

Anti-concentration is (almost) all you need

Markus Heinrich,^{1,*} Jonas Haferkamp,^{2,3} Ingo Roth,⁴ and Jonas Helsen⁵

¹*Institute for Theoretical Physics, University of Cologne, Germany*

²*School of Engineering and Applied Science, Harvard University, USA*

³*Department of Mathematics, Saarland University, Germany*

⁴*Quantum Research Center, Technology Innovation Institute, Abu Dhabi, United Arab Emirates*

⁵*QuSoft and CWI, Amsterdam, Netherlands*

Until very recently, it was generally believed that the (approximate) 2-design property is strictly stronger than anti-concentration of random quantum circuits, mainly because it was shown that the latter anti-concentrate in logarithmic depth, while the former generally need linear depth circuits. This belief was disproven by recent results which show that so-called *relative-error* approximate unitary designs can in fact be generated in logarithmic depth, implying anti-concentration. Their result does however not apply to ordinary local random circuits, a gap which we close in this paper, at least for 2-designs. More precisely, we show that anti-concentration of local random quantum circuits already implies that they form relative-error approximate state 2-designs, making them equivalent properties for these ensembles. Our result holds more generally for any random circuit which is invariant under local (single-qubit) unitaries, independent of the architecture.

Random quantum circuits are ubiquitous in quantum information theory, touching a wide range of topics from randomized benchmarking [1–5] to black hole physics [6, 7]. Consequently, significant effort has been devoted to studying the mixing properties of random quantum circuits.

A particular focus of the community concerns the convergence of random quantum circuits to approximate (unitary or state) k -designs. These are probability distributions on the unitary group or state space that appear uniformly random given access to at most k copies. Early works rigorously proved the convergence of random quantum circuits to approximate 2-designs in depth $O(n)$ on n qubits [8, 9]. The convergence was subsequently tied to spectral properties of the k -copy twirling channel [10, 11], although tight bounds were still limited to $k = 2$. Since then, a long line of works extended this result to higher k [12–15], ultimately providing near tight bounds on the k -dependence [16] in this convergence.

At the same time, the linear dependence on the system size was widely considered optimal. This however changed very recently, when it was shown that random quantum circuits already look Haar-random to forward-in-time experiments at logarithmic depth [17, 18].

In hindsight, the rapid onset of *anti-concentration* [19, 20] could be considered as a first hint for the logarithmic convergence of second moments. Anti-concentration of a probability measure ν on unitaries refers, loosely speaking, to the property that the outcome distribution of circuits sampled from ν is ‘well spread’ on average. This property is a key ingredient in complexity-theoretic arguments for sampling-based quantum advantage (see Ref. [21] for a recent review). Anti-concentration is implied by a small value of the (average) *collision probability*

$$Z_\nu = \mathbb{E}_{U \sim \nu} |\langle 0 | U | 0 \rangle|^4. \quad (1)$$

Using a mapping to a statistical mechanics model [22–24], it was shown in Refs. [19, 20] that random quantum circuits with iid gates have a near minimal average collision probability already at log-depth. Although being strictly weaker, we note that anti-concentration is often equated with the convergence of the collision probability in the random circuits literature and we will do the same in this paper.

The logarithmic-depth designs constructed in Refs. [17, 18] can be seen as ‘coarse-grained’ brickwork circuits in the sense that certain entangling blocks are deleted. This raises the question whether this deletion is actually advantageous, or whether it is simply a remnant of the proof technique. Intuitively, the insertion of random gates into the circuit should not slow down the mixing time, but such effects are known to occur in Markov chains. A similar behavior was recently observed in quantum circuits involving Haar-random unitaries that act on an extensive number of qubits [25]. As such, the latter does however not extend to local random quantum circuits.

In this paper, we provide the first evidence that standard random quantum circuit indeed converge as fast as the coarse-grained circuits in Refs. [17, 18] by proving the convergence of standard brickwork random quantum circuits to so-called relative-error approximate *state* 2-designs in logarithmic depth. In other words, we show that in the case of the state 2-design property the extra structure in Refs. [17, 18] is not necessary and that the result of Ref. [25] does not qualitatively apply to local random quantum circuits. Our proof is remarkably short and reduces the relative-error state 2-design property to the convergence of the collision probability (i.e. *anti-concentration*). Interestingly, the inverse implication is always true, hence *anti-concentration is all you need* for the here considered state ensembles. Finally, we also briefly discuss the case of unitary designs and why anti-concentration may generally not be enough there. These

intricacies are illustrated in parallel work [26] which also gives evidence that anti-concentration may nevertheless be enough for the unitary 2-design property in 1D brick-work circuits.

Complementary evidence for the fast convergence of unstructured random quantum circuits was recently obtained in Ref. [27], which shows that the structure of the coarse-grained circuits in Refs. [17, 18] does not change the relative entropy decay too much. This decay then implies designs secure in non-adaptive experiments in depth $\text{polylog}(n)$, even for higher k .

Preliminaries. We consider a system of n qudits of local dimension q . The collision probability (1) is minimal for circuits producing uniform outcome distributions (e.g. a layer of Hadamards), $Z_{\text{uni}} = q^{-2n}$, while for Haar-random unitaries, we have $Z_H = 2q^{-n}(q^n + 1)^{-1}$. We say that ν *anti-concentrates* if $Z_\nu \leq \alpha q^{-2n}$ for some $\alpha \geq 1$. While generally speaking any $\alpha \geq 1$ will do, we consider in the following the case $Z_\nu \leq (1 + \varepsilon)Z_H$ with $\varepsilon \in [0, 1)$. Previous results on anti-concentration of random quantum circuits (RQCs) show that any constant ε can be achieved at the cost of a constant overhead in the total number of gates [19, 20].

A probability measure ν on $U(q^n)$ is called a *relative-error ε -approximate unitary k -design* (or short *relative-error design*) if the k -fold twirling channel $M_{k,\nu} := \mathbb{E}_{U \sim \nu} U^{\otimes k}(\cdot) U^{\dagger \otimes k}$ fulfills the operator inequalities

$$(1 - \varepsilon)M_{k,H} \leq_{\text{CP}} M_{k,\nu} \leq_{\text{CP}} (1 + \varepsilon)M_{k,H}, \quad (2)$$

where $\mathcal{A} \leq_{\text{CP}} \mathcal{B}$ iff $\mathcal{B} - \mathcal{A}$ is completely positive (CP), and the index H refers the integration w.r.t. the Haar measure μ_H on $U(q^n)$. To see that ε is indeed a relative error, consider positive-semidefinite (psd) operators $A, B \geq 0$. Then, the definition (2) implies that

$$\left| \frac{\text{tr}(A M_{k,\nu}(B)) - \text{tr}(A M_{k,H}(B))}{\text{tr}(A M_{k,H}(B))} \right| \leq \varepsilon, \quad (3)$$

i.e. all *psd Haar moments* are approximated within relative error ε . Moreover, we say that the generated state ensemble $\{U|0\rangle\}_{U \sim \nu}$ is a *relative-error ε -approximate state k -design* if Eq. (3) holds for any $A \geq 0$ and $B = |0\rangle\langle 0|^{\otimes k}$ (here $0 \equiv 0^n$ denotes the all-zero state). Setting $k = 2$ and $A = B = |0\rangle\langle 0|^{\otimes 2}$ in Eq. (3), we recover the well-known fact that relative-error (state or unitary) 2-designs with error ε anti-concentrate with $\alpha = 2(1 + \varepsilon)$.

In the following, we study such 2-designs in the spirit of the statistical mechanics model of *local RQCs* [19, 22–24]. Here, a local RQC is a circuit which is composed of Haar-random 2-local unitaries arranged in a prespecified manner. We will assume the RQC is invariant under local, single-qudit unitaries (LU)—this is simply to avoid technicalities on the support of single instances of the RQCs. This is true for many ensembles and can be straightforwardly imposed by a layer of

single-qudit gates at the start of the circuit.

State designs. We show that if a local RQC anti-concentrates, it also forms a relative-error state 2-design:

Theorem 1. *Let ν be the probability measure of a local RQC on n qudits and suppose it anti-concentrates in the sense that $Z_\nu \leq (1 + \varepsilon)Z_H$. Then, ν generates a relative-error ε' -approximate state 2-design, where $\varepsilon' = 2 \frac{q^n + 1}{q^n - q} \frac{\varepsilon}{1 - q^{-1}} \approx 4\varepsilon$.*

The theorem immediately implies that local RQCs in a 1D nearest-neighbor or all-to-all architecture form relative-error state 2-designs in logarithmic depth.

The argument is simple, centered around a single application of Hölder’s inequality. For the sake of notation we set $M_\nu \equiv M_{2,\nu}$ in the following.

Proof. We first establish some facts about the collision probabilities Z_ν and Z_H . Note that the LU invariance implies that $m_\nu := M_\nu(|0\rangle\langle 0|^{\otimes 2})$ commutes with $(U_1 \otimes \dots \otimes U_n)^{\otimes 2}$ for $U_i \in U(q)$. Thus, applying Schur-Weyl duality locally on every qudit, we can expand m_ν in the local permutation basis $\{\mathbb{1}, F\}^{\otimes n}$, where F is the flip operator permuting two tensor copies of \mathbb{C}^q :

$$m_\nu = \sum_{x \in \mathbb{F}_2^n} m_x F_x, \quad (4)$$

with $F_x := \bigotimes_{i=1}^n F^{x_i}$ and \mathbb{F}_2 is the binary field. Denoting the canonical dual basis by $\{\hat{F}_x\}$, we can write the coefficients as $m_x = \text{tr}(\hat{F}_x m_\nu)$. As any F_x acts trivially on $|0\rangle^{\otimes 2}$, we have the relation $Z_\nu = \text{tr}(|0\rangle\langle 0|^{\otimes 2} m_\nu) = \sum_{x \in \mathbb{F}_2^n} m_x$. Note that $m_H := M_H(|0\rangle\langle 0|^{\otimes 2})$ only features contributions from $x = 0$ and $x = 1$, the all-zero and all-one bitstrings. We can thus expand $Z_H = \text{tr}(\hat{F}_0 m_H) + \text{tr}(\hat{F}_1 m_H)$ and use that $M_H = M_H M_\nu$ by the invariance of the Haar measure. Then, we find

$$\begin{aligned} Z_H &= \text{tr} \left((\hat{F}_0 + \hat{F}_1) M_H(m_\nu) \right) \\ &= \sum_{x \in \mathbb{F}_2^n} \text{tr} \left((\hat{F}_0 + \hat{F}_1) M_H(F_x) \right) \text{tr}(\hat{F}_x m_\nu) \\ &= m_0 + m_1 + \sum_{x \notin \{0,1\}} \alpha_{|x|} m_x, \end{aligned} \quad (5)$$

where the last line follows from writing out M_H in the local permutation basis (see the SM for details). Here, $\alpha_{|x|} := \frac{q^{|x|} + q^{n-|x|}}{q^n + 1}$ and $|x|$ is the Hamming weight of the binary vector x . Using that the maximum of α over $x \neq 0, 1$ is attained at $|x| = 1$ and $Z_\nu \leq (1 + \varepsilon)Z_H$, we have

$$\begin{aligned} \sum_{x \notin \{0,1\}} m_x &= Z_\nu - m_0 - m_1 \\ &\leq (1 + \varepsilon)Z_H - Z_H + \alpha_1 \sum_{x \notin \{0,1\}} m_x. \end{aligned}$$

With $\alpha_1 < 1$ we then find the following bound

$$\sum_{x \notin \{0,1\}} m_x \leq \frac{\varepsilon}{1 - \alpha_1} Z_H =: \frac{\varepsilon'}{2} Z_H. \quad (6)$$

Explicitly, we have $\varepsilon' = 2 \frac{q^{n+1}}{q^n - q} \frac{\varepsilon}{1 - q^{-1}}$ where $\frac{q^{n+1}}{q^n - q}$ is quickly converging to 1 from above and $\frac{1}{1 - q^{-1}} \leq 2$. Thus, for sufficiently large n (say $n \approx 10$), $\varepsilon' \approx 4\varepsilon$.

Finally, we bound the relative error of $\text{tr}(A\mathbf{m}_\nu)$ for any psd operator A . For local RQCs, it was shown that $m_x = \text{tr}(\hat{F}_x \mathbf{m}_\nu) \geq 0$ are non-negative numbers depending on the architecture and depth of the circuit [19]. With this and the expansions (4) and (5), a simple application of Hölder's inequality yields

$$\begin{aligned} & |\text{tr}(A\mathbf{m}_\nu) - \text{tr}(A\mathbf{m}_H)| \\ &= \left| \sum_{x \notin \{0,1\}} \left(\text{tr}(AF_x) - \text{tr}(A)\alpha_{|x|} \right) m_x \right| \\ &\leq 2 \text{tr}(A) \sum_{x \notin \{0,1\}} m_x \\ &\leq \varepsilon' \text{tr}(A) Z_H = \varepsilon' \text{tr}(A\mathbf{m}_H), \end{aligned}$$

where we used Eq. (6) in the last line and the fact that $\text{tr}(A\mathbf{m}_H) = \text{tr}(A)Z_H$ since \mathbf{m}_H is proportional to the projector onto the global symmetric subspace. This completes the argument. \square

We think that the factor in front of ε can be improved to 1, as we can rather trivially upper bound $\text{tr}(A\mathbf{m}_\nu)$ using Hölder's inequality as follows:

$$\text{tr}(A\mathbf{m}_\nu) = \sum_x \text{tr}(AF_x) m_x \leq \text{tr}(A) Z_\nu \leq (1 + \varepsilon) \text{tr}(A\mathbf{m}_H).$$

Obtaining the lower bound however requires a more careful analysis.

We remark that our proof works for any measure ν for which the expansion (4) has non-negative coefficients m_x . This is in particular the case for circuits composed of Haar-random 2-local gates as we assumed in Thm. 1, but also for more structured circuits [28].

Unitary designs. Unfortunately, a straightforward extension of the ideas in the last section to the unitary 2-design case is not possible. In fact, we encounter an exponential blow-up in the relation between the collision probability and the design error. To understand why such an argument might be difficult, we will briefly discuss possible strategies in the following. To do so, it will be convenient to change the basis to the one given by the mutually orthogonal local projectors $P_a := \otimes_{i=1}^n P_{a_i}$, $a \in \mathbb{F}_2^n$ with $P_0 = \frac{1}{2}(\mathbb{1} + F)$ and $P_1 = \frac{1}{2}(\mathbb{1} - F)$. We denote their rank as $D_a = 2^{-n} q^n (q - 1)^{|a|} (q + 1)^{n - |a|}$.

Because of the local $U(q)$ invariance and $P_a \geq 0$, it is sufficient to verify Eq. (3) on the *local projector basis* (see

the SM for details). We thus aim to bound the expression

$$\varepsilon \leq \max_{a,b} \frac{|\text{tr}(P_a(\mathbf{M}_\nu - \mathbf{M}_H)(P_b))|}{\text{tr}(P_a \mathbf{M}_H(P_b))}.$$

This already reduces the problem to bounding a finite number of moments. However we found no easy way to do so even for 1D brickwork circuits. Let us now make the simplifying assumption that \mathbf{M}_ν is a psd superoperator. This is true, for instance, for random circuits composed of a single Haar-random local gate per layer, for 1D brickwork circuits with an odd number of layers, or more generally for ensembles that are invariant under inverses (if one is willing to double the depth of the circuit). Under this assumption, Belkin *et al.* [26] show that it is sufficient to probe only the ‘diagonal’ elements in the local projector basis, i.e. the relative error is given by. In fact,

$$\begin{aligned} \varepsilon &= \max_{a,b} \frac{|\text{tr}(P_a(\mathbf{M}_\nu - \mathbf{M}_H)(P_b))|}{\text{tr}(P_a \mathbf{M}_H(P_b))} \\ &= \max_a \frac{\text{tr}(P_a \mathbf{M}_\nu(P_a))}{\text{tr}(P_a \mathbf{M}_H(P_a))} - 1 \\ &= q^n \max_a \left(q^n + (-1)^{|a|} \right) \frac{\text{tr}(P_a \mathbf{M}_\nu(P_a))}{2D_a^2} - 1. \quad (7) \end{aligned}$$

Here, we used that $\mathbf{M}_\nu - \mathbf{M}_H$ is psd since it has the same spectrum as \mathbf{M}_ν , except that two ‘1’ eigenvalues are set to zero. Moreover, $\text{tr}(P_a \mathbf{M}_H(P_a)) = 2D_a^2 q^{-n} / (q^n + (-1)^{|a|})$.

We remark that the term with $a = 0$ exactly corresponds to the relative anti-concentration error $Z_\nu / Z_H - 1$. A priori it is not clear how this error should bound the maximum over all a . Indeed, numerical studies [26] show that the behaviour of the anti-concentration error and the relative design error ε can be very different and generally depends highly on the concrete random circuit ensemble and the connectivity. This indicates that anti-concentration and relative unitary designs might be less related than one might hope from our results on state designs.

Let us add some final remarks on Eq. (7). We can show that $\text{tr}(P_a \mathbf{M}_\nu(P_b)) / D_a$ takes its maximal value at $a = b = 0$ (see SM). The maximum of the remaining factor in Eq. (7) is attained at $a = 1$ for large n . We, thus, see that there is a competition between these two terms. We spent a fair amount of time trying to bound this quantity for 1D random brickwork circuits, using the statistical mechanics approach [19, 23], but failed. This is a source of some embarrassment to the authors, and we welcome any suggestions.

ACKNOWLEDGEMENTS

We thank D. Belkin for fruitful discussions on the unitary design case and for sharing an earlier draft of their work [26]. M.H. acknowledges funding by the Deutsche

Forschungsgemeinschaft (DFG, German Research Foundation) - 54759578 and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 – 390534769. J. Helsen acknowledges funding from the Dutch Research Council (NWO) through a Veni grant (grant No.VI.Veni.222.331) and the Quantum Software Consortium (NWO Zwaartekracht Grant No.024.003.037). The result on state designs was derived by the authors during the 2024 Random Quantum Circuits workshop in Amsterdam.

* markus.heinrich@uni-koeln.de

- [1] J. Emerson, R. Alicki, and K. Życzkowski, Scalable noise estimation with random unitary operators, *Journal of Optics B: Quantum and Semiclassical Optics* **7**, S347 (2005), publisher: IOP Publishing.
- [2] 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, *Physical Review A* **77**, 012307 (2008).
- [3] E. Magesan, J. M. Gambetta, and J. Emerson, Characterizing quantum gates via randomized benchmarking, *Physical Review A* **85**, 042311 (2012).
- [4] J. Helsen, I. Roth, E. Onorati, A. Werner, and J. Eisert, General Framework for Randomized Benchmarking, *PRX Quantum* **3**, 020357 (2022).
- [5] M. Heinrich, M. Kliesch, and I. Roth, Randomized benchmarking with random quantum circuits (2023), 2212.06181.
- [6] A. R. Brown and L. Susskind, Second law of quantum complexity, *Physical Review D* **97**, 086015 (2018), publisher: American Physical Society.
- [7] C. Akers, A. Bouland, L. Chen, T. Kohler, T. Metger, and U. Vazirani, Holographic pseudoentanglement and the complexity of the AdS/CFT dictionary (2024), 2411.04978.
- [8] A. W. Harrow and R. A. Low, Random Quantum Circuits are Approximate 2-designs, *Communications in Mathematical Physics* **291**, 257 (2009).
- [9] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Exact and approximate unitary 2-designs and their application to fidelity estimation, *Physical Review A* **80**, 012304 (2009).
- [10] W. G. Brown and L. Viola, Convergence rates for arbitrary statistical moments of random quantum circuits, *Physical Review Letters* **104**, 250501 (2010), arXiv: 0910.0913.
- [11] W. Brown and O. Fawzi, Scrambling speed of random quantum circuits, arXiv preprint arXiv:1210.6644 (2012).
- [12] F. G. Brandao, A. W. Harrow, and M. Horodecki, Local random quantum circuits are approximate polynomial-designs, *Communications in Mathematical Physics* **346**, 397 (2016).
- [13] A. Harrow and S. Mehraban, Approximate unitary t -designs by short random quantum circuits using nearest-neighbor and long-range gates, *Communications in Mathematical Physics* **401**, 1531 (2023), arXiv:1809.06957.
- [14] J. Haferkamp and N. Hunter-Jones, Improved spectral gaps for random quantum circuits: Large local dimensions and all-to-all interactions, *Physical Review A* **104**, 022417 (2021).
- [15] J. Haferkamp, Random quantum circuits are approximate unitary t -designs in depth $O(nt^{5+o(1)})$, *Quantum* **6**, 795 (2022).
- [16] C.-F. Chen, J. Haah, J. Haferkamp, Y. Liu, T. Metger, and X. Tan, Incompressibility and spectral gaps of random circuits, arXiv preprint arXiv:2406.07478 (2024).
- [17] T. Schuster, J. Haferkamp, and H.-Y. Huang, Random unitaries in extremely low depth, *Science* **389**, 92 (2025).
- [18] N. LaRacuenta and F. Leditzky, Approximate Unitary k -Designs from Shallow, Low-Communication Circuits, in *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 325, edited by R. Meka (Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2025) pp. 69:1–69:2, iSSN: 1868-8969.
- [19] A. M. Dalzell, N. Hunter-Jones, and F. G. S. L. Brandão, Random quantum circuits anti-concentrate in log depth, *PRX Quantum* **3**, 010333, 2011.12277.
- [20] B. Barak, C.-N. Chou, and X. Gao, Spoofing Linear Cross-Entropy Benchmarking in Shallow Quantum Circuits, in *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 185, edited by J. R. Lee (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2021) pp. 30:1–30:20, iSSN: 1868-8969.
- [21] D. Hangleiter and J. Eisert, Computational advantage of quantum random sampling, *Reviews of Modern Physics* **95**, 035001 (2023).
- [22] A. Nahum, S. Vijay, and J. Haah, Operator Spreading in Random Unitary Circuits, *Physical Review X* **8**, 021014 (2018).
- [23] N. Hunter-Jones, Unitary designs from statistical mechanics in random quantum circuits, arXiv:1905.12053 [cond-mat, physics:hep-th, physics:quant-ph] (2019), 1905.12053.
- [24] T. Zhou and A. Nahum, Emergent statistical mechanics of entanglement in random unitary circuits, *Physical Review B* **99**, 174205 (2019).
- [25] D. Belkin, J. Allen, and B. K. Clark, Absence of censoring inequalities in random quantum circuits (2025), arXiv:2502.15995.
- [26] D. Belkin, J. Allen, and B. K. Clark, Apparent universal behavior in 2nd moments of random quantum circuits (2025), to appear on arXiv on 29 October 2025.
- [27] N. Laracuenta, Quantum relative entropy decay composition yields shallow, unstructured k -designs, arXiv preprint arXiv:2510.08537 (2025).
- [28] R. Suzuki, H. Katsura, Y. Mitsuhashi, T. Soejima, J. Eisert, and N. Yoshioka, More global randomness from less random local gates, arXiv preprint arXiv:2410.24127 (2024).

Anti-concentration is (almost) all you need

– *Supplemental material* –

EXPANSIONS IN THE LOCAL PERMUTATION BASIS

Using Schur's lemma and the projectors onto the globally symmetric or antisymmetric subspaces $P_{\vee/\wedge} = \frac{1}{2}(\mathbb{1} + F_1)$ with dimensions $D_{\vee/\wedge} = q^n(q^n \pm 1)/2$, respectively, we find:

$$\begin{aligned} M_H(F_x) &= \frac{\text{tr}(P_{\vee}F_x)}{D_{\vee}}P_{\vee} + \frac{\text{tr}(P_{\wedge}F_x)}{D_{\wedge}}P_{\wedge} \\ &= \left(\frac{\text{tr}(F_x) + \text{tr}(F_1F_x)}{4D_{\vee}} + \frac{\text{tr}(F_x) - \text{tr}(F_1F_x)}{4D_{\wedge}} \right) F_0 + \left(\frac{\text{tr}(F_x) + \text{tr}(F_1F_x)}{4D_{\vee}} - \frac{\text{tr}(F_x) - \text{tr}(F_1F_x)}{4D_{\wedge}} \right) F_1 \\ &= \frac{q^{2n-|x|} - q^{|x|}}{q^{2n} - 1} F_0 + \frac{q^{n+|x|} - q^{n-|x|}}{q^{2n} - 1} F_1 \\ &=: h_{0,x}F_0 + h_{1,x}F_1 \end{aligned} \tag{T1}$$

In particular,

$$h_{0,x} + h_{1,x} = \frac{q^{2n-|x|} - q^{|x|} + q^{n+|x|} - q^{n-|x|}}{q^{2n} - 1} = \frac{(q^n - 1)(q^{n-|x|} + q^{|x|})}{q^{2n} - 1} = \frac{q^{n-|x|} + q^{|x|}}{q^n + 1}.$$

We can write the dual basis explicitly by noting that the local permutation basis factorizes and by using the single-qudit Weingarten matrix:

$$\hat{F}_x = \bigotimes_{i=1}^n \hat{F}_{x_i}, \quad \hat{F}_{x_i} = \sum_{y_i} w_{x_i, y_i} F_{y_i}, \quad w := \frac{1}{q^2 - 1} \begin{pmatrix} 1 & -1/q \\ -1/q & 1 \end{pmatrix}.$$

In particular, $\hat{F}_0 = \frac{1}{q^2-1}(\mathbb{1} - \frac{1}{q}F)$ and $\hat{F}_1 = \frac{1}{q^2-1}(-\frac{1}{q}\mathbb{1} + F)$.

SOME IDENTITIES IN THE LOCAL PROJECTOR BASIS

We can decompose any psd operators A, B which are invariant under local unitaries (LU) by Schur's lemma as

$$A = \sum_{a \in \mathbb{F}_2^n} \frac{A_a}{D_a} P_a, \quad B = \sum_{b \in \mathbb{F}_2^n} \frac{B_b}{D_b} P_b.$$

Here, $A_a = \text{tr}(AP_a) \geq 0$ and $B_b = \text{tr}(BP_b) \geq 0$. Then, assuming that

$$|\text{tr}(P_a M_{\nu}(P_b)) - \text{tr}(P_a M_H(P_b))| \leq \delta \text{tr}(P_a M_H(P_b)),$$

we find using triangle inequality and positivity of the coefficients:

$$|\text{tr}(AM_{\nu}(B)) - \text{tr}(AM_H(B))| \leq \sum_{a,b} \frac{A_a B_b}{D_a D_b} |\text{tr}(P_a M_{\nu}(P_b)) - \text{tr}(P_a M_H(P_b))| \leq \delta \text{tr}(AM_H(B)).$$

As in Eq. (T1), we can compute the Haar moments for $A = P_a$ and $B = P_b$ and find that the projectors have to have support in the same global irrep, meaning that $|a|$ and $|b|$ have to be both even or both odd. Then,

$$\text{tr}(P_a M_H(P_b)) = D_a D_b \times \begin{cases} D_{\vee}^{-1} & \text{if } |a|, |b| \text{ even} \\ D_{\wedge}^{-1} & \text{if } |a|, |b| \text{ odd} \\ 0 & \text{else} \end{cases}.$$

We note that the LU-invariance of ν also implies that $\text{tr}(P_a M_{\nu}(P_b)) = 0$ whenever the parity of $|a|$ and $|b|$ are not equal. To see this, note that by the definition of M_{ν} , we have $M_{\nu}(F_1 B) = F_1 M_{\nu}(B)$. Recall that F_1 is the global flip, thus $\text{tr}(P_a M_{\nu}(P_b)) = \text{tr}(P_a M_{\nu}(P_{\vee/\wedge} P_b)) = \text{tr}(P_a P_{\vee/\wedge} M_{\nu}(P_b))$ where \vee/\wedge is chosen according to the parity of b .

Note that the $\{P_a\}$ basis is orthogonal and $\hat{P}_a = P_a/D_a$ is its dual basis. This basis is exactly the Fourier transform of the local permutation basis $\{F_x\}$:

$$P_a = \bigotimes_{i=1}^n (\mathbb{1} + (-1)^{a_i} F) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x} F_x, \quad \hat{P}_b = \frac{1}{D_b} P_b = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot y} \hat{F}_y.$$

Hence the matrix representation of M_ν in the local projector basis, $\tilde{m}_{a,b} = \text{tr}(\hat{P}_a M_\nu(P_b)) = \text{tr}(P_a M_\nu(P_b))/D_a$, is just the Fourier transform of its representation in permutation basis. The latter can be understood as a non-negative function on $\mathbb{F}_2^n \times \mathbb{F}_2^n$. We can thus invoke Bochner's theorem to conclude that the matrix $\tilde{A}_{c,d}^{a,b} := \tilde{m}_{a+c,b+d}$ is psd. In particular, we have the non-negativity of the principal minor

$$0 \leq \begin{vmatrix} \tilde{m}_{0,0} & \tilde{m}_{a+c,b+d} \\ \tilde{m}_{a+c,b+d} & \tilde{m}_{0,0} \end{vmatrix} = \tilde{m}_{0,0}^2 - \tilde{m}_{a+c,b+d}^2,$$

thus $\tilde{m}_{0,0} \geq \tilde{m}_{a,b}$ for all a, b . We can then write Eq. (7) of the main text as

$$\varepsilon = \frac{q^n}{2} \max_a \tilde{m}_{a,a} \frac{q^n + (-1)^{|a|}}{2D_a} - 1.$$

As we have shown above the term $\tilde{m}_{a,a}$ is maximized by $a = 0$, while the maximum of the other, at least for large n , is given by $a = 1$.