Optimal Error Pseudodistributions for Read-Once Branching Programs

Eshan Chattopadhyay*  Jyun-Jie Liao*
Cornell University  Cornell University
eshanc@cornell.edu  jjliao@cs.cornell.edu

May 3, 2020

Abstract

In a seminal work, Nisan (Combinatorica’92) constructed a pseudorandom generator for length $n$ and width $w$ read-once branching programs with seed length $O(\log n \cdot \log(nw) + \log n \cdot \log(\frac{1}{\varepsilon}))$ and error $\varepsilon$. It remains a central question to reduce the seed length to $O(\log(nw/\varepsilon))$, which would prove that $\text{BPL} = \text{L}$. However, there has been no improvement on Nisan’s construction for the case $n = w$, which is most relevant to space-bounded derandomization.

Recently, in a beautiful work, Braverman, Cohen and Garg (STOC’18) introduced the notion of a pseudorandom pseudo-distribution (PRPD) and gave an explicit construction of a PRPD with seed length $\tilde{O}(\log n \cdot \log(nw) + \log(1/\varepsilon))$. A PRPD is a relaxation of a pseudorandom generator, which suffices for derandomizing $\text{BPL}$ and also implies a hitting set. Unfortunately, their construction is quite involved and complicated. Hoza and Zuckerman (FOCS’18) later constructed a much simpler hitting set generator with seed length $O(\log n \cdot \log(nw) + \log(1/\varepsilon))$, but their techniques are restricted to hitting sets.

In this work, we construct a PRPD with seed length $O(\log n \cdot \log(nw) \cdot \log \log(nw) + \log(1/\varepsilon))$.

This improves upon the construction in [BCG18] by a $O(\log \log(1/\varepsilon))$ factor, and is optimal in the small error regime. In addition, we believe our construction and analysis to be simpler than the work of Braverman, Cohen and Garg.

1 Introduction

A major challenge in computational complexity is to understand to what extent randomness is useful for efficient computation. It is widely believed that randomness does not provide substantial savings in time and space for algorithms. Indeed, under plausible assumption, every randomized algorithm for decision problem can be made deterministic with only a polynomial factor slowdown in time ($\text{BPP} = \text{P}$) [IW97] or a constant factor blowup in space ($\text{BPL} = \text{L}$) [KvM02].

*Supported by NSF grant CCF-1849899.
However, it remains open for decades to prove these results unconditionally. For derandomization in the time-bounded setting, it is known that proving $\text{BPP} = \text{P}$ implies circuit lower bounds which seem much beyond reach with current proof techniques [KI04]. However, no such implications are known for the space-bounded setting, and there has been some progress. Savitch’s theorem [Sav70] implies that $\text{RL} \subseteq \text{L}^2$. Borodin, Cook, Pippenger [BCP83] and Jung [Jun81] proved that $\text{PL} \subseteq \text{L}^2$, which implies $\text{BPL} \subseteq \text{L}^2$.

Nisan [Nis92, Nis94] constructed a pseudorandom generator for log-space computation with seed length $O(\log^2 n)$, and used it to show that $\text{BPL}$ can be simulated with $O(\log^2 n)$ space and polynomial time. Saks and Zhou [SZ99] used Nisan’s generator in a non-trivial way to show that $\text{BPL} \subseteq \text{L}^{3/2}$, which remains the best known result so far. We refer the interested reader to the beautiful survey by Saks [Sak96] for more background and relevant prior work.

We introduce the notion of a read-once branching programs, which is a non-uniform model for capturing algorithms that use limited memory.

**Definition 1.1** (Read-once branching program). A $(n, w)$-read-once branching program (ROBP) $B$ is a directed graph on the vertex set $V = \bigcup_{i=0}^{n} V_i$, where each set $V_i$ contains $w$ nodes. Every edge in this directed graph is labeled either 0 or 1. For every $i < n$, and every node $v \in V_i$, there exists exactly two edges starting from $v$, one with label 0 and the other with label 1. Every edge starting from a node in $V_i$ connects to a node in $V_{i+1}$. We say $n$ is the length of $B$, $w$ is the width of $B$ and $V_i$ is the $i$-th layer of $B$.

Moreover, there exists exactly one starting state $s \in V_0$, and exactly one accepting state $t \in V_n$. For every $x = (x_1, \ldots, x_n) \in \{0, 1\}^n$, we define $B(x) = 1$ if starting from $s$ we will reach $t$ following the edges labeled by $x_1, \ldots, x_n$. Otherwise we define $B(x) = 0$.

It is well-known the computation of a probabilistic Turing machine that uses space $S$ and tosses $n$ coins, on a given input $y$, can be carried out by a $(n, 2^{O(S)})$-ROBP $B_y$. In particular, if the string $x \in \{0, 1\}^n$ corresponds to the $n$ coin tosses, then $B_y(x)$ is the output of the Turing machine.

A standard derandomization technique is via pseudorandom generators. We define this notion for the class of ROBPs.

**Definition 1.2** (Pseudorandom generator). A function $G : \{0, 1\}^s \to \{0, 1\}^n$ is a $(n, w, \varepsilon)$-pseudorandom generator (PRG) if for every $(n, w)$-ROBP $B$,

$$\left| \mathbb{E}_{x \in \{0, 1\}^n} [B(x)] - \mathbb{E}_{r \in \{0, 1\}^s} [B(G(r))] \right| \leq \varepsilon.$$ 

The seed length of $G$ is $s$. $G$ is explicit if $G$ is computable in $O(s)$ space.

To derandomize space-bounded computation given an explicit $(n, w, \varepsilon)$-PRG, one can enumerate $B(G(r))$ for every $r \in \{0, 1\}^s$ with $O(s)$ additional space to compute an $\varepsilon$-approximation of the quantity $\mathbb{E}_x [B(x)]$.

Nisan [Nis92] constructed a $(n, w, \varepsilon)$-PRG with seed length $O(\log n \cdot \log(nw/\varepsilon))$, which implies $\text{BPL} \subseteq \text{L}^2$. While there is a lot of progress in constructing PRG with better seed length for restricted family of ROBP (see, e.g., [NZ96, Arm98, BV10, BDVY13, BRRY14, KNP11, De11, Ste12, MRT19] and references therein), Nisan’s generator and its variants [Nis92, INW94, RR99] remain the best-known generators in the general case.
1.1 Pseudorandom pseudodistribution

Recently, a beautiful work of Braverman, Cohen and Garg [BCG18] introduced the notion of a *pseudorandom pseudodistribution* (PRPD) that relaxes the definition of a PRG.

**Definition 1.3 (Pseudorandom pseudodistribution).** A pair of functions $(G, \rho) : \{0,1\}^s \to \{0,1\}^n \times \mathbb{R}$ generates a $(n, w, \varepsilon)$-pseudorandom pseudodistribution (PRPD) if for every $(n, w)$-ROBP $B$,

$$\left| \mathbb{E}_{x \in \{0,1\}^n}[B(x)] - \mathbb{E}_{r \in \{0,1\}^s}[\rho(r) \cdot B(G(r))] \right| \leq \varepsilon.$$ 

We say $s$ is the seed length of $(G, \rho)$. We say $(G, \rho)$ is $k$-bounded if $|\rho(x)| \leq k$ for every $x \in \{0,1\}^s$. We say $(G, \rho)$ is explicit if they are computable in space $O(s)$.

Note that a $(n, w, \varepsilon)$-PRG $G$ of seed length $s$ with a constant function $\rho(x) = 1$ generates a 1-bounded $(n, w, \varepsilon)$-PRPD. Similar to a PRG, it is possible to derandomize $\text{BPL}$ by enumerating all seeds of a PRPD and computing an $\varepsilon$-approximation for $\mathbb{E}_x[B(x)]$. In [BCG18] they observe that given $(G, \rho)$ which generates an $(n, w, \varepsilon)$-PRPD, the function $G$ itself is an $\varepsilon$-hitting set generator for $(n, w)$-ROBP.

The main result in [BCG18] is an explicit construction of a $(n, w, \varepsilon)$-PRPD with seed length

$$O \left( (\log n \cdot \log(nw) + \log(1/\varepsilon)) \cdot \log \log(nw/\varepsilon) \right),$$

which is $\text{poly}(nw/\varepsilon)$-bounded. This improves on the seed-length of Nisan’s generator and provides near optimal dependence on error.

Unfortunately, the construction and analysis in [BCG18] is highly complicated. Hoza and Zuckerman [HZ18] provided a dramatically simpler hitting set generator with slightly improved seed length. However, it is not clear how to extend their techniques for constructing a PRPD (or PRG).

1.2 Main result

In this paper, we construct a PRPD with optimal dependence on error (up to constants).

**Theorem 1.** There exists an explicit $(n, w, \varepsilon)$-PRPD generator $(G, \rho)$ with seed length

$$O \left( (\log n \cdot \log(nw) + \log(1/\varepsilon)) \cdot \log \log(nw/\varepsilon) \right),$$

which is $\text{poly}(1/\varepsilon)$-bounded.

This improves upon the construction in [BCG18] by a factor of $O(\log \log(1/\varepsilon))$, for any $\varepsilon < n^{-\Omega(\log(nw) \log(nw))}$.

As observed in [BCG18], the small-error regime is well motivated for application to derandomizing space-bounded computation. In particular, Saks and Zhou [SZ99] instantiated Nisan’s PRG with error $n^{-\omega(1)}$ to obtain the result $\text{BPL} \subseteq L^{3/2}$. We note that one can replace the PRG in the Saks-Zhou scheme\(^1\) with a PRPD which is $\text{poly}(w, 1/\varepsilon)$-bounded, and hence improvements to our result will lead to improved derandomization of $\text{BPL}$.

Our construction uses a strategy similar to [BCG18] with the following key differences.

\(^1\)technically, the Saks-Zhou scheme requires a high-probability property in Nisan’s generator, but Armoni [Arm08] observed that one can use an averaging sampler to obtain this property for any PRG (see also [HU17]). The same argument works for PRPD with bounded weight.
The construction in [BCG18] has a more bottom-up nature: their construction follows the binary tree structure in Nisan’s generator [Nis92], but in each node they maintain a sophisticated “leveled matrix representation” (LMR) which consists of many pieces of small-norm matrices, and they show how to combine pieces in two LMRs one by one to form a LMR in the upper level. Our construction follows the binary tree structure in Nisan’s generator, but has a more top-down spirit. We give a clean recursive formula which generates a “robust PRPD” for $(n,w)$-PRPD given robust PRPDs for $(n/2,w)$-ROBP, where a robust PRPD is a family of pseudodistributions such that the approximation error of pseudodistribution drawn from this family is small on average. (A formal definition can be found in Definition 6.3.) The top-down nature of our construction significantly simplifies the construction and analysis.

Following [BCG18], we use an averaging sampler in our recursive construction, but we further observe that we can apply a simple “flattening” operation to limit the growth of seed length. With this observation, we not only improve the seed length but also simplify the construction and analysis by avoiding some special case treatments that are necessary in [BCG18]. (Specifically, we do not need the special multiplication rule “outer product” in [BCG18].)

Independent work. Independent work of Cheng and Hoza [CH20] remarkably prove that a hitting set generator (HSG) for ROBPs can be used for derandomizing BPL. Their first result shows that every $(n,w)$-ROBP $f$ can be deterministically approximated within error $\varepsilon$ with an explicit HSG for $(\text{poly}(nw^2),\text{poly}(nw^2))$-ROBP with seed length $s$. The space complexity of their first derandomization is $O(s + \log(nw/\varepsilon))$. Their second result shows that every $(n,w)$-ROBP $f$ can be deterministically approximated within error $\varepsilon$ with an explicit HSG for $(n,\text{poly}(w))$-ROBP with seed length $s$. Their second derandomization has space complexity $O(s + w \log(n/\varepsilon))$, and only requires black-box access to $f$.

Their first result does not imply better derandomization algorithms with the state-of-art HSGs so far. Plugging in the HSG from [HZ18], their second result gives a black-box derandomization algorithm for $(n,w)$-ROBP in space $O(\log(n) \log(nw) + w \log(n/\varepsilon))$. This is better than the black-box derandomization with our PRPD for the restricted case of $w = O(1)$. We note that an advantage of PRPDs (over hitting sets) is that they are applicable in the Saks and Zhou’s scheme [SZ99] (as mentioned above, when applied with Armoni’s sampler trick [Arm98]).

Organization. In Section 2, we present the matrix representation of ROBPs, see how a pseudodistribution can be interpreted as matrices, and introduce some basic rules for translating between matrix operations and operations on pseudodistribution. We use Section 3 to present an outline of our main construction and proof. Section 4 contains necessary preliminaries. In Section 5, we formally prove several lemmas about using samplers on approximate matrix multiplication. In Section 6, we present and prove correctness of our main construction. We conclude with possible future directions in Section 7.
2 ROBPs and Matrices

We introduce the matrix representation of ROBPs and some related definitions that are useful in the rest of the paper. First, we setup some notation.

Notation: Given two strings \(x, y\), we use \(x \| y\) to denote the concatenation of \(x\) and \(y\). For every \(n \in \mathbb{N}\), we use \([n]\) to denote the set \(\{1, 2, \ldots, n\}\). We denote a collection of objects \(A_i^j\) with subscript \(i \in S\) and superscript \(j \in T\) by \([A]^S_T\) for short.

Given a \((n, w)\)-ROBP \(B\) with layers \(V_0, \ldots, V_n\), we can represent the transition from layer \(V_{t-1}\) to \(V_t\) by two stochastic matrices \(M^0_t\) and \(M^1_t\) as follows: suppose layer \(V_j\) consists of the nodes \(\{v_{j,1}, \ldots, v_{j,w}\}\). The entry \((M^0_t)_{i,j} = 1\) if and only if there exist a 0-labeled edge from \(v_{t-1,i}\) to \(v_{t,j}\) (else \((M^0_t)_{i,j} = 0\)). The matrix \(M^1_t\) is defined similarly according to the edges that labeled 1 between layers \(V_{t-1}\) and \(V_t\). More generally, we can also represents multi-step transition by a stochastic matrix. That is, for every \(0 \leq a \leq b \leq n\), and every \(r = (r_a+1, \ldots, r_b) \in \{0, 1\}^{b-a}\), we can define

\[M^r_{a,b} = \prod_{t=a+1}^{b} M^r_t\]

which corresponds to the transition matrix from layer \(a\) to layer \(b\) following the path labeled by \(r\). Note that every row of \(M^r_{a,b}\) contains exactly one 1, and the other entries are 0.

An \(n\)-step random walk starting from the first layer can be represented with the following matrix:

\[M_{0..n} = \frac{1}{2^n} \sum_{r \in \{0, 1\}^n} M^r_{0..n} = \prod_{t=1}^{n} \frac{1}{2} \left(M^0_t + M^1_t\right) .\]

By definition of \(M^0_t, M^1_t\) one can observe that the \((i, j)\) entry of \(M_{0..n}\) is the probability that a random walk from \(v_{0,i} \in V_0\) reaches \(v_{n,j} \in V_n\). Therefore, suppose \(v_{0,i} \in V_0\) is the starting state of \(B\), \(v_{n,j} \in V_n\) is the accepting state of \(B\), then \(\mathbb{E}_x [B(x)]\) equals the \((i, j)\) entry of \(M_{0..n}\).

Recall that a generator of a \((n, w, \varepsilon)\)-PRPD is a pair of function \((G, \rho)\) such that for every \((n, w)\)-ROBP \(B\),

\[\left| \mathbb{E}_r \left[ \rho(r) \cdot B(G(r)) \right] - \mathbb{E}_{x \in \{0, 1\}^n} [B(x)] \right| \leq \varepsilon .\]

Equivalently, for every transition matrices \(M^0_t, M^1_t, \ldots, M^0_n, M^1_n\), we have

\[\| \mathbb{E}_r \left[ \rho(r) \cdot M^0_{0..n} \right] - M_{0..n} \|_{\text{max}} \leq \varepsilon ,\]

where \(\|A\|_{\text{max}}\) denotes \(\max_{i,j} |A(i,j)|\).

Therefore it is natural to represents a PRPD \((G, \rho)\) with a mapping \(G : \{0, 1\}^S \rightarrow \mathbb{R}^{w \times w}\) where \(G(r) = \rho(r) \cdot M^0_{0..n}\). More generally, we will use a notation similar to the "matrix bundle sequence" (MBS) introduced in [BCG18] to represent a PRPD.

**Definition 2.1.** Consider a \((n, w)\)-ROBP \([M]\) and a pair of functions \((G, \rho) : \{0, 1\}^{s_{\text{out}}} \times [S_{\text{in}}] \rightarrow \{0, 1\}^S \times \mathbb{R}\). The matrix form of \((G, \rho)\) on \([M]\) is a mapping \(A : \{0, 1\}^{s_{\text{out}}} \times [S_{\text{in}}] \rightarrow \mathbb{R}^{w \times w}\) such that for every \(x \in \{0, 1\}^{s_{\text{out}}}\) and \(y \in [S_{\text{in}}]\),

\[A(x, y) = \rho(x, y) \cdot M^{G(x,y)}_{0..n} .\]
For every $x \in \{0, 1\}^{s_{\text{out}}}$ we abuse the notation and define

$$A(x) = \mathbb{E}_y [A(x, y)].$$

Besides, we define $\langle A \rangle = \mathbb{E}_{x,y} [A(x, y)]$. We say $s_{\text{out}}$ is the outer seed length of $A$, denoted by $s_{\text{out}}(A)$, and $S_{\text{in}}$ is the inner size of $A$, denoted by $S_{\text{in}}(A)$. We also define $s_{\text{in}}(A) = \lceil \log S_{\text{in}} \rceil$ to be the inner seed length of $A$, and $s(A) = s_{\text{out}}(A) + s_{\text{in}}(A)$ to be the seed length of $A$.

**Remark 2.2.** For every fixed $x$, the collection $\{A(x, y) : y \in [S_{\text{in}}]\}$ corresponds to the “matrix bundle” in [BCG18]. This should be treated as a collection of matrices which “realizes” the matrix $A(x)$. The whole structure $A$ corresponds to the “matrix bundle sequence” in [BCG18], and should be treated as a uniform distribution over the set $\{A(x) : x \in \{0, 1\}^{s_{\text{out}}}\}$.

When the ROBP $[M]_{[n]}^{[0,1]}$ is clear in the context, we will use the matrix form $A$ to represent the pseudodistribution $(G, \rho)$ directly. We will apply arithmetic operations on matrices $A(x)$, and these operations can be easily translated back to operations on pseudodistributions as follows.

**Definition 2.3.** Consider a $(n, w)$-ROBP $[M]_{[n]}^{[0,1]}$, and a pair of function $(F, \sigma) : [S] \rightarrow \{0, 1\}^n \times \mathbb{R}$. The matrix that is realized by $(F, \sigma)$ on $M_{0..n}$ is $\mathbb{E}_{i \in [S]} [\sigma(i) \cdot M_{0..n}^{F(i)}]$. We say $S$ is the size of $(F, \sigma)$.

Scaling the matrix corresponds to scaling the coefficients in the pseudodistribution.

**Claim 1.** Consider a $(n, w)$-ROBP $[M]_{[n]}^{[0,1]}$, let $A$ be a matrix realized by matrix bundle $(F_A, \sigma_A)$ on $M_{0..n}$. Then $cA$ is realized by a matrix bundle $(F'_A, \sigma'_A)$ of size $S_A$ s.t. $F'_A = cF_A$ and $\sigma'_A(x) = c\sigma_A(x)$ for every $x \in [S]$. The summation on matrices corresponds to re-weighting and union on pseudodistributions.

**Claim 2.** Consider a $(n, w)$-ROBP $[M]_{[n]}^{[0,1]}$, let $A$ be a matrix realized by matrix bundle $(F_A, \sigma_A)$ of size $S_A$ on $M_{0..n}$ and $B$ be a matrix realized by matrix bundle $(F_B, \sigma_B)$ of size $S_B$ on $M_{0..n}$. Then $A + B$ is realized by a matrix bundle $(F', \sigma')$ of size $S_A + S_B$ on $M_{0..n}$ s.t.

$$F'(x) = \begin{cases} F_A(x) & \text{if } x \leq S_A \\ F_B(x - S_A) & \text{if } x > S_A \end{cases}$$

$$\text{and } \sigma'(x) = \begin{cases} \sigma_A(x) & \text{if } x \leq S_A \\ \sigma_B(x - S_A) & \text{if } x > S_A \end{cases}$$

The multiplication on matrices corresponds to concatenation of pseudodistributions.

**Claim 3.** Consider a $(n, w)$-ROBP $[M]_{[n]}^{[0,1]}$, let $A$ be a matrix realized by matrix bundle $(F_A, \sigma_A)$ of size $S_A$ on $M_{0..n/2}$ and $B$ be a matrix realized by matrix bundle $(F_B, \sigma_B)$ of size $S_B$ on $M_{n/2..n}$. Fix a bijection $\pi : [S_A] \times [S_B] \rightarrow [S_A \cdot S_B]$. Then $AB$ is realized by a matrix bundle $(F', \sigma')$ of size $S_A \cdot S_B$ s.t. for every $a \in [S_A], b \in [S_B]$,

$$F'((a, b)) = F_A(a) \| F_B(b)$$

and

$$\sigma'(\pi(a, b)) = \sigma(a) \cdot \sigma(b).$$
3 Proof Overview

In this section we give an outline of our construction and proof. In Section 3.1, we briefly recap how a sampler is used in [BCG18] to achieve better seed length in the small-error regime. We discuss our construction ideas in Section 3.2.

3.1 The sampler argument

Nisan’s generator and its variants recursively use a lemma of the following form.

**Lemma 3.1.** Consider a (n, w)-ROBP $[M]_{[n]}^{[0,1]}$. Let $A$ be the matrix form of a distribution on $M_{0,.n/2}$, and $B$ be the matrix form of a distribution on $M_{n/2,.n}$. Suppose $s(A) = s(B) = s$. Then there exists a distribution whose matrix form $C$ on $M_{0,.n}$ of seed length $s + O(\log(w/\delta))$ such that

$$\|\langle C \rangle - \langle A \rangle \langle B \rangle\|_{\max} \leq \delta.$$ 

This lemma is usually achieved with a pseudorandom object. For example, the INW generator [INW94] uses a bipartite expander with degree poly$(w/\delta)$ to construct the distribution $C$ in the above lemma. That is, for every edge $(x, y)$ in the expander $G$, they add $A(x)B(y)$ into $C$. A similar lemma can also be obtained with universal hash functions [Nis92] or seeded extractors [RR99]. By recursively constructing good approximations of $M_{0,.n/2}$ and $M_{n/2,.n}$ and applying Lemma 3.1, one can obtain a PRG which has seed length $O(\log n \cdot \log(nw/\epsilon))$ ($\delta$ is taken to be $\epsilon/n$ because of a union bound). Observe that in such constructions, one needs to pay $O(\log(1/\epsilon))$ (in seed length) per level of recursion.

The crucial idea in [BCG18] is to amortize this cost over all log $n$ levels. What makes this possible is the following argument, which we will refer to as the sampler argument. First we define the notion of an averaging sampler.

**Definition 3.2.** A function $g : \{0, 1\}^n \times \{0, 1\}^d \to \{0, 1\}^m$ is an $(\epsilon, \delta)$-(averaging) sampler if for every function $f : \{0, 1\}^m \to [0, 1]$, 

$$\Pr_{x \in \{0, 1\}^n, \delta \in \{0, 1\}^d} \left[ \| \mathbb{E}_{s \in \{0, 1\}^d} [f(g(x, s))] - \mathbb{E}_{y \in \{0, 1\}^m} [f(y)] \| \leq \epsilon \right] \geq 1 - \delta.$$ 

The crucial observation in [BCG18] is that if one uses a sampler to prove Lemma 3.1, the error actually scales with the norm of one of the matrix forms.

**Lemma 3.3 ([BCG18]).** Consider a (n, w)-ROBP with matrix representation $[M]_{[n]}^{[0,1]}$. Let $A$ and $B$ be (pseudo)distributions in matrix form on $M_{0,.n/2}$ and $M_{n/2,.n}$ respectively. Let $n = s_{out}(A)$, $m = s_{out}(B)$. Suppose $\forall x \in \{0, 1\}^n, \|A(x)\| \leq 1$ and $\forall y \in \{0, 1\}^m, \|B(y)\| \leq 1$. Let $g : \{0, 1\}^n \times \{0, 1\}^d \to \{0, 1\}^m$ be a $(\epsilon, \delta)$ sampler. Then there exists a (pseudo)distribution $C$ such that

$$\|\langle C \rangle - \langle A \rangle \langle B \rangle\| \leq O\left(\delta^2 + \epsilon \mathbb{E}_x \|A(x)\| \right).$$ 

Besides, $C$ has outer seed length $n = s_{out}(A)$, and for every $x \in \{0, 1\}^n$,

$$C(x) = \mathbb{E}_s [A(x)B(g(x, s))].$$ 

Note that $s_{in}(C) = s_{in}(A) + s_{in}(B) + d$. 


The intuition behind this approximation is as follows. If we want to compute the matrix product precisely, we take every $A(x)$ and multiply it with $E_y[B(y)]$. However, with the help of sampler, we can use $x$ as our seed to select some samples from $B$, and take their average as an estimate of $E_y[B(y)]$. The error of this approximation comes in two different way. For those $x$ which are not good choices of a seed for the sampler, the samples chosen with such an $x$ can deviate from the average arbitrarily. However, only $\delta$ fraction of $x$ can be bad, so they incur at most $\delta$ error. The second kind of error is the estimation error between average of samples $E_s[B(g(x,s))]$ and the real average $E_y[B(y)]$, which can be at most $\varepsilon$. Since this gets multiplied with $A(x)$, this kind of error actually scales with $\|A(x)\|$.

The first kind of error (which is $\delta$) does not benefit from $\|A\|$ being small, in [BCG18] they observe that, the parameter $\delta$ has almost no influence on the seed length in some cases. To discuss this more precisely, we first recall explicit constructions of samplers.

**Lemma 3.4** ([RVW01, Gol11]). For every $\delta, \varepsilon > 0$ and integer $m$, there exists a space efficient $(\varepsilon, \delta)$-sampler $f : \{0, 1\}^n \times \{0, 1\}^d \to \{0, 1\}^m$ s.t. $d = O(\log \log (1/\delta) + \log (1/\varepsilon))$ and $n = m + O(\log (1/\delta)) + O(\log (1/\varepsilon))$.

Note that in Lemma 3.3, $s(C) = s(A) + d + s_m(B)$. Therefore if $n \geq m + O(\log (1/\delta)) + O(\log (1/\varepsilon))$, $\delta$ has almost no impact on the seed length.

To use the above ideas, it boils down to working with matrices with small norm, and making sure that every multiplication is “unbalanced” enough so that $\delta$ has no impact. [BCG18] applies a delicate telescoping sum trick (which they called “delta sampler”) to divide an $\varepsilon$-approximation into a base approximation with $1/\text{poly}(n)$ error and several “correcting terms” which have small norm. By carefully choosing the samplers and discarding all the non-necessary terms, they roughly ensure the following properties: first, a matrix with large seed length must have small norm; second, every matrix multiplication is unbalanced enough so that $\delta$ has no impact on the seed length.

With these properties and the sampler argument, they show that the total seed length is bounded by $\tilde{O}(\log (1/\varepsilon) + \log n \log (nw))$.

### 3.2 Our construction

In executing the ideas sketched above, the construction and analysis in [BCG18] turns out to be quite complicated and involved. One thing which complicates the construction and analysis is its bottom-up nature. That is, when multiplying two terms, they create more terms with the telescoping sum trick. Moreover, in the telescoping sum trick one needs to choose the parameters of each sampler very carefully to make sure the seed length of each term does not exceed its “smallness”.

Our first step toward a simpler construction is the following top-down formula, which we will apply recursively to compute an approximation of $M_{0..n}$:

**Lemma 3.5.** Let $\|\cdot\|$ be a sub-multiplicative matrix norm, and $A, B$ be two matrices s.t. $\|A\|, \|B\| \leq 1$. Let $k \in \mathbb{N}$ and $\gamma < 1$. For every $0 \leq i \leq k$, let $A_i$ be a $\gamma^{i+1}$-approximation of $A$, and let $B_i$ be a $\gamma^{i+1}$-approximation of $B$. Then

$$\sum_{i=0}^{k} A_i B_{k-i} - \sum_{i=0}^{k-1} A_i B_{k-1-i}$$

8
Our hope is to use an average for every $i$.

**Proof.** We have,

$$
\left\| \sum_{i=0}^{k} A_i B_{k-i} - \sum_{i=0}^{k-1} A_i B_{k-1-i} \right\| - AB
$$

$$
= \left\| \sum_{i=0}^{k} (A - A_i)(B - B_{k-i}) - \sum_{i=0}^{k-1} (A - A_i)(B - B_{k-1-i}) + (A_k - A)B + A(B_k - B) \right\|
$$

$$
\leq \sum_{i=0}^{k} \| A - A_i \| \cdot \| B - B_{k-i} \| + \sum_{i=0}^{k-1} \| A - A_i \| \cdot \| B - B_{k-1-i} \|
$$

$$
+ \| A_k - A \| \cdot \| B \| + \| A \| \cdot \| B_k - B \|
$$

$$
\leq (k + 2)\gamma^{k+1} + (k + 1)\gamma^{k+2}
$$

\[ \square \]

This formula shares an important property with the BCG construction: we never need a $\gamma^k$-approximation (which implies large seed length) on both sides simultaneously. The benefit of our top-down formula is that we are treating the PRPD as one object instead of the sum of many different terms. One obvious effect of such treatment is we don’t need to analyze the “smallness” of each term and the accuracy of the whole PRPD separately.

In this top-down formula, we do not explicitly maintain small-norm matrices as in [BCG18]. However, observe that in the proof of Lemma 3.5, we are using the fact that $A_k - A$ is a small norm matrix. Our goal is to apply the sampler argument (Lemma 3.3) on these “implicit” small-norm matrices. The following is our main technical lemma.

**Lemma 3.6** (main lemma, informal). Let $A, B \in \mathbb{R}^{w \times w}$, $k \in \mathbb{N}$ and $\gamma < 1$. Suppose for every $i \leq k$ there exists pseudodistribution $A_i, B_i$ such that $\mathbb{E}_x[\|A_i(x) - A\|] \leq \gamma^{i+1}$, $\mathbb{E}_x[\|B_i(x) - B\|] \leq \gamma^{i+1}$, and $\|A_i(x)\|, \|B_i(x)\| \leq 1$ for every $x$. Then there exists a pseudodistribution $C_k$ such that

$$
\mathbb{E}_x[\|C_k(x) - AB\| \leq O(\gamma)k+1],
$$

where $C_k(x) = \sum_{i+j=k} A_{x,i} B_{x,j} - \sum_{i+j=k-1} A_{x,i} B_{x,j}$. $A_{x,i}$ and $B_{x,i}$ are defined as follows.

- If $i > [k/2]$, $A_{x,i} = A_i(x)$ and $B_{x,i} = B_i(x)$.

- If $i \leq [k/2]$, $A_{x,i} = \mathbb{E}_a[\overline{A}(g_i(x,s))]$ and $A_{x,i} = \mathbb{E}_a[\overline{B}(g_i(x,s))]$, where $g_i$ is a $C_i, B_i$ denote the “flattened” form of $A_i$ and $B_i$.

We leave the explanation of “flattened” for later and explain the intuition behind the lemma first. Our goal is to construct $C_k$ such that $C_k(x)$ is a good approximation of $AB$ on average over $x$. We know that $A_i$ and $B_i$ are $\gamma^{i+1}$-approximation of $A$ and $B$ on average. Our hope is to use $x$ to draw samples $A_i$ and $B_i$ from $A_i$ and $B_i$, and apply the formula in Lemma 3.5 to get a good approximation of $AB$. In particular, a natural choice would be setting $A_{x,i} = A_i(x)$ and $B_{x,i} = B_i(x)$ for every $i \leq k$. However, if there exists a term $A_{x,i} B_{x,j}$ such that $A_{x,i}$ and $B_{x,j}$ are both bad approximation for a large enough fraction of $x$, we cannot guarantee to get a $O(\gamma^{k+1})$-approximation on average.
To avoid the above case, for every \( i \leq \lceil k/2 \rceil \) we use a sampler to approximate \( \langle A_i \rangle \) and \( \langle B_i \rangle \). This ensures that the chosen samples \( A_{x,i} \) and \( B_{x,i} \) are good with high probability. This guarantees that in each term \( A_{x,i}B_{x,j} \), at least one of \( A_{x,i} \) or \( B_{x,j} \) will be a good choice with high probability over \( x \). If \( A_{x,i} \) is a good choice with high probability, we can apply the average-case guarantee on \( B_{x,i} \) to get an average-case guarantee for \( C_k \), and vice versa. (Indeed, this is the sampler argument.) Therefore we can ensure that \( C_k(x) \) is good on average. Note that we only apply a sampler on \( A_i \) (or \( B_i \)) when \( i \leq \lceil k/2 \rceil \), which means \( A_i \) (or \( B_i \)) has small seed length. Therefore we don’t need to add too much redundant seed to make the sampler argument work.

In executing the above sketched idea, we run into the following problem: in each multiplication, the inner seed on both sides aggregates to the upper level. If we start with pseudodistributions with non-zero inner seed in the bottom level, the inner seed would become \( \Omega(n) \) in the topmost level. Therefore we need a way to limit the aggregation of inner seed.

In [BCG18], they run into a similar problem. To deal with this, they apply a different multiplication rule, “outer product,” in some special cases to deal with this. However, the seed.

\[ \text{come } \Omega(\log(1/\epsilon) + \log n \cdot \log(nw)) \]

\[ \text{This ensure that the chosen samples } A_{x,i} \text{ and } B_{x,i} \text{ are good with high probability over } x. \]

If \( A_{x,i} \) is a good choice with high probability, we can apply the average-case guarantee on \( B_{x,i} \) to get an average-case guarantee for \( C_k \), and vice versa. (Indeed, this is the sampler argument.) Therefore we can ensure that \( C_k(x) \) is good on average. Note that we only apply a sampler on \( A_i \) (or \( B_i \)) when \( i \leq \lceil k/2 \rceil \), which means \( A_i \) (or \( B_i \)) has small seed length. Therefore we don’t need to add too much redundant seed to make the sampler argument work.

In executing the above sketched idea, we run into the following problem: in each multiplication, the inner seed on both sides aggregates to the upper level. If we start with pseudodistributions with non-zero inner seed in the bottom level, the inner seed would become \( \Omega(n) \) in the topmost level. Therefore we need a way to limit the aggregation of inner seed.

In [BCG18], they run into a similar problem. To deal with this, they apply a different multiplication rule, “outer product,” in some special cases to deal with this. However, the outer product does not seem applicable in our construction. Nevertheless, we observe that whenever we use a sampler to select matrix \( A_{x,i} \), we only care about whether \( \langle A_i \rangle \) is close to \( A \), and we don’t need most of \( A_i(x) \) to be close to \( A \) anymore. Therefore we will “flatten” \( A_i \) whenever we apply a sampler. That is, recall that each \( A_i(x) \) is realized by the average of some matrices, \( \mathbb{E}_y [A_i(x, y)] \). We define the flattened form of \( A_i \), denoted by \( \overline{A}_i \), such that \( \overline{A}_i(x|y) = A_i(x, y) \). Observe that \( \langle \overline{A}_i \rangle = \langle A_i \rangle \) and \( s_{in}(\overline{A}_i) = 0 \). This guarantees that the inner seed length of \( A_i \) will not aggregate in \( C_k \). Moreover, while the flattening will increase the outer seed length of \( \overline{A}_i \), this is almost for free since we only flatten \( A_i \) when \( i \leq \lceil k/2 \rceil \), i.e. when \( A_i \) has relatively small seed length. As a result, this operation also helps us save a \( O(\log \log(1/\epsilon)) \) factor in the seed length.

We conclude by briefly discussing the seed length analysis. First note that we set \( \gamma = \frac{1}{\text{poly}(n)} \) to make sure that the error is affordable after a union bound. Now consider the inner seed length. Consider a term \( A_i B_j \) such that \( i \geq j \). In this term, part of the inner seed of \( C \) is passed to \( A_i \), and the other is used for the sampler on \( B_j \). Since the seed length of the sampler only needs to be as large as the “precision gap” between \( A_i \) and \( C_k \), the inner seed length of \( C_k \) can be maintained at roughly \( O(k \log(1/\gamma)) = O(\log(1/\epsilon)) \). However, after each multiplication, there’s actually a \( O(\log(nw/\gamma)) = O(\log(nw)) \) additive overhead. Note that this is necessary since the \( k = 0 \) case degenerates to the INW generator. Therefore after \( \log n \) levels of recursion, the inner seed length will be \( O(\log(1/\epsilon) + \log n \cdot \log(nw)) \).

Besides, we also need the outer seed length of \( C_k \) to be long enough so that we can apply a sampler on \( A_{[k/2]} \) and \( B_{[k/2]} \). The seed length caused by approximation accuracy \( \epsilon \) can be bounded similarly as the inner seed length. However, the \( O(\log n \cdot \log(nw)) \) inner seed length will be added to the outer seed length several times, because of the flattening operation. Nevertheless, since we only do flattening for \( A_i \) and \( B_i \) where \( i \leq \lceil k/2 \rceil \), this ensures that the flattening operation happens at most \( \log k \) times. So the total outer seed length will be bounded by \( O(\log(1/\epsilon) + \log k \cdot \log n \cdot \log(nw)) = O(\log(1/\epsilon) + \log \log(1/\epsilon) \cdot \log n \cdot \log(nw)) \), which is bounded by \( O(\log(1/\epsilon) + \log \log(nw) \cdot \log n \cdot \log(nw)) \) since \( O(\log(1/\epsilon)) \) is the dominating term when \( \log(1/\epsilon) \geq \log^3(nw) \).
4 Preliminaries

4.1 Averaging samplers

Definition 4.1. A function \( g : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m \) is a \((\varepsilon, \delta)\) (averaging) sampler if for every function \( f : \{0, 1\}^m \rightarrow [0, 1] \),

\[
\Pr_{x \in \{0, 1\}^n} \left[ \left| \frac{1}{|S|} \sum_{s \in \{0, 1\}^d} f(g(x, s)) - \frac{1}{|Y|} \sum_{y \in \{0, 1\}^m} f(y) \right| \leq \varepsilon \right] \geq 1 - \delta.
\]

It’s easy to show that samplers also work for \( f \) with general range by scaling and shifting.

Claim 4. Let \( g : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m \) be a \((\varepsilon, \delta)\)-sampler, and let \( \ell < r \in \mathbb{R} \). Then for every \( f : \{0, 1\}^m \rightarrow [\ell, r] \),

\[
\Pr_{x \in \{0, 1\}^n} \left[ \left| \frac{1}{|S|} \sum_{s \in \{0, 1\}^d} f(g(x, s)) - \frac{1}{|Y|} \sum_{y \in \{0, 1\}^m} f(y) \right| \leq \varepsilon (r - \ell) \right] \geq 1 - \delta.
\]

Proof. Let \( f' \) be the function such that \( f'(y) = (f(y) - \ell)/(r - \ell) \). Observe that the range of \( f' \) is in \([0, 1]\). By definition of sampler,

\[
\Pr_{x \in \{0, 1\}^n} \left[ \left| \frac{1}{|S|} \sum_{s \in \{0, 1\}^d} f'(g(x, s)) - \frac{1}{|Y|} \sum_{y \in \{0, 1\}^m} f'(y) \right| \leq \varepsilon \right] \geq 1 - \delta.
\]

By multiplying \((r - \ell)\) on both sides of the inequality inside the probability above we prove the claim. \(\square\)

In our construction, we will use the following sampler which is explicitly computable with small space.

Lemma 4.2 ([RVW01, Gol11]). For every \( \delta, \varepsilon > 0 \) and integer \( m \), there exists a \((\varepsilon, \delta)\)-sampler \( f : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m \) s.t. \( d = O(\log \log(1/\delta) + \log(1/\varepsilon)) \) and \( n = m + O(\log(1/\delta)) + O(\log(1/\varepsilon)) \). Moreover, for every \( x, y \), \( f(x, y) \) can be computed in space \( O(m + \log(1/\delta) + \log(1/\varepsilon)) \).

Remark 4.3. The original sampler in [RVW01] has a restriction on \( \varepsilon \). Such a restriction will cause a \( 2^{O(\log^*(nw/\varepsilon))} \) factor in our construction, as in [BCG18]. However, [RVW01] pointed out that the restriction is inherited from the extractor in [Zuc97], which breaks down when the error is extremely small. As observed in [Gol11], this restriction can be removed by plugging in a more recent extractor construction in [GUV09]. Note that there exists a space-efficient implementation of [GUV09] in [KNW08], so the resulting sampler is also space-efficient. For completeness we include a proof in Appendix A.

4.2 Matrix norms

As in [BCG18], we will use the infinity norm in this paper.

Definition 4.4. For every matrix \( A \in \mathbb{R}^{w \times w} \), \( \|A\| = \max_i \sum_j |A_{i,j}| \).

We record some well known properties of the infinity norm.
Claim 5. Let $A, B \in \mathbb{R}^{w \times w}$, $c \in \mathbb{R}$. Then

- $\|cA\| = |c| \|A\|
- \|A\| + \|B\| \leq \|A + B\|
- \|AB\| \leq \|A\| \|B\|
- \max_{i,j} |A_{i,j}| \leq \|A\|
- If $A$ is stochastic, then $\|A\| = 1$

Note that for any $(n,w)$-ROBP represented by $w \times w$ matrices $M_{[n]}^{(0,1)}$, $\|M_{i,j}\| = 1$ for every $0 \leq i \leq j \leq n$.

5 Approximate Matrix Multiplication via Samplers

In this section we formally prove the sampler arguments which will be used in our construction. Our proof strategy resembles that of [BCG18], with the following two crucial differences. First, we will define two different notions of “smallness” for our flattening idea. Second, in our construction we need the case where we use samplers to select matrices on both sides (Lemma 5.4).

We will consider mappings $A : \{0,1\}^n \rightarrow \mathbb{R}^{w \times w}$ which correspond to the implicit small norm matrices we discussed in the previous section. Borrowing notation from Definition 2.1, we use $\langle A \rangle$ to denote $\mathbb{E}_x [A(x)]$. First we define two different norms for the mapping $A$. The robust norm is similar to the notion of “smallness” in [BCG18], i.e. the average of norm of $A(x)$, while the norm of $A$ is simply the norm of $\langle A \rangle$, i.e. the norm of average of $A(x)$.

Definition 5.1. For every function $A : \{0,1\}^n \rightarrow \mathbb{R}^{w \times w}$, we define the norm of $A$ to be $\|A\| = \left\| \mathbb{E}_{x \in \{0,1\}^n} [A(x)] \right\|$, and the robust norm of $A$ to be $\|A\|_r = \mathbb{E}_{x \in \{0,1\}^n} [\|A(x)\|]$. Besides, we define the weight of $A$ to be $\mu(A) = \max_x \|A(x)\|$.

Claim 6. $\|A\| \leq \|A\|_r \leq \mu(A)$.

Proof. $\|A\| \leq \|A\|_r$ is by sub-additivity of $\|\cdot\|$, and $\|A\|_r \leq \mu(A)$ since $\|A\|_r$ is the average of values no larger than $\mu(A)$.

Next we show a simple lemma which will be used later. That is, a sampler for functions with range $[0,1]$ is also a sampler for matrix-valued functions, where the error is measured with infinity norm.

Lemma 5.2. For every function $A : \{0,1\}^m \rightarrow \mathbb{R}^{w \times w}$ and every $(\varepsilon, \delta)$-sampler $g : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$,

$$\Pr_{x \in \{0,1\}^n} \left[ \left\| \mathbb{E}_{s \in \{0,1\}^d} [A(g(x,s))] - \langle A \rangle \right\| \leq 2w\mu(A)\varepsilon \right] \geq 1 - w^2\delta.$$
Proof. Let $\mathcal{E}(y) = \mathcal{A}(y) - \langle A \rangle$. For every $i, j \in [w]$, observe that
\[
\max_y \mathcal{E}(y)_{i,j} - \min_y \mathcal{E}(y)_{i,j} = \max_y \mathcal{A}(y)_{i,j} - \min_y \mathcal{A}(y)_{i,j}
\]
By the property of sampler it follows that
\[
\Pr_{x \in \{0,1\}^n} \left[ \mathbb{E}_{s \in \{0,1\}^d} \left\| E_s \left[ \mathcal{E}(g(x,s))_{i,j} \right] \right\| \leq 2\varepsilon \mu(\mathcal{A}) \right] \geq 1 - \delta.
\]
Using a union bound,
\[
\Pr_{x \in \{0,1\}^n} \left[ \forall i, j \in [w], \mathbb{E}_{s \in \{0,1\}^d} \left[ \mathcal{E}(g(x,s))_{i,j} \right] \leq 2\varepsilon \mu(\mathcal{A}) \right] \geq 1 - w^2 \delta.
\]
Thus by definition of the infinity norm, we can conclude that
\[
\Pr_{x \in \{0,1\}^n} \left[ \left\| \mathbb{E}_{s \in \{0,1\}^d} \left[ \mathcal{E}(g(x,s)) \right] \right\| \leq 2w \mu(\mathcal{A}) \varepsilon \right] \geq 1 - w^2 \delta.
\]
which by sub-additivity of $\| \cdot \|$ implies
\[
\Pr_{x \in \{0,1\}^n} \left[ \left\| \mathbb{E}_{s \in \{0,1\}^d} \left[ \mathcal{A}(g(x,s)) \right] \right\| \leq \| A \| + 2w \mu(\mathcal{A}) \varepsilon \right] \geq 1 - w^2 \delta.
\]
\]

Corollary 5.3. For every function $\mathcal{A} : \{0,1\}^m \rightarrow \mathbb{R}^{w \times w}$ and every $(\varepsilon, \delta)$-sampler $g : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$,
\[
\Pr_{x \in \{0,1\}^n} \left[ \left\| \mathbb{E}_{s \in \{0,1\}^d} \left[ \mathcal{A}(g(x,s)) \right] \right\| \leq \| A \| + 2w \mu(\mathcal{A}) \varepsilon \right] \geq 1 - w^2 \delta.
\]
\]
\]

Proof. By sub-additivity of $\| \cdot \|$, \[ \left\| \mathbb{E}_{s \in \{0,1\}^d} \left[ \mathcal{A}(g(x,s)) \right] - \langle A \rangle \right\| \leq 2w \mu(\mathcal{A}) \varepsilon \] implies \[ \left\| \mathbb{E}_{s \in \{0,1\}^d} \left[ \mathcal{A}(g(x,s)) \right] \right\| \leq \| \langle A \rangle \| + 2w \mu(\mathcal{A}) \varepsilon. \] The claim now directly follows from Lemma 5.2. □

Now we introduce three different matrix multiplication rules. The first one is applying a sampler on both sides, and the second and third are applying sampler on only one side.

Lemma 5.4 (symmetric product). Consider $\mathcal{A} : \{0,1\}^n \rightarrow \mathbb{R}^{w \times w}$ and $\mathcal{B} : \{0,1\}^m \rightarrow \mathbb{R}^{w \times w}$. Let $f : \{0,1\}^k \times \{0,1\}^d \rightarrow \{0,1\}^n$ be a $(\delta, \varepsilon_A)$ sampler, and $g : \{0,1\}^k \times \{0,1\}^d \rightarrow \{0,1\}^m$ be a $(\delta, \varepsilon_B)$ sampler. Then
\[
\mathbb{E}_z \left[ \left\| \mathbb{E}_{x,y} \left[ \mathcal{A}(f(z,x)) \mathcal{B}(g(z,y)) \right] \right\| \right] \leq 2w^2 \delta \mu(\mathcal{A}) \mu(\mathcal{B}) + \left( \| A \| + 2w \mu(\mathcal{A}) \varepsilon_A \right) \left( \| B \| + 2w \mu(\mathcal{B}) \varepsilon_B \right).
\]
\]
\]

Proof. Let
\[
E_A = \left\{ z : \left\| \mathbb{E} \left[ \mathcal{A}(f(z,x)) \right] \right\| > \| A \| + 2w \mu(\mathcal{A}) \varepsilon_A \right\}.
\]

13
and
\[ E_B = \left\{ z : \left\| \mathbb{E}_y [\mathcal{B}(g(z, y))] \right\| > \|\mathcal{B}\| + 2w\mu(\mathcal{B})\varepsilon_B \right\}. \]

Define \( E = E_A \cup E_B \). By Lemma 5.3 and union bound, \( \Pr_z [z \in E] < 2w^2\delta \). Therefore
\[
\mathbb{E}_z \left[ \left\| \mathbb{E}_{x,y} [\mathcal{A}(f(z, x)) \mathcal{B}(g(z, y))] \right\| \right] = \Pr_z [z \in E] \mathbb{E}_{x,y} \left[ \left\| \mathbb{E}_y [\mathcal{A}(f(z, x)) \mathcal{B}(g(z, y))] \right\| \right]
+ \Pr_z [z \notin E] \mathbb{E}_{x,y} \left[ \left\| \mathbb{E}_y [\mathcal{A}(f(z, x))] \mathbb{E}_x [\mathcal{B}(g(z, y))] \right\| \right]
\leq 2w^2\delta \mu_\delta(\mathcal{A}) \mu(\mathcal{B}) + \mathbb{E}_{x,y} \left[ \left\| \mathbb{E}_x [\mathcal{A}(f(z, x))] \right\| \left\| \mathbb{E}_y [\mathcal{B}(g(z, y))] \right\| \right]
\leq 2w^2\delta \mu_\delta(\mathcal{A}) \mu(\mathcal{B}) + (\|\mathcal{A}\| + 2w\mu(\mathcal{A})\varepsilon_A) (\|\mathcal{B}\| + 2w\mu(\mathcal{B})\varepsilon_B).
\]
The second last inequality is by the fact that \( \|\cdot\| \) is non-negative and sub-multiplicative.

**Lemma 5.5** (left product). Consider \( \mathcal{A} : \{0,1\}^k \to \mathbb{R}^{w \times w} \) and \( \mathcal{B} : \{0,1\}^m \to \mathbb{R}^{w \times w} \). Let \( g : \{0,1\}^k \times \{0,1\}^{d_B} \to \{0,1\}^m \) be a \((\delta, \varepsilon_B)\) sampler. Then
\[
\mathbb{E}_z \left[ \left\| \mathbb{E}_y [\mathcal{A}(z) \mathcal{B}(g(z, y))] \right\| \right] \leq w^2\delta \mu_\delta(\mathcal{A}) \mu(\mathcal{B}) + \|\mathcal{A}\| \left(\|\mathcal{B}\| + 2w\mu(\mathcal{B})\varepsilon_B\right).
\]

**Proof.** Let
\[ E = \left\{ z : \left\| \mathbb{E}_y [\mathcal{B}(g(z, y))] \right\| > \|\mathcal{B}\| + 2w\mu(\mathcal{B})\varepsilon_B \right\}. \]

By Lemma 5.3, \( \Pr_z [z \in E] < 2w^2\delta \). Therefore
\[
\mathbb{E}_z \left[ \left\| \mathbb{E}_y [\mathcal{A}(z) \mathcal{B}(g(z, y))] \right\| \right] = \Pr_z [z \in E] \mathbb{E}_{x,y} \left[ \left\| \mathbb{E}_y [\mathcal{A}(z) \mathcal{B}(g(z, y))] \right\| \right]
+ \Pr_z [z \notin E] \mathbb{E}_{x,y} \left[ \left\| \mathbb{E}_y [\mathcal{A}(z)] \mathbb{E}_x [\mathcal{B}(g(z, y))] \right\| \right]
\leq w^2\delta \mu_\delta(\mathcal{A}) \mu(\mathcal{B}) + \Pr_z [z \notin E] \cdot \mathbb{E}_{x,y} \left[ \left\| \mathcal{A}(z) \right\| \left\| \mathbb{E}_y [\mathcal{B}(g(z, y))] \right\| \right]
\leq w^2\delta \mu_\delta(\mathcal{A}) \mu(\mathcal{B}) + \Pr_z [z \notin E] \mathbb{E}_{x,y} \left[ \|\mathcal{A}(z)\| \cdot (\|\mathcal{B}\| + 2w\mu(\mathcal{B})\varepsilon_B) \right]
\leq w^2\delta \mu_\delta(\mathcal{A}) \mu(\mathcal{B}) + \|\mathcal{A}\| \left(\|\mathcal{B}\| + 2w\mu(\mathcal{B})\varepsilon_B\right).
\]
The third last inequality is by sub-multiplicativity of \( \|\cdot\| \), the second last inequality is by non-negativity of \( \|\cdot\| \), and the last inequality is by the fact that
\[
\Pr_z [z \notin E] \cdot \mathbb{E}_{x,y} \left[ \|\mathcal{A}(z)\| \right] = \mathbb{E}_z \left[ \|\mathcal{A}(z)\| \cdot 1(z \notin E) \right] = \|\mathcal{A}\|.
\]

**Lemma 5.6** (right product). Consider \( \mathcal{A} : \{0,1\}^k \to \mathbb{R}^{w \times w} \) and \( \mathcal{B} : \{0,1\}^m \to \mathbb{R}^{w \times w} \). Let \( f : \{0,1\}^k \times \{0,1\}^{d_A} \to \{0,1\}^m \) be a \((\delta, \varepsilon_A)\) sampler. Then
\[
\mathbb{E}_z \left[ \left\| \mathbb{E}_x [\mathcal{A}(f(z, x)) \mathcal{B}(z)] \right\| \right] \leq w^2\delta \mu_\delta(\mathcal{A}) \mu(\mathcal{B}) + (\|\mathcal{A}\| + 2w\mu(\mathcal{A})\varepsilon_A) \|\mathcal{B}\|.
\]

14
Proof. Let
\[
E = \left\{ z : \| \mathbb{E}_x [A(f(z, x))] \| > \| A \| + 2w \mu(A) \varepsilon_A \right\}.
\]
By Lemma 5.3, \( \Pr_z [z \in E] < w^2 \delta \). Therefore
\[
\mathbb{E}_z \left[ \| \mathbb{E}_x [A(f(z, x))B(z)] \| \right] = \Pr_z [z \in E] \mathbb{E}_z \left[ \| \mathbb{E}_x [A(f(z, x))B(z)] \| \right]
+ \Pr_z [z \not\in E] \mathbb{E}_z \left[ \| \mathbb{E}_x [A(f(z, x))B(z)] \| \right]
\leq w^2 \mu(A) \mu(B) + \Pr_z [z \not\in E] \cdot \mathbb{E}_z \left[ \| \mathbb{E}_x [A(f(z, x))] \| \| B(z) \| \right]
\leq w^2 \mu(A) \mu(B) + (\| A \| + 2w \mu(A) \varepsilon_A) \cdot \Pr_z [z \not\in E] \mathbb{E}_z \| B(z) \|
\leq w^2 \mu(A) \mu(B) + (\| A \| + 2w \mu(A) \varepsilon_A) \| B \|_r.
\]

\[
\square
\]

6 Main Construction

In this section we show our main construction and prove its correctness. We first introduce several definitions.

**Definition 6.1.** For every mapping \( \mathcal{A} : \{0, 1\}^n \rightarrow \mathbb{R}^{w \times w} \) and every matrix \( A \in \mathbb{R}^{w \times w} \), we define \( A - A \) to be the mapping s.t. \( (A - A)(x) = A(x) - A \).

**Definition 6.2.** Consider \( A \in \mathbb{R}^{w \times w} \) and \( \mathcal{A} : \{0, 1\}^n \rightarrow \mathbb{R}^{w \times w} \). \( \mathcal{A} \) is a \( \varepsilon \)-approximator of \( A \) if \( \| \mathbb{E}_x [A(x)] - A \| \leq \varepsilon \), i.e. \( \| \mathcal{A} - A \| \leq \varepsilon \). \( \mathcal{A} \) is a \( \varepsilon \)-robust approximator of \( A \) if \( \mathbb{E}_x [\| \mathcal{A}(x) - A \|] \leq \varepsilon \), i.e. \( \| \mathcal{A} - A \|_r \leq \varepsilon \).

Now we define a robust PRPD. Note that a \((n, w, \varepsilon)\)-robust PRPD \((G, \rho)\) is also a \(\mu(G, \rho)\)-bounded \((n, w, \varepsilon)\)-PRPD.

**Definition 6.3.** \((G, \rho) : \{0, 1\}^{s_{\text{out}}} \times \{0, 1\}^{s_{\text{in}}} \times [\mu] \rightarrow \{0, 1\}^n \times \mathbb{R} \) is a \((n, w, \varepsilon)\)-robust PRPD if for every \((n, w)\)-ROBP and its matrix representation \([M]_{[0, 1]}^{(n)}\) the following holds. Let \( \mathcal{A} : \{0, 1\}^{s_{\text{out}}} \times \{0, 1\}^{s_{\text{in}}} \rightarrow \mathbb{R}^{w \times w} \) denote the mapping
\[
\mathcal{A}(x, y) = \mathbb{E}_{i \in [\mu]} \left[ \rho(x, y, i) \cdot M_{0..n}^{G(x, y, i)} \right].
\]

- Every \( \rho(x, y, i) \) is either \( \mu \) or \( -\mu \). In other word, \( \mathcal{A}(x, y) \) is the summation of transition matrices with coefficient \( \pm 1 \).
- Let \( \hat{\mathcal{A}} \) denote the mapping \( \hat{\mathcal{A}}(x) = \mathbb{E}_y [\mathcal{A}(x, y)] \). Then \( \hat{\mathcal{A}} \) is a \( \varepsilon \)-robust approximator for \( M_{0..n} \).

We say \( \mu \) is the weight of \((G, \rho)\), denoted by \( \mu(G, \rho) \). \( s_{\text{out}} \) is the outer seed length of \((G, \rho)\), denoted by \( s_{\text{out}}(G, \rho) \). \( s_{\text{in}} \) is the inner seed length of \((G, \rho)\), denoted by \( s_{\text{in}}(G, \rho) \). We write \( s(G, \rho) = s_{\text{out}}(G, \rho) + s_{\text{in}}(G, \rho) \) for short. We say \((G, \rho)\) is explicit if it can be computed in \( O(s(G, \rho)) \) space.

We say \( \mathcal{A} \) is the matrix form of \((G, \rho)\) on \( M_{0..n} \), and the definition of \( s_{\text{out}}, s_{\text{in}}, \mu \) on \((G, \rho)\) also apply to \( \mathcal{A} \). We say \( \hat{\mathcal{A}} \) is the robust matrix form of \((G, \rho)\) on \( M_{0..n} \).
Remark 6.4. The above definition is similar to Definition 2.1, but each matrix \( A(x, y) \) is realized with \( \mu \) matrices instead of one matrix. These \( \mu \) matrices will never be separated even after flattening. We do this in order to ensure that the matrix form always take bit-strings as input. This ensures that we can increase the outer and inner seed length of \( A \) arbitrarily: we can construct the new mapping \( A' : \{0, 1\}^s_{\text{out}} \times \{0, 1\}^s_{\text{in}} \rightarrow \{0, 1\}^n \times \mathbb{R} \) be \( \{0, 1\}^n \times \mathbb{R} \) be a \((n, w, \varepsilon)\)-robust PRPD.

The following is some additional basic properties about robust PRPD and its flattened form.

Claim 7. Let \((G, \rho) : \{0, 1\}^s_{\text{out}} \times \{0, 1\}^s_{\text{in}} \times [\mu] \rightarrow \{0, 1\}^n \times \mathbb{R} \) be a \((n, w, \varepsilon)\)-robust PRPD. For every \((n, w)\)-ROBP \( M_0^0, M_1^1, \ldots, M_n^n \) the following holds.

- Let \( \hat{A} \) be the robust matrix form of \((G, \rho)\) on \( M_{0..n} \). Then \( \mu(\hat{A}) \leq \mu(G, \rho) \).
- Let \( A \) denote the matrix form of \((G, \rho)\) on \( M_{0..n} \). Let \( \overline{A} : \{0, 1\}^s_{\text{out}} + s_{\text{in}} \rightarrow \mathbb{R}^{w \times w} \) denote the mapping \( \overline{A}(x|y) = A(x, y) \). We say \( \overline{A} \) is the flattened matrix form of \((G, \rho)\) on \( M_{0..n} \). Then \( \overline{A} \) is an \( \varepsilon \)-approximator for \( M_{0..n} \), and \( \mu(\overline{A}) \leq \mu(G, \rho) \).

Proof. Recall that for every string \( r \in \{0, 1\}^n \), \( \|M_{0..n}^r\| = 1 \). By sub-additivity of \( \|\cdot\| \) we have \( \|A(x, y)\| \leq \mu(G, \rho) \) for every \( x, y \), which implies \( \mu(\overline{A}) \leq \mu(G, \rho) \). By sub-additivity and scalibility of \( \|\cdot\| \), we have \( \mu(\overline{A}) \leq \mu(A) \). To show that \( \overline{A} \) is an \( \varepsilon \)-approximator of \( M_{0..n} \), observe that \( \overline{A}' \) is also an \( \varepsilon \)-approximator of \( M_{0..n} \) by Claim 6, and note that \( \langle A \rangle = \langle A' \rangle \). \( \square \)

Now we prove our main lemma. The following lemma allows us to construct robust PRPDs for \((2m, w)\) ROBPs from robust PRPDs for \((m, w)\) ROBPs, without increasing the seed length too much. We will recursively apply this lemma for \( \log n \) levels to get a \((n, w, \varepsilon)\)-robust PRPD. The basic idea is as described in Lemma 3.6.

Lemma 6.5. Suppose there exists \( s_{\text{out}}, s_{\text{in}} \) such that the following conditions hold.

- For every \( 0 \leq i \leq k \), there exists a \((m, w, \gamma^{i+1})\)-robust \( \text{PRPD} \) \( (G_i, \rho_i) \) s.t. \( \mu(G_i, \rho_i) \leq \binom{m}{i}^{-1} \) and \( s_{\text{out}}(G, \rho) \leq s_{\text{out}} \). Moreover, for every \( 0 \leq i \leq \lfloor k/2 \rfloor \), \( s(G_i, \rho_i) \leq s_{\text{out}} \).
- For every \( i \leq \lfloor k/2 \rfloor \), there exists a \((\varepsilon_i, \delta)\)-sampler \( g_i : \{0, 1\}^{s_{\text{out}}} \times \{0, 1\}^{d_i} \rightarrow \{0, 1\}^{s(G_i, \rho_i)} \), where \( \varepsilon_i \leq \gamma^{i+1}/(w \cdot \binom{m}{i}) \) and \( \delta \leq \gamma^{k+1}/(w^2 \cdot \binom{2^m}{i}) \).
- For every \( i \geq j \geq 0 \) s.t. \( i + j \leq k \), if \( j \leq i \leq \lfloor k/2 \rfloor \), then \( d_i + d_j \leq s_{\text{in}} \). If \( i > \lfloor k/2 \rfloor \), then \( s_{\text{in}}(G_i, \rho_i) + d_j \leq s_{\text{in}} \).

Then there exists a \((2m, w, (11\gamma)^{k+1})\)-robust \( \text{PRPD} \) \( (G, \rho) \) s.t. \( s_{\text{out}}(G, \rho) = s_{\text{out}}, s_{\text{in}}(G, \rho) = s_{\text{in}} \) and \( \mu(G, \rho) \leq \binom{2^m}{i}^{-1} \).

Proof. Fix any \((2m, w)\)-ROBP with matrix representation \( M_{[2m]}^{[0,1]} \). Let \( A = M_{0..m} \) and \( B = M_{m..2m} \). For every \( 0 \leq i \leq k \), let \( A_i, \hat{A}_i, \overline{A}_i \) denote the matrix form, robust matrix form and flattened matrix form of \((G, \rho)\) on \( M_{0..m} \) respectively. Let \( B_i, \hat{B}_i, \overline{B}_i \) denote the matrix form, robust matrix form and flattened matrix form of \((G, \rho)\) on \( M_{m..2m} \) respectively. By definition,
\( \hat{A}_i \) and \( \hat{B}_i \) are \( \gamma^{i+1} \)-robust approximator for \( A \) and \( B \) respectively. By Claim 7, \( \mathcal{A}_i \) and \( \mathcal{B}_i \) are \( \gamma^{i+1} \)-approximator for \( A \) and \( B \) respectively. Moreover, we will increase the outer seed length of \( \mathcal{A}_i \) and \( \mathcal{B}_i \) to match the length of the given input when necessary. (See Remark 6.4)

Now for every \( x, y \) we define a mapping \( C_k : \{0, 1\}^{s_{\mathrm{out}} + s_{\mathrm{in}}} \rightarrow \mathbb{R}^{w \times w} \) as follows. Note that \( C_k \) corresponds to the matrix form of \( (G, \rho) \) on \( M_{0..2m} \).

1. For every \( 0 \leq i \leq \lceil k/2 \rceil \), let \( a_i \) be the prefix of \( y \) of length \( d_i \) and \( b_i \) be the suffix of \( y \) of length \( d_i \). Define \( A_{x,y,i} = \mathcal{A}_i(g_i(x, a_i)) \) and \( B_{x,y,i} = \mathcal{B}_i(g_i(x, b_i)) \).

2. For every \( \lceil k/2 \rceil < i \leq k \), let \( a_i \) be the prefix of \( y \) of length \( s_{\mathrm{in}}(A_i) \) and \( b_i \) be the suffix of \( y \) of length \( s_{\mathrm{in}}(B_i) \). Define \( A_{x,y,i} = \mathcal{A}_i(x, a_i) \) and \( B_{x,y,i} = \mathcal{B}_i(x, b_i) \).

3. Define \( C_k(x, y) = \sum_{i+j=k} A_{x,y,i}B_{x,y,j} \) - \( \sum_{i+j=k-1} A_{x,y,i}B_{x,y,j} \).

Note that for every \( i + j \leq k \), prefix \( a_i \) and suffix \( b_j \) of \( y \) never overlap.

By expanding every \( A_{x,y,i}B_{x,y,j} \) term with distributive law, we can see that each small term in \( A_{x,y,i}B_{x,y,j} \) has coefficient \( \pm 1 \), which satisfies the first condition of robust PRPD. Moreover, the total number of terms after expanding is

\[
\mu(C_k) \leq \sum_{i+j=k} \binom{m-1}{i} \binom{m-1}{j} + \sum_{i+j=k-1} \binom{m-1}{i} \binom{m-1}{j} = \binom{2m-1}{k}.
\]

It remains to show that \( C_k \) satisfies the second condition of robust PRPD, i.e. \( \mathbb{E}_y[C_k(x, y)] \) is a good approximation of \( M_{0..2m} = AB \) on average over \( x \). Observe that

\[
\mathbb{E}_x \left[ \left\| \mathbb{E}_y[C_k(x, y)] - AB \right\| \right] = \mathbb{E}_x \left[ \left\| \mathbb{E}_y[C_k(x, y)] - AB \right\| \right]
\]

\[
\leq \sum_{i+j=k} \mathbb{E}_x \left[ \left\| \mathbb{E}_y[(A_{x,y,i} - A)(B_{x,y,j} - B)] \right\| \right]
\]

\[
+ \sum_{i+j=k-1} \mathbb{E}_x \left[ \left\| \mathbb{E}_y[(A_{x,y,i} - A)(B_{x,y,j} - B)] \right\| \right]
\]

\[
+ \mathbb{E}_x \left[ \left\| \mathbb{E}_y[(A_{x,y,k} - A)B] \right\| \right] + \mathbb{E}_x \left[ \left\| \mathbb{E}_y[A(B_{x,y,k} - B)] \right\| \right],
\]

by decomposing \( C_k(x, y) - AB \) with the equation in the proof of Lemma 3.5 and applying sub-additivity of \( \| \cdot \| \).

First we consider the last two terms. Since \( \| B \| = 1 \), by sub-multiplicativity we have

\[
\mathbb{E}_x \left[ \left\| \mathbb{E}_y[(A_{x,y,k} - A)B] \right\| \right] \leq \mathbb{E}_x \left[ \left\| \mathbb{E}_y[A_{x,y,k} - A] \right\| \right].
\]

Now consider two cases. If \( k \geq 2 \), then

\[
\mathbb{E}_x \left[ \left\| \mathbb{E}_y[A_{x,y,k} - A] \right\| \right] = \mathbb{E}_x \left[ \left\| \hat{A}_k(x) - A \right\| \right] \leq \gamma^{k+1}
\]

by definition. If \( k < 2 \), then

\[
\mathbb{E}_x \left[ \left\| \mathbb{E}_y[A_{x,y,k} - A] \cdot B \right\| \right] = \mathbb{E}_x \left[ \left\| \mathbb{E}_x \left[ \mathcal{A}_k(g_k(x, a_k)) - A \right] \right\| \cdot B \right].
\]
Apply Lemma 5.6 on $\overline{A}_{k} - A$ and the dummy mapping $B$ s.t. $B(x) = B$ for every $x$, we can derive that the above formula is bounded by $w^{2} \delta (m-1)(m-1) + 3 \gamma^{i+j+1}$. For the term $E_{x} \left[ \|E_{y} (A(B_{x,y,k} - B)) \| \right]$ we can get the same bound with a similar proof.

Now consider the terms in the form $E_{x} \left[ \|E_{y} [(A_{x,y,i} - A)(B_{x,y,j} - B)] \| \right]$. First consider the case $i, j \leq \lfloor k/2 \rfloor$. Then

$$E_{x} \left[ \|E_{y} ((A_{x,y,i} - A)(B_{x,y,j} - B)) \| \right]$$

$$= E_{x} \left[ \left\| \frac{A_{i}}{a_{i}} (g_{i}(x,a_{i})) - A \right\| E_{b_{j}} \left[ B_{k}(g_{j}(x,b_{j})) - B \right] \right\|$$ (since $a_{i}, b_{j}$ don’t overlap)

$$\leq 2w^{2} \delta \cdot \left( \frac{m-1}{i} \right) \cdot \left( \frac{m-1}{j} \right) + 9 \gamma^{i+j+2}. \text{(by Lemma 5.4)}$$

Next consider the case $i > \lfloor k/2 \rfloor, j \leq \lfloor k/2 \rfloor$. Then

$$E_{x} \left[ \|E_{y} ((A_{x,y,i} - A)(B_{x,y,j} - B)) \| \right]$$

$$= E_{x} \left[ \left\| \frac{A_{i}}{a_{i}} (x) \cdot E_{b_{j}} \left[ B_{k}(g_{j}(x,b_{j})) - B \right] \right\| \right]$$ (since $a_{i}, b_{j}$ don’t overlap)

$$\leq w^{2} \delta \cdot \left( \frac{m-1}{i} \right) \cdot \left( \frac{m-1}{j} \right) + 3 \gamma^{i+j+2}. \text{(by Lemma 5.6)}$$

Similarly for the case that $i \leq \lfloor k/2 \rfloor, j > \lfloor k/2 \rfloor$ we can show that

$$E_{x} \left[ \|E_{y} ((A_{x,y,i} - A)(B_{x,y,j} - B)) \| \right] \leq w^{2} \delta \cdot \left( \frac{m-1}{i} \right) \cdot \left( \frac{m-1}{j} \right) + 3 \gamma^{i+j+2}$$

by Lemma 5.5. Finally, note that the case $i, j > \lfloor k/2 \rfloor$ does not exist because $i + j \leq k$.

Taking the summation of all the cases, we get

$$E_{x} \left[ \left\| E_{y} [C_{k}(x,y)] - AB \right\| \right] \leq 2w^{2} \delta \cdot \left( \sum_{i+j=k} \left( \frac{m-1}{i} \right) \left( \frac{m-1}{j} \right) + \sum_{i+j=k-1} \left( \frac{m-1}{i} \right) \left( \frac{m-1}{j} \right) + \left( \frac{m-1}{k} \right) \right)$$

$$+ (k+1) \cdot 9 \gamma^{k+2} + k \cdot 9 \gamma^{k+1} + 2 \cdot 3 \gamma^{k+1}$$

$$\leq 4w^{2} \delta \cdot \left( \frac{2m-1}{k} \right) + (9k+9) \gamma^{k+2} + (9k+6) \gamma^{k+1}$$

$$\leq (10k+11) \gamma^{k+1}$$

$$\leq (11 \gamma)^{k+1}.$$
Finally we analyze the seed length of the recursive construction, and present the main theorem.

**Theorem 6.6.** There exists an explicit \((n, w, \varepsilon)\)-robust PRPD \((G, \rho)\) such that

- \(s_{\text{out}}(G, \rho) = O \left( \log(1/\varepsilon) + \log n \log(nw) \log \left( \frac{\log(1/\varepsilon)}{\log n} \right) \right)\)

- \(s_{\text{in}}(G, \rho) = O \left( \log(1/\varepsilon) + \log n \log(nw) \log \left( \frac{\log(1/\varepsilon)}{\log n} \right) \right)\)

- \(\mu(G, \rho) = \text{poly}(1/\varepsilon)\)

Moreover, for every \(B\) the approximator \(G\) has the same corresponding pseudodistribution.

**Proof.** Let \(c\) be the constant such that for every \(\varepsilon, \delta > 0\) there exists a \((\varepsilon, \delta)\)-sampler \(g : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m\) such that \(n = m + c \log(1/\varepsilon) + c \log(1/\delta)\) and \(d = c \log(1/\varepsilon) + c \log \log(1/\delta)\), as guaranteed in Lemma 4.2. WLOG assume that \(n\) is a power of 2. Define \(\gamma = 1/n^4\). For every \(0 \leq h \leq \log n\), every \(k \geq 0\), we will inductively prove that there exists a \((2^h, w, (11^h \gamma)^k+1)\)-robust PRPD \((G_{h,k}, \rho_{h,k})\) with the following parameters.

- If \(k \leq 1\), \(s_{\text{out}}(G_{h,k}, \rho_{h,k}) \leq h \cdot (3ck \log(n/\gamma) + 7c \log(w/\gamma))\)

- If \(k > 1\), \(s_{\text{out}}(G_{h,k}, \rho_{h,k}) \leq 4ck \log(n/\gamma) + (\lfloor \log k \rfloor + 1) \cdot h \cdot (10c \log(w/\gamma))\)

- If \(k \leq 1\), \(s_{\text{in}}(G_{h,k}, \rho_{h,k}) \leq ck \log(n/\gamma) + 4c \log(w/\gamma)\)

- If \(k > 1\), \(s_{\text{in}}(G_{h,k}, \rho_{h,k}) \leq ck \log(n/\gamma) + h \cdot (4c \log(kw/\gamma))\)

- \(\mu(G_{h,k}, \rho_{h,k}) = \max(1, (2^{h-1})^k)\)

We will write \(s_{\text{out}, h, k} = s_{\text{out}}(G_{h,k}, \rho_{h,k})\) and \(s_{\text{in}, h, k} = s_{\text{out}}(G_{h,k}, \rho_{h,k})\) for short. First consider the terminal case \(2k \geq 2^h\) or \(h = 0\). In this case we simply take \(s_{\text{out}, h, k} = 0\), \(s_{\text{in}, h, k} = 2^h \leq 2k\) and \(\mu(G_{h,k}, \rho_{h,k}) = 1\) s.t. \(G_{h,k}(x, y, i) = y\) and \(\rho_{h,k}(x, y, i) = 1\). For the other cases, we show that we can get the intended parameters by constructing \((G_{h,k}, \rho_{h,k})\) with the recursion in Lemma 6.5. Note that based on the induction hypothesis we can assume \(G_{a,h-1,k}\) and \(G_{a+2^{h-1}, h-1, k}\) have exactly the same parameters, so we consider the parameter of \(G_{a,h-1,k}\) only. We have seen that the bound for \(\mu(G_{h,k}, \rho_{h,k})\) is correct. First we show that the bound for \(s_{\text{in}, h, k}\) is correct. Recall that in the recursion we take parameters \(d_i = c \log(1/\varepsilon_i) + c \log \log(1/\delta) \leq ci \log(n/\gamma) + 2c \log(knw/\gamma)\), based on the fact that \(\left(\frac{2^h - 1}{i}\right) \leq n^i\). Now consider the restriction on \(s_{\text{in}}(G_k)\) in our recursion. For \(i + j \leq k\) and \(j \leq i \leq \lceil k/2 \rceil\), we need

\[
d_i + d_j \leq ck \log(n/\gamma) + 4c \log(knw/\gamma) \leq s_{\text{in}, h, k}
\]

which is true. For \(i + j \leq k\) and \(i > \lceil k/2 \rceil\), we need

\[
s_{\text{in}, h-1, i} + d_j \leq ci \log(1/\gamma) + (h - 1) \cdot 4c \log(inw/\gamma) + (cj \log(1/\gamma) + 2c \log(knw/\gamma)) \leq ck \log(1/\gamma) + h \cdot 4c \log(knw/\gamma) \leq s_{\text{in}, h, k}
\]

which is also true. Moreover, observe that when \(k \leq 1\) it is always the case that \(i, j \leq \lceil k/2 \rceil\).

Therefore the third condition is also true. Finally we show that the bound for \(s_{\text{out}, h, k}\) is also
In the last inequality we use the fact that $\lceil k/2 \rceil > 1$. Observe that for every $i \leq \lfloor k/2 \rfloor$,

$$s_{\text{out}, h-1,i} + s_{\text{in}, h-1,i} + c \log(1/\delta) + c \log(1/\varepsilon_i) \leq s_{\text{out}, h,k}.$$ 

Since $s_{\text{out}, h-1,i} \leq s_{\text{out}, h-1,\lfloor k/2 \rfloor}$ and $s_{\text{in}, h-1,i} \leq s_{\text{in}, h-1,\lfloor k/2 \rfloor}$ for every $i$, it suffices to show that

$$s_{\text{out}, h-1,\lfloor k/2 \rfloor} + s_{\text{in}, h-1,\lfloor k/2 \rfloor} + c \log(1/\delta) + c \log(1/\varepsilon_{\lfloor k/2 \rfloor}) \leq s_{\text{out}, h,k}.$$

First we consider $k \leq 1$, which is the case that $\lceil k/2 \rceil = k$. Then

$$s_{\text{out}, h-1,\lfloor k/2 \rfloor} + s_{\text{in}, h-1,\lfloor k/2 \rfloor} + c \log(1/\delta) + c \log(1/\varepsilon_{\lfloor k/2 \rfloor})$$

$$\leq s_{\text{out}}(G_{a,h-1,k}) + 3ck \log(n/\gamma) + 7c \log(n/\gamma)$$

$$\leq h \cdot (3ck \log(n/\gamma) + 7c \log(n/\gamma))$$

$$\leq s_{\text{out}, h,k}.$$ 

Finally we consider the case $k > 1$. Observe that

$$s_{\text{out}, h-1,\lfloor k/2 \rfloor} + s_{\text{in}, h-1,\lfloor k/2 \rfloor} + c \log(1/\delta) + c \log(1/\varepsilon_{\lfloor k/2 \rfloor})$$

$$\leq s_{\text{out}, h-1,\lfloor k/2 \rfloor} + s_{\text{in}, h-1,\lfloor k/2 \rfloor} + \frac{3k + 1}{2} \cdot c \log(n/\gamma) + 3c \log(w/\gamma)$$

$$\leq s_{\text{out}, h-1,\lfloor k/2 \rfloor} + (2k + 1) \cdot c \log(n/\gamma) + (h - 1) \cdot 4c \log(w/\gamma) + 7c \log(w/\gamma)$$

$$\leq 4c \cdot \left(\log(n/\gamma) + \left(\left\lfloor \log\left(\frac{k}{2}\right)\right\rfloor + 1\right) \cdot (h - 1) \cdot (10c \log(nw/\gamma))\right)$$

$$+ (2k + 1) \cdot c \log(n/\gamma) + (h - 1) \cdot 4c \log(w/\gamma) + 7c \log(w/\gamma)$$

$$\leq 4ck \log(n/\gamma) + \left(\left\lfloor \log\left(\frac{k}{2}\right)\right\rfloor + 1\right) \cdot (h - 1) \cdot (10c \log(nw/\gamma)) + h \cdot 10c \log(nw/\gamma)$$

$$\leq s_{\text{out}, h,k}.$$ 

In the last inequality we use the fact that $\lceil \log k \rceil = \lceil \log([k/2]) \rceil + 1$ for every $k > 1$.

Finally, note that $(11 \log n/\gamma) = n^{\log_{31} 11} \cdot n^{-4} \leq n^{-0.5}$. By taking $h = \log n$ and $k = \log(1/\varepsilon) \log(1/n^{0.5})$, we get a $(n, w, \varepsilon)$-robust PRPD.

\[\square\]

**Remark 6.7.** To get the seed length we claimed in Theorem 1, observe that the log(1/\varepsilon) term is dominating when log(1/\varepsilon) ≥ log^3(nw). Therefore we can simply replace the log log(1/\varepsilon) factor on the $O(\log n \log(nw))$ term with log log(nw).

### 7 Discussion and Open Questions

We discuss some natural questions that arise from our work.

- In our construction, we applied the sampler argument in [BCG18] without constructing small-norm matrices explicitly. This is probably hinting that negative weight is not essentially required for the sampler argument. Is it possible to apply the sampler argument to construct a PRG (instead of PRPD) with improved dependency on error?
• Is there an explicit PRPD which matches the seed length of the hitting set generator in [HZ18], i.e. $O(\log(w/\varepsilon))$ when $n = \text{poly} \log(w)$? A possible direction is to adapt our construction to a $t$-ary recursion tree where $t = \log^{1-\Omega(1)} n$ instead of a binary tree, as in [NZ96, Arm98]. However, a direct adaptation requires us to apply a sampler on $(t - 1)$-children in each recursion, and for every sampler we will lose some “inner seed” which cannot be recycled. In our construction we see that the inner seed of a sampler contains a $\log w$ term. Therefore in each recursion we need to pay at least $(t - 1) \log w$ which is too expensive. Is it possible to make the sampler argument work with a shorter inner seed?

• Is it possible to improve the seed length to $\tilde{O}(\log^2 n + \log(w/\varepsilon))$, even in some restricted settings? We note that there are two things which cause the $\Omega(\log n \cdot \log w)$ term in our construction. The first one is the inner seed of sampler, which is related to the question above. The second one is the restriction on the outer seed length, which is analogous to “entropy loss” if we view the samplers as extractors. Note that [RR99] shows how to “recycle entropy” in the INW generator in some restricted settings, but it is not clear how to apply the extractor-type analysis of INW generator in our construction.

References


Proof of Lemma 4.2

Lemma A.1 (Lemma 4.2, restated. [RVW01, Gol11]). For every $\delta, \varepsilon > 0$ and integer $m$, there exists a $(\varepsilon, \delta)$- sampler $f : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ s.t. $d = O(\log \log (1/\delta) + \log (1/\varepsilon))$ and $n = m + O(\log (1/\delta)) + O(\log (1/\varepsilon))$. Moreover, for every $x, y$, $f(x, y)$ can be computed in space $O(m + \log (1/\delta) + \log (1/\varepsilon))$.

We will use the equivalence between seeded randomness extractor and oblivious sampler by Zuckerman [Zuc97]. To achieve the parameter we need, we need a “high-entropy seeded extractor” such that the seed length only depends on entropy loss but not the length of source. We will use the standard “block-source” construction for high-entropy extractor which can be found in [GW97, RVW01]. For simplicity, we will use simple composition instead of zig-zag composition [RVW01] because we are not aiming for optimal entropy loss. We will use the following standard lemmas for the extractor construction. Some of the following lemmas are implicit in their original source, and we recommend the readers to see [GUV09, Vad12] for a proof.

Definition A.2 ([CG88]). $(X_1, X_2)$ is a $(k_1, k_2)$- block source if $X_1$ is a $k_1$-source, and for every $x_1 \in \text{Supp}(X)$, $X_2$ conditioned on $X_1 = x_1$ is a $k_2$-source.

Lemma A.3 ([GW97]). Let $X \in \{0, 1\}^n$ be a $(n - \Delta)$ source. Then for every integer $0 \leq t \leq n$, $X$ is $\varepsilon$- close to a $(t - \Delta, n - t - \Delta - \log (1/\varepsilon))$- block source $(X_1, X_2)$ where $X_1 \in \{0, 1\}^t$ and $X_2 \in \{0, 1\}^{n - t}$.

Lemma A.4 ([NZ96]). Let $E_1 : \{0, 1\}^{n_1} \times \{0, 1\}^d \rightarrow \{0, 1\}^{d_1}$ be a $(k_1, \varepsilon_1)$ extractor and $E_2 : \{0, 1\}^{n_2} \times \{0, 1\}^{d_2} \rightarrow \{0, 1\}^{m}$ be a $(k_2, \varepsilon_2)$ extractor. Define $E((x_1, x_2), s) = E_1(x_2, E_2(x_1, s))$. Then for every $(k_1, k_2)$- block source $(X_1, X_2) \in \{0, 1\}^{n_1} \times \{0, 1\}^{n_2}$, $E((X_1, X_2), U_d)$ is $(\varepsilon_1 + \varepsilon_2)$- close to uniform.

Lemma A.5 ([GW97]). For every $\varepsilon, \Delta > 0$ and integer $n$ there exists a $(n - \Delta, \varepsilon)$ extractor $E : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^n$ with $d = O(\Delta + \log (1/\varepsilon))$, and for every $x, y$, $E(x, y)$ can be computed in space $O(n + \log (1/\varepsilon))$.
Lemma A.6 ([GUV09, KNW08]). For every $\varepsilon > 0$, integer $m > 0$ and $n \geq 2m$, there exists a $(2m, \varepsilon)$ extractor $E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with $d = O(\log m + \log(1/\varepsilon))$, and for every $x,y$, $E(x,y)$ can be computed in space $O(m + \log(1/\varepsilon))$.

Lemma A.7 ([Zuc97]). Every $(n - \log(1/\delta) - 1, \varepsilon)$-extractor is a $(\varepsilon, \delta)$-sampler.

Now we show how to construct the sampler we need, and that it is indeed space efficient.

Proof. Let $\Delta = \log(1/\delta) + 1$. Let $E_1 : \{0,1\}^m \times \{0,1\}^{d_1} \to \{0,1\}^m$ be an $(m - \Delta, \varepsilon/3)$-extractor from Lemma A.5, w.l.o.g. assume that $d_1 \geq \Delta + \log(3/\varepsilon)$. Then let $E_2 : \{0,1\}^{3d_1} \times \{0,1\}^d \to \{0,1\}^{d_1}$ be an $(2d_1, \varepsilon/3)$-extractor from Lemma A.6. Then we claim that $E : \{0,1\}^{m+3d_1} \times \{0,1\}^d \to \{0,1\}^m$, defined as $E((x_1, x_2), s) = E_1(x_1, E_2(x_2, s))$, is a $(m + 3d_1 - \Delta, \varepsilon)$ extractor, and hence a $(\varepsilon, \delta)$ sampler by Lemma A.7.

To prove the claim, consider any $(m + 3d_1 - \Delta)$-source $X$. By Lemma A.3, $X$ is $(\varepsilon/3)$-close to a $(m - \Delta, 3d_1 - \Delta - \log(3/\varepsilon))$-block source $(X_1, X_2) \in \{0,1\}^{3d_1} \times \{0,1\}^m$. By Lemma A.4, $E_1(X_1, E_2(X_2, U_d))$ is $2\varepsilon/3$-close to uniform. Since $E(X, U_d)$ is $\varepsilon/3$-close to $E_1(X_1, E_2(X_2, U_d))$, by triangle inequality it is $\varepsilon$-close to uniform. Moreover, $d = O(\log(d_1/\varepsilon)) = O(\log \log(1/\delta) + \log(1/\varepsilon))$, $n = m + 3d_1 = m + O(\log(1/\delta) + \log(1/\varepsilon))$, and the required space to compute $E$ is $O(m + d + \log(1/\varepsilon)) = O(m + \log(1/\varepsilon) + \log(1/\delta))$. $\square$