# Moments of Random Quantum Circuits and Applications in Random Circuit Sampling

by

Yinchen Liu

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization (Quantum Information)

Waterloo, Ontario, Canada, 2021

## Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

## Statement of Contributions

- Chapter 2 contains my own exposition of previous results with the exception of the proof of Theorem 2.13, which is my own work.
- Chapter 3 contains my own exposition of previous results with the exception of Theorem 3.5, which is my own work.
- Chapter 4 contains my own research work in collaboration with David Gosset.

## Abstract

Random quantum circuits and random circuit sampling (RCS) have recently garnered tremendous attention from all sub-fields of the quantum information community, especially after Google's quantum supremacy announcement in 2019. While the science of RCS draws ideas from diverse disciplines ranging from pure mathematics to electrical engineering, this thesis explores the subject from a theoretical computer science perspective.

We begin by offering a rigorous treatment of the $t$-design and the anti-concentration properties of random quantum circuits in a way that various intermediate lemmas will find further applications in subsequent discussions. In particular, we prove a new upper bound for expressions of the form $\mathbb{E}_V \left[\langle 0^n|V\sigma_p V^\dagger|0^n\rangle^2\right]$ for 1D random quantum circuits $V$ and $n$-qubit Pauli operators $\sigma_p$. Next, we discuss at a high level the RCS supremacy conjecture, which forms the main complexity-theoretic basis supporting the belief that deep random quantum circuits may be just as hard to classically simulate as arbitrary quantum circuits. Finally, we study the performance of quantum and classical spoofing algorithms on the linear cross-entropy benchmark (XEB), a statistical test proposed by Google for the purpose of verifying RCS experiments. We consider an extension of a classical algorithm recently proposed by Barak, Chou, and Gao and try to show that the extended algorithm can achieve higher XEB scores [BCG20]. While we are unable to prove a key conjecture for random quantum circuits with Haar random 2-qubit gates, we do establish the result in other related settings including for Haar random unitaries, random Clifford circuits, and random fermionic Gaussian unitaries.

**Acknowledgements**

I would like to thank

- my supervisor Prof. David Gosset for the quality, frequency, and variety of guidance offered throughout my Master's career;
- Prof. Ashwin Nayak and Prof. Jon Yard for reading this thesis and for the comments and feedback provided;
- our cat Dami for surviving feline infectious peritonitis with severe pleural effusion that a veterinarian deemed unsavable;
- my parents and Cindy for their unconditional love and support.

Figure 1: Portrait of Dami.

# Table of Contents

# List of Figures

# Introduction

Randomness is inherent in quantum computation. Still, randomization in a classical sense, different from randomness induced by measurements, has also been proven a useful tool in quantum information. Over the years, the idea of applying uniformly random unitary transformations, also called Haar random unitaries, has permeated diverse subfields of the quantum information sciences including quantum communication [HLSW04, ADHW09], quantum algorithm [Sen06], quantum hardware benchmarking [EAŻ05], black hole physics [HP07, RY17], quantum tomography [HKP20, HCY21], and one of the topics of this work, quantum supremacy [BIS$^+$18, BFNV18]. A major algorithmic downside of Haar random unitaries is that they cannot be sampled efficiently. In the circuit model of quantum computing, a quantum processor cannot apply in one step a global unitary acting simultaneously on a large number of qubits, and it is known that the number of 2-qubit gates needed to implement an $n$-qubit Haar random unitary grows exponentially in $n$ [Kni95]. Therefore, drawing large unitaries from the Haar distribution is unsuitable for applications where the random unitary needs to be efficiently constructible [DCEL09]. To this end, (Haar) random quantum circuits stand out as natural alternatives to global Haar random unitaries. A (Haar) random quantum circuit is a quantum circuit whose qubit and gate layouts are specified by an underlying circuit architecture, and the unitary transformation applied by each 2-qubit gate is drawn independently and identically according to the Haar distribution over the group of $4 \times 4$ unitary matrices. Since sampling every random 2-qubit gate consumes a constant amount of resources (e.g. time and random bits), an $n$-qubit random quantum circuit with poly($n$) many 2-qubit gates can be sampled efficiently and can be executed on a quantum computer efficiently just like every other polynomial-size quantum circuit. In addition, to better model the qubit layout of real-world quantum computers, one considers geometrically local circuit architectures. For example, in the 1D architecture, qubits are linked in a 1D chain where 2-qubit interactions can only occur between spatially neighbouring qubits (e.g. see Figure 2).

Since a random quantum circuit is composed of a sequence of Haar random 2-qubit gates, many properties of random quantum circuits ultimately reduce to properties of $4 \times 4$ Haar random unitaries. In Chapter 2, building upon a classic result in representation theory known as Schur-Weyl duality, we first give an axiomatic treatment of a few fundamental results involving the moments of Haar random unitaries. We then formalize, in the $t$-design property section, in what sense can random quantum circuits substitute global Haar random unitaries in applications where some properties of the latter are desired. We will show that for every $t \geq 1$, certain $t$-th order moments of 1D random quantum circuits converge to that of Haar random unitaries as the number of gates, or equivalently the circuit depth, goes to

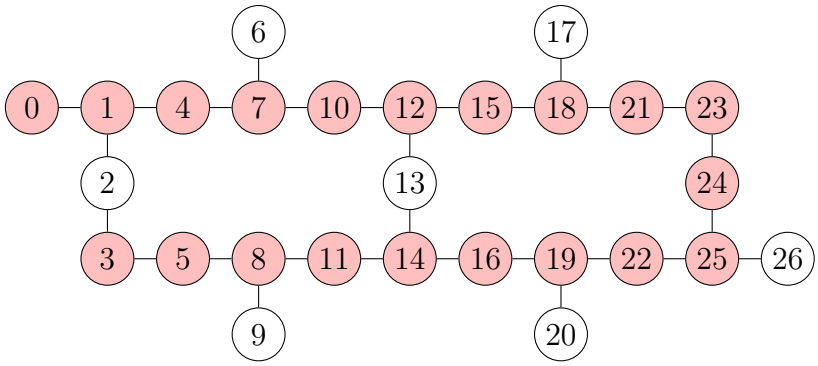


Figure 2: Qubit layout and connectivity of the 27-qubit ibmq_montreal quantum processor; the chain of pink qubits forms a 20-qubit 1D subsystem; image retrieved from `https://quantum-computing.ibm.com/services?services=systems&system=ibmq_montreal`.

infinity, and we also quantify the speed of convergence. In the collision probability and anti-concentration section, we dive deeper into understanding a few second-moment properties of random quantum circuits motivated by their relevance to quantum supremacy.

In 2019, Google claimed the achievement of quantum supremacy with a 53-qubit quantum computer performing a calculation termed random circuit sampling [AAB$^+$19]. Simply put, quantum supremacy seeks to perform on a real-world quantum computer a well-defined computational task impossible to replicate using even the most powerful supercomputer [Pre11, AC16]. Since the problem being solved need not possess any practical value, researchers have identified random circuit sampling (RCS) as a suitable candidate for demonstrating quantum supremacy. RCS consists of simply executing a random quantum circuit on a quantum computer and measuring all the qubits in the computational basis. RCS is suitable for quantum supremacy demonstrations because it is straightforward to execute on noisy experimental quantum computers while at the same time, complexity-theoretic evidence can be found to support its classical computational hardness [BJS11, BMS16, BFNV18]. In Chapter 3, we first give a high-level overview of the yet to be proven RCS supremacy conjecture which forms the main theoretical underpinning of RCS-based quantum supremacy proposals [BFNV18, Mov18]. We then discuss the verification problem of RCS experiments which persists even after the RCS supremacy conjecture is ultimately proven. We will show that for typical $n$-qubit random quantum circuits, the probability of measuring each bit string $z \in \{0,1\}^n$ as the output is roughly $\frac{1}{2^n}$. If a circuit is only executed poly$(n)$ times to collect poly$(n)$ samples, the same bit string will never be observed twice in practice. Thus, how can one distinguish between the outputs gathered from an RCS experiment and a set of uniformly random $n$-bit strings? The output distribution of a typical random quantum circuit will be close to but distinct from the uniform distribution over $\{0,1\}^n$, and in some sense, this slight deviation from uniformity is where all the signal lies. To address this problem, the Google team proposed and adopted a statistical test called the linear cross-entropy benchmark (XEB) for their quantum supremacy experiment [BIS$^+$18, AAB$^+$19]. Once we delegate the verification problem to such a benchmark, to certify the quantumness of a purported quantum computer, it becomes necessary to rule out the possibility of efficient classical algorithms attempting to match the quantum computer's score on the benchmark

without faithfully performing random circuit sampling. In a recent paper, Barak, Chou, and Gao proposed and analyzed the performance of such a classical spoofing algorithm on the linear cross-entropy benchmark [BCG20]. The BCG algorithm works by computing and sampling from the marginal output distributions of a set of qubits with disjoint backward lightcones, and it is efficient and can achieve non-trivial XEB scores for low-depth random quantum circuits [BCG20]. Hence, the existence of the BCG algorithm elucidates the importance of conducting RCS experiments with sufficiently deep random quantum circuits. In Chapter 3, we provide a simpler rendition of the main result of the BCG paper by reusing some of the tools and techniques developed in Chapter 2.

In Chapter 4, we consider an extension of the Barak, Chou, and Gao algorithm which computes and samples every qubit according to its marginal output distribution. The extended BCG algorithm has the same asymptotic time complexity as the BCG algorithm, and we try to show that the extended algorithm attains better XEB scores. While we do not succeed in proving a key conjecture for the general case of (Haar) random quantum circuits, we do establish the result in several other settings including global Haar random unitaries, random Clifford circuits, and random fermionic Gaussian unitaries.

# Chapter 1

# Preliminaries

This work assumes the reader is familiar with basic concepts in quantum computing, and the purpose of this chapter is to establish some definitions and notations that will be used throughout this work.

## 1.1 Notations

Let $n \geq 1$ be an integer and define $[n] = \{1, 2, \ldots, n\}$. For every $w \in \{0,1\}^n$, let $|w| = |\{i \in [n] : w_i = 1\}|$ denote the Hamming weight of $w$. For every finite set $S$, let $\mathcal{U}(S)$ denote the discrete uniform distribution over the sample space $S$. For example, $z \sim \mathcal{U}(\{0,1\}^n)$ is a uniformly random $n$-bit string. Let $N = 2^n$ and let $\mathbb{U}(N)$ denote the group of all $N \times N$ unitary matrices. For examples, $\mathbb{U}(1)$ is the set of all complex numbers with modulus 1, and $\mathbb{U}(4)$ is the set of all 2-qubit quantum gates. Let $j \in [n]$ and $b \in \{0,1\}$. Define $(|b\rangle\langle b|)_j = I^{\otimes(j-1)} \otimes |b\rangle\langle b| \otimes I^{\otimes(n-j)}$. Let $U$ be a 1-qubit gate. Define $U_j = I^{\otimes(j-1)} \otimes U \otimes I^{\otimes(n-j)}$, the $n$-qubit unitary which applies a $U$ gate to the $j$-th qubit and identity to every other qubit. For every $w \in \{0,1\}^n$, define $U(w) = \bigotimes_{j=1}^{n} U^{w_j}$, the $n$-qubit unitary which applies a $U$ gate to every qubit $j$ such that $w_j = 1$ and identity to every other qubit where $w_j = 0$. For every 2-qubit gate $U$ and $j \in [n-1]$, let $U_j = I^{\otimes(j-1)} \otimes U \otimes I^{\otimes(n-j-1)}$ denote the $n$-qubit unitary which applies $U$ to qubits $j$ and $j+1$ and identity to all other qubits.

## 1.2 The Pauli Group and the Clifford Group

Let $I$, $X$, $Y$, and $Z$ denote the 1-qubit Pauli matrices where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \text{ and } \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

**Definition 1.1** ($n$-qubit Pauli Group)**.** The $n$-qubit Pauli group $\mathbf{P}_n$ is the group generated by $X_1, \ldots, X_n$, $Y_1, \ldots, Y_n$, and $Z_1, \ldots, Z_n$.

Elements in $\mathbf{P}_n$ are $n$-fold tensor products of the four 1-qubit Pauli matrices with a global $\pm 1$ or $\pm i$ phase factor. Let $P = e^{i\theta} \bigotimes_{j=1}^{n} P^{(j)} \in \mathbf{P}_n$ where for every $j \in [n]$, $P^{(j)} \in \{I, X, Y, Z\}$. The weight of $P$ is defined as $|\{j \in [n] : P^{(j)} \neq I\}|$, the number of non-identity tensor

factors in $P$, and we call $P$ an $X$, $Y$, or $Z$-type Pauli if for every $j \in [n]$, $P^{(j)} \in \{X, I\}$, $P^{(j)} \in \{Y, I\}$, or $P^{(j)} \in \{Z, I\}$ respectively. Note that $P$ is a $Z$-type Pauli if and only if $P$ is diagonal.

**Definition 1.2** ($n$-qubit Clifford Group)**.** The $n$-qubit Clifford group $\mathbf{C}_n$ is defined by $\mathbf{C}_n = \{C \in \mathbb{U}(N) : C\mathbf{P}_n C^\dagger = \mathbf{P}_n\}/\mathbb{U}(1)$.

Alternatively, $\mathbf{C}_n$ can be characterized as the set of all $n$-qubit quantum circuits that can be constructed using the gate set

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \text{ and } \quad CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

A unitary $U \in \mathbb{U}(N)$ is call a Clifford unitary if $U \in \mathbf{C}_n$.

## 1.3 Superoperators and the Vectorization Isomorphism

Let us consider the Hilbert space $\mathbb{C}^N$ with the computational basis $\{|j\rangle : j \in \{0, 1, \ldots, N-1\}\}$. In quantum information, we often encounter superoperators $\Phi : \mathbb{C}^{N\times N} \to \mathbb{C}^{N\times N}$ acting on linear operator $A : \mathbb{C}^N \to \mathbb{C}^N$ by conjugation such that $\Phi(A) = VAV^\dagger$ for some $V : \mathbb{C}^N \to \mathbb{C}^N$. Since $\Phi$ is a linear transformation, it has a matrix representation such that the action of $\Phi$ on $A$ is represented by matrix-vector multiplication. We can obtain the matrix representation of $\Phi$ in the computational basis via the vectorization isomorphism. The vectorization isomorphism between $\mathbb{C}^{N\times N}$ and $\mathbb{C}^{N^2}$ is defined by its action on the basis elements as $\text{vec}(|i\rangle\langle j|) = |i\rangle \otimes |j\rangle$ for every $i, j \in \{0, 1, \ldots, N-1\}$. For $A = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} a_{ij}|i\rangle\langle j|$, we define the notation

$$|A\rangle = \text{vec}(A) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} a_{ij}\text{vec}(|i\rangle\langle j|) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} a_{ij}|i\rangle \otimes |j\rangle.$$

The definition of $|A\rangle$ implies that

$$\langle A| = (|A\rangle)^\dagger = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} \overline{a_{ij}}\langle i| \otimes \langle j|,$$

so

$$\langle A|A\rangle = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} |a_{ij}|^2 = \text{Tr}\left(A^\dagger A\right).$$

By linearity,

$$|\Phi(A)\rangle = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} a_{ij}V|i\rangle \otimes \overline{V}|j\rangle = (V \otimes \overline{V})|A\rangle.$$

This shows that the matrix representation of $\Phi$ is $V \otimes \overline{V}$.

## 1.4 Permutation Operators

Let $t \geq 1$ be an integer. The symmetric group of order $t$, denoted by $S_t$, is the group of all permutations of $t$ elements. Let $\pi \in S_t$. While $\pi$ can be defined as a bijection between $\{0, 1, \ldots, t-1\}$ and itself, it is common to represent $\pi$ by a $t \times t$ permutation matrix $P_\pi$ which permutes the standard basis vectors, i.e. for every $j \in \{0, 1, \ldots, t-1\}$, $P_\pi|j\rangle = |\pi(j)\rangle$. However, for our purposes, since we will use $\pi$ to permute the $t$ tensor factors of $(\mathbb{C}^N)^{\otimes t}$, we consider another permutation matrix representation of $\pi$ in $\mathbb{U}(N)^{\otimes t}$ as

$$W_\pi^{(N)} = \sum_{i_1,\ldots,i_t \in \{0,1,\ldots,N-1\}} |i_{\pi^{-1}(1)}, \ldots, i_{\pi^{-1}(t)}\rangle\langle i_1, \ldots, i_t|.$$

We observe that

$$|W_\pi^{(N)}\rangle = (W_\pi^{(N)} \otimes \mathbb{1})|\Omega\rangle$$

where

$$|\Omega\rangle = \sum_{i_1,\ldots,i_t \in \{0,1,\ldots,N-1\}} |i_1, \ldots, i_t\rangle \otimes |i_1, \ldots, i_t\rangle.$$

For every $\pi \in S_t$, let $c(\pi)$ denote the number of cycles in $\pi$. We can easily verify the following properties of permutation operators:

**Lemma 1.1.** *For every $\pi, \sigma \in S_t$,*

*(a)* $W_\pi^{(N)} W_\sigma^{(N)} = W_{\pi\sigma}^{(N)}$;

*(b)* $\left(W_\pi^{(N)}\right)^\dagger = W_{\pi^{-1}}^{(N)}$;

*(c)* $\mathrm{Tr}(W_\pi^{(N)}) = N^{c(\pi)}$.

## 1.5 Local Hamiltonians

An $n$-qubit-$k$-local Hamiltonian with $m$ local terms is a hermitian operator of the form $H = \sum_{i=1}^m h_i$ where each local term $h_i \in \mathbb{C}^{2^n \times 2^n}$ only acts non-trivially on at most $k$ qubits. The set of eigenvalues of $H$ is referred to as the energy levels, and a ground state of $H$ is an eigenvector of $H$ corresponding to its minimum eigenvalue. We say $H$ is frustration-free if for every $n$-qubit state $|\psi\rangle$, $|\psi\rangle$ is a ground state of $H$ if and only if $|\psi\rangle$ is the ground state of $h_i$ for every $i \in [m]$. A notable special case (in fact WLOG from a physical perspective) is when $h_i$ is positive semi-definite and not positive definite for every $i \in [m]$, then $H$ is frustration-free if and only if every zero-energy ground state of $H$ is a simultaneous zero-energy ground state of $h_i$ for every $i \in [m]$. We use $\Delta(H)$ to denote the spectral gap of $H$, which is the positive difference between its second smallest and smallest eigenvalues, and when $H$ is positive semi-definite and not positive definite, $\Delta(H)$ simply becomes its second smallest eigenvalue. We say $H$ is translation-invariant if the non-trivial $k$-qubit operator applied by $h_i$ is the same for every $i \in [m]$.

## 1.6 Random Quantum Circuits

We call a probability distribution $\mathcal{D}$ an $n$-qubit random unitary distribution if the sample space of $\mathcal{D}$ is a subset of $\mathbb{U}(N)$. The most natural and fundamental random unitary distribution ought to be the continuous uniform distribution over $\mathbb{U}(N)$, which we denote by $\mu^N_{\text{Haar}}$ as it is also called the Haar measure over $\mathbb{U}(N)$. A unitary drawn from $\mu^N_{\text{Haar}}$ is called a Haar random unitary, and it is equally likely to be any element in $\mathbb{U}(N)$. For a rigorous treatment of the Haar measure, see section 7.2 of [Wat18]. The Haar distribution is the unique probability distribution over $\mathbb{U}(N)$ that is both left and right unitarily invariant. Namely, if $U$ is drawn from $\mu^N_{\text{Haar}}$, then for every $V \in \mathbb{U}(N)$, both $VU$ and $UV$ are distributed according to $\mu^N_{\text{Haar}}$. Other notable random unitary distributions include the discrete uniform distribution over the Clifford group or over some finite universal gate set and distributions that produce quantum circuits.

A random quantum circuit distribution is usually specified by a circuit architecture and a random unitary distribution over $\mathbb{U}(4)$. The architecture dictates the placement of the gates and the topological structure of the circuit but not the actual unitaries being applied. Then, a random quantum circuit is constructed by drawing all the 2-qubit gates independently from the $\mathbb{U}(4)$ random unitary distribution. We first define two families of random quantum circuits that will feature prominently in later chapters.

**Definition 1.3** (Local Random Quantum Circuits)**.** For some random unitary distribution $\mathcal{D}$ over $\mathbb{U}(4)$ and for every $n, s \geq 1$, an $n$-qubit-$s$-gate local random quantum circuit is a quantum circuit constructed using the following procedure. For every $i \in [s]$,

1. sample independently an index $i \sim \mathcal{U}([n-1])$;
2. sample independently a 2-qubit gate $U \sim \mathcal{D}$ and apply $U$ to qubits $i$ and $i+1$.

**Definition 1.4** (1D Random Quantum Circuits)**.** For some random unitary distribution $\mathcal{D}$ over $\mathbb{U}(4)$, for every $n \geq 2$ even and $d \geq 1$, an $n$-qubit-depth-$d$ 1D random quantum circuit is define by the following procedure. For every layer $i \in [d]$, if $i$ is odd, then apply $U^{(i,1)} \otimes U^{(i,3)} \otimes \cdots \otimes U^{(i,n-1)}$, and if $i$ is even, then apply $U^{(i,2)} \otimes U^{(i,4)} \otimes \cdots \otimes U^{(i,n-2)}$ where for every $j$, $U^{(i,j)}$ is drawn independently from $\mathcal{D}$. We use $\mathcal{H}^{\text{path}}_{n,d}$ to denote the distribution of $n$-qubit-depth-$d$ 1D Haar random quantum circuits where $\mathcal{D} = \mu^4_{\text{Haar}}$.

Both local and 1D random quantum circuits belong to a broader family of geometrically local quantum circuits since for both, we can imagine placing the $n$-qubit on a 1D line, and 2-qubit gates can only couple spatially neighbouring qubits. From now on, when we refer to local or 1D random quantum circuits without specifying the unitary distribution $\mathcal{D}$ over $\mathbb{U}(4)$, it is assumed that $\mathcal{D} = \mu^4_{\text{Haar}}$.

A general deterministic circuit architecture can be formally defined in the following way.

**Definition 1.5** (Circuit Architecture)**.** An $n$-qubit-$s$-gate-depth-$d$ circuit architecture $\mathcal{A}$ can be specified by a graph $G = (V, E)$ and a sequence of matchings $M_1, \ldots, M_d$ satisfying the following properties:

(a) $V = [n]$;

(b) an edge $ij \in E$ if and only if a 2-qubit gate can be applied to qubits $i$ and $j$;

(c) $\sum_{i=1}^{d} |M_i| = s$.

In this definition, every vertex in $V$ corresponds to a qubit, and the edge set $E$ specifies the connectivity of the architecture. For every $i \in [d]$, $M_i$ specifies the placement of a layer of gates where an edge $jk \in M_i$ corresponds to applying a 2-qubit gate between qubits $j$ and $k$ in layer $i$. The matching condition ensures that every qubit is affected by at most one gate per layer. For example, under this formalism, the $n$-qubit-depth-$d$ 1D architecture, which we denote by $\mathcal{A}^{\text{path}}_{n,d}$, can be specified by the path graph $P_n = ([n], E)$ and layers $M_1, \ldots, M_d$ where $E = \{e_i = \{i, i+1\} : i \in [n-1]\}$, and for every $i \in [d]$, if $i$ is odd, then $M_i = \{e_j \in E : j \text{ is odd}\}$, and if $i$ is even, then $M_i = \{e_j \in E : j \text{ is even}\}$. Besides the 1D architecture, 2D random quantum circuits constitute another extensively studied [BIS+18, BFNV18, HM18, NLPD+19, BCG20] and experimentally relevant [BIS+18, AAB+19] random quantum circuit family where the $n$ qubits are laid on a $\sqrt{n} \times \sqrt{n}$ grid and gates are restricted to connecting a qubit with its up to four neighbours. While numerous results have been rigorously established for 2D random quantum circuits [HM18, BFNV18, Mov18, NLPD+19, BCG20], some of them are shown for general circuit architectures as the proofs do not assume any spatial regularities from the circuit architecture. Other results that do target the 2D geometry directly sometimes work with customized, nonstandard gate layouts [HM18, NLPD+19]. Within this work, every result applying to 2D random quantum circuits will be proven for general architectures. Next, we discuss some properties of general circuit architectures.

**Definition 1.6** (Backward Lightcone)**.** Let $\mathcal{A}$ be a circuit architecture with graph $G = (V, E)$ and sequence of matchings $M_1, \ldots, M_d$. For every qubit $i \in [n]$, define $L_{d+1}(i) = \{i\}$, and for every $j \in [d]$, define $L_j(i)$ recursively as

$$L_j(i) = L_{j+1}(i) \cup \{k \in [n] : \exists uk \in M_j \text{ s.t. } u \in L_{j+1}(i)\},$$

and we call $L(i) = L_1(i)$ the backward lightcone of qubit $i$. We call $L(\mathcal{A}) = \max_{i \in [n]} |L(i)|$ the lightcone size of the architecture $\mathcal{A}$.

**Lemma 1.2** (Properties of Lightcones)**.** *For every $n$-qubit-depth-$d$ circuit architecture $\mathcal{A}$,*

*(a) for every $i \in [n]$, the marginal output probabilities of qubit $i$ can be computed classically in poly$(2^{|L(i)|})$ time;*

*(b) for every $i, j \in [n]$, if $L(i) \cap L(j) = \emptyset$, then the marginal output distributions of qubits $i$ and $j$ are independent;*

*(c) $L(\mathcal{A}) \leq 2^d$, and in particular, $L(\mathcal{A}^{path}_{n,d}) \leq 2d$.*

For every $i \in [n]$, to compute the marginal output probabilities of qubit $i$ in poly$(2^{|L(i)|})$ time, it suffices to initialize just the qubits in $L(i)$ and simulate only the gates acting on qubits in $L_j(i)$ for every $j \in [d]$ using an explicit matrix and state vector representation.

Lastly, we define some notations and terminologies. A 2-qubit gate $U \sim \mu^4_{\text{Haar}}$ is called a Haar random gate, and a 2-qubit gate $U \sim \mathcal{U}(\mathbf{C}_2)$ is called a random Clifford gate. For every circuit architecture $\mathcal{A}$, we use $\mathcal{H}_{\mathcal{A}}$ and $\mathcal{C}_{\mathcal{A}}$ to denote the random quantum circuit distributions induced by drawing the gates in $\mathcal{A}$ independently and identically according to $\mu^4_{\text{Haar}}$ and $\mathcal{U}(\mathbf{C}_2)$ respectively. A sample $V \sim \mathcal{H}_{\mathcal{A}}$ is called a Haar random quantum circuit, and a sample $C \sim \mathcal{C}_{\mathcal{A}}$ is called a random Clifford circuit.

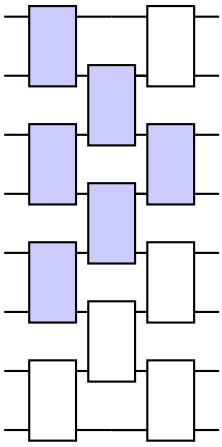

Figure 1.1: An 8-qubit-depth-3 1D circuit diagram; the top six qubits are in the backward lightcone of the third (and fourth) qubit; only gates coloured in purple need to be carried out to compute the marginal output probabilities of the third (or fourth) qubit.

## 1.7 Output Distributions and the Hiding Property

Let $U \in \mathbb{U}(N)$ be an $n$-qubit unitary. Measuring the state $U|0^n\rangle$ in the computational basis induces a probability distribution over the sample space $\{0,1\}^n$ where for every $z \in \{0,1\}^n$, the probability of observing $z$ is given by $q_U(z) = |\langle z|U|0^n\rangle|^2$, and we call $q_U$ the output distribution of $U$. For every $x \in \{0,1\}^n$, define $U_x = X(x)U$ and notice that $\langle x|U|0^n\rangle = \langle 0^n|U_x|0^n\rangle$.

An $n$-qubit random unitary distribution $\mathcal{D}$ is said to have the hiding property if for every $x \in \{0,1\}^n$, if $U$ is drawn from $\mathcal{D}$, then $U_x = X(x)U$ is also distributed according to $\mathcal{D}$. It is the unitary invariance property restricted to $X$-type Pauli operators. The hiding property is very general and holds for a vast range of random unitary distributions including random circuit distributions that apply at least one Haar random or random Clifford gate to every qubit. As a non-example, it is easy to see that local random quantum circuits (recall Definition 1.3) with a large number of qubits and few gates do not enjoy the hiding property. Right away, some basic properties of random quantum circuits can be derived from the hiding property.

**Lemma 1.3.** *Let $\mathcal{D}$ be an $n$-qubit random unitary distribution with the hiding property. Then for every $x \in \{0,1\}^n$, $\mathbb{E}_{U\sim\mathcal{D}}\left[|\langle x|U|0^n\rangle|^2\right] = \frac{1}{2^n}$.*

*Proof.* Let $x \in \{0,1\}^n$. Using the hiding property, we see that

$$\mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[|\langle x|U|0^n\rangle|^2\right] = \mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[|\langle 0^n|U_x|0^n\rangle|^2\right] = \mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[|\langle 0^n|U|0^n\rangle|^2\right].$$

Thus,

$$1 = \mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[\sum_{x\in\{0,1\}^n}|\langle x|U|0^n\rangle|^2\right] = 2^n \mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[|\langle 0^n|U|0^n\rangle|^2\right],$$

so

$$\mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[|\langle x|U|0^n\rangle|^2\right] = \mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[|\langle 0^n|U|0^n\rangle|^2\right] = \frac{1}{2^n}.$$

□

Generally, the output distribution of a random quantum circuit chains two sources of randomness, one from the random unitary distribution $\mathcal{D}$ and the other induced by computational basis measurements. As demonstrated in the proof of Lemma 1.3, the hiding property allows one to examine WLOG just the $0^n$ outcome, thereby removing the need to analyze the randomness originating from measurements in many cases. In other words, we can focus our efforts on understanding the randomness over $\mathcal{D}$.

# Chapter 2

# Properties of Random Quantum Circuits

This chapter aims to build an understanding of random quantum circuits and explore the techniques that have been developed for analyzing them. We have already seen that every $n$-qubit random unitary distribution $\mathcal{D}$ enjoying the hiding property satisfies

$$\mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[|\langle x|U|0^n\rangle|^2\right] = \frac{1}{2^n}$$

for every $x \in \{0,1\}^n$. In other words, we have shown that $\mathbb{E}[X] = \frac{1}{2^n}$ for the random variable $X = |\langle x|U|0^n\rangle|^2$ where the randomness is over $U \sim \mathcal{D}$. As a next step, one may wonder, what about $\mathrm{Var}(X)$? We all know that computing $\mathrm{Var}(X)$ reduces to figuring out $\mathbb{E}[X^2]$ given our knowledge about $\mathbb{E}[X]$. Then, for example, information about $\mathrm{Var}(X)$ enables us to upper bound the probability that $X$ deviates from $\mathbb{E}[X]$ via the Chebyshev inequality. It turns out that in ways analogous to this simple example, the analyses of many interesting properties related to random quantum circuits reduce to analyzing moments of the form

$$\mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right]$$

for some $t \geq 1$ and $A \in (\mathbb{C}^{N\times N})^{\otimes t}$ [BHH16, BGM19, BCG20, DHJB20, LOB+21]. For our example, we see that $\mathbb{E}[X^2]$ can be related to an expression of this form by choosing $t = 2$ and $A = |0^{2n}\rangle\langle 0^{2n}|$.

Since random quantum circuits are composed of layers of random 2-qubit gates, every global property of the circuits is ultimately determined by the properties of the individual gates. Hence, it is instructive to begin by studying the moment operators of the Haar distribution.

## 2.1 The Haar Moment Operator

Let $n \geq 1$ and $t \geq 1$ be integers, and let $N = 2^n$. The $t$-th moment superoperator of an $n$-qubit random unitary distribution $\mathcal{D}$ is defined by

$$\Phi_{\mathcal{D}}^{(t)} : (\mathbb{C}^{N\times N})^{\otimes t} \to (\mathbb{C}^{N\times N})^{\otimes t}$$

$$A \mapsto \mathop{\mathbb{E}}_{U\sim\mathcal{D}} \left[U^{\otimes t} A (U^\dagger)^{\otimes t}\right],$$

and the matrix representation of $\Phi_{\mathcal{D}}^{(t)}$ under the vectorization isomorphism $\mathbb{E}_{U\sim\mathcal{D}} \left[U^{\otimes t} \otimes (\overline{U})^{\otimes t}\right]$ is called the $t$-th moment operator of $\mathcal{D}$. Specializing to the Haar distribution, we get the Haar $t$-th moment superoperator $\Phi_{\mu_{\text{Haar}}^N}^{(t)}$ and its matrix representation

$$P_N^{(t)} = \mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N} \left[U^{\otimes t} \otimes (\overline{U})^{\otimes t}\right].$$

Throughout this work, we will go back and forth between the equivalent operator and superoperator views frequently. We start by stating a version of a classic result in representation theory known as Schur-Weyl duality and effectively accepting it as an "axiom". The theorem statement is borrowed from [RY17]. For a proof, see section 7.1 of [Wat18].

**Theorem 2.1** (Schur-Weyl Duality)**.** *For every linear operator $A \in (\mathbb{C}^{N\times N})^{\otimes t}$, $AV^{\otimes t} = V^{\otimes t}A$ for every $V \in \mathbb{U}(N)$ if and only if $A$ is a linear combination of the permutation operators $W_\pi^{(N)}$, $\pi \in S_t$.*

For the ( $\Longleftarrow$ ) direction, it is easy to verify that for every permutation operator $W_\pi^{(N)}$, $\pi \in S_t$,

$$W_\pi^{(N)} V^{\otimes t} \left(W_\pi^{(N)}\right)^\dagger = V^{\otimes t}$$

for every $V \in \mathbb{U}(N)$, so the result follows. Let $W$ be the $N^{2t}$-by-$t!$ matrix with columns $|W_\pi^{(N)}\rangle$, $\pi \in S_t$. For the ( $\Longrightarrow$ ) direction, consider the system of linear equations

$$Wc = |A\rangle$$

with $c$ being the unknowns. Notice that for different choices of $N$ and $t$, it is possible for $N^{2t} < t!$ or $N^{2t} > t!$, resulting in the system being either underdetermined or overdetermined. The ( $\Longrightarrow$ ) direction of Schur-Weyl duality asserts that the system has solutions for all choices of $N$ and $t$ provided that $A$ commutes with $V^{\otimes t}$ for every $V \in \mathbb{U}(N)$.

The following basic properties of the Haar $t$-th moment operator can be easily derived from the unitary invariance property and Schur-Weyl duality. For a discussion of similar properties in the Pauli basis, see section 3 of [HL09].

**Lemma 2.1.** *The following properties hold for $P_N^{(t)}$:*

*(a) $P_N^{(t)}$ is real symmetric in the computational basis;*

*(b) $P_N^{(t)}$ is an orthogonal projector;*

*(c) the $+1$-eigenspace of $P_N^{(t)}$ equals* $\text{span}\{|W_\pi^{(N)}\rangle : \pi \in S_t\}$.

*Proof.*

(a) We have

$$\left(P_N^{(t)}\right)^\dagger = \mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[(U^\dagger)^{\otimes t}\otimes(U^T)^{\otimes t}\right] = \mathop{\mathbb{E}}_{V\sim\mu_{\text{Haar}}^N}\left[V^{\otimes t}\otimes(\overline{V})^{\otimes t}\right] = P_N^{(t)}$$

by renaming $U^\dagger$ with $V$. Similarly, $\left(P_N^{(t)}\right)^T = P_N^{(t)}$ and together with $\left(P_N^{(t)}\right)^\dagger = P_N^{(t)}$, they imply that $P_N^{(t)}$ is real symmetric.

(b) By the unitary invariance property, for every $A \in (\mathbb{C}^{N\times N})^{\otimes t}$,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{V\sim\mu_{\text{Haar}}^N}\left[V^{\otimes t}\mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right](V^\dagger)^{\otimes t}\right]\\
&= \mathop{\mathbb{E}}_{V\sim\mu_{\text{Haar}}^N}\left[\mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[(VU)^{\otimes t}A((VU)^\dagger)^{\otimes t}\right]\right]\\
&= \mathop{\mathbb{E}}_{V\sim\mu_{\text{Haar}}^N}\left[\mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right]\right]\\
&= \mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right],
\end{aligned}$$

which is equivalent to $P_N^{(t)}P_N^{(t)}|A\rangle = P_N^{(t)}|A\rangle$. Since this is true for every $A \in (\mathbb{C}^{N\times N})^{\otimes t}$, $P_N^{(t)}P_N^{(t)} = P_N^{(t)}$, so $P_N^{(t)}$ is a projector. Since $P_N^{(t)}$ is also hermitian, $P_N^{(t)}$ is an orthogonal projector.

(c) By the ( $\Longleftarrow$ ) direction of Schur-Weyl duality, for every $\pi \in S_t$,

$$\mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[U^{\otimes t}W_\pi^{(N)}(U^\dagger)^{\otimes t}\right] = \mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[W_\pi^{(N)}U^{\otimes t}(U^\dagger)^{\otimes t}\right] = W_\pi^{(N)},$$

so $|W_\pi^{(N)}\rangle$ is a $+1$-eigenvector of $P_N^{(t)}$. Let $A \in (\mathbb{C}^{N\times N})^{\otimes t}$ such that $P_N^{(t)}|A\rangle = |A\rangle$. For every $V \in \mathbb{U}(N)$, we have that

$$V^{\otimes t}A = V^{\otimes t}\Phi_{\mu_{\text{Haar}}^N}^{(t)}(A) = V^{\otimes t}\mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[(V^\dagger U)^{\otimes t}A((V^\dagger U)^\dagger)^{\otimes t}\right] = \Phi_{\mu_{\text{Haar}}^N}^{(t)}(A)V^{\otimes t} = AV^{\otimes t}.$$

Therefore, by Schur-Weyl duality, $A$ is a linear combination of permutation operators, which is equivalent to saying $|A\rangle \in \text{span}\{|W_\pi^{(N)}\rangle : \pi \in S_t\}$.

□

The set of vectors $\{|W_\pi^{(N)}\rangle : \pi \in S_t\}$ may not be linearly independent by a simple dimension argument. Since $|W_\pi^{(N)}\rangle$ is $N^{2t}$ dimensional and $|S_t| = t!$, for constant $N$ and large enough $t$, $t! > N^{2t}$, so in such cases $\{|W_\pi^{(N)}\rangle : \pi \in S_t\}$ cannot be linearly independent.

Lemma 2.1 (b) and (c) imply that for every $A \in (\mathbb{C}^{N\times N})^{\otimes t}$, there exist scalars $c_\pi \in \mathbb{C}, \pi \in S_t$ such that

$$\mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right] = \sum_{\pi\in S_t} c_\pi W_\pi^{(N)}.$$

Next, we work out a formula for the coefficients $c_\pi$ in terms of the Moore-Penrose inverse of a matrix. The form of the formula is borrowed from [RY17].

**Lemma 2.2.** *For every linear operator $A \in (\mathbb{C}^{N\times N})^{\otimes t}$,*

$$\mathop{\mathbb{E}}_{U\sim\mu_{Haar}^N}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right] = \sum_{\pi\in S_t}\left(\sum_{\sigma\in S_t}(Q^+)_{\pi,\sigma}\operatorname{Tr}\left(W_{\sigma^{-1}}^{(N)}A\right)\right)W_\pi^{(N)} \tag{2.1}$$

*where for every $\pi,\sigma\in S_t$, $Q_{\pi,\sigma}=\operatorname{Tr}(W_{\pi^{-1}}^{(N)}W_\sigma^{(N)})$, and $Q^+$ is the Moore-Penrose inverse of $Q$.*

*Proof.* Let $A\in(\mathbb{C}^{N\times N})^{\otimes t}$. Let $W$ be the $N^{2t}$-by-$t!$ matrix with columns $|W_\pi^{(N)}\rangle$, $\pi\in S_t$. We have shown that for $c\in\mathbb{C}^{t!}$, the system of linear equations

$$Wc = P_N^{(t)}|A\rangle$$

has solutions, so

$$c = W^+P_N^{(t)}|A\rangle = (W^\dagger W)^+W^\dagger P_N^{(t)}|A\rangle = (W^\dagger W)^+W^\dagger|A\rangle \tag{2.2}$$

is a solution. By defining $Q=W^\dagger W$, we see that (2.2) expands into the RHS of (2.1). □

The matrix $Q^+$ appearing in Lemma 2.2 has been called the (unitary) Weingarten matrix, and for detailed discussions about the Weingarten calculus, see [Gu13, CMN21]. For another proof of the following well-known lemma, see [Har13].

**Lemma 2.3** ($t$-th Moment of a Haar Random State)**.**

$$\mathop{\mathbb{E}}_{U\sim\mu_{Haar}^N}\left[\left(U|0^n\rangle\langle 0^n|U^\dagger\right)^{\otimes t}\right] = \frac{\sum_{\pi\in S_t}W_\pi^{(N)}}{t!\binom{t+N-1}{t}}$$

*Proof.* By substituting $A=(|0^n\rangle\langle 0^n|)^{\otimes t}$ into Lemma 2.2, we get that

$$\mathop{\mathbb{E}}_{U\sim\mu_{\mathrm{Haar}}^N}\left[\left(U|0^n\rangle\langle 0^n|U^\dagger\right)^{\otimes t}\right] = \sum_{\pi\in S_t}\left(\sum_{\sigma\in S_t}(Q^+)_{\pi,\sigma}\right)W_\pi^{(N)}.$$

Recall that $Q=W^\dagger W$ where $W$ is the $N^{2t}$-by-$t!$ matrix with columns $|W_\pi^{(N)}\rangle$, $\pi\in S_t$. Notice that for every $\pi\in S_t$,

$$\sum_{\sigma\in S_t}Q_{\pi,\sigma} = \sum_{\sigma\in S_t}\operatorname{Tr}\left(W_{\pi^{-1}\sigma}^{(N)}\right) = \sum_{\sigma\in S_t}N^{\text{number of cycles in }\pi^{-1}\sigma}.$$

By a well-known characterization of the Stirling numbers of the first kind,

$$\sum_{k=1}^N N^k\cdot(\text{number of permutations of } n \text{ elements with } k \text{ cycles}) = t!\binom{t+N-1}{t}.$$

Thus, the all-ones vector is an eigenvector of $Q$ with eigenvalue $t!\binom{t+N-1}{t}$. Since $Q$ is hermitian, the all-ones vector is also an eigenvector of $Q^+$ with eigenvalue $\frac{1}{t!\binom{t+N-1}{t}}$. □

## 2.2 The $t$-design property

We begin by defining the notion of an exact unitary $t$-design.

**Definition 2.1** (Exact unitary $t$-design)**.** An $n$-qubit random unitary distribution $\mathcal{D}$ is an exact unitary $t$-design if for every $A \in \left(\mathbb{C}^{N\times N}\right)^{\otimes t}$,

$$\Phi_{\mathcal{D}}^{(t)}(A) = \mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right] = \mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right] = \Phi_{\mu_{\text{Haar}}^N}^{(t)}(A),$$

or equivalently,

$$\mathop{\mathbb{E}}_{U\sim D}\left[U^{\otimes t}\otimes(\overline{U})^{\otimes t}\right] = \mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^N}\left[U^{\otimes t}\otimes(\overline{U})^{\otimes t}\right] = P_N^{(t)}.$$

We can make use of the exact unitary $t$-design condition in a few ways. In one scenario, one may wish to analyze $\mathbb{E}_{U\sim\mu_{\text{Haar}}^N}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right]$ for some $t$ and some special $A \in \left(\mathbb{C}^{N\times N}\right)^{\otimes t}$ for which there exists an exact unitary $t$-design $\mathcal{D}$ such that $\mathbb{E}_{U\sim\mathcal{D}}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right]$ possesses special structures. For example, it is known that the discrete uniform distribution over the Clifford group, $\mathcal{U}(\mathbf{C}_n)$, forms an exact unitary 2-design [DCEL09]. For Pauli operators $\sigma_p \in \{I, X, Y, Z\}^{\otimes n}$, the fact that Clifford operators conjugate Pauli operators to Pauli operators leads to rich exploitable combinatorial structures in the expression

$$\mathop{\mathbb{E}}_{C\sim\mathcal{U}(\mathbf{C}_n)}\left[(C\otimes C)(\sigma_p\otimes\sigma_p)(C^\dagger\otimes C^\dagger)\right].$$

We will explore implementations of this idea in the next section. In another scenario, one may be able to prove some results concerning $\mathbb{E}_{U\sim\mu_{\text{Haar}}^N}\left[U^{\otimes t}A(U^\dagger)^{\otimes t}\right]$ for some $t$ and $A \in \left(\mathbb{C}^{N\times N}\right)^{\otimes t}$, and then in a black-box fashion, the results automatically generalize to all random unitary distributions that form exact unitary $t$-designs. For example, when $A$ is not a Clifford operator, $\mathbb{E}_{C\sim\mathcal{U}(\mathbf{C}_n)}\left[C^{\otimes 2}A(C^\dagger)^{\otimes 2}\right]$ may be hard to analyze, but the 2-design property allows one to perhaps sidestep the difficulty by proving the desired result for Haar random unitaries instead. We record the Clifford 2-design result as a theorem for future references.

**Theorem 2.2** ([DCEL09])**.** *The discrete uniform distribution over the Clifford group, $\mathcal{U}(\mathbf{C}_n)$, forms an exact unitary 2-design.*

In fact, it has been proven more recently that $\mathcal{U}(\mathbf{C}_n)$ forms an exact unitary 3-design.

**Theorem 2.3** ([Web15, Zhu17])**.** *The discrete uniform distribution over the Clifford group, $\mathcal{U}(\mathbf{C}_n)$, forms an exact unitary 3-design but not an exact unitary 4-design.*

We mention that while a uniformly random $n$-qubit Clifford operator can be sampled in $O(n^2)$ time [BM21], no efficient construction of exact unitary $t$-design is currently known for general $t$ [NZO+21].

It turns out that random quantum circuits form approximate but not exact unitary $t$-designs. We formally define approximate unitary $t$-designs below.

**Definition 2.2** ($\epsilon$-approximate unitary $t$-design)**.** An $n$-qubit random unitary distribution $\mathcal{D}$ is an $\varepsilon$-approximate unitary $t$-design if

$$\left\| \mathop{\mathbb{E}}_{U\sim\mathcal{D}} \left[U^{\otimes t} \otimes (\overline{U})^{\otimes t}\right] - P_N^{(t)} \right\|_\infty \leq \varepsilon,$$

where $\|\cdot\|_\infty$ is the Schatten-$\infty$/operator norm.

In our opening sales pitch, we marketed random quantum circuits as efficient drop-in replacements for Haar random unitaries. We will see shortly that the approximate unitary $t$-design condition quantifies the depth required for the $t$-th moments of random quantum circuits to be sufficiently indistinguishable from the $t$-th moments of Haar random unitaries. Depending on the application, many definitions of $\varepsilon$-approximate unitary $t$-designs have been proposed, most involve choosing a different norm [BHH16, HM18]. For applications appearing in this work, the operator norm based definition will suffice. We begin by answering a sanity check question which asks is an approximate $t$-design also an approximate $t'$-design for every $1 \leq t' \leq t$?

**Lemma 2.4.** *For every $t \geq 2$, if an $n$-qubit random unitary distribution $\mathcal{D}$ is an $\varepsilon$-approximate unitary $t$-design, then $\mathcal{D}$ is also an $\varepsilon$-approximate unitary $(t-1)$-design.*

*Proof.* Let $\mathcal{D}$ be an $\varepsilon$-approximate unitary $t$-design for some $t \geq 2$. Let $t' = t-1$. Let $A \in (\mathbb{C}^{N\times N})^{\otimes t'}$ such that $|A\rangle$ attains $\left\|\mathbb{E}_{U\sim\mathcal{D}}\left[U^{\otimes t'} \otimes (\overline{U})^{\otimes t'}\right] - P_N^{(t')}\right\|_\infty$. By the choice of $A$,

$$\begin{aligned}
\left\| \mathop{\mathbb{E}}_{U\sim\mathcal{D}} \left[U^{\otimes t'} \otimes (\overline{U})^{\otimes t'}\right] - P_N^{(t')} \right\|_\infty &= \frac{\left\| \left(\mathbb{E}_{U\sim\mathcal{D}}\left[U^{\otimes t'} \otimes (\overline{U})^{\otimes t'}\right] - P_N^{(t')}\right)|A\rangle \right\|_2}{\||A\rangle\|_2} \\
&= \frac{\left\| \Phi_{\mathcal{D}}^{(t')}(A) - \Phi_{\mu_{\mathrm{Haar}}^N}^{(t')}(A) \right\|_F}{\|A\|_F}.
\end{aligned}$$

By the definition of $\Phi_{\mathcal{D}}^{(t)}$ and properties of $\|\cdot\|_F$ and $\|\cdot\|_\infty$,

$$\begin{aligned}
\frac{\left\| \Phi_{\mathcal{D}}^{(t')}(A) - \Phi_{\mu_{\mathrm{Haar}}^N}^{(t')}(A) \right\|_F}{\|A\|_F} &= \frac{\left\| \left(\Phi_{\mathcal{D}}^{(t')}(A) - \Phi_{\mu_{\mathrm{Haar}}^N}^{(t')}(A)\right) \otimes I \right\|_F}{\|A\otimes I\|_F} \\
&= \frac{\left\| \Phi_{\mathcal{D}}^{(t)}(A\otimes I) - \Phi_{\mu_{\mathrm{Haar}}^N}^{(t)}(A\otimes I) \right\|_F}{\|A\otimes I\|_F} \\
&\leq \left\| \mathop{\mathbb{E}}_{U\sim\mathcal{D}} \left[U^{\otimes t} \otimes (\overline{U})^{\otimes t}\right] - P_N^{(t)} \right\|_\infty \\
&\leq \varepsilon
\end{aligned}$$

where $I$ is the $n$-qubit identity operator. □

Next, we discuss the techniques first conceived in [BH10] and [BHH16] for showing that local and 1D random quantum circuits form efficient $\varepsilon$-approximate unitary $t$-designs w.r.t the operator norm. For every $i \in [n-1]$, we see that

$$Q_i^{(t)} = I^{\otimes(i-1)} \otimes P_4^{(t)} \otimes I^{\otimes(n-i-1)}$$

is the $t$-th moment operator of the $n$-qubit random unitary distribution that applies a Haar random 2-qubit gate to qubits $i$ and $i+1$ and identity to all other qubits. Note that in the above, $I$ is the $2t$-qubit identity operator. Then by the law of total expectation, the $t$-th moment operator of each gate in a local random quantum circuit (recall Definition 1.3) is

$$M_{\text{local}}^{(t)} = \frac{1}{n-1}\sum_{i=1}^{n-1} Q_i^{(t)}.$$

Since matrix-matrix multiplication represents function composition, the $t$-th moment operator of $n$-qubit-$s$-gate local random quantum circuits is $\left(M_{\text{local}}^{(t)}\right)^s$. Before discussing the efficiency part, we first settle another sanity check question which asks why is it the case that $\left(M_{\text{local}}^{(t)}\right)^s$ asymptotically converges to $P_N^{(t)}$ as $s$ goes to infinity at all?

**Lemma 2.5** ([BH10, BHH16])**.** *For every $t \geq 1$,*

$$\lim_{s\to\infty}\left(M_{\text{local}}^{(t)}\right)^s = P_N^{(t)}.$$

*Proof.* It suffices to show that

$$\lim_{s\to\infty}\left\|\left(M_{\text{local}}^{(t)}\right)^s - P_N^{(t)}\right\|_\infty = 0.$$

By the unitary invariance property of the Haar measure and linearity,

$$M_{\text{local}}^{(t)} P_N^{(t)} = P_N^{(t)} = P_N^{(t)} M_{\text{local}}^{(t)}.$$

This implies that for every $s \geq 1$,

$$\left\|\left(M_{\text{local}}^{(t)}\right)^s - P_N^{(t)}\right\|_\infty = \left\|\left(M_{\text{local}}^{(t)} - P_N^{(t)}\right)^s\right\|_\infty \leq \left\|M_{\text{local}}^{(t)} - P_N^{(t)}\right\|_\infty^s. \tag{2.3}$$

Thus, it suffices to show that $\left\|M_{\text{local}}^{(t)} - P_N^{(t)}\right\|_\infty < 1$. By Lemma 2.1, $M_{\text{local}}^{(t)}$ is a positive semi-definite operator with all eigenvalues falling in $[0,1]$, and since $P_N^{(t)}$ and $M_{\text{local}}^{(t)}$ commute, they can be simultaneously diagonalized. It is easy to see that $M_{\text{local}}^{(t)}|W_\pi^{(N)}\rangle = |W_\pi^{(N)}\rangle$ for every $\pi \in S_t$, so $M_{\text{local}}^{(t)}$ has a $+1$-eigenspace, and it contains $\text{span}\{|W_\pi^{(N)}\rangle : \pi \in S_t\}$. Hence, to show $\left\|M_{\text{local}}^{(t)} - P_N^{(t)}\right\|_\infty < 1$, it suffices to show that the $+1$-eigenspace of $M_{\text{local}}^{(t)}$ coincides with the $+1$-eigenspace of $P_N^{(t)}$, which is shown to be $\text{span}\{|W_\pi^{(N)}\rangle : \pi \in S_t\}$ in Lemma 2.1.

Let $A \in (\mathbb{C}^{N\times N})^{\otimes t}$ such that $M_{\text{local}}^{(t)}|A\rangle = |A\rangle$. Since $Q_i^{(t)}$ is an orthogonal projector for every $i \in [n-1]$, $M_{\text{local}}^{(t)}|A\rangle = |A\rangle$ if and only if $Q_i^{(t)}|A\rangle = |A\rangle$ for every $i \in [n-1]$. Let $V_i$ be an arbitrary 2-qubit gate acting on qubits $i$ and $i+1$ for some $i \in [n-1]$. Then,

$$V_i^{\otimes t} A = V_i^{\otimes t} \mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^4}\left[(V_i^\dagger U_i)^{\otimes t} A (U_i^\dagger V_i)^{\otimes t}\right] = A V_i^{\otimes t}. \tag{2.4}$$

Let $V \in \mathbb{U}(N)$ be an arbitrary $n$-qubit unitary. Since the set of all 2-qubit gates acting on nearest neighbour qubits is exactly universal for quantum computation, there exist $r \geq 1$, 2-qubit gates $V^{(1)}, \ldots, V^{(r)} \in \mathbb{U}(4)$, qubit indices $i_1, \ldots, i_r \in [n-1]$ such that $V = V_{i_r}^{(r)} \cdots V_{i_1}^{(1)}$. Then by (2.4) applied to $V_{i_1}^{(1)}, \ldots, V_{i_r}^{(r)}$ in sequence, $V^{\otimes t} A = A V^{\otimes t}$. Therefore, by Schur-Weyl duality, $|A\rangle \in \text{span}\{|W_\pi^{(N)}\rangle : \pi \in S_t\}$. □

The proof of Lemma 2.5 reveals a few useful properties of $M_{\text{local}}^{(t)}$ which we record below as corollaries.

**Corollary 2.1.**

*(a) The eigenvalues of $M_{\text{local}}^{(t)}$ fall in $[0,1]$, and the $+1$-eigenspace of $M_{\text{local}}^{(t)}$ is span$\{|W_\pi^{(N)}\rangle : \pi \in S_t\}$;*

*(b) $M_{\text{local}}^{(t)} - P_N^{(t)}$ is positive semi-definite;*

*(c) $\left\|M_{\text{local}}^{(t)} - P_N^{(t)}\right\|_\infty$ is the second largest eigenvalue of $M_{\text{local}}^{(t)}$.*

The proof also suggests a method to bound the rate at which $\left(M_{\text{local}}^{(t)}\right)^s$ converges to $P_N^{(t)}$. Namely, if we can show that $\left\|M_{\text{local}}^{(t)} - P_N^{(t)}\right\|_\infty \leq 1-\delta$, then by (2.3), for every $\varepsilon > 0$,

$$\left\|\left(M_{\text{local}}^{(t)}\right)^s - P_N^{(t)}\right\|_\infty \leq (1-\delta)^s \leq e^{-\delta s} \leq \varepsilon \tag{2.5}$$

for $s \geq \frac{1}{\delta}\ln(1/\varepsilon)$. Therefore, the problem reduces to upper bounding $\left\|M_{\text{local}}^{(t)} - P_N^{(t)}\right\|_\infty$ which by our proof of Lemma 2.5, is simply the second largest eigenvalue of $M_{\text{local}}^{(t)}$.

We recognize that $M_{\text{local}}^{(t)}$ has the form of a translation-invariant 1D 2-local Hamiltonian with projective local terms $Q_i^{(t)}$. $M_{\text{local}}^{(t)}$ can be put into a canonical form

$$H_n^{(t)} = \sum_{i=1}^{n-1}\left(I^{\otimes n} - Q_i^{(t)}\right)$$

by flipping the $+1$-eigenspace of $M_{\text{local}}^{(t)}$ to be the zero-energy ground space of $H_n^{(t)}$. Note that $H_n^{(t)}$ is frustration-free. It is easy to see that

$$M_{\text{local}}^{(t)} = I^{\otimes n} - \frac{H_n^{(t)}}{n-1},$$

so

$$\left\|M_{\text{local}}^{(t)} - P_N^{(t)}\right\|_\infty = 1 - \frac{\Delta(H_n^{(t)})}{n-1} \tag{2.6}$$

where $\Delta(H_n^{(t)})$ denotes the spectral gap of $H_n^{(t)}$. Thus, the problem further reduces to lower bounding $\Delta(H_n^{(t)})$. Lower bounding the spectral gap of local Hamiltonians is an intensely studied problem in Hamiltonian complexity theory with several known techniques, in particular for the special case of frustration-free Hamiltonians [Kna88, Nac96]. The authors of [BHH16] succesfully applied a method due to Nachtergaele [Nac96] to arrive at the following theorem.

**Theorem 2.4** ([BHH16])**.** *For every $n \geq 2$ and $t \geq 1$,*

$$\Delta(H_n^{(t)}) \geq \frac{1}{62500et^{9.5}\lceil\log_2(4t)\rceil^2}.$$

Note that the spectral gap is independent of $n$ and is a constant for constant $t$. By combining Theorem 2.4 and (2.6) with (2.5), we arrive at the main result.

**Theorem 2.5** ([BHH16])**.** *Local random quantum circuits of size* $O\left(nt^{9.5}\log(t)^2\log(1/\varepsilon)\right)$ *form an* $\varepsilon$*-approximate unitary* $t$*-design w.r.t the operator norm.*

Stronger and more explicit bounds for the spectral gap and design size can be obtained for $t \in \{2,3\}$ using the Knabe bound [Kna88], a technique much simpler than the one adopted by [BHH16].

**Theorem 2.6** ([BH10, HHJ21])**.** *For every* $n \geq 6$ *and* $t \in \{2,3\}$*,*

$$\Delta(H_n^{(t)}) \geq \frac{1}{5}.$$

**Theorem 2.7** ([BH10, HHJ21])**.** *Local random quantum circuits of size* $5n\ln(1/\varepsilon)$ *form an* $\varepsilon$*-approximate unitary* 3*-design w.r.t the operator norm.*

Next, we show how to translate Theorem 2.5 and Theorem 2.7 to 1D random quantum circuits via a powerful yet simple tool in Hamiltonian complexity theory called the detectability lemma [AALV09, AAV16]. Define

$$P_{\text{odd}}^{(t)} = Q_1^{(t)}Q_3^{(t)}\cdots Q_{n-1}^{(t)} \quad \text{and} \quad P_{\text{even}}^{(t)} = Q_2^{(t)}Q_4^{(t)}\cdots Q_n^{(t)}. \tag{2.7}$$

Notice that $P_{\text{odd}}^{(t)}$ and $P_{\text{even}}^{(t)}$ are the $t$-th moment operators of the odd- and even-numbered layers in 1D random quantum circuits respectively, and the $t$-th moment operator of $\mathcal{H}_{n,2k+1}^{\text{path}}$, $k \geq 1$ (recall Definition 1.4) is

$$\left(P_{\text{odd}}^{(t)}P_{\text{even}}^{(t)}P_{\text{odd}}^{(t)}\right)^k.$$

By mirroring the proof of Lemma 2.5, one can show (using Lemma A.3) the following lemma by establishing the corresponding properties in Corollary 2.1 for $P_{\text{odd}}^{(t)}P_{\text{even}}^{(t)}P_{\text{odd}}^{(t)}$.

**Lemma 2.6.** *For every* $t \geq 1$*,*

$$\lim_{k\to\infty}\left(P_{\text{odd}}^{(t)}P_{\text{even}}^{(t)}P_{\text{odd}}^{(t)}\right)^k = P_N^{(t)}.$$

**Corollary 2.2.**

*(a) The eigenvalues of* $P_{\text{odd}}^{(t)}P_{\text{even}}^{(t)}P_{\text{odd}}^{(t)}$ *fall in* $[0,1]$*, and the* $+1$*-eigenspace of* $P_{\text{odd}}^{(t)}P_{\text{even}}^{(t)}P_{\text{odd}}^{(t)}$ *is span*$\{|W_\pi^{(N)}\rangle : \pi \in S_t\}$*;*

*(b)* $P_{\text{odd}}^{(t)}P_{\text{even}}^{(t)}P_{\text{odd}}^{(t)} - P_N^{(t)}$ *is positive semi-definite;*

*(c)* $\left\|P_{\text{odd}}^{(t)}P_{\text{even}}^{(t)}P_{\text{odd}}^{(t)} - P_N^{(t)}\right\|_\infty$ *is the second largest eigenvalue of* $P_{\text{odd}}^{(t)}P_{\text{even}}^{(t)}P_{\text{odd}}^{(t)}$.

Again in a completely analogous fashion, to show that 1D random quantum circuits form approximate $t$-designs, it suffices to upper bound $\left\|P_{\text{odd}}^{(t)}P_{\text{even}}^{(t)}P_{\text{odd}}^{(t)} - P_N^{(t)}\right\|_\infty$. The main difference is that in place of (2.6), the detectability lemma is what allows us to reduce upper bounding $\left\|P_{\text{even}}^{(t)}P_{\text{odd}}^{(t)} - P_N^{(t)}\right\|_\infty$ to lower bounding $\Delta(H_n^{(t)})$.

**Lemma 2.7** (The Detectability Lemma (DL)[AAV16]). *Let $H = \sum_{i=1}^{m} Q_i$ be a frustration-free Hamiltonian with projective local terms $\{Q_1, \ldots, Q_m\}$ such that each $Q_i$ commutes with all but $g$ others. Then for every state $|\psi^{\perp}\rangle$ orthogonal to the ground space of $H$,*

$$\left\| \prod_{i=1}^{m} (I - Q_i) |\psi^{\perp}\rangle \right\|_2^2 \leq \frac{1}{\Delta(H)/g^2 + 1}$$

*where the product $\prod_{i=1}^{m}(I - Q_i)$ can be taken in any order.*

By applying the DL to $H_n^{(t)}$ with the ordering $P_{\text{even}}^{(t)} P_{\text{odd}}^{(t)}$, Corollary 2.2, and the variational characterization of eigenvalues, we get the following bound.

**Lemma 2.8.**

$$\left\| P_{\text{odd}}^{(t)} P_{\text{even}}^{(t)} P_{\text{odd}}^{(t)} - P_N^{(t)} \right\|_{\infty} \leq \frac{1}{\Delta(H_n^{(t)})/4 + 1}$$

By combining Lemma 2.8 with Theorem 2.4, we get the following $t$-design depth bound for 1D random quantum circuits.

**Theorem 2.8.** *1D random quantum circuits of depth $O\left(t^{9.5} \log(t)^2 \log(1/\varepsilon)\right)$ form an $\varepsilon$-approximate unitary $t$-design w.r.t the operator norm.*

Alternatively, Lemma 2.8 and Theorem 2.6 yield the following explicit 3-design depth bound for 1D random quantum circuits.

**Theorem 2.9.** *1D random quantum circuits of depth $43 \ln(1/\varepsilon)$ form an $\varepsilon$-approximate unitary 3-design w.r.t the operator norm.*

Skeptical readers may find it doubtful that the design depths can be independent of $n$. To resolve the apparent contradiction, we will soon see that typical applications will require $\varepsilon = \frac{O(1)}{2^{nt}}$ or even smaller, thereby introducing the intuitively expected dependence on $n$.

## 2.3 Collision Probability and Anti-Concentration

A probability distribution over some sample space of size $N$ is said to concentrate if a $1 - o(1)$ fraction of the total probability mass is assigned to a constant fraction of the sample space. Conversely, a distribution is said to anti-concentrate if it does not concentrate; that is, every constant fraction of the sample space is assigned a constant fraction of the probability mass. Let $V \in \mathbb{U}(N)$ be an $n$-qubit unitary and consider its output distribution $q_V$. Let $p_{\text{med}}$ be the median of $q_V$. If $q_V$ anti-concentrates according to the above definition, then a simple argument shows that $p_{\text{med}} = \frac{\alpha}{N}$ for some constant $\alpha \in (0, 2)$. Thus, we get that

$$\Pr_{x \sim \mathcal{U}(\{0,1\}^n)} \left( |\langle x|V|0^n\rangle|^2 \geq \frac{\alpha}{2^n} \right) \geq \frac{1}{2}.$$

This motivates the following definition for the anti-concentration property of random quantum circuits.

**Definition 2.3** (Anti-Concentration of Random Unitary Distributions)**.** An $n$-qubit random unitary distribution $\mathcal{D}$ is said to have the anti-concentration property if there exist constants $\alpha > 0$ and $\delta \in (0, 1)$ such that for every $x \in \{0, 1\}^n$,

$$\Pr_{U \sim \mathcal{D}} \left[ |\langle x|U|0^n\rangle|^2 \geq \frac{\alpha}{2^n} \right] \geq 1 - \delta.$$

The collision probability of a distribution is the probability that two independent samples drawn from the distribution take the same value. In the random quantum circuits scenario, we formalize the idea of collision probability in the following definition.

**Definition 2.4** (Collision Probability of Random Unitary Distributions)**.** The (expected) collision probability of an $n$-qubit random unitary distribution $\mathcal{D}$ is

$$\mathrm{Coll}(\mathcal{D}) = \mathop{\mathbb{E}}_{U \sim \mathcal{D}} \left[ \Pr_{x,y \sim q_U} (x = y) \right] = \mathop{\mathbb{E}}_{U \sim \mathcal{D}} \left[ \sum_{z \in \{0,1\}^n} |\langle z|U|0^n\rangle|^4 \right]$$

where $q_U$ is the output distribution of $U$, and $x$ and $y$ are drawn independently.

It is easy to show that if $\mathcal{D}$ has the hiding property, then

$$\mathrm{Coll}(\mathcal{D}) = 2^n \mathop{\mathbb{E}}_{U \sim \mathcal{D}} \left[ |\langle 0^n|U|0^n\rangle|^4 \right].$$

Intuitively, if a probability distribution is concentrated, then its collision probability will be high and vice versa. The forward direction of this intuition can be formally established via the Paley-Zygmund inequality, where we show that for random quantum circuits, having a small collision probability is a sufficient condition for anti-concentration. The following lemma statement is borrowed from [BMS16].

**Lemma 2.9** (Paley-Zygmund Inequality)**.** *If $R$ is a non-negative random variable with finite variance, then for every $0 < \alpha < 1$,*

$$\Pr(R \geq \alpha\, \mathbb{E}[R]) \geq (1 - \alpha)^2 \frac{\mathbb{E}[R]^2}{\mathbb{E}[R^2]}.$$

**Lemma 2.10.** *Let $\mathcal{D}$ be an $n$-qubit random unitary distribution with the hiding property. If $\mathrm{Coll}(\mathcal{D}) \leq \frac{O(1)}{2^n}$, then $\mathcal{D}$ has the anti-concentration property.*

*Proof.* Using the hiding property, we see that

$$\mathop{\mathbb{E}}_{U \sim \mathcal{D}} \left[ |\langle 0^n|U|0^n\rangle|^2 \right]^2 = \frac{1}{2^{2n}}$$

and

$$\mathop{\mathbb{E}}_{U \sim \mathcal{D}} \left[ |\langle 0^n|U|0^n\rangle|^4 \right] = \frac{\mathrm{Coll}(\mathcal{D})}{2^n} \leq \frac{O(1)}{2^{2n}}.$$

Then the claim follows directly from the Paley-Zygmund inequality. □

Therefore, to show anti-concentration for a random unitary distribution, it suffices to upper bound its collision probability by some constant over $2^n$. On the other hand, if we can show a $\frac{\omega(1)}{2^n}$ lower bound for the collision probability of some random unitary distribution $\mathcal{D}$, then it suggests that $\mathcal{D}$ does not anti-concentrate. In fact, given their close connections, some authors have formally defined the anti-concentration property in terms of the collision probability [DHJB20]. In the rest of this work, we will interpret the condition $\text{Coll}(\mathcal{D}) \leq \frac{O(1)}{2^n}$ as being synonymous with anti-concentration.

The significance of the collision probability and anti-concentration is twofold. For one, the anti-concentration property is one of two main technical conditions needed to complete the program outlined by Aaronson for proving the random circuit sampling supremacy conjecture [AA11]. For two, the mathematical expressions that come up in the analyses of the collision probability will reappear in analyzing the performance of both quantum and classical algorithms on the linear cross-entropy benchmark proposed by Google [BCG20]. We will expand on both applications in Chapter 3.

In the remainder of this section, we will develop an understanding of the collision probability as a function of circuit depths. We begin by computing the collision probability of the Haar distribution over $\mathbb{U}(N)$, which by Lemma 2.6, also corresponds to the infinite circuit depth limit for 1D random quantum circuits.

**Theorem 2.10.** $\text{Coll}(\mu^N_{Haar}) = \frac{2}{2^n+1}$

*Proof.* There are numerous proofs for this basic result, and arguably the most straightforward of which involves little more than substituting $t = 2$ into Lemma 2.3. Instead of doing that, we will proceed with a more combinatorial argument for the purpose of previewing a technique that will be useful again and was alluded to in section 2.2. By the definition of $\text{Coll}(\mu^N_{\text{Haar}})$, we see that

$$\begin{aligned}\text{Coll}(\mu^N_{\text{Haar}}) &= \mathop{\mathbb{E}}_{U\sim\mu^N_{\text{Haar}}}\left[\sum_{z\in\{0,1\}^n} |\langle z|U|0^n\rangle|^4\right] \\ &= \mathop{\mathbb{E}}_{U\sim\mu^N_{\text{Haar}}}\left[\sum_{z\in\{0,1\}^n} \langle 0^{2n}|(U^\dagger\otimes U^\dagger)(|z\rangle\langle z|\otimes|z\rangle\langle z|)(U\otimes U)|0^{2n}\rangle\right].\end{aligned}$$

We can show with some simple algebra (see Lemma A.1) that

$$\sum_{z\in\{0,1\}^n} |z\rangle\langle z|\otimes|z\rangle\langle z| = \frac{1}{2^n}\sum_{w\in\{0,1\}^n} Z(w)\otimes Z(w).$$

Thus,

$$\text{Coll}(\mu^N_{\text{Haar}}) = \frac{1}{2^n}\sum_{w\in\{0,1\}^n}\mathop{\mathbb{E}}_{U\sim\mu^N_{\text{Haar}}}\left[\langle 0^{2n}|(U^\dagger\otimes U^\dagger)(Z(w)\otimes Z(w))(U\otimes U)|0^{2n}\rangle\right]. \tag{2.8}$$

Let $w \in \{0,1\}^n \setminus \{0^n\}$. Since $\mathcal{U}(\mathbf{C}_n)$, the discrete uniform distribution over the $n$-qubit Clifford group, forms an exact unitary 2-design (recall Theorem 2.2),

$$\mathop{\mathbb{E}}_{U\sim\mu^N_{\text{Haar}}}\left[\langle 0^{2n}|(U^\dagger\otimes U^\dagger)(Z(w)\otimes Z(w))(U\otimes U)|0^{2n}\rangle\right]$$

$$= \mathop{\mathbb{E}}_{C\sim\mathcal{U}(\mathbf{C}_n)} \left[\langle 0^{2n}|(C^\dagger \otimes C^\dagger)(Z(w)\otimes Z(w))(C\otimes C)|0^{2n}\rangle\right]$$
$$= \mathop{\mathbb{E}}_{C\sim\mathcal{U}(\mathbf{C}_n)} \left[\langle 0^{n}|C^\dagger Z(w) C|0^{n}\rangle^2\right].$$

Let $C \sim \mathcal{U}(\mathbf{C}_n)$. Since $C$ is a uniformly random Clifford operator and $Z(w)$ is a non-identity Pauli, $C^\dagger Z(w) C$ is a uniformly random element in $\mathbf{P}_n \setminus \{\pm I^{\otimes n}\}$ with $\pm 1$ phases. Thus, $\langle 0^n|C^\dagger Z(w)C|0^n\rangle \in \{-1, 0, 1\}$, implying $\langle 0^n|C^\dagger Z(w)C|0^n\rangle^2 = |\langle 0^n|C^\dagger Z(w)C|0^n\rangle| \in \{0,1\}$. Since $|\langle 0^n|C^\dagger Z(w)C|0^n\rangle| = 1$ if and only if $C^\dagger Z(w) C$ is a $Z$-type Pauli, we have

$$\begin{aligned}
\mathop{\mathbb{E}}_{C\sim\mathcal{U}(\mathbf{C}_n)} \left[\langle 0^{n}|C^\dagger Z(w) C|0^{n}\rangle^2\right] &= \Pr_{C\sim\mathcal{U}(\mathbf{C}_n)} \left(|\langle 0^{n}|C^\dagger Z(w) C|0^{n}\rangle| = 1\right) \\
&= \Pr_{C\sim\mathcal{U}(\mathbf{C}_n)} \left(C^\dagger Z(w) C \text{ is a } Z\text{-type Pauli}\right) \\
&= \sum_{j=1}^{n} \frac{1}{3^j} \Pr_{C\sim\mathcal{U}(\mathbf{C}_n)} (C^\dagger Z(w) C \text{ has weight } j) \\
&= \sum_{j=1}^{n} \frac{1}{3^j} \cdot \frac{\binom{n}{j} 3^j}{4^n - 1} \\
&= \frac{1}{2^n + 1}.
\end{aligned}$$

Therefore,

$$(2.8) = \frac{1}{2^n}\left(1 + \frac{2^n - 1}{2^n + 1}\right) = \frac{2}{2^n + 1}.$$

□

We record an intermediary finding as a corollary.

**Corollary 2.3.** *For every $w \in \{0,1\}^n \setminus \{0^n\}$,*

$$\mathop{\mathbb{E}}_{U\sim\mu_{Haar}^N} \left[\langle 0^{2n}|(U\otimes U)(Z(w)\otimes Z(w))(U^\dagger \otimes U^\dagger)|0^{2n}\rangle\right] = \frac{1}{2^n+1}.$$

Theorem 2.10 implies the following lemma.

**Lemma 2.11.** *For every $n$-qubit random unitary distribution $\mathcal{D}$ with the hiding property that forms an $\frac{O(1)}{2^{2n}}$-approximate unitary 2-design,* $\mathrm{Coll}(\mathcal{D}) \le \frac{O(1)}{2^n}$.

*Proof.* By the approximate 2-design condition,

$$\langle 0^{4n}|\Big(\mathop{\mathbb{E}}_{U\sim\mathcal{D}} \left[U^{\otimes 2}\otimes(\overline{U})^{\otimes 2}\right] - P_N^{(2)}\Big)|0^{4n}\rangle \le \Big\| \mathop{\mathbb{E}}_{U\sim\mathcal{D}} \left[U^{\otimes 2}\otimes(\overline{U})^{\otimes 2}\right] - P_N^{(2)}\Big\|_\infty \le \frac{O(1)}{2^{2n}}. \quad (2.9)$$

By the hiding property,

$$\begin{aligned}
\mathrm{Coll}(\mathcal{D}) &= 2^n \mathop{\mathbb{E}}_{U\sim\mathcal{D}} \left[\langle 0^{2n}|(U\otimes U)|0^{2n}\rangle\langle 0^{2n}|(U^\dagger\otimes U^\dagger)|0^{2n}\rangle\right] \\
&= 2^n \langle 0^{4n}| \mathop{\mathbb{E}}_{U\sim\mathcal{D}} \left[U^{\otimes 2}\otimes(\overline{U})^{\otimes 2}\right]|0^{4n}\rangle
\end{aligned}$$

$$
\begin{aligned}
&\leq 2^n \langle 0^{4n} | P_N^{(2)} | 0^{4n} \rangle + \frac{O(1)}{2^n} \\
&= \mathrm{Coll}(\mu_{\mathrm{Haar}}^N) + \frac{O(1)}{2^n} \\
&\leq \frac{O(1)}{2^n}.
\end{aligned}
$$

□

**Corollary 2.4.** $\mathrm{Coll}\left(\mathcal{H}_{n,O(n)}^{path}\right) \leq \frac{O(1)}{2^n}$

Although having the approximate 2-design property is sufficient for anti-concentration, we do not believe the two properties are equivalent in general since there is no reason to expect that the first inequality in (2.9) is tight. Indeed, to arrive at

$$
\langle 0^{4n} | \Big( \mathop{\mathbb{E}}_{U \sim \mathcal{D}} \left[ U^{\otimes 2} \otimes (\overline{U})^{\otimes 2} \right] - P_N^{(2)} \Big) | 0^{4n} \rangle \leq \frac{O(1)}{2^{2n}},
$$

it suffices to just assume

$$
\left\| \Big( \mathop{\mathbb{E}}_{U \sim \mathcal{D}} \left[ U^{\otimes 2} \otimes (\overline{U})^{\otimes 2} \right] - P_N^{(2)} \Big) | 0^{4n} \rangle \right\|_2 \leq \frac{O(1)}{2^{2n}},
$$

whereas for $\mathcal{D}$ to satisfy the $\frac{O(1)}{2^{2n}}$-approximate 2-design condition

$$
\left\| \mathop{\mathbb{E}}_{U \sim \mathcal{D}} \left[ U^{\otimes 2} \otimes (\overline{U})^{\otimes 2} \right] - P_N^{(2)} \right\|_\infty \leq \frac{O(1)}{2^{2n}},
$$

it would require

$$
\left\| \Big( \mathop{\mathbb{E}}_{U \sim \mathcal{D}} \left[ U^{\otimes 2} \otimes (\overline{U})^{\otimes 2} \right] - P_N^{(2)} \Big) | A \rangle \right\|_2 \leq \frac{O(1)}{2^{2n}}
$$

for every $A \in (\mathbb{C}^{N \times N})^{\otimes 2}$ with $\|A\|_F = 1$. Thus, anti-concentration can be viewed as a less demanding requirement for formally classifying a random unitary distribution $\mathcal{D}$ as being close to Haar.

Next, we report a recently established, much stronger collision probability upper bound for the 1D architecture, implying 1D random quantum circuits anti-concentrate in $O(\log n)$-depth.

**Theorem 2.11** ([BCG20],[DHJB20])**.** *For every $d \geq 1$,* $\mathrm{Coll}\left(\mathcal{H}_{n,d}^{path}\right) \leq \frac{2}{2^n} \exp\left(\left(\frac{4}{5}\right)^{d-1} n\right)$.

*Proof.* This proof is based on [DHJB20]. We have that

$$
\mathrm{Coll}\left(\mathcal{H}_{n,d}^{\mathrm{path}}\right) = 2^n \mathop{\mathbb{E}}_{U \sim \mathcal{H}_{n,d}^{\mathrm{path}}} \left[ \langle 0^{2n} | (U \otimes U) | 0^{2n} \rangle \langle 0^{2n} | (U^\dagger \otimes U^\dagger) | 0^{2n} \rangle \right].
$$

By the unitary invariance property applied separately to the first $\frac{n}{2}$ random 2-qubit gates in the 1D architecture, we can prepend a random 1-qubit gate to every qubit. Algebraically, we get that

$$
\mathop{\mathbb{E}}_{U \sim \mathcal{H}_{n,d}^{\mathrm{path}}} \left[ (U \otimes U) | 0^{2n} \rangle \langle 0^{2n} | (U^\dagger \otimes U^\dagger) \right]
$$

$$= \mathop{\mathbb{E}}_{U\sim\mathcal{H}_{n,d}^{\text{path}}} \left[ (U\otimes U) \bigotimes_{i=1}^{n} \mathop{\mathbb{E}}_{V\sim\mu_{\text{Haar}}^2} \left[ (V\otimes V)|00\rangle\langle 00|(V^\dagger\otimes V^\dagger) \right] (U^\dagger\otimes U^\dagger) \right].$$

Let $S_2 = \{\pi_1, \pi_2\}$ for $\pi_1$ being the identity permutation and $\pi_2$ being swap. By substituting $N = 2$ and $t = 2$ into Lemma 2.3, we get that

$$\mathop{\mathbb{E}}_{V\sim\mu_{\text{Haar}}^2} \left[ (V\otimes V)|00\rangle\langle 00|(V^\dagger\otimes V^\dagger) \right] = \frac{1}{6}(I+S)$$

where we define $I = W_{\pi_1}^{(2)}$ and $S = W_{\pi_2}^{(2)}$. Thus,

$$\bigotimes_{i=1}^{n} \mathop{\mathbb{E}}_{V\sim\mu_{\text{Haar}}^2} \left[ (V\otimes V)|00\rangle\langle 00|(V^\dagger\otimes V^\dagger) \right] = \frac{1}{6^n}(I+S)^{\otimes n}.$$

For the ease of notation, we will treat a binary string $x \in \{I, S\}^n$ with alphabet $\{I, S\}$ also as the $n$-fold tensor product operator $\bigotimes_{i=1}^n x_i$. With this notation, we can write

$$\mathop{\mathbb{E}}_{U\sim\mathcal{H}_{n,d}^{\text{path}}} \left[ (U\otimes U)|0^{2n}\rangle\langle 0^{2n}|(U^\dagger\otimes U^\dagger) \right] = \frac{1}{6^n} \sum_{\gamma_0\in\{I,S\}^n} \mathop{\mathbb{E}}_{U\sim\mathcal{H}_{n,d}^{\text{path}}} \left[ (U\otimes U)\gamma_0(U^\dagger\otimes U^\dagger) \right].$$

Let $s$ denote the number of 2-qubit gates in a circuit drawn from $\mathcal{H}_{n,d}^{\text{path}}$. Note that $s$ is a function of $d$, the circuit depth. Let $i_1, \ldots, i_s \in [n-1]$ be qubit indices such that for every $j \in [s]$, the $j$-th gate acts on qubits $i_j$ and $i_j + 1$. Let $\gamma_0 \in \{I, S\}^n$. Since each random 2-qubit gate is drawn independently,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{U\sim\mathcal{H}_{n,d}^{\text{path}}} \left[ (U\otimes U)\gamma_0(U^\dagger\otimes U^\dagger) \right] \\
&= \mathop{\mathbb{E}}_{U^{(1)},\ldots,U^{(s)}\sim\mu_{\text{Haar}}^4} \left[ (U_{i_s}^{(s)}\otimes U_{i_s}^{(s)})\cdots(U_{i_1}^{(1)}\otimes U_{i_1}^{(1)})\gamma_0(U_{i_1}^{(1)}\otimes U_{i_1}^{(1)})^\dagger\cdots(U_{i_s}^{(s)}\otimes U_{i_s}^{(s)})^\dagger \right] \\
&= \mathop{\mathbb{E}}_{U^{(s)}\sim\mu_{\text{Haar}}^4} \left[ (U_{i_s}^{(s)}\otimes U_{i_s}^{(s)})\cdots \mathop{\mathbb{E}}_{U^{(1)}\sim\mu_{\text{Haar}}^4} \left[ (U_{i_1}^{(1)}\otimes U_{i_1}^{(1)})\gamma_0(U_{i_1}^{(1)}\otimes U_{i_1}^{(1)})^\dagger \right] \cdots (U_{i_s}^{(s)}\otimes U_{i_s}^{(s)})^\dagger \right].
\end{aligned}$$

Since each moment superoperator only acts non-trivially on two qubits, to workout

$$\mathop{\mathbb{E}}_{U^{(1)}\sim\mu_{\text{Haar}}^4} \left[ (U_{i_1}^{(1)}\otimes U_{i_1}^{(1)})\gamma_0(U_{i_1}^{(1)}\otimes U_{i_1}^{(1)})^\dagger \right],$$

it suffices to consider the following four combinations. By Lemma 2.1(c), we have

$$\mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^4} \left[ (U\otimes U)(I\otimes I)(U^\dagger\otimes U^\dagger) \right] = I\otimes I$$

and

$$\mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^4} \left[ (U\otimes U)(S\otimes S)(U^\dagger\otimes U^\dagger) \right] = S\otimes S.$$

By explicit calculations using Lemma 2.2, we get that

$$\mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^4} \left[ (U\otimes U)(I\otimes S)(U^\dagger\otimes U^\dagger) \right] = \mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^4} \left[ (U\otimes U)(S\otimes I)(U^\dagger\otimes U^\dagger) \right] = \frac{2}{5}(I\otimes I + S\otimes S)$$

where by rearranging the qubit wires, we can make $W_\pi^{(4)} = W_\pi^{(2)} \otimes W_\pi^{(2)}$ for both $\pi \in S_2$. Let $i$ and $j$ be the two qubits that $U^{(1)}$ acts on. The above formulas suggest a transition rule from $\gamma_0$ to $\gamma_1$ where if $(\gamma_0)_i(\gamma_0)_j \in \{II, SS\}$, then $\gamma_1 = \gamma_0$, and if $(\gamma_0)_i(\gamma_0)_j \in \{IS, SI\}$, then $\gamma_0$ splits into two binary strings $\gamma_1$ and $\gamma_1'$ where $(\gamma_1)_i(\gamma_1)_j = II$, $(\gamma_1')_i(\gamma_1')_j = SS$, and $(\gamma_0)_k = (\gamma_1)_k = (\gamma_1')_k$ for every $k \in [n] \setminus \{i, j\}$. By linearity, we can evaluate

$$\mathop{\mathbb{E}}_{U^{(2)} \sim \mu_{\text{Haar}}^4} \left[ (U_{i_2}^{(2)} \otimes U_{i_2}^{(2)}) \gamma_1 (U_{i_2}^{(2)} \otimes U_{i_2}^{(2)})^\dagger \right]$$

and

$$\mathop{\mathbb{E}}_{U^{(2)} \sim \mu_{\text{Haar}}^4} \left[ (U_{i_2}^{(2)} \otimes U_{i_2}^{(2)}) \gamma_1' (U_{i_2}^{(2)} \otimes U_{i_2}^{(2)})^\dagger \right]$$

separately and scale both terms by a weight of $\frac{2}{5}$. Applying this argument inductively to all $s$ random 2-qubit gates, a sequence $\vec{\gamma} = (\gamma_0, \ldots, \gamma_s)$ of binary strings forms a trajectory, and a trajectory is valid if for every $i \in \{0, 1, \ldots, s-1\}$, $\gamma_{i+1}$ can be obtained from $\gamma_i$ by the above transition rule. For every valid trajectory $\vec{\gamma} = (\gamma_0, \ldots, \gamma_s)$, we define its weight to be $w(\vec{\gamma}) = \left(\frac{2}{5}\right)^{|\{i : \gamma_i \neq \gamma_{i+1}\}|}$. Then, we can write

$$\mathop{\mathbb{E}}_{U \sim \mathcal{H}_{n,d}^{\text{path}}} \left[ (U \otimes U) |0^{2n}\rangle\langle 0^{2n}| (U^\dagger \otimes U^\dagger) \right] = \sum_{\vec{\gamma} = (\gamma_0, \ldots, \gamma_s)} w(\vec{\gamma}) \gamma_s.$$

Therefore,

$$\begin{aligned} \text{Coll}\left(\mathcal{H}_{n,d}^{\text{path}}\right) &= \frac{2^n}{6^n} \sum_{\vec{\gamma} = (\gamma_0, \ldots, \gamma_s)} w(\vec{\gamma}) \langle 0^{2n} | \gamma_s | 0^{2n} \rangle \\ &= \frac{1}{3^n} \sum_{\vec{\gamma} = (\gamma_0, \ldots, \gamma_s)} w(\vec{\gamma}), \end{aligned}$$

effectively reducing the problem of evaluating $\text{Coll}\left(\mathcal{H}_{n,d}^{\text{path}}\right)$ to the combinatorial problem of enumerating valid trajectories and their associated weights. While the reduction steps so far hold more generally for any circuit architecture with the hiding property, the rest of the proof will heavily exploit specific structures within the 1D architecture.

Let $\vec{\gamma} = (\gamma_0, \ldots, \gamma_s)$ be a valid trajectory and let $i \in \{0, \ldots, s\}$. A key observation is that the binary string $\gamma_i \in \{I, S\}^n$ can be uniquely specified by its first symbol $(\gamma_i)_0$ and a sorted list of distinct indices $L_i = \{j \in \{0, \ldots, n-1\} : (\gamma_i)_j \neq (\gamma_i)_{j+1}\}$ such that the mapping $\mathcal{L}(\vec{\gamma}) = \vec{L} = (L_0, \ldots, L_s)$ is 2-to-1. Namely, only $\vec{\gamma}$ and its complement trajectory $(\vec{\gamma})^c = (\overline{\gamma_0}, \ldots, \overline{\gamma_s})$ are mapped to $\vec{L}$ by $\mathcal{L}$. We say a sequence of indices $\vec{L}'$ is valid if there exists a valid trajectory $\vec{\gamma}'$ such that $\mathcal{L}(\vec{\gamma}') = \vec{L}'$. Since gates in the 1D architecture only act on adjacent pairs of qubits, the transition rule for $\vec{\gamma}$ induces a transition rule for $\vec{L}$. When a moment superoperator acts on an adjacent pair of qubits, for every $i \in \{0, \ldots, s-1\}$, if $\gamma_{i+1} = \gamma_i$, then $L_{i+1} = L_i$, and if $\gamma_{i+1} \neq \gamma_i$, then $L_{i+1}$ can be updated from $L_i$ by either deleting the first or last index, deleting two adjacent indices, or shifting one of the indices in $L_i$ by 1. For example, for $\gamma_i = SSIS$ with $L_i = \{2, 3\}$, if $\gamma_{i+1} = SSSS$, then $L_{i+1} = \emptyset$, and if $\gamma_{i+1} = SIIS$, then $L_{i+1} = \{1, 3\}$. We define $w(\vec{L}) = w(\vec{\gamma})$ and see that

$w(\vec{L}) = \left(\frac{2}{5}\right)^{|\{i:L_i \neq L_{i+1}\}|}$. Therefore, the task of enumerating all valid trajectories reduces to enumerating all valid sequences of indices. By the transition rule for $\vec{L}$, $|L_i| \geq |L_{i+1}|$ for every $i \in \{0, \ldots, s-1\}$, so if $L_i = \emptyset$, then $L_j = \emptyset$ for every $j \in \{i, \ldots, s\}$. Let

$$G_0^{(d)} = \{(I_0, \ldots, I_s) : (I_0, \ldots, I_s) \text{ is a valid sequence of indices and } I_s = \emptyset\}$$

and

$$G_1^{(d)} = \{(J_0, \ldots, J_s) : (J_0, \ldots, J_s) \text{ is a valid sequence of indices and } |J_0| = |J_s|\}.$$

Notice that the only sequence which belongs to both $G_0^{(d)}$ and $G_1^{(d)}$ is $(\emptyset, \ldots, \emptyset)$, and every valid sequence of indices $\vec{L} = (L_0, \ldots, L_s)$ can be decomposed as $(L_0, \ldots, L_s) = (I_0 \cup J_0, \ldots, I_s \cup J_s)$ such that $\vec{I} = (I_0, \ldots, I_s) \in G_0^{(d)}$, $\vec{J} = (J_0, \ldots, J_s) \in G_1^{(d)}$, and $w(\vec{L}) = w(\vec{I}) \cdot w(\vec{J})$. Therefore, since $w(\vec{L}) \geq 0$ for every valid $\vec{L}$,

$$\begin{aligned}
\operatorname{Coll}\left(\mathcal{H}_{n,d}^{\text{path}}\right) &= \frac{1}{3^n} \sum_{\vec{\gamma}} w(\vec{\gamma}) \\
&= \frac{2}{3^n} \sum_{\vec{L}} w(\vec{L}) \\
&\leq \left(\frac{2}{3^n} \sum_{\vec{I} \in G_0^{(d)}} w(\vec{I})\right)\left(\sum_{\vec{J} \in G_1^{(d)}} w(\vec{J})\right).
\end{aligned}$$

We first consider a seemly loose upper bound for the sum over $G_1^{(d)}$. Let $k \in [n]$, and let $J_0$ be an initial list of indices with $|J_0| = k$. Clearly, there are at most $\binom{n}{k}$ choices for $J_0$. Notice that for a sequence in $G_1^{(d)}$ starting with $J_0$, after the first layer, every index will be moved in every layer by a gate, branching the current sequence of indices into at most two sequences, each incurring a weight penalty of $\frac{2}{5}$. Therefore,

$$\begin{aligned}
\sum_{\vec{J} \in G_1^{(d)}} w(\vec{J}) &\leq \sum_{k=0}^{n} \binom{n}{k} 2^{k(d-1)} \left(\frac{2}{5}\right)^{k(d-1)} \\
&\leq \left(1 + \left(\frac{4}{5}\right)^{d-1}\right)^n \\
&\leq \exp\left(\left(\frac{4}{5}\right)^{d-1} n\right).
\end{aligned}$$

To handle the sum over $G_0^{(d)}$, we observe that for every $\vec{I} = (I_0, \ldots, I_s) \in G_0^{(d)}$, $(I_0, \ldots, I_s, \emptyset, \ldots, \emptyset) \in G_0^{(d+1)}$, and since the weights are all non-negative,

$$\sum_{\vec{I} \in G_0^{(d)}} w(\vec{I}) \leq \sum_{\vec{I} \in G_0^{(d+1)}} w(\vec{I}).$$

Since $G_0^{(d)}$ is a subset of all valid sequences of indices,

$$\frac{2}{3^n}\sum_{\vec{I}\in G_0^{(d)}} w(\vec{I}) \leq \frac{2}{3^n}\sum_{\vec{L}} w(\vec{L}) = \mathrm{Coll}\left(\mathcal{H}_{n,d}^{\mathrm{path}}\right).$$

Therefore,

$$\begin{aligned}\frac{2}{3^n}\sum_{\vec{I}\in G_0^{(d)}} w(\vec{I}) &\leq \lim_{d\to\infty}\frac{2}{3^n}\sum_{\vec{I}\in G_0^{(d)}} w(\vec{I}) \\ &\leq \lim_{d\to\infty}\mathrm{Coll}\left(\mathcal{H}_{n,d}^{\mathrm{path}}\right) \\ &= \mathrm{Coll}(\mu_{\mathrm{Haar}}^N) \\ &= \frac{2}{2^n+1},\end{aligned}$$

and this concludes the proof. □

Now, we turn to establish a generic collision probability lower bound for arbitrary circuit architectures. The main observation is that we can adapt the Pauli weight counting argument used in the proof of Theorem 2.10 from $n$-qubit random Clifford operators to random Clifford circuits. Recall that $\mathcal{C}_{\mathcal{A}}$ is the distribution of random circuits over some architecture $\mathcal{A}$ where each gate is a uniformly random 2-qubit Clifford gate.

**Lemma 2.12.** *For every $n$-qubit-depth-$d$ circuit architecture $\mathcal{A}$, and for every $w \in \{0,1\}^n$,*

$$\Pr_{C\sim\mathcal{C}_{\mathcal{A}}}\left(C^\dagger Z(w)C \text{ is a } Z\text{-type Pauli}\right) \geq \frac{1}{3^{|w|}}\left(\frac{2}{5}\right)^{|w|d}.$$

*Proof.* Let $w \in \{0,1\}^n$. We have that

$$\begin{aligned}&\Pr_{C\sim\mathcal{C}_{\mathcal{A}}}\left(C^\dagger Z(w)C \text{ is a } Z\text{-type Pauli}\right) \\ =&\sum_{j=0}^{n}\frac{1}{3^j}\Pr_{C\sim\mathcal{C}_{\mathcal{A}}}\left(C^\dagger Z(w)C \text{ has weight } j\right) \\ \geq&\frac{1}{3^{|w|}}\Pr_{C\sim\mathcal{C}_{\mathcal{A}}}\left(C^\dagger Z(w)C \text{ has weight } |w|\right).\end{aligned}$$

We proceed by induction on $d$ to show that

$$\Pr_{C\sim\mathcal{C}_{\mathcal{A}}}\left(C^\dagger Z(w)C \text{ has weight } |w|\right) \geq \left(\frac{2}{5}\right)^{|w|d}.$$

For the base case, we consider $C \sim \mathcal{C}_{\mathcal{A}}$ with $d = 1$. Let $P = Z(w)$ such that $P = \bigotimes_{j=1}^n P^{(j)}$, and let $Q = C^\dagger Z(w)C$ such that $Q = \pm\bigotimes_{j=1}^n Q^{(j)}$ and $Q^{(j)} \in \{I, X, Y, Z\}$ for every $j \in [n]$. Let $i \in [n]$ such that $P^{(i)} \neq I$. If no gate in $C$ acts on qubit $i$, then $Q_i = P_i \neq I$. Now suppose qubit $i$ is acted on by a unique 2-qubit gate that acts on qubits $i$ and $j$, for some

$j \in [n] \setminus \{i\}$. If $P_j \neq I$, then the probability that $Q_i \neq I$ and $Q_j \neq I$ is $\frac{9}{15} \geq \frac{2}{5}$. If $P_j = I$, then the probability that exactly one of $Q_i \neq I$ or $Q_j \neq I$ is $\frac{6}{15} = \frac{2}{5}$. Therefore, when $d = 1$, $\Pr_{C \sim \mathcal{C}_\mathcal{A}}(C^\dagger Z(w) C \text{ has weight } |w|) \geq \left(\frac{2}{5}\right)^{|w|}$. Now suppose $d \geq 2$. For $C \sim \mathcal{C}_\mathcal{A}$, we can decompose $C$ into layers $C = C_d \cdots C_1$. Let $P = C_2^\dagger \cdots C_d^\dagger Z(w) C_d \cdots C_2$. Then

$$\begin{aligned}
&\Pr_{C \sim \mathcal{C}_\mathcal{A}} \left(C^\dagger Z(w) C \text{ has weight } |w|\right) \\
&\geq \Pr_{C \sim \mathcal{C}_\mathcal{A}} \left(C_1^\dagger P C_1 \text{ has weight } |w| \middle| P \text{ has weight } |w|\right) \Pr_{C \sim \mathcal{C}_\mathcal{A}} \left(P \text{ has weight } |w|\right).
\end{aligned}$$

By the inductive hypothesis,

$$\Pr_{C \sim \mathcal{C}_\mathcal{A}} \left(P \text{ has weight } |w|\right) \geq \left(\frac{2}{5}\right)^{|w|(d-1)}.$$

By the same argument as in the base case,

$$\Pr_{C \sim \mathcal{C}_\mathcal{A}} \left(C_1^\dagger P C_1 \text{ has weight } |w| \middle| P \text{ has weight } |w|\right) \geq \left(\frac{2}{5}\right)^{|w|}.$$

□

**Theorem 2.12.** *For every $n$-qubit-depth-$d$ circuit architecture $\mathcal{A}$,*

$$\mathrm{Coll}(\mathcal{H}_\mathcal{A}) \geq \frac{1}{2^n} \left(1 + \frac{1}{3}\left(\frac{2}{5}\right)^d\right)^n.$$

*Proof.* Using Lemma A.1, we get that

$$\mathrm{Coll}(\mathcal{H}_\mathcal{A}) = \frac{1}{2^n} \sum_{w \in \{0,1\}^n} \mathrm{Tr}\left( (Z(w) \otimes Z(w)) \mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ (V \otimes V) |0^{2n}\rangle\langle 0^{2n}| (V^\dagger \otimes V^\dagger) \right] \right).$$

Since each random 2-qubit gate is drawn independently, by applying the exact unitary 2-design property of $\mathcal{U}(\mathbf{C}_2)$ inductively to each random 2-qubit gate, we get that

$$\mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ (V \otimes V) |0^{2n}\rangle\langle 0^{2n}| (V^\dagger \otimes V^\dagger) \right] = \mathop{\mathbb{E}}_{C \sim \mathcal{C}_\mathcal{A}} \left[ (C \otimes C) |0^{2n}\rangle\langle 0^{2n}| (C^\dagger \otimes C^\dagger) \right].$$

Thus, by Lemma 2.12,

$$\begin{aligned}
\mathrm{Coll}(\mathcal{H}_\mathcal{A}) &= \frac{1}{2^n} \sum_{w \in \{0,1\}^n} \mathop{\mathbb{E}}_{C \sim \mathcal{C}_\mathcal{A}} \left[ \langle 0^{2n}| (C^\dagger \otimes C^\dagger)(Z(w) \otimes Z(w))(C \otimes C) |0^{2n}\rangle \right] \\
&= \frac{1}{2^n} \sum_{w \in \{0,1\}^n} \Pr_{C \sim \mathcal{C}_\mathcal{A}} \left( C^\dagger Z(w) C \text{ is a } Z\text{-type Pauli} \right) \\
&\geq \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} \frac{1}{3^k} \left(\frac{2}{5}\right)^{kd} \\
&= \frac{1}{2^n} \left(1 + \frac{1}{3}\left(\frac{2}{5}\right)^d\right)^n.
\end{aligned}$$

□

We remark that Theorem 2.12 makes no assumption about any special structures in the circuit architecture, hence it serves as a general lower bound for all circuit architectures. Theorem 2.11 and Theorem 2.12 together suggest that the phase transition for anti-concentration occurs precisely at depth $\Theta(\log n)$ for the 1D architecture.

**Corollary 2.5.** *For the 1D architecture,* $\mathrm{Coll}\left(\mathcal{H}^{path}_{n,\ln n}\right) > \frac{\omega(1)}{2^n}$ *and* $\mathrm{Coll}\left(\mathcal{H}^{path}_{n,5(\ln n)00+1}\right) \leq \frac{O(1)}{2^n}$.

*Proof.* Substitute $d = 5(\ln n) + 1$ into Theorem 2.11 and $d = \ln n$ into Theorem 2.12. □

We can extract another interesting corollary from Lemma 2.12 and the proof of Theorem 2.12.

**Corollary 2.6.** *For every $n$-qubit-depth-$d$ circuit architecture $\mathcal{A}$, and for every $n$-qubit Pauli operator $\sigma_p \in \{I, X, Y, Z\}^{\otimes n}$,*

$$\mathop{\mathbb{E}}_{V\sim\mathcal{H}_{\mathcal{A}}}\left[\langle 0^n|V^\dagger\sigma_p V|0^n\rangle^2\right] \geq e^{-O(|\sigma_p|d)}.$$

*Proof.* By the gate-wise Haar unitary invariance property, there exists a $Z$-type Pauli operator $Z(w)$ with $w \in \{0,1\}^n$ and $|w| = |\sigma_p|$ such that

$$\mathop{\mathbb{E}}_{V\sim\mathcal{H}_{\mathcal{A}}}\left[\langle 0^n|V^\dagger\sigma_p V|0^n\rangle^2\right] = \mathop{\mathbb{E}}_{V\sim\mathcal{H}_{\mathcal{A}}}\left[\langle 0^n|V^\dagger Z(w) V|0^n\rangle^2\right].$$

Then the proof of Theorem 2.12 and Lemma 2.12 imply that

$$\mathop{\mathbb{E}}_{V\sim\mathcal{H}_{\mathcal{A}}}\left[\langle 0^n|V^\dagger Z(w) V|0^n\rangle^2\right] \geq e^{-O(|w|d)}.$$

□

Do we have the tools to derive an upper bound for $\mathbb{E}_{V\sim\mathcal{H}_{\mathcal{A}}}\left[\langle 0^n|V^\dagger\sigma_p V|0^n\rangle^2\right]$? In a recent paper [LOB+21], the authors studied this expression for the 1D architecture, and they are able to prove that

$$\mathop{\mathbb{E}}_{V\sim\mathcal{H}^{\mathrm{path}}_{n,d}}\left[\langle 0^n|V^\dagger\sigma_p V|0^n\rangle^2\right] \leq e^{-\Omega(d)} + \frac{1}{2^n}$$

for every $\sigma_p \in \{I, X, Y, Z\}^{\otimes n} \setminus \{I^{\otimes n}\}$ with $|\sigma_p| \leq 3$ by adapting the trajectory counting technique from the proof of Theorem 2.11. They further conjectured that for every $\sigma_p \in \{I, X, Y, Z\}^{\otimes n} \setminus \{I^{\otimes n}\}$,

$$\mathop{\mathbb{E}}_{V\sim\mathcal{H}^{\mathrm{path}}_{n,d}}\left[\langle 0^n|V^\dagger\sigma_p V|0^n\rangle^2\right] \leq e^{-\Omega(|\sigma_p|+d)} + \frac{1}{2^n}.$$

We prove this conjecture here.

**Theorem 2.13.** *Let $\sigma_p \in \{I, X, Y, Z\}^{\otimes n} \setminus \{I^{\otimes n}\}$. Let $r$ be the number of nearest neighbour pairs of qubits on which $\sigma_p$ acts non-trivially. Let $n' = \min(n, 2rd)$. Then for every $d \geq 10$,*

$$\mathop{\mathbb{E}}_{V\sim\mathcal{H}^{path}_{n,d}}\left[\langle 0^n|V\sigma_p V^\dagger|0^n\rangle^2\right] \leq e^{-\Omega(|\sigma_p|+d)} + \frac{1}{2^{n'}}.$$

*Proof.* By the unitary invariance property of the Haar measure, we can assume WLOG that $\sigma_p \in \{I, Z\}^{\otimes n} \setminus \{I^{\otimes n}\}$. We first define some notations. Let $|\sigma_p\rangle$ denote the vectorized representation of $\sigma_p \otimes \sigma_p$. Let $P_{\text{odd}}$ and $P_{\text{even}}$ denote $P^{(2)}_{\text{odd}}$ and $P^{(2)}_{\text{even}}$ respectively. Let $d \geq 10$. We first consider the case where $d$ is odd. Let $k = \frac{d-1}{2}$. Recall the $t$-th moment operator of $\mathcal{H}^{\text{path}}_{n,d}$ (see (2.7)). Observe that,

$$\begin{aligned}
&\left|\langle 0^{4n}| \left(P_{\text{odd}}P_{\text{even}}P_{\text{odd}}\right)^k - P_N^{(2)}|\sigma_p\rangle\right| \\
=&\left|\langle 0^{4n}| \left(P_{\text{odd}}P_{\text{even}}P_{\text{odd}}\right)^{\lceil \frac{k}{2} \rceil} \left(\left(P_{\text{odd}}P_{\text{even}}P_{\text{odd}}\right)^{\lfloor \frac{k}{2} \rfloor} - P_N^{(2)}\right) P_{\text{odd}}|\sigma_p\rangle\right| \\
\leq&\|\langle 0^{4n}| \left(P_{\text{odd}}P_{\text{even}}P_{\text{odd}}\right)^{\lceil \frac{k}{2} \rceil}\|_\infty \cdot \|\left(P_{\text{odd}}P_{\text{even}}P_{\text{odd}}\right)^{\lfloor \frac{k}{2} \rfloor} - P_N^{(2)}\|_\infty \cdot \|P_{\text{odd}}|\sigma_p\rangle\|_\infty \\
=&\|\left(P_{\text{odd}}P_{\text{even}}P_{\text{odd}}\right)^{\lfloor \frac{k}{2} \rfloor} - P_N^{(2)}\|_\infty \cdot \sqrt{\langle 0^{4n}| \left(P_{\text{odd}}P_{\text{even}}P_{\text{odd}}\right)^{2\lceil \frac{k}{2} \rceil} |0^{4n}\rangle} \cdot \sqrt{\langle \sigma_p|P_{\text{odd}}|\sigma_p\rangle}.
\end{aligned}$$

Combining Lemma 2.8 and Theorem 2.6, we get

$$\left\|\left(P_{\text{odd}}P_{\text{even}}P_{\text{odd}}\right)^{\lfloor \frac{k}{2} \rfloor} - P_N^{(2)}\right\|_\infty \leq \left(\frac{20}{21}\right)^{\lfloor \frac{k}{2} \rfloor}.$$

By Lemma 2.2,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{U\sim\mu^4_{\text{Haar}}} \left[(U \otimes U)(Z \otimes Z \otimes Z \otimes Z)(U^\dagger \otimes U^\dagger)\right] \\
=&\mathop{\mathbb{E}}_{U\sim\mu^4_{\text{Haar}}} \left[(U \otimes U)(Z \otimes I \otimes Z \otimes I)(U^\dagger \otimes U^\dagger)\right] \\
=&\mathop{\mathbb{E}}_{U\sim\mu^4_{\text{Haar}}} \left[(U \otimes U)(I \otimes Z \otimes I \otimes Z)(U^\dagger \otimes U^\dagger)\right] \\
=&\frac{1}{15}\left(4S - I \otimes I \otimes I \otimes I\right)
\end{aligned}$$

where $S$ is the swap gate defined by $S|\psi\rangle|\phi\rangle = |\phi\rangle|\psi\rangle$. We have[1]

$$\langle ZZZZ|S\rangle = \text{Tr}\left((Z \otimes Z \otimes Z \otimes Z)S\right) = 4.$$

Similarly,

$$\langle ZIZI|S\rangle = \langle IZIZ|S\rangle = 4.$$

Thus,

$$\langle ZZZZ|P_N^{(2)}|ZZZZ\rangle = \langle ZIZI|P_N^{(2)}|ZIZI\rangle = \langle IZIZ|P_N^{(2)}|IZIZ\rangle = \frac{16}{15}.$$

Therefore,

$$\langle \sigma_p|P_{\text{odd}}|\sigma_p\rangle = \left(\frac{16}{15}\right)^r 16^{\frac{n}{2}-r} = 4^n \left(\frac{1}{15}\right)^r.$$

By Theorem 2.11,

$$\langle 0^{4n}| \left(P_{\text{odd}}P_{\text{even}}P_{\text{odd}}\right)^{2\lceil \frac{k}{2} \rceil} |0^{4n}\rangle \leq \frac{2}{4^n} \exp\left(\left(\frac{4}{5}\right)^{d-1} n\right).$$

[1]Here, we use a shorthand notation $ZZZZ = Z \otimes Z \otimes Z \otimes Z$.

Therefore,

$$\langle 0^{4n}| \left(P_{\text{odd}} P_{\text{even}} P_{\text{odd}}\right)^k |\sigma_p\rangle \leq \sqrt{2} \left(\frac{1}{15}\right)^{\frac{r}{2}} \exp\left(\left(\frac{4}{5}\right)^{d-1} \frac{n}{2}\right) \left(\frac{20}{21}\right)^{\lfloor \frac{k}{2} \rfloor} + \langle 0^{4n}| P_N^{(2)} |\sigma_p\rangle.$$

Running the same argument again with $\left(P_{\text{odd}} P_{\text{even}}\right)^k$ for even-depth circuits ($d$ even, $k = \frac{d}{2}$), we get that

$$\langle 0^{4n}| \left(P_{\text{odd}} P_{\text{even}}\right)^k |\sigma_p\rangle \leq \sqrt{2} \left(\frac{1}{15}\right)^{\frac{r}{2}} \exp\left(\left(\frac{4}{5}\right)^{d-1} \frac{n}{2}\right) \left(\sqrt{\frac{20}{21}}\right)^{\lfloor \frac{k}{2} \rfloor} + \langle 0^{4n}| P_N^{(2)} |\sigma_p\rangle.$$

By Corollary 2.3, $\langle 0^{4n}| P_N^{(2)} |\sigma_p\rangle = \frac{1}{2^n+1}$. If $n \leq 2rd$, then

$$\begin{aligned}
\mathop{\mathbb{E}}_{V \sim \mathcal{H}_{n,d}^{\text{path}}} \left[\langle 0^n | V \sigma_p V^\dagger | 0^n \rangle^2\right] &\leq \sqrt{2} \left(\frac{\left(\exp\left(\left(\frac{4}{5}\right)^{d-1} d\right)\right)^2}{15}\right)^{\frac{r}{2}} \left(\sqrt{\frac{20}{21}}\right)^{\frac{d-1}{4}} + \frac{1}{2^n} \\
&\leq \sqrt{2} \left(0.98\right)^{\frac{r}{2}} \left(\sqrt{\frac{20}{21}}\right)^{\frac{d-1}{4}} + \frac{1}{2^n}
\end{aligned}$$

for $d \geq 10$. Now suppose $n > 2rd$. Suppose $\sigma_p = \otimes_{i=1}^n \sigma_p^{(i)}$. By the lightcone size constraint of 1D circuits, there exist qubits that lie outside the backward lightcone of every other qubit $i$ such that $\sigma_p^{(i)} \neq I$, and we can throw away those qubits. Thus, there exists $\sigma_p' \in \{I, Z\}^{\otimes 2rd} \setminus \{I^{\otimes 2rd}\}$ with $|\sigma_p'| = |\sigma_p|$ such that

$$\begin{aligned}
\mathop{\mathbb{E}}_{V \sim \mathcal{H}_{n,d}^{\text{path}}} \left[\langle 0^n | V \sigma_p V^\dagger | 0^n \rangle^2\right] &= \mathop{\mathbb{E}}_{V \sim \mathcal{H}_{2rd,d}^{\text{path}}} \left[\langle 0^{2rd} | V \sigma_p' V^\dagger | 0^{2rd} \rangle^2\right] \\
&\leq \sqrt{2} \left(0.98\right)^{\frac{r}{2}} \left(\sqrt{\frac{20}{21}}\right)^{\frac{d-1}{4}} + \frac{1}{2^{2rd}}.
\end{aligned}$$

□

We suspect that the upper bound established in Theorem 2.13 is not tight. To reproduce the phase transition phenomenon near $d = \Theta(\log n)$ established by Theorem 2.11 using the characterization

$$\text{Coll}(\mathcal{H}_{n,d}^{\text{path}}) = \frac{1}{2^n} \sum_{w \in \{0,1\}^n} \mathop{\mathbb{E}}_{V \sim \mathcal{H}_{n,d}^{\text{path}}} \left[\langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2\right],$$

we need an upper bound like

$$\mathop{\mathbb{E}}_{V \sim \mathcal{H}_{n,d}^{\text{path}}} \left[\langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2\right] \leq e^{-\Omega(|w|d)} + \frac{1}{2^n}$$

for every $w \in \{0,1\}^n \setminus \{0^n\}$. We record this updated conjecture for future work.

**Conjecture 2.1.** *Let $\sigma_p \in \{I, X, Y, Z\}^{\otimes n} \setminus \{I^{\otimes n}\}$. Let $r$ be the number of nearest neighbour pairs of qubits on which $\sigma_p$ acts non-trivially. Let $n' = \min(n, 2rd)$. Then,*

$$\mathop{\mathbb{E}}_{V \sim \mathcal{H}_{n,d}^{path}} \left[ \langle 0^n | V \sigma_p V^\dagger | 0^n \rangle^2 \right] \leq e^{-\Omega(|\sigma_p| d)} + \frac{1}{2^{n'}}.$$

# Chapter 3

# Applications in Random Circuit Sampling

Quantum supremacy seeks to perform on a quantum computer a well-defined computational task whose classical computational cost exceeds the limits of feasible classical computation [Pre11, AC16]. The challenge to claim quantum supremacy is both experimental and theoretical. On the one hand, a successful quantum supremacy experiment requires maintaining and controlling complex quantum systems involving enough qubits for long enough coherence times [AAB+19], as otherwise, the resulting quantum dynamics may fall within the realm of state-of-the-art classical simulation techniques [MFIB18, ZSW20]. On the other hand, one needs to provide convincing complexity-theoretic evidence for the classical intractability of the problem that the quantum computer is designed to solve [BJS11, AA11, BMS16, AC16]. The obvious proposal is to "simply" build a fault-tolerant quantum computer to factor large integers using Shor's algorithm [Sho99]. Although the factoring proposal satisfies the theoretical requirement to a large extent hence sufficient for demonstrating quantum supremacy, such a feat may still be decades away given the current progress of quantum computing technologies [SR20]. One crucial aspect of quantum supremacy is that it is unnecessary for the quantum computer to solve a practically useful problem. Hence, to help minimize experimental difficulties, it becomes instrumental to search for computational problems, even contrived ones, that are intrinsically easy to solve quantum mechanically, as long as complexity-theoretic evidence can be found to support their classical hardness. For these reasons, researchers have identified random circuit sampling as a promising candidate suitable for the demonstration of quantum supremacy [BIS+18, AAB+19].

## 3.1 The RCS Supremacy Conjecture

Informally speaking, random circuit sampling (RCS) is a computational problem whose input is a random quantum circuit, and the task is to sample a bit string drawn from some distribution close to the quantum circuit's output distribution. The built-in error allowance in the problem is natural because even a fault-tolerant quantum computer can only perform RCS up to some small error, hence it will also be unfair to require a classical simulator to sample from a quantum circuit's output distribution exactly. From the experimental

perspective, RCS is straightforward to execute on noisy quantum computers without error correction such that the quality of the samples will be determined by the fidelity characteristics of the device [MFIB18, BIS+18, AAB+19]. Meanwhile, theoretical investigations into the RCS problem have advanced our understanding of its computational complexity [BFNV18, Mov18]. At the core of this line of work lies the RCS supremacy conjecture which asserts that no efficient classical algorithm can exist to perform RCS in polynomial time for some small but reasonable error margin. In this section, we give a high-level overview of the RCS supremacy conjecture and the proof strategy initially proposed by Aaronson [AA11]. For discussions on the same topic with more mathematical details, see [BFNV18, KMM21]. For formal definitions of complexity classes that will appear such as #**P** and the polynomial hierarchy, see [AB09].

Before stating the RCS supremacy conjecture, we first need to get familiar with the various notions of classical simulation of quantum circuits that will take part in the discussion. For example, one may be interested in understanding the computational complexity of the additive error worst case probability estimation problem. Recall our definition of circuit architectures from Chapter 1 (see Definition 1.5).

**Problem 3.1** (Additive Error Worst Case Probability Estimation)**.** For some $n$-qubit circuit architecture $\mathcal{A}$ and some $\varepsilon \geq 0$, on input an arbitrary quantum circuit $C$ with the architecture $\mathcal{A}$, output a value $p$ satisfying $|p - |\langle 0^n|C|0^n\rangle|^2| \leq \varepsilon$.

Intuitively, Problem 3.1 seems computationally hard since when $\varepsilon$ is sufficiently small, this problem is even beyond the capabilities of efficient quantum computation. Indeed, it is known that this problem is #**P**-hard for certain circuit architectures.

**Theorem 3.1** ([Aar11, KMM21])**.** *There exists a (uniform) family of $n$-qubit-$s$-gate circuit architectures $\mathcal{A}_{n,s}$ such that the additive error worst case probability estimation problem over $\mathcal{A}_{n,s}$ is #**P**-hard for $\varepsilon < 1/2^{s^c}$ for every constant $c > 0$.*

On the contrary, the additive error average case sampling problem seems less demanding and is modelled after the capabilities of fault-tolerant quantum computers. Recall that for an $n$-qubit quantum circuit $C$, we have defined $q_C(x) = |\langle x|C|0^n\rangle|^2$ for every $x \in \{0,1\}^n$. Also recall that we use the notation $\mathcal{H}_{\mathcal{A}}$ to denote the distribution of Haar random quantum circuits with the architecture $\mathcal{A}$.

**Problem 3.2** (Additive Error Average Case Sampling)**.** For some $n$-qubit circuit architecture $\mathcal{A}$, $\delta \in (0,1)$, and $\varepsilon \geq 0$, on input a random quantum circuit $C \sim \mathcal{H}_{\mathcal{A}}$, output a sample $z \in \{0,1\}^n$ drawn according to some distribution $\tilde{q}$ such that $\sum_{x\in\{0,1\}^n} |\tilde{q}(x) - q_C(x)| \leq \varepsilon$ with probability at least $1 - \delta$ over the choice of the random circuit $C$.

We note that Problem 3.2 can be taken as the formal definition of the RCS problem. The RCS supremacy conjecture asserts that even Problem 3.2 is intractable for certain circuit architectures.

**Conjecture 3.1** (RCS Supremacy Conjecture)**.** *There exists a (uniform) family of $n$-qubit circuit architectures $\mathcal{A}_n$ such that for some $\varepsilon = 1/\mathrm{poly}(n)$ and some constant $\delta$, if there exists a classical polynomial-time algorithm solving the additive error average case sampling problem for $\mathcal{A}_n$, $\varepsilon$, and $\delta$, then the polynomial hierarchy collapses.*

To describe the proof strategy proposed by Aaronson [AA11], we need to define another variant of the classical simulation problem.

**Problem 3.3** (Additive Error Average Case Probability Estimation)**.** For some $n$-qubit circuit architecture $\mathcal{A}$, $\delta \in (0,1)$, and $\varepsilon \geq 0$, on input a random quantum circuit $C \sim \mathcal{H}_{\mathcal{A}}$, output a value $p$ satisfying $|p - |\langle 0^n|C|0^n\rangle|^2| \leq \varepsilon$ with probability at least $1-\delta$ over the choice of the random circuit $C$.

The proof strategy involves a three stage reduction from Problem 3.2 to Problem 3.1 via Problem 3.3. We first choose a (uniform) family of $n$-qubit architectures $\mathcal{A}$ such that $\mathcal{H}_{\mathcal{A}}$ has the hiding property, the collision probability of $\mathcal{H}_{\mathcal{A}}$ satisfies

$$\mathrm{Coll}(\mathcal{H}_{\mathcal{A}}) = 2^n \mathop{\mathbb{E}}_{C\sim\mathcal{H}_{\mathcal{A}}} \left[|\langle 0^n|C|0^n\rangle|^4\right] \leq \frac{O(1)}{2^n}, \tag{3.1}$$

and that Problem 3.1 is $\#\mathbf{P}$-hard for $\mathcal{A}$. For instance, we can consider the $\mathrm{poly}(n)$-depth 1D architecture $\mathcal{A}^{\mathrm{path}}_{n,\mathrm{poly}(n)}$. We will ignore $\delta$ as it is straightforward to manage and highlight how $\varepsilon$ evolves throughout the argument. For the first reduction step, given a classical randomized polynomial time algorithm $A$ solving Problem 3.2 with $\varepsilon_1 = 1/\mathrm{poly}(n)$, the authors of [AA11] and [BMS16] showed how to use Stockmeyer's approximate counting theorem [Sto85] to construct from $A$ an algorithm in the polynomial hierarchy[1] solving Problem 3.3 with additive error

$$\varepsilon_2 \leq O\left(\frac{\varepsilon_1}{2^n} + \frac{|\langle 0^n|C|0^n\rangle|^2}{\mathrm{poly}(n)}\right).$$

For the second step, by (3.1), we can use Chebyshev's inequality[2] to show that

$$\Pr_{C\sim\mathcal{H}_{\mathcal{A}}}\left(|\langle 0^n|C|0^n\rangle|^2 \leq \frac{O(1)}{2^n}\right) \geq \Omega(1).$$

Thus, for at least some constant probability over the choice of $C \sim \mathcal{H}_{\mathcal{A}}$,

$$\varepsilon_2 \leq \frac{O(1)}{\mathrm{poly}(n)2^n}.$$

The final step involves a worst to average case reduction inspired by the randomized self-reducibility technique first discovered for showing the average case $\#\mathbf{P}$-hardness of computing the permanents of matrices [Lip91]. More specifically, the authors of [KMM21] and [BFLL21] showed how to construct, from an algorithm solving Problem 3.3 with additive error $\varepsilon$, an algorithm solving Problem 3.1 with error $\varepsilon' = 2^{O(s\log s)}\varepsilon$ where $s$ is the number of gates in the circuit. If we substitute $\varepsilon_2$ into the theorems of [KMM21] and [BFLL21], then we get an algorithm in the polynomial hierarchy solving Problem 3.1 with additive error

$$\varepsilon_3 = O\left(\frac{2^{O(s\log s)}}{\mathrm{poly}(n)2^n}\right).$$

[1] More formally, an $\mathbf{FBPP}^{\mathbf{NP}^A}$ machine.

[2] We use formally a *concentration* inequality as opposed to the anti-concentration inequalities appearing originally in [AA11] and [BMS16]; the collision probability upper bound requirement is the same.

In order to invoke Theorem 3.1, we need to reduce the error blow up in the third step from $2^{O(s \log s)}$ to roughly $2^{O(n)}$, and it is still an open problem whether this can be achieved. If it can be done, then Theorem 3.1 together with Toda's theorem [Tod91], which states that the polynomial hierarchy is contained in $\mathbf{P}^{\#\mathbf{P}}$, imply that the entire polynomial hierarchy is contained in some finite level. In other words, the polynomial hierarchy collapses, and it is believed to be very unlikely. For prospects and known barriers to closing the robustness gap, see discussions in [BFLL21].

We remark that the known reductions also do not imply the classical hardness of solving Problem 3.2 with $\varepsilon_1 = 0$ since the error introduced by Stockmeyer's theorem is inherent in this proof strategy. However, assuming the existence of an efficient classical algorithm solving Problem 3.3 with $\varepsilon_2 = 0$ is sufficient for invoking Theorem 3.1 via the known worst to average case reductions, thereby collapsing the polynomial hierarchy.

**Theorem 3.2** ([BFNV18, Mov18])**.** *There exists a (uniform) family of $n$-qubit circuit architectures $\mathcal{A}_n$ and a constant $\delta > 0$ such that if there exists an efficient classical algorithm solving Problem 3.3 for $\mathcal{A}_n$ with failure probability $\delta$ and error $\varepsilon = 0$, then the polynomial hierarchy collapses.*

Theoretical studies into the RCS supremacy conjecture are initiated by the real-world pursuit of quantum supremacy, and they have for sure provided important guidance to experimental designs. Practical implications aside, the RCS supremacy conjecture also possesses inherent complexity-theoretic values in the direction of separating efficient quantum computation from efficient classical computation. Indeed, while not as glorious as unconditionally proving $\mathbf{BQP} \neq \mathbf{P}$ and not even about decision problems, Theorem 3.2 presents some of the strongest complexity-theoretic evidence known to date in favour of the power of efficient quantum computers over their classical counterparts.

This concludes our coverage of the RCS supremacy conjecture. While the RCS supremacy conjecture may one day be proven, there remains at least one more interesting theoretical question related to RCS experiments.

## 3.2 The Linear Cross-Entropy Benchmark

In a prototypical RCS experiment, a random quantum circuit is drawn from a fixed $n$-qubit circuit architecture and fed to a purported quantum computer $k$ times to collect $k$ output bit strings $z_1, \ldots, z_k \in \{0,1\}^n$. At this point, an important issue yet to be addressed is, by examining these $k$ bit strings, how can we verify whether the quantum computer has solved RCS or not? Since there are $2^n$ possible outputs, and if our quantum device is indeed working properly, the probability of observing each $z \in \{0,1\}^n$ will be in the order of $\frac{1}{2^n}$, so in reality, we will never observe the same string twice if we only collect $\mathrm{poly}(n)$ many samples. How do we distinguish a set of $k$ bit strings drawn according to the random quantum circuit's output distribution from a set of $k$ uniformly random bit strings? In Google's quantum supremacy proposal, they adopted a statistical test called the linear cross-entropy benchmark to address the verification problem [AAB+19]. For two probability distributions $p$ and $q$ over $\{0,1\}^n$,

the cross-entropy of $q$ relative to $p$ is given by

$$H(p,q) = \mathop{\mathbb{E}}_{z\sim p}[-\log q(z)] = \sum_{z\in\{0,1\}^n} p(z)\log\left(\frac{1}{q(z)}\right).$$

Based on this, the Google team defined linear cross-entropy by simply replacing the $\log\left(\frac{1}{q(z)}\right)$ term in the above expression by $q(z)$ [AAB+19]. More formally, the (expected) linear cross-entropy benchmark for random quantum circuits is defined as follows:

**Definition 3.1** ((Expected) Linear Cross-Entropy Benchmark [AAB+19])**.** Let $\mathcal{D}$ be an $n$-qubit random unitary distribution. Let $A$ be an algorithm which takes as input $U \sim \mathcal{D}$ and outputs a string $z \in \{0,1\}^n$, and let $A_U$ denote the output distribution of $A$ on input $U$. The (expected) linear cross-entropy benchmark score of $A$ with respect to $\mathcal{D}$ is

$$\mathrm{XEB}_{\mathcal{D}}(A) = \mathop{\mathbb{E}}_{U\sim\mathcal{D},z\sim A_U}\left[|\langle z|U|0^n\rangle|^2\right] = \mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[\sum_{z\in\{0,1\}^n} A_U(z)q_U(z)\right].$$

On the one extreme, the XEB score of the trivial algorithm, which ignores the input and outputs a string drawn from $\mathcal{U}(\{0,1\}^n)$, is $\frac{1}{2^n}$ for every $\mathcal{D}$. On the other extreme, we will see that the score of the quantum simulation algorithm, which exactly simulates the input circuit, will be roughly $\frac{2}{2^n}$ for deep random quantum circuits. The Google proposal makes explicitly the strong assumption that for deep random quantum circuits, no efficient classical algorithm can achieve an XEB score higher than $\frac{1}{2^n}$, essentially conjecturing that the trivial algorithm is optimal [BIS+18]. Under this strong assumption, even if a purported quantum computer can only achieve a score of $\frac{1+\varepsilon}{2^n}$ for some small $\varepsilon > 0$, that computer must have accomplished the feat quantum mechanically, thus certifying the "quantumness" of the device. It is worth noting that the quantum simulation algorithm is not a maximizer of the XEB score since an exponential time classical algorithm can find the $z^* \in \{0,1\}^n$ with the highest output probability[3] and output $z^*$.

In a real experiment, the XEB score is approximated using a Monte-Carlo estimator. Given an input circuit $V$, the device is executed $k$ times independently on the same input $V$ to collect $k$ samples $z_1,\ldots,z_k \in \{0,1\}^n$. We then compute the sample mean $\frac{1}{k}\sum_{i=1}^k |\langle z_i|V|0^n\rangle|^2$ where the output probabilities $|\langle z_i|V|0^n\rangle|^2$ are computed using exponential time classical simulation. It is clear that the sample mean is an unbiased estimator of the expectation. While this approach remains feasible for verifying 40-50 qubit experiments if we delegate the classical simulation to a supercomputer, heuristic extrapolation arguments are needed when the number of qubits is increased to the supremacy regime where classical simulation becomes prohibitive [AAB+19].

It is important to note that, although the linear cross-entropy benchmark is intended for the verification of RCS, they are merely two related but different computational problems. Even if the RCS supremacy conjecture is true, it does not rule out the possibility that efficient classical algorithms directly targeting the benchmark could exist. We devote the rest of this work to developing an understanding of the computational complexity of the linear cross-entropy benchmark, especially on the classical complexity of attaining non-trivial XEB scores in relation to Google's strong conjecture.

[3]The maximum value depends on $\mathcal{D}$, and for $\mathcal{D} = \mu_{\mathrm{Haar}}^N$, it is known to be $O(n)/2^n$ [Kre21].

## 3.3 The Quantum Simulation Algorithm

We use $QS$ to denote the quantum simulation algorithm which simply executes the input circuit and measures all qubits in the computational basis, and it models the behaviour of an ideal, noise-less quantum computer. By Definition 3.1, for every $n$-qubit random unitary distribution $\mathcal{D}$,

$$\mathrm{XEB}_{\mathcal{D}}(QS) = \mathop{\mathbb{E}}_{U\sim\mathcal{D},z\sim q_U}\left[|\langle z|U|0^n\rangle|^2\right] = \mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[\sum_{z\in\{0,1\}^n}|\langle z|U|0^n\rangle|^4\right] = \mathrm{Coll}(\mathcal{D}).$$

Therefore, analysing the performance of the quantum simulation algorithm coincides exactly with analysing the collision probability, which is the topic of section 2.3. We obtain the following theorem by reinterpreting the results proven in section 2.3.

**Theorem 3.3.**

*(a)*

$$\mathrm{XEB}_{\mu^N_{Haar}}(QS) = \frac{2}{2^n+1};$$

*(b) For every $n$-qubit-depth-$d$ circuit architecture $\mathcal{A}$,*

$$\mathrm{XEB}_{\mathcal{H}_{\mathcal{A}}}(QS) \geq \frac{1}{2^n}\left(1+\frac{1}{3}\left(\frac{2}{5}\right)^d\right)^n;$$

*(c) For the 1D architecture,*

$$\mathrm{XEB}_{\mathcal{H}^{path}_{n,d}}(QS) \leq \frac{2}{2^n}\exp\left(\left(\frac{4}{5}\right)^{d-1}n\right).$$

In particular, the general XEB score lower bound highlights from a theoretical perspective the importance of choosing large circuit depths in RCS experiments. While the $\frac{2}{2^n}$ figure is widely cited as the "ideal" score, it is crucial to note that this estimate is only accurate for sufficiently deep circuits. Therefore, in future RCS experiments, it is necessary to combine increases in the qubit count with increases in the circuit depth.

## 3.4 The BCG Algorithm

The algorithm of Barak, Chou, and Gao is a classical algorithm designed for spoofing the Linear Cross-Entropy Benchmark [BCG20]. Recall the definition of lightcones from Chapter 1 (see Definition 1.6). On input an $n$-qubit quantum circuit $V$, the BCG algorithm first selects a set $I$ of $m = \lfloor n/L \rfloor$ qubits with mutually disjoint backward lightcones, where $L$ is the lightcone size of $V$. Note that the choice of $I$ only depends on the architecture but not the specific circuit instantiation. The algorithm then computes the marginal output probabilities of each qubit in $I$. To construct an output string $z \in \{0,1\}^n$, for every bit $z_i$,

$i \in [n]$, if $i \in I$, then the algorithm samples $z_i$ according to the marginal output distribution of qubit $i$; otherwise, $z_i$ is sampled uniformly at random.

The BCG algorithm is well-defined for arbitrary random unitary distributions, and its time complexity is $\text{poly}(n, 2^L)$ since computing the marginal output probabilities of a qubit can be done in $O(2^L)$ time (recall section 1.6). Unfortunately, the BCG algorithm is only efficient for circuit architectures with a small lightcone size since $\text{poly}(n, 2^L)$ is polynomial in $n$ only if $L$ is at most $O(\log n)$. Therefore, the BCG algorithm is not in the position to refute Google's strong conjecture on the linear cross-entropy benchmark because the algorithm is inefficient for deep random quantum circuits with $\text{poly}(n)$ lightcone sizes. Nevertheless, we will show that the BCG algorithm does imply that the deep circuit depth assumption in Google's strong conjecture is necessary. We first show a lower bound for the XEB score of the BCG algorithm by reusing some of the tools developed in section 2.3. The following proof is based on the same ideas as in the original proof appearing in [BCG20] but is expressed in terms of standard mathematical notations.

**Theorem 3.4.** *For every $n$-qubit-depth-$d$ circuit architecture $\mathcal{A}$ with lightcone size $L$,*

$$\text{XEB}_{\mathcal{H}_\mathcal{A}}(BCG) \geq \frac{1}{2^n}\left(1 + \frac{1}{3}\left(\frac{2}{5}\right)^d\right)^m$$

*where $m = \lfloor n/L \rfloor$.*

*Proof.* Let $I$ be the set of $m = \lfloor n/L \rfloor$ qubits selected by the BCG algorithm where qubits in $I$ have mutually disjoint backward lightcones. Let $W(I) = \{w \in \{0,1\}^n : \forall j \notin I, w_j = 0\}$, so $|W(I)| = 2^m$. Recall that for every $b \in \{0,1\}$ and $j \in [n]$, we have defined the notation $(|b\rangle\langle b|)_j = I^{\otimes(j-1)} \otimes |b\rangle\langle b| \otimes I^{\otimes(n-j)}$. We wish to lower bound the expression

$$\text{XEB}_{\mathcal{H}_\mathcal{A}}(BCG) = \mathop{\mathbb{E}}_{V\sim\mathcal{H}_\mathcal{A}}\left[\sum_{z\in\{0,1\}^n}\langle 0^n|V^\dagger|z\rangle\langle z|V|0^n\rangle\frac{1}{2^{n-m}}\prod_{j\in I}\langle 0^n|V^\dagger(|z_j\rangle\langle z_j|)_jV|0^n\rangle\right] \quad (3.2)$$

where $\langle 0^n|V^\dagger|z\rangle\langle z|V|0^n\rangle = |\langle z|V|0^n\rangle|^2 = q_V(z)$, for every $j \in I$, $\langle 0^n|V^\dagger(|z_j\rangle\langle z_j|)_jV|0^n\rangle$ encodes the probability that the $j$-th qubit measures $z_j$, and $\frac{1}{2^{n-m}}\prod_{j\in I}\langle 0^n|V^\dagger(|z_j\rangle\langle z_j|)_jV|0^n\rangle$ represents the probability that the BCG algorithm outputs $z$ on input $V$. By properties of the tensor product, we can write

$$(3.2)$$
$$= \frac{1}{2^{n-m}}\mathop{\mathbb{E}}_{V\sim\mathcal{H}_\mathcal{A}}\left[(\langle 0^n|V^\dagger)^{\otimes(m+1)}\left(\sum_{z\in\{0,1\}^n}\left(\bigotimes_{k=1}^n|z_k\rangle\langle z_k|\right)\otimes\left(\bigotimes_{j\in I}(|z_j\rangle\langle z_j|)_j\right)\right)(V|0^n\rangle)^{\otimes(m+1)}\right].$$

It is straightforward to show (analogous to the proof of Lemma A.2) that

$$\sum_{z\in\{0,1\}^n}\left(\bigotimes_{k=1}^n|z_k\rangle\langle z_k|\right)\otimes\left(\bigotimes_{j\in I}(|z_j\rangle\langle z_j|)_j\right) = \frac{1}{2^m}\sum_{w\in W(I)}Z(w)\otimes\left(\bigotimes_{j\in I}Z_j^{w_j}\right).$$

Therefore,

$$(3.2) = \frac{1}{2^n}\sum_{w\in W(I)}\mathop{\mathbb{E}}_{V\sim\mathcal{H}_\mathcal{A}}\left[\langle 0^n|V^\dagger Z(w)V|0^n\rangle\prod_{j\in I}\langle 0^n|V^\dagger Z_j^{w_j}V|0^n\rangle\right]$$

$$= \frac{1}{2^n} \sum_{w \in W(I)} \mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2 \right]$$

since for every $w \in W(I)$,

$$\prod_{j \in I} \langle 0^n | V^\dagger Z_j^{w_j} V | 0^n \rangle = \langle 0^n | V^\dagger Z(w) V | 0^n \rangle$$

by the disjoint backward lightcones condition. By Lemma 2.12,

$$\begin{aligned}
&\frac{1}{2^n} \sum_{w \in W(I)} \mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2 \right] \\
\geq &\frac{1}{2^n} \sum_{k=0}^{m} \binom{m}{k} \frac{1}{3^k} \left( \frac{2}{5} \right)^{kd} \\
= &\frac{1}{2^n} \left( 1 + \frac{1}{3} \left( \frac{2}{5} \right)^d \right)^m .
\end{aligned}$$

□

Theorem 3.4 implies that for constant depth circuits, the trivial algorithm which samples bit strings uniformly at random is not a maximizer of the XEB score among efficient classical algorithms. Therefore, similar to the implication of Theorem 3.3(b), Theorem 3.4 also elucidates the importance of increasing the circuit depth along with the number of qubits in future larger-scale experiments.

As a loose upper bound, we show that the quantum simulation algorithm outperforms the BCG algorithm for arbitrary quantum circuits.

**Theorem 3.5.** *For every circuit architecture $\mathcal{A}$,* $\mathrm{XEB}_{\mathcal{H}_\mathcal{A}}(BCG) \leq \mathrm{XEB}_{\mathcal{H}_\mathcal{A}}(QS)$.

*Proof.* Let $\mathcal{A}$ be an arbitrary $n$-qubit circuit architecture, and let $V$ be an arbitrary quantum circuit over $\mathcal{A}$. Let $B_V : \{0,1\}^n \to [0,1]$ denote the output distribution of the BCG algorithm on input $V$, and let $I$ denote the set of qubits with disjoint backward lightcones selected with $m = |I|$. First observe that

$$\mathop{\mathbb{E}}_{z \sim q_V} [q_V(z)] = \sum_{z \in \{0,1\}^n} q_V(z)^2 = \sum_{x \in \{0,1\}^m} \sum_{\substack{y \in \{0,1\}^n \\ s.t.\ y_I = x}} q_V(y)^2. \tag{3.3}$$

Then by the Cauchy-Schwarz inequality,

$$(3.3) \geq \sum_{x \in \{0,1\}^m} \frac{1}{2^{n-m}} \left( \sum_{\substack{y \in \{0,1\}^n \\ s.t.\ y_I = x}} q_V(y) \right)^2 = \sum_{z \in \{0,1\}^n} B_V(z) q_V(z) = \mathop{\mathbb{E}}_{z \sim B_V} [q_V(z)] .$$

Therefore,

$$\mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \mathop{\mathbb{E}}_{z \sim q_V} [q_V(z)] \right] \geq \mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \mathop{\mathbb{E}}_{z \sim B_V} [q_V(z)] \right].$$

□

We remark that the above bound does not depend on the randomness over $\mathcal{H}_\mathcal{A}$.

# Chapter 4

# An Extended BCG Algorithm

In this chapter, we consider an extension of the BCG algorithm for spoofing the linear cross-entropy benchmark. Instead of sampling only a subset of qubits according to their marginal output distributions, the EBCG algorithm samples every qubit according to its marginal output distribution. Similar to the BCG algorithm, the EBCG algorithm's time complexity is $\text{poly}(n, 2^L)$ for a circuit architecture with lightcone size $L$. We wish to understand whether or not the EBCG algorithm outperforms the BCG algorithm on the linear cross-entropy benchmark. Let $\mathcal{A}$ be a circuit architecture with lightcone size $L$. Our goal is to analyze the expression

$$\text{XEB}_{\mathcal{H}_{\mathcal{A}}}(EBCG) = \mathop{\mathbb{E}}_{V\sim\mathcal{H}_{\mathcal{A}}}\left[\sum_{z\in\{0,1\}^n}\langle 0^n|V^\dagger|z\rangle\langle z|V|0^n\rangle\prod_{j=1}^{n}\langle 0^n|V^\dagger(|z_j\rangle\langle z_j|)_jV|0^n\rangle\right]. \tag{4.1}$$

In the above equation, $\langle 0^n|V^\dagger|z\rangle\langle z|V|0^n\rangle = |\langle z|V|0^n\rangle|^2$ encodes the probability of sampling $z \in \{0,1\}^n$ from $V$'s output distribution, and for every $j \in [n]$, $\langle 0^n|V^\dagger(|z_j\rangle\langle z_j|)_jV|0^n\rangle$ represents the probability that the $j$-th qubit measures $z_j$ where we have used the notation $(|z_j\rangle\langle z_j|)_j = I^{\otimes(j-1)} \otimes |z_j\rangle\langle z_j| \otimes I^{\otimes(n-j)}$. By properties of the tensor product, we can write

$$(4.1) = \mathop{\mathbb{E}}_{V\sim\mathcal{H}_{\mathcal{A}}}\left[(\langle 0^n|V^\dagger)^{\otimes(n+1)}\left(\sum_{z\in\{0,1\}^n}\left(\bigotimes_{k=1}^{n}|z_k\rangle\langle z_k|\right)\otimes\left(\bigotimes_{j=1}^{n}(|z_j\rangle\langle z_j|)_j\right)\right)(V|0^n\rangle)^{\otimes(n+1)}\right]. \tag{4.2}$$

We show in Lemma A.2 the identity

$$\sum_{z\in\{0,1\}^n}\left(\bigotimes_{k=1}^{n}|z_k\rangle\langle z_k|\right)\otimes\left(\bigotimes_{j=1}^{n}(|z_j\rangle\langle z_j|)_j\right) = \frac{1}{2^n}\sum_{w\in\{0,1\}^n}Z(w)\otimes\left(\bigotimes_{j=1}^{n}Z_j^{w_j}\right). \tag{4.3}$$

Substituting (4.3) into (4.2), we get that

$$\begin{aligned}\text{XEB}_{\mathcal{H}_{\mathcal{A}}}(EBCG) &= \frac{1}{2^n}\mathop{\mathbb{E}}_{V\sim\mathcal{H}_{\mathcal{A}}}\left[(\langle 0^n|V^\dagger)^{\otimes(n+1)}\left(\sum_{w\in\{0,1\}^n}Z(w)\otimes\left(\bigotimes_{j=1}^{n}Z_j^{w_j}\right)\right)(V|0^n\rangle)^{\otimes(n+1)}\right]\\ &= \frac{1}{2^n}\sum_{w\in\{0,1\}^n}\mathop{\mathbb{E}}_{V\sim\mathcal{H}_{\mathcal{A}}}\left[\langle 0^n|V^\dagger Z(w)V|0^n\rangle\prod_{j=1}^{n}\langle 0^n|V^\dagger Z_j^{w_j}V|0^n\rangle\right].\end{aligned}$$

For every $w \in \{0,1\}^n$, define $\mathrm{Supp}(w) = \{j \in [n] : w_j = 1\}$. Let

$G = \{w \in \{0,1\}^n : \mathrm{Supp}(w)$ corresponds to a set of qubits with disjoint backward lightcones$\}$.

Similar to the set of qubits selected by the BCG algorithm, the set $G$ is completely specified by the circuit architecture. By the disjoint backward lightcones condition, for every $w \in G$,

$$\prod_{j=1}^{n} \langle 0^n | V^\dagger Z_j^{w_j} V | 0^n \rangle = \langle 0^n | V^\dagger Z(w) V | 0^n \rangle.$$

Let $B = \{0,1\}^n \setminus G$. Then, we can write

$$\begin{aligned}
&\mathrm{XEB}_{\mathcal{H}_\mathcal{A}}(EBCG) \\
=&\frac{1}{2^n} \sum_{w \in G} \mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2 \right] + \frac{1}{2^n} \sum_{w \in B} \mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle \prod_{j=1}^{n} \langle 0^n | V^\dagger Z_j^{w_j} V | 0^n \rangle \right].
\end{aligned}$$

Let $I$ be the set of $m = \lfloor n/L \rfloor$ qubits with mutually disjoint backward lightcones that would be selected by the BCG algorithm. Let $W(I) = \{w \in \{0,1\}^n : \forall i \notin I, w_i = 0\}$. Since $W(I) \subseteq G$, we get that for an arbitrary $n$-qubit quantum circuit $V$,

$$\sum_{w \in G} \langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2 \geq \sum_{w \in W(I)} \langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2.$$

This implies that

$$\frac{1}{2^n} \sum_{w \in G} \mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2 \right] \geq \frac{1}{2^n} \sum_{w \in W(I)} \mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2 \right] = \mathrm{XEB}_{\mathcal{H}_\mathcal{A}}(BCG).$$

Indeed, the analysis of the EBCG algorithm contains that of the BCG algorithm since for every $w \in G$, $\mathbb{E}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2 \right]$ can also be lower bounded using Lemma 2.12. However, for every $w \in B$, the term $\prod_{j=1}^{n} \langle 0^n | V^\dagger Z_j^{w_j} V | 0^n \rangle$ does not collapse to $\langle 0^n | V^\dagger Z(w) V | 0^n \rangle$, so the expression

$$\begin{aligned}
&\mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle \prod_{j=1}^{n} \langle 0^n | V^\dagger Z_j^{w_j} V | 0^n \rangle \right] \\
= &\mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ (\langle 0^n | V^\dagger)^{\otimes (n+1)} \left( Z(w) \otimes \left( \bigotimes_{j=1}^{n} Z_j^{w_j} \right) \right) (V | 0^n \rangle)^{\otimes (n+1)} \right]
\end{aligned}$$

always involves the $t$-th moment of $\mathcal{H}_\mathcal{A}$ for some $t \geq 3$ which renders second-moment specific lower bound methods like Lemma 2.12 inapplicable. Nonetheless, to show that the EBCG algorithm achieves higher XEB scores than the BCG algorithm, it suffices to show that

$$\sum_{w \in B} \mathop{\mathbb{E}}_{V \sim \mathcal{H}_\mathcal{A}} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle \prod_{j=1}^{n} \langle 0^n | V^\dagger Z_j^{w_j} V | 0^n \rangle \right] \geq 0.$$

We make a slightly stronger claim in the following conjecture.

**Conjecture 4.1** (The EBCG Conjecture)**.** *For every* $w \in \{0,1\}^n$*,*

$$\mathop{\mathbb{E}}_{V\sim\mathcal{H}_\mathcal{A}}\left[\langle 0^n|V^\dagger Z(w)V|0^n\rangle\prod_{j=1}^{n}\langle 0^n|V^\dagger Z_j^{w_j}V|0^n\rangle\right]\geq 0. \tag{4.4}$$

At the moment, the computational complexity of the linear cross-entropy benchmark is mostly uncharted territory awaiting exploration. While the analysis of the BCG algorithm can be viewed as a first step in investigating the classical computational complexity of attaining non-trivial XEB scores, our study of the EBCG algorithm makes up the second attempt to discover better algorithms for the same task. One may ask, for various choices of the circuit depth $d$, what is the highest XEB score attainable by an efficient classical algorithm? Google has conjectured that for $d = \text{poly}(n)$, the trivial uniform algorithm is optimal, and we have argued that for small enough $d$ rendering the BCG algorithm efficient, for example when $d$ is constant, Theorem 3.4 shows that the trivial algorithm is not optimal. Likewise, proving the EBCG conjecture will imply the sub-optimality of the BCG algorithm in these low-depth regimes. Then one may ask, could the EBCG algorithm be the optimal linear cross-entropy benchmark spoofing algorithm for constant $d$? If Google's strong conjecture is true, then there is no known evidence against this possibility. On the other hand, if one hopes to design a spoofing algorithm efficient for even deep random quantum circuits, thereby refuting Google's strong conjecture, we will argue in section 4.2 why such algorithms may need to employ tactics drastically different from the EBCG algorithm.

We will refer to the LHS of (4.4) as the EBCG expression. The rest of the chapter is devoted to studying the EBCG expression in various settings. While the goal is to prove the EBCG conjecture for random quantum circuits, our techniques fall short of what is needed to do so. On the upside, we provide numerical evidence in favour of the EBCG conjecture for 1D random quantum circuits by exactly computing the EBCG expression for small circuit sizes. We are also able to prove the EBCG conjecture for the special cases of depth-1 and $\text{poly}(n)$-depth random quantum circuits by analyzing the EBCG expression with expectation over $\mu^N_{\text{Haar}}$, as well as when $|w| \leq 2$, by analyzing the EBCG expression for random Clifford circuits. In the last section, we show that the EBCG expression is non-negative for random fermionic Gaussian unitaries and derive a formula for its exact value.

## 4.1 EBCG Does Not Always Outperform BCG

We begin by arguing that the expectation over $\mathcal{H}_\mathcal{A}$ is necessary in the EBCG conjecture. Recall that w.r.t. the architecture $\mathcal{A}$, we have defined

$G = \{w \in \{0,1\}^n : \text{Supp}(w) \text{ corresponds to a set of qubits with disjoint backward lightcones}\}$

and $B = \{0,1\}^n \setminus G$.

**Lemma 4.1.** *For* $n = 3$*, there exists a* 3*-qubit quantum circuit* $V$ *such that*

$$\langle 0^n|V^\dagger Z(w)V|0^n\rangle\prod_{j=1}^{n}\langle 0^n|V^\dagger Z_j^{w_j}V|0^n\rangle < 0$$

*for at least one* $w \in B$*.*

*Proof.* Let us consider $n = 3$ and the probability distribution over $\{0,1\}^n$ given by

| $z$ | $\Pr(z)$ |
|---|---|
| 000 | 0 |
| 001 | 0.25 |
| 010 | 0.3 |
| 011 | 0 |
| 100 | 0.3 |
| 101 | 0 |
| 110 | 0.15 |
| 111 | 0 |

In this example, 000 is the outcome that EBCG thinks is the most likely, but in reality, the probability of observing 000 is zero. Clearly, there exists a quantum circuit $V$ on three qubits whose output distribution on input $|0^3\rangle$ is exactly the distribution given in the table.[1] We can verify that the performance of the EBCG algorithm on input $V$ is

$$0.075625 \times 0.25 + 0.185625 \times 0.3 \times 2 + 0.151875 \times 0.15 = 0.1530625$$

while by choosing $I = \{1\}$ containing just the right most qubit, the BCG algorithm achieves a score of

$$0.0625 \times 0.25 + 0.1875 \times 0.75 = 0.15625.$$

Thus, the BCG algorithm outperforms the EBCG algorithm for this specific input $V$. Since

$$\sum_{w \in G} \langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2 \geq \sum_{w \in W(I)} \langle 0^n | V^\dagger Z(w) V | 0^n \rangle^2,$$

it must be the case that

$$\sum_{w \in B} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle \prod_{j=1}^{n} \langle 0^n | V^\dagger Z_j^{w_j} V | 0^n \rangle \right] < 0,$$

and the conclusion follows. □

## 4.2 Haar Random Unitary

In this section, we first establish a lower bound for $\mathrm{XEB}_{\mu_{\mathrm{Haar}}^N}(EBCG)$. The proof will also imply the non-negativity of the EBCG expression when the expectation is taken over $\mu_{\mathrm{Haar}}^N$.

**Theorem 4.1.**

$$\mathrm{XEB}_{\mu_{Haar}^N}(EBCG) \geq \frac{1}{2^n} + \frac{n}{(2^n+n)(2^n+n-1)}$$

[1] For example, using the construction described in section 4.5 of [NC10].

*Proof.* Let $w \in \{0,1\}^n$. We have that

$$\begin{aligned}&\mathop{\mathbb{E}}_{V\sim\mu_{\mathrm{Haar}}^N}\Big[\langle 0^n|V^\dagger Z(w)V|0^n\rangle\prod_{j=1}^n\langle 0^n|V^\dagger Z_j^{w_j}V|0^n\rangle\Big]\\ =&\mathrm{Tr}\bigg(Z(w)\otimes\bigg(\bigotimes_{j=1}^n Z_j^{w_j}\bigg)\mathop{\mathbb{E}}_{V\sim\mu_{\mathrm{Haar}}^N}\left[(V|0^n\rangle\langle 0^n|V^\dagger)^{\otimes(n+1)}\right]\bigg).\end{aligned}$$

By substituting $t = n+1$ into Lemma 2.3, the above expression equals

$$\begin{aligned}&\frac{1}{(n+1)!\binom{n+2^n}{n+1}}\mathrm{Tr}\bigg(Z(w)\otimes\bigg(\bigotimes_{j=1}^n Z_j^{w_j}\bigg)\sum_{\pi\in S_{n+1}}W_\pi^{(N)}\bigg)\\ =&\frac{1}{(n+1)!\binom{n+2^n}{n+1}}\sum_{\pi\in S_{n+1}}\sum_{i_0,i_1,\ldots,i_n\in\{0,1\}^n}\langle i_0,\ldots,i_n|\bigg(Z(w)\otimes\bigg(\bigotimes_{j=1}^n Z_j^{w_j}\bigg)\bigg)|i_{\pi^{-1}(0)},\ldots,i_{\pi^{-1}(n)}\rangle\\ =&\frac{(2^n-1)!}{(2^n+n)!}\sum_{\pi\in S_{n+1}}\sum_{i_0,i_1,\ldots,i_n\in\{0,1\}^n}\langle i_0|Z(w)|i_{\pi^{-1}(0)}\rangle\prod_{j=1}^n\langle i_j|Z_j^{w_j}|i_{\pi^{-1}(j)}\rangle.\end{aligned}$$

Let $\pi \in S_{n+1}$. We construct an undirected graph $G_\pi = (V, E)$ where $V = \{0, 1, \ldots, n\}$ and $E = \{uv : v = \pi(u)\}$. Let $H_1, \ldots, H_c$ be the components of $G_\pi$. For $Z$-type Pauli's, we have $\langle a|Z(w)|b\rangle \neq 0$ if and only if $a = b$ and

$$\sum_{i\in\{0,1\}^n}\langle i|Z(w)|i\rangle = \begin{cases}2^n & \text{if } w = 0^n\\ 0 & \text{otherwise}\end{cases}.$$

Define $Z(0) = Z(w)$, and for every $j \in [n]$, define $Z(j) = Z_j^{w_j}$. Then, we can write

$$\sum_{i_0,i_1,\ldots,i_n\in\{0,1\}^n}\langle i_0|Z(w)|i_{\pi^{-1}(0)}\rangle\prod_{j=1}^n\langle i_j|Z_j^{w_j}|i_{\pi^{-1}(j)}\rangle = \sum_{i_0,i_1,\ldots,i_n\in\{0,1\}^n}\prod_{j=0}^n\langle i_j|Z(j)|i_{\pi^{-1}(j)}\rangle. \quad (4.5)$$

In the above expression, for $\prod_{j=0}^n\langle i_j|Z(j)|i_{\pi^{-1}(j)}\rangle \neq 0$, we need $i_j = i_{\pi^{-1}(j)}$ for every $j$. Thus,

$$\begin{aligned}(4.5) =& \sum_{i_1,\ldots,i_c\in\{0,1\}^n}\prod_{j=1}^c\prod_{u\in V(H_j)}\langle i_j|Z(u)|i_j\rangle\\ =&\prod_{j=1}^c\sum_{i_j\in\{0,1\}^n}\langle i_j|\bigg(\prod_{u\in V(H_j)}Z(u)\bigg)|i_j\rangle\\ =&\begin{cases}2^{cn} & \text{if } \{0\}\cup\mathrm{Supp}(w) \text{ is contained in } V(H_j) \text{ for some } j\in\{1,\ldots,c\}\\ 0 & \text{otherwise}\end{cases}.\end{aligned}$$

For every $w \in \{0,1\}^n$, let $\Pi_w = \{\pi \in S_{n+1} : \{0\} \cup \mathrm{Supp}(w) \text{ is contained in one cycle of } \pi\}$. For every $\pi \in S_{n+1}$, let $c(\pi)$ denote the number of cycles in $\pi$. Then,

$$\mathrm{XEB}_{\mu_{\mathrm{Haar}}^N}(EBCG)$$

$$
\begin{aligned}
=&\frac{1}{2^n}\sum_{w\in\{0,1\}^n}\mathop{\mathbb{E}}_{V\sim\mu_{\mathrm{Haar}}^N}\left[\langle 0^n|V^\dagger Z(w)V|0^n\rangle\prod_{j=1}^n\langle 0^n|V^\dagger Z_j^{w_j}V|0^n\rangle\right]\\
=&\frac{(2^n-1)!}{2^n(2^n+n)!}\sum_{w\in\{0,1\}^n}\sum_{\pi\in S_{n+1}}\sum_{i_0,i_1,\ldots,i_n\in\{0,1\}^n}\langle i_0|Z(w)|i_{\pi^{-1}(0)}\rangle\prod_{j=1}^n\langle i_j|Z_j^{w_j}|i_{\pi^{-1}(j)}\rangle\\
=&\frac{(2^n-1)!}{2^n(2^n+n)!}\sum_{w\in\{0,1\}^n}\sum_{\pi\in\Pi_w}2^{c(\pi)n}.
\end{aligned}
$$

We first consider the case where $w=0^n$. For $w=0^n$, $\Pi_w=S_{n+1}$. For every $j\in[n+1]$, the number of permutations in $S_{n+1}$ with exactly $j$ cycles is given by the unsigned Stirling numbers of the first kind $\begin{bmatrix}n+1\\ j\end{bmatrix}$. Thus, for $w=0^n$,

$$
\begin{aligned}
\sum_{\pi\in\Pi_w}2^{c(\pi)n}&=\sum_{j=1}^{n+1}\begin{bmatrix}n+1\\ j\end{bmatrix}2^{jn}\\
&=(2^n)^{\overline{n+1}}\\
&=\frac{(2^n+n)!}{(2^n-1)!}.
\end{aligned}
$$

Thus,

$$
\frac{(2^n-1)!}{2^n(2^n+n)!}\sum_{w\in\{0,1\}^n}\sum_{\pi\in\Pi_w}2^{c(\pi)n}=\frac{1}{2^n}+\frac{(2^n-1)!}{2^n(2^n+n)!}\sum_{w\in\{0,1\}^n\backslash\{0^n\}}\sum_{\pi\in\Pi_w}2^{c(\pi)n}.
$$

Now let $w\in\{0,1\}^n\backslash\{0^n\}$. Let $k=|w|$. For every $j\in\{0,\ldots,n\}$, the number of permutations in $\Pi_w$ with exactly $j+1$ cycles is

$$
\sum_{l=k+1}^{n+1}\binom{n+1-(k+1)}{l-(k+1)}(l-1)!\begin{bmatrix}n+1-l\\ j\end{bmatrix}
$$

where $l$ is the length of the cycle that contains $\{0\}\cup\mathrm{Supp}(w)$ and $(l-1)!$ is the number of cycles of length $l$. Thus,

$$
\begin{aligned}
\sum_{w\in\{0,1\}^n\backslash\{0^n\}}\prod_{\pi\in\Pi_w}2^{c(\pi)n}&=\sum_{k=1}^n\binom{n}{k}\sum_{l=k+1}^{n+1}\binom{n-k}{l-k-1}(l-1)!\sum_{j=0}^{n+1-l}\begin{bmatrix}n+1-l\\ j\end{bmatrix}2^{(j+1)n}\\
&=\sum_{k=1}^n\sum_{l=k+1}^{n+1}\binom{n}{k}\binom{n-k}{l-k-1}(l-1)!2^n\frac{(2^n+n-l)!}{(2^n-1)!}.
\end{aligned}
$$

Therefore,

$$
\frac{(2^n-1)!}{2^n(2^n+n)!}\sum_{w\in\{0,1\}^n\backslash\{0^n\}}\sum_{\pi\in\Pi_w}2^{c(\pi)n}
$$

$$
\begin{aligned}
&= \sum_{k=1}^{n} \sum_{l=k+1}^{n+1} \frac{\binom{n}{k}\binom{n-k}{l-k-1}}{l\binom{2^n+n}{l}} \\
&= \sum_{l=2}^{n+1} \frac{\binom{n}{l-1}}{l\binom{2^n+n}{l}} \sum_{k=1}^{l-1} \binom{l-1}{k} \\
&= \sum_{l=2}^{n+1} \frac{(2^{l-1}-1)\binom{n}{l-1}}{l\binom{2^n+n}{l}} \\
&\geq \frac{n}{(2^n+n)(2^n+n-1)}
\end{aligned}
$$

by truncating the sum at $l = 2$. □

In fact, we can analyze the XEB score of further generalizations of the EBCG algorithm for Haar random unitaries using Lemma 2.3. Let $w \in \{0,1\}^n$. For $n = mr$, we can divide $w$ into $r$ consecutive blocks each of length $m$. For every $j \in [r]$, define $w(m,j) \in \{0,1\}^n$ where for every $i \in \{m(j-1)+1, \ldots, mj\}$, $w(m,j)_i = w_i$, and for every $i \in [n] \setminus \{m(j-1)+1, \ldots, mj\}$, $w(m,j)_i = 0$. For each choice of $n = mr$, we can consider an algorithm which partitions the $n$ qubits into $r$ blocks of size $m$, and it computes and samples according to the $m$-qubit marginal output distributions. We can show that for every $n$-qubit random unitary distribution $\mathcal{D}$, the XEB score of this algorithm is given by the expression

$$
\frac{1}{2^n} \sum_{w \in \{0,1\}^n} \mathop{\mathbb{E}}_{V \sim \mathcal{D}} \Big[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle \prod_{j=1}^{r} \langle 0^n | V^\dagger Z(w(m,j)) V | 0^n \rangle \Big].
$$

Note that when $m = n$ and $r = 1$, this algorithm reduces to the quantum simulation algorithm, and by choosing $m = 1$ and $r = n$, we recover the EBCG algorithm. By slight generalizations of the arguments used to prove Theorem 4.1, we can prove the following lower bound.

**Theorem 4.2.** *For every way of factoring $n = mr$,*

$$
\frac{1}{2^n} \sum_{w \in \{0,1\}^n} \mathop{\mathbb{E}}_{V \sim \mu_{Haar}^N} \Big[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle \prod_{j=1}^{r} \langle 0^n | V^\dagger Z(w(m,j)) V | 0^n \rangle \Big] \geq \frac{1}{2^n} + \frac{r(2^m-1)}{(2^n+r)(2^n+r-1)}.
$$

We observe that in order to attain an XEB score of $\frac{1+1/n^k}{2^n}$ for some $k > 0$, we need $m = n - k \log n$. It suggests that for deep random quantum circuits, this family of algorithms does not achieve non-trivial XEB scores until the algorithm is very close to quantum simulation despite always having an exponential time complexity. This phenomenon can be viewed as preliminary evidence supporting the belief which underlies Google's strong conjecture that for deep random quantum circuits, attaining non-trivial XEB scores may be just as difficult as performing random circuit sampling.

## 4.3 Random Quantum Circuits

Theorem 4.1 implies the EBCG conjecture for depth-1 random quantum circuits. By the $t$-design property, Theorem 4.1 also implies the EBCG conjecture for poly($n$)-depth 1D random

quantum circuits via a generalization of the arguments made in the proof of Lemma 2.11. We will show in the next section that the EBCG expression is non-negative with expectation over random Clifford circuits. Thus, by applying the 3-design property of $\mathcal{U}(\mathbf{C}_2)$ to each gate of a random quantum circuit inductively, the lower bound shown for random Clifford circuits implies the EBCG conjecture for $w \in \{0,1\}^n$ such that $|w| = 2$.

We briefly discuss some of the difficulties faced in adapting the techniques developed in Chapter 2 for proving the EBCG conjecture. For a general $w \in \{0,1\}^n$ such that $|w| \geq 3$, the EBCG expression

$$\mathop{\mathbb{E}}_{V \sim \mathcal{H}_{\mathcal{A}}} \left[ \langle 0^n | V^\dagger Z(w) V | 0^n \rangle \prod_{j=1}^{n} \langle 0^n | V^\dagger Z_j^{w_j} V | 0^n \rangle \right]$$

involves the $t$-th moment of $\mathcal{H}_{\mathcal{A}}$ for some $t \geq 4$, so we cannot apply the Clifford 3-design property (Theorem 2.3) to replace the expectation to be over $\mathcal{C}_{\mathcal{A}}$ (recall that $\mathcal{C}_{\mathcal{A}}$ is the distribution of random Clifford circuits with the architecture $\mathcal{A}$). Thus, combinatorial arguments like the ones used in the proof of Theorem 2.10 and Lemma 2.12 that are fruitful for lower bounding second-moment expressions are inapplicable to higher order moment expressions.

We can also try to modify the proof of Theorem 2.13. Theorem 4.1 implies that the EBCG expression is strictly positive for every $w \in \{0,1\}^n$ for depth-1 random quantum circuits. We intuitively believe that depth-2 random quantum circuits cannot differ from depth-1 random quantum circuits by that much. Thus, the value of the EBCG expression for depth-2 random quantum circuits should not differ from the depth-1 value by that much, hence implying the EBCG conjecture for depth-2 circuits. More generally, we may wish to argue by induction that if the EBCG expression is positive for depth-$d$ random quantum circuits, then it is also positive for depth-$(d+1)$ random quantum circuits, and we have already established the $d = 1$ base case. We can express this idea algebraically for 1D random quantum circuits using their $t$-th moment operators (recall (2.7)). Let $w \in \{0,1\}^n$ and let $|x\rangle$ denote the vectorized representation of

$$Z(w) \otimes \left( \bigotimes_{j=1}^{n} Z_j^{w_j} \right).$$

Let $P_{\text{odd}}$ and $P_{\text{even}}$ denote $P_{\text{odd}}^{(n+1)}$ and $P_{\text{even}}^{(n+1)}$ respectively. For example, for every even $k \geq 1$, we can write the difference between the EBCG expressions of depth-$(2k+1)$ and depth-$(2k+3)$ 1D random quantum circuits as

$$\begin{aligned}
&|\langle 0^{2n(n+1)}| \left(P_{\text{odd}} P_{\text{even}} P_{\text{odd}}\right)^k - \left(P_{\text{odd}} P_{\text{even}} P_{\text{odd}}\right)^{k+1} |x\rangle| \\
=&|\langle 0^{2n(n+1)}| \left(P_{\text{odd}} P_{\text{even}} P_{\text{odd}}\right)^{\frac{k}{2}} \left( \left(P_{\text{odd}} P_{\text{even}} P_{\text{odd}}\right)^{\frac{k}{2}} - \left(P_{\text{odd}} P_{\text{even}} P_{\text{odd}}\right)^{\frac{k}{2}+1} \right) P_{\text{odd}} |x\rangle| \\
\leq&\| \left(P_{\text{odd}} P_{\text{even}} P_{\text{odd}}\right)^{\frac{k}{2}} - \left(P_{\text{odd}} P_{\text{even}} P_{\text{odd}}\right)^{\frac{k}{2}+1} \|_\infty \sqrt{\langle 0^{2n(n+1)}| \left(P_{\text{odd}} P_{\text{even}} P_{\text{odd}}\right)^k |0^{2n(n+1)}\rangle} \sqrt{\langle x | P_{\text{odd}} | x \rangle}.
\end{aligned}$$

The $\langle x | P_{\text{odd}} | x \rangle$ term, which is the only term involving $|x\rangle$, can be worked out exactly using Lemma 2.2 since $P_{\text{odd}}$ is only depth-1. Unfortunately, we do not know how to handle the other two terms. The $\langle 0^{2n(n+1)}| \left(P_{\text{odd}} P_{\text{even}} P_{\text{odd}}\right)^k |0^{2n(n+1)}\rangle$ term generalizes the collision probability appearing in the proof of Theorem 2.13, and we do not know of a generalization

of Theorem 2.11 for upper bounding $\langle 0^{2n(n+1)}| \left(P_{\text{odd}}P_{\text{even}}P_{\text{odd}}\right)^k |0^{2n(n+1)}\rangle$. It is not hard to show that

$$\|(P_{\text{odd}}P_{\text{even}}P_{\text{odd}})^{\frac{k}{2}} - (P_{\text{odd}}P_{\text{even}}P_{\text{odd}})^{\frac{k}{2}+1}\|_\infty \leq \|(P_{\text{odd}}P_{\text{even}}P_{\text{odd}})^{\frac{k}{2}} - P_N^{(n+1)}\|_\infty.$$

Thus, by combining Theorem 2.4 and Lemma 2.8, we can conclude that

$$\|(P_{\text{odd}}P_{\text{even}}P_{\text{odd}})^{\frac{k}{2}} - P_N^{(n+1)}\|_\infty \leq e^{-\Delta k}$$

for some small positive $\Delta$ that depends on $t = n+1$. For this upper bound to be non-trivial, $k$ needs to be at least $\text{poly}(t)$ to overcome $\Delta$, so it does not reflect our intuition in the case of shallow random quantum circuits with consecutive numbers of layers. In addition, the $k = \text{poly}(n)$ regime has been handled adequately by the Haar random unitary results of section 4.2.

The architecture agnostic part of the proof of Theorem 2.11 can be generalized to obtain an algorithm for exactly computing the EBCG expression for random quantum circuits. For example, let us consider $w = 1^n$. We wish to compute

$$\begin{aligned}
&\mathop{\mathbb{E}}_{V\sim\mathcal{H}_\mathcal{A}} \left[\langle 0^n|V^\dagger Z(w)V|0^n\rangle \prod_{j=1}^n \langle 0^n|V^\dagger Z_j V|0^n\rangle\right] \\
=&\mathop{\mathbb{E}}_{V\sim\mathcal{H}_\mathcal{A}} \left[(\langle 0^n|V^\dagger)^{\otimes(n+1)} \left(Z(w)\otimes\left(\bigotimes_{j=1}^n Z_j\right)\right)(V|0^n\rangle)^{\otimes(n+1)}\right].
\end{aligned}$$

For each 2-qubit gate in the last layer, we need to evaluate

$$\mathop{\mathbb{E}}_{U\sim\mu_{\text{Haar}}^4} \left[(U^\dagger\otimes U^\dagger\otimes U^\dagger)(Z(11)\otimes Z(10)\otimes Z(01))(U\otimes U\otimes U)\right] \tag{4.6}$$

after cancellations, which is a third moment expression even though we are considering $w = 1^n$. By applying Lemma 2.2, we get that

$$(4.6) = \frac{1}{45}(W_{\pi_1}^{(4)} - 2W_{\pi_2}^{(4)} - 2W_{\pi_3}^{(4)} + 4W_{\pi_4}^{(4)} + 4W_{\pi_5}^{(4)} - 2W_{\pi_6}^{(4)})$$

where

$$\pi_1 = (1)(2)(3), \pi_2 = (12)(3), \pi_3 = (1)(23), \pi_4 = (132), \pi_5 = (123), \pi_6 = (13)(2)$$

in the disjoint cycle notation. Note that the coefficients in front of each permutation operator can be either positive or negative. More generally, the algorithm proceeds gate by gate from the last to the first layer. After handling all the gates directly conjugating the starting $Z$-type Pauli operators, the operator evaluated so far can be maintained as a linear combination of tensor product of permutation operators. To process each additional gate, the algorithm simply applies Lemma 2.2 and linearity. We implement this algorithm to compute the EBCG expressions of small 1D random quantum circuits. See Figure 4.1 and Figure 4.2. Since the algorithm's space complexity is roughly $O((|w|!)^n)$, it is only feasible to execute up to $n = 8$ and $|w| = 3$ on a laptop.[2]

[2]With $n = 8$ and $|w| = 3$, the algorithm is effectively simulating a 32-qubit system.

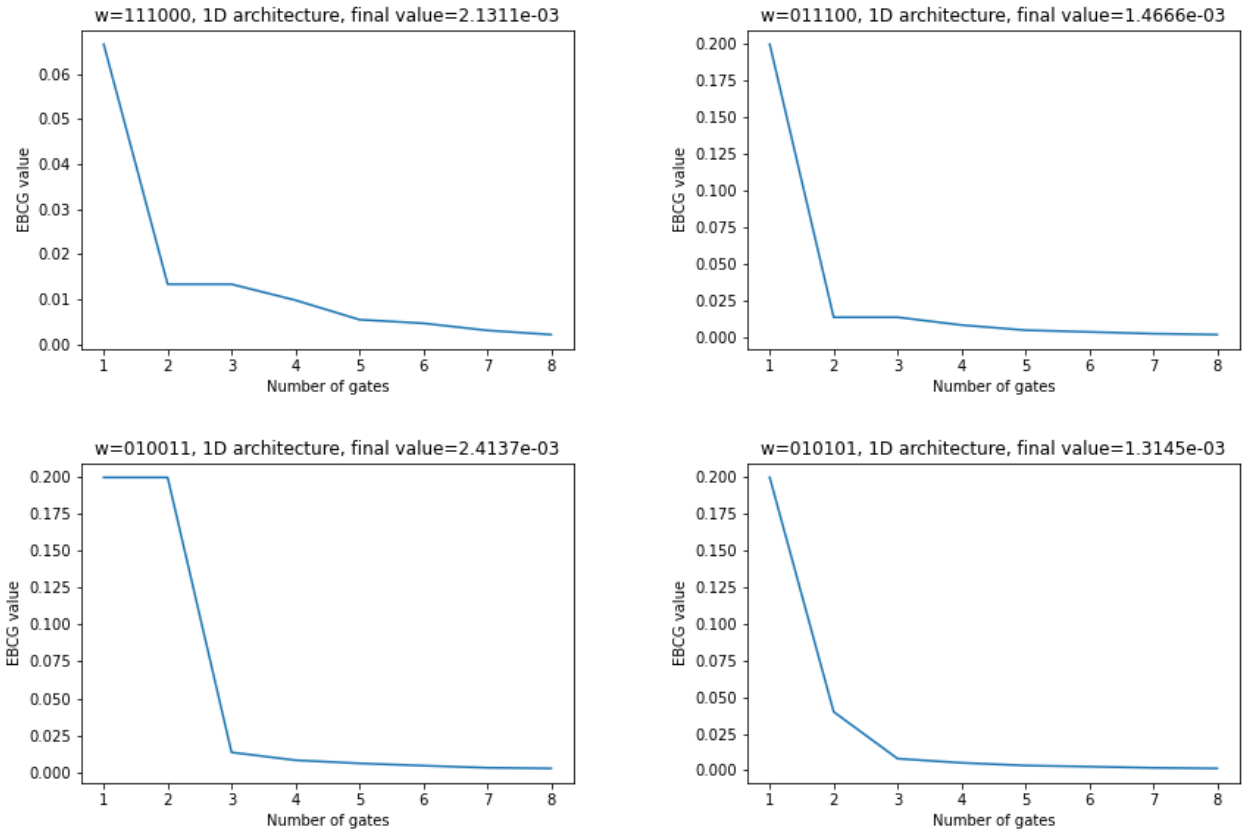


Figure 4.1: Exact EBCG values for 6 qubits and $|w| = 3$.

In summary, if the EBCG conjecture is true, then the EBCG algorithm attains higher XEB scores than the BCG algorithm for random quantum circuits. However, we expect the asymptotic scaling of the XEB scores of both algorithms to be similar; namely, we expect $\mathrm{XEB}_{\mathcal{H}_{\mathcal{A}}}(EBCG)$ to scale like $\frac{e^{\Delta^d n}}{2^n}$ for some constant $\Delta \in (0,1)$ where $e^{\Delta^d n}$ is understood as an increasing function of $n$ and decreasing function of $d$. Since the two algorithms also have the same asymptotic time complexity, the EBCG algorithm may reveal little additional insights into the classical computational complexity aspect of the linear cross-entropy benchmark. That being said, just like Conjecture 2.1, the EBCG conjecture itself represents an interesting mathematical question about an inherent property of random quantum circuits with a current lack of understanding. Hopefully, future efforts in resolving the EBCG conjecture will lead to the discovery of new techniques for analyzing $t$-th moment expressions of random quantum circuits for arbitrary $t \geq 3$. As a speculation, we expect such new ideas to be effective for analyzing $\mathbb{E}_{V\sim\mathcal{H}_{\mathcal{A}}}\left[V^{\otimes t}A(V^\dagger)^{\otimes t}\right]$ for at least an arbitrary $Z$-type Pauli operator $A$. Resolving the EBCG conjecture may also shed light in ways to improve the $t$ dependence in Theorem 2.8 or generalizing Theorem 2.9 to $t \geq 4$. It is also interesting to see whether the EBCG conjecture will be resolved by a method that merely establishes the non-negativity of the EBCG expression while not implying any non-trivial lower bound.

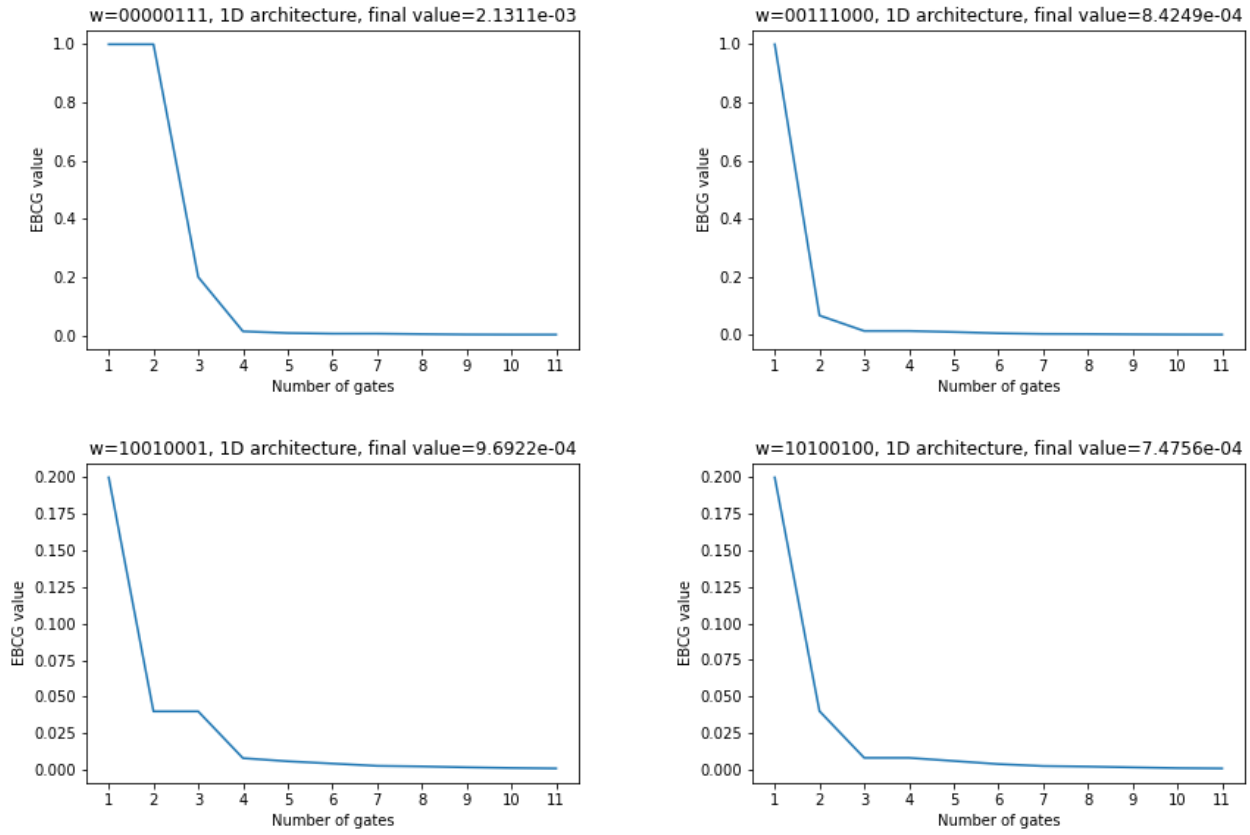


Figure 4.2: Exact EBCG values for 8 qubits and $|w| = 3$.

## 4.4 Random Clifford Circuits

In this section, we show that the EBCG conjecture is true for random Clifford circuits with a proof that depends on neither the circuit architecture nor the randomness over $\mathcal{C}_{\mathcal{A}}$.

**Theorem 4.3.** *For every $w \in \{0,1\}^n$,*

$$\mathop{\mathbb{E}}_{V\sim\mathcal{C}_{\mathcal{A}}}\left[\langle 0^n|V^\dagger Z(w)V|0^n\rangle \prod_{j=1}^{n}\langle 0^n|V^\dagger Z_j^{w_j}V|0^n\rangle\right] \geq 0.$$

*Proof.* Let $V$ be an arbitrary Clifford circuit over the architecture $\mathcal{A}$, and let $w \in \{0,1\}^n$. Notice that either $V^\dagger Z_j V$ is a $Z$-type Pauli for every $j \in \mathrm{Supp}(w)$, or there exists $j \in \mathrm{Supp}(w)$ such that $V^\dagger Z_j V$ is not a $Z$-type Pauli. If $V^\dagger Z_j V$ is a $Z$-type Pauli for every $j \in \mathrm{Supp}(w)$, then

$$\prod_{j\in\mathrm{Supp}(w)}\langle 0^n|V^\dagger Z_j V|0^n\rangle = \langle 0^n|\left(\prod_{j\in\mathrm{Supp}(w)} V^\dagger Z_j V\right)|0^n\rangle = \langle 0^n|V^\dagger Z(w)V|0^n\rangle.$$

Thus,

$$\langle 0^n|V^\dagger Z(w)V|0^n\rangle \prod_{j=1}^{n}\langle 0^n|V^\dagger Z_j^{w_j}V|0^n\rangle = \langle 0^n|V^\dagger Z(w)V|0^n\rangle^2 \geq 0.$$

If there exists $j \in \text{Supp}(w)$ such that $V^\dagger Z_j V$ is not a $Z$-type Pauli, then $\langle 0^n|V^\dagger Z_j V|0^n\rangle = 0$, which implies that

$$\langle 0^n|V^\dagger Z(w)V|0^n\rangle \prod_{j=1}^{n} \langle 0^n|V^\dagger Z_j^{w_j} V|0^n\rangle = 0.$$

Therefore, in both cases,

$$\langle 0^n|V^\dagger Z(w)V|0^n\rangle \prod_{j=1}^{n} \langle 0^n|V^\dagger Z_j^{w_j} V|0^n\rangle \geq 0,$$

so

$$\mathop{\mathbb{E}}_{V\sim\mathcal{C}_\mathcal{A}} \left[\langle 0^n|V^\dagger Z(w)V|0^n\rangle \prod_{j=1}^{n} \langle 0^n|V^\dagger Z_j^{w_j} V|0^n\rangle\right] \geq 0.$$

□

We also show that for random Clifford circuits, the EBCG algorithm can never outperform the quantum simulation algorithm.

**Theorem 4.4.**

$$\text{XEB}_{\mathcal{C}_\mathcal{A}}(EBCG) \leq \text{XEB}_{\mathcal{C}_\mathcal{A}}(QS)$$

*Proof.* Recall that the quantum simulation algorithm achieves a score of

$$\text{XEB}_{\mathcal{C}_\mathcal{A}}(QS) = \frac{1}{2^n} \sum_{w\in\{0,1\}^n} \mathop{\mathbb{E}}_{V\sim\mathcal{C}_\mathcal{A}} \left[\langle 0^n|V^\dagger Z(w)V|0^n\rangle^2\right].$$

Let $V$ be an arbitrary Clifford circuit over the architecture $\mathcal{A}$, and let $w \in \{0,1\}^n$. If $\langle 0^n|V^\dagger Z(w)V|0^n\rangle = 0$, then

$$\langle 0^n|V^\dagger Z(w)V|0^n\rangle^2 = 0 = \langle 0^n|V^\dagger Z(w)V|0^n\rangle \prod_{j=1}^{n} \langle 0^n|V^\dagger Z_j^{w_j} V|0^n\rangle.$$

If $|\langle 0^n|V^\dagger Z(w)V|0^n\rangle| = 1$, then

$$\langle 0^n|V^\dagger Z(w)V|0^n\rangle^2 = 1 \geq \langle 0^n|V^\dagger Z(w)V|0^n\rangle \prod_{j=1}^{n} \langle 0^n|V^\dagger Z_j^{w_j} V|0^n\rangle.$$

Thus,

$$\begin{aligned}
\text{XEB}_{\mathcal{C}_\mathcal{A}}(EBCG) &= \frac{1}{2^n} \sum_{w\in\{0,1\}^n} \mathop{\mathbb{E}}_{V\sim\mathcal{C}_\mathcal{A}} \left[\langle 0^n|V^\dagger Z(w)V|0^n\rangle \prod_{j=1}^{n} \langle 0^n|V^\dagger Z_j^{w_j} V|0^n\rangle\right] \\
&\leq \frac{1}{2^n} \sum_{w\in\{0,1\}^n} \mathop{\mathbb{E}}_{V\sim\mathcal{C}_\mathcal{A}} \left[\langle 0^n|V^\dagger Z(w)V|0^n\rangle^2\right] \\
&= \text{XEB}_{\mathcal{C}_\mathcal{A}}(QS).
\end{aligned}$$

□

## 4.5 Random Fermionic Gaussian Unitary

In this section, we consider the EBCG expression w.r.t another classically efficiently simulable yet highly expressive subset of $\mathbb{U}(N)$ called the fermionic Gaussian unitaries. To begin, we give a purely algebraic definition of fermionic Gaussian unitaries and state a few of their key properties. For more detailed treatments taking into account the physics perspective, see [TD02] and [BG17]. Let $n \geq 1$. For every $j \in [n]$, define the so-called Majorana operators

$$c_{2j-1} = Z_1 \cdots Z_{j-1} X_j,$$
$$c_{2j} = Z_1 \cdots Z_{j-1} Y_j.$$

An $n$-qubit unitary $U$ is called a fermionic Gaussian unitary if there exists $R \in O(2n)$ such that for every $j \in [2n]$,

$$U c_j U^\dagger = \sum_{k=1}^{2n} R_{j,k} c_k. \tag{4.7}$$

Conversely, every $R \in O(2n)$ determines a unique fermionic Gaussian unitary $U$ up to global phase such that for every $j \in [2n]$,

$$U c_j U^\dagger = \sum_{k=1}^{2n} R_{j,k} c_k.$$

For example, for every $j \in [2n]$, $c_j$ is a fermionic Gaussian unitary, and we see that that its corresponding $R \in O(2n)$ is diagonal with $R_{j,j} = 1$ and $R_{k,k} = -1$ for every $k \in [2n] \setminus \{j\}$. Another primitive type of fermionic Gaussian unitaries are those that only conjugate non-trivially between a pair of Majorana operators. Namely, for every $j, k \in [2n], j \neq k$ and $\theta \in [0, 2\pi)$, we can define an $n$-qubit fermionic Gaussian unitary $U$ by its action

$$U c_j U^\dagger = (\cos\theta) c_j + (\sin\theta) c_k \quad \text{and} \quad U c_k U^\dagger = -(\sin\theta) c_j + (\cos\theta) c_k,$$

corresponding to Givens rotations acting non-trivially on the $(j, k)$-plane by an angle of $\theta$. We can also verify using (4.7) that for two $n$-qubit fermionic Gaussian unitaries $U$ and $V$ with corresponding orthogonal matrices $R$ and $S$,

$$V U c_j U^\dagger V^\dagger = \sum_{k=1}^{2n} (RS)_{j,k} c_k.$$

For every $R \in O(2n)$, by applying the QR factorization algorithm using Givens rotations to $R$ while also requiring the resulting upper-triangular matrix to be the identity, $R$ can be decomposed as a product of $O(n^2)$ Givens rotations and diagonal reflection operators. Consequently, every $n$-qubit fermionic Gaussian unitary can be decomposed as a product of $O(n^2)$ of the two types of primitive fermionic Gaussian unitaries defined above.

An $n$-qubit state $|\psi\rangle$ is called a fermionic Gaussian state if there exists a fermionic Gaussian unitary $U$ such that $|\psi\rangle = U|0^n\rangle$. Every $n$-qubit fermionic Gaussian state $|\psi\rangle$ is associated with a $2n \times 2n$ covariance matrix $M$ defined by its matrix elements

$$M_{j,k} = \frac{-i}{2} \langle\psi| c_j c_k - c_k c_j |\psi\rangle \tag{4.8}$$

for every $j, k \in [2n]$. Let $M_0$ denote the covariance matrix of $|0^n\rangle$. The following well-known properties of the covariance matrices of fermionic Gaussian states can be derived from (4.7) and (4.8).

**Lemma 4.2** ([TD02, Bra04, BG17])**.**

*(a) The covariance matrix of every fermionic Gaussian state is real skew-symmetric;*

*(b)*

$$M_0 = \bigoplus_{j=1}^{n} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix};$$

*(c) For every fermionic Gaussian state $|\psi\rangle$ with associated covariance matrix $M$, and for every fermionic Gaussian unitary $U$ with associated rotation matrix $R \in O(2n)$, the covariance matrix of $U|\psi\rangle$ is $RMR^T$.*

For every $2n \times 2n$ skew-symmetric matrix $M$, the Pfaffian of $M$ is defined by

$$\mathrm{pf}(M) = \frac{1}{2^n n!} \sum_{\sigma \in S_{2n}} \mathrm{sgn}(\sigma) \prod_{j=1}^{n} M_{\sigma(2j-1),\sigma(2j)}.$$

It is easy to verify from the definition that $\mathrm{pf}(aM) = a^n \mathrm{pf}(M)$ for every $2n \times 2n$ skew-symmetric matrix $M$ and $a \in \mathbb{C}$. For every $x \in \{0,1\}^{2n}$, define the Majornara monomial $c(x) = c_1^{x_1} c_2^{x_2} \cdots c_{2n}^{x_{2n}}$, and for every $2n \times 2n$ matrix $M$, let $M[x]$ denote the submatrix of $M$ that includes the $j$-th row and column if and only if $x_j = 1$.

**Lemma 4.3** ([TD02, BG17])**.** *For every $n$-qubit fermionic Gaussian state $|\psi\rangle$ with covariance matrix $M$, and for every $x \in \{0,1\}^{2n}$,*

$$\langle\psi|c(x)|\psi\rangle = \mathrm{pf}(iM[x]).$$

Let $\mathcal{U}(\mathbf{FG}_n)$ denote the uniform distribution over the set of all $n$-qubit fermionic Gaussian unitaries, and let $\mathcal{U}(O(2n))$ denote the uniform distribution over $O(2n)$. Similar to the Haar distribution over $\mathbb{U}(N)$, $\mathcal{U}(\mathbf{FG}_n)$ is invariant under left and right multiplication of arbitrary $U \in \mathbf{FG}_n$, and $\mathcal{U}(O(2n))$ is invariant under left and right multiplication of arbitrary $R \in O(2n)$. In the remainder of this section, we analyze the EBCG expression with expectation over $\mathcal{U}(\mathbf{FG}_n)$. For every $w \in \{0,1\}^n$, define $\bar{w} \in \{0,1\}^{2n}$ by $\bar{w}_{2j-1} = \bar{w}_{2j} = w_j$ for every $j \in [n]$.

**Lemma 4.4.** *For every $w \in \{0,1\}^n$ and every $n$-qubit fermionic Gaussian state $|\psi\rangle$ with covariance matrix $M$,*

$$\langle\psi|Z(w)|\psi\rangle = \mathrm{pf}(M[\bar{w}]).$$

*Proof.* Let $|\psi\rangle$ be an $n$-qubit fermionic Gaussian state, and let $w \in \{0,1\}^n$ with $k = |w|$. By the definition of the Majorana operators, it is easy to see that for every $j \in [n]$,

$$Z_j = -ic_{2j-1}c_{2j},$$

and more generally,

$$Z(w) = (-i)^k \prod_{j=1}^{n} c_{2j-1}^{w_j} c_{2j}^{w_j} = (-i)^k c(\bar{w}).$$

Thus, by Lemma 4.3,

$$\langle\psi|Z(w)|\psi\rangle = (-i)^k \langle\psi|c(\bar{w})|\psi\rangle = \mathrm{pf}(M[\bar{w}]).$$

□

**Lemma 4.5.** *For every $w \in \{0,1\}^n$ with $k = |w|$,*

$$\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)} \Big[\langle 0^n|U^\dagger Z(w)U|0^n\rangle \prod_{j=1}^{n} \langle 0^n|U^\dagger Z_j^{w_j} U|0^n\rangle\Big] = \frac{1}{(2k-1)!!} \mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)} \big[\langle 0^n|U^\dagger Z(w)U|0^n\rangle^2\big]$$

*where $(-1)!! = 1$.*

*Proof.* Let $w \in \{0,1\}^n$ with $k = |w|$. Let $L = \{\{1,2\},\{3,4\},\ldots,\{2k-1,2k\}\}$. For every $\sigma \in S_{2k}$, define

$$\sigma(L) = \{\{\sigma(1),\sigma(2)\},\{\sigma(3),\sigma(4)\},\ldots,\{\sigma(2k-1),\sigma(2k)\}\}.$$

Let $\Pi$ be the set of all partitions of $\{1,2,\ldots,2k\}$ into $k$ parts, each part of size 2. It is easy to see that $|\Pi| = \frac{(2k)!}{2^k k!} = (2k-1)!!$. For every $\alpha \in \Pi$, define $P_\alpha = \{\sigma \in S_{2k} : \sigma(L) = \alpha\}$. Let $M$ be a $2k \times 2k$ skew-symmetric matrix. We see that $\{P_\alpha : \alpha \in \Pi\}$ is a partition of $S_{2k}$ into $(2k-1)!!$ parts such that for every $\alpha \in \Pi$ and $\sigma,\tau \in P_\alpha$,

$$\mathrm{sgn}(\sigma) \prod_{j=1}^{k} M_{\sigma(2j-1),\sigma(2j)} = \mathrm{sgn}(\tau) \prod_{j=1}^{k} M_{\tau(2j-1),\tau(2j)}.$$

For every $\alpha \in \Pi$, let $\bar{\alpha}$ denote an arbitrary representative in $P_\alpha$. Then by the skew-symmetry of $M$, we get that

$$\mathrm{pf}(M) = \frac{1}{2^k k!} \sum_{\alpha\in\Pi} \sum_{\sigma\in P_\alpha} \mathrm{sgn}(\sigma) \prod_{j=1}^{k} M_{\sigma(2j-1),\sigma(2j)} = \sum_{\alpha\in\Pi} \mathrm{sgn}(\bar{\alpha}) \prod_{j=1}^{k} M_{\bar{\alpha}(2j-1),\bar{\alpha}(2j)}.$$

By Lemma 4.4,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)} \big[\langle 0^n|U^\dagger Z(w)U|0^n\rangle^2\big] \\
=&\mathop{\mathbb{E}}_{R\sim\mathcal{U}(O(2n))} \big[\mathrm{pf}((RM_0R^T)[\bar{w}])^2\big] \\
=&\sum_{\bar{\alpha}\in\Pi} \mathop{\mathbb{E}}_{R\sim\mathcal{U}(O(2n))} \Big[\mathrm{pf}((RM_0R^T)[\bar{w}])\mathrm{sgn}(\bar{\alpha}) \prod_{j=1}^{k} ((RM_0R^T)[\bar{w}])_{\bar{\alpha}(2j-1),\bar{\alpha}(2j)}\Big].
\end{aligned}$$

For every $\alpha \in \Pi$, there exists a permutation matrix $Q_{\bar{\alpha}} \in O(2n)$ such that

$$\begin{aligned}
&\mathop{\mathbb{E}}_{R\sim\mathcal{U}(O(2n))}\Big[\mathrm{pf}((RM_0R^T)[\bar{w}])\mathrm{sgn}(\bar{\alpha})\prod_{j=1}^{k}((RM_0R^T)[\bar{w}])_{\bar{\alpha}(2j-1),\bar{\alpha}(2j)}\Big]\\
=&\mathop{\mathbb{E}}_{R\sim\mathcal{U}(O(2n))}\Big[\mathrm{pf}((RQ_{\bar{\alpha}}M_0Q_{\bar{\alpha}}^TR^T)[\bar{w}])\prod_{j=1}^{k}((RQ_{\bar{\alpha}}M_0Q_{\bar{\alpha}}^TR^T)[\bar{w}])_{2j-1,2j}\Big]\\
=&\mathop{\mathbb{E}}_{R\sim\mathcal{U}(O(2n))}\Big[\mathrm{pf}((RM_0R^T)[\bar{w}])\prod_{j=1}^{k}((RM_0R^T)[\bar{w}])_{2j-1,2j}\Big].
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\left[\langle 0^n|U^\dagger Z(w)U|0^n\rangle^2\right]\\
=&(2k-1)!!\mathop{\mathbb{E}}_{R\sim\mathcal{U}(O(2n))}\Big[\mathrm{pf}((RM_0R^T)[\bar{w}])\prod_{j=1}^{k}((RM_0R^T)[\bar{w}])_{2j-1,2j}\Big]\\
=&(2k-1)!!\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\Big[\langle 0^n|U^\dagger Z(w)U|0^n\rangle\prod_{j=1}^{n}\langle 0^n|U^\dagger Z_j^{w_j}U|0^n\rangle\Big].
\end{aligned}$$

□

While Lemma 4.5 already implies the non-negativity of the EBCG expression for random fermionic Gaussian unitaries, we will be able to derive its exact value because Lemma 4.5 reduces computing the fermionic Gaussian EBCG expression to computing a second-moment expression of random fermionic Gaussian unitaries. At this point, it would be really nice if $\mathcal{U}(\mathbf{FG}_n)$ forms an exact unitary 2-design (recall Definition 2.1) mirroring that of random Clifford unitaries. However, our results below will imply the opposite. In fact, it is known that no random unitary distributions over the set of fermionic Gaussian unitaries can form an exact unitary 2-design in the sense of Definition 2.1 [BG17]. Inspired by a property of random Clifford unitaries known as Pauli mixing, Bravyi and Gosset defined a condition called Majorana mixing as an alternative for the 2-design property [BG17].

**Definition 4.1** ([BG17])**.** A random unitary distribution $\mathcal{D}$ over the set of all fermionic Gaussian unitaries is said to be Majorana mixing if for every $w \in \{0,1\}^{2n}$ with $k = |w|$,

$$\mathop{\mathbb{E}}_{U\sim\mathcal{D}}\left[(U\otimes U)(c(w)\otimes c(w))(U^\dagger\otimes U^\dagger)\right] = \binom{2n}{k}^{-1}\sum_{x\in\{0,1\}^{2n}:|x|=k} c(x)\otimes c(x).$$

**Lemma 4.6.** *$\mathcal{U}(\mathbf{FG}_n)$ is Majorana mixing.*

*Proof Sketch.* We provide a proof outline and leave some of the details to the reader. Similar to the proof of Lemma 2.1, We can show using the invariance property of $\mathcal{U}(\mathbf{FG}_n)$ that the superoperator

$$\Phi_{\mathbf{FG}} : A \mapsto \mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\left[(U\otimes U)A(U^\dagger\otimes U^\dagger)\right]$$

is an orthogonal projector and that for every $x, y \in \{0,1\}^{2n}$ such that $x \neq y$,

$$\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)} \left[(U\otimes U)(c(x)\otimes c(y))(U^\dagger\otimes U^\dagger)\right] = 0. \tag{4.9}$$

To show (4.9), for the case where $|x|$ and $|y|$ are both odd, we can consider $j \in [2n]$ such that $x_j = 1$ and $y_j = 0$. Then $c_j c(x) c_j = c(x)$ and $c_j c(y) c_j = -c(y)$. Thus,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)} \left[(U\otimes U)(c(x)\otimes c(y))(U^\dagger\otimes U^\dagger)\right] \\
&= \mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)} \left[((Uc_j)\otimes(Uc_j))(c(x)\otimes c(y))((Uc_j)^\dagger\otimes(Uc_j)^\dagger)\right] \\
&= -\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)} \left[(U\otimes U)(c(x)\otimes c(y))(U^\dagger\otimes U^\dagger)\right],
\end{aligned}$$

and this implies that

$$\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)} \left[(U\otimes U)(c(x)\otimes c(y))(U^\dagger\otimes U^\dagger)\right] = 0.$$

The other cases can be handled analogously. Let $w \in \{0,1\}^{2n}$ with $k = |w|$. The fact that $\Phi_{\mathbf{FG}}$ is a projector and (4.9) together imply that there exist coefficients $a_x \in \mathbb{C}$, $x \in \{0,1\}^{2n}$ such that

$$\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)} \left[(U\otimes U)(c(w)\otimes c(w))(U^\dagger\otimes U^\dagger)\right] = \sum_{x\in\{0,1\}^{2n}} a_x c(x)\otimes c(x) \tag{4.10}$$

and

$$\sum_{x\in\{0,1\}^{2n}} a_x = 1.$$

In the next step, we want to show that for an arbitrary $n$-qubit fermionic Gaussian unitary $U$,

$$Uc(w)U^\dagger = \sum_{x\in\{0,1\}^{2n}:|x|=k} \beta_x c(x) \tag{4.11}$$

for some coefficients $\beta_x \in \mathbb{C}$. Since every fermionic Gaussian unitary can be decomposed into a product of the two types of primitive unitaries described at the beginning of this section, it suffices to show (4.11) for those unitaries. Let $U$ be defined by

$$Uc_jU^\dagger = (\cos\theta)c_j + (\sin\theta)c_k \quad \text{and} \quad Uc_kU^\dagger = -(\sin\theta)c_j + (\cos\theta)c_k$$

for some $j, k \in [2n], j \neq k$ and some $\theta \in [0, 2\pi)$. For the case where $w_j = 1$ and $w_k = 1$, we have

$$\begin{aligned}
Uc(w)U^\dagger &= \pm \prod_{j\in\mathrm{Supp}(w)} Uc_jU^\dagger \\
&= \pm\Bigg(\prod_{p\in\mathrm{Supp}(w):p\neq j,k} c_p\Bigg)((\cos\theta)c_j + (\sin\theta)c_k)(-(\sin\theta)c_j + (\cos\theta)c_k) \\
&= \pm c(w)
\end{aligned}$$

where the $\pm$ phases are determined by the order in which the products are taken. The other cases can be handled analogously. Then, (4.10) and (4.11) together imply that

$$\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\left[(U\otimes U)(c(w)\otimes c(w))(U^\dagger\otimes U^\dagger)\right]=\sum_{x\in\{0,1\}^{2n}:|x|=k}a_x c(x)\otimes c(x).$$

To workout the values of $a_x$, we can use a symmetrization argument. We recall that $S_{2n}$ denotes the group of all permutations of $2n$ elements. For every $\pi\in S_{2n}$, $\pi$ can be represented by a permutation matrix $R_\pi\in O(2n)$ which defines a fermionic Gaussian unitary $V_\pi$ such that for every $x\in\{0,1\}^{2n}$, $V_\pi c(x)V_\pi^\dagger=c(x')$ where $x'$ is obtained from $x$ by permuting the bits of $x$ according to $\pi$. Thus, by the invariance property of $\mathcal{U}(\mathbf{FG}_n)$,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\left[(U\otimes U)(c(w)\otimes c(w))(U^\dagger\otimes U^\dagger)\right]\\
=&\frac{1}{(2n)!}\sum_{\pi\in S_{2n}}(V_\pi\otimes V_\pi)\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\left[(U\otimes U)(c(w)\otimes c(w))(U^\dagger\otimes U^\dagger)\right](V_\pi^\dagger\otimes V_\pi^\dagger)\\
=&\frac{1}{(2n)!}\sum_{\pi\in S_{2n}}\sum_{x\in\{0,1\}^{2n}:|x|=k}a_x(V_\pi\otimes V_\pi)(c(x)\otimes c(x))(V_\pi^\dagger\otimes V_\pi^\dagger)\\
=&\frac{1}{(2n)!}\sum_{y\in\{0,1\}^{2n}:|y|=k}\left(\sum_{x\in\{0,1\}^{2n}:|x|=k}a_x\frac{(2n)!}{\binom{2n}{k}}\right)c(y)\otimes c(y)\\
=&\binom{2n}{k}^{-1}\sum_{y\in\{0,1\}^{2n}:|y|=k}c(y)\otimes c(y).
\end{aligned}$$

□

**Theorem 4.5.** *For every $w\in\{0,1\}^n$ with $k=|w|$,*

$$\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\left[\langle 0^n|U^\dagger Z(w)U|0^n\rangle^2\right]=\frac{\binom{n}{k}}{\binom{2n}{2k}}.$$

*Proof.* Let $w\in\{0,1\}^n$ with $k=|w|$. Then by Lemma 4.6,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\left[\langle 0^n|U^\dagger Z(w)U|0^n\rangle^2\right]\\
=&(-i)^{2k}\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\left[\langle 0^{2n}|(U^\dagger\otimes U^\dagger)(c(\bar{w})\otimes c(\bar{w}))(U\otimes U)|0^{2n}\rangle\right]\\
=&(-i)^{2k}\binom{2n}{2k}^{-1}\sum_{y\in\{0,1\}^{2n}:|y|=2k}\langle 0^{2n}|(c(y)\otimes c(y))|0^{2n}\rangle\\
=&\frac{\binom{n}{k}}{\binom{2n}{2k}}.
\end{aligned}$$

□

Lemma 4.6 and Theorem 4.5 may find other independent applications. For example, Theorem 4.5 implies that $\mathcal{U}(\mathbf{FG}_n)$ is not an exact unitary 2-design as otherwise,

$$\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\left[\langle 0^n|U^\dagger Z(w)U|0^n\rangle^2\right]$$

should equal $\frac{1}{2^n+1}$ per Corollary 2.3. Finally, we arrive at the exact value of the EBCG expression for uniformly random fermionic Gaussian unitaries.

**Corollary 4.1.** *For every $w\in\{0,1\}^n$ with $k=|w|$,*

$$\mathop{\mathbb{E}}_{U\sim\mathcal{U}(\mathbf{FG}_n)}\left[\langle 0^n|U^\dagger Z(w)U|0^n\rangle\prod_{j=1}^{n}\langle 0^n|U^\dagger Z_j^{w_j}U|0^n\rangle\right]=\frac{(2(n-k)-1)!!}{(2n-1)!!}$$

*where $(-1)!!=1$.*

*Proof.* It easily follows from Lemma 4.5 and Theorem 4.5 with the double factorial identity $(2k-1)!!=\frac{(2k)!}{2^k k!}$ for every $k\geq 1$. □

We leave for future work to analyze the EBCG expression w.r.t random fermionic Gaussian circuits, which are random quantum circuits composed of random 2-qubit fermionic Gaussian gates.

# Bibliography


[AA11] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342, 2011.

[AAB+19] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A. Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574:505–510, 2019.

[AALV09] Dorit Aharonov, Itai Arad, Zeph Landau, and Umesh Vazirani. The detectability lemma and quantum gap amplification. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 417–426, 2009.

[Aar11] Scott Aaronson. A linear-optical proof that the permanent is# p-hard. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467(2136):3393–3405, 2011.

[AAV16] Anurag Anshu, Itai Arad, and Thomas Vidick. Simple proof of the detectability lemma and spectral gap amplification. *Physical Review B*, 93(20):205142, 2016.

[AB09] Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[AC16] Scott Aaronson and Lijie Chen. Complexity-theoretic foundations of quantum supremacy experiments. *arXiv preprint arXiv:1612.05903*, 2016.

[ADHW09] Anura Abeyesinghe, Igor Devetak, Patrick Hayden, and Andreas Winter. The mother of all protocols: Restructuring quantum information's family tree. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 465(2108):2537–2563, 2009.

[BCG20] Boaz Barak, Chi-Ning Chou, and Xun Gao. Spoofing linear cross-entropy benchmarking in shallow quantum circuits. *arXiv preprint arXiv:2005.02421*, 2020.

[BFLL21] Adam Bouland, Bill Fefferman, Zeph Landau, and Yunchao Liu. Noise and the frontier of quantum supremacy. *arXiv preprint arXiv:2102.01738*, 2021.

[BFNV18] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. Quantum supremacy and the complexity of random circuit sampling. *arXiv preprint arXiv:1803.04402*, 2018.

[BG17] Sergey Bravyi and David Gosset. Complexity of quantum impurity problems. *Communications in Mathematical Physics*, 356(2):451–500, 2017.

[BGM19] Sergey Bravyi, David Gosset, and Ramis Movassagh. Classical algorithms for quantum mean values. *arXiv preprint arXiv:1909.11485*, 2019.

[BH10] Fernando GSL Brandao and Michal Horodecki. Exponential quantum speed-ups are generic. *arXiv preprint arXiv:1010.3654*, 2010.

[BHH16] Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki. Local random quantum circuits are approximate polynomial-designs. *Communications in Mathematical Physics*, 346(2):397–434, 2016.

[BIS+18] Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J Bremner, John M Martinis, and Hartmut Neven. Characterizing quantum supremacy in near-term devices. *Nature Physics*, 14(6):595–600, 2018.

[BJS11] Michael J Bremner, Richard Jozsa, and Dan J Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467(2126):459–472, 2011.

[BM21] Sergey Bravyi and Dmitri Maslov. Hadamard-free circuits expose the structure of the clifford group. *IEEE Transactions on Information Theory*, 67(7):4546–4563, 2021.

[BMS16] Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. Average-case complexity versus approximate simulation of commuting quantum computations. *Physical review letters*, 117(8):080501, 2016.

[Bra04] Sergey Bravyi. Lagrangian representation for fermionic linear optics. *arXiv preprint quant-ph/0404180*, 2004.

[CMN21] Benoit Collins, Sho Matsumoto, and Jonathan Novak. The weingarten calculus. *arXiv preprint arXiv:2109.14890*, 2021.

[DCEL09] C Danker, R Cleve, J Emerson, and E Livine. Exact and approximate unitary 2-designs: Constructions and applications. *Physical Review A*, 80:012304, 2009.

[DHJB20] Alexander M Dalzell, Nicholas Hunter-Jones, and Fernando GSL Brandão. Random quantum circuits anti-concentrate in log depth. *arXiv preprint arXiv:2011.12277*, 2020.

[EAŻ05] Joseph Emerson, Robert Alicki, and Karol Życzkowski. Scalable noise estimation with random unitary operators. *Journal of Optics B: Quantum and Semiclassical Optics*, 7(10):S347, 2005.

[Gu13] Yinzheng Gu. Moments of random matrices and weingarten functions. Master's thesis, Queen's University, 2013.

[Har13] Aram W Harrow. The church of the symmetric subspace. *arXiv preprint arXiv:1308.6595*, 2013.

[HCY21] Hong-Ye Hu, Soonwon Choi, and Yi-Zhuang You. Classical shadow tomography with locally scrambled quantum dynamics. *arXiv preprint arXiv:2107.04817*, 2021.

[HHJ21] Jonas Haferkamp and Nicholas Hunter-Jones. Improved spectral gaps for random quantum circuits: large local dimensions and all-to-all interactions. *Physical Review A*, 104(2):022417, 2021.

[HKP20] Hsin-Yuan Huang, Richard Kueng, and John Preskill. Predicting many properties of a quantum system from very few measurements. *Nature Physics*, 16(10):1050–1057, 2020.

[HL09] Aram W Harrow and Richard A Low. Random quantum circuits are approximate 2-designs. *Communications in Mathematical Physics*, 291(1):257–302, 2009.

[HLSW04] Patrick Hayden, Debbie Leung, Peter W Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250(2):371–391, 2004.

[HM18] Aram Harrow and Saeed Mehraban. Approximate unitary $t$-designs by short random quantum circuits using nearest-neighbor and long-range gates. *arXiv preprint arXiv:1809.06957*, 2018.

[HP07] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of high energy physics*, 2007(09):120, 2007.

[KMM21] Yasuhiro Kondo, Ryuhei Mori, and Ramis Movassagh. Fine-grained analysis and improved robustness of quantum supremacy for random circuit sampling. *arXiv preprint arXiv:2102.01960*, 2021.

[Kna88] Stefan Knabe. Energy gaps and elementary excitations for certain vbs-quantum antiferromagnets. *Journal of statistical physics*, 52(3):627–638, 1988.

[Kni95] Emanuel Knill. Approximation by quantum circuits. *arXiv preprint quant-ph/9508006*, 1995.

[Kre21] William Kretschmer. The quantum supremacy tsirelson inequality. *Quantum*, 5:560, 2021.

[Lip91] Richard Lipton. New directions in testing. *Distributed computing and cryptography*, 2:191–202, 1991.

[LOB+21] Yunchao Liu, Matthew Otten, Roozbeh Bassirianjahromi, Liang Jiang, and Bill Fefferman. Benchmarking near-term quantum computers via random circuit sampling. *arXiv preprint arXiv:2105.05232*, 2021.

[MFIB18] Igor L Markov, Aneeqa Fatima, Sergei V Isakov, and Sergio Boixo. Quantum supremacy is both closer and farther than it appears. *arXiv preprint arXiv:1807.10749*, 2018.

[Mov18] Ramis Movassagh. Efficient unitary paths and quantum computational supremacy: A proof of average-case hardness of random circuit sampling. *arXiv preprint arXiv:1810.04681*, 2018.

[Nac96] Bruno Nachtergaele. The spectral gap for some spin chains with discrete symmetry breaking. *Communications in mathematical physics*, 175(3):565–606, 1996.

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[NLPD+19] John Napp, Rolando L La Placa, Alexander M Dalzell, Fernando GSL Brandao, and Aram W Harrow. Efficient classical simulation of random shallow 2d quantum circuits. *arXiv preprint arXiv:2001.00021*, 2019.

[NZO+21] Yoshifumi Nakata, Da Zhao, Takayuki Okuda, Eiichi Bannai, Yasunari Suzuki, Shiro Tamiya, Kentaro Heya, Zhiguang Yan, Kun Zuo, Shuhei Tamate, et al. Quantum circuits for exact unitary $t$-designs and applications to higher-order randomized benchmarking. *arXiv preprint arXiv:2102.12617*, 2021.

[Pre11] John Preskill. Quantum computing and the entanglement frontier. *arXiv preprint arXiv:1203.5813*, 2011.

[RY17] Daniel A Roberts and Beni Yoshida. Chaos and complexity by design. *Journal of High Energy Physics*, 2017(4):121, 2017.

[Sen06] Pranab Sen. Random measurement bases, quantum state distinction and applications to the hidden subgroup problem. In *21st Annual IEEE Conference on Computational Complexity (CCC'06)*, pages 14–pp. IEEE, 2006.

[Sho99] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[SR20] Jaime Sevilla and C Jess Riedel. Forecasting timelines of quantum computing. *arXiv preprint arXiv:2009.05045*, 2020.

[Sto85] Larry Stockmeyer. On approximation algorithms for #p. *SIAM Journal on Computing*, 14:849–861, 1985.

[TD02] Barbara M Terhal and David P DiVincenzo. Classical simulation of noninteracting-fermion quantum circuits. *Physical Review A*, 65(3):032325, 2002.

[Tod91] Seinosuke Toda. Pp is as hard as the polynomial-time hierarchy. *SIAM J. Comput.*, 20:865–877, 1991.

[Wat18] John Watrous. *The theory of quantum information*. Cambridge university press, 2018.

[Web15] Zak Webb. The clifford group forms a unitary 3-design. *arXiv preprint arXiv:1510.02769*, 2015.

[Zhu17] Huangjun Zhu. Multiqubit clifford groups are unitary 3-designs. *Physical Review A*, 96(6):062336, 2017.

[ZSW20] Yiqing Zhou, E Miles Stoudenmire, and Xavier Waintal. What limits the simulation of quantum computers? *Physical Review X*, 10(4):041038, 2020.

# Appendix A

# Useful Algebraic Identities

**Lemma A.1.**

$$\sum_{z\in\{0,1\}^n} |z\rangle\langle z| \otimes |z\rangle\langle z| = \frac{1}{2^n} \sum_{w\in\{0,1\}^n} Z(w) \otimes Z(w)$$

*Proof.* First recall that

$$|00\rangle\langle 00| = (|0\rangle\langle 0|) \otimes (|0\rangle\langle 0|) = \left(\frac{I+Z}{2}\right) \otimes \left(\frac{I+Z}{2}\right) = \frac{I\otimes I + I\otimes Z + Z\otimes I + Z\otimes Z}{4}$$

and

$$|11\rangle\langle 11| = (|1\rangle\langle 1|) \otimes (|1\rangle\langle 1|) = \left(\frac{I-Z}{2}\right) \otimes \left(\frac{I-Z}{2}\right) = \frac{I\otimes I - I\otimes Z - Z\otimes I + Z\otimes Z}{4}.$$

Thus,

$$\begin{aligned}
\sum_{z\in\{0,1\}^n} (|z\rangle\langle z|)_A \otimes (|z\rangle\langle z|)_B &= \sum_{z\in\{0,1\}^n} (|z\rangle_A \otimes |z\rangle_B)(\langle z|_A \otimes \langle z|_B) \\
&= (|0_A 0_B\rangle\langle 0_A 0_B| + |1_A 1_B\rangle\langle 1_A 1_B|)^{\otimes n} \\
&= \left(\frac{I_A \otimes I_B + Z_A \otimes Z_B}{2}\right)^{\otimes n} \\
&= \frac{1}{2^n} \sum_{w\in\{0,1\}^n} Z(w)_A \otimes Z(w)_B.
\end{aligned}$$

□

**Lemma A.2.**

$$\sum_{z\in\{0,1\}^n} \left(\bigotimes_{k=1}^n |z_k\rangle\langle z_k|\right) \otimes \left(\bigotimes_{j=1}^n (|z_j\rangle\langle z_j|)_j\right) = \frac{1}{2^n} \sum_{w\in\{0,1\}^n} Z(w) \otimes \left(\bigotimes_{j=1}^n Z_j^{w_j}\right)$$

*Proof.*

$$\sum_{z\in\{0,1\}^n} \left(\bigotimes_{k=1}^n |z_k\rangle\langle z_k|\right) \otimes \left(\bigotimes_{j=1}^n (|z_j\rangle\langle z_j|)_j\right)$$

$$
\begin{aligned}
&= \bigotimes_{j=1}^{n} ((|0\rangle\langle 0|) \otimes (|0\rangle\langle 0|)_j + (|1\rangle\langle 1|) \otimes (|1\rangle\langle 1|)_j) \\
&= \bigotimes_{j=1}^{n} \left( \left( \frac{I+Z}{2} \right) \otimes \left( \frac{I_j + Z_j}{2} \right) + \left( \frac{I-Z}{2} \right) \otimes \left( \frac{I_j - Z_j}{2} \right) \right) \\
&= \bigotimes_{j=1}^{n} \frac{I \otimes I_j + Z \otimes Z_j}{2} \\
&= \frac{1}{2^n} \sum_{w \in \{0,1\}^n} Z(w) \otimes \left( \bigotimes_{j=1}^{n} Z_j^{w_j} \right)
\end{aligned}
$$

□

## A.1 Products of Orthogonal Projectors

**Lemma A.3.** *For every orthogonal projector $P$ and $Q$, and every state $|x\rangle$,*

*(a) if $PQ|x\rangle = |x\rangle$, then $P|x\rangle = |x\rangle$ and $Q|x\rangle = |x\rangle$;*

*(b) the set of non-trivial eigenvalues of $PQ$ and $PQP$ are the same counting multiplicity;*

*(c) the set of eigenvalues of $PQ$ fall in $[0, 1]$.*

*Proof.*

(a) Since $P$ and $Q$ are orthogonal projectors, $PQ|x\rangle = |x\rangle \implies PQ|x\rangle = P|x\rangle \implies P|x\rangle = |x\rangle$. Since $\||x\rangle\| = \|PQ|x\rangle\| \leq \|Q|x\rangle\| \leq \||x\rangle\|$, $Q|x\rangle = |x\rangle$.

(b) Let $\lambda \neq 0$ such that $PQ|x\rangle = \lambda|x\rangle$. Then $PQ|x\rangle = \lambda P|x\rangle$, so $PQP|x\rangle = \frac{1}{\lambda} PQPQ|x\rangle = \lambda|x\rangle$. Let $\lambda \neq 0$ such that $PQP|x\rangle = \lambda|x\rangle$. Then $PQP|x\rangle = \lambda P|x\rangle \implies P|x\rangle = |x\rangle \implies PQ|x\rangle = \lambda|x\rangle$.

(c) Let $PQ|x\rangle = \lambda|x\rangle$. Then $|\lambda| \cdot \||x\rangle\| = \|PQ|x\rangle\| \leq \||x\rangle\| \implies |\lambda| \leq 1$. Part 2 implies $\lambda \geq 0$.

□