Translationally Invariant Random Quantum Circuits

Rowechen Zhong

May 13, 2023

1 Abstract

Random quantum circuits have a wide range of applications, spanning from quantum computing and quantum many-body systems to the study of black holes in physics. In quantum information science, their usages abound [10]; they are ubiquitous in protocols for transferring information through quantum channels, quantum data-hiding, encryption, and information locking.

The gold standard for the generation of pseudorandom unitaries is the Haar measure, which is the natural "uniform" distribution over unitary matrices. The natural way to quantify how close a given distribution is to the Haar measure, is through the notion of "approximate k-designs;" a distribution is a k-design if it has k-th moments equal to those of the Haar distribution.

Significant progress has been made on this front in the past few years. In 2005, Emerson et al. [4] showed that random quantum circuits in fact converge to the Haar measure. In 2009, Harrow and Low [9] showed that random circuits of polynomial length are approximate 2-designs. In 2019, Brandão et al. [2] showed that in fact, *nearest-neighbor* two-qubit gates are sufficient to form approximate unitary t-designs. Specifically, they studied the circuit formed by interleaving 2-qubit unitaries in a "brickwork architecture." Their work represented a significant amalgamation of mathematical theory, incorporating quantum many-body theory, representation theory, and the theory of stochastic processes. Finally, in August 2022, Haferkamp [8] reduced the constant factors required by their construction significantly.

When Brandão et al. specialized to the brickwork architecture, they introduced a degree of *locality* into the problem. In particular, the local entanglement caused by geometrically adjacent two-qubit gates was shown to be sufficient to form global entanglement across the entire system. This specialization was physically and practically motivated. Quantum hardware is typically designed to allow robust operations between neighboring qubits. Studying such random circuits may also yield interesting insights into the nature of physical systems, as modeled using local interactions on a lattice.

In this paper, we will study variations of this question, which are also physically motivated. One direction is to consider the limiting distribution of a series of *symmetric* entangling operators on a circle of $N = 2n$ qubits. We will perform the *same* Haar-random unitary on pairs of adjacent qubits, in a brickwork architecture. It is a well-known paradigm that symmetries in a system yield conservation laws; in this case, one would expect that the symmetries yield nontrivial subspaces preserved by all operations; then the distribution is expected to converge to some (presumably Haar-random) distribution across each subspace.

We will refer to Fulton's textbook [7] and [5] as a reference for representation theory.

2 Background

Consider the unitary group $U(D)$ over a dimension-D Hilbert space. Suppose you wanted to design a uniform measure μ for the Borel algebra $\mathcal{B}(U(D))$. Such a measure ought to be invariant under actions by elements of $U(D)$;

$$\mu(gS) = \mu(S), \qquad \forall g \in U(D), S \in \mathcal{B}(U(D))$$

It turns out that such a distribution is essentially *unique*, after imposing some sanity conditions: inner and outer regularity and finiteness on compact sets. The resulting measure is called the *Haar measure* on $U(D)$.

The subject of this paper is the following random circuit:

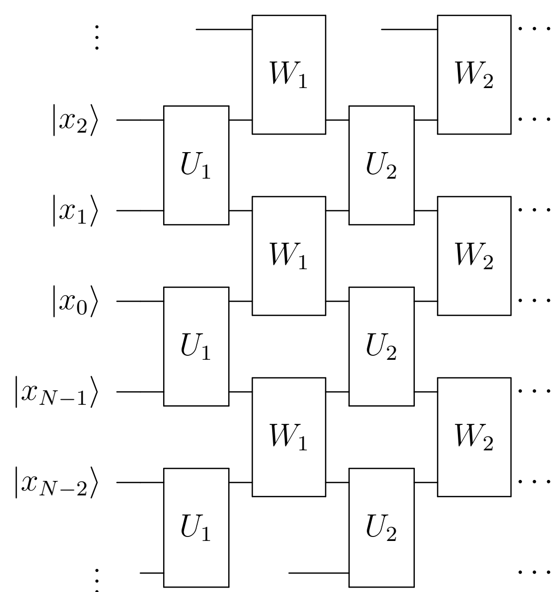

Figure 1: Translation-Invariant Brickwork Architecture

We conceptualize there being $N = 2n$ qubits total, with qubits enumerated modulo N, such that the network is entirely symmetric under rotation by 2 qubits. On layer k, two random two-qubit unitaries $U_k, W_k \in U(4)$ are sampled from the Haar measure. For notation, for any two-qubit unitary U, let $U(a,b) \in U(2^N)$ denote the action of U on qubits a and b. We then apply $U(2m, 2m+1)$ for all m, followed by $W(2m+1, 2m+2)$ for all m. Let $M_k \in U(2^N)$ denote the entire unitary enacted by layer k, and let $T_k \in U(2^N)$ denote the entire unitary consisting of the product of all operators up to layer k.

Each U_k, W_k is a random variable, and thus so is T_k. The goal of this paper is to analyze the limiting distribution of T_k as $k \to \infty$.

We define the *rotation operator* $\mathcal{R}$ by its action on pure tensors;

$$\mathcal{R}\,|a_1 a_2 \cdots a_N\rangle = |a_3 a_4 \cdots a_N a_1 a_2\rangle$$

and extend by linearity. Define the *rotation superoperator* $\mathfrak{R}$ as

$$\mathfrak{R}(U) = \prod_{i=1}^{n} \mathcal{R}^i U \mathcal{R}^{-i}$$

Thus,

$$M_k = \mathfrak{R}(U_k(0,1))\mathfrak{R}(W_k(1,2))$$

The motivation behind our main theorem is the following series of observations:

Lemma 1 *$\mathcal{R}$ commutes with $\mathfrak{R}(U)$ for all $U \in U(2^N)$.*

Proof.

$$\mathcal{R}\mathfrak{R}(U) = \mathcal{R}\prod_{i=1}^{n} \mathcal{R}^i U \mathcal{R}^{-i} = \prod_{i=1}^{n} \mathcal{R}^{i+1} U \mathcal{R}^{-i} = \mathfrak{R}(U)\mathcal{R}$$

□

We will forever let $\omega_n = e^{2\pi i/n}$.

$\mathcal{R}^n = 1$, thus $\mathcal{R}$ has eigenvalues ω_n^k for $k = 0, 1, \ldots, n-1$. Let $V_k \subset \mathbb{C}^{2^N}$ be the ω_n^k-eigenspace of $\mathcal{R}$, for $k = 0, 1, \ldots, n-1$. Then, by the previous lemma, each eigenspace is left invariant by all $\mathfrak{R}(U)$; in particular, each eigenspace is left invariant by T_k for all k. Thus, the limiting distribution consists of unitary matrices that are *block-diagonal* in any basis respecting V_k.

Lemma 2 *We can write down a complete set of orthonormal projectors onto each V_k;*

$$P_k = \frac{1}{n}\sum_{i=0}^{n-1} \omega^{-ik}\mathcal{R}^i$$

Proof. This is essentially clear;

$$\begin{aligned}P_kP_\ell &= \frac{1}{n^2}\sum_{0\le i,j<n}\omega^{-ik}\omega^{-j\ell}\mathcal{R}^{i+j} = \frac{1}{n^2}\sum_{0\le i,j<n}\omega^{-i(k-\ell)}\omega^{-(i+j)\ell}\mathcal{R}^{i+j}\\ &= \frac{1}{n^2}\sum_{0\le i,j<n}\omega^{-i(k-\ell)}\omega^{-j\ell}\mathcal{R}^{j} = \delta_{k\ell}P_\ell\end{aligned}$$

and

$$\sum_{k=0}^{n-1}P_k = \frac{1}{n}\sum_{k=0}^{n-1}\sum_{i=0}^{n-1}\omega^{-ik}\mathcal{R}^i = \mathcal{R}^0 = I$$

P_k leaves ω-eigenspace V_k invariant, since for any $v\in V_k$,

$$P_kv = \frac{1}{n}\sum_{i=0}^{n-1}\omega^{-ik}\mathcal{R}^iv = \frac{1}{n}\sum_{i=0}^{n-1}\omega^{-ik}\omega^{ik}v = v$$

(similarly they kill V_ℓ for $\ell\neq k$). They are clearly Hermitian. □

Clearly, P_k commutes with all $\mathfrak{R}(U)$; they can be pulled to the front of all expressions. All we're trying to do is single out an eigenspace.

Let $\mathcal{M}^{(k)}$ be all elements of the form MP^k, where $M = \mathfrak{R}(U(0,1))\mathfrak{R}(W(1,2))$ as usual.

By abuse of notation, we will sometimes consider P_k as a map $V\to V_k$ by inclusion; the risk of confusion is minimal.

Thus, we have our blocks: for each $0\le k<n$, let $M_t^{(k)} = M_tP^k$ and $T_t^{(k)} = T_tP^k$ be operators over $U(V_k)$ (unitary operators which are nonzero only in the V_k block). By block-diagonality, it is clear that

$$T_t = T_t^{(0)}\oplus\cdots\oplus T_t^{(n-1)},\qquad T_t^{(k)} = M_1^{(k)}M_2^{(k)}\cdots M_t^{(k)}$$

This motivates:

Theorem 1 (Main Theorem) *For each $0\le k<n$, as $t\to\infty$, $T_t^{(k)}$ converges uniformly to the Haar distribution over $U(V_k)$.*

While we do not prove this theorem, it will be reduced to a combinatorial problem, which is amenable to algorithmic simulation.

3 Measure Theory

Let $\mathcal{F}$ denote the set of probability measures over $U(V_k)$. $M_t^{(k)}$ is drawn at random from some complicated measure which we will call $f\in\mathcal{F}$.

Then, the distribution of $T_t^{(k)}$ is naturally described via convolution;

$$P(T_t^{(k)} = g) = \underbrace{f * f * \cdots f}_{k \text{ times}} = \int d\mu(h_{t-1}) \cdots d\mu(h_1) f(g h_{t-1}^{-1}) \cdots f(h_2 h_1^{-1}) f(h_1)$$

where $d\mu(g)$ is the Haar measure over $U(D)$.

The following intuitive theorem is due to Emerson et al.[4], and saves us from tangling too much with measure theory.

Theorem 2 (Generation implies convergence) *Suppose f is a probability measure over the compact Lie group $U(D)$. If f has support on a subset of $U(D)$ that generates $U(D)$, then f^{*m} converges uniformly to the Haar measure on $U(D)$.*

The theorem is natural, because if f^{*m} converges, then it clearly must converge to the Haar measure; the trick is to show that it converges at all.

In any case, we have our first reduction:

Reduction 1 (Generation) *The main theorem follows if f has support on a subset of $U(V_k)$ that generates $U(V_k)$.*

In particular, call the subgroup generated by $\mathcal{M}^{(k)}$ $\mathcal{S} \subset U(V_k)$; the claim is that $\mathcal{S} = U(V_k)$.

4 Lie Algebra

The space of unitary matrices is pretty complicated. The associated *Lie algebra*, which consists of *infinitesimal* unitaries, is much easier to handle.

$U(D)$ is a compact and simply connected Lie group; as such, there is a well-known correspondence via the exponential map $\exp : \mathfrak{u}(D) \to U(D)$ is $U(D)$ that maps $\mathfrak{u}(D)$ surjectively over $U(D)$. Keep in mind that all lie algebras described are *real*. Thus, it would suffice to show that infinitesimal elements of $\mathcal{M}^{(k)}$ generate the lie algebra of $U(V_k)$.

We will now be making extensive use of the (generalized) Pauli matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

which are also called $\sigma^0, \sigma^1, \sigma^2, \sigma^3$ respectively; and $\sigma^s = \sigma^{s_0} \cdots \sigma^{s_{n-1}}$ for $s \in \{0,1,2,3\}^n$.

Well, we can easily write down the infinitesimal generators of $\mathcal{M}^{(k)}$, which we identity with the lie algebra $\mathfrak{M}^{(k)}$: when $U = I + iA$, $T = I + iB$ with A, B infinitesimal hermitian 2×2 matrices,

$$\begin{aligned} M &= \prod_{i=1}^{n} \mathcal{R}^i U(0,1) \mathcal{R}^{-i} \prod_{j=1}^{n} \mathcal{R}^j T(1,2) \mathcal{R}^{-j} P_k \\ &= P_k + P_k^\dagger \sum_{i=1}^{n} \mathcal{R}^i \left(iA(0,1) + iB(1,2) \right) \mathcal{R}^{-i} P_k \\ &= P_k + P_k^\dagger \left(iA(0,1) + iB(1,2) \right) P_k \end{aligned} \tag{$\star$}$$

Clearly, A, B can be taken to be 2-qubit Pauli strings.

More infinitesimal elements of M can be generated through linear operations and the lie bracket (the commutator). Let $\mathcal{H}(D)$ denote the $D \times D$ hermitian matrices. Observe that for any $A, B \in \mathcal{H}(2^N)$,

$$[P_k^\dagger iAP_k, P_k^\dagger iBP_k] = P_k^\dagger 2i \underbrace{\frac{1}{2i} \left(\sum_j A\mathcal{R}^j B \mathcal{R}^{-j} - \mathcal{R}^j B \mathcal{R}^{-j} A \right)}_{A \tilde{*} B} P_k$$

This motivates the definition of the *convolution commutator*:

$$A \tilde{*} B = \frac{1}{2i} \left(\sum_j A\mathcal{R}^j B \mathcal{R}^{-j} - \mathcal{R}^j B \mathcal{R}^{-j} A \right)$$

It will soon be clear why this is an appropriate name.

$\mathfrak{u}(2^N)$ consists of the $2^N \times 2^N$ antihermitian matrices, which can be identified with linear combinations of Pauli strings of length N. To distinguish the basis elements (individual Pauli strings) from linear combinations of Pauli strings, I will use the adjective "pure." An arbitrary example is

$$iX \otimes Y \otimes Z \in \mathfrak{u}(2^3)$$

Thus, the infinitesimal elements of $U(V_k)$ are simply

$$iP_k \sigma^s P_k$$

All we need to do is show that we can create all elements of the above form using linear combinations and commutators of $\star$. Dropping the wrapping P_k's and the i prefactor, we produce our next reduction.

Reduction 2 (Lie Generation) *The following implies the main theorem.*

Suppose there exists a (real) linear subspace $S \subset \mathcal{H}(2^N)$ such that:

1. *For any hermitian $A \in U(4)$, $A(0,1), A(1,2) \in S$.*
2. *For any $X, Y \in S$, $X \tilde{*} Y \in S$.*
3. *For any $X \in S$, $\mathcal{R} X \mathcal{R}^{-1} \in S$.*

Then, $S = \mathcal{H}(2^N)$.

5 Combinatorics

Item (3) of the previous reduction means we only care about the generated operators up to equivalence classes under rotation. Thus, we present the following notation, which is best explained with examples in the $n = 3$ case:

$$\begin{aligned} Xx &\equiv \{XXIIII, IIXXIIX, IIIIXX\} \\ Xy &\equiv \{XYIIII, IIXYII, IIIXYI\} \\ xX &\equiv \{IXXIII, IIIXXI, XIIIIX\} \\ XiZ &\equiv \{XIZIII, IIXIZI, ZIIIXI\} \\ XiXiXi &\equiv \{XIXIXI\} \end{aligned}$$

Explicitly: we only care about elements up to rotation by 2 qubits; capital letters denote even indices and lowercase letters denote odd indices; leading and trailing I's are omitted.

Here is what a generic convolution commutator looks like:

$$Xx\tilde{*}yZ = \frac{1}{2i}[XXIIII, IYZIII+IIIYZI+ZIIIIY] = XZZIII+0-YXIIIY = XzZ-yYx$$

It is now apparent that the $\frac{1}{2i}$ factor was chosen to kill the irrelevant global phase factors that will always occur in such a commutation.

For hand-calculation of these convolution commutators, several things quickly become apparent:

- The background I's commute with everything; thus they can safely be ignored.
- In order for two Pauli strings to *fail* to commute, they must differ in an odd number of entries.
- Global phase factors of ± 1 can be dropped, but one must remain vigilant for local phase flips.

And the following lemma:

Lemma 3 (Symmetric Constructions) *X, Y, Z are essentially symmetric. In addition, there is symmetry about reversing all strings, and translating by 1 unit. Thus, after finding $XxY \in S$, we immediately know $YyX, YyZ, xZz, \cdots \in S$.*

In order to prove a statement like 2, one would have to design an algorithm that, given a Pauli string, generates a sequence of convolution commutations evaluating to the Pauli string.

While I was unable to design such an algorithm, we offer some constructions that may eventually lead to such an algorithm.

One insight is that there are two possible ways this algorithm could conceivably work: a *local* method, and a *global* method. A local method only ever requires strings that are of bounded length in order to create a pauli string of fixed length; in other words, to create the string XyZ

when $N = 10^{10}$, one would not have to create strings of length $O(N)$ as intermediate steps. In contrast, a global method is significantly more complex, making use of the finiteness of N, such that convolutions must wrap around the circle of qubits to construct desired Pauli strings.

Figure 2: A "local" method (left) would only interact with a bounded number of qubits (red) in order to construct a desired Pauli string (blue). A "global" method (right) would have to wrap around the circle of qubits to construct a desired Pauli string.

Unfortunately, through numerical simulations as described later, I have been unable to construct the simple string XyZ locally. Thus, we present a global construction that may facilitate the construction of a global algorithm.

Theorem 3 (Chains) *It is possible to form arbitrarily long chains of the form $XzZ \cdots ZzX$ and $XzZ \cdots zZy$ (whose length is bounded by N). In particular, one can create a chain $Zz \cdots Z$ of length $N - 1$.*

Proof. Begin with $Xx\tilde{*}yX = XzX$. Then, $XzX\tilde{*}Yy = XzZy$. Continuing, $XzZy\tilde{*}yY = yZzZy$; this is symmetric to $XzZzX$. Apply Yy again, ad nauseam, to yield strings $XzZ \cdots ZzX$ and $XzZ \cdots zZy$.

We eventually reach $XzZ \cdots ZzX$ of length $N - 1$:

$$\cdots ZzZz\underbrace{XiXz}ZzZ\cdots$$

Applying Yy as usual, we find

$$\cdots ZzZz\underbrace{ZyXz}ZzZ\cdots$$

Applying yY one last time, we achieve

$$\cdots ZzZz\underbrace{ZiZz}ZzZ\cdots$$

as desired. $\square$

Previously, all strings were padded by I's on both sides; this construction shows that we can change the "background" we choose to work in to be Z's instead of I's.

This substrate is significantly more reactive than I's; attempting to use this construction combined with local constructions tends to cause large amounts of anticommutations to occur at once, rendering hand calculations difficult.

6 Computer Analysis

6.1 Methods

For any finite n, the approach is straightforward; there are a finite number of pauli strings to generate, so we just enumerate all pauli strings through brute force. Specifically, the dimension of our space is simply 4^N, and pauli strings can be naively encoded as vectors in $\mathbb{R}^{4^N}$. I call this method of encoding the algebra the *vector method*.

Of course, this takes exponential time. Thus I implemented the following optimizations:

- Only consider equivalence classes of pauli strings under shifts by 2 qubits. Automatically include the symmetric constructions under the lemma.
- While general elements of our algebra are linear combinations of pauli strings, significant progress can be made by restricting ourselves to pure pauli strings. This is done for as long as possible; then operations like checking for linear independence become trivial (using a hash table). I call this method of encoding the algebra as the *dictionary method*.
- Originally, I attempted to check linear independence through singular-value decomposition. This proved to be too slow, so I switched to using the QR decomposition.

In addition, while attempting to discover a local algorithm, I worked in the context of "unbounded" pauli strings; we imagine $N \to \infty$ such that we never have to consider convolutions that wrap around.

6.2 Results

If we count by groups of two qubits, there are three possible types of 6-qubit pauli strings:

- AAA, of which there are 16.
- AAB, of which there are $16 \cdot 15 = 240$.
- ABC, of which there are $16 \cdot 15 \cdot 14/3 = 1120$.

In total, there are 1376 distinct pauli strings up to cyclic rotations.

Unfortunately, both the vector and dictionary methods were unable to enumerate all 1376 distinct pauli strings in 6-qubit case; only 1374 were found. The 8-qubit case appears to be too large to feasibly simulate on computational resources I have access to, even with all the accelerations above.

All code can be found on github at github.com/rowechenzhong/QIS-Project.

In addition, in the unbounded case was able to produce a large list of pauli strings, which can be used for any N due to their local nature. Some small examples of pure states we can generate include:

$$XxX, XyX, XyZz, XxYy, XyYz, XyZx, XxYxX, \cdots$$

Note that we are missing local constructions for two simple 3-qubit interactions, XyZ and XxY. Indeed, although we can form many linear combinations of 3-qubit interactions such as $XyY - zZx = zY\tilde{*}Xx$, these do not span the space of 3-qubit interactions. In retrospect, this is expected.

7 Conclusion

The most immediate extension of this work would be to discover a general construction for all pauli strings. After this, one could begin work on the convergence properties of our quantum circuit; in particular, we might ask whether it converges to an t-design at the same rate as previous work [2][8].

In addition, by restricting ourselves to work in subspaces of the full space of operators, we ignored possible correlations that would occur *between* the subspaces – it is clearly not true in general that a joint distribution is completely determined by its marginals. Thus, while I do not expect there to be a "clean" answer in this case, additional studies on the mixing between the V_k subspaces would be interesting.

Finally, observe that the graph structure of our qubits is a *directed* $2n$-cycle, with symmetry group C_n. At the beginning of this project, I worked extensively on the case of the *undirected* n-cycle, which may naively seem easier.

Here, the vertical lines are controlled-Z gates, our sole (symmetric) entangling operation. Unfortunately, I soon came to realize that the symmetry group of this circuit is not C_n, but rather the dihedral group D_n; the circuit is invariant under $x_i \to x_{n+1-i}$. Importantly, D_n is *not* abelian. This seemingly innocuous detail destroys our theorem. Our existing V_k subspaces are still invariant (where V_k are eigenspaces under rotation by 1 qubit). However, one can define two additional subspaces W_+ and W_-, which are the eigenspaces under *reflection* about the axis passing through qubit $|x_0\rangle$. These subspaces do not intersect nicely with the V_k subspaces; it is a general fact of linear algebra that in a dimension N vector space, two subspaces of size a, b need not intersect at all if $a + b \leq N$.

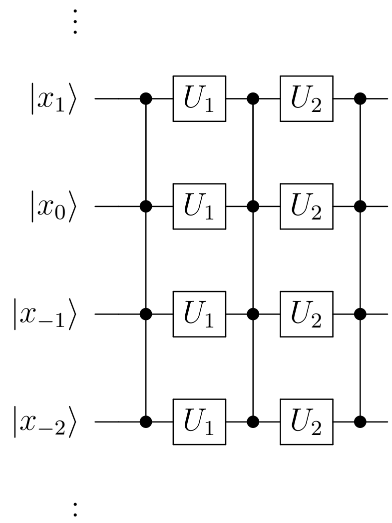

Figure 3: Cyclically Symmetric Circuit

Thus, the D_n case is significantly more complicated than the C_n case. The analogous statement of our main theorem is *wrong* for $n = 3$ where $D_6 = S_3$ is nonabelian. In the language of graph theory, the *automorphism group* of the undirected n-cycle is nonabelian.

However, this yields a natural question: does our above analysis extend to arbitrary graphs with abelian automorphism groups? There are many such graphs of interest.

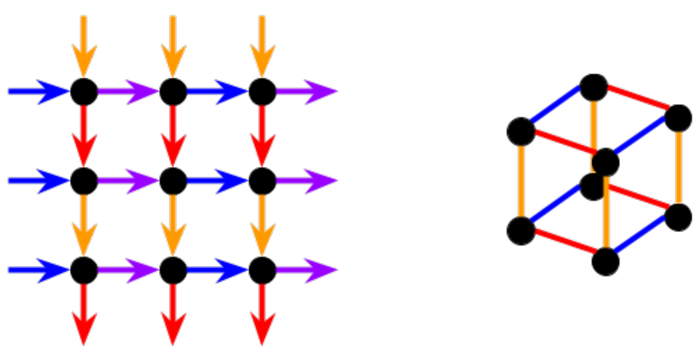

Figure 4: The graph on the left is a section of a colored, directed graph. The graph is understood to eventually wrap around on the left and right, as well as top and bottom, such that it forms a torus. If there are $2m \times 2n$ qubits (vertices) in the graph, then the automorphism group is $C_m \oplus C_n$, an abelian group. The undirected graph on the right is a hypercube of dimension $D = 3$. The automorphism group is $C_2^{\oplus D}$, also an abelian group.

Conjecture 1 (Informal) *Given some (possibly directed, or colored) graph G with abelian automorphism group, one can construct a quantum circuit whose qubits are identified with the vertices and whose gates are identified with the edges.*

The gates are arranged into layers. On each layer, to each color of edge, we apply the same *randomly chosen unitary operation. This is possible to do simultaneously so long as no two edges of the same color share a vertex.*

As this procedure is taken to the limit, the entire unitary enacted on this circuit approaches some limiting distribution.

It is easy to see that such a limiting distribution must block-diagonalize into the subrepresentations of the automorphism group. Does it converge to a Haar distribution on each block?

The well-known *structure theorem for finite abelian groups* states that any finite abelian group G is isomorphic to a direct product of cyclic groups, which was precisely the case studied in this paper. Perhaps future work may reveal the relationship between these two cases.

8 Acknowledgements

I would like to thank Professor Soonwon Choi for his phenomenal Quantum Information Science course, and for suggesting this topic to me. I learned lots of quantum computing from Michael Nielson and Isaac Chuang's *Quantum Computation and Quantum Information* textbook, which is a good resource.

References

[1] Dave Bacon, Isaac L. Chuang, and Aram W. Harrow. The quantum schur transform: I. efficient qudit circuits, 2005.

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

[3] Benoît Collins and Piotr Śniady. Integration with respect to the haar measure on unitary, orthogonal and symplectic group. *Communications in Mathematical Physics*, 264(3):773–795, mar 2006.

[4] Joseph Emerson, Etera Livine, and Seth Lloyd. Convergence conditions for random quantum circuits. *Physical Review A*, 72(6), dec 2005.

[5] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina. Introduction to representation theory, 2009. cite arxiv:0901.0827 Comment: 108 pages. In the latest version, misprints and errors were corrected and new exercises were added, in particular ones suggested by Darij Grinberg.

[6] Matthew P.A. Fisher, Vedika Khemani, Adam Nahum, and Sagar Vijay. Random quantum circuits. *Annual Review of Condensed Matter Physics*, 14(1):335–379, mar 2023.

[7] William Fulton and Joe Harris. *Representation theory: A first course*. Springer, 2004.

[8] Jonas Haferkamp. Random quantum circuits are approximate unitary t-designs in depth $o(nt^{5+o(1)})$. *Quantum*, 6:795, sep 2022.

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

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