

Random Quantum Circuits are Approximate 2-designs

Aram W. Harrow and Richard A. Low*

Department of Computer Science, University of Bristol, Bristol, U.K.

May 28, 2018

Abstract

Given a universal gate set on two qubits, it is well known that applying random gates from the set to random pairs of qubits will eventually yield an approximately Haar-distributed unitary. However, this requires exponential time. We show that random circuits of only polynomial length will approximate the first and second moments of the Haar distribution, thus forming approximate 1- and 2-designs. Previous constructions required longer circuits and worked only for specific gate sets. As a corollary of our main result, we also improve previous bounds on the convergence rate of random walks on the Clifford group.

1 Introduction: Pseudo-Random Quantum Circuits

There are many examples of algorithms that make use of random states or unitary operators (e.g. [5, 28]). However, exactly sampling from the uniform Haar distribution is inefficient. In many cases, though, only pseudo-random operators are required. To quantify the extent to which the pseudo-random operators behave like the uniform distribution we use the notion of *k-designs* (often referred to as *t-designs*). A *k*-design has *k*th moments equal to those of the Haar distribution. For most uses of random states or unitaries, this is sufficient. Constructions of exact *k*-designs on states are known (see [3] and references therein) and some are efficient. Ambainis and Emerson [3] introduced the notion of approximate state *k*-designs, which can be implemented efficiently for any *k*. However, the known constructions of unitary *k*-designs are inefficient to implement. Approximate unitary 2-designs have been considered [14, 10, 18], although the approaches are specific to 2-designs.

We consider a general class of random circuits where a series of two-qubit gates are chosen from a universal gate set. We give a framework for analysing the *k*th moments of these circuits. Our conjecture, based on an analogous classical result [23], is that a random circuit on *n* qubits of length $\text{poly}(n, k)$ is an approximate *k*-design. While we do not prove this, we instead give a tight analysis of the *k* = 2 case. We find that in a broad class of natural random circuit models (described in Section 1.1), a circuit of length $O(n(n + \log 1/\epsilon))$ yields an ϵ -approximate 2-design. Our definition of an approximate *k*-design is in Section 2.2. Our results also apply to an alternative definition of an approximate 2-design from [10], for which we show random circuits of length $O(n(n + \log 1/\epsilon))$ yield

*low@cs.bris.ac.uk

ϵ -approximations, thus extending the results of that paper to a larger class of circuits. Moreover, our results also apply to random stabiliser circuits, meaning that a random stabiliser circuit of length $O(n(n + \log 1/\epsilon))$ will be an ϵ -approximate 2-design. This both simplifies the construction and tightens the efficiency of the approach of [14], which constructed ϵ -approximate 2-designs in time $O(n^6(n^2 + \log 1/\epsilon))$ using $O(n^3)$ elementary quantum gates.

1.1 Random Circuits

The random circuit we will use is the following. Choose a 2-qubit gate set that is universal on $U(4)$ (or on the stabiliser subgroup of $U(4)$). One example of this is the set of all one qubit gates together with the controlled-NOT gate. Another is simply the set of all of $U(4)$. Then, at each step, choose a random pair of qubits and apply a gate from the universal set chosen uniformly at random. For the $U(4)$ case, the distribution will be the Haar measure on $U(4)$. One such circuit is shown in Fig. 1 for $n = 4$ qubits. This is based on the approach used in Refs. [26, 9] but our analysis is both simpler and more general.

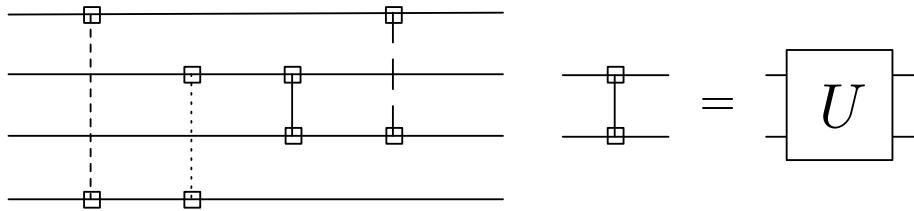


Figure 1: An example of a random circuit. Different lines indicate a different gate is applied at each step.

Since the universal set can generate the whole of $U(2^n)$ in this way, such random circuits can produce any unitary. Further, since this process converges to a unitarily invariant distribution and the Haar distribution is unique, the resulting unitary must be uniformly distributed amongst all unitaries [15]. Therefore this process will eventually converge to a Haar distributed unitary from $U(2^n)$. This is proven rigorously in Lemma 3.7. However, a generic element of $U(2^n)$ has 4^n real parameters, and thus to even have $\Omega(4^{-n})$ fidelity with the Haar distribution requires $\Omega(4^n)$ 2-qubit unitaries. We address this problem by considering only the lower-order moments of the distribution and showing these are nearly the same for random circuits as for Haar-distributed unitaries. This claim is formally described in Theorem 2.10.

Our paper is organised as follows. In Section 2 we define unitary k -designs and explain how a random circuit could be used to construct a k -design. In Section 3 we work out how the state evolves after a single step of the random circuit. We then extend this to multiple steps in Section 4 and prove our general convergence results. A key simplification will be (following [26]) to map the evolution of the second moments of the quantum circuit onto a classical Markov chain. We then prove a tight convergence result for the case where the gates are chosen from $U(4)$ in Section 5. This section contains most of the technical content of the paper. Using our bounds on mixing time we put together the proof that random circuits yield approximate unitary 2-designs in Section 6. Section 7 concludes with some discussion of applications.

2 Preliminaries

2.1 Pauli expansion

Much of the following will be done in the Pauli basis. The Pauli operators will be taken as $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ and defined to be

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

If $|\psi\rangle \in \mathbb{C}^{2^n}$ is a state on n qubits then we write $\psi = |\psi\rangle\langle\psi|$. We can expand ψ in the Pauli basis as

$$\psi = 2^{-n/2} \sum_p \gamma(p) \sigma_p \quad (2.1)$$

where $\sigma_p = \sigma_{p_1} \otimes \dots \otimes \sigma_{p_n}$ for the string $p = p_1 \dots p_n$. Inverting, the coefficients $\gamma(p)$ are given by

$$\gamma(p) = 2^{-n/2} \text{tr } \sigma_p \psi. \quad (2.2)$$

It is easy to show that the coefficients $\gamma(p)$ are real and, with the chosen normalisation, the squares sum to $\text{tr } \psi^2$, which is 1 for pure ψ . In general

$$\sum_p \gamma^2(p) \leq 1$$

with equality if and only if ψ is pure. Note also that $\text{tr } \psi = 1$ is equivalent to $\gamma(0) = 2^{-n/2}$.

This notation is extended to states on nk qubits by treating γ as a function of k strings from $\{0, 1, 2, 3\}^n$. Thus a state ρ on nk qubits is written as

$$\rho = 2^{-nk/2} \sum_{p_1, \dots, p_k} \gamma_0(p_1, \dots, p_k) \sigma_{p_1} \otimes \dots \otimes \sigma_{p_k}. \quad (2.3)$$

2.2 k -designs

We will say that a k -design is efficient if the effort required to sample a state or unitary from the design is polynomial in n and k . Note that we do not require the number of states to be polynomial because, even for approximate unitary designs, an exponential number of unitaries is required. Rather, the number of random bits needed to specify an element of the design should be $\text{poly}(n, k)$.

2.2.1 State designs

A (state) k -design is an ensemble of states such that, when one state is chosen from the ensemble and copied k times, it is indistinguishable from a uniformly random state. This is a way of quantifying the pseudo-randomness of the state and is a quantum analogue of k -wise independence. Hayashi et al. [20] give an inefficient construction of k -designs for any n and k .

The state k -design definition we use is due to Ref. [3]:

Definition 2.1. An ensemble of quantum states $\{p_i, |\psi_i\rangle\}$ is a state k -design if

$$\sum_i p_i (|\psi_i\rangle\langle\psi_i|)^{\otimes k} = \int_{\psi} (|\psi\rangle\langle\psi|)^{\otimes k} d\psi \quad (2.4)$$

where the integration is taken over the left invariant Haar measure on the unit sphere in \mathbb{C}^d , normalised so that $\int_{\psi} d\psi = 1$.

It is well known that the above integral is equal to $\frac{\Pi_{+k}}{\binom{k+d-1}{k}}$, where Π_{+k} is the projector onto the symmetric subspace of k d -dimensional spaces. For a rigorous proof, see Ref. [16] and for a less precise proof but from a quantum information perspective see Ref. [7].

2.2.2 Unitary designs

A unitary k -design is, in a sense, a stronger version of a state design. Just as applying a Haar-random unitary to an arbitrary pure state results in a uniformly random pure state, applying a unitary chosen from a unitary k -design to an arbitrary pure state should result in a state k -design. Another way to say this is that the state obtained by acting $U^{\otimes k}$, where U is drawn from a unitary k -design on $U(d)$, on any d^k -dimensional state should be indistinguishable from the case where U is drawn uniformly from $U(d)$. Formally, we have:

Definition 2.2. Let $\{p_i, U_i\}$ be an ensemble of unitary operators. Define

$$\mathcal{G}_W(\rho) = \sum_i p_i U_i^{\otimes k} \rho (U_i^{\dagger})^{\otimes k} \quad (2.5)$$

and

$$\mathcal{G}_H(\rho) = \int_U U^{\otimes k} \rho (U^{\dagger})^{\otimes k} dU. \quad (2.6)$$

Then the ensemble is a unitary k -design iff $\mathcal{G}_W = \mathcal{G}_H$.

Unitary designs can also be defined in terms of polynomials, so that if p is a polynomial with degree k in the matrix elements of U and k in the matrix elements of U^* , then averaging p over a unitary k -design should give the same answer as averaging over the Haar measure. To see the equivalence with Definition 2.2 note that averaging a monomial over our ensemble can be expressed as $\langle i_1, \dots, i_k | \mathcal{G}_W(|j_1, \dots, j_k\rangle\langle j'_1, \dots, j'_k|) | i'_1, \dots, i'_k \rangle$, and so if $\mathcal{G}_W = \mathcal{G}_H$ then any polynomial of degree k will have the same expectation over both distributions.

2.3 Approximate k -designs

2.3.1 Approximate state designs

Numerous examples of exact efficient state 2-design constructions are known (e.g. [8]) but general exact constructions are not efficient in n and k . Approximate state designs were first introduced by Ambainis and Emerson [3] and they constructed efficient approximate state k -designs for any k . Aaronson [1] also gives an efficient approximate construction.

We define approximate state designs as follows.

Definition 2.3. An ensemble of quantum states $\{p_i, |\psi_i\rangle\}$ is an ϵ -approximate state k -design if

$$(1 - \epsilon) \int_{\psi} (|\psi\rangle\langle\psi|)^{\otimes k} d\psi \leq \sum_i p_i (|\psi_i\rangle\langle\psi_i|)^{\otimes k} \leq (1 + \epsilon) \int_{\psi} (|\psi\rangle\langle\psi|)^{\otimes k} d\psi \quad (2.7)$$

In [3], a similar definition was proposed but with the additional requirement that the ensemble also forms a 1-design (exactly), i.e.

$$\sum_i p_i |\psi_i\rangle\langle\psi_i| = \int_{\psi} |\psi\rangle\langle\psi| d\psi$$

This requirement was necessary there only so that a suitably normalised version of the ensemble would form a POVM. We will not use it.

By taking the partial trace one can show that a k -design is a k' -design for $k' \leq k$. Thus approximate k -designs are always at least approximate 1-designs.

2.3.2 Approximate unitary designs

It was shown in Ref. [4] that a quantum analogue of a one time pad requires $2n$ bits to exactly randomise an n qubit state. However, in Ref. [5] it was shown that $n + o(n)$ bits suffice to do this approximately. Translated into k -design language, this says an exact unitary 1-design requires 2^{2n} unitaries but can be done approximately with $2^{n+o(n)}$. So approximate designs can have fewer unitaries than exact designs. Here, we are interested in improving the efficiency of implementing the unitaries. There are no known efficient exact constructions of unitary k -designs; it is hoped that our approach will yield approximate unitary designs efficiently.

We will require approximate unitary k -designs to be close in the diamond norm [24]:

Definition 2.4. The diamond norm of a superoperator T

$$\|T\|_{\diamond} = \sup_d \|T \otimes id_d\|_{\infty} = \sup_d \sup_{X \neq 0} \frac{\|(T \otimes id_d)X\|_1}{\|X\|_1}$$

where id_d is the identity channel on d dimensions.

Operationally, the diamond norm of the difference between two quantum operations tells us the largest possible probability of distinguishing the two operations if we are allowed to have them act on part of an arbitrary, possibly entangled, state. In the supremum over ancilla dimension d , it can be shown that d never needs to be larger than the dimension of the system that T acts upon. The diamond norm is closely related to completely bounded norms (cb-norms), in that $\|T\|_{\diamond}$ is the cb-norm of T^{\dagger} and can also be interpreted as the $L_1 \rightarrow L_1$ cb-norm of T itself [11, 27].

We can now define approximate unitary k -designs.

Definition 2.5. \mathcal{G}_W is an ϵ -approximate unitary k -design if

$$\|\mathcal{G}_W - \mathcal{G}_H\|_{\diamond} \leq \epsilon, \quad (2.8)$$

where \mathcal{G}_W and \mathcal{G}_H are defined in Definition 2.2.

In Ref. [10], they consider approximate twirling, which is implemented using an approximate 2-design. They give an alternative definition of closeness which is more convenient for this application:

Definition 2.6 ([10]). *Let $\{p_i, U_i\}$ be an ensemble of unitary operators. Then this ensemble is an ϵ -approximate twirl if*

$$\max_{\Lambda} \left\| \mathbb{E}_W W(\Lambda(W^\dagger \rho W))W^\dagger - \mathbb{E}_U U(\Lambda(U^\dagger \rho U))U^\dagger \right\|_\diamond \leq \frac{\epsilon}{d^2} \quad (2.9)$$

where the first expectation is over W chosen from the ensemble and the second is the Haar average. The maximisation is over channels Λ and d is the dimension (2^n in our case).

Our results work for both definitions with the same efficiency.

2.4 Random Circuits as k -designs

If a random circuit is to be an approximate k -design then Eqn. 2.8 must be satisfied where the U_i are the different possible random circuits. We can think of this as applying the random circuit not once but k times to k different systems.

Suppose that applying t random gates yields the random circuit W . If $W^{\otimes k}$ acts on an nk -qubit state ρ , then following the notation of Eqn. 2.8, the resulting state is

$$\rho_W := W^{\otimes k} \rho (W^\dagger)^{\otimes k} = 2^{-nk/2} \sum_{p_1, \dots, p_k} \gamma_0(p_1, \dots, p_k) W \sigma_{p_1} W^\dagger \otimes \dots \otimes W \sigma_{p_k} W^\dagger. \quad (2.10)$$

For this to be a k -design, the expectation over all choices of random circuit should match the expectation over Haar-distributed $W \in U(2^n)$.

We are now ready to state our main results. Our results apply to a large class of gate sets which we define below:

Definition 2.7. *Let $\mathcal{E} = \{p_i, U_i\}$ be a discrete ensemble of elements from $U(d)$. Define an operator $G_{\mathcal{E}}$ by*

$$G_{\mathcal{E}} := \sum_i p_i U_i^{\otimes k} \otimes (U_i^*)^{\otimes k} \quad (2.11)$$

More generally, we can consider continuous distributions. If μ is a probability measure on $U(d)$ then we can define G_{μ} by analogy as

$$G_{\mu} := \int_{U(d)} d\mu(U) U^{\otimes k} \otimes (U^*)^{\otimes k} \quad (2.12)$$

Then \mathcal{E} (or μ) is k -copy gapped if $G_{\mathcal{E}}$ (or G_{μ}) has only $k!$ eigenvalues with absolute value equal to 1.

For any discrete ensemble $\mathcal{E} = \{p_i, U_i\}$, we can define a measure $\mu = \sum_i p_i \delta_{U_i}$. Thus, it suffices to state our theorems in terms of μ and G_{μ} .

The condition on G_{μ} in the above definition may seem somewhat strange. We will see in Section 3 that when $d \geq k$ there is a $k!$ -dimensional subspace of $(\mathbb{C}^d)^{\otimes 2k}$ that is acted upon trivially by any

G_μ . Additionally, when μ is the Haar measure on $U(d)$ then G_μ is the projector onto this space. Thus, the k -copy gapped condition implies that vectors orthogonal to this space are shrunk by G_μ .

We will see that G_μ is k -copy gapped in a number of important cases. First, we give a definition of universality that can apply not only to discrete gates sets, but to arbitrary measures on $U(4)$.

Definition 2.8. *Let μ be a distribution on $U(4)$. Suppose that for any open ball $S \subset U(4)$ there exists a positive integer ℓ such that $\mu^{\star\ell}(S) > 0$. Then we say μ is universal [for $U(4)$].*

Here $\mu^{\star\ell}$ is the ℓ -fold convolution of μ with itself; i.e.

$$\mu^{\star\ell} = \int \delta_{U_1 \dots U_\ell} d\mu(U_1) \cdots d\mu(U_\ell).$$

When μ is a discrete distribution over a set $\{U_i\}$, Definition 2.8 is equivalent to the usual definition of universality for a finite set of unitary gates.

Theorem 2.9. *The following distributions on $U(4)$ are k -copy gapped:*

- (i) Any universal gate set. Examples are $U(4)$ itself, any entangling gate together with all single qubit gates, or the gate set considered in [26].
- (ii) Any approximate (or exact) unitary k -design on 2 qubits, such as the uniform distribution over the 2-qubit Clifford group, which is an exact 2-design.

Proof.

(i) This is proven in Lemma 3.7.

(ii) This follows straight from Definition 2.2. \square

Theorem 2.10. *Let μ be a 2-copy gapped distribution and W be a random circuit on n qubits obtained by drawing t random unitaries according to μ and applying each of them to a random pair of qubits. Then there exists C (depending only on μ) such that for any $\epsilon > 0$ and any $t \geq C(n(n + \log 1/\epsilon))$, \mathcal{G}_W is an ϵ -approximate unitary 2-design according to either Definition 2.5 or Definition 2.6.*

To prove Theorem 2.10, we show that the second moments of the random circuits converge quickly to those of a uniform Haar distributed unitary. For W a circuit as in Theorem 2.10, write $\gamma_W(p_1, p_2)$ for the Pauli coefficients of $\rho_W = W^{\otimes 2} \rho (W^\dagger)^{\otimes 2}$. Then write $\gamma_t(p_1, p_2) = \mathbb{E}_W \gamma_W(p_1, p_2)$ where W is a circuit of length t . Then we have

Lemma 2.11. *Let μ and W be as in Theorem 2.10. Let the initial state be ρ with $\gamma_0(p, p) \geq 0$ and $\sum_p \gamma_0(p, p) = 1$ (for example the state $|\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi|$ for any pure state $|\psi\rangle$). Then there exists a constant C (possibly depending on μ) such that for any $\epsilon > 0$*

(i)

$$\sum_{\substack{p_1, p_2 \\ p_1 p_2 \neq 00}} \left(\gamma_t(p_1, p_2) - \delta_{p_1 p_2} \frac{1}{2^n (2^n + 1)} \right)^2 \leq \epsilon \quad (2.13)$$

for $t \geq Cn \log 1/\epsilon$.

(ii)

$$\sum_{\substack{p_1, p_2 \\ p_1 p_2 \neq 00}} \left| \gamma_t(p_1, p_2) - \delta_{p_1 p_2} \frac{1}{2^n (2^n + 1)} \right| \leq \epsilon \quad (2.14)$$

for $t \geq Cn(n + \log 1/\epsilon)$ or, when μ is the uniform distribution on $U(4)$ or its stabiliser subgroup, $t \geq Cn \log \frac{n}{\epsilon}$.

We can then extend this to all states by a simple corollary:

Corollary 2.12. *Let μ , W and γ_W be as in Lemma 2.11. Then, for any initial state $\rho = \frac{1}{2^n} \sum_{p_1, p_2} \gamma_0(p_1, p_2) \sigma_{p_1} \otimes \sigma_{p_2}$, there exists a constant C (possibly depending on μ) such that for any $\epsilon > 0$*

(i)

$$\sum_{\substack{p_1, p_2 \\ p_1 p_2 \neq 00}} \left(\gamma_t(p_1, p_2) - \delta_{p_1 p_2} \frac{\sum_{p \neq 0} \gamma_0(p, p)}{4^n - 1} \right)^2 \leq \epsilon \quad (2.15)$$

for $t \geq Cn(n + \log 1/\epsilon)$.

(ii)

$$\sum_{\substack{p_1, p_2 \\ p_1 p_2 \neq 00}} \left| \gamma_t(p_1, p_2) - \delta_{p_1 p_2} \frac{\sum_{p \neq 0} \gamma_0(p, p)}{4^n - 1} \right| \leq \epsilon \quad (2.16)$$

for $t \geq Cn(n + \log 1/\epsilon)$.

By the usual definition of an approximate design (Definition 2.5), we only need convergence in the 2-norm (Eqn. 2.15), which is implied by 1-norm convergence (Eqn. 2.16) but weaker. However, Definition 2.6, which requires the map to be close to the twirling operation, requires 1-norm convergence (i.e. Eqn. 2.16). Thus, Theorem 2.10 for Definition 2.5 follows from Corollary 2.12(i) and Theorem 2.10 for Definition 2.6 follows from Corollary 2.12(ii). Theorem 2.10 is proved in Section 6 and Corollary 2.12 in Section 4.

We note that, in the course of proving Lemma 2.11, we prove that the eigenvalue gap (defined in Section 4.3) of the Markov chain that gives the evolution of the $\gamma(p, p)$ terms is $O(1/n)$. It is easy to show that this bound is tight for some gate sets.

Related work: Here we summarise the other efficient constructions of approximate unitary 2-designs.

- The uniform distribution over the Clifford group on n qubits is an exact 2-design [14]. Moreover, [14] described how to sample from the Clifford group using $O(n^8)$ classical gates and $O(n^3)$ quantum gates. Our results show that applying $O(n(n + \log 1/\epsilon))$ random two-qubit Clifford gates also achieve an ϵ -approximate 2-design (although not necessarily a distribution that is within ϵ of uniform on the Clifford group).
- Dankert et al. [10] gave a specific circuit construction of an approximate 2-design. To achieve small error in the sense of Definition 2.5, their circuits require the same $O(n(n + \log 1/\epsilon))$ gates that our random circuits do. However, when we use Definition 2.6, the circuits from [10] only need $O(n \log 1/\epsilon)$ gates while the random circuits analysed in this paper need to be length $O(n(n + \log 1/\epsilon))$.

- The closest results to our own are in the papers by Oliveira et al. [26, 9], which considered a specific gate set (random single qubit gates and a controlled-NOT) and proved that the second moments converge in time $O(n^2(n + \log 1/\epsilon))$. Our strategy of analysing random quantum circuits in terms of classical Markov chains is also adapted from [26, 9]. In Section 3, we generalise this approach to analyse the k^{th} moments for arbitrary k .

The main results of our paper extend the results of [26, 9] to a larger class of gate sets and improve their convergence bounds. Some of these improvements have been conjectured by [30], which presented numerical evidence in support of them.

3 Analysis of the Moments

In order to prove our results, we need to understand how the state evolves after each step of the random circuit. In this section we consider just one step and a fixed pair of qubits. Later on we will extend this to prove convergence results for multiple steps with random pairs of qubits drawn at every step. We consider first the Haar distribution over the full unitary group and then will discuss the more general case of any 2-copy gapped distribution.

In this section, we work in general dimension d and with a general Hermitian orthogonal basis $\sigma_0, \dots, \sigma_{d^2-1}$. Later we will take d to be either 4 or 2^n and the σ_i to be Pauli matrices. However, in this section we keep the discussion general to emphasise the potentially broader applications.

Fix an orthonormal basis for $d \times d$ Hermitian matrices: $\sigma_0, \dots, \sigma_{d^2-1}$, normalised so that $\text{tr } \sigma_p \sigma_q = d \delta_{p,q}$. Let σ_0 be the identity. We need to evaluate the quantity

$$\mathbb{E}_U \left(U^{\otimes k} \sigma_{p_1} \otimes \dots \otimes \sigma_{p_k} (U^\dagger)^{\otimes k} \right) =: T(\mathbf{p}) \quad (3.1)$$

where the expectation is over Haar distributed $U \in U(d)$. We will need this quantity in two cases. Firstly, for $d = 2^n$, these are the moments obtained after applying a uniformly distributed unitary so we know what the random circuit must converge to. Secondly, for $d = 4$, this tells us how a random $U(4)$ gate acts on any chosen pair.

Call the quantity in Eqn. 3.1 $T(\mathbf{p})$ (we use **bold** to indicate a k -tuple of coefficients; take $\mathbf{p} = (p_1, \dots, p_k)$) and write it in the σ_p basis as

$$T(\mathbf{p}) = \sum_{\mathbf{q}} \hat{G}(\mathbf{q}; \mathbf{p}) \sigma_{q_1} \otimes \dots \otimes \sigma_{q_k}. \quad (3.2)$$

Here, $\hat{G}(\mathbf{q}; \mathbf{p})$ is the coefficient in the Pauli expansion of $T(\mathbf{p})$ and we define \hat{G} as the matrix with entries equal to $\hat{G}(\mathbf{q}; \mathbf{p})$. We have left off the usual normalisation factor because, as we shall see, with this normalisation \hat{G} is a projector. Inverting this, we have

$$\begin{aligned} \hat{G}(\mathbf{q}; \mathbf{p}) &= d^{-k} \text{tr} (\sigma_{q_1} \otimes \dots \otimes \sigma_{q_k} T(\mathbf{p})) \\ &= d^{-k} \mathbb{E}_U \text{tr} \left((\sigma_{q_1} \otimes \dots \otimes \sigma_{q_k}) U^{\otimes k} (\sigma_{p_1} \otimes \dots \otimes \sigma_{p_k}) (U^\dagger)^{\otimes k} \right) \end{aligned} \quad (3.3)$$

Note that \hat{G} is real since T and the basis are Hermitian.

We can gain all the information we need about the Haar integral in Eqn. 3.1 with the following observations:

Lemma 3.1. $T(\mathbf{p})$ commutes with $U^{\otimes k}$ for any unitary U .

Proof. Follows from the invariance of the Haar measure on the unitary group. \square

Corollary 3.2. $T(\mathbf{p})$ is a linear combination of permutations from the symmetric group S_k .

Proof. This follows from Schur-Weyl duality (see e.g. [16]). \square

From this, we can prove that \hat{G} is a projector and find its eigenvectors.

Theorem 3.3. \hat{G} is symmetric, i.e. $\hat{G}(\mathbf{q}; \mathbf{p}) = \hat{G}(\mathbf{p}; \mathbf{q})$.

Proof. Follows from the invariance of the trace under cyclic permutations. \square

Theorem 3.4. P_π is an eigenvector of \hat{G} with eigenvalue 1 for any permutation operator P_π i.e.

$$\sum_{\mathbf{q}} \hat{G}(\mathbf{p}; \mathbf{q}) \text{tr} (\sigma_{q_1} \otimes \dots \otimes \sigma_{q_k} P_\pi) = \text{tr} (\sigma_{p_1} \otimes \dots \otimes \sigma_{p_k} P_\pi).$$

Further, any vector orthogonal to this set has eigenvalue 0.

Proof. For the first part,

$$\begin{aligned} & \sum_{\mathbf{q}} \hat{G}(\mathbf{p}; \mathbf{q}) \text{tr} (\sigma_{q_1} \otimes \dots \otimes \sigma_{q_k} P_\pi) \\ &= d^{-k} \sum_{\mathbf{q}} \mathbb{E}_U \text{tr} \left(\sigma_{q_1} U \sigma_{p_1} U^\dagger \right) \dots \text{tr} \left(\sigma_{q_k} U \sigma_{p_k} U^\dagger \right) \text{tr} (\sigma_{q_1} \otimes \dots \otimes \sigma_{q_k} P_\pi) \\ &= d^{-k} \text{tr} \left(P_\pi \mathbb{E}_U \sum_{q_1} \text{tr} \left(\sigma_{q_1} U \sigma_{p_1} U^\dagger \right) \sigma_{q_1} \otimes \dots \otimes \sum_{q_k} \text{tr} \left(\sigma_{q_k} U \sigma_{p_k} U^\dagger \right) \sigma_{q_k} \right) \end{aligned} \quad (3.4)$$

Writing $U^\dagger \sigma_p U$ in the σ_p basis, we find

$$\frac{1}{d} \sum_q \text{tr} \left(\sigma_q U \sigma_p U^\dagger \right) \sigma_q = U \sigma_p U^\dagger.$$

Therefore Eqn. 3.4 becomes

$$\text{tr} \left(P_\pi \mathbb{E}_U U^\dagger \sigma_{p_1} U \otimes \dots \otimes U^\dagger \sigma_{p_k} U \right) = \text{tr} (\sigma_{p_1} \otimes \dots \otimes \sigma_{p_k} P_\pi).$$

For the second part, consider any vector v which is orthogonal to the permutation operators (we can neglect the complex conjugate because P_π is real in this basis), i.e.

$$\sum_{\mathbf{q}} \text{tr} (\sigma_{q_1} \otimes \dots \otimes \sigma_{q_k} P_\pi) v(\mathbf{q}) = 0 \quad (3.5)$$

for any permutation π . Then

$$\sum_{\mathbf{q}} \hat{G}(\mathbf{p}; \mathbf{q}) v(\mathbf{q}) = d^{-k} \sum_{\mathbf{q}} \text{tr} (\sigma_{q_1} \otimes \dots \otimes \sigma_{q_k} T(\mathbf{p})) v(\mathbf{q})$$

which is zero since $T(\mathbf{p})$ is a linear combination of permutations and v is orthogonal to this by Eqn. 3.5. \square

Theorem 3.5. $\hat{G}^2 = \hat{G}$, i.e. $\sum_{\mathbf{q}'} \hat{G}(\mathbf{p}; \mathbf{q}') \hat{G}(\mathbf{q}'; \mathbf{q}) = \hat{G}(\mathbf{p}; \mathbf{q})$.

Proof. Using Eqn. 3.3,

$$\sum_{\mathbf{q}'} \hat{G}(\mathbf{p}; \mathbf{q}') \hat{G}(\mathbf{q}'; \mathbf{q}) = \sum_{\mathbf{q}'} \hat{G}(\mathbf{p}; \mathbf{q}') d^{-k} \text{tr} \left(\sigma_{q'_1} \otimes \dots \otimes \sigma_{q'_k} T(\mathbf{q}) \right).$$

From Corollary 3.2, $T(\mathbf{q})$ is a linear combination of permutations. This implies, using Theorem 3.4 that

$$\begin{aligned} \sum_{\mathbf{q}'} \hat{G}(\mathbf{p}; \mathbf{q}') d^{-k} \text{tr} \left(\sigma_{q'_1} \otimes \dots \otimes \sigma_{q'_k} T(\mathbf{q}) \right) &= d^{-k} \text{tr} (\sigma_{p_1} \otimes \dots \otimes \sigma_{p_k} T(\mathbf{q})) \\ &= \hat{G}(\mathbf{p}; \mathbf{q}) \end{aligned}$$

as required. \square

Corollary 3.6. \hat{G} is a projector so has eigenvalues 0 and 1.

We now evaluate \hat{G} and T for the cases of $k = 1$ and $k = 2$ since these are the cases we are interested in for the remainder of the paper.

3.1 $k = 1$

The $k = 1$ case is clear: the random unitary completely randomises the state. Therefore all terms in the expansion are set to zero apart from the identity i.e.

$$T(p) = \begin{cases} \sigma_0 & p = 0 \\ 0 & p \neq 0. \end{cases} \quad (3.6)$$

3.2 $k = 2$

For $k = 2$, there are just two permutation operators, identity I and swap \mathcal{F} . Therefore there are just two eigenvectors with non-zero eigenvalue ($n > 1$). In normalised form, taking them to be orthogonal, their components are

$$\begin{aligned} f_1(q_1, q_2) &= \delta_{q_1 0} \delta_{q_2 0} \\ f_2(q_1, q_2) &= \frac{1}{d^2 - 1} \delta_{q_1 q_2} (1 - \delta_{q_1 0}) \end{aligned}$$

We will now prove three properties of \hat{G} that we need:

1. $\hat{G}(p_1, p_2; q_1, q_2) = 0$ if $p_1 \neq p_2$ or $q_1 \neq q_2$.

Proof. Consider the function $f(q_1, q_2) = \delta_{q_1 a} \delta_{q_2 b}$ with $a \neq b$. This function has zero overlap with the eigenvectors f_1 and f_2 so it goes to zero when acted on by \hat{G} . Therefore $\hat{G}(p_1, p_2; a, b) = 0$. The claim follows from the symmetry property (Theorem 3.3). \square

With this we will write $\hat{G}(p; q) \equiv \hat{G}(p_1, p_2; q_1, q_2)$.

2. $\hat{G}(p; 0) = \delta_{p0}$.

Proof. Let \hat{G} act on eigenvector f_1 . \square

3. $\hat{G}(p; a) = \frac{1}{d^2-1}$ for $a, p \neq 0$.

Proof. Let \hat{G} act on the input δ_{qa} . This has zero overlap with f_1 and overlap $\frac{1}{d^2-1}$ with f_2 . \square

Therefore we have

$$\hat{G}(p_1, p_2; q_1, q_2) = \begin{cases} 0 & p_1 \neq p_2 \text{ or } q_1 \neq q_2 \\ 1 & p_1 = p_2 = q_1 = q_2 = 0 \\ \frac{1}{d^2-1} & p_1 = p_2 \neq 0, q_1 = q_2 \neq 0 \end{cases} \quad (3.7)$$

Since $T(p_1, p_2) = \sum_{q_1, q_2} \hat{G}(p_1, p_2; q_1, q_2) \sigma_{q_1} \otimes \sigma_{q_2}$, we have

$$T(p_1, p_2) = \begin{cases} 0 & p_1 \neq p_2 \\ \sigma_0 \otimes \sigma_0 & p_1 = p_2 = 0 \\ \frac{1}{d^2-1} \sum_{p' \neq 0} \sigma_{p'} \otimes \sigma_{p'} & p_1 = p_2 \neq 0. \end{cases} \quad (3.8)$$

Therefore the terms $\sigma_{p_1} \otimes \sigma_{p_2}$ with $p_1 \neq p_2$ are set to zero. Further, the sum of the diagonal coefficients $\gamma(p, p)$ is conserved. This allows us to identify this with a probability distribution (after renormalising) and use Markov chain analysis. To see this, write again the starting state

$$\rho = \frac{1}{d} \sum_{q_1, q_2} \gamma_0(q_1, q_2) \sigma_{q_1} \otimes \sigma_{q_2}$$

with state after application of any unitary W

$$\rho_W = \frac{1}{d} \sum_{q_1, q_2} \gamma_W(q_1, q_2) \sigma_{q_1} \otimes \sigma_{q_2} = 2^{-n} \sum_{q_1, q_2} \gamma(q_1, q_2) \left(W \sigma_{q_1} W^\dagger \right) \otimes \left(W \sigma_{q_2} W^\dagger \right).$$

Then

$$\begin{aligned} \sum_q \gamma_W(q, q) &= \frac{1}{d} \sum_q \text{tr} (\sigma_q \otimes \sigma_q \rho_W) \\ &= \text{tr} (\mathcal{F} \rho_W) \\ &= \frac{1}{d} \sum_{q_1, q_2} \gamma(q_1, q_2) \text{tr} \left(\mathcal{F} \left(W \sigma_{q_1} W^\dagger \right) \otimes \left(W \sigma_{q_2} W^\dagger \right) \right) \\ &= \frac{1}{d} \sum_{q_1, q_2} \gamma(q_1, q_2) \text{tr} (\sigma_{q_1} \sigma_{q_2}) \\ &= \sum_q \gamma(q, q) \end{aligned}$$

as required, where \mathcal{F} is the swap operator and we have used Lemmas A.2 and A.1.

3.3 Moments for General Universal Random Circuits

We now consider universal distributions μ that in general may be different from the uniform (Haar) measure on $U(d)$. Our main result in this section will be to show that a universal distribution on $U(4)$ is also 2-copy gapped. In fact, we will phrase this result in slightly more general terms and show that a universal distribution on $U(d)$ is also k -copy gapped for any k . Universality (Definition 2.8) generalises in the obvious way to $U(d)$, whereas when we say that μ is k -copy gapped, we mean that

$$\|G_\mu - G_{U(d)}\|_\infty < 1, \quad (3.9)$$

where $G_? = \mathbb{E}_U U^{\otimes k} \otimes (U^*)^{\otimes k}$, with the expectation taken over μ for G_μ or over the Haar measure for $G_{U(d)}$.

The reason Eqn. 3.9 represents our condition for μ to be k -copy gapped is as follows: Observe that \hat{G} and G are unitarily related, so the definition of k -copy gapped could equivalently be given in terms of \hat{G} . We have shown above that $\hat{G}_{U(d)}$ (and thus $G_{U(d)}$) has all eigenvalues equal to 0 or 1; i.e. is a projector. By contrast, G_μ may not even be Hermitian. However, we will prove below that all eigenvectors of $G_{U(d)}$ with eigenvalue 1 are also eigenvectors of G_μ with eigenvalue 1. Thus, Eqn. 3.9 will imply that $\lim_{t \rightarrow \infty} (\hat{G}_\mu)^t = \hat{G}_{U(d)}$, just as we would expect for a gapped random walk.

We would like to show that Eqn. 3.9 holds whenever μ is universal. This result was proved in [6] (and was probably known even earlier) when μ had the form $(\delta_{U_1} + \delta_{U_2})/2$. Here we show how to extend the argument to any universal μ .

Lemma 3.7. *Let μ be a distribution on $U(d)$. Then all eigenvectors of $G_{U(d)}$ with eigenvalue 1 are eigenvectors of G_μ with eigenvalue one. Additionally, if μ is universal then μ is k -copy gapped for any positive integer k (cf. Eqn. 3.9).*

In particular, if $k = 2$ this Lemma implies that μ is 2-copy gapped (cf. Theorem 2.9).

Proof. Let $V \cong \mathbb{C}^d$ be the fundamental representation of $U(d)$, where the action of $U \in U(d)$ is simply U itself. Let V^* be its dual representation, where U acts as U^* . The operators G_μ and $G_{U(d)}$ act on the space $V^{\otimes k} \otimes (V^*)^{\otimes k}$. We will see that $G_{U(d)}$ is completely determined by the decomposition of $V^{\otimes k} \otimes (V^*)^{\otimes k}$ into irreducible representations (irreps). Suppose that the multiplicity of (r_λ, V_λ) in $V^{\otimes k} \otimes (V^*)^{\otimes k}$ is m_λ , where the V_λ 's are the irrep spaces and $r_\lambda(U)$ the corresponding representation matrices. In other words

$$V^{\otimes k} \otimes (V^*)^{\otimes k} \cong \bigoplus_\lambda V_\lambda \otimes \mathbb{C}^{m_\lambda} \quad (3.10)$$

$$U^{\otimes k} \otimes (U^*)^{\otimes k} \sim \sum_\lambda |\lambda\rangle\langle\lambda| \otimes r_\lambda(U) \otimes I_{m_\lambda} \quad (3.11)$$

Here \sim indicates that the two sides are related by conjugation by a fixed (U -independent) unitary.

Let $\lambda = 0$ denote the trivial irrep: i.e. $V_0 = \mathbb{C}$ and $r_0(U) = 1$ for all U . We claim that $\mathbb{E}_U r_\lambda(U) = 0$ whenever $\lambda \neq 0$ and the expectation is taken over the Haar measure. To show this, note that $\mathbb{E}_U r_\lambda(U)$ commutes with $r_\lambda(V)$ for all $V \in U(d)$ and thus, by Schur's Lemma, we must have $\mathbb{E}_U r_\lambda(U) = cI$ for some $c \in \mathbb{C}$. However, by the translation-invariance of the Haar measure we have $cI = \mathbb{E}_U r_\lambda(U) = \mathbb{E}_U r_\lambda(UV) = cr_\lambda(V)$ for all $V \in U(d)$. Since $\lambda \neq 0$, we cannot have $r_\lambda(V) = I$ for all V and so it must be that $c = 0$.

Thus, if we write $G_{U(d)}$ and G_μ using the basis on the RHS of Eqn. 3.11, we have

$$G_{U(d)} = |0\rangle\langle 0| \otimes I_{m_0} \quad (3.12)$$

where $|0\rangle\langle 0|$ is a projector onto the trivial irrep. On the other hand,

$$G_\mu = |0\rangle\langle 0| \otimes I_{m_0} + \sum_{\lambda \neq 0} |\lambda\rangle\langle\lambda| \otimes \left(\int r_\lambda(U) d\mu(U) \right) \otimes I_{m_\lambda} \quad (3.13)$$

Thus, every eigenvector of $G_{U(d)}$ with eigenvalue one is also fixed by G_μ . For the remainder of the space, the direct sum structure means that

$$\|G_{U(d)} - G_\mu\|_\infty = \max_{\substack{\lambda \neq 0 \\ m_\lambda \neq 0}} \left\| \int r_\lambda(U) d\mu(U) \right\|_\infty. \quad (3.14)$$

Note that this maximisation only includes λ with $\dim V_\lambda > 1$. This is because non-trivial one-dimensional irreps of $U(d)$ have the form $\det U^m$ for some non-zero integer m . Under the map $U \mapsto e^{i\phi}U$, such irreps pick up a phase of $e^{im\phi}$. However, $U^{\otimes k} \otimes (U^*)^{\otimes k}$ is invariant under $U \mapsto e^{i\phi}U$. Thus $V^{\otimes k} \otimes (V^*)^{\otimes k}$ cannot contain any non-trivial one-dimensional irreps.

Now suppose by contradiction that there exists $\lambda \neq 0$ with $m_\lambda \neq 0$ and $\|\int r_\lambda(U) d\mu(U)\|_\infty = 1$. (We do not need to consider the case $\|\int r_\lambda(U) d\mu(U)\|_\infty > 1$, since $\|r_\lambda(U)\|_\infty = 1$ for all U and $\|\cdot\|_\infty$ obeys the triangle inequality.) Indeed, the triangle inequality further implies that there exists a unit vector $|v\rangle \in V_\lambda$ such that

$$\int d\mu(U) r_\lambda(U) |v\rangle = \omega |v\rangle,$$

for some $\omega \in \mathbb{C}$ with $|\omega| = 1$.

By the above argument we can assume that $\dim V_\lambda > 1$. Since V_λ is irreducible, it cannot contain a one-dimensional invariant subspace, implying that there exists $U_0 \in U(d)$ such that

$$|\langle v | r_\lambda(U_0) | v \rangle| = 1 - \delta,$$

for some $\delta > 0$. Since $U \mapsto |\langle v | r_\lambda(U) | v \rangle|$ is continuous, there exists an open ball S around U_0 such that $|\langle v | r_\lambda(U) | v \rangle| \leq 1 - \delta/2$ for all $U \in S$. Define $\bar{S} := U(d) \setminus S$.

Now we use the fact that μ is universal to find an ℓ such that $\mu^{*\ell}(S) > 0$. Next, observe that $\int d\mu^{*\ell}(U) \langle v | r_\lambda(U) | v \rangle = \omega^\ell$. Taking the absolute value of both sides yields

$$\begin{aligned} 1 &= \left| \int_{U(d)} d\mu^{*\ell}(U) \langle v | r_\lambda(U) | v \rangle \right| \\ &\leq \int_{U(d)} d\mu^{*\ell}(U) |\langle v | r_\lambda(U) | v \rangle| \\ &= \int_S d\mu^{*\ell}(U) |\langle v | r_\lambda(U) | v \rangle| + \int_{\bar{S}} d\mu^{*\ell}(U) |\langle v | r_\lambda(U) | v \rangle| \\ &\leq \mu^{*\ell}(S) \left(1 - \frac{\delta}{2} \right) + \left(1 - \mu^{*\ell}(S) \right) \\ &< 1, \end{aligned}$$

a contradiction. We conclude that $\|G_{U(d)} - G_\mu\|_\infty < 1$. □

4 Convergence

In Section 3 we saw that iterating any universal gate set on $U(d)$ eventually converges to the uniform distribution on $U(d)$. Since the set of all two-qubit unitaries is universal on $U(2^n)$, this implies that random circuits eventually converge to the Haar measure. In this section, we turn to proving upper bounds on this convergence rate, focusing on the first two moments.

Let $\hat{G}^{(ij)}$ be the matrix with \hat{G} (with $d = 4$) acting on qubits i and j and the identity on the others. Then, if the pair (i, j) is chosen at step t , we can find the coefficients at step $t + 1$ by multiplying by $\hat{G}^{(ij)}$. In general, a random pair is chosen at each step. So

$$\gamma_{t+1}(\mathbf{p}) = \sum_{\mathbf{q}} \frac{1}{n(n-1)} \sum_{i \neq j} \hat{G}^{(ij)}(\mathbf{p}; \mathbf{q}) \gamma_t(\mathbf{q}) \quad (4.1)$$

where γ_{t+1} are the expected coefficients at step t . We can think of this evolution as repeated application of the matrix

$$P = \frac{1}{n(n-1)} \sum_{i \neq j} \hat{G}^{(ij)}. \quad (4.2)$$

For $k = 2$, the key idea of Oliveira et al. [26] was to map the evolution of the $\gamma(p, p)$ coefficients to a Markov chain. The $\gamma(p_1, p_2)$ coefficients with $p_1 \neq p_2$ just decay as each qubit is chosen and can be analysed directly.

However, we can only map the $\gamma(p, p)$ coefficients to a probability distribution when they are non-negative, which is not the case for general states. Most of the rest of the paper is dedicated to proving Lemma 2.11, which only applies to states with $\gamma(p, p) \geq 0$ and normalised so their sum is 1. Corollary 2.12 then extends this to all states:

of Corollary 2.12. Lemma 2.11 still applies to the $\gamma(p_1, p_2)$ terms with $p_1 \neq p_2$. Therefore we just need to show how to apply Lemma 2.11 to states that initially have some negative $\gamma(p, p)$ terms.

For the $\gamma(p, p)$ terms, Lemma 2.11 says that the random walk starting with any initial probability distribution converges to uniform in some bounded time t . Let $g_t(p, p; q, q)$ be the coefficients after t steps of the walk starting at a particular point q (i.e. $g_0(p, p; q, q) = \delta_{p,q}$). Now, for any starting state ρ , let the initial coefficients be $\gamma_0(p, p)$. Then, by linearity, we can write the expected coefficients after t steps $\gamma_t(p, p) := \mathbb{E}\gamma_W(p, p)$ as

$$\gamma_t(p, p) = \sum_{q \neq 0} \gamma_0(q, q) g_t(p, p; q, q) \quad (4.3)$$

for $p \neq 0$.

We can now prove convergence rates for the expected coefficients $\gamma_t(p, p)$:

- (i) For the 2-norm, we have from Lemma 2.11 that for $t \geq Cn \log 1/\epsilon$

$$\sum_{p \neq 0} \left(g_t(p, p; q, q) - \frac{1}{4^n - 1} \right)^2 \leq \epsilon \quad (4.4)$$

for any q . Note that the normalisation for the $\gamma(p, p)$ terms with $p \neq 0$ has changed from Lemma 2.11 since we are neglecting the $\gamma(0, 0)$ term here. Now

$$\begin{aligned}
& \sum_{p \neq 0} \left(\gamma_t(p, p) - \frac{\sum_{q \neq 0} \gamma_0(q, q)}{4^n - 1} \right)^2 \\
&= \sum_{p \neq 0} \left(\sum_{q \neq 0} \gamma_0(q, q) \left(g_t(p, p; q, q) - \frac{1}{4^n - 1} \right) \right)^2 \\
&\leq \sum_{q \neq 0} \gamma_0(q, q)^2 \sum_{q' \neq 0} \sum_{p \neq 0} \left(g_t(p, p; q', q') - \frac{1}{4^n - 1} \right)^2 \\
&\leq (4^n - 1)\epsilon \sum_{q \neq 0} \gamma_0(q, q)^2 \\
&\leq 4^n \epsilon \sum_{q_1, q_2} \gamma_0(q_1, q_2)^2 \\
&= 4^n \epsilon \text{tr } \rho^2 \\
&\leq 4^n \epsilon
\end{aligned}$$

where the first inequality is the Cauchy-Schwarz inequality. Therefore for $t \geq Cn(n + \log 4^n / \epsilon)$, the 2-norm distance from stationarity for the $\gamma(p, p)$ terms is at most ϵ . Choose C' such that $C'n(n + \log 1/\epsilon) \geq Cn(n + \log 4^n / \epsilon)$ to obtain the result.

(ii) For the 1-norm, Lemma 2.11 says that for $t \geq Cn(n + \log 1/\epsilon)$

$$\sum_{p \neq 0} \left| g_t(q; p, p) - \frac{1}{4^n - 1} \right| \leq \epsilon. \quad (4.5)$$

We can then proceed much as for the 2-norm case:

$$\begin{aligned}
& \sum_{p \neq 0} \left| \gamma_t(p, p) - \frac{\sum_{q \neq 0} \gamma_0(q, q)}{4^n - 1} \right| \\
&= \sum_{p \neq 0} \left| \sum_{q \neq 0} \gamma_0(q, q) \left(g_t(p, p; q, q) - \frac{1}{4^n - 1} \right) \right| \\
&\leq \sum_{q \neq 0} |\gamma_0(q, q)| \sum_{p \neq 0} \left| g_t(p, p; q, q) - \frac{1}{4^n - 1} \right| \\
&\leq \epsilon \sum_{q \neq 0} |\gamma_0(q, q)| \\
&\leq 2^n \epsilon.
\end{aligned}$$

The last inequality follows from $|\sigma_q \otimes \sigma_q| = \sigma_0 \otimes \sigma_0$. Therefore for $t \geq Cn(n + \log 2^n / \epsilon)$, the 1-norm distance from stationarity for the $\gamma(p, p)$ terms is at most ϵ . \square

We now proceed to prove Lemma 2.11. Firstly, we will consider the simple case of $k = 1$ to prove this process forms a 1-design as this will help us to understand the more complicated case of $k = 2$.

4.1 First Moments Convergence

Recall that $\rho = 2^{-n/2} \sum_p \gamma(p) \sigma_p$ and we wish to evaluate the moments of the coefficients. So for the first moments to converge, we want to know $\mathbb{E}\gamma(p)$.

For $k = 1$, the $U(4)$ random circuit uniformly randomises each pair that is chosen. More precisely, a pair of sites i, j are chosen at random and all the coefficients with $p_i \neq 0$ or $p_j \neq 0$ are set to zero. Thus we get an exact 1-design when all sites have been hit. For other gate sets, the terms do not decay to zero but decay by a factor depending on the gap of \hat{G} . Call the gap Δ ; for $U(4)$ $\Delta = 1$ and for others $0 < \Delta \leq 1$ and Δ is independent of n . Therefore once each site has been hit m times the terms have decayed by a factor $(1 - \Delta)^m$.

For a bound like the mixing time (see Section 4.3 for definition), we want to bound the quantity $\sum_{p \neq 0} |\mathbb{E}_W \gamma_W(p)|$ where $\gamma_W(p)$ is the Pauli coefficient after applying the random circuit W . We also want 2-norm bounds, so we bound $\sum_{p \neq 0} (\mathbb{E}_W \gamma_W(p))^2$ too. We will in fact find bounds on $\sum_{p \neq 0} \mathbb{E}_W |\gamma_W(p)|$ and $\sum_{p \neq 0} (\mathbb{E}_W |\gamma_W(p)|)^2$, which are stronger.

A standard problem in the theory of randomised algorithms is the ‘coupon collector’ problem. If a magazine comes with a free coupon, which is chosen uniformly randomly from n different types, how many magazines should you buy to have a high probability of getting all n coupons? It is not hard to show that $n \ln \frac{n}{\epsilon}$ samples (magazines) have at least a $1 - \epsilon$ probability of including all n coupons. Using this, we expect all sites to be hit with probability at least $1 - \epsilon$ after $\Theta(n \log \frac{n}{\epsilon})$ steps. This argument can be made precise in this context by bounding the non-identity coefficients. We find, as expected, that the sum is small after $O(n \log n)$ steps:

Lemma 4.1. *After $O(n \log 1/\epsilon)$ steps*

$$\sum_{p \neq 0} (\mathbb{E}_W |\gamma_W(p)|)^2 \leq \epsilon$$

and after $O(n \log \frac{n}{\epsilon})$ steps,

$$\sum_{p \neq 0} \mathbb{E}_W |\gamma_W(p)| \leq \epsilon. \quad (4.6)$$

Proof. At each step, a pair of sites is chosen at random and any terms with non-identity coefficients for this pair decay by a factor $(1 - \Delta)$. For example, the term $\sigma_1 \otimes \sigma_0^{\otimes(n-1)}$ decays whenever the first site is chosen. Thus the probability of each term decaying depends on the number of zeroes. We start with the 1-norm bound.

Suppose the circuit applied after t steps is W_t . Consider $\mathbb{E}_{W_t} |\gamma_{W_t}(p)|$ for any p with d non-zeroes. Since the state ρ is physical, $\text{tr } \rho^2 \leq 1$ so $\sum_p \gamma_0^2(p) \leq 1$. Now, in each step, if any site is chosen where p is non-zero, this term decays by a factor $(1 - \Delta)$. This occurs with probability $1 - \frac{(d-n)(d-n-1)}{n(n-1)} \geq d/n$, the probability of choosing a pair where at least one site is non-zero. Therefore

$$\mathbb{E} |\gamma_{W_t}(p)| \leq ((1 - \Delta)d/n + (1 - d/n)) |\gamma_{W_{t-1}}(p)|$$

where the expectation is over the circuit applied at step t . If we iterate this t times we find

$$\mathbb{E}_W |\gamma_W(p)| \leq \exp(-\Delta t d/n) |\gamma_0(p)|$$

where the expectation here is over all random circuits for the t steps. We now sum over all p :

$$\sum_{p \neq 0} \mathbb{E}_W |\gamma_W(p)| \leq \sum_{d=1}^n \exp(-\Delta t d/n) \sum_{d(p)=d} |\gamma_0(p)|$$

where $d(p)$ is the number of non-zeroes in p . For the 1-norm bound, we can simply bound $|\gamma_0(p)| \leq 1$ to give $\sum_{d(p)=d} |\gamma_0(p)| \leq \binom{n}{d} 3^d$ so

$$\sum_{p \neq 0} \mathbb{E}_W |\gamma_W(p)| \leq (1 + 3 \exp(-\Delta t/n))^n - 1$$

where we have used the binomial theorem. Now let $t = \frac{n}{\Delta} \ln \frac{3n}{\epsilon}$. This gives

$$\sum_{p \neq 0} \mathbb{E}_W |\gamma_W(p)| \leq (1 + \epsilon/n)^n - 1 = O(\epsilon).$$

For the 2-norm bound,

$$\begin{aligned} \sum_{p \neq 0} (\mathbb{E}_W |\gamma_W(p)|)^2 &\leq \sum_{p \neq 0} \exp(-2\Delta t d/n) \gamma_0^2(p) \\ &= \sum_{d=1}^n \exp(-2\Delta t d/n) \sum_{d(p)=d} \gamma_0^2(p) \\ &\leq \sum_{d=1}^n \exp(-2\Delta t d/n) \\ &\leq \frac{\exp(-2\Delta t/n)}{1 - \exp(-2\Delta t/n)} \end{aligned}$$

where we have used $\sum_p \gamma_0^2(p) \leq 1$. We find after $\frac{n}{2\Delta} \ln 1/\epsilon$ steps that

$$\sum_{p \neq 0} (\mathbb{E}_W |\gamma_W(p)|)^2 \leq \frac{\epsilon}{1 - \epsilon} \quad \square$$

4.2 Second Moments Convergence

Firstly, the $\sigma_{p_1} \otimes \sigma_{p_2}$ terms for $p_1 \neq p_2$ decay in a similar way to the non-identity terms in the 1-design analysis. In fact, the proof of Lemma 4.1 carries over almost identically to this case to give

Lemma 4.2. *After $O(n \log 1/\epsilon)$ steps*

$$\sum_{p_1 \neq p_2} (\mathbb{E}_W |\gamma_W(p_1, p_2)|)^2 \leq \epsilon$$

and after $O(n(n + \log 1/\epsilon))$ steps

$$\sum_{p_1 \neq p_2} \mathbb{E}_W |\gamma_W(p_1, p_2)| \leq \epsilon.$$

Proof. Instead of the number of zeroes governing the decay rate, we need to count the number of places where p_1 and p_2 differ. This gives

$$\mathbb{E}|\gamma_{W_t}(p_1, p_2)| \leq ((1 - \Delta)d/n + (1 - d/n)) |\gamma_{W_{t-1}}(p_1, p_2)|$$

where now d is the number of differing sites. There are $\binom{n}{d} 12^d 4^{n-d}$ states that differ in d places so we find

$$\sum_{p_1 \neq p_2} \mathbb{E}_W |\gamma_W(p_1, p_2)| \leq 4^n [(1 + 3 \exp(-\Delta t/n))^n - 1].$$

Set $t = \frac{n}{\Delta}(\ln 4 + \ln 1/\epsilon)$ to make this $O(\epsilon)$. The 2-norm bound follows in the same way as for Lemma 4.1. \square

We now need to prove the $\gamma(p, p)$ terms converge quickly. We have seen above that the sum of the terms $\gamma(p, p)$ is conserved and, for the purposes of proving Lemma 2.11, we assume the sum is 1 and $\gamma(p, p) \geq 0$ for all p .

To illustrate the evolution, consider the simplest case when the gates are chosen from $U(4)$. We have evaluated \hat{G} in Section 3.2 for $k = 2$ for this case. Translated into coefficients this yields the following update rule, where we have written it for the case when qubits 1 and 2 are chosen:

$$\begin{aligned} \gamma_{t+1}(r_1, r_2, r_3, \dots, r_n, s_1, s_2, s_3, \dots, s_n) \\ = \begin{cases} 0 & (r_1, r_2) \neq (s_1, s_2) \\ \gamma_t(0, 0, r_3, \dots, r_n, 0, 0, s_3, \dots, s_n) & (r_1, r_2) = (s_1, s_2) = (0, 0) \\ \frac{1}{15} \sum_{\substack{r'_1, r'_2 \\ r'_1 r'_2 \neq 0}} \gamma_t(r'_1, r'_2, r_3, \dots, r_n, r'_1, r'_2, s_3, \dots, s_n) & (r_1, r_2) = (s_1, s_2) \neq (0, 0). \end{cases} \quad (4.7) \end{aligned}$$

The key idea of Oliveira et al. [26] was to map the evolution of the $\gamma(p, p)$ coefficients to a Markov chain. We can apply this here to get, on state space $\{0, 1, 2, 3\}^n$, the evolution:

1. Choose a pair of sites uniformly at random.
2. If the state is 00 it remains 00.
3. Otherwise, choose the state uniformly at random from $\{0, 1, 2, 3\}^2 \setminus \{00\}$.

This is the correct evolution since, if the initial state is distributed according to $\gamma_t(q, q)$, the final state is distributed according to $\gamma_{t+1}(p, p)$.

The evolution for other gate sets will be similar, but the states will not be chosen uniformly randomly in the third step. However, the state 00 will remain 00 and the stationary distribution on the other 15 states is the same. We will find the convergence times for general gate sets and then consider the $U(4)$ gate set since we can perform a tight analysis for this case.

4.3 Markov Chain Analysis

Before finding the convergence rate for our problem, we will briefly introduce the basics of Markov chain mixing time analysis. All of these standard results can be found in Ref. [25] and references therein.

A process is Markov if the evolution only depends on the current state rather than the full state history. Therefore the evolution of the state can be thought of as a matrix, the *transition matrix*, acting on a vector which represents the current distribution. We will only be interested in discrete time processes so the state after t steps is given by the t^{th} power of the transition matrix acting on the initial distribution.

We say a Markov chain is *irreducible* if it is possible to get from one state to any other state in some number of steps. Further, a chain is *aperiodic* if it does not return to a state at regular intervals. If a chain is both irreducible and aperiodic then it is said to be *ergodic*. A well known result of Markov chain theory is that all ergodic chains converge to a unique stationary distribution. In matrix language this says that the transition matrix P has eigenvalue 1 with no multiplicity and all other eigenvalues have absolute value strictly less than 1. We will also need the notion of *reversibility*. A Markov chain is reversible if the time reversed chain has the same transition matrix, with respect to some distribution. This condition is also known as *detailed balance*:

$$\pi(x)P(x, y) = \pi(y)P(y, x). \quad (4.8)$$

It can be shown that a reversible ergodic Markov chain is only reversible with respect to the stationary distribution. So above $\pi(x)$ is the stationary distribution of P . An immediate consequence of this is that for a chain with uniform stationary distribution, it is reversible if and only if it is symmetric (i.e. $P(x, y) = P(y, x)$). Note also that reversible chains have real eigenvalues, since they are similar to the symmetric matrix $\sqrt{\frac{\pi(x)}{\pi(y)}}P(x, y)$.

With these definitions and concepts, we can now ask how quickly the Markov chain converges to the stationary distribution. This is normally defined in terms of the 1-norm mixing time. We use (half the) 1-norm distance to measure distances between distributions:

$$\|s - t\| = \frac{1}{2} \|s - t\|_1 = \frac{1}{2} \sum_i |s_i - t_i|. \quad (4.9)$$

We assume all distributions are normalised so then $0 \leq \|s - t\| \leq 1$. We can now define the mixing time:

Definition 4.3. *Let π be the stationary distribution of P . Then if P is ergodic the mixing time τ is*

$$\tau(\epsilon) = \max_s \min_t \{t \geq 0 : \|P^t s - \pi\| \leq \epsilon\}. \quad (4.10)$$

We will also use the (weaker) 2-norm mixing time (note this is not the same as τ_2 in Ref. [25]):

Definition 4.4. *Let π be the stationary distribution of P . Then if P is ergodic the 2-norm mixing time τ_2 is*

$$\tau_2(\epsilon) = \max_s \min_t \{t \geq 0 : \|P^t s - \pi\|_2 \leq \epsilon\}. \quad (4.11)$$

Unless otherwise stated, when we say mixing time we are referring to the 1-norm mixing time.

There are many techniques for bounding the mixing time, including finding the second largest eigenvalue of P . This gives a good measure of the mixing time because components parallel to the second largest eigenvector decay the slowest. We have (for reversible ergodic chains)

Theorem 4.5 (see Ref. [25], Corollary 1.15).

$$\tau(\epsilon) \leq \frac{1}{\Delta} \ln \frac{1}{\pi_* \epsilon}$$

where $\pi_* = \min \pi(x)$ and $\Delta = \min(1 - \lambda_2, 1 + \lambda_{\min})$ where λ_2 is the second largest eigenvalue and λ_{\min} is the smallest. Δ is known as the gap.

If the chain is irreversible, it may not even have real eigenvalues. However, we can bound the mixing time in terms of the eigenvalues of the reversible matrix PP^* where $P^*(x, y) = \frac{\pi(y)}{\pi(x)} P(y, x)$. In this case we have ([25], Corollary 1.14)

$$\tau(\epsilon) \leq \frac{2}{\Delta_{PP^*}} \ln \frac{1}{\pi_* \epsilon} \quad (4.12)$$

where now Δ_{PP^*} is the gap of the chain PP^* . Note that for a reversible chain $P = P^*$ and $\Delta_{PP^*} \approx 2\Delta$ so the bounds are approximately the same.

This can also be converted into a 2-norm mixing time bound:

$$\tau_2(\epsilon) \leq \frac{2}{\Delta_{PP^*}} \ln 1/\epsilon. \quad (4.13)$$

To bound the gap, we will use the comparison theorem in Theorem 4.6 below. In this Theorem, we are thinking of the Markov chain as a directed graph where the vertices are the states and there are edges for allowed transitions (i.e. transitions with non-zero probability). For irreducible chains, it is possible to make a path from any vertex to any other; we call the path length the number of transitions in such a path (which will in general depend on the choice of path).

Theorem 4.6 (see Ref. [25], Theorem 2.14). *Let P and \hat{P} be two Markov chains on the same state space Ω with the same stationary distribution π . Then, for every $x \neq y \in \Omega$ with $\hat{P}(x, y) > 0$ define a directed path γ_{xy} from x to y along edges in P and let its length be $|\gamma_{xy}|$. Let Γ be the set of all such paths. Then*

$$\Delta \geq \hat{\Delta}/A$$

for the gaps Δ and $\hat{\Delta}$ where

$$A = A(\Gamma) = \max_{a \neq b, P(a,b) \neq 0} \frac{1}{\pi(a)P(a,b)} \sum_{x \neq y: (a,b) \in \gamma_{xy}} \pi(x)\hat{P}(x,y)|\gamma_{xy}|.$$

For example, when comparing 1-dimensional random walks there is no choice in the paths; they must pass through every point between x and y . Further, the walk can only progress one step at a time so (without loss of generality, for reversible chains) let $b = a + 1$ to give

$$\begin{aligned} A &= \max_a \frac{1}{\pi(a)P(a,a+1)} \sum_{x \leq a} \sum_{y \geq a+1} \pi(x)\hat{P}(x,y)(y-x) \\ &= \max_a \frac{\hat{P}(a,a+1)}{P(a,a+1)}. \end{aligned} \quad (4.14)$$

A generalisation of the comparison theorem involves constructing flows, which are weighted sets of paths between states. This can give a tighter bound since bottlenecks are averaged over. This gives a modified comparison theorem:

Theorem 4.7 ([12], Theorem 2.3). *Let P and \hat{P} be two Markov chains on the same state space Ω with the same stationary distribution π . Then, for every $x \neq y \in \Omega$ with $\hat{P}(x, y) > 0$, construct a set of directed paths \mathcal{P}_{xy} from x to y along edges in P . We define the flow function f which maps each path $\gamma_{xy} \in \mathcal{P}_{xy}$ to a real number in the interval $[0, 1]$ such that*

$$\sum_{\gamma_{xy} \in \mathcal{P}_{xy}} f(\gamma_{xy}) = \hat{P}(x, y).$$

Again, let the length of each path be $|\gamma_{xy}|$. Then

$$\Delta \geq \hat{\Delta}/A$$

for the gaps Δ and $\hat{\Delta}$ where

$$A = A(f) = \max_{a \neq b, P(a,b) \neq 0} \frac{1}{\pi(a)P(a,b)} \sum_{x \neq y, \gamma_{xy} \in \mathcal{P}_{xy}: (a,b) \in \gamma_{xy}} \pi(x)f(\gamma_{xy})|\gamma_{xy}|. \quad (4.15)$$

Note that we recover the comparison theorem when there is just one path between each x and y .

4.3.1 log-Sobolev Constant

We will need tighter, but more complicated, mixing time results to prove the tight result for the $U(4)$ case. We use the log-Sobolev constant:

Definition 4.8. *The log-Sobolev constant ρ of a chain with transition matrix P and stationary distribution π is*

$$\rho = \min_f \frac{\sum_{x \neq y} (f(x) - f(y))^2 P(x, y) \pi(y)}{\sum_x \pi(x) f(x)^2 \log \frac{f(x)^2}{\sum_y \pi(y) f(y)^2}}.$$

The mixing time result is:

Lemma 4.9 (see Ref. [13], Theorem 3.7'). *The mixing time of a finite, reversible, irreducible Markov chain is*

$$\tau(\epsilon) = O\left(\frac{1}{\rho} \log \log \frac{1}{\pi_*} + \frac{1}{\Delta} \log \frac{d}{\epsilon}\right) \quad (4.16)$$

where ρ is the Sobolev constant, π_* is the smallest value of the stationary distribution, Δ is the gap and d is the size of the state space.

Further, the comparison theorem (Theorem 4.6) works just the same to give

$$\rho \geq \hat{\rho}/A.$$

We will need one more result, due to Diaconis and Saloff-Coste:

Lemma 4.10 ([13], Lemma 3.2). *Let P_i , $i = 1, \dots, d$, be Markov chains with gaps Δ_i and Sobolev constants ρ_i . Now construct the product chain P . This chain has state space equal to the product*

of the spaces for the chains P_i and at each step one of the chains is chosen at random and run for one step. Then P has spectral gap given by:

$$\Delta = \frac{1}{d} \min_i \Delta_i$$

and Sobolev constant:

$$\rho = \frac{1}{d} \min_i \rho_i.$$

4.4 Convergence Proof

We now prove the Markov chain convergence results to show that the $\gamma(p, p)$ terms converge quickly. We have already shown that the $\gamma(p_1, p_2)$ terms with $p_1 \neq p_2$ converge quickly and that there is no mixing between these terms and the $\gamma(p, p)$ terms. Therefore, in this section, we remove such terms from \hat{G} .

We want to prove the Markov chain with transition matrix (Eqn. 4.2)

$$P = \frac{1}{n(n-1)} \sum_{i \neq j} \hat{G}^{(ij)}$$

converges quickly. Firstly, we know from Section 3.3 that P has two eigenvectors with eigenvalue 1. The first is the identity state $(\sigma_0 \otimes \sigma_0)$ and the second is the uniform sum of all non-identity terms $(\frac{1}{4^n-1} \sum_{p \neq 0} \sigma_p \otimes \sigma_p)$. From now on, we remove the identity state. This makes the chain irreducible. Since we know it converges, it must be aperiodic also so the chain is ergodic and all other eigenvalues are strictly between 1 and -1.

We show here that the gap of this chain, up to constants, does not depend on the choice of 2-copy gapped gate set. In the second half of the paper we find a tight bound on the gap for the $U(4)$ case which consequently gives a tight bound on the gap for all universal sets.

Since the stationary distribution is uniform, the chain is reversible if and only if P is a symmetric matrix. A sufficient condition for P to be symmetric is for $\hat{G}^{(ij)}$ to be symmetric. We saw in Theorem 3.3 that for the $U(4)$ gate set case $\hat{G}^{(ij)}$ is symmetric. In fact, the proof works identically to show that $\hat{G}^{(ij)}$ is symmetric for any gate set, provided the set is invariant under Hermitian conjugation. However, 2-copy gapped gate sets do not necessarily have this property so the Markov chain is not necessarily reversible. We will find equal bounds (up to constants) for the gaps of both P (if \hat{G} is symmetric) and PP^* (if \hat{G} is not symmetric) below:

Theorem 4.11. *Let μ be any 2-copy gapped distribution of gates. If μ is invariant under Hermitian conjugation then let Δ_P be the eigenvalue gap of the resulting Markov chain matrix P . Then*

$$\Delta_P = \Omega(\Delta_{U(4)}) \tag{4.17}$$

where $\Delta_{U(4)}$ is the eigenvalue gap of the $U(4)$ chain. If μ is not invariant under Hermitian conjugation then let Δ_{PP^*} be the eigenvalue gap of the resulting Markov chain matrix PP^* . Then

$$\Delta_{PP^*} = \Omega(\Delta_{U(4)}). \tag{4.18}$$

Proof. We will use the comparison method with flows (Theorem 4.7). Firstly consider the case where μ is closed under Hermitian conjugation i.e. \hat{G} is symmetric.

We will compare P to the $U(4)$ chain, which we call $P_{U(4)}$. Recall that this chain chooses a pair at random and does nothing if the pair is 00 and chooses a random state from $\{0, 1, 2, 3\}^2 \setminus \{00\}$ otherwise.

To apply Theorem 4.7, we need to construct the flows between transitions in $P_{U(4)}$. We will choose paths such that only one pair is modified throughout. For example (with $n = 4$), the transition $1000 \rightarrow 2000$ is allowed in $P_{U(4)}$. To construct a path in P , we need to find allowed transitions between these two paths in P . \hat{G} may not include the transition $10 \rightarrow 20$ directly, however, \hat{G} is irreducible on this subspace of just two pairs. This means that a path exists and can be of maximum length 14 if it has to cycle through all intermediate states (in fact, since \hat{G} is symmetric the maximum path length is 8; all that is important here is that it is constant). For example, the transitions $10 \rightarrow 11 \rightarrow 20$ might be allowed. Then we could choose the full path to be $1000 \rightarrow 1100 \rightarrow 2000$. In this case we have chosen the path to involve transitions pairing sites 1 and 2. However, we could equally well have chosen any pairing; we could pair the first site with any of the others. We can choose 3 paths in this way. For this example, the flow we want to choose will be all 3 of these paths equally weighted. We now use this idea to construct flows between all transitions in $P_{U(4)}$ to prove the result.

Let $x \neq y \in \Omega$ and let $d(x, y)$ be the Hamming distance between the states ($d(x, y)$ gives the number of places at which x and y differ). There are two cases where $P_{U(4)}(x, y) \neq 0$:

1. $d(x, y) = 2$. Here we must choose a unique pairing, specified by the two sites that differ. Make all transitions in P using this pair giving just one path.
2. $d(x, y) = 1$. For this case, choose all possible pairings of the changing site that give allowed transitions in $P_{U(4)}$. For each pairing, construct a path in P modifying only this pair. If the differing site is initially non-zero then there are $n - 1$ such pairings; if the differing site is initially zero then there are $n - z(x)$ pairings where $z(x)$ is the number of zeroes in the state x .

All the above paths are of constant length since we have to (at most) cycle through all states of a pair. We must now choose the weighting $f(\gamma_{xy})$ for each path such that

$$\sum_{\mathcal{P}_{xy}} f(\gamma_{xy}) = P_{U(4)}(x, y) \quad (4.19)$$

where \mathcal{P}_{xy} is the set of all paths from x to y constructed above. We choose the weighting of each path to be uniform. We just need to calculate the number of paths in \mathcal{P}_{xy} to find f :

1. $d(x, y) = 2$. There is just one path so $f(\gamma_{xy}) = P_{U(4)}(x, y) = \Theta(1/n^2)$.
2. $d(x, y) = 1$. If the differing site is initially non-zero then $P_{U(4)}(x, y) = \Theta(1/n)$ and there are $n - 1$ paths so $f(\gamma_{xy}) = \frac{P_{U(4)}(x, y)}{n-1} = \Theta(1/n^2)$. If the differing site is initially zero then $P_{U(4)}(x, y) = \Theta\left(\frac{n-z(x)}{n^2}\right)$ and there are $n - z(x)$ paths so $f(\gamma_{xy}) = \frac{P_{U(4)}(x, y)}{n-z(x)} = \Theta(1/n^2)$.

So for all paths, $f = \Theta(1/n^2)$. We now just need to know how many times each edge (a, b) in P is used to calculate A :

$$A = \max_{a \neq b, P(a,b) \neq 0} A(a, b) \quad (4.20)$$

where

$$A(a, b) = \frac{1}{P(a, b)} \sum_{x \neq y, \gamma_{xy} \in \mathcal{P}_{xy}: (a, b) \in \gamma_{xy}} f(\gamma_{xy}). \quad (4.21)$$

We have cancelled the factors of $\pi(x)$ because the stationary distribution is uniform. We have also ignored the lengths of the paths since they are all constant.

To evaluate $A(a, b)$, we need to know how many paths pass through each edge (a, b) . We again consider the two possibilities separately:

1. $d(a, b) = 2$. Suppose a and b differ at sites i and j . Firstly, we need to count how many transitions from x to y in $P_{U(4)}$ could use this edge, and then how many paths for each transition actually use the edge.

To find which x and y could use the edge, note that x and y must differ at sites i, j or both. Furthermore, the values at the sites other than i and j must be the same as for a (and therefore b). There is a constant number of x, y pairs that satisfy this condition. Now, for each x, y pair satisfying this, paths that use this edge must use the pairing i, j for all transitions. Since in the paths we have chosen above there is a unique path from x to y for each pairing, there is at most one path for each x, y pair that uses edge a, b .

For $d(a, b) = 2$, $P(a, b) = \Theta(1/n^2)$ so $A(a, b)$ is a constant for this case.

2. $d(a, b) = 1$. Let there be r pairings that give allowed transitions in P between a and b . As above, each pairing gives a constant number of paths. So the numerator is $\Theta(r/n^2)$. Further, $P(a, b) = \Theta(r/n^2)$. So again $A(a, b)$ is constant.

Combining, A is a constant so the result is proven for the case \hat{G} is symmetric.

We now turn to the irreversible case. We now need to bound the gap of $PP^* = PP^T$. This chain selects two (possibly overlapping) pairs at random and applies \hat{G} to one of them and \hat{G}^T to the other. We can use the above exactly by choosing \hat{G} to perform the transitions above and \hat{G}^T to just loop the states back to themselves. By aperiodicity (the greatest common divisor of loop lengths is 1), we can always find constant length paths that do this. \square

Now we need to know the gap of the $U(4)$ chain. We can, by a simple application of the comparison theorem, show it is $\Omega(1/n^2)$. However, in the second half of this paper we show it is $\Theta(1/n)$. This gives us (using Theorem 4.5):

Corollary 4.12. *The Markov chain P has mixing time $O(n(n + \log 1/\epsilon))$ and 2-norm mixing time $O(n \log 1/\epsilon)$.*

We conjecture that the mixing time (as well as Lemma 4.2) can be tightened to $\Theta(n \log \frac{n}{\epsilon})$, which is asymptotically the same as for the $U(4)$ case:

Conjecture 4.13. *The second moments for the case of general 2-copy gapped distributions have 1-norm mixing time $\Theta(n \log \frac{n}{\epsilon})$.*

It seems likely that an extension of our techniques in Section 5 could be used to prove this. Combining the convergence results we have proved our general result Lemma 2.11:

of Lemma 2.11. Combining Corollary 4.12 (for the $\gamma(p, p)$ terms) and Lemma 4.2 (for the $\gamma(p_1, p_2)$, $p_1 \neq p_2$ terms) proves the result. \square

We have now shown that the first and second moments of random circuits converge quickly. For the remainder of the paper we prove the tight bound for the gap and mixing time of the $U(4)$ case and show how mixing time bounds relate to the closeness of the 2-design to an exact design. Only for the $U(4)$ case is the matrix \hat{G} a projector so in this sense the $U(4)$ random circuit is the most fundamental. While we expect the above mixing time bound is not tight, we can prove a tight mixing time result for the $U(4)$ case. However, using our definition of an approximate k -design, the gap rather than the mixing time governs the degree of approximation.

5 Tight Analysis for the $U(4)$ Case

We have already found tight bounds for the first moments in Lemma 4.1: just set $\Delta = 1$.

5.1 Second Moments Convergence

We need to prove a result analogous to Lemma 4.2 for the terms $\sigma_{p_1} \otimes \sigma_{p_2}$ where $p_1 \neq p_2$. We already have a tight bound for the 2-norm decay, by setting $\Delta = 1$ into Lemma 4.2. We tighten the 1-norm bound:

Lemma 5.1. *After $O(n \log \frac{n}{\epsilon})$ steps*

$$\sum_{p_1 \neq p_2} \mathbb{E}_W |\gamma_W(p_1, p_2)| \leq \epsilon \quad (5.1)$$

Proof. We will split the random circuits up into classes depending on how many qubits have been hit. Let H be the random variable giving the number of different qubits that have been hit. We can work out the distribution of H and bound the sum of $|\gamma_W(p_1, p_2)|$ for each outcome.

Firstly we have, after t steps,

$$\mathbb{P}(H \leq h) \leq \binom{n}{h} \left(\frac{h(h-1)}{n(n-1)} \right)^t \leq \binom{n}{h} (h/n)^t.$$

Now, for each qubit hit, each coefficient which has p_1 and p_2 differing in this place is set to zero. So after h have been hit, there are only (at most) $16^{(n-h)}$ terms in the sum in Eqn. 5.1. As before, the state is a physical state, $\text{tr } \rho^2 \leq 1$ so $\sum_{p_1 p_2} \gamma^2(p_1, p_2) \leq 1$ so $\sum_{p_1 p_2} |\gamma(p_1, p_2)| \leq \sqrt{N}$ if there

are at most N non-zero terms in the sum. Therefore we have, after t steps,

$$\begin{aligned}
\sum_{p_1 \neq p_2} \mathbb{E}_W |\gamma_W(p_1, p_2)| &\leq \sum_{h=1}^{n-1} \mathbb{P}(H = h) 16^{(n-h)/2} \\
&\leq \sum_{h=1}^{n-1} \mathbb{P}(H \leq h) 4^{(n-h)} \\
&\leq \sum_{h=1}^{n-1} \binom{n}{h} (h/n)^t 4^{(n-h)} \\
&= \sum_{h=1}^{n-1} \binom{n}{h} (1 - h/n)^t 4^h \quad h \rightarrow n - h \\
&\leq \sum_{h=1}^{n-1} \binom{n}{h} \exp(-ht/n) 4^h.
\end{aligned}$$

Now, let $t = n \ln \frac{n}{\epsilon}$:

$$\begin{aligned}
\sum_{p_1 \neq p_2} \mathbb{E}_W |\gamma_W(p_1, p_2)| &\leq \sum_{h=1}^{n-1} \binom{n}{h} \left(\frac{4\epsilon}{n}\right)^h \\
&= \left(1 + \frac{4\epsilon}{n}\right)^n - 1 - \left(\frac{4\epsilon}{n}\right)^n = O(\epsilon)
\end{aligned}$$

where the last line follows from the binomial theorem. \square

This, combined with the mixing time result we prove below, completes the proof that the second moments of the random circuit converge in time $O(n \log \frac{n}{\epsilon})$.

5.2 Markov Chain of Coefficients

The Markov chain acting on the coefficients is reducible because the state $\{0\}^n$ is isolated. However, if we remove it then the chain becomes irreducible. The presence of self loops implies aperiodicity therefore the chain is ergodic. We have already seen that the chain converges to the Haar uniform distribution (in Section 1.1) therefore the stationary state is the uniform state $\pi(x) = 1/(4^n - 1)$. Further, since the chain is symmetric and has uniform stationary distribution, the chain satisfies detailed balance (Eqn. 4.8) so is reversible. We now turn to obtaining bounds on the mixing time of this chain.

We want to show that the full chain converges to stationarity in time $\Theta(n \log \frac{n}{\epsilon})$. This implies (see later) that the gap is $\Theta(1/n)$. To prove this, we will construct another chain called the zero chain. This is the chain that counts the number of zeroes in the state. Since it is the zeroes that slow down the mixing, this chain will accurately describe the mixing time of the full chain.

Lemma 5.2. *The zero chain has transition matrix P on state space (we count non-zero positions) $\Omega = \{1, 2, \dots, n\}$.*

$$P(x, y) = \begin{cases} 1 - \frac{2x(3n-2x-1)}{5n(n-1)} & y = x \\ \frac{2x(x-1)}{5n(n-1)} & y = x-1 \\ \frac{6x(n-x)}{5n(n-1)} & y = x+1 \\ 0 & \text{otherwise} \end{cases} \quad (5.2)$$

for $1 \leq x, y \leq n$.

Proof. Suppose there are $n - x$ zeroes (so there are x non-zeroes). Then the only way the number of zeroes can decrease (i.e. for x to increase) is if a non-zero item is paired with a zero item and one of the 9 (out of 15) new states is chosen with no zeroes. The probability of choosing such a pair is $\frac{2x(n-x)}{n(n-1)}$ so the overall probability is $\frac{9}{15} \frac{2x(n-x)}{n(n-1)}$.

The number of zeroes can increase only if a pair of non-zero items is chosen and one of the 6 states is chosen with one zero. The probability of this occurring is $\frac{6}{15} \frac{x(x-1)}{n(n-1)}$.

The probability of the number of zeroes remaining unchanged is simply calculated by requiring the probabilities to sum to 1. \square

We see that the zero chain is a one-dimensional random walk on the line. It is a lazy random walk because the probability of moving at each step is < 1 . However, as the number of zeroes decreases, the probability of moving increases monotonically:

$$1 - P(x, x) = \frac{2x(3n - 2x - 1)}{5n(n - 1)} \geq 2x/5n < 1. \quad (5.3)$$

Lemma 5.3. *The stationary distribution of the zero chain is*

$$\pi_0(x) = \frac{3^x \binom{n}{x}}{4^n - 1}. \quad (5.4)$$

Proof. This can be proven by multiplying the transition matrix in Lemma 5.2 by the state Eqn. 5.4. Alternatively, it can be proven by counting the number of states with $n - x$ zeroes. There are $\binom{n}{x}$ ways of choosing which sites to make non-zero and each non-zero site can be one of three possibilities: 1, 2 or 3. The total number of states is $4^n - 1$, which gives the result. \square

Below we will prove the following theorem:

Theorem 5.4. *The zero chain mixes in time $\Theta(n \log \frac{n}{\epsilon})$.*

The 2-norm mixing time follows easily:

Theorem 5.5. *The zero chain has 2-norm mixing time $O(n \log 1/\epsilon)$.*

Proof. We use a lower bound on the 1-norm mixing time to show that the gap of the zero chain is $\Omega(1/n)$ and then use the 2-norm mixing bound Eqn. 4.13. In [25], Theorem 4.9, they prove the lower bound:

$$\tau_1(\epsilon) \geq \frac{1 - \Delta}{\Delta} \ln \frac{1}{2\epsilon} \quad (5.5)$$

where Δ is the eigenvalue gap. In Theorem 5.4, we showed $\tau_1(\epsilon) \leq Cn \ln \frac{n}{\epsilon}$ for some constant C . Combining,

$$\frac{1 - \Delta}{\Delta} \ln \frac{1}{2\epsilon} \leq Cn \ln \frac{n}{\epsilon} \quad (5.6)$$

for all $\epsilon > 0$. Divide by $\ln 1/\epsilon$ and take the limit $\epsilon \rightarrow 0$ to find

$$\frac{1 - \Delta}{\Delta} \leq Cn \quad (5.7)$$

which implies the gap is $\Omega(1/n)$. The 2-norm bound now follows from Eqn. 4.13. \square

Before proving Theorem 5.4, we will show how the mixing time of the full chain follows from this.

Corollary 5.6. *The full chain mixes in time $\Theta(n \log \frac{n}{\epsilon})$.*

Proof. Once the zero chain has approximately mixed, the distribution of zeroes is almost correct. We need to prove that the distribution of non-zeroes is correct after $O(n \log \frac{n}{\epsilon})$ steps too.

Once each site of the full chain has been hit, meaning it is chosen and paired with another site so not both equal zero, the chain has mixed. This is because, after each site has been hit, the probability distribution over the states is uniform. When the zero chain has approximately mixed, a constant fraction of sites are zero so the probability of hitting a site at each step is $\Theta(1/n)$. By the coupon collector argument, each site will have been hit with probability at least $1 - \epsilon$ in time $O(n \log \frac{n}{\epsilon})$. Once the zero chain has mixed to ϵ' , we can run the full chain this extra number of steps to ensure each site has been hit with high probability. Since the mixing of the zero chain only increases with time, the distance to stationarity of the full chain is now $1 - \epsilon - \epsilon'$. We make this formal below.

After $t_0 = O(n \log \frac{n}{\epsilon'})$ steps, the number of zeroes is ϵ' -close to the stationary distribution π_0 by Theorem 5.4 and only gets closer with more steps since the distance to stationarity decreases monotonically. The stationary distribution Eqn. 5.4 is approximately a Gaussian peaked at $3n/4$ with $O(n)$ variance. This means that, with high probability, the number of non-zeroes is close to $3n/4$. We will in fact only need that there is at least a constant fraction of non-zeroes; with probability at least $1 - \epsilon' - \exp(-\Omega(n))$ there will be at least $n/2$.

To prove the mixing time, we run the chain for time t_0 so the zero chain mixes to ϵ' . Then run for t_1 additional steps. Let $H_{i,t}$ be the event that site i is hit at step t . Let $H_i = \cup_{t=t_0+1}^{t_0+t_1} H_{i,t}$ and $H = \cap_{i=1}^n H_i$. We want to show $\mathbb{P}(H)$ is close to 1, or, in other words, that all sites are hit with high probability. Further let X_t be the random variable giving the number of non-zeroes at step t .

If at step $t-1$ site i is non-zero then the event $H_{i,t}$ occurs if the qubit is chosen, which occurs with probability $2/n$. If, however, it was zero then it must be paired with a non-zero thing for $H_{i,t}$ to hold. Conditioned on any history with $X_{t-1} \geq n/2$, this probability is $\geq 1/n$. In particular, we can condition on not having previously hit i and the bound does not change. Combining we have

$$\mathbb{P}\left(H_{i,t}^c \middle| [X_{t-1} \geq n/2] \cap \left(\bigcap_{t'=t_0+1}^{t-1} H_{i,t'}^c \right)\right) \leq 1 - 1/n.$$

Then, after t_1 extra steps,

$$\mathbb{P}\left(H_i^c \middle| \bigcap_{t=t_0}^{t_0+t_1-1} [X_t \geq n/2]\right) \leq (1 - 1/n)^{t_1}$$

which, using the union bound, gives

$$\mathbb{P}\left(H^c \middle| \bigcap_{t=t_0}^{t_0+t_1-1} [X_t \geq n/2]\right) \leq n(1 - 1/n)^{t_1}.$$

Now, since the zero chain has mixed to ϵ' ,

$$\mathbb{P}\left(\bigcap_{t=t_0}^{t_0+t_1-1} [X_t \geq n/2]\right) \leq t_1 \sum_{x=n/2}^{n-1} \pi_0(x) + \epsilon' \leq t_1 \exp(-O(n)) + \epsilon'$$

so

$$\mathbb{P}(H^c) \leq n(1 - 1/n)^{t_1} + t_1 \exp(-O(n)) + \epsilon'.$$

Now, choose $t_1 = n \ln \frac{2n}{\epsilon}$ so that $\mathbb{P}(H^c) \leq \delta$ where $\delta = \epsilon + t_1 \exp(-O(n))$. Choose $\epsilon = 1/n$ so that δ is $1/\text{poly}(n)$. Now, using the bound on $\mathbb{P}(H^c)$, we can write the state v after $t_1 = O(n \log n)$ steps as

$$v = (1 - \delta)\pi + \delta\pi'$$

where π is the stationary distribution and π' is any other distribution. Using this,

$$\|v - \pi\| \leq \delta.$$

We now apply Lemma A.15 to show that after $O(n \log \frac{n}{\epsilon})$ steps the distance to stationarity of the full chain is ϵ . \square

5.3 Proof of Theorem 5.4

We will now proceed to prove Theorem 5.4. We present an outline of the proof here; the details are in Section A.2.

Firstly, note that by the coupon collector argument, the lower bound on the time is $\Omega(n \log n)$. We need to prove an upper bound equal to this. Intuition says that the mixing time should take time $O(n \log n)$ because the walk has to move a distance $\Theta(n)$ and the waiting time at each step is proportional to $n, n/2, n/3, \dots$ which sums to $O(n \log n)$, provided each site is not hit too often. We will show that this intuition is correct using Chernoff bound and log-Sobolev (see later) arguments.

We will first work out concentration results of the position after some number of *accelerated* steps. The zero chain has some probability of staying still at each step. The accelerated chain is the zero chain conditioned on moving at each step. We define the accelerated chain by its transition matrix:

Definition 5.7. *The transition matrix for the accelerated chain is*

$$P_a(x, y) = \begin{cases} 0 & y = x \\ \frac{x-1}{3n-2x-1} & y = x-1 \\ \frac{3(n-x)}{3n-2x-1} & y = x+1 \\ 0 & \text{otherwise.} \end{cases} \quad (5.8)$$

We use the accelerated chain in the proof to firstly prove the accelerated chain mixes quickly, then to bound the waiting time at each step to obtain a mixing time bound for the zero chain.

To prove the mixing time bound, we will split the walk up into three phases. We will split the state space into three (slightly overlapping) parts and the phase can begin at any point within that space. So each phase has a state space $\Omega_i \subset [1, n]$, an entry space $E_i \subset \Omega_i$ and an exit condition T_i . We say that a phase completes successfully if the exit condition is satisfied in time $O(n \log n)$ for an initial state within the entry space. When the exit condition is satisfied, the walk moves onto the next phase.

The phases are:

1. $\Omega_1 = [1, n^\delta]$ for some constant δ with $0 < \delta < 1/2$. $E_1 = \Omega_1$ (i.e. it can start anywhere) and T_1 is satisfied when the walk reaches n^δ . For this part, the probability of moving backwards (gaining zeroes) is $O(n^{\delta-1})$ so the walk progresses forwards at each step with high probability. This is proven in Lemma A.8. We show that the waiting time is $O(n \log n)$ in Lemma A.9.
2. $\Omega_2 = [n^\delta/2, \theta n]$ for some constant θ with $0 < \theta < 3/4$. $E_2 = [n^\delta, \theta n]$ and T_2 is satisfied when the walk reaches θn . Here the walk can move both ways with constant probability but there is a $\Omega(1)$ forward bias. Here we use a monotonicity argument: the probability of moving forward at each step is

$$\begin{aligned} p(x) &= \frac{3(n-x)}{3n-2x-1} \\ &\geq \frac{3(n-x)}{3n-2x} \\ &\geq \frac{3(1-\theta)}{3-2\theta}. \end{aligned}$$

If we model this random walk as a walk with constant bias equal to $\frac{3(1-\theta)}{3-2\theta}$ we will find an upper bound on the mixing time since mixing time increases monotonically with decreasing bias. Further, the waiting time at $x = a$ stochastically dominates the waiting time at $x = b$ for $b \geq a$. The true bias decreases with position so the walk with constant bias spends more time at the early steps. Thus the position of this simplified walk is stochastically dominated by the position of the real walk while the waiting time stochastically dominates the waiting time of the real walk.

3. $\Omega_3 = [\frac{\theta}{2}n, n]$ and $E_3 = [\theta n, n]$. T_3 is satisfied when this restricted part of the chain has mixed to distance ϵ . Here the bias decreases to zero as the walk approaches $3n/4$ but the moving probability is a constant. We show that this walk mixes quickly by bounding the log-Sobolev constant of the chain.

Showing these three phases complete successfully will give a mixing time bound for the whole chain. We now prove in the Appendix that the phases complete successfully with probability at least $1 - 1/\text{poly}(n)$:

Lemma 5.8.

$$\mathbb{P}(\text{Phase 1 completes successfully}) \geq 1 - n^{2\delta-1} - 2n^{-\delta}$$

Lemma 5.9.

$$\mathbb{P}(\text{Phase 2 completes successfully}) \geq 1 - \exp\left(-\frac{2}{3}\mu\theta n\right) - \left(\frac{4}{\theta n}\right)^{\frac{3}{2\mu}} - \frac{2 \exp\left(\frac{-\mu n^\delta}{4}\right)}{1 - \exp(-\mu/2)} - (q/p)^{n^\delta/2}$$

where $\mu = \frac{6(1-\theta)}{3-2\theta} - 1$.

Lemma 5.10.

$$\mathbb{P}(\text{Phase 3 completes successfully}) \geq 1 - \left(\frac{\theta}{3(2-\theta)}\right)^{\theta n/2}$$

We can now finally combine to prove our result:

of Theorem 5.4. The stationary distribution has exponentially small weight in the tail with lots of zeroes. We show that, provided the number of zeroes is within phase 3, the walk mixes in time $O(n \log \frac{n}{\epsilon})$. We also show that if the number of zeroes is initially within phase 1 or 2, after $O(n \log n)$ steps the walk is in phase 3 with high probability. We can work out the distance to the stationary distribution as follows.

Let p_f be the probability of failure. This is the sum of the error probabilities in Lemmas 5.8, 5.9 and 5.10. The key point is that $p_f = 1/\text{poly}(n)$. Then after $O(n \log \frac{n}{\epsilon})$ steps (the sum of the number of steps in the 3 phases), the state is equal to $(1 - p_f)v_3 + p_f v'$ where v_3 is the state in the phase 3 space and v' is any other distribution, which occurs if any one of the phases fails. Since the distance to stationarity in phase 3 is ϵ , $\|v_3 - \pi_3\| \leq \epsilon$, where π_3 is the stationary distribution on the state space of phase 3. In Lemma A.13 we show that $\pi_3(x) = \pi(x)/(1 - w)$ where $w = \sum_{x=1}^{\theta n/2-1} \pi(x)$. Since $\pi(x)$ is exponentially small in this range, w is exponentially small in n . Now use the triangle inequality to find

$$\|v_3 - \pi\| \leq \|v_3 - \pi_3\| + \|\pi_3 - \pi\|. \quad (5.9)$$

Since the chain in phase 3 has mixed to ϵ , the first term is $\leq \epsilon$. We can evaluate $\|\pi_3 - \pi\|$:

$$\begin{aligned} \|\pi_3 - \pi\| &= \frac{1}{2} \sum_{x=1}^n \|\pi_3(x) - \pi(x)\| \\ &= \frac{1}{2} \left(\sum_{x=1}^{\theta n/2-1} \pi(x) + \sum_{x=\theta n/2}^n (\pi(x)/(1 - w) - \pi(x)) \right) \\ &= \frac{1}{2} (w + 1 - (1 - w)) = w. \end{aligned}$$

So now,

$$\begin{aligned} \|(1 - p_f)v_3 + p_f v' - \pi\| &= \|(1 - p_f)(v_3 - \pi) + p_f(v' - \pi)\| \\ &\leq (1 - p_f)\|v_3 - \pi\| + p_f\|v' - \pi\| \\ &\leq (1 - p_f)(\epsilon + w) + p_f \\ &\leq \delta \end{aligned}$$

where $\delta = \epsilon + w + p_f$. We are free to choose ϵ : choose it to be $1/n$ so that δ is $1/\text{poly}(n)$. So now the running time to get a distance δ is $t = O(n \log n)$. We then apply Lemma A.15 to obtain the result.

This concludes the proof of Theorem 5.4 so Corollary 5.6 is proved. \square

We have now proven Lemma 2.11 and consequently Corollary 2.12. We now show how Theorem 2.10 follows.

6 Main Result

We will now show how the mixing time results imply that we have an approximate 2-design.

Proof of Theorem 2.10: We will go via the 2-norm since this gives a tight bound when working with the Pauli operators. The supremum can be taken over just physical states ρ [29]. We write ρ in the Pauli basis as usual (as Eqn. 2.3).

$$\begin{aligned} \|\mathcal{G}_W - \mathcal{G}_H\|_{\diamond}^2 &= \sup_{\rho} \|(\mathcal{G}_W \otimes I)(\rho) - (\mathcal{G}_H \otimes I)(\rho)\|_1^2 \\ &\leq 2^{4n} \sup_{\rho} \|(\mathcal{G}_W \otimes I)(\rho) - (\mathcal{G}_H \otimes I)(\rho)\|_2^2 \\ &= \sup_{\rho} \left\| \sum_{\substack{p_1, p_2, p_3, p_4 \\ p_1 p_2 \neq 00}} \gamma_0(p_1, p_2, p_3, p_4) (\mathcal{G}_W(\sigma_{p_1} \otimes \sigma_{p_2}) \otimes \sigma_{p_3} \otimes \sigma_{p_4} \right. \\ &\quad \left. - \mathcal{G}_H(\sigma_{p_1} \otimes \sigma_{p_2}) \otimes \sigma_{p_3} \otimes \sigma_{p_4}) \right\|_2^2 \end{aligned}$$

Now, write (for $p_1 p_2 \neq 00$) $\mathcal{G}_W(\frac{1}{2^n} \sigma_{p_1} \otimes \sigma_{p_2}) = \frac{1}{2^n} \sum_{q_1, q_2} g_t(q_1, q_2; p_1, p_2) \sigma_{q_1} \otimes \sigma_{q_2}$. We get

$$\begin{aligned} &\sup_{\rho} \left\| \sum_{\substack{p_1, p_2, p_3, p_4, q_1, q_2 \\ p_1 p_2 \neq 00, q_1 q_2 \neq 00}} \gamma_0(p_1, p_2, p_3, p_4) \left(g_t(q_1, q_2; p_1, p_2) - \frac{\delta_{q_1 q_2} \delta_{p_1 p_2}}{2^n (2^n + 1)} \right) \right. \\ &\quad \left. \sigma_{q_1} \otimes \sigma_{q_2} \otimes \sigma_{p_3} \otimes \sigma_{p_4} \right\|_2^2 \\ &= 2^{4n} \sup_{\rho} \sum_{\substack{p_1, p_2, p_3, p_4, q_1, q_2 \\ p_1 p_2 \neq 00, q_1 q_2 \neq 00}} \gamma_0^2(p_1, p_2, p_3, p_4) \left(g_t(q_1, q_2; p_1, p_2) - \frac{\delta_{q_1 q_2} \delta_{p_1 p_2}}{2^n (2^n + 1)} \right)^2 \\ &\leq 2^{4n} \sup_{\rho} \sum_{\substack{p_1, p_2, p_3, p_4 \\ p_1 p_2 \neq 00}} \gamma_0^2(p_1, p_2, p_3, p_4) \epsilon^2 \\ &\leq 2^{4n} \epsilon^2 \end{aligned}$$

where the first equality comes from the orthogonality of the Pauli operators under the Hilbert-Schmidt inner product and the last inequality comes from the fact that ρ is a physical state so has $\text{tr } \rho^2 \leq 1$. This proves the result for the diamond norm, Definition 2.5. For the distance measure defined in Definition 2.6, the argument in [10] can be used together with the 1-norm bound to prove the result. \square

It is unfortunate that there is still a dimension factor remaining in the above proof. To get a distance ϵ we have to run the random circuit for $O(n(n + \log 1/\epsilon))$ steps. However, closeness in the diamond-norm may be too stringent a requirement. After $O(n(n + \log 1/\epsilon))$ steps, the random circuit gives a 2-design in the measure used by Dankert et al. (see [10] and Definition 2.6). This is in contrast to the $O(n \log 1/\epsilon)$ steps required by the explicit circuit construction of Dankert et al.

7 Conclusions

We have proved tight convergence results for the first two moments of a random circuit. We have used this to show that random circuits are efficient approximate 1- and 2-unitary designs. Our framework readily generalises to k -designs for any k and the next step in this research is to prove that random circuits give approximate k -designs for all k .

We have shown that, provided the random circuit uses gates from a universal gate set that is also universal on $U(4)$, the circuit is still an efficient 2-design. We also see that the random circuit with gates chosen uniformly from $U(4)$ is the most natural model. We note that the gates from $U(4)$ can be replaced by gates from any approximate 2-design on two qubits without any change to the asymptotic convergence properties.

One application of this work is to give an efficient method of decoupling two quantum systems by applying a random unitary from a 2-design to one system and then discarding part of it. This technique is used in [2] to construct a variety of encoding circuits for tasks in quantum Shannon theory; thus, we (like [10]) reduce the encoding complexity in [2] (and related works, such as [21]) to $O(n^2)$. Unfortunately, the decoding circuits still remain inefficient.

An algorithmic application of random circuits was given in [19], where they were used to construct a new class of superpolynomial quantum speedups. In that paper, random circuits of length $O(n^3)$ were used in order to guarantee that they were so-called “dispersing” circuits. Our results immediately imply that circuits of length $O(n^2)$ would instead suffice. We believe that this could be further improved with a specialised argument, since [19] assumed that the input to the random circuit was always a computational basis state.

Another potential application of random circuits is to model the evolution of black holes [22]. In Ref. [22], they conjecture that short random local quantum circuits are approximately 2-designs, and thus can be used for decoupling quantum systems (as in [2]). This, in turn, is used to make claims about the rate at which black holes leak information. While our model differs from that of Ref. [22] in that they consider nearest-neighbour interactions and we do not, our techniques and results could be readily extended to cover the case they consider.

Finally, random circuits are interesting physical models in their own right. The original purpose of [26] was to answer the physical question of how quickly entanglement grows in a system with random two party interactions. Lemma 2.11(i) shows that $O(n(n + \log 1/\epsilon))$ steps suffice (in contrast to $O(n^2(n + \log 1/\epsilon))$ which they prove) to give almost maximal entanglement in such a system.

Acknowledgements. We are grateful for funding from the Army Research Office under grant W9111NF-05-1-0294, the European Commission under Marie Curie grants ASTQIT (FP6-022194) and QAP (IST-2005-15848), and the U.K. Engineering and Physical Science Research Council through “QIP IRC.” We thank Raphaël Clifford, Ashley Montanaro and Dan Shepherd for helpful discussions.

A Appendix

A.1 Permutation Operators

The following theorems about permutation operators will be used repeatedly.

Lemma A.1. *Let C be a cycle of length c in S_c . Then*

$$\text{tr} (C (A_1 \otimes A_2 \otimes \dots \otimes A_c)) = \text{tr} (A_{C(1)} A_{C^{\circ 2}(1)} A_{C^{\circ 3}(1)} \dots A_1).$$

Proof. We have

$$\begin{aligned} \text{tr} (C (A_1 \otimes A_2 \otimes \dots \otimes A_c)) &= \sum_{i_1, i_2, \dots, i_c} \langle i_1 i_2 \dots i_c | C (A_1 \otimes A_2 \otimes \dots \otimes A_c) | i_1 i_2 \dots i_c \rangle \\ &= \sum_{i_1, i_2, \dots, i_c} \langle i_1 | A_{C(1)} | i_{C(1)} \rangle \langle i_2 | A_{C(2)} | i_{C(2)} \rangle \dots \langle i_c | A_{C(c)} | i_{C(c)} \rangle \\ &= \sum_{i_1, i_2, \dots, i_c} \langle i_1 | A_{C(1)} | i_{C(1)} \rangle \langle i_{C(1)} | A_{C^{\circ 2}(1)} | i_{C^{\circ 2}(1)} \rangle \dots \langle i_{C^{\circ c-1}(1)} | A_1 | i_1 \rangle \end{aligned}$$

since $C^{\circ c}(1) = 1$. Evaluate the sum using the resolution of the identity to get the result. \square

With this we can work out the Pauli expansion of the swap operator:

Lemma A.2. *The swap operator \mathcal{F} on two d dimensional systems can be written as*

$$\frac{1}{d} \sum_p \sigma_p \otimes \sigma_p.$$

where $\{\sigma_p\}$ form a Hermitian orthogonal basis with $\text{tr} \sigma_p^2 = d$.

Proof. Expand \mathcal{F} in the basis and use Lemma A.1:

$$\begin{aligned} \text{tr} \sigma_p \otimes \sigma_q \mathcal{F} &= \text{tr} \sigma_p \sigma_q \\ &= \begin{cases} d & p = q \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

The given sum has the correct coefficients in the basis therefore $\frac{1}{d} \sum_p \sigma_p \otimes \sigma_p = \mathcal{F}$. \square

A.2 Zero chain mixing time proofs

A.2.1 Asymmetric Simple Random Walk

We will use some facts about asymmetric simple random walks i.e. a random walk on a 1D line with probability p of moving right at each step and probability $q = 1 - p$ of moving left.

The position of the walk after k steps is tightly concentrated around $k(p - q)$:

Lemma A.3. Let X_k be the random variable giving the position of a random walk after k steps starting at the origin with probability p of moving right and probability $q = 1 - p$ of moving left. Let $\mu = p - q$. Then for any $\eta > 0$,

$$\mathbb{P}(X_k \geq \mu k + \eta) \leq \exp\left(-\frac{\eta^2}{2k}\right)$$

and

$$\mathbb{P}(X_k \leq \mu k - \eta) \leq \exp\left(-\frac{\eta^2}{2k}\right).$$

Proof. The standard Chernoff bound for 0/1 variables \tilde{Y}_i gives, with \tilde{Y}_i equal to 1 with probability p and for $Y_k = \sum_{i=1}^k \tilde{Y}_i$,

$$\begin{aligned}\mathbb{P}(Y_k \geq kp + \eta) &\leq \exp\left(-\frac{2\eta^2}{k}\right) \\ \mathbb{P}(Y_k \leq kp - \eta) &\leq \exp\left(-\frac{2\eta^2}{k}\right).\end{aligned}$$

For our case, set $\tilde{Y}_i = 2\tilde{X}_i - 1$ to give the desired result. \square

This result is for a walk with constant bias. We will need a result for a walk with varying (but bounded from below) bias:

Lemma A.4. Let X_k be the random variable giving the position of a random walk after k steps starting at the origin with probability $p_i \geq p$ of moving right and probability $q_i \leq p$ of moving left at step i . Let $\mu = p - (1 - p)$. Then for any $\eta > 0$,

$$\mathbb{P}(X_k \geq \mu k + \eta) \leq \exp\left(-\frac{\eta^2}{2k}\right)$$

and

$$\mathbb{P}(X_k \leq \mu k - \eta) \leq \exp\left(-\frac{\eta^2}{2k}\right).$$

Proof. Let \tilde{Y}_i be a random variable equal to 1 with probability p and 0 with probability $1 - p$. Then let \tilde{Z}_i be a random variable equal to 1 with probability p_i and 0 with probability $1 - p_i$. Let $Y_k = \sum_{i=1}^k \tilde{Y}_i$ and $Z_k = \sum_{i=1}^k \tilde{Z}_i$. Then following the standard Chernoff bound derivation (for $\lambda > 0$),

$$\begin{aligned}\mathbb{P}(Z_k \geq kp + \eta) &= \mathbb{P}\left(e^{\lambda Z_k} \geq e^{\lambda(kp+\eta)}\right) \\ &\leq \frac{e^{\lambda(kp+\eta)}}{\mathbb{E}e^{\lambda Z_k}} \\ &\leq \frac{e^{\lambda(kp+\eta)}}{\mathbb{E}e^{\lambda Y_k}} \\ &\leq \exp\left(-\frac{2\eta^2}{k}\right).\end{aligned}$$

We can then, as above, set $\tilde{Z}_i = 2\tilde{X}_i - 1$. The calculation is similar for the bound on $\mathbb{P}(X_k \leq \mu k - \eta)$. \square

From Lemma A.3 we can prove a result about how often each site is visited. If the walk runs for t steps the walk is at position $t\mu$ with high probability so we might expect from symmetry that each site will have been visited about $1/\mu$ times. Below is a weaker concentration result of this form but is strong enough for our purposes. It says that the amount of time spent $\leq x$ is about x/μ .

Lemma A.5. *For $\gamma > 2$ and integer $x > 0$,*

$$\mathbb{P}\left(\sum_{k=1}^{\infty} \mathbb{I}(X_k \leq x) \geq \gamma x/\mu\right) \leq 2 \exp\left(-\frac{\mu x(\gamma-2)}{2}\right),$$

where \mathbb{I} is the indicator function.

Proof. Let $Y_k = \mathbb{I}(X_k \leq x)$. From Lemma A.3,

$$\mathbb{P}(Y_k = 0) \leq \exp\left(-\frac{(k\mu - x)^2}{2k}\right)$$

for $k \leq x/\mu$ and

$$\mathbb{P}(Y_k = 1) \leq \exp\left(-\frac{(k\mu - x)^2}{2k}\right)$$

for $k \geq x/\mu$.

Then the quantity to evaluate is

$$\mathbb{P}\left(\sum_{k=1}^{\infty} Y_k \geq \gamma x/\mu\right).$$

We use a standard trick to split this into two mutually exclusive possibilities and then bound the probabilities separately. Write

$$\begin{aligned} \mathbb{P}\left(\sum_{k=1}^{\infty} Y_k \geq \gamma x/\mu\right) &= \\ \mathbb{P}\left(\left(\sum_{k=1}^{\infty} Y_k \geq \gamma x/\mu\right) \cap \left(\bigcap_{j=1}^{\lceil \gamma x/\mu \rceil} [Y_j = 1]\right)\right) + \mathbb{P}\left(\left(\sum_{k=1}^{\infty} Y_k \geq \gamma x/\mu\right) \cap \left(\bigcup_{j=\lceil \gamma x/\mu \rceil+1}^{\infty} [Y_j = 0]\right)\right). \end{aligned} \quad (\text{A.1})$$

We can bound the first term:

$$\begin{aligned} \mathbb{P}\left(\left(\sum_{k=1}^{\infty} Y_k \geq \gamma x/\mu\right) \cap \left(\bigcap_{j=1}^{\lceil \gamma x/\mu \rceil} [Y_j = 1]\right)\right) &= \mathbb{P}\left(\bigcap_{k=1}^{\lceil \gamma x/\mu \rceil} Y_k = 1\right) \\ &\leq \mathbb{P}(Y_{\gamma x/\mu} = 1) \\ &\leq \exp\left(-\frac{\mu x(\gamma-1)^2}{2\gamma}\right) \\ &\leq \exp\left(-\frac{\mu x(\gamma-2)}{2}\right) \end{aligned}$$

The second term similarly:

$$\begin{aligned}
\mathbb{P} \left(\left(\sum_{k=1}^{\infty} Y_k \geq \gamma x / \mu \right) \cap \left(\bigcup_{j=1}^{\gamma x / \mu} [Y_j = 0] \right) \right) &\leq \mathbb{P} \left(\bigcup_{k=\frac{\gamma x}{\mu}+1}^{\infty} [Y_k = 1] \right) \\
&\leq \sum_{k=\frac{\gamma x}{\mu}+1}^{\infty} \mathbb{P}(Y_k = 1) \\
&\leq \sum_{k=\frac{\gamma x}{\mu}+1}^{\infty} \exp \left(-\frac{(k\mu - x)^2}{2k} \right) \\
&\leq \exp \left(-\frac{\mu x(\gamma - 2)}{2} \right)
\end{aligned}
\quad \square$$

The last fact we need about asymmetric simple random walks is a bound on the probability of going backwards. If $p > q$ then we expect the walk to go right in the majority of steps. The probability of going left a distance a is exponentially small in a . This is a well known result, often stated as part of the gambler's ruin problem:

Lemma A.6 (See e.g. [17]). *Consider an asymmetric simple random walk that starts at $a > 0$ and has an absorbing barrier at the origin. The probability that the walk eventually absorbs at the origin is 1 if $p \leq q$ and $(q/p)^a$ otherwise.*

This result is for infinitely many steps. If we only consider finitely many steps, the probability of absorption must be at most this.

A.2.2 Waiting Time

From above we saw that the probability of moving is at least $2x/5n$ when at position x . The length of time spent waiting at each step is therefore stochastically dominated by a geometric distribution with parameter $2x/5n$. The following concentration result will be used to bound the waiting time (in our case $\beta = 2/5$):

Lemma A.7. *Let the waiting time at each site be $W(x) \sim \text{Geo}(\beta x/n)$, the total waiting time $W = \sum_{x=1}^t W(x)$ and $t' = \frac{n \ln t}{\beta}$. Then*

$$\mathbb{P}(W \geq Ct') \leq 2t^{(1-C)/2}.$$

Proof. By Markov's inequality for $\lambda > 0$,

$$\mathbb{P}(W \geq Ct') \leq \frac{\mathbb{E}e^{\lambda W}}{e^{\lambda Ct'}}.$$

The $W(x)$ are independent so

$$\mathbb{E}e^{\lambda W} = \prod_{x=1}^t \mathbb{E}e^{\lambda W(x)}.$$

Summing the geometric series we find

$$\mathbb{E}e^{\lambda W(x)} = \frac{\frac{\beta x}{n}}{e^{-\lambda} - 1 + \frac{\beta x}{n}}$$

provided $e^\lambda < \frac{1}{1 - \frac{\beta x}{n}}$ for all $1 \leq x \leq t$. Therefore e^λ is of the form $\frac{1}{1 - \frac{\alpha \beta}{n}}$ where $0 < \alpha < 1$. With this,

$$\mathbb{E}e^{\lambda W(x)} = \frac{x}{x - \alpha}$$

and

$$\mathbb{E}e^{\lambda W} = \frac{t! \Gamma(1 - \alpha)}{\Gamma(t + 1 - \alpha)}.$$

We are free to choose α within its range to optimise the bound. However, for simplicity, we will choose $\alpha = 1/2$. From Lemma A.14,

$$\mathbb{E}e^{\lambda W} \leq 2\sqrt{t}.$$

The result follows, using the inequality $1 - x \leq e^{-x}$. \square

A.2.3 Phase 1

Here we prove that phase 1 completes successfully with high probability. The bias here is large so the walk moves right every time with high probability:

Lemma A.8. *The probability that the accelerated chain moves right at each step, starting from $x = 1$ for t steps, is at least*

$$1 - t^2/n.$$

Proof. The probability of moving right at each step is

$$\begin{aligned} \prod_{x=1}^t \frac{3(n-x)}{3n-2x-1} &= \frac{(n-2)(n-3)\dots(n-t)}{(n-5/3)(n-7/3)\dots(n-(2t+1)/3)} \\ &\geq (1-2/n)(1-3/n)\dots(1-t/n) \\ &\geq (1-t/n)^t \geq 1 - t^2/n \end{aligned}$$

\square

Let $t = n^\delta$. Provided $\delta < 1/2$ this probability is close to one. Therefore, with high probability, the walk moves to n^δ in n^δ steps. Using Lemma A.7 the waiting time can be bounded:

Lemma A.9. *Let $W^{(1)}$ be the waiting time during phase 1. Let H be the event that the walk moves right at each step. Then*

$$\mathbb{P}\left(W^{(1)} \geq Ct' | H\right) \leq 2n^{\delta(1-C)/2} \tag{A.2}$$

where $t' = \frac{5\delta n \ln n}{2}$.

Proof. This follows directly from Lemma A.7, since each site is hit exactly once. \square

We now combine these two lemmas to prove that phase 1 completes successfully with high probability:

Proof of Lemma 5.8. In Lemma A.8, we show that in n^δ accelerated steps, the walk moves right at each step with probability $\geq 1 - n^{2\delta-1}$. Call this event H . Then $\mathbb{P}(H) \geq 1 - n^{2\delta-1}$. Lemma A.9 shows that the waiting time $W^{(1)}$ is bounded with high probability (choosing $C = 3$):

$$\mathbb{P}(W^{(1)} \leq 15n\delta \ln n/2 | H) \geq 1 - 2n^{-\delta}.$$

Then we can bound the probability of phase 1 completing successfully:

$$\begin{aligned} \mathbb{P}(\text{Phase 1 completes successfully}) &\geq \mathbb{P}(H \cap W^{(1)} \leq 15n\delta \ln n/2) \\ &= \mathbb{P}(H)\mathbb{P}(W^{(1)} \leq 15n\delta \ln n/2 | H) \\ &\geq (1 - n^{2\delta-1})(1 - 2n^{-\delta}) \\ &\geq 1 - n^{2\delta-1} - 2n^{-\delta}. \end{aligned} \quad \square$$

A.2.4 Phase 2

Phase 2 starts at $n^\delta/2$ and finishes when the walk has reached θn for some constant $0 < \theta < 3/4$. We show that, with high probability, this also takes time $O(n \log n)$. The probability of moving right during this phase is at least $p = \frac{3(1-\theta)}{3-2\theta}$. We first define some constants that we will derive bounds in terms of. Let γ be a constant > 2 . Let $\mu = p - (1-p)$ and $\tilde{\mu} = \mu/\gamma$. Finally let $s = \tilde{\mu}t$ for some t (which will be the number of accelerated steps). Then, with high probability, the walk will have passed s after t steps:

Lemma A.10. *Let X_t be the position of the walk at accelerated step t , where $X_0 = n^\delta$. Then*

$$\mathbb{P}(X_t \leq s) \leq \exp(-\mu^2 t(1 - 1/\gamma)^2/2).$$

Proof. Let $X'_t = X_t - n^\delta$. Then from Lemma A.4,

$$\mathbb{P}(X'_t \leq \mu t - \eta) \leq \exp\left(-\frac{\eta^2}{2t}\right).$$

Now let $\eta = \mu t - s$ and use

$$\begin{aligned} \mathbb{P}(X_t \leq s) &= \mathbb{P}(X'_t \leq s - n^\delta) \\ &\leq \mathbb{P}(X'_t \leq s) \end{aligned}$$

to complete the proof. \square

We now prove a bound on the waiting time:

Lemma A.11. *Let $W^{(2)}$ be the waiting time in phase 2. Then, assuming the walk does not go back beyond $n^\delta/2$,*

$$\mathbb{P}\left(W^{(2)} \geq \frac{15n \ln s}{\mu}\right) \leq (4/s)^{3/2\mu} + \frac{2 \exp\left(\frac{-\mu n^\delta}{4}\right)}{1 - \exp\left(\frac{-\mu}{2}\right)}. \quad (\text{A.3})$$

Proof. Let $W_k \sim Geo\left(\frac{2X_k}{5n}\right)$ where X_k is the position of the walk at accelerated step k ($X_0 = n^\delta$). We want to bound (w.h.p.) the waiting time $W^{(2)} = \sum_{k=1}^t W_k$ of t steps of the accelerated walk. Define the event H to be

$$H = \left\{ \bigcap_{x \geq n^\delta/2} \left[\sum_{k=1}^{\infty} \mathbb{I}(X_k \leq x) \leq x/\tilde{\mu} \right] \right\}. \quad (\text{A.4})$$

If H occurs, no sites have been hit too often and the walk has not gone back further than $n^\delta/2$. It is important that we also use the restriction that $X_k \geq n^\delta/2$ because the waiting time grows the longer the walk moves back. However, it is very unlikely that the walk will go backwards (even to $n^\delta/2$).

We now define some more notation to bound the waiting time. Let $\mathbf{X} = (X_1, X_2, \dots, X_t)$ be a tuple of positions and let $N_x(\mathbf{X})$ be the number of times that x appears in \mathbf{X} and let $\mathbf{N}(\mathbf{X}) = (N_1(\mathbf{X}), N_2(\mathbf{X}), \dots, N_n(\mathbf{X}))$. Then we have $\sum_x N_x(\mathbf{X}) = t$.

As we said above, the waiting time at $x = a$ stochastically dominates the waiting time at $x = b$ for $b \geq a$. In other words,

$$W_k \trianglerighteq W_{k'} \text{ if } X_k \leq X_{k'} \quad (\text{A.5})$$

where $X \trianglerighteq Y$ means that X stochastically dominates Y . Now write the waiting time for all steps

$$\begin{aligned} W^{(2)}(\mathbf{X}) &= \sum_{k=1}^t W_k \\ &= \sum_x \sum_{h=1}^{N_x(\mathbf{X})} W_h(x) \end{aligned} \quad (\text{A.6})$$

where $W_h(x) \sim Geo\left(\frac{2x}{5n}\right)$.

If event H occurs, we can put some bounds on N_x . We find that, for all $x \geq n^\delta/2$,

$$\sum_{y=n^\delta/2}^x N_y(\mathbf{X}) \leq x/\tilde{\mu} \quad (\text{A.7})$$

and $N_x(\mathbf{X}) = 0$ for $x < n^\delta/2$. Now let \mathbf{X}_m be such that $N_{n^\delta/2}(\mathbf{X}_m) = \frac{n^\delta}{2\tilde{\mu}}$ and $N_x(\mathbf{X}_m) = 1/\tilde{\mu}$ for $x > n^\delta/2$. Then

$$\sum_{y=n^\delta/2}^x N_y(\mathbf{X}_m) = x/\tilde{\mu}. \quad (\text{A.8})$$

Now we introduce the relation \preceq :

Definition A.12. Let \mathbf{x} and \mathbf{y} be n -tuples. Then $\mathbf{x} \preceq \mathbf{y}$ if

$$\sum_{i=1}^k x_i \leq \sum_{i=1}^k y_i \quad (\text{A.9})$$

for all $1 \leq k \leq n$ with equality for $k = n$.

Note that this is like majorisation, except the elements of the tuples are not sorted. Using this, we find that $\mathbf{N}(\mathbf{X}) \preceq \mathbf{N}(\mathbf{X}_m)$ (Using $\sum_y N_y(\mathbf{X}) = \sum_y N_y(\mathbf{X}') = t$ for all \mathbf{X}, \mathbf{X}' .)

If we combine Equations A.5 and A.6 we find that $W^{(2)}(\mathbf{X}) \geq W^{(2)}(\mathbf{X}')$ if $\mathbf{N}(\mathbf{X}) \succeq \mathbf{N}(\mathbf{X}')$. Roughly speaking, this is simply saying that the waiting time is larger if the earlier sites are hit more often. But since for all \mathbf{X} that satisfy H , $\mathbf{X} \preceq \mathbf{X}_m$, we have $W^{(2)}(\mathbf{X}) \leq W^{(2)}(\mathbf{X}_m)$ provided H occurs. We will simplify further by noting that $\mathbf{X}_m \preceq \mathbf{X}_0$ where $N_x(\mathbf{X}_0) = 1/\tilde{\mu}$ for $1 \leq x \leq \tilde{\mu}t = s$ and zero elsewhere. Therefore

$$\mathbb{P}\left(W^{(2)}(\mathbf{X}) \geq \frac{5Cn \ln s}{2\tilde{\mu}} \mid H\right) \leq \mathbb{P}\left(W^{(2)}(\mathbf{X}_0) \geq \frac{5Cn \ln s}{2\tilde{\mu}}\right).$$

We can bound this by applying Lemma A.7. Let $W_h = \sum_{x=1}^s W_h(x)$. From Lemma A.7,

$$\mathbb{P}(W_h \geq Ct') \leq 2s^{\frac{1-C}{2}} \quad (\text{A.10})$$

where $t' = \frac{5n \ln s}{2}$. However, we want a bound on $\mathbb{P}\left(\sum_{h=1}^{1/\tilde{\mu}} W_h \geq Ct'/\tilde{\mu}\right)$. The same reasoning as in Lemma A.7 bounds this as

$$\mathbb{P}\left(\sum_{h=1}^{1/\tilde{\mu}} W_h \geq Ct'/\tilde{\mu}\right) \leq \left(2s^{\frac{1-C}{2}}\right)^{1/\tilde{\mu}}. \quad (\text{A.11})$$

Therefore

$$\mathbb{P}\left(W^{(2)}(\mathbf{X}_0) \geq \frac{5Cn \ln s}{2\tilde{\mu}}\right) \leq 2^{1/\tilde{\mu}} s^{\frac{(1-C)/2}{\tilde{\mu}}}. \quad (\text{A.12})$$

To complete the proof, we just need to find $\mathbb{P}(H^c)$. We can bound it using the union bound and Lemma A.5:

$$\begin{aligned} \mathbb{P}(H^c) &= \mathbb{P}\left(\bigcup_{x=n^\delta/2}^n \left[\sum_{k=1}^{\infty} \mathbb{I}(X_k \leq x) > x/\tilde{\mu}\right]\right) \\ &\leq \sum_{x=n^\delta/2}^n \mathbb{P}\left(\sum_{k=1}^{\infty} \mathbb{I}(X_k \leq x) \geq x/\tilde{\mu}\right) \\ &\leq \sum_{x=n^\delta/2}^n 2 \exp\left(\frac{-\mu x(\gamma-2)}{2}\right) \\ &\leq \sum_{x=n^\delta/2}^{\infty} 2 \exp\left(\frac{-\mu x(\gamma-2)}{2}\right) \\ &= \frac{2 \exp\left(\frac{-\mu n^\delta(\gamma-2)}{4}\right)}{1 - \exp\left(\frac{-\mu(\gamma-2)}{2}\right)} \end{aligned}$$

Now, for any events A and B

$$\begin{aligned}\mathbb{P}(A) &= \mathbb{P}(A \cap B) + \mathbb{P}(A \cap B^c) \\ &= \mathbb{P}(A|B)\mathbb{P}(B) + \mathbb{P}(A \cap B^c) \\ &\leq \mathbb{P}(A|B) + \mathbb{P}(B^c)\end{aligned}$$

and set $C = 2$ and $\gamma = 3$ to obtain the result. \square

We now combine these two lemmas to prove that phase 2 completes successfully with high probability:

Proof of Lemma 5.9. Phase 2 can fail if:

- The walk does not reach θn . The probability of this is bounded by Lemma A.10:

$$\mathbb{P}(X_t \leq \theta n) \leq \exp\left(-\frac{2}{3}\mu\theta n\right).$$

This follows from setting $t = \frac{3\theta n}{\mu}$ and $\gamma = 3$.

- The waiting time is too long. This probability is bounded by Lemma A.11:

$$\mathbb{P}\left(W^{(2)} \geq \frac{15n \ln(\theta n)}{\mu}\right) \leq \left(\frac{4}{\theta n}\right)^{\frac{3}{2\mu}} + \frac{2 \exp\left(\frac{-\mu n^\delta}{4}\right)}{1 - \exp(-\mu/2)} + (q/p)^{n^\delta/2}.$$

- The walk gets back to $n^\delta/2$. This is bounded by Lemma A.6:

$$\mathbb{P}\left(\text{Walk gets to } n^\delta/2\right) \leq (q/p)^{n^\delta/2}.$$

So, using the union bound we can bound the overall probability of failure:

$$\mathbb{P}(\text{Phase 2 fails}) \leq \exp\left(-\frac{2}{3}\mu\theta n\right) + \left(\frac{4}{\theta n}\right)^{\frac{3}{2\mu}} + \frac{2 \exp\left(\frac{-\mu n^\delta}{4}\right)}{1 - \exp(-\mu/2)} + (q/p)^{n^\delta/2}. \quad \square$$

A.2.5 Phase 3

This phase starts at θn . We show that this mixes quickly using log-Sobolev arguments.

Lemma A.13. *The zero chain on the restricted state space $x \in [m, n]$ where $m = \theta n/2$ for $0 \leq \theta \leq 3/4$ has mixing time $O(n \log \frac{n}{\epsilon})$.*

Proof. We restrict the Markov chain to only run from m by adjusting the holding probability at m , $P(m, m)$. Construct the chain P' with transition matrix

$$P'(x, y) = \begin{cases} 0 & x < m \text{ or } y < m \\ 1 - P(m, m+1) & x = y = m \\ P(x, y) & \text{otherwise} \end{cases} \quad (\text{A.13})$$

where P is the transition matrix of the full zero chain. This chain then has stationary distribution

$$\pi'(x) = \begin{cases} \pi(x)/(1-w) & m \leq x \leq n \\ 0 & \text{otherwise} \end{cases} \quad (\text{A.14})$$

where $w = \sum_{x=1}^{m-1} \pi(x)$. To see this, first note that the distribution is normalised. We want to show that

$$\sum_{x=m}^n P'(x, y) \pi'(x) = \pi'(y). \quad (\text{A.15})$$

When $y = m$ we are required to prove that $P'(m, m)\pi'(m) + P'(m+1, m)\pi'(m+1) = \pi'(m)$. This follows from the reversibility of the unrestricted zero chain, using $P'(m, m) = 1 - P(m, m+1)$. For $y > m$, Eqn. A.15 is satisfied simply because $\pi(x)$ is the stationary distribution of P and related by a constant factor to $\pi'(x)$.

We can now prove this final mixing time result, making use of Lemma 4.10. Let Q_i be the chain that uniformly mixes site i . This converges in one step and has a log-Sobolev constant independent of n ; call it ρ_1 . Let Q be the chain that chooses a site at random and then uniformly mixes that site. This is the product chain of the Q_i so, by Lemma 4.10, has gap $1/n$ and Sobolev constant $\rho_Q = \rho_1/n$. We can construct the zero chain for this and find its Sobolev constant.

The Sobolev constant is defined (Definition 4.8) in terms of a minimisation over functions on the state space. For the chain Q we can write

$$\rho_Q = \inf_{\phi} f(\phi).$$

If we restrict the infimum to be over functions ϕ with $\phi(x) = \phi(y)$ for x and y containing the same number of zeroes then we obtain the Sobolev constant for the zero- Q chain, ρ_{Q_0} , which is chain which counts the number of zeroes in the full chain Q . Since taking the infimum over less functions cannot give a smaller value,

$$\rho_{Q_0} \geq \rho_Q \geq \rho_1/n.$$

We can now compare this chain to the zero- P chain. The stationary distributions are the same. The transition matrix for the zero- Q chain is

$$Q_0(x, y) = \begin{cases} \frac{n+2x}{4n} & y = x \\ \frac{x}{4n} & y = x-1 \\ \frac{3(n-x)}{4n} & y = x+1 \\ 0 & \text{otherwise} \end{cases}$$

Then construct Q'_0 by restricting the space to only run from m in exactly the same was as P' is constructed from P . Q'_0 has the same stationary distribution as P' . Now we can perform the comparison. From Eqn. 4.14:

$$\begin{aligned} A &= \max_{a \geq m} \frac{Q'_0(a, a+1)}{P'(a, a+1)} \\ &= \max_{a \geq m} \frac{5(n-1)}{8a} \leq \frac{5}{8\theta}. \end{aligned}$$

Therefore $\rho_{P'} \geq \frac{8\theta\rho_1}{5n}$. Exactly the same argument applies to show the gap is $\Omega(1/n)$ so the mixing time is (from Eqn. 4.16) $O(n \log \frac{n}{\epsilon})$. \square

Now we can prove that phase 3 completes successfully with high probability:

of Lemma 5.10. In Lemma A.13, we show that after $O(n \log \frac{n}{\epsilon})$ steps the chain mixes to distance ϵ . We just need to show that the walk goes back to $\theta n/2$ with small probability. This follows from Lemma A.6. \square

A.3 Moment Generating Function Calculations

The following lemma is needed in the moment generating function calculations.

Lemma A.14. *For Integer $s > 0$,*

$$\frac{\Gamma(s+1)\Gamma(1/2)}{\Gamma(s+1/2)} \leq 2\sqrt{s} \quad (\text{A.16})$$

Proof. From expanding the Γ functions, Eqn. A.16 becomes

$$\begin{aligned} \frac{s!2^s}{(2s-1)!!} &= \frac{2 \times 4 \times 6 \times \dots \times 2(s-1) \times 2s}{1 \times 3 \times 5 \times \dots \times (2s-3) \times (2s-1)} \\ &= \prod_{x=1}^s \frac{2x}{2x-1} \end{aligned}$$

We then proceed by induction. $\prod_{x=1}^1 \frac{2x}{2x-1} = 2$ and by the inductive hypothesis

$$\prod_{x=1}^{s+1} \frac{2x}{2x-1} \leq \frac{2(s+1)}{2(s+1)-1} 2\sqrt{s}.$$

It is easy to show that $\frac{2(s+1)}{2(s+1)-1} \leq \sqrt{\frac{s+1}{s}}$ and the result follows. \square

A.4 Mixing Times

We find bounds for the mixing time above that are valid with high probability. Below we turn these into full mixing time bounds.

Lemma A.15. *If after $O(n \log n)$ steps the state v of a random walk satisfies*

$$\|v - \pi\| \leq \delta$$

where π is the stationary distribution and δ is $1/\text{poly}(n)$ then the number of steps required to be at most a distance ϵ from stationarity is

$$O\left(n \log \frac{n}{\epsilon}\right).$$

Proof. Let s be the slowest mixing initial state. Then, after $t = O(n \log n)$ steps we have at worst the state

$$(1 - \delta)\pi + \delta s$$

and if we repeat kt times δ becomes δ^k . So to get a distance ϵ , $k = \left\lceil \frac{\log \epsilon}{\log \delta} \right\rceil$.

Now we evaluate the mixing time:

$$\begin{aligned}
kt &= O(n \log n) \left\lceil \frac{\log \epsilon}{\log \delta} \right\rceil = O(n \log n) \left\lceil \frac{\log 1/\epsilon}{\log 1/\delta} \right\rceil \\
&= O(n \max(\log n, \log 1/\epsilon)) \\
&= O\left(n \log \frac{n}{\epsilon}\right)
\end{aligned}
\quad \square$$

References

- [1] S. Aaronson. Quantum Copy-Protection and Quantum Money. *IEEE Conference on Computational Complexity 2009*, 2009.
- [2] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter. The mother of all protocols: Restructuring quantum information's family tree, 2006. arXiv:quant-ph/0606225.
- [3] A. Ambainis and J. Emerson. Quantum t-designs: t-wise independence in the quantum world. *IEEE Conference on Computational Complexity 2007*, 2007. arXiv:quant-ph/0701126v2.
- [4] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private Quantum Channels. *FOCS 2000*, pages 547–553, 2000.
- [5] A. Ambainis and A. Smith. Small Pseudo-Random Families of Matrices: Derandomizing Approximate Quantum Encryption. *Lecture Notes in Computer Science*, 3122/2004:249–260, 2004. arXiv:quant-ph/0404075.
- [6] V. I. Arnold and A. L. Krylov. Uniform distribution of points on a sphere and some ergodic properties of solutions of linear ordinary differential equations in a complex domain. *Soviet Math. Dokl.*, 4(1), 1962.
- [7] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello. Stabilization of quantum computations by symmetrization. *SIAM J. Comput.*, 26(5):1541–1557, 1997. arXiv:quant-ph/9604028.
- [8] H. Barnum. Information-disturbance tradeoff in quantum measurement on the uniform ensemble and on the mutually unbiased bases, 2002. arXiv:quant-ph/0205155.
- [9] O. C. O. Dahlsten, R. Oliveira, and M. B. Plenio. The emergence of typical entanglement in two-party random processes. *Journal of Physics A Mathematical General*, 40:8081–8108, 2007. arXiv:quant-ph/0701125.
- [10] C. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and Approximate Unitary 2-Designs: Constructions and Applications, 2006. arXiv:quant-ph/0606161.
- [11] I. Devetak, M. Junge, C. King, and M.B. Ruskai. Multiplicativity of completely bounded p-norms implies a new additivity result. *Commun. Math. Phys.*, 266:37–63, 2006. arXiv:quant-ph/0506196.

- [12] P. Diaconis and L. Saloff-Coste. Comparison Theorems for Reversible Markov Chains. *Ann. Appl. Probab.*, 3(3):696–730, 1993.
- [13] P. Diaconis and L. Saloff-Coste. Logarithmic Sobolev inequalities for finite Markov chains. *Ann. Appl. Probab.*, 6(3):695–750, 1996.
- [14] D. DiVincenzo, D. Leung, and B. Terhal. Quantum data hiding. *Information Theory, IEEE Transactions on*, 48(3):580–598, 2002. arXiv:quant-ph/0103098.
- [15] J. Emerson, E. Livine, and S. Lloyd. Convergence conditions for random quantum circuits. *Phys. Rev. A*, 72(060302), 2005. arXiv:quant-ph/0503210.
- [16] R. Goodman and N. Wallach. *Representations and Invariants of the Classical Groups*. Cambridge University Press, Cambridge, UK, 1998.
- [17] G. Grimmett and D. Welsh. *Probability: An Introduction*. Oxford University Press, Oxford, UK, 1986.
- [18] D. Gross, K. Audenaert, and J. Eisert. Evenly distributed unitaries: On the structure of unitary designs. *J. Math. Phys.*, 48(052104), 2007. arXiv:quant-ph/0611002.
- [19] S. Hallgren and A. W. Harrow. Superpolynomial speedups based on almost any quantum circuit, 2008. arXiv:0805.0007.
- [20] A. Hayashi, T. Hashimoto, and M. Horibe. Reexamination of optimal quantum state estimation of pure states. *Phys. Rev. A*, 72(032325), 2006. arXiv:quant-ph/0410207.
- [21] P. Hayden, M. Horodecki, J. Yard, and A. Winter. A decoupling approach to the quantum capacity, February 2007. arXiv:quant-ph/0702005.
- [22] P. Hayden and J. Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 09(120), 2007. arXiv:0708.4025.
- [23] S. Hoory and A. Brodsky. Simple Permutations Mix Even Better, 2004. arXiv:math/0411098.
- [24] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, Boston, MA, USA, 2002.
- [25] R. Montenegro and P. Tetali. Mathematical aspects of mixing times in Markov chains. *Found. Trends Theor. Comput. Sci.*, 1(3):237–354, 2006.
- [26] R. Oliveira, O. C. O. Dahlsten, and M. B. Plenio. Efficient Generation of Generic Entanglement. *Phys. Rev. Lett.*, 98(130502), 2007. arXiv:quant-ph/0605126.
- [27] V. I. Paulsen. *Completely bounded maps and dilations*. John Wiley & Sons, Inc., New York, NY, 1987.
- [28] P. Sen. Random measurement bases, quantum state distinction and applications to the hidden subgroup problem. *IEEE Conference on Computational Complexity 2006*, pages 274–287, 2005. arXiv:quant-ph/0512085.

- [29] J. Watrous. Notes on super-operator norms induced by Schatten norms. *Quantum Information and Computation*, 5(1):58–68, 2005. arXiv:quant-ph/0411077.
- [30] M. Znidaric. Optimal two-qubit gate for generation of random bipartite entanglement. *Phys. Rev. A*, 76(012318), 2007. arXiv:quant-ph/0702240.