguishers $\mathcal{D}$. Then, $\mathcal{D}$ can be fooled by a wPRG (G'',ω'') of the same complexity such that $\omega'' : \{0,1\}^{k''} \to \{-B(k), +B(k)\}$ and $k'' = O(k)$, where the same complexity includes also the complexity of computing B.*

The restriction $B(k) \geq 1$ is justified by Observation 3 (assuming that $\mathcal{D}$ contains the all-1 function), whereas $B(k) \leq \exp(O(k))$ seems natural and holds in all known constructions. (The latter condition is required for the proof, which increases the seed length by an additive $\log_2 B(k)$ term.)

Proof: Letting $B \leftarrow B(k)$, we may assume (w.l.o.g.) that the weight function ω takes values that are multiples of B/F such that $F = O(2^k \cdot B/\epsilon)$ (This can be justified by rounding the weights to the closest multiple of B/F, incurring a deviation of less that $2^k \cdot B/F \leq \epsilon/2$.) Consequently, for every $s \in \{0,1\}^k$ such that $\omega(s) \neq 0$, it holds that $F \cdot |\omega(s)|/B$ is a natural number.

Now, let $G' : \{0,1\}^k \times [F] \to \{0,1\}^n$ such that $G'(s,i) = G(s)$ and $\omega' : \{0,1\}^k \times [F] \to \{-B, 0, B\}$ such that $\omega'(s,i) = \mathrm{sign}(\omega(s)) \cdot B$ if $i \in [F \cdot |\omega(s)|/B]$ and $\omega'(s,i) = 0$ otherwise. Clearly, $\mathrm{E}_{i\in[F]}[\omega'(s,i)] = (F \cdot \omega(s)/B) \cdot B/F = \omega(s)$ for every s. Hence, for every $D : \{0,1\}^n \to \mathbb{R}$, it holds that

$$\mathrm{E}_{(s,i)}[\omega'(s,i) \cdot D(G'(s,i))] = \mathrm{E}_s[\omega(s) \cdot D(G(s))].$$

[2] The statement of [3, Lem. 5.6] refers to BP and to weights in $[\pm 1]$, but its original proof only uses the fact that the distinguisher class contains the all-1 function and the hypothesis that the weights do not exceed 1.

Lastly, we modify (G', ω') so to avoid zero weights by replacing a seed with zero weight (i.e., $\omega'(s') = 0$) by a pair of seeds (i.e., $s'0$ and $s'1$) such that one seed has weight B and the other has weight $-B$ (i.e., $\omega''(s'0) = B$ and $\omega''(s'1) = -B$). A seed with non-zero weight is replaced by a pair of seeds that are assigned the same weight (i.e., if $\omega'(s') \neq 0$, then $\omega''(s'0) = \omega''(s'1) = \omega'(s')$). Letting $G''(s', b) = G'(s')$, the claim follows (because, for every $D : \{0,1\}^n \to \mathbb{R}$, it holds that $\mathrm{E}_{(s',b)}[\omega''(s', b) \cdot D(G''(s', b))] = \mathrm{E}_{s'}[\omega'(s') \cdot D(G'(s'))]$). ■

Observation 5 (linear combination of two standard PRGs): *Let $B, (G, \omega)$ and $\mathcal{D}$ be as in Observation 4. Then, $\mathcal{D}$ can be fooled by a linear combination L (i.e., $L(x, y) = \alpha \cdot x + \beta \cdot y$) of a pair of standard PRG (G', G'') of similar complexity; that is, for every $D :\in \mathcal{D}$, it holds that*

$$L(\mathrm{E}_{s'}[D(G'(s'))], \mathrm{E}_{s''}[D(G''(s''))]) \approx \mathrm{E}_u[D(u)],$$

where L can also be computed within the same complexity.

Needless to say, such a linear combination yields a wPRG with weights 2α and 2β (which invokes each PRG with probability $1/2$).

Proof: Letting $B \leftarrow B(k)$ and using Observation 4, we may assume that $\omega : \{0,1\}^k \to \{-B, +B\}$. Now, let

- $G' : \{0,1\}^{k'} \to \{0,1\}^n$ such that G' uses its seeds to sample $\omega^{-1}(B)$ (almost) uniformly, obtains $s \in \omega^{-1}(B)$, and outputs $G(s)$.
- $G'' : \{0,1\}^{k''} \to \{0,1\}^n$ such that G'' uses its seeds to sample $\omega^{-1}(-B)$ (almost) uniformly, obtains $s \in \omega^{-1}(-B)$, and outputs $G(s)$.
- $\alpha = B \cdot \Pr_s[\omega(s) = B]$ and $\beta = -B \cdot \Pr_s[\omega(s) = -B]$.

Then, for every $D : \{0,1\}^n \to \mathbb{R}$, it holds that

$$\begin{aligned}
&\alpha \cdot \mathrm{E}_{s'}[D(G'(s'))] + \beta \cdot \mathrm{E}_{s''}[D(G''(s''))] \\
&\quad \approx \quad \alpha \cdot \mathrm{E}_{s \in \omega^{-1}(B)}[D(G(s))] + \beta \cdot \mathrm{E}_{s \in \omega^{-1}(-B)}[D(G(s))] \\
&\quad = \quad B \cdot 2^{-k} \cdot \sum_{s \in \omega^{-1}(B)} D(G(s)) - B \cdot 2^{-k} \cdot \sum_{s \in \omega^{-1}(-B)} D(G(s)) \\
&\quad = \quad \mathrm{E}_s[\omega(s) \cdot D(G(s))]
\end{aligned}$$

and the claim follows. ■

The complexity of the weights. In the context of "derandomization-oriented" pseudorandom generators, one typically uses PRGs whose complexity exceeds the complexity of the distinguishers. A natural question is whether this is needed also for the weighting function of a wPRG. A partial affirmative answer is provided next.

Observation 6 (low complexity weights are useless): *Suppose that (G, ω) ϵ-fools a class of distinguishers $\mathcal{D}$ that contains the all-1 function and that the mapping $G(s) \mapsto \omega(s)$ is computable in $\mathcal{D}$, which indeed implies that $\omega(s) = \omega(s')$ if $G(s) = G(s')$. Then, $\mathcal{D}$ can be $O(\epsilon)$-fooled by a standard PRG of the same complexity. Moreover, the conclusion holds also if we only require the sign of the weight to be computable in $\mathcal{D}$.*

We stress that the computation is required to be correct only for outcomes of the wPRG; when given an input that is not in the image of G, the answer may be arbitrary. Indeed, it is more natural to consider the complexity of the mapping $s \mapsto \omega(s)$. Still, in case the wPRG outputs its seed (as part of the output sequence)[3], the ability to compute (or evaluate) ω implies the ability to compute the mapping $G(s) \mapsto \omega(s)$.

Proof: We shall consider the contribution of negative weights to the average value of the weighting function; that is, we consider the quantity

$$N_\omega \stackrel{\text{def}}{=} 2^{-k} \cdot \sum_{s \in \{0,1\}^k : \omega(s) < 0} |\omega(s)|. \tag{2}$$

We shall show that if $N_\omega \leq 3\epsilon$, then $\mathcal{D}$ can be fooled by a standard PRG, whereas the complementary case is impossible.

Suppose that $N_\omega \leq 3\epsilon$. Consider the weighting function $\omega' : \{0,1\}^k \to \mathbb{R}^+$ such that $\omega'(s) = 0$ if $\omega(s) < 0$ and $\omega'(s) = \omega(s)$ otherwise. Then, for every $D : \{0,1\}^n \to [0,1]$ it holds that

$$\mathrm{E}_{s \in \{0,1\}^k}[\omega'(s) \cdot D(G(s))] = \mathrm{E}_{s \in \{0,1\}^k}[\omega(s) \cdot D(G(s))] \pm 3\epsilon.$$

Recalling that (G, ω) fools (i.e., ϵ-fools) $\mathcal{D}$, it follows that (G, ω') fools (i.e., 4ϵ-fools) $\mathcal{D}$. Using Observation 2, we infer that there exists a standard PRG that fools $\mathcal{D}$.

We next show that $N_\omega > 3\epsilon$ is impossible. Assuming towards the contradiction that $N_\omega > 3\epsilon$ and recalling that $\mathrm{E}_s[\omega(s)] = 1 \pm \epsilon$ (by Observation 1), it follows that

$$2^{-k} \cdot \sum_{s \in \{0,1\}^k : \omega(s) > 0} \omega(s) > 1 - \epsilon + 3\epsilon = 1 + 2\epsilon.$$

Now, consider the distinguisher D_ω such that $D_\omega(G(s)) = 1$ if $\omega(s) > 0$ and $D_\omega(G(s)) = 0$ if $\omega(s) \leq 0$. (Indeed, the value of D_ω on inputs not at the image of G is arbitrary, as long as it is in $[0,1]$ (which can be easily enforced).) Then,

$$\mathrm{E}_{s \in \{0,1\}^k}[\omega(s) \cdot D_\omega(G(s))] = 2^{-k} \cdot \sum_{s \in \{0,1\}^k : \omega(s) > 0} \omega(s) > 1 + 2\epsilon,$$

whereas $\mathrm{E}_{u \in \{0,1\}^n}[D_\omega(u)] \leq 1$. But this contradicts the hypothesis that (G, ω) ϵ-fools D_ω, since D_ω is in $\mathcal{D}$. ■

Sufficiently good approximation

Bearing in mind that wPRGs are used for derandomization of algorithms that may be made to have small error probability (by repetitions), it suffices to distinguish between a value close to 1 and a value close to 0. In that context, sufficiently bounded weights can be eliminated as shown next.

[3] See, e.g., the PRG of [7], as analyzed in [5, Sec. 8.3.2.2]. It seems that the PRG of [6] can also be adapted to satisfy this feature. Furthermore, any PRG against bounded-width ROBP can be converted to output its own seed as a prefix of its output sequence: Let G be such a generator and let $\mathtt{EXT}$ be a 2-source extractor for linear min-entropy that can be computed in linear space (e.g., [4]). Then, the new PRG is given by $G'(s,r) = (s, r, G(\mathtt{EXT}(s,r))$. (The transformation applies also to wPRGs; however, it may not preserve the complexity of computing the weights.)

Observation 7 (weights in $[-2.999, 2.999]$ are of limited use): *For any constant $B \in [1,3)$ suppose that $\omega : \{0,1\}^k \to [-B,+B]$ and that (G,ω) fools (ϵ-fools) a class of distinguishers $\mathcal{D}$ that contains the all-1 function. Then, for sufficiently small constant $\delta > 0$, there exist a standard PRG G' of similar complexity such that for every $D \in \mathcal{D}$ it holds that*

1. *If $\mathrm{E}_u[D(u)] \geq 1-\delta$, then $\mathrm{E}_{s'}[D(G'(s'))] = 0.5 + \Omega(1)$.*
2. *If $\mathrm{E}_u[D(u)] \leq \delta$, then $\mathrm{E}_{s'}[D(G'(s'))] = 0.5 - \Omega(1)$.*

Proof: Again, using Observation 4, we may assume (w.l.o.g.) that $\omega : \{0,1\}^k \to \{-B,+B\}$. Letting $p \stackrel{\text{def}}{=} \Pr_s[\omega(s) = -B]$, it holds that $\mathrm{E}_s[\omega(s)] = (1-p)\cdot B - p \cdot B$. Recalling that $\mathrm{E}_s[\omega(s)] = 1 \pm \epsilon$ (by Observation 1), we get $p = \frac{1}{2} - \frac{1\pm\epsilon}{2B} \approx \frac{B-1}{2B} < 1/2$. Hence, for every D, it holds that

$$\begin{aligned}\mathrm{E}_{s\in\{0,1\}^k}[\omega(s)\cdot D(G(s))] &= (1-p)\cdot B \cdot \mathrm{E}_{s\in\omega^{-1}(B)}[D(G(s))] - p\cdot B\cdot \mathrm{E}_{s\in\omega^{-1}(-B)}[D(G(s))] \\ &\approx \frac{B+1}{2}\cdot \mathrm{E}_{s\in\omega^{-1}(B)}[D(G(s))] - \frac{B-1}{2}\cdot \mathrm{E}_{s\in\omega^{-1}(-B)}[D(G(s))],\end{aligned}$$

which yields

$$\mathrm{E}_{s\in\omega^{-1}(B)}[D(G(s))] \approx \frac{2}{B+1}\cdot \mathrm{E}_{s\in\{0,1\}^k}[\omega(s)\cdot D(G(s))] + \frac{B-1}{B+1}\cdot \mathrm{E}_{s\in\omega^{-1}(-B)}[D(G(s))].$$

Hence, for $D \in \mathcal{D}$, we have

$$\mathrm{E}_{s\in\omega^{-1}(B)}[D(G(s))] = \frac{2}{B+1}\cdot \mathrm{E}_u[D(u)] + \frac{B-1}{B+1}\cdot \mathrm{E}_{s\in\omega^{-1}(-B)}[D(G(s))] \pm O(\epsilon).$$

Define G' as in the proof of Observation 5 (i.e., G' uses its seeds to sample $\omega^{-1}(B)$ (almost) uniformly, obtains $s \in \omega^{-1}(B)$, and outputs $G(s)$). So, for some $Q_{D\circ G,\omega} \in [0,1]$, we have

$$\mathrm{E}_{s'}[D(G'(s'))] = \frac{2}{B+1}\cdot \mathrm{E}_u[D(u)] + \frac{B-1}{B+1}\cdot Q_{D\circ G,\omega} \pm O(\epsilon). \tag{3}$$

Now, for any constant $B < 3$ and sufficiently small $\delta > 0$, we consider the following two cases:

1. If $\mathrm{E}_u[D(u)] \geq 1-\delta$, then $\mathrm{E}_{s'}[D(G'(s'))] \geq \frac{2}{B+1}\cdot(1-\delta) - O(\epsilon) = 0.5 + \Omega(1)$, where the first inequality uses Eq. (3) and the second inequality uses $B < 3$ and a sufficiently small $\delta > 0$.
2. If $\mathrm{E}_u[D(u)] \leq \delta$, then $\mathrm{E}_{s'}[D(G'(s'))] \leq \frac{2}{B+1}\cdot\delta + \frac{B-1}{B+1} + O(\epsilon) = 0.5 - \Omega(1)$, where the first inequality uses Eq. (3) and the second inequality uses $B < 3$ and a sufficiently small $\delta > 0$.

The claim follows. ■

Open problems

While Observation 6 refers to the complexity of the weights, it actually considers the complexity of the mapping $G(s) \mapsto \omega(s)$. Indeed, it is more natural to consider the complexity of the mapping $s \mapsto \omega(s)$.

Open Problem 1 (easily computable weights): *Suppose that (G, ω) fools a class of distinguishers $\mathcal{D}$ and that ω is computable in $\mathcal{D}$. Is it the case that $\mathcal{D}$ can be fooled by a standard PRG of the same complexity? If not, then are there additional conditions that yield an affirmative answer?*

Similarly, while Observations 3 and 7 refer to bounded weights, they refer to very restricted cases.

Open Problem 2 (bounded weights, revisited): *Suppose that for some constant $B \geq 1$ it holds that $\omega : \{0,1\}^k \to [-B, +B]$ and that (G, ω) fools a class of distinguishers $\mathcal{D}$. Is it the case that $\mathcal{D}$ can be fooled by a standard PRG of the same complexity? If not, then are there additional conditions that yield an affirmative answer?*

Of course, affirmative answers will beg the question of extending the result to adequately bounded functions $B : \mathbb{N} \to \mathbb{N}$.

References

[1] Mark Braverman, Gil Cohen, and Sumegha Garg. Pseudorandom Pseudo-distributions with Near-Optimal Error for Read-Once Branching Programs. *SIAM Journal on Computing*, Vol. 49 (5), 2020. Preliminary version in *50th STOC*, 2018.

[2] Gil Cohen, Dean Doron, Oren Renard, Ori Sberlo, and Amnon Ta-Shma. Error Reduction for Weighted PRGs Against Read Once Branching Programs. In *36th CCC*, pages 22:1–22:17, 2021,

[3] Ben Chen, Gil Cohen, Dean Doron, Yuval Khaskelberg, and Amnon Ta-Shma. Toward Improving Nisan's PRG via Deweightization. *ECCC*, TR26-064, 2026.

[4] Yevgeniy Dodis, Ariel Elbaz, Roberto Oliveira, and Ran Raz. Improved Randomness Extraction from Two Independent Sources. In *8th RANDOM*, LNCS 3122, Springer, pages 334–344, 2004.

[5] Oded Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, 2008.

[6] Noam Nisan. Pseudorandom Generators for Space Bounded Computation. *Combinatorica*, Vol. 12 (4), pages 449–461, 1992. Preliminary version in *22nd STOC*, 1990.

[7] Noam Nisan and Avi Wigderson. Hardness vs Randomness. *Journal of Computer and System Science*, Vol. 49, No. 2, pages 149–167, 1994. Preliminary version in *29th FOCS*, 1988.

[8] Edward Pyne and Salil Vadhan. Pseudodistributions That Beat All Pseudorandom Generators. In *36th CCC*, pages 33:1–33:15, 2021,

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il