

Efficient unitary designs and pseudorandom unitaries from permutations

Chi-Fang Chen,¹ Adam Bouland,² Fernando G.S.L. Brandão,^{1,3}

Jordan Docter,² Patrick Hayden,^{4,5} and Michelle Xu^{4,5}

¹*Institute for Quantum Information and Matter,
California Institute of Technology, Pasadena, CA, USA*

²*Department of Computer Science, Stanford University*

³*AWS Center for Quantum Computing, Pasadena, CA*

⁴*Stanford Institute for Theoretical Physics*

⁵*Department of Physics, Stanford University*

In this work we give an efficient construction of unitary k -designs using $\tilde{O}(k \cdot \text{poly}(n))$ quantum gates, as well as an efficient construction of a parallel-secure pseudorandom unitary (PRU). Both results are obtained by giving an efficient quantum algorithm that lifts random permutations over $\mathcal{S}(N)$ to random unitaries over $\mathcal{U}(N)$ for $N = 2^n$. In particular, we show that products of exponentiated sums of $\mathcal{S}(N)$ permutations with random phases approximately match the first $2^{\Omega(n)}$ moments of the Haar measure. By substituting either $\tilde{O}(k)$ -wise independent permutations, or quantum-secure pseudorandom permutations (PRPs) in place of the random permutations, we obtain the above results. The heart of our proof is a conceptual connection between the large dimension (large- N) expansion in random matrix theory and the polynomial method, which allows us to prove query lower bounds at finite- N by interpolating from the much simpler large- N limit. The key technical step is to exhibit an orthonormal basis for irreducible representations of the partition algebra that has a low-degree large- N expansion. This allows us to show that the distinguishing probability is a low-degree rational polynomial of the dimension N .

CONTENTS

I. Introduction	1
A. Main results	3
B. Proof idea	6
1. A single exponential as a sum of words	8
2. Large- N limit	9
3. Central limit theorem	10
4. Verifying the requirements for interpolation	10
C. Road map	12
D. Acknowledgments	12
II. Notation	12
A. Random matrix ensembles	14
B. Pseudorandomness and k -designs	15

III. Preliminaries	15
A. Markov’s “other” inequality for polynomials	15
B. Basic algebraic notions	17
C. Representations of the symmetric group	19
1. Integer partitions	19
2. Young diagrams and Young tableaux	20
3. Irreducible modules	20
4. The computational basis	21
D. The partition algebra	22
1. Set-partitions	23
2. Explicit presentation	24
3. Algebraic structure	27
IV. New lemmas	28
A. Asymptotic freeness of random permutations	28
B. Large N structure	34
C. Basis for the partition algebra	35
1. An abstract construction of irreps	36
2. Explicit basis	37
3. Orthogonality and matrix elements	41
4. Projector onto irreducible representations as a sum over diagrams	43
D. Extending test operators	44
V. Proof of main result	48
A. Expanding one exponential into words	49
B. Proof of Theorem I.3	50
1. The large- N limit	51
2. Interpolating to finite N	51
C. Truncation error for exponentials	54
A. Lindeberg arguments	55
B. Comparing the Gaussian CP map with a unitary channel	57
C. Unitary k -designs from k' -wise permutations	59
1. Bootstrapping nonadaptive designs to adaptive designs	62
References	63

I. INTRODUCTION

Pseudorandom states and unitaries are fundamental tools in quantum information. By efficiently creating ensembles of states/unitaries that mimic the Haar measure, we can access Haar random properties without paying a cost exponential in the number of qubits. Broadly speaking, two types of quantum pseudorandomness have been previously considered. The first is *information-theoretic* pseudorandomness, where the goal is to generate unitary or state k -designs, i.e., ensembles that match the first k moments of the Haar measure. These are the natural quantum analogs of k -wise independent functions or permutations. This yields information-theoretic k -copy security, and suffices for many applications, such as randomized benchmarking [EAŽ05, KLR⁺08, DCEL09], cryptography [DLT02, ABW09], shadow tomography [HKP20], communication [HHWY08, SDTR13], and phase retrieval [KL17]. The second is *computational* pseudorandomness, where the goal is to create pseudorandom states and unitaries (PRs and PRUs) that are computationally indistinguishable from Haar [JLS18]. These are the quantum analogs of pseudorandom functions (PRFs) or permutations (PRPs), and have found significant applications both in quantum cryptography (e.g., [Kre21, KQST23]) and in the complexity of physical systems, e.g., [BFV19, KTP20, ABF⁺24, YE23]. This relaxed security notion allows one to obtain properties impossible in information-theoretic settings, such as small ensemble (key) sizes, many copy security, and low entanglement [JLS18, ABF⁺24].

Many questions remain open in both branches of the quantum pseudorandomness family tree. On the k -design side, a significant open problem has been to efficiently generate unitary k -designs on n qubits. It is known that this task requires at least $\Omega(nk)$ quantum gates [BHH16] but so far existing constructions have not achieved the bound, despite much work in the area [Web15, ZKGG16, Zhu17, MY23, HL09b, HL09a, BHH16, HM23, Haf22, HJ19, DCEL09, CLLW16, OBK⁺17, NHKW17, BNZZ19, NZO⁺21, BNOZ22, OSP23, KKS⁺23, HLT24, CDX⁺24]. The first efficient and systematic constructions of approximate unitary k -designs which work for large values of k were given by [BHH16], who showed that random local circuits achieved the goal in $\mathcal{O}(k^{10.5}n^2)$ time. This was followed by an improvement to $\tilde{\mathcal{O}}(k^5n^2)$ by [Haf22] using an improved analysis. Very recently, this was improved to $\tilde{\mathcal{O}}(k^2n^2)$ quantum gates by two independent works with different constructions [HLT24, CDX⁺24], which is still quadratically off from the lower bound. This stands in contrast to related k -wise independent objects, as optimal constructions with linear scaling in k are known for quantum state designs (e.g., [BS19]) as well as for analogous classical objects, namely k -wise independent functions [Jof74, WC81, ABI86] or approximate k -wise independent permutations [Kas07, CK23]. We note that linear scaling¹ in k has previously been shown² only in restricted cases, such as the limit of large local dimension [HHJ21], or if the number of moments matched is small ($k \ll \mathcal{O}(\sqrt{n})$) [NHKW17]. This problem is not only a fundamental and natural question in

¹ We emphasize that this refers to the quantum gate count – which is typically the bottleneck in applications – rather than the scaling in the number of bits of classical randomness which was recently achieved by [OSP23].

² We note there have also been plausible arguments that certain continuous time Brownian motions should attain linear scaling [JBS23] but the cost of simulating them on a quantum computer remains to be analyzed.

theoretical computer science, but has also gathered the attention of the quantum gravity community, because the linear growth in circuit complexity associated with an efficient t -design ensemble (see e.g., [RY17]) is believed to play a role in resolving certain paradoxes in quantum gravity [BS18].

On the *computational* pseudorandomness side, a significant open problem is to construct pseudorandom unitaries (PRUs) from standard cryptographic assumptions, such as the existence of quantum-secure one-way functions (OWFs). While several efficient constructions of pseudorandom state ensembles are known [JLS18, BS19, ABF⁺24, GTB23, JMW23, Ma23], progress has been much more difficult in the unitary case. While several PRU candidates have been proposed [JLS18], none of them have proven security. However, a number of objects intermediate between a PRS and a PRU have been rigorously constructed. For example, Ananth et al. constructed pseudorandom function-like states, a generalization of a PRS that allows one to create polynomially many independent PRSs [AQY22, AGQY22]. Subsequently, Lu et al. constructed what they call pseudorandom state scramblers, which are ensembles of unitaries that produce a PRS from any *fixed* input state [LQS⁺23]. There has also been a recent construction of parallel-secure pseudorandom isometries between spaces of differing dimensions [AGKL23], as well as another variant of a pseudorandom state scrambler for real (orthogonal) states [BM24]. However, the existence of efficient pseudorandom unitaries with general query security remains open.

In this work, we make progress on both quantum pseudorandomness open problems simultaneously. First, we give a construction of a unitary k -design using quantum gates scaling near-linearly with k , which matches the lower bound on k -dependence up to logarithmic factors.

Theorem I.1 (Efficient quantum k -designs). *There exists an efficient quantum algorithm to generate an ϵ -approximate unitary k -design (in diamond norm) using $\tilde{O}(k \text{ poly}(n))$ one and two-qubit quantum gates. The $\tilde{O}(\cdot)$ absorbs polylogarithmic dependence on n, k, ϵ^{-1} .*

Second, we also give a construction of a pseudorandom unitary ensemble with nonadaptive security.

Theorem I.2 (Parallel PRU from quantum-secure OWF). *The existence of a one-way function secure against quantum attack implies an efficient quantum algorithm to generate parallel-secure pseudorandom unitaries.*

We recently became aware of independent work of Metger, Poremba, Sinha and Yuen [MPSY24] which obtain similar results for parallel-secure PRUs and k -designs, via a completely different construction and analysis.

To achieve the above results, we demonstrate that the following meta-result:

$$(Pseudo)random \text{ permutations can be efficiently lifted to } (pseudo)random \text{ unitaries.} \quad (1.1)$$

More formally, we show there is an efficient quantum algorithm which, given black-box access to random permutations (and their inverses) in $\mathcal{S}(N)$ for $N = 2^n$, creates an ensemble of n -qubit

unitaries that is close to the Haar measure in an appropriate sense. In particular, we show that the ensemble is an approximate unitary k -design for a large value of k , namely $k = 2^{\Omega(n)}$. Our main results are then obtained by substituting different forms of pseudorandomness for the black box permutations from $\mathcal{S}(N)$. To obtain our k -design result, we show that it suffices to substitute in approximate $\tilde{O}(k)$ -wise independent permutations [Kas07, CK23]. (See Theorem C.2.) Here, the key point is that high-precision k -wise independent permutations are known to be implementable in $\mathcal{O}(\text{poly}(n)k)$ -time, so this efficiency then directly lifts to our unitary construction. To obtain our parallel PRU, we substitute in quantum secure pseudorandom permutations (PRPs, inverse allowed), which can be derived from quantum-secure one-way functions [Zha16].

A. Main results

To describe our main construction, the basic building blocks are *random phased permutations*, random permutation with random *complex* signs:

$$\begin{aligned} \mathbf{Z} &:= \mathbf{D}_z \cdot \mathbf{S}, \quad \text{where} && \text{(random phased permutations)} \\ \mathbf{S} &\stackrel{\text{unif}}{\sim} \mathcal{S}(N) && \text{(uniformly random permutations on } N \text{ elements)} \\ \mathbf{D}_z : (\mathbf{D}_z)_{ij} &= \delta_{ij} z_i \quad \text{where} \quad z_i \stackrel{i.i.d.}{\sim} \mathcal{U}(1). && \text{(random diagonal complex phases)} \end{aligned}$$

While we will eventually pursue pseudorandomness, in most of our discussions, it will suffice to treat the $\mathbf{Z}$ as truly random. Eventually, they will be replaced as needed by suitable classical pseudorandom counterparts.

The central object we build from random phased permutations $\mathbf{Z}$ is the matrix exponential

$$e^{i\theta_m \mathbf{A}_m} \quad \text{for} \quad \theta_m = \mathcal{O}(1), \quad (1.2)$$

where these $2m$ -sparse Hermitian matrices $\mathbf{A}_m$ are made of i.i.d. copies of $\mathbf{Z}$ and their adjoints

$$\mathbf{A}_m := \frac{1}{\sqrt{2m}} \sum_{a=1}^m (\mathbf{Z}_a + \mathbf{Z}_a^\dagger) \quad \text{where} \quad \mathbf{Z}_a \stackrel{i.i.d.}{\sim} \mathbf{Z}, \quad (1.3)$$

which can be thought of as the adjacency matrix for a random graph weighted by random phases.

The main result of this work is that the product of a few independent copies of these exponentiated sparse random matrices $e^{i\theta_m \mathbf{A}_m}$, left and right multiplied by independent phased permutations $\mathbf{Z}_L$ and $\mathbf{Z}_R$, approximates a Haar random unitary for quantum computers making nonadaptive (i.e., parallel) queries. Formally, this nonadaptive query access model considers the quantum channel associated with the k -fold tensor product of random unitary $\mathbf{U}$

$$\mathcal{N}_{2k, \mathbf{U}}[\rho] := \mathbb{E}_{\mathbf{U}}[\mathbf{U}^{\otimes k} \rho \mathbf{U}^{\dagger \otimes k}] \quad \text{with the diamond norm} \quad \|\mathcal{N}_1 - \mathcal{N}_2\|_\diamond := \|(\mathcal{N}_1 - \mathcal{N}_2) \otimes \mathcal{I}\|_{1-1}, \quad (1.4)$$

to quantify the probability of distinguishing our construction from Haar using *arbitrary* entangled inputs and measurements. We say that an ensemble of unitaries is an ϵ -approximate k -design (see, e.g., [Low10]) if the induced channel is close to the k -fold Haar channel in the diamond norm. That is, no possible quantum experiment (with arbitrary computation and ancillas) can distinguish the ensemble from the Haar measure given parallel access to k copies of the unitary.

Definition I.1 (Approximate unitary k -designs). *An ensemble of unitaries $\mathbf{U}$ is an ϵ -approximate k -design if $\|\mathcal{N}_{2k,\mathbf{U}} - \mathcal{N}_{2k,\mathbf{U}_{Haar}}\|_{\diamond} \leq \epsilon$, where $\mathbf{U}_{Haar}$ is drawn from Haar random unitaries $\mathbf{U}(N)$.*

We can now state the main technical result: the product of exponentials of sums of random phased permutations is an ϵ -approximate k -design for large values of k and small values of ϵ .

Theorem I.3 (Unitary designs from product of sparse exponentials). *For each $m, \ell \in \mathbb{Z}^+$, let $\mathbf{V}$ be the N -dimensional random unitary formed by a product of the ℓ independent exponentials of the random matrices $\mathbf{A}_m^{(1)}, \mathbf{A}_m^{(2)}, \dots, \mathbf{A}_m^{(\ell)}$, left and right multiplied by random permutations $\mathbf{Z}_L, \mathbf{Z}_R$, i.e.*

$$\mathbf{V} := \mathbf{Z}_L \left(\prod_{j=1}^{\ell} e^{i\theta_m \mathbf{A}_m^{(j)}} \right) \mathbf{Z}_R, \quad (1.5)$$

for some m -dependent angle $\theta_m = \mathcal{O}(1)$. Then, $\mathbf{V}$ is an approximate k -design in diamond distance. More precisely, for $N = 2^n$,

$$\|\mathcal{N}_{2k,\mathbf{V}} - \mathcal{N}_{2k,\mathbf{U}_{Haar}}\|_{\diamond} \leq \mathcal{O}\left(\frac{k^8 \ell^8 (m^4 n^8 + n^8)}{N} + \frac{k^4}{m^{\ell}}\right). \quad (1.6)$$

The point is that the ensemble is an approximate k -design for a *superpolynomial* value of k , using only very few, specifically $\tilde{\mathcal{O}}(m\ell)$, random permutations from $\mathcal{S}(N)$. Since sampling uniformly random permutations requires exponentially many bits of randomness, we are not evading known lower bounds on the cardinality of a unitary design [BHH16, RY17]. Crucially, however, the number of iterations ℓ can be small. For example, setting $m = 2$ and $\ell = n$ yields an approximate k -design for very large value of $k = 2^{\Omega(n)}$, but even $m = 2$ and $\ell = \log^2(n)$ suffices for a superpolynomial design; on the contrary, spectral gap approaches (e.g., [BHH16]) to unitary designs often cost $\Omega(nk)$ rounds of products.

While truly random permutations are still costly to sample from, the key point is that by substituting *pseudorandom* permutations in their place, we establish the link between classical pseudorandom permutations and quantum pseudorandom unitaries, as seen from the following two corollaries, establishing the aforementioned Theorem I.1 and Theorem I.2. First, we consider substituting information-theoretically secure pseudorandom permutations (i.e., k -wise independent permutations) in place of the truly random permutations to obtain an efficient unitary k -design. This requires choosing suitable parameters m and ℓ (see Corollary C.1 for completeness).

Corollary I.1 (Unitary k -designs from k' -wise independence (informal)). *There is a constant c such that for $k \leq 2^{cn}$, an ϵ -approximate quantum unitary k -design can be efficiently implemented*

by applying our construction with k' -wise independent (discrete) phases and k' -wise independent permutations in place of the truly random phases/permutations, where

$$k' = \mathcal{O}(k \log(k/\epsilon)). \quad (1.7)$$

Here, we are making key use of the fact that our construction only relies on $k' = \tilde{\mathcal{O}}(k)$ -th moments of the permutations via efficient Hamiltonian simulation algorithms (e.g. [BCC⁺15, GSLW19]). Thus our result “lifts” the efficient construction of k' -wise independent permutations and functions to the construction of unitary k -designs. This is in a similar spirit to recent results of Brakerski and Shmueli that lift $2k$ -wise independent functions to approximate quantum state k -designs [BS19].

To achieve an efficient unitary design, we now need to leverage the fact that k' -wise independent permutations and functions can be implemented in only $\mathcal{O}(\text{poly}(n)k')$ time. However, one caveat is that the best known classical k' -wise independent permutations (Definition C.1) are only approximately k' -wise independent. Fortunately, explicit, high-accuracy classical k -wise independent permutations do exist, which are of sufficiently low error to not affect the construction. This gives us unitary k -designs that are nearly algorithmically and information-theoretically optimal (in terms of k dependence and in the diamond distance). See section C for further discussion.

Corollary I.2 (Efficient quantum k -designs with almost linear k -scaling). *There is a constant c such that for $k \leq 2^{cn}$, an ϵ -approximate unitary k -design can be implemented using*

$$\tilde{\mathcal{O}}(\text{poly}(n)k) \text{ one and two-qubit gates} \quad \text{and} \quad \mathcal{O}(nk) \text{ bits of classical randomness} \quad (1.8)$$

where the notation $\tilde{\mathcal{O}}$ absorbs factors polylogarithmic in n, k and $1/\epsilon$. Thus, the k -dependence in the gate complexity and the seed length are both (nearly) optimal.

Previously, the best known systematic construction of unitary k -designs for superpolynomially large k has gate complexity $\tilde{\mathcal{O}}(n^2 k^2)$ [HLT24, CDX⁺24].

Moving on to computational pseudorandomness, we substitute cryptographically secure pseudorandom permutations (i.e., PRPs) in place of the truly random permutations to obtain a parallel-secure PRU:

Corollary I.3 (Quantum secure-PRP implies parallel-PRU). *Suppose quantum-secure pseudorandom permutations exist. Then our construction $\mathbf{V}$ gives a pseudorandom unitary under nonadaptive queries.*

Proof. Implement our unitary $\mathbf{V}$ using any efficient quantum algorithm given query access to polynomially many $\mathbf{Z}_i$ to super-polynomial precision. We obtain computational pseudorandomness from information-theoretic pseudorandomness by replacing the random phased permutations with the pseudorandom alternatives and applying a simple hybrid argument. Note that the controlled permutations can be efficiently implemented given function queries of permutations (and their inverses). ■

Note that the existence of quantum-secure PRPs (with inverses) only requires assuming the existence of quantum-secure pseudorandom functions [Zha16], which is a standard cryptographic assumption. Furthermore, if there exists a low-depth implementation of quantum-secure PRPs, then our PRU can also be low-depth with suitable parameters m, ℓ and standard quantum algorithmic implementations.

B. Proof idea

In a nutshell, multiplying sparse matrices is an efficient way to get a dense matrix, but controlling the diamond distance from Haar requires careful analysis. Prior approaches to unitary k -designs have often been based on the spectral gaps of random walks (e.g., [BHH16]), which bootstrap the statistical distance from a comparatively more tractable spectral gap. However, this approach necessarily requires a log-dimensional factor $\mathcal{O}(\log(N^k)) = \mathcal{O}(nk)$ multiplicative blowup in the gate complexity due to the conversion from 2-norm to 1-norm. For cryptographic applications, the attacker may perform an arbitrary polynomial number of queries, so security requires a *fixed* poly-time construction of a superpolynomial k -design, posing a fundamental barrier for spectral gap approaches.

The essence of our alternative argument can be captured in the following observation:

$$\mathbf{G} \stackrel{(1)}{\approx} \frac{1}{\sqrt{m^\ell}} \sum_{i=1}^{m^\ell} \mathbf{Z}_i \stackrel{(2)}{\approx} \left(\frac{1}{\sqrt{m}} \sum_{i=1}^m \mathbf{Z}_i^{(\ell)} \right) \cdots \left(\frac{1}{\sqrt{m}} \sum_{i=1}^m \mathbf{Z}_i^{(1)} \right), \quad (1.9)$$

where the $\mathbf{Z}_i$ are i.i.d. copies of a random phased permutation. The first approximation (1) is nothing more than a central limit theorem (CLT) established using a matrix Lindeberg argument similar to those in [CDB⁺23, CDX⁺24], but it allows us to obtain a very nice random matrix: $\mathbf{G}$ is drawn from the Ginibre ensemble [Gin65], which is a complex Gaussian matrix that is both left and right unitarily invariant. However, the CLT-type convergence rate is too slow (polynomial in the number of summands) and will incur a large $\Omega(\text{poly}(k))$ -cost scaling with the number of queries k .

The crux of our argument for circumventing the large number of i.i.d. copies is the second approximation (2): a product of sums reproduces the statistics of an *independent* sum but using many fewer ($\tilde{\mathcal{O}}(m\ell)$) copies of $\mathbf{Z}_i$, as stated in following loosely stated principle:

In the large- N limit, distinct words of permutations are effectively independent of each other.

As an instructive example, when the dimension N is large, the following correlated words of $\mathbf{Z}_1, \mathbf{Z}_2$ acting on $|i\rangle$ are almost independent of each other:

$$(\mathbf{Z}_1 |i\rangle, \mathbf{Z}_2 |i\rangle, \mathbf{Z}_1 \mathbf{Z}_2 |i\rangle, \mathbf{Z}_2 \mathbf{Z}_1 |i\rangle) \stackrel{dist}{\approx} (\mathbf{Z}_1 |i\rangle, \mathbf{Z}_2 |i\rangle, \mathbf{Z}_3 |i\rangle, \mathbf{Z}_4 |i\rangle). \quad (1.10)$$

Indeed, knowing $\mathbf{Z}_1 |i\rangle$ and $\mathbf{Z}_2 |i\rangle$ tells us nothing about $\mathbf{Z}_2 \mathbf{Z}_1 |i\rangle$, unless the very unlikely collision $\mathbf{Z}_2 |i\rangle \propto |i\rangle$ occurs. Applying this intuition to the product of sums, we can get m^ℓ independent $\mathbf{Z}$ s from merely $\tilde{\mathcal{O}}(m\ell)$ many truly independent $\mathbf{Z}$ s!

At first glance, the above analysis may appear strange, as if we get “more randomness for free” from a much smaller ($m\ell$) number of independent elements. Careful thought reveals the approximation in Eq. (1.9) is possible because we only consider *low-moment* properties of the permutations, i.e., we are fixing $k \ll N$ and then taking a large- N limit. In the $N \rightarrow \infty$ limit, the large amount of randomness in the permutations themselves effectively “decouples” the different terms, as collisions become vanishingly improbable. Strictly speaking, this precise statement only holds in a *non-adaptive* setting, i.e., when the inputs are fixed in advance. Of course, sequential/adaptive queries would reveal correlations between these words – for example, if one were able to query $\mathbf{Z}_2$ *after* knowing the result of $\mathbf{Z}_1 |i\rangle$, it would coincide with $\mathbf{Z}_2 \mathbf{Z}_1 |i\rangle$. However, the key point is that under non-adaptive queries³, such attacks are not possible, and the words effectively decouple.

Unfortunately, proving the validity of the argument above in finite dimensions N is nontrivial. There are nonasymptotic correlations, however tiny, between the distinct words because those words are made of only $\tilde{O}(m\ell)$ -many independent random phased permutations. To complete the proof, the remaining and most substantial technical argument is a framework to control those finite- N corrections effectively.

In principle, since permutations are reasonably nice objects, we could brute force through the combinatorics using diagrammatic calculations. With more work, it is possible to go beyond the limit and perform a *large- N expansion*: for “nice” random matrices ensembles, the Weingarten calculus and its variants frequently yield sums over diagrams with coefficients being rational functions of N . To prove our results, however, it is necessary to control the total contribution coming from all orders in the $1/N$ expansion. Moreover, it is very challenging to systematically capture the fine-grained combinatorics and *cancellations* required to deliver strong enough nonasymptotic bounds.

Our main strategy is the following large- N -interpolation principle that guides the path forward:

“Nice” random matrix properties at finite N are controlled by the large- N limit.

Conceptually, we are looking for an *interpolation* argument: instead of directly calculating a complicated random matrix quantity at finite N , we start with the much simpler large- N limit, and control the finite- N corrections by arguing that the function “changes slowly” as a function of $\frac{1}{N}$.

The crucial mathematical tool is a basic fact in polynomial approximation (see [section III A](#)): Markov’s “other” inequality states that a real-valued, *low-degree* polynomial $f(x)$ whose values are *bounded* on an interval will have bounded derivatives. This seemingly innocent property of polynomials has found profound implications in establishing lower bounds in classical circuit [Bei93] and quantum query complexity, a strategy referred to as the *polynomial method*, e.g., [BBC⁺01, AS04, BSS01, NW99, Kut05, Raz03]. By identifying an often nonobvious interpolation parameter x such that $f(x_1)$ and $f(x_2)$ correspond to the acceptance probabilities of the quantum algorithm

³ We conjecture our ensemble also gives adaptive security, but we note this would require further proof ideas, such as defining a more refined notion of independence of different words.

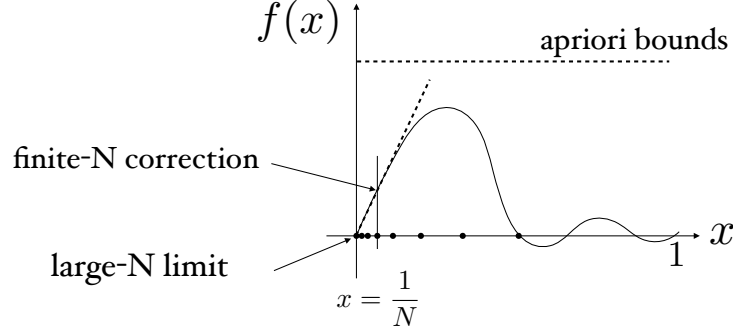


Figure 1: Interpolating the $\frac{1}{N}$ expansion. For suitable quantities dependent on the dimension N , we control the finite- N behavior by interpolating from the large- N limit. This argument requires that (1) the quantity of interest be a low-degree rational function of N , (2) the function obeys a small apriori bound, and (3) the large- N limit can be effectively calculated.

on the two cases to distinguish, one can prove that the difference of the distinguishing probabilities $f(x_1) - f(x_2)$ is extremely small. While explicitly understanding *all possible* adversarial quantum algorithms is essentially impossible, we often do have sufficient structural restrictions to guarantee that $f(x_1) - f(x_2)$ is a bounded degree polynomial which, remarkably, proves to be sufficient.

Our key insight is to draw a direct connection between the large- N expansion in random matrix theory and polynomial approximation by setting the interpolation parameter to be (Figure 1)

$$x = \frac{1}{N} \quad \text{to control the finite-}N \text{ corrections} \quad \left| f\left(\frac{1}{\infty}\right) - f\left(\frac{1}{N}\right) \right|, \quad (1.11)$$

which requires constructing a suitable function that fulfills the requirements of the polynomial methods, as the most substantial part of our proof.

We further explain the above high-level intuition in the following sections. The sum of permutations is not unitary, so we need to consider an exponential of sums, introducing an infinite series in section IB 1; in section IB 2, we argue that the distinct words $\mathbf{Z}_1 \mathbf{Z}_3 \cdots$ are independent in the large- N limit; in section IB 3, we spell out the central limit theorem for independent sums; in section IB 4, we explain how to control the finite- N corrections through interpolation, which is the most involved step.

1. A single exponential as a sum of words

To begin with, let us study one exponential of our sparse random matrices $e^{i\theta \mathbf{A}_m}$. The Taylor series expansion can be formally expressed as a weighted sum over *words*:⁴ any product of symbols $\mathbf{Z}_1, \cdots, \mathbf{Z}_m$ and their inverses $\mathbf{Z}_a^{-1} = \mathbf{Z}_a^\dagger$ subject only to the trivial cancellations $\mathbf{Z}_a \mathbf{Z}_a^\dagger = \mathbf{Z}_a^\dagger \mathbf{Z}_a = \mathbf{I}$,

⁴ This is also known as the *free group* when there are no nontrivial relations between the generators.

such as

$$\mathbf{Z}_1, \mathbf{Z}_1^\dagger, \mathbf{Z}_2^\dagger \mathbf{Z}_1, \mathbf{Z}_1^3 \mathbf{Z}_2^\dagger \mathbf{Z}_1, \dots \quad (1.12)$$

We denote the set of such words by $\mathcal{W}(\{\mathbf{Z}_a\}_{a=1}^m)$.

$$e^{i\theta \mathbf{A}_m} = \mathbf{I} + \frac{i\theta}{\sqrt{2m}} \sum_{a=1}^m (\mathbf{Z}_a + \mathbf{Z}_a^\dagger) - \frac{\theta^2}{2} \frac{1}{2m} \left(\sum_{a=1}^m \mathbf{Z}_a + \mathbf{Z}_a^\dagger \right)^2 + \dots \quad (1.13)$$

$$= \sum_i w_i \mathbf{W}_i \quad \text{where} \quad \mathbf{W}_i \in \mathcal{W}(\{\mathbf{Z}_a\}_{a=1}^m). \quad (1.14)$$

The expression above is basically a sum over m independent $\mathbf{Z}_i$ and their adjoints but with higher-order corrections due to unitarity. Now, we take iterated *products* of independent copies of these sparse exponentials

$$\prod_{j=1}^{\ell} e^{i\theta \mathbf{A}_m^{(j)}} = \sum_{i=(i_1, \dots, i_\ell)} w_i \mathbf{W}_i \quad \text{where} \quad w_i = (w_{i_1}, \dots, w_{i_\ell}) \quad \text{and} \quad \mathbf{W}_i = \mathbf{W}_{i_1} \cdots \mathbf{W}_{i_\ell}.$$

(distinct words: $\mathbf{W}_i \neq \mathbf{W}_j$ for each $i \neq j$)

We expect the sparsity (and the number of distinct words) to increase exponentially with ℓ , so that merely $\ell \sim \log(N)$ iteration may already produce a very dense matrix. To see that the above product is anywhere close to Haar, the hints come from first analyzing the *large- N limit* where the structure drastically simplifies.

2. Large- N limit

[Lemma IV.1](#) will establish that in the limit of infinite dimension N , fixing the length of the words and the number of queries k , all distinct nontrivial (i.e., non-identity) words can be simultaneously *replaced* with *independent* phased permutations. This means that we may replace our complicated, correlated sum with an independent sum in the diamond norm

$$\mathbf{Z}_L \left(\sum_i w_i \mathbf{W}_i \right) \mathbf{Z}_R \stackrel{N \rightarrow \infty}{\rightrightarrows} \mathbf{Z}_L \left(\sum_i w_i \mathbf{Z}_i \right) \mathbf{Z}_R.$$

(distinct words are independent in the large- N limit: [Lemma IV.1](#))

The additional left and right symmetrizations help prove independence in the parallel query model while also being algorithmically affordable.⁵ The (phased) permutation symmetry reduces the effective dimension so much that the input state can be restricted to a space of dimension depending only on k and independent of N , which allows us to control the statistical distance (diamond norm) without paying an N -dependent conversion loss, which could have been problematic when taking the large- N limit.

⁵ We expect the result to hold even without such symmetrization.

3. Central limit theorem

The nice feature of independent sums is that we can invoke the central limit theorem

$$\sum_i w_i(\theta) \mathbf{Z}_i \stackrel{m^\ell \gg 1}{\approx} \mathbf{G} \quad \text{since} \quad \mathbb{E}[\mathbf{Z}_i^{(\dagger)} \otimes \mathbf{Z}_i^{(\dagger)}] = \mathbb{E}[\mathbf{G}_i^{(\dagger)} \otimes \mathbf{G}_i^{(\dagger)}] \quad (\text{in the sense of } k\text{-fold CP channels})$$

where $\mathbf{G}$ is the *Ginibre ensemble* [Gin65], a random nonhermitian matrix with i.i.d. Gaussian entries. (See section II for the definition.) Indeed, since the second (mixed) moments match, in the limit of many summands,⁶ the fine-grained details of the weights w_i are washed away, and the sum converges to a Gaussian random matrix; see Lemma A.1 for nonasymptotic bounds demonstrated using a Lindeberg principle [CDB⁺23]. While the Ginibre ensemble is not unitary, its effect in a k -fold Completely positive channel is *equal* to Haar in the large- N limit (Lemma B.1)

$$\mathbf{G} \stackrel{N \rightarrow \infty}{=} \mathbf{U}_{Haar}. \quad (\text{in the sense of } k\text{-fold CP channels})$$

Intuitively, the Ginibre ensemble $\mathbf{G}$ has the same symmetry as a Haar random unitary (left and right unitary invariance) and also behaves like a unitary for fixed input states, as seen by the expectation $\mathbb{E}[\mathbf{G}^\dagger \mathbf{G}] = \mathbf{I}$.

4. Verifying the requirements for interpolation

The last and most significant step in our argument is to control the finite- N corrections through an interpolation argument from the large- N limit. In particular, we choose the function of interest f to be the distinguishing probability between the unitaries $\mathbf{V} = \mathbf{Z}_L \left(\prod_{j=1}^\ell e^{i\theta_m A_m^{(j)}} \right) \mathbf{Z}_R$ and $\mathbf{U}_{Haar}$ by defining the key quantity

$$f_{\rho, \mathbf{O}} \left(\frac{1}{N} \right) := \text{Tr}[\mathbf{O} \mathcal{N}_1 \rho] - \text{Tr}[\mathbf{O} \mathcal{N}_2 \rho] \quad \text{for each } \rho \text{ and } \mathbf{O} \quad (1.15)$$

where $\mathcal{N}_1 = \mathcal{N}_{2k, \mathbf{V}}$ and $\mathcal{N}_2 = \mathcal{N}_{2k, \mathbf{U}_{Haar}}$ are the corresponding channels.

We aim to control the finite- N distinguishing probability $f_{\rho, \mathbf{O}}(\frac{1}{N})$ from the large- N limit $f_{\rho, \mathbf{O}}(\frac{1}{\infty})$ for arbitrary fixed ρ and $\mathbf{O}$ that the quantum attacks may use. We spell out the structural requirements for $f_{\rho, \mathbf{O}}(\frac{1}{N})$ for interpolation:

Low-degree rational functions of N (Lemma IV.15). The random permutations are very nice objects that are defined consistently across dimensions $N' \neq N$, inducing channels $\mathcal{N}_1^{(N')}$ and $\mathcal{N}_2^{(N')}$. In particular, the average over permutations can be calculated using a well-defined diagrammatic expansion (Figure III D 2), with coefficients that are low-degree rational functions of N .⁷ However, the problem is that the test quantum state ρ and the test operator $\mathbf{O}$, which are selected adversarially, do not obviously apply in other dimensions. Finding the suitable extension

⁶ and with some requirement that weights are all reasonably small.

⁷ Qualitatively, this can be regarded as the analog of Weingarten expansion in the unitary case.

requires a few arguments: first, the permutation symmetry substantially reduces the number of parameters. Specifically, the Schur-Weyl duality for the commutant of permutations restricts the effective input state ρ to a much smaller object, the *partition algebra* $\mathbf{P}_k(N)$ (Figure III D 2), whose *algebraic structure* only depends on the number of copies k , in particular being *independent* of N as long as the dimension is large $N \geq 2k$ [HR05, HJ20].⁸ While the partition algebra has been studied in the algebraic combinatorics literature, our argument necessitates explicitly describing the embedding with respect to the computational basis in order to verify that the embedding “does not change too quickly” as N increases. This requires a detailed foray into the structure of the partition algebra and writing down an explicit orthogonal basis (section IV C 2) as a diagrammatic sum to establish that the basis coefficients are rational polynomials in $\frac{1}{N}$.

The above understanding of the algebraic structure allows us to handcraft the suitable extension $f_{\rho, \mathcal{O}}$ for other dimensions $N' \neq N$

$$f_{\rho, \mathcal{O}}\left(\frac{1}{N'}\right) = \text{Tr}\left[\mathcal{O}^{(N')} \mathcal{N}_1^{(N')} \rho^{(N')}\right] - \text{Tr}\left[\mathcal{O}^{(N')} \mathcal{N}_2^{(N')} \rho^{(N')}\right] \quad (1.16)$$

by defining a family of test operators

$$\left(\mathcal{O}^{(N')}, \rho^{(N')}\right) \quad \text{for each} \quad 2k \leq N' \leq \infty \quad (1.17)$$

$$\text{such that} \quad \left(\mathcal{O}^{(N)}, \rho^{(N)}\right) = (\mathcal{O}, \rho). \quad (1.18)$$

The operators $\rho^{(N)}, \mathcal{O}^{(N)}$ for other dimensions N' relate to the original $\rho, \mathcal{O}$ in dimension N by substituting the basis we found for the partition algebra. In the end, the function $f_{\rho, \mathcal{O}}(\frac{1}{N})$ is (approximately⁹) a rational polynomial of N with degree $\text{poly}(k)$ and poles at small integers $1, \dots, \tilde{\mathcal{O}}(2k\ell)$.

A priori bounds. The expression is a difference between probabilities such that

$$\left|f_{\rho, \mathcal{O}}\left(\frac{1}{N'}\right)\right| \leq 2 \quad \text{for each integer} \quad N'. \quad (1.19)$$

Large- N limits (Lemma IV.1). The large- N limits of each channel coincide a pair of nicer ones: $\mathcal{N}_1$ to the sum over independent permutations $\sum w_i \mathbf{W}_i \rightarrow \sum w_i \mathbf{Z}_i$, and $\mathcal{N}_2$ to the “Gaussian” model: $U_{\text{Haar}} \rightarrow G_{\text{Ginibre}}$.

$$\begin{aligned} \text{Tr}[\mathcal{O}_{N'} \mathcal{N}_1 \rho_{N'}] &\stackrel{N' \rightarrow \infty}{\equiv} \text{Tr}[\mathcal{O}_{N'} \mathcal{N}_1^{(\text{free})} \rho_{N'}] \\ \text{Tr}[\mathcal{O}_{N'} \mathcal{N}_2 \rho_{N'}] &\stackrel{N' \rightarrow \infty}{\equiv} \text{Tr}[\mathcal{O}_{N'} \mathcal{N}_2^{(\text{Ginibre})} \rho_{N'}]. \end{aligned} \quad (1.20)$$

The independent sums $\mathcal{N}_1^{(\text{free})}$ and Gaussian $\mathcal{N}_1^{(\text{Ginibre})}$ can be compared by the Lindeberg principle [CDB⁺23, CDX⁺24], with an error suppressed by $\text{poly}(1/m^\ell)$ typical in central limit theorems (Lemma A.1). While the most general Lindeberg argument works in any finite dimension N , the large- N limits simplify the calculations.

⁸ In fact, the partition algebras stabilize and are all *isomorphic* for large enough dimension $N \geq 2k$ (Theorem III.2).

⁹ We need to truncate the rapidly converging Taylor expansion for the exponential function.

C. Road map

The remaining sections begin with a summary of the notation and the various random matrix ensembles we will encounter (section II), followed by preliminary background (section III): Markov’s other inequality (section III A), basic notions in algebra (section III B), the representation theory of the symmetric group (section III C), and lastly a self-contained introduction to the partition algebra (section III D).

We then derive the main lemmas: how distinct words of permutations can be replaced by independent permutations in the large- N limit (section IV A), deriving an explicit basis for the partition algebra that is low degree in N (section IV B), then extending the test state ρ and observable $\mathbf{O}$ across dimensions (section IV D). The complete proof of the main result is assembled in section V.

D. Acknowledgments

We thank Chris Bowman, Dmitry Grinko, Jeongwan Haah, Aram Harrow, Jonas Haferkamp, Tom Halverson, William He, Hsin-Yuan Huang, Martin Kassabov, Yunchao Liu, Fermi Ma, Tony Metger, Quynh Nguyen, Ryan O’Donnell, Alexander Poremba, Arun Ram, Makrand Sinha, Norah Tan, Joel Tropp, Jorge Garza Vargas, and Henry Yuen for stimulating discussions. We thank the Simons Institute for the Theory of Computing. A.B. was supported in part by the DOE QuantISED grant DE-SC0020360, the AFOSR under grant FA9550-21-1-0392, and by the U.S. DOE Office of Science under Award Number DE-SC0020266. P.H. acknowledges support from AFOSR (award FA9550-19-1-0369), DOE (Q-NEXT), CIFAR and the Simons Foundation.

II. NOTATION

This section summarizes our notation. We write constants and integration elements in roman font (e, π, i and dt, dx), scalar variables in lowercase (a, b), vectors in bras and kets $|\psi\rangle$, matrices in bold uppercase ($\mathbf{G}, \mathbf{U}$), and vectorized matrices in curly bras and kets $|\mathbf{O}\rangle$. We use curly font for several objects: super-operators ($\mathcal{N}$), sets ($\mathcal{S}$), and algorithms ($\mathcal{A}$).

n	number of qubits
$N(= 2^n)$	local dimension
k	number of copies
$z \in \mathbb{C}$	complex numbers
$\mathbb{E}[\cdot]$	Expectation

Linear algebra:

$\ \psi\rangle\ :$	the Euclidean norm of a vector $ \psi\rangle$
$ \mathbf{O}\rangle :$	vectorized operator $\mathbf{O}$
$\ \mathbf{A}\ := \sup_{ \psi\rangle, \phi\rangle} \frac{\langle\phi \mathbf{A} \psi\rangle}{\ \psi\rangle\ \cdot \ \phi\rangle\ }$	the operator norm of a matrix $\mathbf{A}$
$\mathbf{A}^* :$	the entry-wise complex conjugate of a matrix $\mathbf{A}$
$\mathbf{A}^\dagger :$	the Hermitian conjugate of a matrix $\mathbf{A}$
$\mathbf{A}^T :$	the transpose of a matrix $\mathbf{A}$
$\ \mathbf{A}\ _p := (\text{Tr} \mathbf{A} ^p)^{1/p}$	the Schatten p-norm of a matrix $\mathbf{A}$
$\ \mathcal{N}\ _{p-p} := \sup_{\mathbf{A}} \frac{\ \mathcal{N}[\mathbf{A}]\ _p}{\ \mathbf{A}\ _p}$	the induced $p - p$ norm of a superoperator $\mathcal{N}$
$\ \mathcal{N}\ _\diamond := \ \mathcal{N} \otimes \mathcal{I}\ _{1-1}$	the diamond distance to capture inputs entangled with ancillas
$\mathcal{N}_{2k, \mathbf{O}} := \mathbb{E} \mathbf{O}^{\otimes k}[\cdot] \mathbf{O}^{\dagger \otimes k}$	the CP map associated with k -fold tensor product of $\mathbf{O}$

Representation theory:

$\lambda \vdash m$	integer partitions $(\lambda_1, \lambda_2, \dots)$ of m such that $\sum_i \lambda_i = m, \lambda_1 \geq \lambda_2 \geq \dots$
$\lambda^* = (\lambda_2, \dots)$	integer partitions with the first entry removed
$\Pi \vdash [2k]$	set-partitions for $2k$ elements
$\mathbf{O}_\Pi$	diagram corresponding to set-partition Π acting on $(\mathbb{C}^N)^{\otimes k}$
$\mathbf{O}'_\Pi$	like $\mathbf{O}_\Pi$, but distinct blocks have distinct indices
$\mathbf{P}_k(N)$	the partition algebra for $(\mathbb{C}^N)^{\otimes k}$
$\Lambda_{k, N}$	set of integer partitions corresponding to irreps of $\mathbf{P}_k(N)$
$\mathbf{J}_m$	span of diagrams with at most m propagating blocks
$\sigma \in \mathbf{S}_m$	Symmetry group acting on m elements
p_μ	Young symmetrizer corresponding to irreps labeled by integer partition μ
$t \in SYT(\mu)$	the set of standard Young tableaux associated with shape $\mu \vdash m$.

A. Random matrix ensembles

Our technical argument relies on specific properties of several random matrix ensembles. In dimension N (which is often 2^n for n qubits), we denote

$$\mathbf{U} \stackrel{Haar}{\sim} \mathbf{U}(N) \quad (\text{Haar random unitaries})$$

$$\mathbf{S} \stackrel{unif}{\sim} \mathbf{S}(N) \quad (\text{uniformly random permutations})$$

$$\mathbf{D}_z : (\mathbf{D}_z)_{ij} = \delta_{ij} z_i \quad \text{where} \quad z_i \stackrel{Haar}{\sim} \mathbf{U}(1) \quad (\text{random diagonal phases})$$

$$\mathbf{G} : (\mathbf{G})_{ij} \sim \frac{g + \mathrm{i}g'}{\sqrt{2N}}. \quad (\text{Ginibre ensemble})$$

We will use different notations for the symmetric group to highlight the two distinct roles that the group plays in the paper. $\mathbf{S}(N)$ acts on individual N -dimensional systems while $\mathbf{S}_m$ acts by permuting copies of those systems for $m \leq k$. In the above, all Gaussians are i.i.d. centered with unit variance $\mathbb{E}[g] = 0, \mathbb{E}[g^2] = 1$. The Ginibre ensemble consists of non-Hermitian random matrices, which we normalize such that

$$\mathbb{E}[\mathbf{G}^\dagger \mathbf{G}] = \mathbf{1} \cdot \mathbf{I}, \quad (2.1)$$

making it behave like a unitary in some regards. The random diagonal matrices are not interesting on their own and are meant to multiply with the permutation by

$$\mathbf{Z} := \mathbf{D}_z \mathbf{S}. \quad (\text{random phased permutations})$$

These *1-sparse* matrices are basic building blocks enabled by standard pseudorandomness assumptions (Q-PRPs, [Definition II.1](#); inverses allowed). The central object we consider is the exponential $\mathrm{e}^{\mathrm{i}\theta \mathbf{A}_m}$ of the sparse random matrices

$$\mathbf{A}_m := \frac{1}{\sqrt{2m}} \sum_{a=1}^m (\mathbf{Z}_a + \mathbf{Z}_a^\dagger) \quad \text{where} \quad \mathbf{Z}_a \stackrel{i.i.d.}{\sim} \mathbf{Z}. \quad (\text{adjacency matrix for phased random graph})$$

The normalization ensures that $\mathbb{E}[\mathbf{A}_m^\dagger \mathbf{A}_m] = \mathbf{I}$. The exponentials of the above sparse random matrices can be efficiently simulated on quantum computers using standard algorithms.

Proposition II.1 (Efficient implementation [[GSLW19](#)]). *For each $m, \ell \in \mathbb{Z}^+$ and $\theta \in \mathbb{R}$, the unitary for $\mathrm{e}^{\mathrm{i}\theta \mathbf{A}_m}$ can be implemented at precision ϵ at cost*

$$\mathcal{O}\left(\log(m)m(\theta\sqrt{m} + \log(1/\epsilon))\right) \quad \text{one and two-qubit gates}, \quad (2.2)$$

$$\mathcal{O}(\log(m)) \quad \text{ancillas}, \quad (2.3)$$

$$\text{and} \quad \mathcal{O}\left(\theta\sqrt{m} + \log(1/\epsilon)\right) \quad \text{controlled-queries} \quad (2.4)$$

to the *SELECT* operator (or its adjoint)

$$\sum_{a=1}^m |a\rangle \langle a| \otimes \mathbf{Z}_a. \quad (2.5)$$

Proof. Use LCU with uniform weights $(1/\sqrt{2m}, \dots, 1/\sqrt{2m})$ to create a block-encoding for $\frac{1}{\sqrt{2m}}\mathbf{A}_m$. Then, apply QSVT. $\blacksquare$

B. Pseudorandomness and k -designs

We briefly recall the notions of both computational pseudorandomness and k -designs.

Definition II.1 (Quantum-secure pseudorandom permutations [Zha16]). *We say a keyed family of permutations $\mathbf{S}_w \in \mathcal{S}(2^n)$ is quantum-secure pseudorandom permutation (PRP) if each $\mathbf{S}_w$ can efficiently generated, and for any poly-time quantum algorithm $\mathcal{A}$,*

$$\left| \mathbb{E}_w \mathcal{A}(\mathbf{S}_w, \mathbf{S}_w^{-1}) - \mathbb{E}_{\mathbf{S} \in \mathcal{S}(N)} \mathcal{A}(\mathbf{S}, \mathbf{S}^{-1}) \right| \leq \frac{1}{\text{superpoly}(n)}. \quad (2.6)$$

That is, the difference in the algorithms' acceptance probability on a random element of the PRP ensemble and on a truly random permutation is super-polynomially small.

On the other hand, a quantum unitary k -design (Definition I.1) is an information-theoretic notion. When the error is zero, this simply amounts to saying that the following $2k$ -fold tensors are equal:

$$\mathbb{E}_{\mathbf{V}}[\mathbf{V}^{\otimes k} \otimes \mathbf{V}^{*\otimes k}] = \mathbb{E}_{U_{Haar}}[U_{Haar}^{\otimes k} \otimes U_{Haar}^{*\otimes k}]. \quad (2.7)$$

In the presence of error, the diamond distance (Definition I.1) quantifies the best a quantum computationally unbounded distinguisher can do given parallel access to the unitary ensemble. Various other norms yield qualitatively different operational meanings in the presence of error, but the unconditional interconversion costs can easily scale with the dimension.

III. PRELIMINARIES

In this section, we collect several technical facts that form the raw ingredients of the argument. In particular, we include a largely self-contained summary of the relevant facts from abstract algebra.

A. Markov's "other" inequality for polynomials

One of the very few techniques available for proving query complexity lower bounds is the *polynomial method*. The starting point is a rather simple classical result in low-degree polynomials.

Lemma III.1 (Markov's other inequality [Mar89, Mar16, RC66, EZ64]). *Let $f(x) : \mathbb{R} \rightarrow \mathbb{R}$ be a real polynomial of degree d .*

$$\sup_{x \in [0,1]} |f'(x)| \leq d^2 \max_{x \in [0,1]} |f(x)|.$$

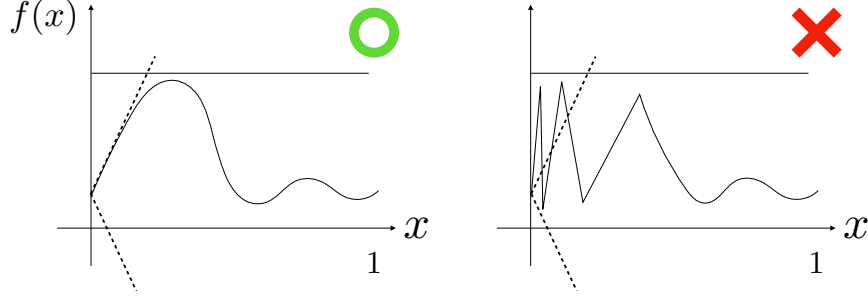


Figure 2: Markov's other inequality states that a bounded, low-degree polynomial cannot change too quickly. This simple fact can prove nontrivial query complexity lower bounds through careful choice of the interpolation parameter x and the low-degree quantity $f(x)$.

The standard recipe for applying the above to lower-bounding the number of queries required for distinguishing tasks goes roughly as follows: cook up a quantity f that depends on an interpolation parameter x such that

- The values $f(x_1)$ and $f(x_2)$ correspond to the acceptance probabilities for the two cases to be distinguished.
- The function $f(x)$ is a low-degree polynomial with a degree d roughly the number of queries.
- The function $f(x)$ can be *extended* to a larger interval $[x_1, x_3]$ with $x_3 - x_1 \gg x_2 - x_1$ such that its value remains bounded.

Then, the distinguishing probability must not change too quickly between the two cases provided the degree d is small:

$$|f(x_1) - f(x_2)| \leq d^2 \frac{|x_1 - x_2|}{|x_1 - x_3|} \max_{x \in [x_1, x_3]} |f(x)|. \quad (3.1)$$

Applying the above requires a case-by-case adaptation, and creativity is often required to satisfy the combination of constraints. In our setting, the natural yet powerful approach is to select the interpolation parameter to be the inverse-dimension

$$x = \frac{1}{N} \quad \text{with interpolation range} \quad 0 \leq x \leq 1, \quad (3.2)$$

which connects to the idea of the $\frac{1}{N}$ expansion in physics and in random matrix theory.

We will use the following specialized versions as a black-box. ¹⁰

Lemma III.2 (Large- N interpolation). *Let $f(x) : \mathbb{R} \rightarrow \mathbb{R}$ be a real polynomial of degree d and let N, N_0 be any nonnegative integers. Suppose that $d^2 \leq \frac{N_0+1}{2}$,*

$$\sup_{N \geq N_0} N \left| f\left(\frac{1}{N}\right) - f(0) \right| \leq \sup_{x \in [0, \frac{1}{N_0}]} |f'(x)| \leq 2d^2 \cdot N_0 \sup_{N \geq N_0} \left| f\left(\frac{1}{N}\right) \right|. \quad (3.3)$$

¹⁰ We thank the authors of [CvHVT] for allowing us to include this variant of Markov's other inequality for $\frac{1}{N}$ -interpolation from their upcoming concurrent work pursuing a different direction, initiated around the same time in the early stages.

In our case, the interpolation range will need to effectively shrink

$$0 \leq x \leq 1 \rightarrow 0 \leq x \leq \frac{1}{N_0} \quad (3.4)$$

to handle the presence of gaps in the integer reciprocals $\{\frac{1}{1}, \frac{1}{2}, \dots, \frac{1}{N}, \dots\}$; this will further worsen the dependence on the degree by roughly $\mathcal{O}(d^2) \rightarrow \mathcal{O}(d^4)$ (since $N_0 \geq d^2 - 1$).

Lemma III.3 (Markov inequality for rational polynomials with clustered poles). *Consider a rational polynomial of integer N*

$$f\left(\frac{1}{N}\right) = \frac{a(N)}{b(N)} \quad \text{where} \quad b(N) = \prod_i (N - b_i)^{m_i}. \quad (3.5)$$

Suppose the poles b_i are located within a disc of radius $|b_i| \leq B$, and the total degree is $d = \sum_i m_i$. Then, suppose $N_0 \geq 8dB + d^2 - 1$, and $f(\frac{1}{\infty}) < \infty$, we have that

$$\sup_{N \geq N_0} N \left| f\left(\frac{1}{N}\right) - f\left(\frac{1}{\infty}\right) \right| \leq 2d^2(N_0 + 10dB) \sup_{N \geq N_0} \left| f\left(\frac{1}{N}\right) \right|. \quad (3.6)$$

The above allows us to only keep track of the locations and multiplicity of the pole without worrying about the polynomial degree on the numerator.

B. Basic algebraic notions

The partition algebra represented on the Hilbert space $\mathbf{B}(\mathbb{C}(\mathcal{H})^{\otimes k})$ is an *algebra* (matrix addition and multiplication) with *involution* (matrix conjugate transpose). This abstract algebraic structure already imposes structure that will be helpful. We introduce the minimal algebraic assumption as follows.

Definition III.1 (Associative algebras over the complex numbers (abbreviated as algebras in this work)). *A $\mathbb{C}$ -algebra $\mathbf{A}$ is a set of elements such that*

- (Closed under scalar multiplication) For any $z \in \mathbb{C}$ and $\mathbf{A}_1 \in \mathbf{A}$,

$$z\mathbf{A}_1 \in \mathbf{A}. \quad (3.7)$$

- (Closed under addition and multiplication) For any $\mathbf{A}_1, \mathbf{A}_2 \in \mathbf{A}$,

$$\mathbf{A}_1 + \mathbf{A}_2 \in \mathbf{A} \quad (3.8)$$

$$\mathbf{A}_1 \cdot \mathbf{A}_2 \in \mathbf{A}. \quad (3.9)$$

- (Distributive and associative) For any $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3 \in \mathbf{A}$,

$$(\mathbf{A}_1 \cdot \mathbf{A}_2) \cdot \mathbf{A}_3 = \mathbf{A}_1 \cdot (\mathbf{A}_2 \cdot \mathbf{A}_3) \quad (3.10)$$

$$(\mathbf{A}_1 + \mathbf{A}_2) + \mathbf{A}_3 = \mathbf{A}_1 + (\mathbf{A}_2 + \mathbf{A}_3) \quad (3.11)$$

Definition III.2 ($\dagger$ -algebra). A $\dagger$ -algebra $\mathbf{A}$ is an $\mathbb{C}$ -algebra with involution $(\cdot)^\dagger$ such that

- For any $\mathbf{A}_1 \in \mathbf{A}$,

$$(\mathbf{A}_1^\dagger)^\dagger = \mathbf{A}_1. \quad (3.12)$$

- For any $\mathbf{A}_1, \mathbf{A}_2 \in \mathbf{A}$,

$$(\mathbf{A}_1 + \mathbf{A}_2)^\dagger = \mathbf{A}_1^\dagger + \mathbf{A}_2^\dagger \quad (3.13)$$

$$(\mathbf{A}_1 \mathbf{A}_2)^\dagger = \mathbf{A}_2^\dagger \mathbf{A}_1^\dagger. \quad (3.14)$$

- For any $z \in \mathbb{C}$,

$$(z\mathbf{A}_1)^\dagger = z^* \mathbf{A}_1^\dagger. \quad (3.15)$$

Definition III.3 ($\dagger$ -homomorphism). A $\dagger$ -homomorphism is a map between $\dagger$ -algebras $f : \mathbf{A} \rightarrow \mathbf{A}'$ such that

$$f(\mathbf{A}_1 + \mathbf{A}_2) = f(\mathbf{A}_1) + f(\mathbf{A}_2), \quad (3.16)$$

$$f(\mathbf{A}_1 \cdot \mathbf{A}_2) = f(\mathbf{A}_1) \cdot f(\mathbf{A}_2), \quad (3.17)$$

$$f(\mathbf{A}_1^\dagger) = f(\mathbf{A}_1)^\dagger. \quad (3.18)$$

Definition III.4 (Ideals). A left-ideal $\mathbf{J}$ of a ring $\mathbf{R}$ is a subring that is closed under multiplying the ring on the left

$$\mathbf{R}\mathbf{J} \subset \mathbf{J}. \quad (3.19)$$

Vice versa for the right ideals. A two-sided ideal is both a left and right ideal.

Definition III.5 (Factor). An algebra whose center consists only of multiples of the identity is called a factor.

Definition III.6 (Matrix algebra). For any finite-dimensional complex Hilbert space $\mathcal{H}$, the matrix algebra $\mathbf{B}(\mathcal{H})$ is the set of linear transformations $\mathcal{H} \rightarrow \mathcal{H}$. Moreover, the adjoint or, equivalently, the conjugate transpose w.r.t. any orthogonal basis defines a canonical involution of the algebra.

Theorem III.1 ($\dagger$ -Subalgebras of matrix algebras). Any $\dagger$ -subalgebra $\mathbf{A}$ of a finite dimensional matrix algebra $\mathbf{B}(\mathbb{C}^N)$ is unitarily conjugate to a direct sum of factors (labeled by λ)

$$\mathbf{U}\mathbf{B}\mathbf{U}^\dagger = \bigoplus_{\lambda} \mathbf{M}_{\lambda} \otimes \mathbf{I} \quad \text{where} \quad \mathbf{M}_{\lambda} = \mathbf{B}(\mathbb{C}^{d_{\lambda}}). \quad (3.20)$$

Further, any two-sided ideal $\mathbf{J}$ of $\mathbf{A}$ must have the structure

$$\mathbf{U}\mathbf{J}\mathbf{U}^\dagger = \bigoplus_{\lambda} \mathbf{M}'_{\lambda} \otimes \mathbf{I} \quad \text{where} \quad \mathbf{M}'_{\lambda} = \mathbf{M}_{\lambda} \quad \text{or} \quad \mathbf{M}'_{\lambda} = 0, \quad (3.21)$$

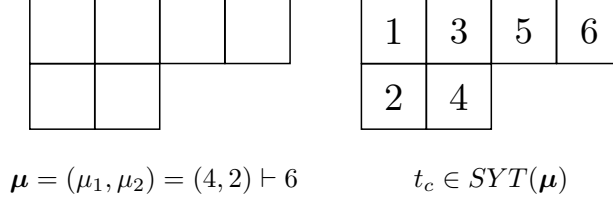


Figure 3: (Left) A Young diagram corresponding to the integer partition $\boldsymbol{\mu} \vdash 6$. (Right) The column-reading Young tableau $t_c \in SYT(\boldsymbol{\mu})$ as a special case of standard Young tableaux.

and the quotient is isomorphic to another ideal

$$\frac{A}{J} \simeq J' \simeq \bigoplus_{\lambda} M''_{\lambda} \otimes \mathbf{I} \quad \text{where} \quad M''_{\lambda} = 0 \quad \text{or} \quad M''_{\lambda} = M_{\lambda}. \quad (3.22)$$

The quotient can be naturally understood as a projector $\mathcal{Q}_J : A \rightarrow J' \subset A$ by $\mathcal{Q}_J[M_{\lambda} \otimes \mathbf{I}] = M_{\lambda''} \otimes \mathbf{I}$, which is also a $\dagger$ -homomorphism.

Proof. This is a consequence of the Artin-Wedderburn theorem. See [HR05] for a self-contained exposition. ■

Definition III.7 (Group algebra with complex coefficients). *For a group G , the group algebra $\mathbb{C}G$ consists of formal weighted linear combination of elements $G_i \in G$*

$$\sum_i z_i G_i \in \mathbb{C}G, \quad (3.23)$$

with multiplication given by the group multiplication $G_1 \cdot G_2$.

C. Representations of the symmetric group

This section includes a minimal review of the representation theory of the symmetric group that will be helpful for working with the partition algebra; see [Sag13] for a textbook introduction.

1. Integer partitions

For any nonnegative integer $N \in \mathbb{Z}$ and vector of nonnegative integers $\boldsymbol{\lambda}$, we say that $\boldsymbol{\lambda}$ is an *integer partition* of N , or

$$\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_{\ell}) \vdash N \quad \text{whenever} \quad \lambda_1 + \dots + \lambda_{\ell} = N \quad \text{and} \quad \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_{\ell}. \quad (3.24)$$

We will also denote the related notions by

$$|\boldsymbol{\lambda}| := \lambda_1 + \dots + \lambda_{\ell} \quad \text{and} \quad \boldsymbol{\lambda}^* := (\lambda_2, \dots, \lambda_{\ell}). \quad (3.25)$$

In our usage for labeling the irreducible representations of the partition algebra $\mathbf{P}_k(N)$ by $\lambda \in \Lambda_{k,N}$, we will often consider a partition of the local dimension N such that the first row is $|\lambda| - |\lambda^*| \geq N - k$. Since the length of the first row is fixed by the remaining boxes $\lambda_1 = N - |\lambda^*|$, we will also only focus on the partition of the remaining boxes, often denoted by $\lambda^* = \mu \vdash m$.

2. Young diagrams and Young tableaux

Any integer partition $\mu \vdash m$ corresponds to a *Young diagram* (Fig. 3). In particular, one can fill in numbers $1, \dots, m$ in arbitrary order, giving a *Young tableau*. For a given shape $\mu \vdash m$, a *standard Young tableau* $t \in SYT(\mu)$ has its rows increase from left to right, and the columns increase from top to bottom. For each integer partition μ , the *column-reading tableau* $t_c \in SYT(\mu)$ fills in the Young diagram by going down the columns from left to right from 1 to m .

3. Irreducible modules

This section describes the irreducible modules of the symmetric group algebra, and the notions presented here will prove useful when studying the partition algebra. For each Young tableau t of shape μ , define the particular permutation

$$\sigma_t \quad \text{such that} \quad \sigma_t : t_c \rightarrow t \in SYT(\mu). \quad (3.26)$$

That is, σ_t is the permutation that sends the column-reading Young tableau t_c to the Young tableau t .

For each integer partition $\mu \vdash m$, consider the *Young symmetrizer*

$$p_\mu := \sum_{\sigma \in C(t_c)} \sum_{\sigma' \in R(t_c)} \text{sgn}(\sigma) \sigma \sigma' \in \mathbb{C}S_m \quad (3.27)$$

where $\mathbb{C}S_m$ is the group algebra (Definition III.7) for the symmetric group S_m , $C(t_c)$ is the subgroup of permutations that preserves the rows of t_c , $R(t_c)$ the one for the columns, and $\text{sgn}(\sigma)$ is the sign of the permutation σ .

Lemma III.4 (Irreducible module of $\mathbb{C}S_m$ [Sag13]). *For each integer partition $\mu \vdash m$, the space*

$$\mathbb{C}\text{-span}\{\sigma_t p_\mu\}_{t \in SYT(\mu)} \subset \mathbb{C}S_m \quad (3.28)$$

is a copy of the irreducible module S_m^μ labeled by μ in the left regular representation of $\mathbb{C}S_m$.

Lemma III.5 (An orthonormal basis). *There exist $u_t \in \mathbb{C}\text{-span}\{\sigma_{t'}\}_{t' \in SYT(\mu)}$ such that*

$$\mathbb{C}\text{-span}\{\sigma_t p_\mu\}_{t \in SYT(\mu)} = \mathbb{C}\text{-span}\{u_t p_\mu\}_{t \in SYT(\mu)} \quad (3.29)$$

and the map

$$\mathbf{u}_t \mathbf{p}_\mu \mathbf{p}_\mu^\dagger \mathbf{u}_{t'}^\dagger \rightarrow |t\rangle \langle t'| \quad \text{is a } \dagger\text{-isomorphism.} \quad (3.30)$$

Therefore, the span

$$\mathbb{C}\text{-span}\{\mathbf{u}_t \mathbf{p}_\mu \mathbf{p}_\mu^\dagger \mathbf{u}_{t'}^\dagger\}_{t,t' \in SYT(\mu)} \subset \mathbb{C} \mathbf{S}_m \quad (3.31)$$

is a factor as a $\dagger$ -subalgebra.

Proof. For each irrep labeled by μ , run any orthogonalization procedure and fix it. The point is that this solely depends on the irrep label μ for the symmetric group (and not on the dimension of the computation basis). $\blacksquare$

Note that the above notions can be discussed abstractly without considering the computational basis (or we could represent the permutation by acting on m many copies of N -dimensional Hilbert space $\mathbf{S}_m$). In contrast, the multiplication rule for the partition algebra $\mathbf{P}_k(N)$ depends on N , and we expect the basis to also explicitly depend on N . We will see that the inclusion $\mathbb{C}[\mathbf{S}_m] \otimes \mathbf{I}_{k-m} \subset \mathbf{P}_k(N)$ will be very helpful in analyzing the structure of the partition algebra, and the objects $\mathbf{u}_t \mathbf{p}_\mu \in \mathbf{P}_k(N)$ defined above will play a crucial role.

4. The computational basis

Consider k copies of N -dimensional Hilbert spaces $(\mathbb{C}^N)^{\otimes k}$ and its matrix algebra $\mathbf{B}((\mathbb{C}^N)^{\otimes k})$. A natural choice of orthonormal basis is the computational (orthonormal) basis $|m\rangle$, which naturally extends by the tensor product structure

$$\mathcal{H} = \mathbb{C}^N = \text{Span}\{|m\rangle\}_{m \in [N]} \quad (3.32)$$

$$\text{inducing } (\mathbb{C}^N)^{\otimes k} = \text{Span}\{|m_1\rangle \otimes \cdots \otimes |m_k\rangle\}_{m_i \in [N]}, \quad (3.33)$$

$$\text{inducing } \mathbf{B}((\mathbb{C}^N)^{\otimes k}) = \text{Span}\{\underbrace{|m_1\rangle \otimes \cdots \otimes |m_k\rangle \cdot \langle m_{k+1}| \otimes \cdots \otimes \langle m_{2k}|}_{=:\mathbf{O}_m}\}_{m_i \in [N]}, \quad (3.34)$$

$$\stackrel{vec.}{\equiv} \text{Span}\{\underbrace{|m_1\rangle \otimes \cdots \otimes |m_k\rangle \cdot |m_{k+1}\rangle \otimes \cdots \otimes |m_{2k}\rangle}_{=:|\mathbf{O}_m\rangle}\}_{m_i \in [N]}. \quad (3.35)$$

The algebra $\mathbf{B}((\mathbb{C}^N)^{\otimes k})$ as a $\mathbb{C}$ -vector space is naturally endowed with the Hilbert-Schmidt inner product $\text{Tr}[\mathbf{O}_1^\dagger \mathbf{O}_2]$. When the multiplication structure is unimportant, we may *vectorize* (*vec.* as above) the matrices into vectors of doubled dimension to focus on the Hilbert space structure. The inner product remains the same by $(\mathbf{O}_1 | \mathbf{O}_2) := \text{Tr}[\mathbf{O}_1^\dagger \mathbf{O}_2]$.

Formally, for a matrix $\mathbf{A}$, let us denote its vectorization (or purification) by

$$|\mathbf{A}\rangle := (I \otimes T) \mathbf{A} \quad (3.36)$$

using the “transpose” map $T|i\rangle = |i\rangle$ to turn bras into kets. Consequently, the definition extends to the *vectorization* of a superoperator by

$$\mathcal{N}[\cdot] = \sum_j \alpha_j \mathbf{A}_j[\cdot] \mathbf{B}_j \rightarrow \mathcal{N} = \sum_j \alpha_j \mathbf{A}_j \otimes \mathbf{B}_j^T$$

where $\mathbf{B}_j^T$ denotes the transpose of the matrix $\mathbf{B}_j$ in the computational basis $|i\rangle$. We use curly fonts $\mathcal{N}$ for superoperators and bold fonts $\mathcal{N}$ for the vectorized superoperators, which are themselves matrices.

D. The partition algebra

In quantum information, we often consider the commutant of tensor copies of unitaries

$$\left(\{U^{\otimes k}\}_{U \in U(N)}\right)' \subset \mathbf{B}((\mathbb{C}^N)^{\otimes k}). \quad (3.37)$$

This commutant algebra is completely characterized by Schur-Weyl duality and the representation theory of the symmetric group. In this article, we are interested in the commutant of tensored *permutations* $\mathbf{S}^{\otimes k}$, called the *partition algebra* $\mathbf{P}_k(N)$, which depends on the number of copies k and the dimension N :

$$\mathbf{P}_k(N) := (\{\mathbf{S}^{\otimes k}\}_{\mathbf{S} \in \mathbf{S}(N)})' \subset \mathbf{B}((\mathbb{C}^N)^{\otimes k}) \quad \text{where} \quad \mathbf{S}|i\rangle = |S(i)\rangle \quad \text{for each} \quad i = 1, \dots, N. \quad (3.38)$$

In the case $N \geq 2k$, Schur-Weyl duality also holds as follows:

$$\mathbf{P}_k(N) \equiv \bigoplus_{\lambda \in \Lambda_{k,N}} \mathbf{P}_\lambda \otimes \mathbf{I}_{\mathbf{S}_\lambda} \quad \text{and} \quad \mathbb{C}\text{-span}\{\mathbf{S}^{\otimes k}\}_{\mathbf{S} \in \mathbf{S}(N)} = \bigoplus_{\lambda \in \Lambda_{k,N}} \mathbf{I}_{\mathbf{P}_\lambda} \otimes \mathbf{S}_\lambda \quad (3.39)$$

$$\text{acting on} \quad (\mathbb{C}^N)^{\otimes k} \equiv \bigoplus_{\lambda \in \Lambda_{k,N}} \mathcal{H}_{\mathbf{P}_\lambda} \otimes \mathcal{H}_{\mathbf{S}_\lambda} \quad (3.40)$$

where the irreps are labeled by integer partitions

$$\lambda \in \Lambda_{k,N} := \{\lambda \vdash N \mid 0 \leq |\lambda^*| \leq k\}. \quad (3.41)$$

Indeed, since the permutations acting naturally on the computational basis are a special subset of the unitaries, $\mathbf{S}(N) \subset \mathbf{U}(N)$, the commutant is larger $(\{U^{\otimes k}\}_{U \in U(N)})' \subset \mathbf{P}_k(N)$. Crucially for our later argument, the algebra “stops changing” after $N \geq 2k$ ¹¹.

Theorem III.2 ([HJ20]). *If $N \geq 2k$, the dimension of the partition algebra (sum of dimensions of the irreps) is $\dim(\mathbf{P}_k(N)) = \text{Bell}_{2k}$, which is independent of N . In fact, for each fixed k , the partition algebra stabilizes in terms of N . That is, the irreducible algebra representations are isomorphic (as algebras)*

$$\mathbf{P}_\lambda \simeq \mathbf{P}_{\lambda'} \quad \text{whenever} \quad \lambda^* = \lambda'^* \quad \text{and} \quad |\lambda|, |\lambda'| \geq 2k. \quad (3.42)$$

¹¹ This is a different regime from some other applications where $N \ll 2k$, e.g., [FTH23, Ngu23, GBO23a, GBO23b].

Proposition III.1 (Bounds on the Bell number, e.g., [Low10]). *The Bell numbers are bounded by*

$$Bell_n \leq n! \quad \text{for each } n \in \mathbb{Z}. \quad (3.43)$$

Lemma III.6 (Hook formula [Sag13, Theorem 3.10.2]). *For each integer partition $\lambda \in \Lambda_{k,N}$, the dimension of the corresponding irreducible representation of the symmetric group is a polynomial of N*

$$\dim \mathbf{S}_\lambda = \frac{N!}{\prod_{(i,j) \in \lambda} h(i,j)} = \frac{N^{b_0(\lambda)} (N-1)^{b_1(\lambda)} \cdot (N-2k-1)^{b_{2k-1}(\lambda)}}{\prod_{(i,j) \in \lambda^*} h(i,j)} = s_\lambda(N) \quad (3.44)$$

where $h(i,j)$ is the hook length of the Young diagram associated with shape λ

$$b_j = 0, 1 \quad \text{and} \quad \deg(s_\lambda) = \sum b_j = |\lambda^*| \leq k. \quad (3.45)$$

From Equation 3.44, viewing the dimension as a function of N , we see that the zeros are located at integer values in a bounded range and have multiplicity at most one. Strictly speaking, we can restrict to a stronger symmetry as we actually use phased permutations (see, e.g., Lemma IV.1). Nevertheless, most of the discussions will consider the permutation $\mathbf{S}(N)$ as it is more general and well-studied.

1. Set-partitions

Following the notation of [Low10], consider partitions Π of a set with ℓ elements. (It will be convenient to distinguish notationally from the integer partitions discussed in section III C 1.) We write

- $\Pi \vdash \{1, \dots, \ell\}$ iff Π is a set-partition of $\{1, \dots, \ell\}$.
- $(i, j) \in \Pi$ iff (i, j) are in the same *block* (also known as a *cycle*) of Π .
- $|\Pi| := (\text{number of blocks of } \Pi)$.
- $\Pi_1 \leq \Pi_2$ iff $(i, j) \in \Pi_1 \implies (i, j) \in \Pi_2$, which reads “ Π_1 is a refinement of Π_2 .”

For example, let $\Pi = \{\{1, 3\}, \{2\}\}$, then

$$\Pi \vdash \{1, 2, 3\}, \quad (1, 3) \in \Pi, \quad \text{and} \quad |\Pi| = 2. \quad (3.46)$$

The partial order structure between integer partitions will become important, and we will make use of generalized inclusion-exclusion principles. This can be understood in linear algebraic terms.

Lemma III.7 (Linear extension of partial order [DP02]). *Any finite set with partial order can be extended as a subset of a totally ordered set. Therefore, the partial order can be (nonuniquely) represented as an upper triangular 0/1-matrix $\mathbf{M}$ satisfying $M_{ij} = 1$ if and only if $i \geq j$.*

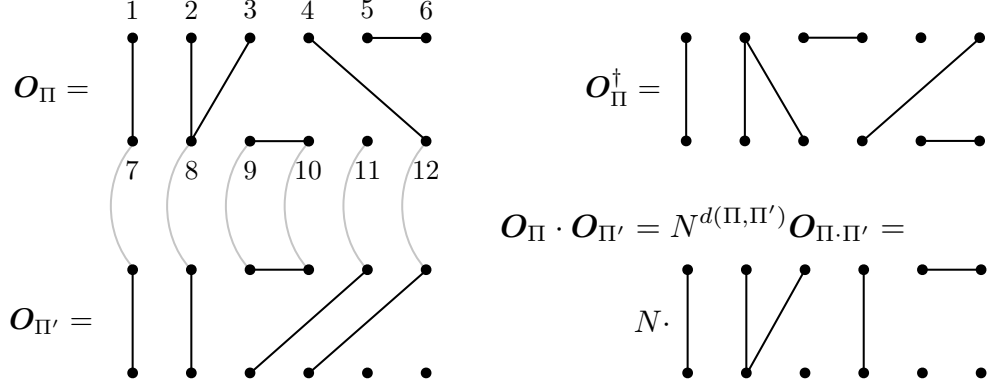


Figure 4: (Left) The diagrams O_Π and $O_{\Pi'}$ corresponding to set-partitions $\Pi = ((1, 7), (2, 3, 8), (9, 10), (4, 12), (11), (5, 6))$ and $\Pi' = ((1, 7), (2, 8), (3, 4), (5, 9), (10, 6), (11), (12))$ for $k = 6$. (Top right) The conjugation $O_\Pi^\dagger$ is simply flipping the diagram upside down. (Bottom right) Multiplying two diagrams amounts to identifying the adjacent rows (indicated by gray lines) and simplifying the diagram to remove any connected components lying completely within the identified rows. A factor of N appears for each component removed during diagram simplification, accounted for by $d(\Pi, \Pi')$. Thus, although the diagrams and set-partitions do not explicitly refer to the local dimension N , the partition algebra is a priori dependent on N .

Lemma III.8 (Restricting partial order). *For any finite set with partial order induced a partial order for any subset. Restriction of an upper triangular matrix on a subset of indices remains upper triangular.*

Lemma III.9 (Inverting triangular matrices). *Any upper triangular matrix with nonzero diagonals is invertible by another upper triangular matrix.*

Proof. This follows immediately from the expression for the inverse of a matrix in terms of its adjugate [HJ12]. ■

2. Explicit presentation

The partition algebra $P_k(N)$ can be defined abstractly but, for concreteness, we will explicitly present it in the computational basis throughout this work. We need to introduce new notation to capture this high-dimensional object. In particular, for our purposes, the notation in this section assumes we are in the stable range where $N \geq 2k > 0$. Let

$$\begin{aligned}
 \mathbf{m} &= (m_1, \dots, m_{2k}) \in \{1, \dots, N\}^{2k} && \text{(tuple of indices)} \\
 M'_\Pi &:= \{\mathbf{m} : m_i = m_j \text{ iff } (i, j) \in \Pi\}. && \text{(set of } \mathbf{m} \text{ whose partition is exactly } \Pi) \\
 M_\Pi &:= \{\mathbf{m} : m_i = m_j \text{ if } (i, j) \in \Pi\}. && \text{(set of } \mathbf{m} \text{ whose partition is refined by } \Pi)
 \end{aligned}$$

The two types of sets M_Π , M'_Π are related by the union

$$M_\Pi = \bigcup_{\Pi' \geq \Pi} M'_{\Pi'}, \quad (3.47)$$

where each $M'_{\Pi'}$ are disjoint from each other.

The cardinality of sets M_Π, M'_Π is given by an elementary calculation:

$$|M'_\Pi| = N(N-1) \cdots (N - |\Pi| + 1) \quad \text{and} \quad |M_\Pi| = N^{|\Pi|}. \quad (3.48)$$

In particular, observe that both quantities are polynomials in N , and the zeros are located at integer values – this seemingly innocent structure will play a crucial role in our interpolation argument. Using the above notation, the partition algebra $\mathbf{P}_k(N) \subset \mathbf{B}((\mathbb{C}^N)^{\otimes k})$ is a $\dagger$ -algebra presented by a $\mathbb{C}$ -linear combination of the following operators (using the notation of (3.34)):

$$\mathbf{P}_k(N) = \text{Span}_{\mathbb{C}}\{\mathbf{O}_\Pi\}_\Pi \quad \text{where} \quad \mathbf{O}_\Pi := \sum_{m \in M_\Pi} \mathbf{O}_m \quad \text{for each} \quad \Pi \vdash \{1, \dots, 2k\}. \quad (3.49)$$

These can be described diagrammatically, as illustrated in Figure 4. The *involution* (i.e., adjoint) acts as

$$(\mathbf{O}_\Pi)^\dagger = \mathbf{O}_{\Pi^\dagger} \quad \text{where} \quad \Pi^\dagger \vdash \{1, \dots, 2k\}. \quad (3.50)$$

Graphically, the involuted partition $\Pi^\dagger$ amounts to flipping it “upside down,” which is consistent with the matrix adjoint. The multiplication operation (realized as matrix multiplication) acts nicely on these operators by

$$\mathbf{O}_{\Pi_2} \mathbf{O}_{\Pi_1} = \mathbf{O}_{\Pi_2 \cdot \Pi_1} \cdot N^{d(\Pi_2, \Pi_1)}, \quad (3.51)$$

where the multiplication rule for set-partitions $\Pi_2 \cdot \Pi_1$ is summarized in Figure 4 and given in more detail in [HR05, HJ20]. The integer d is a function of both Π_1 and Π_2 but independent of N . Graphically,

$$d = \#(\text{components without free legs after multiplying } \Pi_1 \text{ and } \Pi_2). \quad (3.52)$$

While $\mathbf{P}_k(N)$ depends on both k and N , the algebraic structure is mainly determined by k since $\Pi \vdash \{1, \dots, 2k\}$; the dependence on N only comes in as a multiplicative weight $N^{d(\Pi_2, \Pi_1)}$. Alternatively, we may describe the algebra in the orthogonal basis

$$\mathbf{O}'_\Pi := \sum_{m \in M'_\Pi} \mathbf{O}_m \quad \text{such that} \quad \text{Tr}[\mathbf{O}'_{\Pi'} \mathbf{O}'_\Pi] = \delta_{\Pi, \Pi'} \cdot \|\mathbf{O}'_\Pi\|_2^2 \quad \text{for each} \quad \Pi, \Pi' \vdash \{1, \dots, 2k\}, \quad (3.53)$$

as drawn in [Figure 5](#). This new set of operators is related to the original ones by a *Möbius* inversion (a generalized inclusion-exclusion principle for partial orders, [Lemma III.7](#), [Lemma III.9](#))

$$\mathbf{O}_\Pi = \sum_{\Pi' \geq \Pi} \mathbf{O}'_{\Pi'} \quad (3.54)$$

$$= \sum_{\Pi' \vdash \{1, \dots, 2k\}} K_{\Pi\Pi'} \mathbf{O}'_{\Pi'} \quad \text{where} \quad K_{\Pi\Pi'} := \mathbb{1}(\Pi' \geq \Pi) \quad (3.55)$$

$$\mathbf{O}'_\Pi = \sum_{\Pi' \vdash \{1, \dots, 2k\}} (K^{-1})_{\Pi\Pi'} \mathbf{O}_{\Pi'} \quad (3.56)$$

where $\mathbf{K}^{-1}$ is the Möbius inversion of $\mathbf{K}$; indeed, the matrix $\mathbf{K}$ is upper triangular with ones on the diagonals and thus invertible ([Lemma III.9](#)). Importantly, the entries of matrix $\mathbf{K}$ only depend on the combinatorial structure of $\Pi \vdash 2k$ and are independent of N .

For simplicity, we can ignore the multiplicative structure and vectorize the operators (by turning bras to kets ([3.35](#))). In this picture, it is convenient to think about the orthogonal basis $|\mathbf{O}'_\Pi\rangle$ which, as we've seen, can be expressed by a linear combination of $|\mathbf{O}_\Pi\rangle$.

$$|\mathbf{O}'_\Pi\rangle := \sum_{m \in M'_\Pi} |\mathbf{O}_m\rangle \quad \text{where} \quad (\mathbf{O}'_\Pi | \mathbf{O}'_\Pi) = \|\mathbf{O}'_\Pi\|_2^2 = |M'_\Pi| \quad \text{for each} \quad \Pi \vdash \{1, \dots, 2k\}. \quad (3.57)$$

Then, the action of tensored permutations can be written as a superoperator projecting $\mathbf{B}((\mathbb{C}^N)^{\otimes k}) \rightarrow \mathbf{P}_k(N) \subset \mathbf{B}((\mathbb{C}^N)^{\otimes k})$

$$\mathcal{N}_{2k,S} := \mathbb{E}[\mathbf{S}^{\otimes k}(\cdot) \mathbf{S}^{\dagger \otimes k}] = \sum_{\Pi \vdash 2k} \frac{\mathbf{O}'_\Pi \text{Tr}[\mathbf{O}'_\Pi(\cdot)]}{\|\mathbf{O}'_\Pi\|_2^2}, \quad (3.58)$$

or as an operator after vectorization

$$\mathcal{N}_{2k,S} := \mathbb{E}[\mathbf{S}^{\otimes k} \otimes \mathbf{S}^{*\otimes k}] = \sum_{\Pi \vdash 2k} \frac{|\mathbf{O}'_\Pi\rangle \langle \mathbf{O}'_\Pi|}{\|\mathbf{O}'_\Pi\|_2^2}, \quad (3.59)$$

where the Hilbert-Schmidt norm reads $\|\mathbf{O}\|_2 = \sqrt{\text{Tr}[\mathbf{O}^\dagger \mathbf{O}]} = \sqrt{(\mathbf{O} | \mathbf{O})}$. Importantly, for each Π , the zeros of the normalization factors $|M'_\Pi|$ are contained in the integer set $\{0, 1, \dots, 2k\}$ by [Equation 3.48](#). The operators $\mathbf{O}_\Pi$ are also nice in the sense that

$$\text{Tr}[\mathbf{O}_{\Pi_1}^\dagger \mathbf{O}_{\Pi_2}] = N^{c(\Pi_1, \Pi_2)} \quad \text{for each partition} \quad \Pi \vdash \{1, \dots, 2k\} \quad (3.60)$$

for an integer $c(\Pi_1, \Pi_2)$ depending only on Π_1, Π_2 (and independent of N); graphically,

$$c(\Pi_1, \Pi_2) = \#(\text{connected components after fully contracting } \Pi_1^\dagger \text{ and } \Pi_2). \quad (3.61)$$

This also gives the inner product

$$\frac{\text{Tr}[\mathbf{O}_{\Pi_1}^\dagger \mathbf{O}_{\Pi_2}]}{\|\mathbf{O}_{\Pi_1}\|_2 \|\mathbf{O}_{\Pi_2}\|_2} = \frac{1}{\sqrt{N}^{\delta c(\Pi_1, \Pi_2)}} \quad \text{where} \quad \delta c(\Pi_1, \Pi_2) = c(\Pi_1, \Pi_1) + c(\Pi_2, \Pi_2) - 2c(\Pi_1, \Pi_2). \quad (3.62)$$

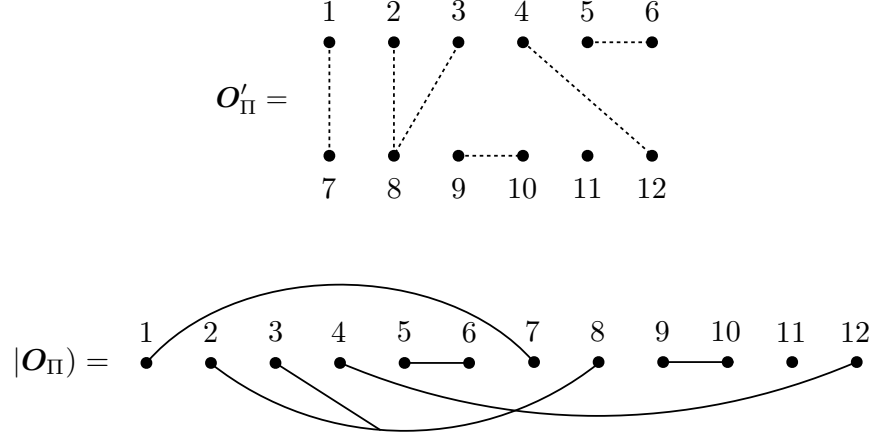


Figure 5: Related notions. The operator O'_Π is modified from O_Π such that distinct blocks have distinct labels (denoted by dotted lines). The vectorization $|O_\Pi)$ treats the bras and kets equally.

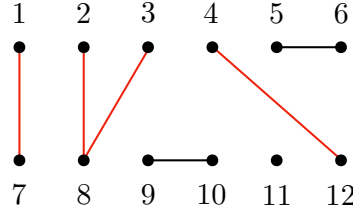


Figure 6: An illustration for propagating blocks, highlighted in red. The lines between (5, 6) and (9, 10) do not propagate since they are completely within the top and the bottom. The number of propagating blocks is 3, i.e., the above diagram is in $\mathbf{J}_3(N)$ but not in $\mathbf{J}_2(N)$.

3. Algebraic structure

The two-sided ideals $\mathbf{J}_m(N)$ for $0 \leq m \leq k$ defined by

$$\mathbf{J}_m(N) := \mathbb{C}\text{-span}\{O_\Pi \mid \Pi \vdash 2k \text{ has at most } m \text{ propagating blocks}\} \quad (3.63)$$

will play a central role in understanding the algebraic structure. A block in Π is propagating if it contains both nodes at the bottom and the top (Figure 6). Indeed, since diagram multiplication, from either the left or the right, cannot increase the number of propagating blocks, we have that

$$\mathbf{P}_k(N)\mathbf{J}_m(N) = \mathbf{J}_m(N)\mathbf{P}_k(N) \subset \mathbf{J}_m(N). \quad (3.64)$$

These ideals are naturally related by

$$\mathbf{J}_0 \subset \mathbf{J}_1 \subset \cdots \mathbf{J}_k = \mathbf{P}_k(N). \quad (3.65)$$

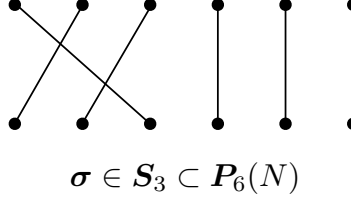


Figure 7: The symmetric group S_m embedded into the partition algebra $P_k(N)$ by acting on the leftmost nodes.

Lemma III.10 (Projection onto subalgebra). *The quotient projector acting on the partition algebra $P_k(N)$ can be written as*

$$\mathcal{Q}_{J_m}[\cdot] = \sum_{|\lambda^*| > m} \Pi_\lambda \cdot \Pi_\lambda, \quad (3.66)$$

where the projectors $\Pi_\lambda \in P_k(N)$ correspond to the irreps of the partition algebra $P_k(N)$ labeled by $\lambda \in \Lambda_{k,N}$.

Proof. For any $\lambda \in \Lambda_{k,N}$, consider the orthogonal basis representatives we construct later in Lemma IV.11, and note that the matrix element is written as some element in $J_{|\lambda^*|}$ modulo $J_{|\lambda^*|-1}$. Therefore, if $|\lambda^*| > m$, $\mathcal{Q}_{J_m}$ acts as the identity, and otherwise, it acts as zero, which coincides with the advertised expression. ■

It will also be crucial to consider the symmetric group algebra as a subalgebra

$$\mathbb{C}S_m \subset P_k(N) \quad \text{for each } 1 \leq m \leq k \quad (3.67)$$

where S_m acts on the leftmost m nodes (Figure 7).

IV. NEW LEMMAS

In this section, we prove the key new lemmas that are foundational for our main results.

A. Asymptotic freeness of random permutations

The power of large- N limits is that a version of “freeness” kicks in for random permutations: different *words* are effectively independent from each other. The concepts of free groups and free words will be particularly helpful.

Definition IV.1 (Free words). *For a countable set of symbols $\{s_i\}$, we denote the set of free words by*

$$\mathcal{W}(\{s_i\}_i) = \{e, s_1, s_2, s_1 s_2, s_2 s_1, s_1^{-2}, \dots\}, \quad (4.1)$$

which are also the elements of the free group generated by $\{s_i\}_i$.

Lemma IV.1 (Effective asymptotic freeness of phased random permutations). *Consider the free words generated by a set of m independent uniformly random phased permutations*

$$\mathcal{W}(\{\mathbf{Z}_a\}_{a=1}^m) \quad \text{where} \quad \mathbf{Z}_a \stackrel{i.i.d.}{\sim} \mathbf{Z}. \quad (4.2)$$

Fix integers ℓ, k and fix a set of ℓ distinct words $\mathbf{W}_1, \dots, \mathbf{W}_\ell \in \mathcal{W}$. Consider a corresponding set of ℓ independent permutations

$$\mathbf{Z}_i := \begin{cases} \stackrel{i.i.d.}{\sim} \mathbf{Z} & \text{if } \mathbf{W}_i \neq \mathbf{I} \\ \mathbf{I} & \text{if } \mathbf{W}_i = \mathbf{I}. \end{cases} \quad (4.3)$$

Then, for each $\mathbf{j} \in [\ell]^{2k}$, in the large- N limit,

$$\lim_{N \rightarrow \infty} \left\| \mathcal{N}_{2k, \mathbf{Z}} \circ \left(\mathcal{N}_{\mathbf{j}, \{\mathbf{W}_i\}} - \mathcal{N}_{\mathbf{j}, \{\mathbf{Z}_i\}} \right) \circ \mathcal{N}_{2k, \mathbf{Z}} \right\|_{\diamond} = 0, \quad (4.4)$$

where

$$\mathcal{N}_{\mathbf{j}, \{\mathbf{W}_i\}} := \mathbb{E} \mathbf{W}_{j_1} \otimes \dots \otimes \mathbf{W}_{j_k} [\cdot] \mathbf{W}_{j_{k+1}}^\dagger \otimes \mathbf{W}_{j_{2k}}^\dagger, \quad \mathbf{j} \in [\ell]^{2k}, \quad (4.5)$$

$$\mathcal{N}_{2k, \mathbf{Z}} := \mathbb{E} \mathbf{Z}^{\otimes k} [\cdot] \mathbf{Z}^{\dagger \otimes k} \quad (4.6)$$

Roughly speaking, we want to show that in the large- N limit, distinct nontrivial words can be replaced by independent random permutations $\{\mathbf{W}_i\} \rightarrow \{\mathbf{Z}_i\}$ (identity remains the identity) in the sense of tensored mixed moments (which may not be completely-positive). Here, we are showing this channel equivalence holds, when the overall channel is first symmetrized by a random phased permutation before and after our words by the channel $\mathcal{N}_{2k, \mathbf{Z}}$. This symmetrization allows us to restrict the test operators to a *proper subalgebra* of the partition algebra with nicer properties. Let

$$B_{2k} := \{\Pi \vdash \{1, \dots, 2k\} | \text{each block has an equal number of sites on top and bottom.}\} \quad (4.7)$$

then, the commutant of phased permutations are exactly the associated diagrams. In particular, every block is propagating.

Lemma IV.2 (Commutant of $\mathbf{Z}^{\otimes k}$).

$$(\mathbf{Z}^{\otimes k})' = \mathbb{C}\text{-Span}\{\mathbf{O}'_\Pi | \Pi \in B_{2k}\} = \mathbb{C}\text{-Span}\{\mathbf{O}_\Pi | \Pi \in B_{2k}\}. \quad (4.8)$$

Proof of Lemma IV.2. Recall that the random phased permutation can be written as $\mathbf{Z} := \mathbf{D}_z \mathbf{S}$. We already have that the commutant of $(\mathbf{S}^{\otimes k})'$ is the partition algebra $\mathbf{P}_k(N)$ with orthogonal basis $\{\mathbf{O}'_\Pi | \Pi \vdash 2k\}$. It follows that $(\mathbf{Z}^{\otimes k})' \subset (\mathbf{S}^{\otimes k})' = \mathbf{P}_k(N)$. Any $\mathbf{O}'_\Pi$ for $\Pi \in B_{2k}$ is contained in the commutant $(\mathbf{Z}^{\otimes k})'$ as the balanced signs from $\mathbf{D}_z$ cancel each other out, and the unsigned permutations $\mathbf{S}$ fixes the diagram

$$\begin{aligned} \mathcal{N}_{2k, \mathbf{Z}}[\mathbf{O}'_\Pi] &= \mathcal{N}_{2k, \mathbf{S}} \circ \mathcal{N}_{2k, \mathbf{D}_z}[\mathbf{O}'_\Pi] \\ &= \mathcal{N}_{2k, \mathbf{S}}[\mathbf{O}'_\Pi] && (\text{Since } \Pi \in B_{2k}) \\ &= \mathbf{O}'_\Pi. && (\text{Since } \mathbf{O}'_\Pi \in \mathbf{P}_k(N)) \end{aligned} \quad (4.9)$$

Conversely, for any other diagram $\Pi \notin B_{2k}$, there exists a non-balanced block, and thus the operator $\mathbf{O}'_{\Pi}$ would vanish under the symmetrization $\mathcal{N}_{2k, \mathbf{Z}}$ due to the unbalanced signs on that block. Next, we show that $\mathbf{O}_{\Pi}$ for $\Pi \in B_{2k}$ also form a basis for the commutant $(\mathbf{Z}^{\otimes k})'$. This is because each diagram $\mathbf{O}_{\Pi}$ for $\Pi \in B_{2k}$ can be written as $\mathbf{O}'_{\Pi}$ for $\Pi \in B_{2k}$

$$\mathbf{O}_{\Pi} = \sum_{\Pi' \geq \Pi} \mathbf{O}'_{\Pi'} \quad (4.10)$$

and that each $\Pi \in B_{2k}$ can only be refinements of $\Pi' \in B_{2k}$

$$\Pi' \geq \Pi, \Pi \in B_{2k} \implies \Pi' \in B_{2k}. \quad (4.11)$$

Therefore,

$$\mathbb{C}\text{-Span}\{\mathbf{O}_{\Pi} | \Pi \in B_{2k}\} \subset \mathbb{C}\text{-Span}\{\mathbf{O}'_{\Pi} | \Pi \in B_{2k}\}. \quad (4.12)$$

Since the two vector spaces have the same dimensions, they must be equal. ■

We can now prove the asymptotic freeness of phased random permutations.

Proof of Lemma IV.1. We begin with controlling the 1-norm for particular “factorized” inputs (see (3.34))

$$\left\| \left(\mathcal{N}_{j, \{\mathbf{W}_i\}} - \mathcal{N}_{j, \{\mathbf{Z}_i\}} \right) [\mathbf{O}_m] \right\|_1 \quad \text{for any fixed } m \in M'_{\Pi}. \quad (4.13)$$

This effectively becomes a classical probability problem since the input is factorized. The case for $\mathbf{Z}$ is simple

$$\mathcal{N}_{j, \{\mathbf{Z}_j\}} [\mathbf{O}_m] \stackrel{N \rightarrow \infty}{\rightrightarrows} \begin{cases} \frac{\mathbf{O}_{\Pi(j, m)}}{\|\mathbf{O}_{\Pi(j, m)}\|_1} & \text{if each block of } m \text{ is acted by “balanced” top-bottom pairs of } \mathbf{Z}_j \text{ and } \mathbf{Z}_j^{\dagger} \\ 0 & \text{else} \end{cases} \quad (4.14)$$

where the convergence is accounted in 1-norm. Basically, the signs need to cancel each other within each block of m for the expression to contribute (i.e., if $\mathbf{Z}_3$ appears in the top row of a block, then $\mathbf{Z}_3^{\dagger}$ must appear in the bottom row.). When they are perfectly balanced and the signs all cancelled, they give a mixture of random $\mathbf{O}_{m'}$ that (up to $1/N$ correction in trace distance) corresponds to a particular partition $\Pi(\mathbf{j}, m) \geq \Pi$ which refines the partition Π of m according to the types of $\mathbf{Z}_j$ present in the same block. In particular, this newly produced partition remains in $\Pi(\mathbf{j}, m) \in B_{2k}$, and is propagating. The case of $\mathbf{W}_j$ is very much the same, up to a vanishing “collision probability” $\sim \frac{1}{N}$ (fixing the length of words and k). To see this, first sample the permutations within $\mathbf{W}_j$ without the signs. With high probability $1 - \mathcal{O}(\frac{1}{N})$ (“without collision”), the signs for each $\mathbf{W}_j$

in different blocks will be independent. That is, after sampling over signs (conditioned on the permutations), we have a situation very similar to $\mathbf{Z}_i$ s:

$$\mathcal{N}_{j,\{\mathbf{W}_i\}}[\mathbf{O}_m] \stackrel{N \rightarrow \infty}{=} \begin{cases} \frac{\mathbf{O}_{\Pi(j,m)}}{\|\mathbf{O}_{\Pi(j,m)}\|_1} & \text{if each block of } m \text{ is acted by “balanced” } \mathbf{W}_j \text{ and its conjugates } \mathbf{W}_j^\dagger \\ 0 & \text{else.} \end{cases} \quad (4.15)$$

When the signs perfectly cancel out, in the large- N limit, distinct words acting on distinct inputs are independent from each other, which again gives $\frac{\mathbf{O}_{\Pi(j,m)}}{\|\mathbf{O}_{\Pi(j,m)}\|_1}$. That is,

$$\lim_{N \rightarrow \infty} \left\| \left(\mathcal{N}_{j,\{\mathbf{W}_i\}} - \mathcal{N}_{j,\{\mathbf{Z}_i\}} \right) [\mathbf{O}_m] \right\|_1 = 0. \quad (4.16)$$

Now, we use the above to prove for general unentangled PSD $\mathbf{Z}$ -symmetrized inputs $\boldsymbol{\rho} = \mathcal{N}_{2k,\mathbf{Z}}[\boldsymbol{\rho}]$. Any such input can be written as a weighted sum over (orthogonal) diagram operators squared

$$\boldsymbol{\rho} = \left(\sum_{\Pi \in B_{2k}} c_\Pi \frac{\mathbf{O}'_\Pi}{\|\mathbf{O}'_\Pi\|_2} \right) \left(\sum_{\Pi \in B_{2k}} c_\Pi \frac{\mathbf{O}'_\Pi}{\|\mathbf{O}'_\Pi\|_2} \right)^\dagger \quad \text{such that} \quad \sum_{\Pi} |c_\Pi|^2 = 1, \quad (4.17)$$

In particular, we observe that each cross terms has bounded 1-norms

$$\left\| \frac{\mathbf{O}'_\Pi}{\|\mathbf{O}'_\Pi\|_2} \frac{\mathbf{O}'_{\Pi'}^\dagger}{\|\mathbf{O}'_{\Pi'}\|_2} \right\|_1 \leq 1 \quad (\text{Cauchy-Schwarz})$$

and that

$$\mathbf{O}'_\Pi \mathbf{O}'_{\Pi'} \propto \mathbf{O}'_{\Pi''} \quad \text{for } \Pi, \Pi', \Pi'' \in B_{2k}. \quad (4.18)$$

This allows us to study the inputs as individual diagrams $\mathbf{O}'_\Pi$ (instead of arbitrary linear combinations). Remarkably, $\mathbf{O}'_\Pi$ (when normalization by its 1-norm) behaves very much like a classical probability distribution in the following sense

$$\frac{\mathbf{O}'_\Pi}{\|\mathbf{O}'_\Pi\|_1} = \frac{1}{M'_\Pi} \sum_{m \in M'_\Pi} \mathbf{O}_m \quad \text{where } \|\mathbf{O}_m\|_1 = 1. \quad (4.19)$$

This is because the “balanced” structure allows us to calculate its 1-norm by permuting the top row $\|\mathbf{O}_\Pi\|_1 = \|\mathbf{O}_\sigma \mathbf{O}_\Pi\|_1 = M'_\Pi$; otherwise the 1-norm normalization may not have a good connection to $\frac{1}{M'_\Pi} \sum_{m \in M'_\Pi} \mathbf{O}_m$. It is crucial here that all blocks are propagating, as a nice feature of these “balanced” diagrams in B_{2k} .

Based on the above, we can then put together the bounds by decomposing inputs into $\mathbf{O}_m$ s (at a

multiplicative cost depending only on k)

$$\left\| \left(\mathcal{N}_{j, \{\mathbf{w}_i\}} - \mathcal{N}_{j, \{\mathbf{z}_i\}} \right) [\boldsymbol{\rho}] \right\|_1 \leq \sum_{\Pi, \Pi'} |c_{\Pi}| |c_{\Pi'}| \left\| \left(\mathcal{N}_{j, \{\mathbf{w}_i\}} - \mathcal{N}_{j, \{\mathbf{z}_i\}} \right) \left[\frac{\mathbf{O}'_{\Pi}}{\|\mathbf{O}'_{\Pi}\|_2} \frac{\mathbf{O}'_{\Pi'}}{\|\mathbf{O}'_{\Pi'}\|_2} \right] \right\|_1 \quad (\text{By (4.17)})$$

$$\leq \sum_{\Pi, \Pi'} |c_{\Pi}| |c_{\Pi'}| \cdot \sup_{\Pi \in B_{2k}} \frac{\left\| \left(\mathcal{N}_{j, \{\mathbf{w}_i\}} - \mathcal{N}_{j, \{\mathbf{z}_i\}} \right) [\mathbf{O}'_{\Pi}] \right\|_1}{\|\mathbf{O}'_{\Pi}\|_1} \quad (\text{By (4.18)})$$

$$\leq \sum_{\Pi, \Pi'} |c_{\Pi}| |c_{\Pi'}| \cdot \sup_{\Pi \in B_{2k}} \sup_{m \in M'_{\Pi}} \left\| \left(\mathcal{N}_{j, \{\mathbf{w}_i\}} - \mathcal{N}_{j, \{\mathbf{z}_i\}} \right) [\mathbf{O}'_m] \right\|_1 \quad (\text{By (4.19)})$$

$$\stackrel{N \rightarrow \infty}{=} 0. \quad (\text{Since } \sum_{\Pi, \Pi'} |c_{\Pi}| |c_{\Pi'}| \text{ is independent of } N \text{ and by (4.16)})$$

Accounting for ancillas (whose dimension is independent of N) incurring a N -independent multiplicative blowup (Lemma IV.14) and inputs with positive and negative parts, we deduce that the diamond norm is also zero in the large N limit. ■

Lemma IV.3 (Norm properties from independence). *Fix an integer ℓ and consider a set of phased permutations $\mathbf{Z}_1, \dots, \mathbf{Z}_{\ell} \stackrel{i.i.d.}{\sim} \mathbf{Z}$ such that all but at most one of them are independent uniformly random (with at most one identity). Then, in the large- N limit, for each $j \in [\ell]^{2k}$,*

(1) *If $\mathbf{Z}_i$ are paired up:*

$$\lim_{N \rightarrow \infty} \|\mathcal{N}_{2k, \mathbf{Z}}^{\dagger} \circ \mathcal{N}_{j, \{\mathbf{Z}_i\}}^{\dagger} [\mathbf{I}] - \mathbf{I}\|_{\infty} = 0. \quad (4.20)$$

(2) *Else:*

$$\lim_{N \rightarrow \infty} \|\mathcal{N}_{2k, \mathbf{Z}}^{\dagger} \circ \mathcal{N}_{j, \{\mathbf{Z}_i\}}^{\dagger} [\mathbf{I}]\|_{\infty} = 0. \quad (4.21)$$

Proof of Lemma IV.3. We begin by evaluating

$$\mathcal{N}_{j, \{\mathbf{Z}_i\}}^{\dagger} [\mathbf{I}] = \mathbb{E} \mathbf{W}_{i_1} \otimes \dots \otimes \mathbf{W}_{i_k} \quad (4.22)$$

where the words are each the product of the left and right $\mathbf{Z}_i$'s. Following the arguments from the proof of Lemma IV.1, we optimize over $\mathbf{O}'_{\Pi}$ for $\Pi \in B_{2k}$ due to the symmetrization $\mathcal{N}_{2k, \mathbf{Z}}^{\dagger}$, and it suffices to control inputs as the “factorized” operators $\mathbf{O}_m$:

$$|\text{Tr}[\mathbb{E} \mathbf{W}_{i_1} \otimes \dots \otimes \mathbf{W}_{i_k} \mathbf{O}_m]| = |\mathbb{E} \langle m_{k+1} | \mathbf{W}_{i_1} | m_1 \rangle \otimes \dots \otimes \langle m_{2k} | \mathbf{W}_{i_k} | m_k \rangle| \quad (4.23)$$

$$= \mathcal{O}\left(\frac{k}{N}\right) \quad \text{if any } \mathbf{W}_{i_j} \text{ are nontrivial.} \quad (4.24)$$

Thus, unless all $\mathbf{Z}_i$ are paired up with their conjugates,

$$\|\mathcal{N}_{2k, \mathbf{Z}}^{\dagger} \circ \mathcal{N}_{j, \{\mathbf{Z}_i\}}^{\dagger} [\mathbf{I}]\|_{\infty} = \sup_{\|\boldsymbol{\rho}\|_1=1} \left| \text{Tr}[\mathcal{N}_{2k, \mathbf{Z}}^{\dagger} [\mathbb{E} \mathbf{W}_{i_1} \otimes \dots \otimes \mathbf{W}_{i_k}] \boldsymbol{\rho}] \right| \quad (4.25)$$

$$\leq f(k) \sup_m |\text{Tr}[\mathbb{E} \mathbf{W}_{i_1} \otimes \dots \otimes \mathbf{W}_{i_k} \mathbf{O}_m]| \quad (\text{By (4.17), (4.18), and (4.19).})$$

$$\stackrel{N \rightarrow \infty}{=} 0, \quad (4.26)$$

as advertised. ■

Corollary IV.1 (A rescaled CPTP map).

$$\lim_{N \rightarrow \infty} \left\| \mathcal{N}_{2k, \mathbf{S}}^\dagger \circ \mathcal{N}_{j, \{\mathbf{Z}_i\}}^\dagger [\mathbf{I}] - \mathbf{I} \cdot \overline{\text{Tr}}[\mathcal{N}_{2k, \mathbf{S}}^\dagger \circ \mathcal{N}_{j, \{\mathbf{Z}_i\}}^\dagger [\mathbf{I}]] \right\|_\infty = 0. \quad (4.27)$$

Corollary IV.2 (Complete positivity in the large- N limit). *Suppose $\sum_i |w_i|^2 = 1$, then the CP map associated with $2k$ -fold tensor product of $\sum_i w_i \mathbf{Z}_i$ is trace-preserving in the large- N limit*

$$\lim_{N \rightarrow \infty} \left\| \mathcal{N}_{2k, \mathbf{S}}^\dagger \circ \mathcal{N}_{2k, \sum_i w_i \mathbf{Z}_i}^\dagger [\mathbf{I}] - \mathbf{I} \right\|_\infty = 0. \quad (4.28)$$

That is, $\mathcal{N}_{2k, \sum_i w_i \mathbf{Z}_i} \circ \mathcal{N}_{2k, \mathbf{S}}$ is a rescaled trace-preserving map. They are also completely positive as the $\mathbf{Z}_i$ need to pair up with each other.

Proof. Expand

$$\begin{aligned} \mathcal{N}_{2k, \sum_i w_i \mathbf{Z}_i}^\dagger [\mathbf{I}] &= \mathbb{E} \left(\left(\sum_i w_i \mathbf{Z}_i \right)^\dagger \left(\sum_i w_i \mathbf{Z}_i \right) \otimes \left(\sum_i w_i \mathbf{Z}_i \right)^\dagger \left(\sum_i w_i \mathbf{Z}_i \right) \cdots \right. \\ &= \mathbf{I}^{\otimes 2k} + (\text{cross terms}) \quad (\mathbf{Z}^\dagger \mathbf{Z} = \mathbf{I}) \\ &\stackrel{N \rightarrow \infty}{\equiv} \mathbf{I}^{\otimes 2k}, \quad (\text{Lemma IV.3}) \end{aligned} \quad (4.29)$$

where the cross terms result from multiplying out the bilinear tensor products. For example, for $k = 2$,

$$\left(\sum_i w_i \mathbf{Z}_i \right)^\dagger \left(\sum_i w_i \mathbf{Z}_i \right) \otimes \left(\sum_i w_i \mathbf{Z}_i \right)^\dagger \left(\sum_i w_i \mathbf{Z}_i \right) = \left(\mathbf{I} + \sum_{i \neq j} w_i w_j \mathbf{Z}_i^\dagger \mathbf{Z}_j \right) \otimes \left(\mathbf{I} + \sum_{i \neq j} w_i w_j \mathbf{Z}_i^\dagger \mathbf{Z}_j \right) \quad (4.30)$$

$$= \mathbf{I} \otimes \mathbf{I} + (\text{cross terms}). \quad (4.31)$$

Note that the number of cross-terms is independent of N . ■

Corollary IV.3 (Combination of permutations and Gaussians). *The above holds with any linear combination $\sum_i w_i \mathbf{Z}_i + \sum_i w'_i \mathbf{G}_i$ provided that $\sum_i |w_i|^2 + \sum_i |w'_i|^2 = 1$.*

Proof. Recall the central limit theorem (for any fixed dimension N)

$$\lim_{m \rightarrow \infty} \sum_{i=1}^m \frac{1}{\sqrt{m}} \mathbf{Z}_i \stackrel{\text{dist.}}{\sim} \mathbf{G}. \quad (4.32)$$

The error in the central limit theorem is bounded in the operator norm by

$$\frac{1}{m} f_1(w_i, k) + \frac{1}{m^2} f_2(w_i, k) + \cdots, \quad (4.33)$$

where the leading contributions are cases when each $\mathbf{Z}_i$ shows up either two or zero times (reproducing the Wick contractions up to $\mathcal{O}(1/m)$ corrections), and the subleading contributions are cases when there are terms $\mathbf{Z}_i$ that show up four times. In particular, the norm bounds of the error terms are functions independent of N (depending on the pattern of the occurrences among the k indices and the w_i coefficients), so the limits $m \rightarrow \infty$ and $N \rightarrow \infty$ commute. ■

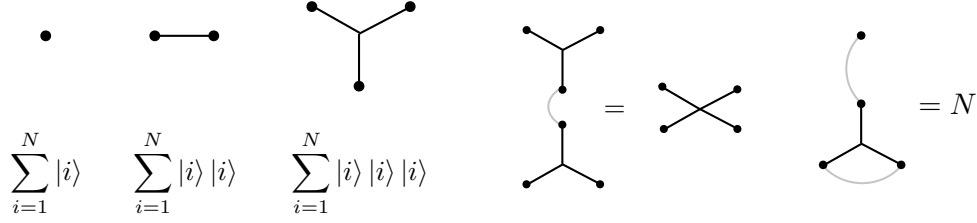


Figure 8: Diagrams for tensor components. Each dot represents a node, and each star-like component is a sum over index i .

B. Large N structure

In order to use the Markov inequality, we need to confirm that the distinguishing probability is indeed a rational polynomial of N . Nicely, expressions involving random permutations, like random unitary, have a pronounced large- N expansion.

Lemma IV.4 (Large- N expression in random phased permutations). *Consider $\mathcal{N}_{j,\{\mathbf{w}_i\}}$ as in Lemma IV.1, and suppose the length of the words is bounded by ℓ . Then, for each pair of partitions $\Pi_1, \Pi_2 \vdash 2k$,*

$$\text{Tr}[\mathbf{O}_{\Pi_2} \mathcal{N}_{j,\{\mathbf{w}_i\}} [\mathbf{O}_{\Pi_1}]] \quad (4.34)$$

is a rational function in N where the poles can be located up to $2k\ell - 1$, each with multiplicity at most $2k\ell$.

The strategy is to expand the expression by canonical pieces of tensors (Figure 8) and argue that any contraction must yield a polynomial of N . This formal dependence on N is the only structural property we need; no further combinatorial calculations are required.

Lemma IV.5 (Breaking $\mathbf{O}_{\Pi}$ into components). *The vectorized operator is factorized into individual tensors*

$$|\mathbf{O}_{\Pi}\rangle = \bigotimes_i |T_b\rangle \quad \text{where} \quad |T_b\rangle = \sum_{i=1}^N |i\rangle^{\otimes t_b} \quad (4.35)$$

and $\sum_b t_b = 2k$.

Lemma IV.6 (The power of N is the number of components). *For any tensor contraction made of components T_i , it evaluates exactly to*

$$N^c \quad \text{where} \quad c = \#(\text{connected components after full contraction}). \quad (4.36)$$

In particular, this implies (3.60) as a special case.

Lemma IV.7 (Expanding diagonal phases as diagrams). *There exists coefficients $\alpha(\Pi)$ independent of N such that*

$$|\mathbb{E} D_z^{\otimes k} \otimes D_z^{\dagger \otimes k}) = \sum_{\Pi \vdash 4k} \alpha(\Pi) |\mathcal{O}_\Pi|. \quad (4.37)$$

Proof.

$$|\mathbb{E} D_z^{\otimes k} \otimes D_z^{\dagger \otimes k}) = \mathbb{E} \left[\left(\sum_{i=1}^N z_i |i\rangle |i\rangle \right)^{\otimes k} \otimes \left(\sum_{i=1}^N z_i^* |i\rangle |i\rangle \right)^{\otimes k} \right] \quad (4.38)$$

$$= \sum_{i=1}^N z_i^k z_i^{*k} (|i\rangle |i\rangle \otimes |i\rangle |i\rangle)^{\otimes k} + \sum_{N \geq i_2 > i_1 \geq 1} (\cdot) + \cdots + \sum_{N \geq i_{2k} > \cdots > i_1 \geq 1} (\cdot) \quad (4.39)$$

$$= \sum_{\Pi \vdash 4k} \alpha'(\Pi) |\mathcal{O}'_\Pi| \quad (4.40)$$

$$= \sum_{\Pi \vdash 4k} \alpha(\Pi) |\mathcal{O}_\Pi|. \quad (\text{Möbius inversion (3.56)})$$

The second line sums over possible patterns of distinct z_i s, and uses that each z_i must pair with its complex conjugate since

$$\mathbb{E}[z_i^b] = \begin{cases} 1 & \text{if integer } b = 0 \\ 0 & \text{else} \end{cases}. \quad (4.41)$$

Thus, the nonvanishing contribution has merely unity coefficient $|z_i|^2 = 1$. Note that the Hilbert space dimension is N^{4k} instead of N^{2k} as the object we consider is a (vectorized) superoperator. ■

Proof of Lemma IV.4. Decompose the phased permutations by the diagonal phases and the permutation $\mathbf{Z} = \mathbf{D}_z \mathbf{S}$. Then, the superoperator $\mathcal{N}_{j, \{\mathbf{w}_i\}}$ can be decomposed into sum and products of

$$\mathbb{E} \mathbf{S}^a \otimes \mathbf{S}^a, \quad \mathbb{E} \mathbf{D}_z^a \otimes \mathbf{D}_z^{*a} \quad \text{for } 1 \leq a \leq 2k\ell \quad (4.42)$$

which can be written as diagrams $\mathcal{O}_\Pi$ and expanded as tensor components (Lemma IV.5). After contraction, the poles may accumulate through the occurrences of $\mathbb{E} \mathbf{S}^a \otimes \mathbf{S}^a$ for different possible independent permutations $\mathbf{S}_1, \mathbf{S}_2, \dots$. These expectations produce poles via (3.58) such that after taking account of all of them, the poles can be located up to $2k\ell - 1$, each with multiplicity at most $2k\ell$.¹² ■

C. Basis for the partition algebra

The crux of our large- N interpolation argument is to extend the distinguishing probability for N to other values of $N' \neq N$. In particular, we need to “smoothly” extend the test operators $\rho, \mathcal{O}$ to

¹² This is likely a loose bound but is qualitatively sufficient.

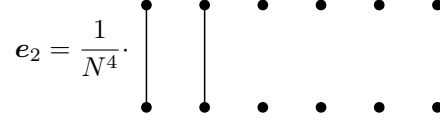


Figure 9: The diagram for e_m for $m = 2$. It has identities on the leftmost nodes, and the rest are isolated nodes. The normalization is such that $e_m^2 = e_m$.

different other dimensions. Fortunately, we do know that the partition algebra $P_k(N)$ stabilizes for large enough $N \geq 2k$ and the individual factors $\{P_\lambda\}_\lambda$ depend *only* on k and are *independent* of N if $N \geq 2k$ (Theorem III.2). Naturally, it is tempting to keep the test operator the same in this invariant decomposition into factors.

However, our polynomial interpolation argument requires that the block-diagonalizing unitary transformation “depends nicely” on N in the following sense.

Question IV.0.1 (Writing irreps in the computation basis). *For each k , assume $N \geq 2k$. Does there exist a choice of orthonormal basis $|v_i^\lambda\rangle$ for each factor P_λ of the partition algebra such that the following holds: the matrix elements $E_{ij}^\lambda = |v_i^\lambda\rangle\langle v_j^\lambda| \otimes \mathbf{I}_{S_\lambda}$ satisfy that*

$$\text{Tr}[E_{ij}^\lambda \mathbf{O}_\Pi] \text{ is a degree } \mathcal{O}(k) \text{ rational polynomial of } N \text{ for each } \lambda, i, j, \Pi? \quad (4.43)$$

We do not need *any* knowledge of the rational polynomial except for its *degree*, and the polynomial can very well depend on λ, i, j, Π . To answer the above question, we need to dive into the partition algebra and construct an orthogonal basis. Although our ensemble actually uses a stronger symmetry $\mathbf{Z}$ (random phased permutations) instead of $\mathbf{S}(N)$, it is sufficient to consider the weaker symmetry.

1. An abstract construction of irreps

For each irrep labeled by $\lambda \in \Lambda_{k,N}$, [HJ20] constructed the corresponding irreducible module by taking an abstract quotient

$$\mathcal{V}_\lambda := \frac{P_k(N)e_\lambda}{J_{m-1}(N)} \text{ as a } \mathbb{C}\text{-vector space for } m := |\lambda^*| \quad (4.44)$$

$$\text{where } \mathbf{v}_1(\mathbf{v}_2 + \mathbf{J}_{m-1}) \equiv \mathbf{v}_1\mathbf{v}_2 + \mathbf{J}_{m-1} \text{ and} \quad (4.45)$$

$$e_\lambda := p_{\lambda^*} e_m \text{ for } e_m := \frac{1}{N^{k-m}} \mathbf{I}^m \otimes (\text{isolated nodes}) \quad (4.46)$$

such that $e_m^2 = e_m$. The diagrammatic form of e_m is depicted in Figure 9.

Theorem IV.1 ([HJ20]). *The quotient $\mathcal{V}_\lambda$ is isomorphic to the irreducible module labeled by $\lambda \in \Lambda_{k,N}$.*

Since we are interested in finding an orthonormal basis, we first need an *inner product* on this irreducible module $\mathcal{V}_\lambda$ (which was not discussed in [HJ20]). There is a very natural approach:

the abstract quotient by the two-sided ideal $\mathbf{J}_{m-1}$ can be realized as the projector $\mathcal{Q}_{\mathbf{J}_{m-1}}$ onto a subalgebra $\mathcal{Q}_{\mathbf{J}_{m-1}}[\mathbf{P}_k(N)] \subset \mathbf{P}_k(N)$. (See [Theorem III.1](#).) Therefore, the natural choice for the inner product is then to simply induce from the Hilbert-Schmidt inner product of the partition algebra by

$$\langle v_1^\lambda, v_2^\lambda \rangle := \frac{1}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \text{Tr}[\mathcal{Q}_J[v_1^\lambda]^\dagger \mathcal{Q}_J[v_2^\lambda]] \quad \text{for each } v_1^\lambda, v_2^\lambda \in \mathbf{P}_k(N)e_\lambda. \quad (4.47)$$

We can verify that this inner product is *consistent* (dropping scripts λ and $m-1$ for the moment)

$$\langle v_1 + \mathbf{J}_1, v_2 + \mathbf{J}_2 \rangle_\lambda = \frac{1}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \text{Tr}[\mathcal{Q}_J[v_1 + \mathbf{J}_1] \mathcal{Q}_J[v_2 + \mathbf{J}_2]] \quad (4.48)$$

$$= \frac{1}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \text{Tr}[\mathcal{Q}_J[v_1]^\dagger \mathcal{Q}_J[v_2]] \quad (4.49)$$

$$= \langle v_1, v_2 \rangle_\lambda \quad \text{for each } v_1, v_2 \in \mathbf{P}_k(N)e_\lambda \quad \text{and} \quad \mathbf{J}_1, \mathbf{J}_2 \in \mathbf{J} \quad (4.50)$$

and *compatible* with the adjoint from the Hilbert space on which $\mathbf{P}_k(N)$ is represented

$$\langle v_1, \mathbf{O}v_2 \rangle_\lambda = \frac{1}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \text{Tr}[\mathcal{Q}_J[v_1]^\dagger \mathcal{Q}_J[\mathbf{O}v_2]] \quad (4.51)$$

$$= \frac{1}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \text{Tr}[\mathcal{Q}_J[v_1]^\dagger \mathcal{Q}_J[\mathbf{O}] \mathcal{Q}_J[v_2]] \quad (4.52)$$

$$= \frac{1}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \text{Tr}[(\mathcal{Q}_J[\mathbf{O}]^\dagger \mathcal{Q}_J[v_1])^\dagger \mathcal{Q}_J[v_2]] \quad (4.53)$$

$$= \frac{1}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \text{Tr}[(\mathcal{Q}_J[\mathbf{O}^\dagger v_1])^\dagger \mathcal{Q}_J[v_2]] = \langle \mathbf{O}^\dagger v_1, v_2 \rangle_\lambda. \quad (4.54)$$

The second, third, and fourth lines use that $\mathcal{Q}_J[\cdot]$ is a $\dagger$ -homomorphism. (Recall [Definition III.3](#) and [Theorem III.1](#).)

In a nutshell, there is a very simple intuition for this abstract vector space: it is simply one *column* in the corresponding factor of the partition algebra

$$\frac{\mathbf{P}_k(N)e_\lambda}{\mathbf{J}_{m-1}(N)} \sim \mathbb{C}\text{-Span}\{|v_i^\lambda\rangle \langle 0|\} \in \mathbf{P}_\lambda. \quad (4.55)$$

2. Explicit basis

For our later usage, we will also need to extract the explicit structure of the basis from the abstract construction. We will be building on the basis provided by [\[HJ20\]](#). The construction requires some further concepts from the algebraic structure of the partition algebra (see [Figure 10](#)).

Definition IV.2 (*m*-factor). *For any $0 \leq m \leq k$, the set of m -factors F_m are diagrams where the bottom leftmost m nodes propagate and the rightmost $k - m$ nodes are isolated. In particular, the set of noncrossing m -factors NF_m are those m -factors whose propagating edges do not cross when the diagram is drawn under the rule that propagating edges connect to the rightmost vertex of the block in the top row.*

Note that by permuting the bottom row (i.e., concatenating a permutation below), any m -factor can be made noncrossing.

Lemma IV.8 (A basis for $\mathcal{V}_\lambda$ [HJ20]). *Let $m = |\lambda^*|$. Then,*

$$\mathcal{V}_\lambda = \text{Span}\{\mathbf{O}_\omega \sigma_t \mathbf{p}_{\lambda^*} | \omega \in NF_m, t \in \text{SYT}(\lambda^*)\} \pmod{\mathbf{J}_{m-1}}. \quad (4.56)$$

We now construct an explicit *orthonormal* basis for the vector space $\mathcal{V}_\lambda$ for each irrep $\lambda \in \Lambda_{k,N}$. This might be of independent interest in the representation theory of partition algebras.

Theorem IV.2 (Orthonormal basis for $\mathcal{V}_\lambda$). *For each $\lambda \in \Lambda_{k,N}$, the set of vectors*

$$\{v_i^\lambda\} = \left\{ \frac{1}{n(\omega, t)} \hat{\mathbf{O}}_\omega \mathbf{u}_t \mathbf{p}_{\lambda^*} | \omega \in NF_m, t \in \text{SYT}(\lambda^*) \right\} \pmod{\mathbf{J}_{m-1}} \quad (4.57)$$

forms an orthonormal basis for the irreducible representation $\mathcal{V}_\lambda$.

Note that as compared to Lemma IV.8, σ_t has been replaced by the $\mathbf{u}_t$ introduced in Lemma III.5 and $\mathbf{O}_\omega$ was replaced by $\hat{\mathbf{O}}_\omega$. Roughly speaking, for a noncrossing m -factor ω ,

$$\hat{\mathbf{O}}_\omega := (\text{sum over distinct indices for the upper nodes } \{1, \dots, k\} \text{ and lower nodes } \{1, \dots, m\}). \quad (4.58)$$

The precise definition can be found in the proof of Lemma IV.9. These operators are analogs of the $\mathbf{O}'_\omega$ but focus only on a subset of vertices. (That is, when running the inclusion-exclusion principle, we keep the lower right $k - m$ nodes untouched.) This will be crucial for ensuring that the basis vectors are orthogonal and the subspace projector remains a *rational function* of $1/N$.¹³ Later, we will choose the normalization constant $n(\omega)$ to ensure the vectors are exactly unit length (Lemma IV.11). The proof that these operators form an orthonormal basis will take place in two steps.

- The new vectors span the same space (Lemma IV.9 and Lemma IV.10).
- The new vectors are orthogonal (section IV C 3).

Lemma IV.9 (Alternate representatives). *For each integer $1 \leq m \leq k$,*

$$\text{Span}\{\hat{\mathbf{O}}_\omega | \omega \in F_m\} \equiv \text{Span}\{\mathbf{O}_\omega | \omega \in F_m\} \pmod{\mathbf{J}_{m-1}}. \quad (4.59)$$

Proof of Lemma IV.9. To study m -factors, it suffices to consider diagrams where the bottom right $k - m$ nodes are isolated. To that end, let $T_1^{k-m} = (\sum_{i=1}^N \langle i |) \otimes^{k-m}$ and introduce the shorthand

$$\mathbf{O}_{\Gamma \otimes T_1^{k-m}} =: \mathbf{O}_\Gamma \quad \text{where} \quad \Gamma \vdash [k+m] = \{1, \dots, k, k+1, \dots, k+m\}. \quad (4.60)$$

¹³ This point is surprisingly delicate because the subspace dimension is large (superexponential in k), and tiny overlaps can accumulate and wiggle the span.

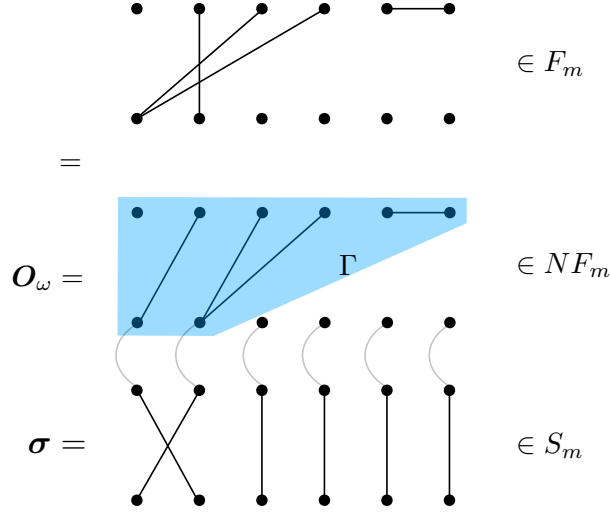


Figure 10: Illustration for m -factors (F_m) for $m = 2$, which can also be written as a noncrossing m -factor ($\omega \in NF_m$) multiplied by a permutation $\sigma \in S_m$ at the bottom (which uniquely makes it noncrossing).

The induced partial order $\geq$ on $\Gamma \vdash [k+m]$ (recall [section III D 1](#)) allows us to run a tailored Möbius inversion argument so that (as in [\(3.55\)](#), [\(3.56\)](#))

$$\mathbf{O}_\Gamma = \sum_{\substack{\Gamma' \geq \Gamma, \\ \Gamma' \vdash [k+m]}} \mathbf{O}'_{\Gamma'} =: \sum_{\Gamma' \vdash [k+m]} K_{\Gamma\Gamma'} \mathbf{O}'_{\Gamma'} \quad (4.61)$$

$$\mathbf{O}'_\Gamma = \sum_{\Gamma' \vdash [k+m]} K_{\Gamma\Gamma'}^{-1} \mathbf{O}_{\Gamma'} \quad (4.62)$$

where $\mathbf{O}'_{\Gamma'}$ are orthogonal (recall [\(3.53\)](#): distinct blocks in Γ have distinct indices) and are related to the original diagrams $\mathbf{O}_\Gamma$ by upper triangular matrices $K_{\Gamma\Gamma'}$ and $K_{\Gamma\Gamma'}^{-1}$ (total order extended from the partial order $\geq$ by [Lemma III.7](#)). Note that the bottom right $k-m$ nodes are untouched throughout the proof. Consider [\(4.62\)](#) for each m -factor $\omega \in F_m$,

$$\mathbf{O}'_\omega = \sum_{\Gamma' \vdash [k+m]} K_{\omega\Gamma'}^{-1} \mathbf{O}_{\Gamma'} \quad (4.63)$$

$$\begin{aligned} &= \sum_{\omega' \in F_m} K_{\omega\omega'}^{-1} \mathbf{O}_{\omega'} + \sum_{\Gamma' \in \mathbf{J}_{m-1}} K_{\omega\Gamma'}^{-1} \mathbf{O}_{\Gamma'} \quad (\text{Any partition } \Gamma \text{ is either in } F_m \text{ or } \mathbf{J}_{m-1}) \\ &\equiv \sum_{\omega' \in F_m} K_{\omega\omega'}^{-1} \mathbf{O}_{\omega'} \pmod{\mathbf{J}_{m-1}}, \end{aligned} \quad (4.64)$$

where we again use $\Gamma' \in \mathbf{J}_{m-1}$ as a shorthand for $\Gamma' \otimes T_1^{k-m} \in \mathbf{J}_{m-1}$. The second line is the observation that any partition $\Gamma \vdash [k+m]$ corresponds to a diagram with at most m propagating blocks (since there are only m nodes at the bottom), and thus any diagram with (1) exactly m -propagating blocks (i.e., an m -factor) is in F_m and those with (2) at most $m-1$ propagating block is by definition in $\mathbf{J}_{m-1}$. Now, since the restriction of an upper triangular matrix remains

upper triangular (or, partial order remains consistent on subsets: [Lemma III.8](#)), we have that

$$K_{\Gamma\Gamma'}^{-1} \quad \text{for } \Gamma, \Gamma' \vdash [k+m] \quad \text{is upper triangular implies the same for} \quad (4.65)$$

$$K_{\omega\omega'}^{-1} \quad \text{for } \omega, \omega' \in F_m. \quad (4.66)$$

Further, since the diagonals are nonzero (just ones), there exists a matrix $K^{(F_m)}$ defined only on $F_m \rightarrow F_m$ that inverts $K_{\omega\omega'}^{-1}$ on $F_m \rightarrow F_m$:

$$\sum_{\omega' \in F_m} K_{\omega\omega'}^{(F_m)} K_{\omega'\omega''}^{-1} = \delta_{\omega\omega''} \quad \text{for each } \omega, \omega'' \in F_m. \quad (4.67)$$

Thus,

$$\sum_{\omega' \in F_m} K_{\omega\omega'}^{(F_m)} \mathbf{O}'_{\omega'} \equiv \mathbf{O}_\omega \pmod{\mathbf{J}_{m-1}}, \quad (4.68)$$

stating that the two spans are equal up to elements in $\mathbf{J}_{m-1}$. ■

Lemma IV.10 (Same span for irreps). *For each $\lambda \in \Lambda_{k,N}$, let $m = |\lambda^*|$, then*

$$\text{Span}\{\mathbf{O}_\omega \sigma_t \mathbf{p}_{\lambda^*} | \omega \in NF_m, t \in SYT(\lambda^*)\} \equiv \text{Span}\{\hat{\mathbf{O}}_\omega \mathbf{u}_t \mathbf{p}_{\lambda^*} | \omega \in NF_m, t \in SYT(\lambda^*)\} \pmod{\mathbf{J}_{m-1}} \quad (4.69)$$

Proof of Lemma IV.10. Starting with [Lemma IV.9](#),

$$\text{Span}\{\hat{\mathbf{O}}_\omega | \omega \in F_m\} \equiv \text{Span}\{\mathbf{O}_\omega | \omega \in F_m\} \pmod{\mathbf{J}_{m-1}}, \quad (4.70)$$

we can pull out permutations to make the partitions noncrossing, giving

$$\text{Span}\{\hat{\mathbf{O}}_\omega \sigma | \omega \in NF_m, \sigma \in S_m\} \equiv \text{Span}\{\mathbf{O}_\omega \sigma | \omega \in NF_m, \sigma \in S_m\} \pmod{\mathbf{J}_{m-1}}, \quad (4.71)$$

noting that we drop the distinctness constraint on the permutation as the distinctness of $\hat{\mathbf{O}}_\omega$ suffices to ensure $\hat{\mathbf{O}}_\omega \sigma = \hat{\mathbf{O}}_{\omega'}$ for some $\omega \in F_m$. Then, we can right multiply the set by

$$\text{Span}\{\mathbf{O}_\omega \sigma \mathbf{p}_{\lambda^*} | \omega \in NF_m, \sigma \in S_m\} \equiv \text{Span}\{\hat{\mathbf{O}}_\omega \sigma \mathbf{p}_{\lambda^*} | \omega \in NF_m, \sigma \in S_m\} \pmod{\mathbf{J}_{m-1}}, \quad (4.72)$$

noting that we relax the quotient $(\text{mod } \mathbf{J}_{m-1} \mathbf{p}_{\lambda^*})$ to $(\text{mod } \mathbf{J}_{m-1})$ by the ideal property $\mathbf{J}_{m-1} \mathbf{p}_{\lambda^*} \subset \mathbf{J}_{m-1}$.

By [Lemma III.4](#), however, $\mathbb{C}\{\sigma \mathbf{p}_{\lambda^*}\}_{\sigma \in S_m} = \mathbb{C}\{\sigma_t \mathbf{p}_{\lambda^*}\}_{t \in SYT(\lambda^*)}$, which allows us to restrict the set of permutations by

$$\text{Span}\{\mathbf{O}_\omega \sigma_t \mathbf{p}_{\lambda^*} | \omega \in NF_m, t \in SYT(\lambda^*)\} \equiv \text{Span}\{\hat{\mathbf{O}}_\omega \sigma_t \mathbf{p}_{\lambda^*} | \omega \in NF_m, t \in SYT(\lambda^*)\} \pmod{\mathbf{J}_{m-1}}. \quad (4.73)$$

Finally, we can use [Lemma III.5](#) and, in particular, that $\text{Span}\{\mathbf{u}_t \mathbf{p}_{\lambda^*}\} = \text{Span}\{\sigma_t \mathbf{p}_{\lambda^*}\}$, to reach

$$\text{Span}\{\mathbf{O}_\omega \sigma_t \mathbf{p}_{\lambda^*} | \omega \in NF_m, t \in SYT(\lambda^*)\} \equiv \text{Span}\{\hat{\mathbf{O}}_\omega \mathbf{u}_t \mathbf{p}_{\lambda^*} | \omega \in NF_m, t \in SYT(\lambda^*)\} \pmod{\mathbf{J}_{m-1}}, \quad (4.74)$$

as advertised. ■

3. Orthogonality and matrix elements

The very nice properties of the basis vectors we chose in [Theorem IV.2](#) are that they are orthogonal and immediately give the matrix elements of the factors of the partition algebra.

Lemma IV.11 (Orthonormal basis for each irrep of $\mathbf{P}_k(N)$). *For each $\lambda \in \Lambda_{k,N}$, set the normalization such that*

$$n(\omega, t) := \sqrt{c(\omega)} \quad \text{for each } \omega \in NF_m \quad \text{and} \quad t \in SYT(\lambda^*). \quad (4.75)$$

where

$$c(\omega) := \frac{N^{k-m}(N-m)!}{(N-m-d(\omega^\dagger, \omega))!} = N^{k-m} \cdot (N-m) \cdot (N-m-1) \cdots \leq N^{k-m+d(\omega^\dagger, \omega)}. \quad (4.76)$$

Then, $|v_j^\lambda\rangle$ forms an orthonormal basis for the irrep labeled by $\lambda \in \Lambda_{k,N}$, and

$$\mathcal{Q}_J[v_i^\dagger v_j] \simeq |v_i^\lambda\rangle \langle v_j^\lambda| \otimes \mathbf{I}_{S_\lambda} \quad \text{for each } i, j \quad (4.77)$$

gives the matrix elements for the irrep labeled by $\lambda \in \Lambda_{k,N}$.

The proof of orthogonality relies on the following multiplicative properties of $\hat{\mathbf{O}}_\omega$. This is precisely why we define our basis using $\hat{\mathbf{O}}_\omega$ instead of $\mathbf{O}_\omega$; despite having a simpler definition, the latter has a more involved algebraic structure.

Lemma IV.12 (Multiplicative properties of $\hat{\mathbf{O}}_\omega$). *For all $\omega, \omega' \in NF_m$,*

$$\hat{\mathbf{O}}_{\omega'}^\dagger \hat{\mathbf{O}}_\omega \equiv c(\omega) \delta_{\omega'\omega} \cdot \mathbf{e}_m \quad (\text{mod } \mathbf{J}_{m-1}). \quad (4.78)$$

The above will be very helpful in the calculation as it imposes $\omega = \omega'$.

Proof of [Lemma IV.12](#). Step 1: Distinctness implies the set of upper blocks matches.

Recall that the $\hat{\mathbf{O}}_\omega$ were constructed specifically so that the outgoing wires of $\hat{\mathbf{O}}_\omega$ were distinct. As illustrated in [Figure 11](#), this implies that the upper block of ω' must be exactly the same partition as that of ω . Otherwise, two different blocks will be contracted to give zero.

Step 2: Fixing the propagating blocks. To establish that the product is actually proportional to $\delta_{\omega'\omega}$, we need to use the properties of $\mathbf{J}_{m-1}$ and the fact that $\omega \in NF_m$ is noncrossing. Since the quotient $\mathbf{J}_{m-1}$ kills any diagram with fewer than m propagating blocks, the product $\hat{\mathbf{O}}_{\omega'}^\dagger \hat{\mathbf{O}}_\omega$ vanishes unless the number of blocks remains m , which requires that the set of upper propagating blocks of ω' exactly matches the set of upper propagating blocks of ω . Furthermore, since ω' is a noncrossing m -factor, this also uniquely fixes how the propagating blocks of ω' are wired to the lower leftmost m nodes (according to the rightmost element of each block).

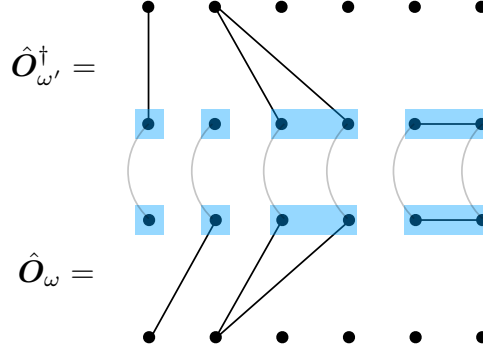


Figure 11: Multiplying two noncrossing m -factors $\hat{O}_{\omega'}^\dagger \cdot \hat{O}_\omega$. Due to the distinctness properties (4.58), the blocks in blue must match exactly, which holds in the above. However, since one propagating block of $\hat{O}_\omega$ is contracted with a nonpropagating block of $\hat{O}_{\omega'}$, the number of propagating blocks decreases. Thus, the above is an element of $\mathbf{J}_1$, and vanishes due to taking quotient.

Step 3: Calculating the constant. Having established orthogonality, we can obtain the final form

$$\hat{O}_\omega^\dagger \hat{O}_\omega \propto \sum_{\text{distinct } i_1, \dots, i_m=1}^N |i_1\rangle \langle i_1| \otimes |i_2\rangle \langle i_2| \cdots |i_m\rangle \langle i_m| \otimes (2k - 2m \text{ isolated nodes}) \quad (4.79)$$

$$\propto \mathbf{I}_m \otimes (2k - 2m \text{ isolated nodes}) \pmod{\mathbf{J}_{m-1}} \quad (4.80)$$

$$\propto \mathbf{e}_m \pmod{\mathbf{J}_{m-1}} \quad (4.81)$$

The second line “completes” the identity by adding suitable elements in $\mathbf{J}_{m-1}$. Lastly, the constant is determined by contracting the upper *nonpropagating* blocks, which gives the falling factorial in $c(\omega)$, and the normalization factor (N^{k-m}) of $\mathbf{e}_m$. ■

Proof of Lemma IV.11. We begin by verifying the algebra relation for matrix elements:

$$\mathbf{E}_{ij} \mathbf{E}_{k\ell} = \delta_{jk} \mathbf{E}_{i\ell}, \quad \mathbf{E}_{ij}^\dagger = \mathbf{E}_{ji}. \quad (4.82)$$

Indeed, we have that

$$\begin{aligned}
\mathcal{Q}_J[v_i v_j^\dagger] \mathcal{Q}_J[v_k v_\ell^\dagger] &= \mathcal{Q}_J[v_i v_j^\dagger v_k v_\ell^\dagger] && \text{(Since } \mathcal{Q}_J \text{ is a } \dagger\text{-homomorphism)} \\
&= \frac{1}{n(\omega_1, t_1) n(\omega_2, t_2) n(\omega_3, t_3) n(\omega_4, t_4)} \mathcal{Q}_J[\hat{O}_{\omega_1} u_{t_1} p_{\lambda^*} p_{\lambda^*}^\dagger u_{t_2}^\dagger \hat{O}_{\omega_2}^\dagger \hat{O}_{\omega_3} u_{t_3} p_{\lambda^*} p_{\lambda^*}^\dagger u_{t_4}^\dagger \hat{O}_{\omega_4}^\dagger] \\
&&& (i, j, k, \ell \rightarrow \omega_1, t_1, \dots, \omega_4, t_4) \\
&= \frac{c(\omega_2)}{n(\omega_1, t_1) n(\omega_2, t_2) n(\omega_3, t_3) n(\omega_4, t_4)} \mathcal{Q}_J[\hat{O}_{\omega_1} e_m u_{t_1} p_{\lambda^*} p_{\lambda^*}^\dagger u_{t_2}^\dagger u_{t_3} p_{\lambda^*} p_{\lambda^*}^\dagger u_{t_4}^\dagger \hat{O}_{\omega_4}^\dagger] \\
&&& \text{(By Lemma IV.12)} \\
&= \frac{c(\omega_2)}{n(\omega_1, t_1) n(\omega_2, t_2) n(\omega_3, t_3) n(\omega_4, t_4)} \mathcal{Q}_J[\hat{O}_{\omega_1} e_m u_{t_1} p_{\lambda^*} p_{\lambda^*}^\dagger u_{t_4}^\dagger \hat{O}_{\omega_4}^\dagger] \\
&&& \text{(By Lemma III.5)} \\
&= \frac{c(\omega_2)}{n(\omega_1, t_1) n(\omega_2, t_2) n(\omega_3, t_3) n(\omega_4, t_4)} \mathcal{Q}_J[\hat{O}_{\omega_1} u_{t_1} p_{\lambda^*} p_{\lambda^*}^\dagger u_{t_4}^\dagger \hat{O}_{\omega_4}^\dagger] \\
&&& \text{(By definition of } e_m) \\
&= \delta_{jk} \mathcal{Q}_J[v_i v_\ell^\dagger], && (4.83)
\end{aligned}$$

and that

$$\left(\mathcal{Q}_J[v_i v_j^\dagger] \right)^\dagger = \mathcal{Q}_J[v_j v_i^\dagger], \quad \text{(Since } \mathcal{Q}_J \text{ is an } \dagger\text{-homomorphism)}$$

as required. ■

4. Projector onto irreducible representations as a sum over diagrams

We have constructed an explicit orthonormal basis but the abstract quotient projector $\mathcal{Q}_{J_m}$ that is required to ensure orthogonality remains somewhat mysterious.

$$\mathcal{Q}_{J_{m-1}}[\cdot] = \sum_{|\lambda^*| \geq m} \Pi_{\lambda} \cdot \Pi_{\lambda}. \quad (4.84)$$

This section further gives a *low-degree* expansion of Π_{λ} in terms of the diagram operator $\mathbf{O}_{\Pi}$.

Lemma IV.13 (A recursive formula for the projector onto irreducible representations). *For each $\lambda \in \Lambda_{k,N}$,*

$$\Pi_{\lambda} = \sum_i \left(v_i^{\lambda} v_i^{\lambda^\dagger} - \sum_{|\mu^*| \leq |\lambda^*| - 1} \Pi_{\mu} v_i^{\lambda} v_i^{\lambda^\dagger} \right). \quad (4.85)$$

Thus, solving the recursion yields

$$\Pi_{\lambda} = \sum_{\Pi} c(\Pi, \lambda) \mathbf{O}_{\Pi} \quad (4.86)$$

where $c(\Pi, \lambda)$ is a rational function of N with poles at integers $0, \dots, k$, each with multiplicity at most k .

Proof of Lemma IV.13.

$$\begin{aligned}
\Pi_\lambda &= \sum_i \mathcal{Q}_{J_{m-1}}[v_i^\lambda v_i^{\lambda^\dagger}] && \text{(Resolution of identity)} \\
&= \sum_i \left(v_i^\lambda v_i^{\lambda^\dagger} - \sum_{|\mu^*| \leq |\lambda^*| - 1} \Pi_\mu v_i^\lambda v_i^{\lambda^\dagger} \Pi_\mu \right) && \text{(Rewriting (4.84))} \\
&= \sum_i \left(v_i^\lambda v_i^{\lambda^\dagger} - \sum_{|\mu^*| \leq |\lambda^*| - 1} \Pi_\mu v_i^\lambda v_i^{\lambda^\dagger} \right). && \text{(Since } v_i^\lambda v_i^{\lambda^\dagger} \in P_k(N))
\end{aligned}$$

The third line drops one of the projectors since Π_μ are projectors for a factor. Solving the recursion implies the projector can be expressed as a formal noncommutative polynomial of the basis representatives

$$\Pi_\lambda = \text{poly} \left(\left\{ \sum_i v_i^\lambda v_i^{\lambda^\dagger} \right\}_{\lambda \in \Lambda_{k,N}} \right) \quad \text{of degree } |\lambda|. \quad (4.87)$$

Further rewriting the basis representatives

$$v_i^\lambda v_i^{\lambda^\dagger} = \frac{1}{n(\omega)^2} \hat{O}_\omega u_t p_{\lambda^*} p_{\lambda^*}^\dagger u_t^\dagger \hat{O}_\omega^\dagger \quad (4.88)$$

$$= \sum_{\Pi} c(\Pi, \lambda) O_\Pi \quad (4.89)$$

where each $c(\Pi, \lambda)$ is a rational function of N with pole at integers $0, \dots, k$ with multiplicity at most 1 by Lemma IV.11. Thus,

$$\Pi_\lambda = \sum_{\Pi} c(\Pi, \lambda) O_\Pi \quad (4.90)$$

with poles at integers $0, \dots, k$ each with multiplicity at most k . We will not ever need to worry about the numerator degree, as it will already be controlled by the denominator degree for the ultimate quantity of interest (bounded by $\mathcal{O}(N^0)$). ■

D. Extending test operators

However, we are still faced with the challenge that the distinguishing probability also depends on the quantum algorithm, which amounts to all possible input states and observables in the parallel query model. To make the distinguishing probability a polynomial, we must specify how we *extend* the quantum algorithm to other dimensions N' . In most circumstances, that would be very unnatural but here, the fact that the partition algebra is *independent* of N for $N \geq 2k$ allows us to define a family of “equivalent” quantum algorithms across larger and smaller dimensions $N' \neq N$. Doing so amounts to choosing the appropriate input state and observable.

First, we need to reduce the size of the ancilla to control the diamond distances.

Lemma IV.14 (Variational expression for diamond distance for (left and right) permutation invariant channels). *For any two channels $\mathcal{N}_1, \mathcal{N}_2$,*

$$\left\| \mathcal{N}_{2k, \mathcal{S}} \circ (\mathcal{N}_1 - \mathcal{N}_2) \circ \mathcal{N}_{2k, \mathcal{S}} \right\|_{\diamond} = \sup_{\rho, \mathbf{O}} \text{Tr}[\mathbf{O}(\mathcal{N}_1 - \mathcal{N}_2)[\rho]] \quad (4.91)$$

where the normalized state ρ and operator $\mathbf{O}$ are supported on bipartite Hilbert space with dimension $N^k \times \max_{\lambda \in \Lambda_{k,N}} d_{\lambda}$, where d_{λ} are the dimensions of the factors in the partition algebra.

In particular, assuming the local dimension is large, specifically $2k \leq N$, the irrep dimension d_{λ} will only depend on k and is independent of N .

Proof. For any input ρ that may be entangled with an N^k -dimensional ancilla, the permutation average enforces the structure

$$\mathcal{N}_{2k, \mathcal{S}}[\rho] = \bigoplus_{\lambda} \rho'_{\lambda} \otimes \tau_{\lambda}. \quad (4.92)$$

where ρ'_{λ} acts on the factors of the partition algebra and the ancilla. Further, since the trace distance is convex, the maximum will be attained at a pure input on one of the factors ρ_{λ} . For such a state, there is a further unitary U_{anc} acting on the ancilla that “compresses” the entanglement (i.e., by Schur decomposition)

$$\rho'_{\lambda} = U_{anc}(|0\rangle\langle 0| \otimes \rho_{\lambda})U_{anc}^{\dagger} \quad (4.93)$$

where ρ_{λ} is a pure state entangled between a d_{λ} -dimensional subspace $\mathcal{H}_{anc}$ and the λ factor in the partition algebra. Further, the distinguishing operator $\mathbf{O}$ achieving maximal distinguishing probability will also be supported on the subspace $\mathcal{H}_{anc} \otimes (\mathbb{C}^N)^{\otimes k}$. Thus, the maximal distinguishing probability can be attained using an ancilla dimension as little as the largest dimension of the factors of the partition algebra $\max_{\lambda \in \Lambda_{k,N}} d_{\lambda}$. ■

Second, since the input is “fixed,” and is independent of the dimension, we can define a family of “equivalent” states across dimensions.

Lemma IV.15 (Extending given inputs and observable to other dimensions). *Consider $\mathcal{N}_{j, \{\mathbf{w}_i\}}$ as in Lemma IV.1. Then, assuming $N \geq 2k$, for any observable and state $\mathbf{A}_N, \rho_N \in \mathbf{B}((\mathbb{C}^N)^{\otimes k})$, there exist matrices $\mathbf{A}_{N'}, \rho_{N'} \in \mathbf{B}((\mathbb{C}^{N'})^{\otimes k})$ such that function*

$$f\left(\frac{1}{N'}\right) := \text{Tr}\left[\mathbf{A}_{N'} \mathcal{N}_{j, \{\mathbf{w}_i\}}[\rho_{N'}]\right] \quad \text{for each integer } N' \geq 2k \quad (4.94)$$

is rational polynomial of N with poles at integers $0, \dots, 2k\ell - 1$ each with multiplicity at most $2k\ell + 3k + 2$.

Proof of Lemma IV.15. For ease of notation, we begin with the case without ancillas, and then argue that the same argument works in the presence of ancillas. Indeed, what is changing is the basis for the partition algebra and the ancilla is fixed. Given any operator and state $\mathbf{A}_N, \boldsymbol{\rho}_N \in \mathbf{P}_k(N) \subset \mathbf{B}((\mathbb{C}^N)^{\otimes k})$, they can be written as

$$\boldsymbol{\rho}_N = \bigoplus_{\lambda \in \Lambda_{k,N}} \sum_{i,j} \rho_{ij}^\lambda |v_i\rangle \langle v_j| \otimes \frac{\mathbf{I}_{S_\lambda}}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \quad (4.95)$$

$$= \sum_{\lambda \in \Lambda_{k,N}} \frac{1}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \sum_{i,j} \mathcal{Q}_\lambda[\mathbf{v}_i \mathbf{v}_j^\dagger] \rho_{ij}^\lambda \quad (4.96)$$

$$\mathbf{A}_N = \bigoplus_{\lambda \in \Lambda_{k,N}} \sum_{i,j} A_{ij}^\lambda |v_i\rangle \langle v_j| \otimes \mathbf{I}_{S_\lambda} \quad (4.97)$$

$$= \sum_{\lambda \in \Lambda_{k,N}} \sum_{i,j} \mathcal{Q}_\lambda[\mathbf{v}_i \mathbf{v}_j^\dagger] A_{ij}^\lambda \quad (4.98)$$

such that

$$\text{Tr}[\boldsymbol{\rho}_N] = \sum_{\lambda \in \Lambda_{k,N}} \sum_i \rho_{ii}^\lambda = 1 \quad \text{and} \quad \|\mathbf{A}_N\|_\infty = \max_\lambda \|\mathbf{A}^\lambda\|_\infty \quad (4.99)$$

and for each $\mathbf{O}_\Pi \in \mathbf{P}_k(N)$,

$$\text{Tr}[\mathbf{O}_\Pi \boldsymbol{\rho}_N] = \sum_{\lambda \in \Lambda_{k,N}} \sum_{i,j} \frac{\text{Tr}[\mathbf{O}_\Pi \mathcal{Q}_\lambda[\mathbf{v}_i \mathbf{v}_j^\dagger]]}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \rho_{ji}^\lambda \quad (4.100)$$

$$\text{Tr}[\mathbf{O}_\Pi \mathbf{A}_N] = \sum_{\lambda \in \Lambda_{k,N}} \sum_{i,j} \text{Tr}[\mathbf{O}_\Pi \mathcal{Q}_\lambda[\mathbf{v}_i \mathbf{v}_j^\dagger]] A_{ji}^\lambda. \quad (4.101)$$

The above can be extended to other dimensions $N' \geq 2k$ as $\mathbf{A}_{N'}, \boldsymbol{\rho}_{N'} \in \mathbf{B}((\mathbb{C}^{N'})^{\otimes k})$, which is

$$\boldsymbol{\rho}_{N'} = \sum_{\lambda' \in \Lambda_{k,N'}} \frac{1}{\text{Tr}[\mathbf{I}_{S_{\lambda'}}]} \sum_{i,j} \mathcal{Q}_{\lambda'}[\mathbf{v}_i \mathbf{v}_j^\dagger] \rho_{ij}^{\lambda'} \quad (4.102)$$

$$\mathbf{A}_{N'} = \sum_{\lambda' \in \Lambda_{k,N'}} \sum_{i,j} \mathcal{Q}_{\lambda'}[\mathbf{v}_i \mathbf{v}_j^\dagger] A_{ij}^{\lambda'}. \quad (4.103)$$

Note that

$$\text{Tr}[\boldsymbol{\rho}_{N'}] = \sum_{\lambda' \in \Lambda_{k,N'}} \sum_i \rho_{ii}^{\lambda'} = 1 \quad \text{and} \quad \|\mathbf{A}_{N'}\|_\infty = \max_{\lambda' \in \Lambda_{k,N'}} \|\mathbf{A}^{\lambda'}\|_\infty. \quad (4.104)$$

Also, we relate the extension $N' \geq 2k$ from N by setting

$$\rho_{ij}^{\lambda'} = \rho_{ij}^\lambda \quad \text{and} \quad A_{ij}^{\lambda'} = A_{ij}^\lambda \quad \text{for each } i, j, \quad \text{if } |\lambda'^*| = |\lambda^*| \quad (4.105)$$

since the irreducible representations λ of $\mathbf{P}_k(N)$ can be identified with λ' of $\mathbf{P}_k(N')$, and similarly

for A_{ij}^λ . We evaluate the expression by inserting resolutions of identity

$$\text{Tr}[\mathbf{A}_{N'} \mathcal{N}_{j, \{\mathbf{w}_i\}} [\boldsymbol{\rho}_{N'}]] = (\mathbf{A}_{N'} | \mathcal{N}_{j, \{\mathbf{w}_i\}} | \boldsymbol{\rho}_{N'}) \quad (4.106)$$

$$= \sum_{\Pi_1, \Pi_2 \vdash 2k} \frac{(\mathbf{A}_{N'} | \mathbf{O}'_{\Pi_2}) (\mathbf{O}'_{\Pi_2} | \mathcal{N}_{j, \{\mathbf{w}_i\}} | \mathbf{O}'_{\Pi_1}) (\mathbf{O}'_{\Pi_1} | \boldsymbol{\rho}_{N'})}{\|\mathbf{O}'_{\Pi_2}\|_2^2 \|\mathbf{O}'_{\Pi_1}\|_2^2} \quad (4.107)$$

$$= \sum_{\Pi_1, \Pi_2 \vdash 2k} \frac{(\mathbf{A}_{N'} | \mathbf{O}'_{\Pi_2}) (\mathbf{O}'_{\Pi_2} | \mathcal{N}_{j, \{\mathbf{w}_i\}} | \mathbf{O}'_{\Pi_1}) (\mathbf{O}'_{\Pi_1} | \boldsymbol{\rho}_{N'})}{\|\mathbf{O}'_{\Pi_2}\|_2^2 \|\mathbf{O}'_{\Pi_1}\|_2^2}. \quad (4.108)$$

Let's count the poles for each:

(i) By (3.57),

$$\frac{1}{\|\mathbf{O}'_{\Pi_2}\|_2^2}, \frac{1}{\|\mathbf{O}'_{\Pi_1}\|_2^2} = \frac{1}{N(N-1)\dots} \quad (4.109)$$

which individually has poles at integers $0, \dots, k$ each with multiplicity at most 1.

(ii) Rewrite in terms of the $\mathbf{O}_\Pi$'s by (3.56)

$$(\mathbf{O}'_{\Pi_2} | \mathcal{N} | \mathbf{O}'_{\Pi_1}) = \sum_{\Pi'_1, \Pi'_2 \vdash 2k} K_{\Pi_2 \Pi'_2}^{-1*} K_{\Pi_1 \Pi'_1}^{-1} (\mathbf{O}_{\Pi'_2} | \mathcal{N} | \mathbf{O}_{\Pi'_1}), \quad (4.110)$$

which, by Lemma IV.4, which has poles at integers $0, \dots, 2k\ell - 1$ each with multiplicity at most $2k\ell$.

(iii)

$$\begin{aligned} (\mathbf{O}'_{\Pi_1} | \boldsymbol{\rho}_{N'}) &= \sum_{\Pi'_1 \vdash 2k} K_{\Pi_1 \Pi'_1}^{-1*} (\mathbf{O}_{\Pi'_1} | \boldsymbol{\rho}_{N'}) \quad (\text{By (3.56)}) \\ &= \sum_{\Pi'_1 \vdash 2k} \sum_{i,j,\lambda} K_{\Pi_1 \Pi'_1}^{-1*} \frac{\text{Tr}[\mathbf{O}_{\Pi'_1} \mathcal{Q}_\lambda [\mathbf{v}_i \mathbf{v}_j^\dagger]]}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \rho_{ji}^\lambda. \end{aligned} \quad (4.111)$$

The poles came from $\mathcal{Q}_\lambda = \sum_\lambda \Pi_\lambda$ and $\mathbf{v}_i \mathbf{v}_j^\dagger$ (Lemma IV.13) and $\text{Tr}[\mathbf{I}_{S_\lambda}]$ (Lemma III.6), which has poles at integers $0, \dots, 2k - 1$ each with multiplicity at most $2k$.

(iv)

$$\begin{aligned} (\mathbf{O}'_{\Pi_1} | \mathbf{A}_{N'}) &= \sum_{\Pi'_1 \vdash 2k} K_{\Pi_1 \Pi'_1}^{-1*} (\mathbf{O}_{\Pi'_1} | \mathbf{A}_{N'}) \quad (\text{By (3.56)}) \\ &= \sum_{\Pi'_1 \vdash 2k} \sum_{i,j,\lambda} K_{\Pi_1 \Pi'_1}^{-1*} \text{Tr}[\mathbf{O}_{\Pi'_1} \mathcal{Q}_\lambda [\mathbf{v}_i \mathbf{v}_j^\dagger]] A_{ji}^\lambda \end{aligned} \quad (4.112)$$

which like the case of (iii), has poles at integers $0, \dots, 2k\ell - 1$ each with multiplicity at most $2k\ell + k$.

Altogether,

$$f\left(\frac{1}{N'}\right) := \text{Tr}[\mathbf{A}_{N'} \mathcal{N}_{j, \{\mathbf{w}_i\}} [\boldsymbol{\rho}_{N'}]] \quad \text{for each integer } N' \geq 2k, \quad (4.113)$$

which has poles at integers $0, \dots, 2k\ell - 1$ each with multiplicity at most $2k\ell + 3k + 2$.

To extend to the case with ancillas, we run the above argument for each irrep $\lambda \in \Lambda_{k,N}$

$$\rho_\lambda = \sum_{i,j} \rho_{ij}^\lambda |v_i\rangle \langle v_j| \otimes \frac{\mathbf{I}_{S_\lambda}}{\text{Tr}[\mathbf{I}_{S_\lambda}]} \otimes \mathbf{O}_{ij} \quad (4.114)$$

$$\mathbf{A} = \bigoplus_{\lambda \in \Lambda_{k,N}} \sum_{i,j} A_{ij}^\lambda |v_i\rangle \langle v_j| \otimes \mathbf{I}_{S_\lambda} \otimes \mathbf{O}'_{ij} \quad (4.115)$$

were $\mathbf{O}_{ij}, \mathbf{O}'_{ij}$ acts on space of dimension d_λ , which encompasses all possible operator $\mathbf{A}$ acting on $(\mathbb{C}^N)^{\otimes k} \otimes \mathbb{C}^{d_\lambda}$ and inheriting the operator norm bounds. $\blacksquare$

Lemma IV.16 (Rational polynomial for Haar channel). *In the setting of Lemma IV.15, the Haar random channel evaluates on the same set of extensions $\rho_{N'}, \mathbf{A}_{N'}$*

$$f\left(\frac{1}{N'}\right) := \text{Tr}[\mathbf{A}_{N'} \mathcal{N}_{2k,U}[\rho_{N'}]] \quad \text{for each integer } N' \geq 2k \quad (4.116)$$

is rational polynomial of N at integers $-(k-1), \dots, 0, 1, 2k-1$, each with multiplicity bounded by $4k+2$.

Proof. The change in the argument of Lemma IV.15 is that

$$(\mathbf{O}'_{\Pi_2} | \mathcal{N} | \mathbf{O}'_{\Pi_1}) = \sum_{\Pi'_1, \Pi'_2 \vdash 2k} K_{\Pi_2 \Pi'_2}^{-1*} K_{\Pi_1 \Pi'_1}^{-1} (\mathbf{O}_{\Pi_2} | \mathcal{N} | \mathbf{O}_{\Pi_1}) \quad (4.117)$$

And we directly invoke the Weingarten function for the unitary group [CMN22, Theorem 4.3], which has poles at $-(k-1), \dots, 0, \dots, (k-1)$ with multiplicity at most k . $\blacksquare$

V. PROOF OF MAIN RESULT

This section contains the formal proof of our main result (Theorem I.3), which we restate as follows.

Theorem I.3 (Unitary designs from product of sparse exponentials). *For each $m, \ell \in \mathbb{Z}^+$, let $\mathbf{V}$ be the N -dimensional random unitary formed by a product of the ℓ independent exponentials of the random matrices $\mathbf{A}_m^{(1)}, \mathbf{A}_m^{(2)}, \dots, \mathbf{A}_m^{(\ell)}$, left and right multiplied by random permutations $\mathbf{Z}_L, \mathbf{Z}_R$, i.e.*

$$\mathbf{V} := \mathbf{Z}_L \left(\prod_{j=1}^{\ell} e^{i\theta_m \mathbf{A}_m^{(j)}} \right) \mathbf{Z}_R, \quad (1.5)$$

for some m -dependent angle $\theta_m = \mathcal{O}(1)$. Then, $\mathbf{V}$ is an approximate k -design in diamond distance. More precisely, for $N = 2^n$,

$$\|\mathcal{N}_{2k,\mathbf{V}} - \mathcal{N}_{2k,U_{\text{Haar}}}\|_{\diamond} \leq \mathcal{O}\left(\frac{k^8 \ell^8 (m^4 n^8 + n^8)}{N} + \frac{k^4}{m^\ell}\right). \quad (1.6)$$

Since the proof requires several lemmas, we first discuss them locally and combine them in the end.

A. Expanding one exponential into words

We first expand the single exponential and collect the distinct words

$$e^{i\theta A_m} = \exp\left(\frac{i\theta}{\sqrt{2m}} \sum_{a=1}^m (\mathbf{Z}_a + \mathbf{Z}_a^\dagger)\right) \quad (5.1)$$

$$= \mathbf{I} + \frac{i\theta}{\sqrt{2m}} \sum_{a=1}^m (\mathbf{Z}_a + \mathbf{Z}_a^\dagger) - \frac{\theta^2}{2} \frac{1}{2m} \left(\sum_{a=1}^m \mathbf{Z}_a + \mathbf{Z}_a^\dagger\right)^2 \dots \quad (5.2)$$

$$= v(\theta)\mathbf{I} + \sum_i w_i(m, \theta) \mathbf{W}_i \quad \text{where} \quad \mathbf{W}_i \in \mathcal{W}(\{\mathbf{Z}_a\}_{a=1}^m). \quad (5.3)$$

Lemma V.1 (Normalized, bounded weights).

$$\sum_i |w_i|^2 = 1 \quad (5.4)$$

$$\max_i |w_i| \leq \frac{1}{\sqrt{m}}. \quad (5.5)$$

Proof. Fix m and taking the large- N limit:

$$1 = \lim_{N \rightarrow \infty} \mathbb{E} \overline{\text{Tr}}[e^{-i\theta A_m} e^{i\theta A_m}] = \sum_i |w_i|^2. \quad (\text{large-}N \text{ limit})$$

The second inequality uses the fact that the normalization trace of a nontrivial word vanishes in the large- N limit. The second claim follows from the symmetry of the paths: each path with nonzero length must map to m other paths by cycling through the labels ($a = 1, \dots, m$). Thus, there cannot be a path contributing more than $1/\sqrt{m}$ due to the sum constraints $\sum_i |w_i|^2 = 1$. ■

The coefficient $v(\theta)$ for the identity operator is a sum over weighted trivial words (i.e., loops on the Cayley graph of the free group of m elements). For example,

$$\frac{1}{2m} \left(\sum_{a=1}^m \mathbf{Z}_a + \mathbf{Z}_a^\dagger\right)^2 = 1 \cdot \mathbf{I} + (\text{nontrivial words}) \quad (5.6)$$

$$\frac{1}{4m^2} \left(\sum_{a=1}^m \mathbf{Z}_a + \mathbf{Z}_a^\dagger\right)^2 = \left(1 + \frac{m-1}{2m}\right) \cdot \mathbf{I} + (\text{nontrivial words}). \quad (5.7)$$

The sum over all paths at order p is exactly the moments of Kesten-McKay distribution [Kes59, McK81]. Thus, the exponentially weighted sum is then the characteristic function

$$v_m(\theta) = \int_{-\infty}^{\infty} e^{i\theta x} p_m(x) dx. \quad (5.8)$$

Definition V.1 (Kesten-McKay distribution [Kes59, McK81]). *The Kesten-McKay distribution is defined by*

$$p_m(x) := \begin{cases} \frac{\sqrt{4\frac{m-1}{m} - x^2}}{2\pi(1 - \frac{x^2}{m})} & \text{if } |x| \leq 2\sqrt{1 - \frac{1}{m}} \\ 0 & \text{else.} \end{cases} \quad (5.9)$$

In the limit $m \rightarrow \infty$, the Kesten-McKay distribution converges to Wigner's semi-circle

$$p_m(x) := \begin{cases} \frac{\sqrt{4-x^2}}{2\pi} & \text{if } |x| \leq 2 \\ 0 & \text{else,} \end{cases} \quad (5.10)$$

and the above gives an exact formula for the correction due to m . Thus, we may eliminate the trivial word $\mathbf{I}$ by choosing the zeros of this function:

$$\theta_m \text{ such that } v_m(\theta_m) = 0, \quad (5.11)$$

i.e., making the exponential traceless in the large- N limit. In particular, the angle is always bounded by an absolute constant $\theta_m = \mathcal{O}(1)$ for any m .

The nice consequence of choosing $v_m(\theta_m) = 0$ is that there is *no cancellation* due to taking the product of exponentials. For example, in the product of two independent copies

$$e^{i\theta A_m} e^{i\theta A'_m} = \sum_i w_i(m, \theta) \mathbf{W}_i \cdot \sum_i w_i(m, \theta) \mathbf{W}'_i \quad (5.12)$$

$$= \sum_{i,j} w_i(m, \theta) w_j(m, \theta) \mathbf{W}_i \mathbf{W}'_j, \quad (5.13)$$

each of the product words is different so that

$$\mathbf{W}_i \mathbf{W}'_j = \mathbf{W}_{i'} \mathbf{W}'_{j'} \text{ if and only if } (i, j) = (i', j'). \quad (5.14)$$

Thus, taking products yields an exponentially growing number of words that we can easily keep track of. Note that taking powers of the same $(e^{i\theta A_m})^2$ could also work in principle with a more careful combinatorial analysis for the cancellation of words.

B. Proof of [Theorem I.3](#)

We begin with a proof sketch. For any integers m, ℓ , the product of ℓ independent exponentials of $2m$ -sparse random matrices can be expanded into distinct words

$$\prod_{j=1}^{\ell} e^{i\theta A_m^{(j)}} = \sum_{\mathbf{i}} w_{\mathbf{i}}(\theta) \mathbf{W}_{\mathbf{i}} \quad (\text{Distinct words: } \mathbf{W}_{\mathbf{i}} \neq \mathbf{W}_{\mathbf{j}} \text{ for each } \mathbf{i} \neq \mathbf{j}.)$$

with fairly spread-out weights $w_{\mathbf{i}}$ (calculated from the individual properties ([Lemma V.1](#)))

$$\begin{aligned} \sum_{\mathbf{i}} |w_{\mathbf{i}}|^2 &= (\sum_i |w_i|^2)^\ell = 1 \\ \max_{\mathbf{i}} |w_{\mathbf{i}}| &= \left(\max_i |w_i| \right)^\ell \leq \frac{1}{\sqrt{m}^\ell}. \end{aligned} \quad (5.15)$$

Intuitively, we expect the resulting product to be a very dense matrix (sparsity $\Omega(m)^\ell$) as we expect the distinct words of permutations to map the same bit string to distinct bit strings.

1. The large- N limit

Indeed, if the dimension N is infinite (fixing the length of the words and the number of queries k), then there will almost surely be no *collision* between the distinct words, and we expect them can be replaced with *independent* permutations. This can be captured by the following equality of limits, with the precise order of limit and choice of norm stated in [Lemma IV.1](#).

$$\begin{aligned} \mathbf{Z}_L \left(\sum_i w'_i(\theta) \mathbf{W}'_i \right) \mathbf{Z}_R &\stackrel{N \rightarrow \infty}{=} \mathbf{Z}_L \left(\sum_i w'_i(\theta) \mathbf{Z}_i \right) \mathbf{Z}_R \\ &\quad \text{(distinct words are free in the large-} N \text{ limit: } \text{Lemma IV.1}) \\ &\stackrel{m^\ell \rightarrow \infty}{=} \mathbf{G}. \quad \text{(Matrix central limit theorem in } k\text{-fold diamond norm)} \end{aligned}$$

Observe that the summands match the second (mixed) moments of a Gaussian matrix

$$\mathbb{E}[\mathbf{Z}_i^{(\dagger)} \otimes \mathbf{Z}_i^{(\dagger)}] = \mathbb{E}[\mathbf{G}_i^{(\dagger)} \otimes \mathbf{G}_i^{(\dagger)}]. \quad (5.16)$$

Thus, in the limit of many summands (with some requirement that the weights all be reasonably small), the sum converges to a Gaussian; see [Lemma A.1](#) for the nonasymptotic bounds.

The Gaussian is a simple random matrix that is left and right unitarily invariant. The Gaussian is nonetheless not the same as a Haar random unitary. In fact, it is not even a unitary matrix, as its singular values are distributed according to the Marchenko-Pastur distribution, which differs from the unitary case. Nevertheless, the Gaussian is effectively Haar in the parallel access model.

$$\mathbf{G} \stackrel{N \rightarrow \infty}{=} \mathbf{U}_{Haar}. \quad \text{(in the diamond distance, } \text{Lemma B.1})$$

Intuitively, for *arbitrary fixed* input state uncorrelated with $\mathbf{G}$, it is nearly *isometric* with *high probability*, as can be seen from the expected value $\mathbb{E} \mathbf{G}^\dagger \mathbf{G} = \mathbf{I}$. Regardless of the interpretation, the presence of Gaussians $\mathbf{G}$ is merely a proof artifact, and all that matters in this context is merely the k -fold CP map $\mathbb{E} \mathcal{N}_{2k, \mathbf{G}}$.

The assertions above together imply that $\mathbf{Z}_L \left(\prod_{j=1}^\ell e^{i\theta A_m^{(j)}} \right) \mathbf{Z}_R \approx \mathbf{U}_{Haar}$ as k -fold channels in the limits of $N \rightarrow \infty, m^\ell \rightarrow \infty$.

2. Interpolating to finite N

To complete the proof, the main technical argument is to handle finite- N corrections. We isolate the finite- N bounds as the following lemma. The crux of the argument is an interpolation argument for the variable $x = \frac{1}{N}$ from the large- N limits. We begin with a sketch of the argument by invoking the partial results we already proved. Define the two channels of interest:

$$\mathcal{N}_1 := \mathcal{N}_{2k, \mathbf{V}} \quad \text{and} \quad \mathcal{N}_2 := \mathcal{N}_{2k, \mathbf{U}_{Haar}}. \quad (5.17)$$

By [Lemma IV.14](#), the diamond distance can be controlled at ancilla size $\max_\lambda d_\lambda$

$$\left\| \mathcal{N}_{2k,S} \circ (\mathcal{N}_1 - \mathcal{N}_2) \circ \mathcal{N}_{2k,S} \right\|_\diamond = \sup_{\rho, \mathcal{O}} \text{Tr}[\mathcal{O} \mathcal{N}_1 \rho] - \text{Tr}[\mathcal{O} \mathcal{N}_2 \rho]. \quad (5.18)$$

where the supremum is over symmetrized operators and states that may involve ancillas. (Even though we have in fact a stronger symmetry $\mathcal{N}_{2k,S}$, it suffices to exploit the $\mathcal{N}_{2k,S}$ symmetry.) We will show that the distinguishing probability is small for each input and output by constructing the function

$$f_{\rho, \mathcal{O}}\left(\frac{1}{N'}\right) = \text{Tr}[\mathcal{O}^{(N')} \mathcal{N}_1^{(N')} \rho^{(N')}] - \text{Tr}[\mathcal{O}^{(N')} \mathcal{N}_2^{(N')} \rho^{(N')}] \quad (5.19)$$

$$= f_1(N') - f_2(N') \quad (5.20)$$

as an extension from the original dimension $N' = N$ by defining a family of operators and superoperators

$$(\mathcal{O}^{(N')}, \mathcal{N}_1^{(N')}, \mathcal{N}_2^{(N')}, \rho^{(N')}) \quad \text{for each} \quad 2k \leq N' \leq \infty \quad (5.21)$$

$$\text{such that} \quad (\mathcal{O}^{(N)}, \mathcal{N}_1^{(N)}, \mathcal{N}_2^{(N)}, \rho^{(N)}) = (\mathcal{O}, \mathcal{N}_1, \mathcal{N}_2, \rho). \quad (5.22)$$

Of course, the operators $\rho^{(N)}, \mathcal{O}^{(N)}$ at other dimensions N' has to be “similar” to the original $\rho, \mathcal{O}$ at dimension N . In order to interpolate using Markov’s inequality, we spell out the requirements for the extension:

- Rational low-degree function ([Lemma IV.15](#), [Lemma IV.16](#)): we extend to other dimensions by choosing the appropriate extensions of the inputs and outputs. Since the exponential is an infinite series, we have to truncate the Taylor expansion ([Lemma V.3](#)) to ensure that the product $\prod_{j=1}^\ell e^{i\theta_m A_m^{(j)}}$ is approximated to error ϵ in the operator norm. See [section V C](#) for the proofs of the following lemma.

Lemma V.2 (Low-degree approximation). *For any ϵ, k , truncating each exponentials $e^{i\theta_m A_m^{(j)}}$ at degree $d_1 = \mathcal{O}(\sqrt{m} \log(k\ell/\epsilon))$ suffices to ensure*

$$\left| f_{\rho, \mathcal{O}, 1}\left(\frac{1}{N}\right) - f_{\rho, \mathcal{O}, 1}^{(trun)}\left(\frac{1}{N}\right) \right| \leq \epsilon. \quad (5.23)$$

Meanwhile, truncated function $f_{\rho, \mathcal{O}}^{(trun)}(\frac{1}{N})$ is a rational polynomial of N at integers

$$0, 1, \dots, 2k\ell d_1 - 1 \quad \text{each with multiplicity at most} \quad 2k\ell d_1 + 3k + 2 \quad (5.24)$$

where $\ell \cdot d_1$ is the maximal length of words of permutations, as coming from the product of ℓ -many degree d_1 words. The case for $f_{\rho, \mathcal{O}, 2}$ ([Lemma IV.16](#)) has fewer multiplicities in a smaller range of integers, and that of $f_{\rho, \mathcal{O}, 1}$ will dominate. The choices for the degrees d_1 will depend on N, m, ℓ, k .

- A priori bounds: This merely came from the structural fact that the expression is a difference between probabilities, bounded between one and zero:

$$\left| f_{\rho, \mathbf{O}}\left(\frac{1}{N'}\right) \right| \leq \left\| \mathcal{N}_1^{(N')} - \mathcal{N}_2^{(N')} \right\|_{1-1} \|\rho_{N'}\|_1 \|\mathbf{O}_{N'}\|_\infty \leq 2 \quad \text{for each integer } N'. \quad (5.25)$$

- Large- N limits ([Lemma IV.1](#), [Lemma B.1](#)): The large- N limit coincide with the “free” model: sum over i.i.d. permutations. Also, the Haar random Channel can be replaced with Ginibre ensembles

$$\begin{aligned} f_{1, \rho, \mathbf{O}}\left(\frac{1}{N'}\right) &= \text{Tr}[\mathbf{O}_{N'} \mathcal{N}_1 \rho_{N'}] \xrightarrow{N' \rightarrow \infty} \text{Tr}[\mathbf{O}_{N'} \mathcal{N}_1^{(free)} \rho_{N'}] = f_{1, \rho, \mathbf{O}}^{(free)}\left(\frac{1}{N'}\right) \\ f_{2, \rho, \mathbf{O}}\left(\frac{1}{N'}\right) &= \text{Tr}[\mathbf{O}_{N'} \mathcal{N}_2 \rho_{N'}] \xrightarrow{N' \rightarrow \infty} \text{Tr}[\mathbf{O}_{N'} \mathcal{N}_2^{(Ginibre)} \rho_{N'}] = f_{2, \rho, \mathbf{O}}^{(Ginibre)}\left(\frac{1}{N'}\right). \end{aligned} \quad (5.26)$$

- Comparing the “nicer” models ([Lemma A.1](#)): We further take a Lindeberg principle to argue that these large- N limits are very close to each other. While the most general Lindeberg argument works at any finite dimension N , the large- N limits simplify the calculations.

$$\left| f_{\rho, \mathbf{O}}\left(\frac{1}{\infty}\right) \right| = \left| \lim_{N' \rightarrow \infty} f_{1, \rho_{N'}, \mathbf{O}_{N'}} - f_{2, \rho_{N'}, \mathbf{O}_{N'}} \right| \quad (5.27)$$

$$= \left| \lim_{N' \rightarrow \infty} f_{1, \rho_{N'}, \mathbf{O}_{N'}}^{(free)} - f_{2, \rho_{N'}, \mathbf{O}_{N'}}^{(Ginibre)} \right| \quad ((5.26))$$

$$\leq \frac{1}{8} \sum_i \left((4k|w_i|)^4 + (4k|w_i|)^{2k} \right) + \frac{1}{8} \sum_i \left((4k|w'_i|)^4 + (4k|w'_i|)^{2k} \right)$$

(Lindeberg argument for both: [Lemma A.1](#))

$$\leq \frac{(4k)^2}{8} \left(\sum_i |w_i|^2 \right) \cdot \max_i \left((4k|w_i|)^2 + (4k|w_i|)^{2k-2} \right) + (w_i \rightarrow w'_i) \quad (\text{Holder's})$$

$$\leq \frac{(4k)^2}{8} 1 \cdot \left(\frac{16k^2}{m^\ell} + \left(\frac{16k^2}{m^\ell} \right)^{k-1} \right) + (m, \ell \rightarrow m', \ell') \quad (5.28)$$

(Bounds on the weights w_i : [\(5.15\)](#))

$$\stackrel{\ell'=2, m' \rightarrow \infty}{\leq} \frac{(4k)^2}{8} \left(\frac{16k^2}{m^\ell} + \left(\frac{16k^2}{m^\ell} \right)^{k-1} \right) \quad (\text{Second term drops due to } m' \rightarrow \infty)$$

$$\leq \min \left(\frac{128k^4}{m^\ell}, 2 \right). \quad (5.29)$$

The last inequality recalls the a priori bound $\left| f_{\rho, \mathbf{O}}\left(\frac{1}{\infty}\right) \right| \leq 2$ to drop the higher order term since we must have $\frac{16k^2}{m^\ell} \leq 1$ for the bound to be better than the a priori bounds.

Proof of [Theorem I.3](#). We put the above together. For any m, ℓ, N ,

$$\left\| \mathcal{N}_{2k, S} \circ \left(\mathcal{N}_1 - \mathcal{N}_2 \right) \circ \mathcal{N}_{2k, S} \right\|_\diamond \leq \sup_{\rho, \mathbf{O}} \left| f_{\rho, \mathbf{O}}\left(\frac{1}{N}\right) \right|. \quad (5.30)$$

We further introduce a truncation error (for the exponential in f_1)

$$\begin{aligned} \left| f_{\rho, \mathbf{O}}\left(\frac{1}{N}\right) \right| &\leq \left| f_{\rho, \mathbf{O}}\left(\frac{1}{N}\right) - f_{\rho, \mathbf{O}}^{(trun)}\left(\frac{1}{N}\right) \right| + \left| f_{\rho, \mathbf{O}}^{(trun)}\left(\frac{1}{N}\right) - f_{\rho, \mathbf{O}}^{(trun)}\left(\frac{1}{\infty}\right) \right| \\ &\quad + \left| f_{\rho, \mathbf{O}}^{(trun)}\left(\frac{1}{\infty}\right) - f_{\rho, \mathbf{O}}\left(\frac{1}{\infty}\right) \right| + \left| f_{\rho, \mathbf{O}}\left(\frac{1}{\infty}\right) \right| \end{aligned} \quad (5.31)$$

We instantiate the truncation error from $\mathcal{N}_1$

$$\left| f_{\rho, \mathcal{O}}\left(\frac{1}{N}\right) - f_{\rho, \mathcal{O}}^{(trun)}\left(\frac{1}{N}\right) \right| \leq \epsilon \quad \text{for any } N. \quad (\text{By Lemma V.2})$$

The truncated function f_1 now have a total number of poles $d = 2k\ell d_1(2k\ell d_1 + 3k + 2)$ and bound on the pole locations $B \leq 2k\ell d_1 - 1$ (which is strictly worse than the Haar random channel (Lemma IV.16)), so we can invoke Markov's inequality for $N_0 \geq d^2 + 8bB - 1$:

$$\begin{aligned} \left| f_{\rho, \mathcal{O}}^{(trun)}\left(\frac{1}{N}\right) - f_{\rho, \mathcal{O}}^{(trun)}\left(\frac{1}{\infty}\right) \right| &\leq \frac{2d^2(N_0 + 10dB)}{N} \sup_{N \geq N_0} \left| f_{\rho, \mathcal{O}}^{(trun)}\left(\frac{1}{N}\right) \right| \quad (\text{By Lemma III.2}) \\ &\leq \mathcal{O}\left(\frac{(k^2\ell^2d_1^2)^4}{N}\right), \end{aligned} \quad (5.32)$$

using that $\left| f_{\rho, \mathcal{O}}^{(trun)}\left(\frac{1}{N_0}\right) \right| \leq \left| f_{\rho, \mathcal{O}}\left(\frac{1}{N_0}\right) \right| + \epsilon \leq 2 + \epsilon \leq 3$. To consolidate the error,

$$\begin{aligned} \left\| \mathcal{N}_{2k, S} \circ \left(\mathcal{N}_1 - \mathcal{N}_2 \right) \circ \mathcal{N}_{2k, S} \right\|_{\diamond} &\leq \epsilon + \mathcal{O}\left(\frac{k^8\ell^8(m^4\log^8(k\ell/\epsilon))}{N}\right) + \min\left(\frac{128k^4}{m^\ell}, 2\right) \quad (5.33) \\ &\leq \mathcal{O}\left(\frac{k^8\ell^8m^4n^8}{N} + \frac{k^4}{m^\ell}\right). \quad (\text{Setting } \epsilon = \mathcal{O}(\frac{k\ell}{N})) \end{aligned}$$

The last line drops the $\min(\cdot)$ since the quantity is a priori bounded by 2. $\blacksquare$

C. Truncation error for exponentials

This section includes a standard truncation argument for Taylor expansion of exponentials.

Lemma V.3 (Taylor expansion for exponentials). *For every degree d there exists a polynomial of h_d such that*

$$\|e^{i\mathbf{H}} - h_d(\mathbf{H})\| \leq \frac{\|\mathbf{H}\|^{d+1}}{(d+1)!} \quad \text{for any Hermitian matrix } \mathbf{H}. \quad (5.34)$$

In particular, choosing

$$d = \mathcal{O}\left(\frac{\|\mathbf{H}\| \log(1/\epsilon)}{\log(\log(1/\epsilon))}\right) \quad \text{ensures that} \quad \|e^{i\mathbf{H}} - h_d(\mathbf{H})\| \leq \epsilon. \quad (5.35)$$

Proof of Lemma V.2. We begin with Taylor expansion

$$\|e^{i\theta_m \mathbf{A}_m} - h_{d_1}(\mathbf{A}_m)\| \leq \frac{\|\theta_m \mathbf{A}_m\|^{d_1+1}}{(d_1+1)!}. \quad (5.36)$$

Since the exponential appears $2k \cdot \ell$ times in $f_{\rho, \mathcal{O}, 1}(\frac{1}{N})$, the error can be accounted for by triangle inequality

$$\begin{aligned} \left| f_{\rho, \mathcal{O}, 1}\left(\frac{1}{N}\right) - f_{\rho, \mathcal{O}, 1}^{(trun)}\left(\frac{1}{N}\right) \right| &\leq \left(1 + \frac{\|\theta_m \mathbf{A}_m\|^{d_1+1}}{(d_1+1)!}\right)^{2k\ell} - 1 \quad (5.37) \\ &\leq \exp\left(2k\ell \frac{\|\theta_m \mathbf{A}_m\|^{d_1+1}}{(d_1+1)!}\right) - 1 \quad (\text{Since } 1 + x \leq e^x) \\ &\leq \epsilon. \quad (\text{Since } \theta_m \|\mathbf{A}_m\| \leq \mathcal{O}(\sqrt{m})) \text{ and } e^x \leq 1 + 2x \text{ for } x \leq 1.) \end{aligned}$$

That last line chooses the suitable $d_1 = \mathcal{O}(\sqrt{m} \log(k\ell/\epsilon))$. $\blacksquare$

Appendix A: Lindeberg arguments

One step of our argument converts an independent sum to a matrix with Gaussian entries. This is not terribly surprising and appeared in [CDB⁺23, CDX⁺24] in a different form. We quickly derive a version suitable for our context.

Lemma A.1 (A Lindeberg argument assuming large- N). *For any $\mathbf{O} = \sum_j w_j \mathbf{Z}_j$ such that $\sum_i |w_i|^2 = 1$, In the large- N limit,*

$$\lim_{N \rightarrow \infty} \|\mathcal{N}_{2k, \mathbf{O}} - \mathcal{N}_{2k, \mathbf{G}}\|_{\diamond} \leq \frac{1}{8} \sum_{j=1} \left((4k|w_j|)^4 + (4k|w_j|)^{2k} \right). \quad (\text{A1})$$

This is an adaptation of the matrix Lindeberg argument [CDB⁺23] with simplification from the large- N limit. The main observation is that the (complex conjugated) second moments are equal for random permutations and Gaussians:

$$\mathbb{E}[\mathbf{Z} \otimes \mathbf{Z}^{\dagger}] = \mathbb{E}[\mathbf{G} \otimes \mathbf{G}^{\dagger}], \quad (\text{A2})$$

and all other (mixed) moments vanished up to 3 copies,

$$\mathbb{E}[\mathbf{G}^{(\dagger)}] = \mathbb{E}[\mathbf{Z}^{(\dagger)}] = 0 \quad (\text{A3})$$

$$\mathbb{E}[\mathbf{G}^{(\dagger)} \otimes \mathbf{G}^{(\dagger)} \otimes \mathbf{G}^{(\dagger)}] = \mathbb{E}[\mathbf{Z}^{(\dagger)} \otimes \mathbf{Z}^{(\dagger)} \otimes \mathbf{Z}^{(\dagger)}] = 0. \quad (\text{A4})$$

Since we are comparing CP maps, the following polarization identity will be useful to turn any superoperator into a weighted sum over CP maps.

Lemma A.2 (Polarization). *For any square matrix $\mathbf{A}, \mathbf{B}$,*

$$\mathbf{A}[\cdot] \mathbf{B}^{\dagger} = \mathbb{E}_{s=\pm 1, \pm i} s (\mathbf{A} + s \mathbf{B})[\cdot] (\mathbf{A} + s \mathbf{B})^{\dagger}.$$

Proof of Lemma A.1. Define the interpolant

$$\mathbf{O}_j := \sum_{i=1}^j \tilde{\mathbf{A}}_i + \sum_{j+1}^m \mathbf{A}_i \quad \text{where} \quad \mathbf{A}_j := w_j \mathbf{Z}_j \quad \text{and} \quad \tilde{\mathbf{A}}_j := w_j \mathbf{G}_j. \quad (\text{A5})$$

Then,

$$\|\mathcal{N}_{2k, \mathbf{O}} - \mathcal{N}_{2k, \mathbf{G}}\|_{\diamond} = \sup_{\rho, \mathbf{O}} \text{Tr}[\mathbf{O}(\mathcal{N}_{2k, \mathbf{O}} - \mathcal{N}_{2k, \mathbf{G}})\rho]. \quad (\text{A6})$$

By Lemma IV.14, it suffices to take the state to be entangled with ancilla of dimension $\max_{\lambda} d_{\lambda}$. Nevertheless, this will not be used anywhere in the proof.

We can expand the difference as a telescoping sum where we exchange one term at a time

$$\text{Tr}[\mathbf{O}(\mathcal{N}_{2k, \mathbf{O}} - \mathcal{N}_{2k, \mathbf{G}})\rho] = \sum_{j=1}^m (n_j - n_{j-1}) \quad \text{where} \quad n_j := \text{Tr}[\mathbf{O} \mathcal{N}_{2k, \mathbf{O}_j}[\rho]]. \quad (\text{A7})$$

In order to analyze the difference, for each intermediate step j , denote

$$\mathbf{O}_- := \mathbf{O}_j - \tilde{\mathbf{A}}_j = \mathbf{O}_{j-1} - \mathbf{A}_j. \quad (\text{A8})$$

When expanding powers of a sum of matrices, keep in mind the scalar binomial expansion:

$$(x + y)^{2k} = \sum_{q=0}^{2k} \binom{2k}{q} x^{2k-q} y^q. \quad (\text{A9})$$

For our matrices of interest, the expansion takes the form

$$\begin{aligned} (\mathbf{O}_- + \mathbf{A}_j)^{\otimes k} [\cdot] (\mathbf{O}_- + \mathbf{A}_j)^{\dagger \otimes k} &= \sum_{\text{words}} \mathbf{S}_- \otimes \cdots \mathbf{A}_j \otimes \mathbf{S}_- \cdots \mathbf{A}_j \mathbf{S}_- [\cdot] \otimes (\mathbf{A}_j \mathbf{S}_- \cdots)^{\dagger} \\ &=: \sum_{q=0}^{2k} \mathbf{M}_q. \end{aligned} \quad (\text{regroup by the occurrences } q \text{ of } \mathbf{A}_j) \quad (\text{A10})$$

To control the norm of the operators $\mathbf{M}_q$, we first polarize the error terms to turn the super-operator into a complex linear combination of completely positive maps (By [Lemma A.2](#)). There are different patterns of $\mathbf{S}_-$ and $\mathbf{A}_j$: (1) If all q -many $\mathbf{A}_j$ only paired with $\mathbf{S}_-$, there are q locations where we need to polarize

$$\begin{aligned} & \left| \text{Tr}[\mathbf{O} \mathbb{E} \mathbf{S}_- \otimes \cdots \mathbf{A}_j \otimes \mathbf{S}_- \cdots \mathbf{A}_j \mathbf{S}_- [\rho] \otimes (\mathbf{A}_j \mathbf{S}_- \cdots)^{\dagger}] \right| \quad (\text{A11}) \\ &= \left| \mathbb{E}_s s \text{Tr}[\mathbf{O} \mathcal{N}_{2, \mathbf{S}_-} \circ \mathcal{N}_{2, (a_j \mathbf{A}_j + s s_- \mathbf{S}_-)} \circ \cdots [\rho]] \right| \quad (\text{By Lemma A.2}) \\ &\leq \mathbb{E}_s \left\| \mathcal{N}_{2, \mathbf{S}_-}^{\dagger} \circ \mathcal{N}_{2, (a_j \mathbf{A}_j + s s_- \mathbf{S}_-)}^{\dagger} [\mathbf{I}] \right\|_{\infty} \quad (\text{Norm bounds for CP maps, } |s| = 1) \\ &\stackrel{N \rightarrow \infty}{=} \mathbb{E}_s \overline{\text{Tr}}[\mathcal{N}_{2, \mathbf{S}_-}^{\dagger} \circ \mathcal{N}_{2, (a_j \mathbf{A}_j + s s_- \mathbf{S}_-)}^{\dagger} [\mathbf{I}]] \quad (\text{By Corollary IV.3}) \\ &\stackrel{N \rightarrow \infty}{=} \mathbb{E} \left[(\overline{\text{Tr}}[\mathbf{S}_-^{\dagger} \mathbf{S}_-])^{k-q} \cdot \overline{\text{Tr}}[|a_j|^2 \mathbf{A}_j^{\dagger} \mathbf{A}_j + |s_-|^2 \mathbf{S}_-^{\dagger} \mathbf{S}_-]^q \right] \quad (\text{A12}) \\ &= \mathbb{E}_- (\overline{\text{Tr}}[\mathbf{S}_-^{\dagger} \mathbf{S}_-])^{\frac{2k-q}{2}} \cdot \mathbb{E}_j \overline{\text{Tr}}[\mathbf{A}_j^{\dagger} \mathbf{A}_j]^{q/2} \quad (\text{Optimize parameters and exploit independence}) \\ &\stackrel{N \rightarrow \infty}{=} (1 - |w_j|^2)^{\frac{2k-q}{2}} \cdot |w_j|^q \leq |w_j|^q. \quad (\text{By } \mathbf{A}_j^{\dagger} \mathbf{A}_j = \mathbf{I} \text{ and Corollary IV.3}) \end{aligned}$$

The fourth inequality uses the permutation symmetry of both channels to use [Corollary IV.3](#). The last equality minimizes the expression for suitable real random scalar variables

$$|a_j|^2 = \sqrt{\frac{\overline{\text{Tr}}[\mathbf{S}_-^{\dagger} \mathbf{S}_-]}{\overline{\text{Tr}}[\mathbf{A}_j^{\dagger} \mathbf{A}_j]}} \quad \text{and} \quad |s_-|^2 = \sqrt{\frac{\overline{\text{Tr}}[\mathbf{A}_j^{\dagger} \mathbf{A}_j]}{\overline{\text{Tr}}[\mathbf{S}_-^{\dagger} \mathbf{S}_-]}}. \quad (\text{A13})$$

The case where $\mathbf{A}_j$ are paired up with $\mathbf{A}_j^{\dagger}$ enjoys the same bound using that the normalization trace is deterministic in the large- N limit for the Gaussian case

$$\lim_{N \rightarrow \infty} \overline{\text{Tr}}[\mathbf{G}^{\dagger} \mathbf{G}] \stackrel{\text{dist.}}{=} 1. \quad (\text{A14})$$

Likewise, $(\mathbf{O}_- + \tilde{\mathbf{A}}_j)^{\otimes k} [\cdot] (\mathbf{O}_- + \tilde{\mathbf{A}}_j)^{\dagger \otimes k} = \sum_{i=1}^m \tilde{\mathbf{M}}_i$ with analogous bounds for the summands.

To proceed, since the first and second (possibly conjugated) moments of the random matrices $\mathbf{A}_i$ and $\tilde{\mathbf{A}}_i$ match for each index i ,

$$\mathbb{E} \mathbf{A}_i^{(\dagger)} \otimes \mathbf{B} = \mathbb{E} \tilde{\mathbf{A}}_i^{(\dagger)} \otimes \mathbf{B}; \quad (\text{A15})$$

$$\mathbb{E} \mathbf{A}_i^{(\dagger)} \otimes \mathbf{A}_i^{(\dagger)} \otimes \mathbf{B} = \mathbb{E} \tilde{\mathbf{A}}_i^{(\dagger)} \otimes \tilde{\mathbf{A}}_i^{(\dagger)} \otimes \mathbf{B} \quad (\text{A16})$$

$$\mathbb{E} \mathbf{A}_i^{(\dagger)} \otimes \mathbf{A}_i^{(\dagger)} \otimes \mathbf{A}_i^{(\dagger)} \otimes \mathbf{B} = \mathbb{E} \tilde{\mathbf{A}}_i^{(\dagger)} \otimes \tilde{\mathbf{A}}_i^{(\dagger)} \otimes \tilde{\mathbf{A}}_i^{(\dagger)} \otimes \mathbf{B} \quad \text{for arbitrary } \mathbf{B} \text{ independent from } \mathbf{A}_i, \tilde{\mathbf{A}}_i. \quad (\text{A17})$$

Crucially, this implies that subtracting the expected moments completely *cancels* the first to third order terms $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3$ and $\tilde{\mathbf{M}}_1, \tilde{\mathbf{M}}_2, \tilde{\mathbf{M}}_3$

$$|n_j - n_{j-1}| = \left| \sum_{q=4}^{2k} \text{Tr}[\mathbf{O}(\mathbf{M}_q - \tilde{\mathbf{M}}_q)[\boldsymbol{\rho}]] \right| \quad (\text{A18})$$

$$\stackrel{N \rightarrow \infty}{\leq} \sum_{q=4}^{2k} \binom{2k}{q} \left(\overline{\text{Tr}}[\mathbb{E} \mathbf{A}_j^\dagger \mathbf{A}_j]^{q/2} + \overline{\text{Tr}}[\mathbb{E} \tilde{\mathbf{A}}_j^\dagger \tilde{\mathbf{A}}_j]^{q/2} \right) \quad (\text{A19})$$

$$\leq 2 \sum_{q=4}^{2k} \binom{2k}{q} |w_j|^q \quad (\text{A20})$$

$$\leq 2 \sum_{q=4}^{2k} (2k)^q |w_j|^q \quad (\text{Since } \binom{2k}{q} \leq (2k)^q)$$

$$\leq \frac{(4k|w_j|)^4 + (4k|w_j|)^{2k}}{8}. \quad (\text{A21})$$

The last inequality bounds the geometric series using the elementary numerical inequality

$$\sum_{q=4}^{2k} x^q = \sum_{q=4}^{2k} 2^{-q} (2x)^q \leq \frac{1}{8} ((2x)^4 + (2x)^{2k}) \quad \text{for } x \geq 0. \quad (\text{A22})$$

Sum over the index j to conclude the proof. ■

Appendix B: Comparing the Gaussian CP map with a unitary channel

Lemma B.1 (Ginibre matrices are effectively Haar unitaries in the diamond distance).

$$\lim_{N \rightarrow \infty} \|\mathcal{N}_{2k,U} - \mathcal{N}_{2k,G}\|_\diamond = 0 \quad (\text{B1})$$

Proof. Since the Ginibre ensemble is left and right unitarily invariant, its action maps between irreps of the commutant of the unitary group. In particular, this commutant algebra has bounded dimensions ($k!$ for fixed k) as the dimension N goes to infinity. We express general normalized PSD symmetrized input in terms of diagrams

$$\rho = \left(\sum_{\sigma} c_{\sigma} \frac{\mathbf{O}_{\sigma}}{\|\mathbf{O}_{\sigma}\|_2} \right) \left(\sum_{\sigma} c_{\sigma} \frac{\mathbf{O}_{\sigma}}{\|\mathbf{O}_{\sigma}\|_2} \right)^{\dagger} \quad \text{such that} \quad \text{Tr}[\rho] = 1. \quad (\text{B2})$$

The normalization can be determined by

$$1 = \text{Tr} \left[\left(\sum_{\sigma} c_{\sigma} \frac{\mathbf{O}_{\sigma}}{\|\mathbf{O}_{\sigma}\|_2} \right) \left(\sum_{\sigma} c_{\sigma} \frac{\mathbf{O}_{\sigma}}{\|\mathbf{O}_{\sigma}\|_2} \right)^{\dagger} \right] = \sum_{\sigma} |c_{\sigma}|^2 + (\text{cross terms.}) \quad (\text{B3})$$

$$\stackrel{N \rightarrow \infty}{=} \sum_{\sigma} |c_{\sigma}|^2. \quad (\text{B4})$$

The second line uses that, in the large N limit, the cross terms vanish since different permutations are orthogonal in the limit

$$\text{Tr}[\mathbf{O}_{\sigma} \mathbf{O}_{\sigma'}^{\dagger}] = \mathcal{O}\left(\frac{1}{N} \|\mathbf{O}_{\sigma}\|_2 \|\mathbf{O}_{\sigma'}\|_2\right) \quad \text{if } \sigma \neq \sigma'. \quad (\text{B5})$$

Now, we control the difference in 1-norm for any PSD input

$$\begin{aligned} \|(\mathcal{N}_{2k,G} - \mathcal{N}_{2k,U})[\rho]\|_1 &\leq \sum_{\sigma, \sigma'} |c_{\sigma} c_{\sigma'}| \left\| (\mathcal{N}_{2k,G} - \mathcal{N}_{2k,U}) \left[\frac{\mathbf{O}_{\sigma}}{\|\mathbf{O}_{\sigma}\|_2} \frac{\mathbf{O}_{\sigma'}^{\dagger}}{\|\mathbf{O}_{\sigma'}\|_2} \right] \right\|_1 \\ &\leq \left(\sum_{\sigma, \sigma'} |c_{\sigma} c_{\sigma'}| \right) \sup_{\sigma} \frac{\|(\mathcal{N}_{2k,G} - \mathcal{N}_{2k,U})[\mathbf{O}_{\sigma}]\|_1}{\|\mathbf{O}_{\sigma}\|_1}. \quad (\text{Since } \mathbf{O}_{\sigma} \mathbf{O}_{\sigma'}^{\dagger} = \mathbf{O}_{\sigma \sigma'^{-1}}) \end{aligned} \quad (\text{B6})$$

Therefore, it suffices to compare the limiting behavior between two maps on each individual diagrams:

$$\begin{aligned} \|(\mathcal{N}_{2k,G} - \mathcal{N}_{2k,U})[\mathbf{O}_{\sigma}]\|_1 &= \|(\mathcal{N}_{2k,G} - 1)[\mathbf{O}_{\sigma}]\|_1 && (\text{Haar random channel acts identity}) \\ &= \|(\mathcal{N}_{2k,G} - 1)[\mathbf{O}'_{\sigma}]\|_1 + o(1) \|\mathbf{O}_{\sigma}\|_1 \\ &&& (\|\mathbf{O}'_{\sigma} - \mathbf{O}_{\sigma}\|_1 = o(1) \|\mathbf{O}_{\sigma}\|_1 \text{ is subleading in } N) \\ &= \|(\mathcal{N}_{2k,G,G',\dots} - 1)[\mathbf{O}'_{\sigma}]\|_1 + o(1) \|\mathbf{O}_{\sigma}\|_1 && (\text{Decouple distinct blocks}) \\ &= \|(\mathcal{N}_{2k,G,G',\dots} - 1)[\mathbf{O}_{\sigma}]\|_1 + o(1) \|\mathbf{O}_{\sigma}\|_1 && (\text{Restoring } \mathbf{O}_{\sigma}) \\ &= o(1) \|\mathbf{O}_{\sigma}\|_1. && (\text{Since } \mathbb{E}[\mathbf{G} \cdot \mathbf{I} \cdot \mathbf{G}^{\dagger}] = \mathbf{I}) \end{aligned}$$

The second line makes the indices distinct at the $\frac{1}{N}$ cost in 1-norm

$$\mathbf{O}_{\sigma} = \sum_{\Pi \geq \sigma} \mathbf{O}'_{\Pi} \quad \text{such that} \quad \|\mathbf{O}_{\sigma} - \mathbf{O}'_{\sigma}\|_1 \leq \frac{f(k)}{N} \|\mathbf{O}_{\sigma}\|_1 \quad (\text{B7})$$

for some combinatorial factors $f(k)$. (Since each $\mathbf{O}'_{\Pi}$ have all blocks propagating if $\Pi \geq \sigma$, the 1-norm is $\|\mathbf{O}'_{\Pi}\|_1 = M'_{\Pi}$, which is at least $\mathcal{O}(\frac{1}{N})$ smaller than M'_{σ} .) The third line is a decoupling argument: distinct rows of Ginibre matrices are independent. Therefore, the distinct blocks of σ (which are the k wires connecting the bottom to the top) are effectively acted by *independent* pairs of $\mathbf{G}$ s

$$\mathcal{N}_{2k,G}[\mathbf{O}'_{\sigma}] = \mathcal{N}_{2k,G,G',\dots}[\mathbf{O}'_{\sigma}] \quad (\text{B8})$$

where the non-CP map $\mathcal{N}_{2k,G,G',\dots}$, depends on the blocks of σ . The fourth line removes the distinctness constraint at error $\|\mathcal{N}_{2k,G,G',\dots}[\mathbf{O}_{\sigma} - \mathbf{O}'_{\sigma}]\|_1 \leq \|\mathbf{O}_{\sigma} - \mathbf{O}'_{\sigma}\|_1$ (using asymptotic CPTP

property of $\mathcal{N}_{2k, \mathbf{G}, \mathbf{G}', \dots}$, [Lemma IV.3](#)). To conclude the proof for the diamond norm, consider arbitrary inputs with positive and negative parts, recall that the prefactor $\sum_{\sigma, \sigma'} |c_{\sigma} c_{\sigma'}|$ is finite in the large- N limit, and uses that the ancilla dimension for the diamond norm is also independent of N (similar to [Lemma IV.14](#)). $\blacksquare$

Appendix C: Unitary k -designs from k' -wise permutations

Our construction of random unitaries from random permutations can recover efficient unitary k -designs in the diamond distance by replacing the truly random phased permutations with $\tilde{\mathcal{O}}(k)$ -wise independent phased permutations. The goal of this section is to prove this argument as the detailed version of [Corollary I.1](#).

Corollary C.1 (Unitary k -designs from k' -wise independence). *There is a constant c such that for $k \leq 2^{cn}$, an ϵ -approximate quantum unitary k -design can be implemented using*

$$\mathcal{O}(\log^2(k/\epsilon)) \quad \text{one and two-qubit gates and} \quad (\text{C1})$$

$$\mathcal{O}(\log^2(k/\epsilon)) \quad \text{controlled-queries} \quad (\text{C2})$$

to $\mathcal{O}(\log(k/\epsilon))$ -many independent samples of $\mathcal{O}(\epsilon N^{-4k'})$ -approximate k' -wise random permutations and their inverses, and to the $\mathcal{O}(\log(k/\epsilon))$ independent samples of exact $2k'$ -wise random functions $[N] \rightarrow [2k' + 1]$ for some almost linear

$$k' = \mathcal{O}(k \log(k/\epsilon)). \quad (\text{C3})$$

The first step of the argument is to replace the truly random phases in each term of the product with $2k'$ -wise independent phases. If the classical $2k'$ -wise independent phased permutations are exact, then the substitution argument is immediate (even with inverses; [\(C13\)](#)). Indeed, this can be done exactly for the phases by replacing them with efficiently implementable, exact $2k'$ -wise independent phases.

Lemma C.1 ($2k'$ -wise independent phases). *For any integer $0 < k' < 2^{cn}$, consider the set of N evenly spread points on the unit circle*

$$S_N := \{1, e^{i\frac{1}{N}2\pi}, e^{i\frac{2}{N}2\pi}, \dots\}. \quad (\text{C4})$$

Then, a $2k'$ -wise independent function $f : [N] \rightarrow S_N$ acting on the diagonal matches exactly the $2k'$ (mixed) moments of diagonal random phases

$$\mathbb{E}[\mathbf{D}_f^{(\dagger)2k'}] = \mathbb{E}[\mathbf{D}_z^{(\dagger)2k'}]. \quad (\text{C5})$$

Further, $\mathbf{D}_f$ can be implemented using $\tilde{\mathcal{O}}(nk')$ gates.

Proof. First, we use $2k'$ -wise independence to replace f with truly random functions on the diagonal. Now that each of the entries is decoupled, and we merely require the discrete points on the unit circle to reproduce the moments,

$$\mathbb{E}_{S_N}[z^p] = \mathbb{E}_{U(1)}[z^p] = 0 \quad \text{for each integer } |p| \leq 2k' \quad (\text{C6})$$

which can be seen from the properties of the discrete Fourier transform. The implementation cost has two parts: first, the cost of classically evaluating a k' -wise independent function $f : [N] \rightarrow [N]$, which is merely $\tilde{O}(nk')$. This is obtained using the classic construction using a random degree $k' - 1$ polynomial over the field $\mathbb{F}_{2^n}$ [Jof74, WC81, ABI86, AL12]). Second, is the cost of then applying these values in $[N]$ as phases in S_N , which can be done by the usual controlled tower of geometrically decreasing rotations at cost $O(n)$. Third, we then uncompute the function f . The net cost is $\tilde{O}(nk')$. ■

The second step of the argument is to replace the truly random permutations with (approximate) $2k'$ -wise independent permutations. While the independence of the phases can be exact, the best known efficient classical k -wise independent permutation for large values of k is approximate. Thus, we have to demand the classical k -wise independent permutation to achieve very high precision at very low costs to compensate for the distance conversion rates against quantum queries.

Definition C.1 (Classical ϵ -approximate k -wise independent permutations). *We say an ensemble of permutations gives a classical ϵ -approximate k -wise independent permutations if*

$$\left\| \mathbb{E}_{S'} \mathbf{S}'^k |i\rangle - \mathbb{E}_S \mathbf{S}^k |i\rangle \right\|_1 \leq \epsilon \quad \text{for each } i \in [1, N]^k. \quad (\text{C7})$$

In the above, we defined the vector ℓ_1 norm

$$\left\| \sum_i c_i |i\rangle \right\|_1 := \sum_i |c_i| \quad (\text{C8})$$

which captures the statistical distance when applied to the difference of two probability distributions.

In our use cases, the above classical statistical notion of distance is not immediately applicable because (1) the quantum inputs can be entangled and (2) our implementation of the unitary makes adaptive queries to both $\mathbf{S}$ and $\mathbf{S}^{-1}$. Fortunately, the above complication can be circumvented entirely by a powerful black-box result that allows us to effectively use $2k$ -wise independent permutations as *exact* in other parts of the paper, provided the precision is high enough.

Theorem C.1 ([AL12, Theorem 1.1]). *Suppose there exists an ϵ -approximate classical k -wise independent permutation $\mathbf{S}_{\text{approx}}$. Then, there exists an exact classical k -wise independent permutation $\mathbf{S}_{\text{exact}}$ that is $\mathcal{O}(\epsilon \cdot N^{4k})$ -statistically close on the distribution of permutations.*

This Theorem of [AL12] is very powerful, as it allows one to transfer the error ϵ in the k -design to an error in the distinguishing probability of the algorithm. This is by a simple hybrid argument:

it's easy to see that for any distributions D, D' on inputs, the probability a quantum (or classical) algorithm accepts on a random input from D vs D' is upper bounded by twice their total variation distance¹⁴. So given a quantum algorithm $\mathbf{A}$ trying to distinguish our ensemble (built from ϵ -approximate k -wise independent permutations) from Haar, substituting in our ensemble with the same one built with $\mathbf{S}_{exact}$ at most changes the acceptance probability¹⁵ (diamond norm value) by ϵN^{4k} . As we will discuss shortly, ϵ can be set to be exponentially small which makes this change negligible.

Proof of Corollary I.1. Recall that our construction

$$\mathbf{V} := \mathbf{Z}_L \left(\prod_{j=1}^{\ell} e^{i\theta_m \mathbf{A}_m^{(j)}} \right) \mathbf{Z}_R, \quad (\text{C9})$$

can be implemented to precision $\mathcal{O}(\epsilon/k)$ using $2 + m\ell$ -many random samples of k' -wise independent permutations and their inverses (Proposition II.1) with

$$k' = \mathcal{O} \left(k \cdot \underbrace{(\sqrt{m} + \log(k\ell/\epsilon))}_{\text{queries per } e^{i\theta_m \mathbf{A}_m}} \right). \quad (\text{C10})$$

In particular, we may choose (assuming $k \leq 2^{cn}$),

$$m = 2, \quad \ell = \mathcal{O}(\log(k/\epsilon)) \quad \text{such that} \quad \|\mathcal{N}_{2k, \mathbf{V}} - \mathcal{N}_{2k, U_{Haar}}\|_{\diamond} = \mathcal{O} \left(\frac{k^8 \ell^8 (m^4 n^8 + n^8)}{N} + \frac{k^4}{m^{\ell}} \right) \leq \mathcal{O}(\epsilon). \quad (\text{C11})$$

If the classical k -wise independent permutations are exact, then the claim follows even in the presence of inverses $\mathbf{S}^{-1}$ since the partial transpose is linear (and that $\mathbf{S}^{-1} = \mathbf{S}^T$)

$$\mathbb{E}_{\mathbf{S}}[\mathbf{S}^{\otimes k}] = \mathbb{E}_{\mathbf{S}'}[\mathbf{S}'^{\otimes k}] \quad (\text{C12})$$

$$\text{implies} \quad \mathbb{E}_{\mathbf{S}}[\mathbf{S}^{\otimes k_1} \otimes (\mathbf{S}^T)^{\otimes (k-k_1)}] = \mathbb{E}_{\mathbf{S}'}[\mathbf{S}'^{\otimes k_1} \otimes (\mathbf{S}'^T)^{\otimes (k-k_1)}]. \quad (\text{C13})$$

Now, by Theorem C.1, we may simply replace the truly random permutation $\mathbf{S}$ with the exact k -wise independent permutations while paying an additive error ϵ in the distinguishing probability between $\mathbf{S}_{exact}$ and $\mathbf{S}_{approx}$. ■

Lastly, we invoke the highly nontrivial construction of efficient k -wise independent permutations [Kas07, CK23] as a black box. Generators that give Cayley graph expanders for the symmetry group (and others) have been known [Kas07, CK23, BGT11]. These explicit constructions [Kas07, CK23] can also be efficiently evaluated (given n -bit inputs) [CHH⁺]. For our purposes,

¹⁴ This is simply because the probability the quantum algorithm accepts is a bounded function in $[0, 1]$ over the domain – so a change of the input distribution by ϵ can change the value of the expectation by at most 2ϵ .

¹⁵ Here one must invoke data processing inequality as well to say the “lifted” ensembles on unitaries are also close in total variation distance.

the recent elegant construction ([CK23, Theorem 1.5])¹⁶ can be efficiently computed classically using finite field arithmetics on large primes, which in turn gives the following classical circuit complexity on k -wise independent permutations on 2^n many elements.

Theorem C.2 (Efficient classical approximate k -wise independent permutations [Kas07, CK23, CHH⁺]). *There exist classical ϵ -approximate k -wise independent permutations on 2^n elements with time complexity*

$$\mathcal{O}\left(\text{poly}(n)\left(nk + \log\left(\frac{1}{\epsilon}\right)\right)\right). \quad (\text{C14})$$

Therefore, we can take a small error $\epsilon = 1/2^{\Omega(nk)}$ to feed into Theorem C.1 to obtain nearly exact k -wise independent permutations at the overall cost $\mathcal{O}(k \cdot \text{poly} \log(n))$.

1. Bootstrapping nonadaptive designs to adaptive designs

Throughout the paper, we have mostly discussed nonadaptive designs in the sense of the diamond norm. This can be bootstrapped to adaptive security at high enough precision (for example, by iterating the same random unitary many times [CDX⁺24, Lemma XI.7].).

Lemma C.2 (From nonadaptive 1-norm to adaptive queries). *Consider two unitary ensembles. The distinguishing probability for any quantum algorithm using k adaptive queries can be controlled by trace distance for parallel distinguishability with additional dimensional factors:*

$$|\mathbb{E}\mathcal{A}(\mathcal{N}_{2k,U}) - \mathbb{E}\mathcal{A}(\mathcal{N}_{2k,V})| \leq 4^k N^{4k} \cdot \|\mathbb{E}\mathcal{N}_{2k,U} - \mathbb{E}\mathcal{N}_{2k,V}\|_{1-1}. \quad (\text{C15})$$

The above continues to hold if the unitaries at each query are different with $U_1, \dots, U_k$ and $V_1, \dots, V_k$ on both RHS and LHS.

Proof. Consider the super operator entries of the channel

$$\mathcal{A}(\mathcal{N}_{2k,U}) - \mathcal{A}(\mathcal{N}_{2k,V}) = \sum_{i'ijj'} \alpha_{i'ijj'} \langle i' | \delta\mathcal{N}[|i\rangle\langle j|] | j' \rangle. \quad (\text{C16})$$

for $\mathbf{j} = (j_1, \dots, j_k) \in [N]^k$. Expecting dimensional factors, we will content ourselves with bounding the entry-wise coefficients $\alpha_{i'ijj'}$. To do so, consider a polarization argument (Lemma A.2) for each system $(i, i', j, j' \in [1, N])$ that turns it into a weighted sum over CP maps

$$|i'\rangle\langle i| \otimes |j\rangle\langle j'| = \mathbb{E}_{z=\pm 1, \pm i} \left[z \left(|i'\rangle\langle i| + z |j'\rangle\langle j| \right) \otimes \left(|i'\rangle\langle i| + z |j'\rangle\langle j| \right)^\dagger \right]. \quad (\text{C17})$$

In particular, the Kraus operator is bounded as

$$\left(|i'\rangle\langle i| + z |j'\rangle\langle j| \right)^\dagger \left(|i'\rangle\langle i| + z |j'\rangle\langle j| \right) \leq 4\mathbf{I}. \quad (\text{C18})$$

¹⁶ We thank Martin Kassabov for this pointing us to this reference.

Thus, the Kraus operator tensored across systems

$$\mathbf{O}_z := \left(|i'_1\rangle \langle i_1| + z_1 |j'_1\rangle \langle j_1| \right) \otimes \cdots \otimes \left(|i'_k\rangle \langle i_k| + z_k |j'_k\rangle \langle j_k| \right) \quad (\text{C19})$$

and the corresponding CP map (with suitable normalization)

$$\mathcal{N}_z := \frac{1}{4^k} \mathbf{O}_z [\cdot] \mathbf{O}_z^\dagger \quad (\text{C20})$$

define a trace-non-increasing map since $\mathcal{N}_z^\dagger[\mathbf{I}] \leq \frac{1}{4^k} (4\mathbf{I})^{\otimes k} \leq \mathbf{I}$, and thus $\mathcal{A}(\mathcal{N}_z)$ is a “valid experiment,” with some possibility of failure. Thus $|\mathcal{A}(\mathcal{N}_z)| \leq 1$.

Combining the above, we obtain the entry-wise bound

$$|\alpha_{i'ijj'}| = \left| 4^k \mathbb{E}_z z_1 \cdots z_k \mathcal{A}(\mathbf{O}_z) \right| \leq 4^k \mathbb{E}_z |\mathcal{A}(\mathbf{O}_z)| \leq 4^k. \quad (\text{C21})$$

Altogether,

$$|\mathcal{A}(\mathcal{N}_{2k,U}) - \mathcal{A}(\mathcal{N}_{2k,V})| = \left| \sum_{i'ijj'} \alpha_{i'ijj'} \langle i' | \delta \mathcal{N} [|i\rangle \langle j|] | j' \rangle \right| \quad (\text{C22})$$

$$\leq \sum_{i'ijj'} |\alpha_{i'ijj'}| \|\delta \mathcal{N}\|_{1-1} \quad (\text{C23})$$

$$\leq 4^k N^{4k} \|\mathbb{E} \mathcal{N}_{2k,U} - \mathbb{E} \mathcal{N}_{2k,V}\|_{1-1} \quad (\text{C24})$$

as advertised. In fact, the identical argument holds if the unitaries at each query are different with $\mathbf{U}_1, \dots, \mathbf{U}_k$ and $\mathbf{V}_1, \dots, \mathbf{V}_k$ on both RHS and LHS. ■

-
- [ABF⁺24] Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou, *Quantum pseudoentanglement*, 15th Innovations in Theoretical Computer Science Conference (ITCS 2024), Schloss-Dagstuhl-Leibniz Zentrum für Informatik, 2024. [1](#), [2](#)
- [ABI86] Noga Alon, László Babai, and Alon Itai, *A fast and simple randomized parallel algorithm for the maximal independent set problem*, Journal of Algorithms **7** (1986), no. 4, 567–583. [1](#), [60](#)
- [ABW09] Andris Ambainis, Jan Bouda, and Andreas Winter, *Nonmalleable encryption of quantum information*, Journal of Mathematical Physics **50** (2009), no. 4, 042106. [1](#)
- [AGKL23] Prabhanjan Ananth, Aditya Gulati, Fatih Kaleoglu, and Yao-Ting Lin, *Pseudorandom isometries*, arXiv preprint arXiv:2311.02901, 2023. [2](#)
- [AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen, *Pseudorandom (function-like) quantum state generators: New definitions and applications*, Theory of Cryptography Conference, Springer, 2022, pp. 237–265. [2](#)
- [AL12] Noga Alon and Shachar Lovett, *Almost k -wise vs. k -wise independent permutations, and uniformity for general group actions*, Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (Berlin, Heidelberg) (Anupam Gupta, Klaus Jansen, José Rolim, and Rocco Servedio, eds.), Springer Berlin Heidelberg, 2012, pp. 350–361. [60](#)

- [AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen, *Cryptography from pseudorandom quantum states*, Annual International Cryptology Conference, Springer, 2022, pp. 208–236. [2](#)
- [AS04] Scott Aaronson and Yaoyun Shi, *Quantum lower bounds for the collision and the element distinctness problems*, Journal of the ACM (JACM) **51** (2004), no. 4, 595–605. [7](#)
- [BBC⁺01] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald De Wolf, *Quantum lower bounds by polynomials*, Journal of the ACM (JACM) **48** (2001), no. 4, 778–797. [7](#)
- [BCC⁺15] Dominic W Berry, Andrew M Childs, Richard Cleve, Robin Kothari, and Rolando D Somma, *Simulating hamiltonian dynamics with a truncated taylor series*, Physical review letters **114** (2015), no. 9, 090502. [5](#)
- [Bei93] Richard Beigel, *The polynomial method in circuit complexity*, [1993] Proceedings of the Eighth Annual Structure in Complexity Theory Conference, IEEE, 1993, pp. 82–95. [7](#)
- [BFV19] Adam Bouland, Bill Fefferman, and Umesh Vazirani, *Computational pseudorandomness, the worm-hole growth paradox, and constraints on the ads/cft duality*, arXiv preprint arXiv:1910.14646, 2019. [1](#)
- [BGT11] Emmanuel Breuillard, Ben J Green, and Terence Tao, *Suzuki groups as expanders*, Groups, Geometry, and Dynamics **5** (2011), no. 2, 281–299. [61](#)
- [BHH16] Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki, *Local random quantum circuits are approximate polynomial-designs*, Communications in Mathematical Physics **346** (2016), 397–434. [1](#), [4](#), [6](#)
- [BM24] Zvika Brakerski and Nir Magrafta, *Real-valued somewhat-pseudorandom unitaries*, arXiv preprint arXiv:2403.16704, 2024. [2](#)
- [BNOZ22] Eiichi Bannai, Yoshifumi Nakata, Takayuki Okuda, and Da Zhao, *Explicit construction of exact unitary designs*, Advances in Mathematics **405** (2022), 108457. [1](#)
- [BNZZ19] Eiichi Bannai, Mikio Nakahara, Da Zhao, and Yan Zhu, *On the explicit constructions of certain unitary t -designs*, Journal of Physics A: Mathematical and Theoretical **52** (2019), no. 49, 495301. [1](#)
- [BS18] Adam R Brown and Leonard Susskind, *Second law of quantum complexity*, Physical Review D **97** (2018), no. 8, 086015. [2](#)
- [BS19] Zvika Brakerski and Omri Shmueli, *(pseudo) random quantum states with binary phase*, Theory of Cryptography Conference, Springer, 2019, pp. 229–250. [1](#), [2](#), [5](#)
- [BSS01] Howard Barnum, Michael Saks, and Mario Szegedy, *Quantum decision trees and semidefinite programming.*, Tech. report, Los Alamos National Lab.(LANL), Los Alamos, NM (United States), 2001. [7](#)
- [CDB⁺23] Chi-Fang (Anthony) Chen, Alexander M Dalzell, Mario Berta, Fernando GSL Brandão, and Joel A Tropp, *Sparse random hamiltonians are quantumly easy*, 2023. [6](#), [10](#), [11](#), [55](#)
- [CDX⁺24] Chi-Fang Chen, Jordan Docter, Michelle Xu, Adam Bouland, and Patrick Hayden, *Efficient unitary t -designs from random sums*, arXiv preprint arXiv:2402.09335, 2024. [1](#), [5](#), [6](#), [11](#), [55](#), [62](#)
- [CHH⁺] Chi-Fang Chen, Jeongwan Haah, Jonas Haferkamp, Yunchao Liu, Tony Metger, and Xinyu Tan, *In prepration*. [61](#), [62](#)
- [CK23] Pierre-Emmanuel Caprace and Martin Kassabov, *Tame automorphism groups of polynomial rings with property (t) and infinitely many alternating group quotients*, Transactions of the American Mathematical Society **376** (2023), no. 11, 7983–8021. [1](#), [3](#), [61](#), [62](#)

- [CLLW16] Richard Cleve, Debbie W. Leung, Li Liu, and Chunhao Wang, *Near-linear constructions of exact unitary 2-designs*, Quantum Inf. Comput. **16** (2016), no. 9, 721–756. [1](#)
- [CMN22] Benoit Collins, Sho Matsumoto, and Jonathan Novak, *The weingarten calculus*, arXiv preprint arXiv:2109.14890, 2022. [48](#)
- [CvHVT] Chi-Fang Chen, Ramon van Handel, Jorge Garza Vargas, and Joel Tropp, In preparation. [16](#)
- [DCEL09] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine, *Exact and approximate unitary 2-designs and their application to fidelity estimation*, Physical Review A **80** (2009), no. 1, 012304. [1](#)
- [DLT02] David P DiVincenzo, Debbie W Leung, and Barbara M Terhal, *Quantum data hiding*, IEEE Transactions on Information Theory **48** (2002), no. 3, 580–598. [1](#)
- [DP02] Brian A Davey and Hilary A Priestley, *Introduction to lattices and order*, Cambridge university press, 2002. [23](#)
- [EAŻ05] Joseph Emerson, Robert Alicki, and Karol Życzkowski, *Scalable noise estimation with random unitary operators*, Journal of Optics B: Quantum and Semiclassical Optics **7** (2005), no. 10, S347. [1](#)
- [EZ64] H. Ehlich and K. Zeller, *Schwankung von polynomen zwischen gitterpunkten*, Mathematische Zeitschrift **86** (1964), 41–44. [15](#)
- [FTH23] Jiani Fei, Sydney Timmerman, and Patrick Hayden, *Efficient quantum algorithm for port-based teleportation*, arXiv preprint arXiv:2310.01637 (2023). [22](#)
- [GBO23a] Dmitry Grinko, Adam Burchardt, and Maris Ozols, *Efficient quantum circuits for port-based teleportation*, arXiv preprint arXiv:2312.03188 (2023). [22](#)
- [GBO23b] ———, *Gelfand-tsetlin basis for partially transposed permutations, with applications to quantum information*, arXiv preprint arXiv:2310.02252 (2023). [22](#)
- [Gin65] Jean Ginibre, *Statistical Ensembles of Complex, Quaternion, and Real Matrices*, Journal of Mathematical Physics **6** (1965), no. 3, 440–449. [6](#), [10](#)
- [GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe, *Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics*, Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, 2019, pp. 193–204. [5](#), [14](#)
- [GTB23] Tudor Giurgica-Tiron and Adam Bouland, *Pseudorandomness from subset states*, arXiv preprint arXiv:2312.09206, 2023. [2](#)
- [Haf22] Jonas Haferkamp, *Random quantum circuits are approximate unitary t -designs in depth $o(nt^{5+o(1)})$* , Quantum **6** (2022), 795. [1](#)
- [HHJ21] Jonas Haferkamp and Nicholas Hunter-Jones, *Improved spectral gaps for random quantum circuits: large local dimensions and all-to-all interactions*, Physical Review A **104** (2021), no. 2, 022417. [1](#)
- [HHWY08] Patrick Hayden, Michał Horodecki, Andreas Winter, and Jon Yard, *A decoupling approach to the quantum capacity*, Open Systems & Information Dynamics **15** (2008), no. 01, 7–19. [1](#)
- [HJ12] Roger A Horn and Charles R Johnson, *Matrix analysis*, Cambridge university press, 2012. [24](#)
- [HJ19] Nicholas Hunter-Jones, *Unitary designs from statistical mechanics in random quantum circuits*, 2019. [1](#)
- [HJ20] Tom Halverson and Theodore N. Jacobson, *Set-partition tableaux and representations of diagram algebras*, Algebraic Combinatorics **3** (2020), no. 2, 509–538 (en). [11](#), [22](#), [25](#), [36](#), [37](#), [38](#)
- [HKP20] Hsin-Yuan Huang, Richard Kueng, and John Preskill, *Predicting many properties of a quantum system from very few measurements*, Nature Physics **16** (2020), no. 10, 1050–1057. [1](#)

- [HL09a] Aram W Harrow and Richard A Low, *Efficient quantum tensor product expanders and k -designs*, International Workshop on Approximation Algorithms for Combinatorial Optimization, Springer, 2009, pp. 548–561. [1](#)
- [HL09b] ———, *Random quantum circuits are approximate 2-designs*, Communications in Mathematical Physics **291** (2009), 257–302. [1](#)
- [HLT24] Jeongwan Haah, Yunchao Liu, and Xinyu Tan, *Efficient approximate unitary designs from random pauli rotations*, arXiv preprint arXiv:2402.05239, 2024. [1](#), [5](#)
- [HM23] Aram W Harrow and Saeed Mehraban, *Approximate unitary t -designs by short random quantum circuits using nearest-neighbor and long-range gates*, Communications in Mathematical Physics (2023), 1–96. [1](#)
- [HR05] Tom Halverson and Arun Ram, *Partition algebras*, European Journal of Combinatorics **26** (2005), no. 6, 869–921. [11](#), [19](#), [25](#)
- [JBS23] Shao-Kai Jian, Gregory Bentsen, and Brian Swingle, *Linear growth of circuit complexity from brownian dynamics*, Journal of High Energy Physics **2023** (2023), no. 8, 1–42. [1](#)
- [JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song, *Pseudorandom quantum states*, Advances in Cryptology—CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38, Springer, 2018, pp. 126–152. [1](#), [2](#)
- [JMW23] Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu, *Subset states and pseudorandom states*, arXiv preprint arXiv:2312.15285, 2023. [2](#)
- [Jof74] A. Joffe, *On a Set of Almost Deterministic k -Independent Random Variables*, The Annals of Probability **2** (1974), no. 1, 161 – 162. [1](#), [60](#)
- [Kas07] Martin Kassabov, *Symmetric groups and expander graphs*, Inventiones mathematicae **170** (2007), no. 2, 327–354. [1](#), [3](#), [61](#), [62](#)
- [Kes59] Harry Kesten, *Symmetric random walks on groups*, Transactions of the American Mathematical Society **92** (1959), no. 2, 336–354. [49](#)
- [KKS⁺23] Ágoston Kaposi, Zoltán Kolarovszki, Adrian Solymos, Tamás Kozsik, and Zoltán Zimborás, *Constructing generalized unitary group designs*, International Conference on Computational Science, Springer, 2023, pp. 233–245. [1](#)
- [KL17] Shelby Kimmel and Yi-Kai Liu, *Phase retrieval using unitary 2-designs*, 2017 International Conference on Sampling Theory and Applications (SampTA), 2017, pp. 345–349. [1](#)
- [KLR⁺08] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized benchmarking of quantum gates*, Phys. Rev. A **77** (2008), 012307. [1](#)
- [KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal, *Quantum cryptography in algorithmica*, Proceedings of the 55th Annual ACM Symposium on Theory of Computing, 2023, pp. 1589–1602. [1](#)
- [Kre21] William Kretschmer, *Quantum pseudorandomness and classical complexity*, arXiv preprint arXiv:2103.09320, 2021. [1](#)
- [KTP20] Isaac Kim, Eugene Tang, and John Preskill, *The ghost in the radiation: Robust encodings of the black hole interior*, Journal of High Energy Physics **2020** (2020), no. 6, 1–65. [1](#)
- [Kut05] Samuel Kutin, *Quantum lower bound for the collision problem with small range*, Theory of Computing **1** (2005), no. 1, 29–36. [7](#)

- [Low10] Richard A Low, *Pseudo-randomness and learning in quantum computation*, Ph.D. thesis, University of Bristol, UK, 2010, arXiv:1006.5227. [4](#), [23](#)
- [LQS⁺23] Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao, *Quantum pseudorandom scramblers*, arXiv preprint arXiv:2309.08941, 2023. [2](#)
- [Ma23] Fermi Ma, December 2023, Personal communication. [2](#)
- [Mar89] A.A. Markov, *On a problem of d.i. mendelev (russian)*, Zapishi Imp. Akad. Nauk **I12** (1889), 1–24. [15](#)
- [Mar16] V.A. Markov, *Über polynome die in einem gegebenen intervall möglichst wenig von null abweichen*, Math. Annalen **77** (1916), 213–258. [15](#)
- [McK81] Brendan D. McKay, *The expected eigenvalue distribution of a large regular graph*, Linear Algebra and its Applications **40** (1981), 203–216. [49](#)
- [MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen, *Simple constructions of linear-depth t -designs and pseudorandom unitaries*, Personal communication, 2024. [2](#)
- [MY23] Yosuke Mitsuhashi and Nobuyuki Yoshioka, *Clifford group and unitary designs under symmetry*, PRX Quantum **4** (2023), no. 4, 040331. [1](#)
- [Ngu23] Quynh T Nguyen, *The mixed schur transform: efficient quantum circuit and applications*, arXiv preprint arXiv:2310.01613 (2023). [22](#)
- [NHKW17] Yoshifumi Nakata, Christoph Hirche, Masato Koashi, and Andreas Winter, *Efficient quantum pseudorandomness with nearly time-independent hamiltonian dynamics*, Physical Review X **7** (2017), no. 2, 021006. [1](#)
- [NW99] Ashwin Nayak and Felix Wu, *The quantum query complexity of approximating the median and related statistics*, Proceedings of the thirty-first annual ACM symposium on Theory of computing, 1999, pp. 384–393. [7](#)
- [NZO⁺21] Yoshifumi Nakata, Da Zhao, Takayuki Okuda, Eiichi Bannai, Yasunari Suzuki, Shiro Tamiya, Kentaro Heya, Zhiguang Yan, Kun Zuo, Shuhei Tamate, et al., *Quantum circuits for exact unitary t -designs and applications to higher-order randomized benchmarking*, PRX Quantum **2** (2021), no. 3, 030339. [1](#)
- [OBK⁺17] Emilio Onorati, Oliver Buerschaper, Martin Kliesch, Winton Brown, Albert H Werner, and Jens Eisert, *Mixing properties of stochastic quantum hamiltonians*, Communications in Mathematical Physics **355** (2017), 905–947. [1](#)
- [OSP23] Ryan O’Donnell, Rocco A Servedio, and Pedro Paredes, *Explicit orthogonal and unitary designs*, 2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS), IEEE, 2023, pp. 1240–1260. [1](#)
- [Raz03] Alexander A Razborov, *Quantum communication complexity of symmetric predicates*, Izvestiya: Mathematics **67** (2003), no. 1, 145. [7](#)
- [RC66] T. J. Rivlin and E. W. Cheney, *A comparison of uniform approximations on an interval and a finite subset thereof*, SIAM Journal of Numerical Analysis **3** (1966), no. 2, 311–320. [15](#)
- [RY17] Daniel A. Roberts and Beni Yoshida, *Chaos and complexity by design*, Journal of High Energy Physics **2017** (2017), no. 4, 121. [2](#), [4](#)
- [Sag13] Bruce E Sagan, *The symmetric group: representations, combinatorial algorithms, and symmetric functions*, vol. 203, Springer Science & Business Media, 2013. [19](#), [20](#), [23](#)

- [SDTR13] Oleg Szehr, Frédéric Dupuis, Marco Tomamichel, and Renato Renner, *Decoupling with unitary approximate two-designs*, New Journal of Physics **15** (2013), no. 5, 053022. [1](#)
- [WC81] Mark N Wegman and J Lawrence Carter, *New hash functions and their use in authentication and set equality*, Journal of computer and system sciences **22** (1981), no. 3, 265–279. [1](#), [60](#)
- [Web15] Zak Webb, *The clifford group forms a unitary 3-design*, 2015. [1](#)
- [YE23] Lisa Yang and Netta Engelhardt, *The complexity of learning (pseudo) random dynamics of black holes and other chaotic systems*, arXiv preprint arXiv:2302.11013, 2023. [1](#)
- [Zha16] Mark Zhandry, *A note on quantum-secure prps*, 2016. [3](#), [6](#), [15](#)
- [Zhu17] Huangjun Zhu, *Multiqubit clifford groups are unitary 3-designs*, Physical Review A **96** (2017), no. 6, 062336. [1](#)
- [ZKGG16] Huangjun Zhu, Richard Kueng, Markus Grassl, and David Gross, *The clifford group fails gracefully to be a unitary 4-design*, arXiv preprint arXiv:1609.08172, 2016. [1](#)