Identity Check Problem for Shallow Quantum Circuits

Sergey Bravyi
IBM Quantum, IBM T.J. Watson Research Center, Yorktown Heights, NY, USA

Natalie Parham
Columbia University, USA

Minh Tran
IBM Quantum, IBM T.J. Watson Research Center, Yorktown Heights, NY, USA

Abstract

Verifying that a quantum circuit correctly implements a desired transformation is essential for validating quantum algorithms. We consider the closely related identity check problem: given a quantum circuit U, estimate the diamond-norm distance between U and the identity channel. Ji and Wu showed that estimating this distance to within an *additive* $1/\mathsf{poly}$ error is QMA-hard, even when U is constant-depth and 1D local – ruling out efficient algorithms in this regime.

We show that this hardness barrier disappears if one seeks a constant *multiplicative*-approximation instead. We present a classical algorithm that, for shallow geometrically local D-dimensional circuits, approximates the distance to the identity within a factor $\alpha = D + 1$, provided that the circuit is sufficiently close to the identity. The runtime of the algorithm scales linearly with the number of qubits for any constant circuit depth and spatial dimension.

We also show that the operator-norm distance to the identity $\|U - I\|$ can be efficiently approximated within a factor $\alpha = 5$ for shallow 1D circuits and, under a certain technical condition, within a factor $\alpha = 2D + 3$ for shallow D-dimensional circuits. A numerical implementation of the identity check algorithm is reported for 1D Trotter circuits with up to 100 qubits.

2012 ACM Subject Classification Theory of computation → Quantum computation theory; Theory of computation → Quantum complexity theory

Keywords and phrases Quantum computing, Identity check problem, quantum circuits, classical simulation of quantum computation, shallow circuits

Digital Object Identifier 10.4230/LIPIcs.ITCS.2026.27

Related Version *Full Version*: `https://arxiv.org/pdf/2401.16525`

Funding *Natalie Parham*: NP is supported by AFOSR award FA9550-21-1-0040, NSF CAREER award CCF-2144219, and the Sloan Foundation.

Acknowledgements SB thanks Steven Flammia and Kristan Temme for helpful discussions. MCT thanks Kunal Sharma for helpful discussions. This work was partially completed while NP was interning at IBM Quantum.

1 Introduction

A fundamental task in the analysis of quantum algorithms and devices is to determine whether a given quantum circuit U implements the intended unitary transformation V. In practice, exact implementation is rarely possible. Common sources of errors include:

1. *Hardware noise:* Imperfect control and decoherence during execution.
2. *Compilation error:* Approximations introduced when mapping the target circuit into a device's native gate set.

3. *Algorithmic error:* Inherent approximations in the algorithm itself. For example, *Hamiltonian simulation* aims to implement the time evolution e^{iHt} of a quantum system with Hamiltonian H. A common method, *Trotterization* approximates this evolution by sequentially applying simpler unitary operations corresponding to terms in H, set by parameters such as the number of Trotter steps. Adjusting these parameters trades off between simulation accuracy and resource cost.

Efficiently estimating how close the implemented circuit U is to the ideal unitary V is therefore crucial both for validating quantum algorithms and for tuning algorithmic or device parameters to improve overall performance. For any unitarily invariant norm $\|U - V\| = \left\|U^\dagger V - I\right\|$, so this task is equivalent to estimating the distance from $U^\dagger V$ to the identity. This latter formulation is known as the *identity check problem*.

Unfortunately, estimating this distance between n-qubit unitaries is computationally difficult. Rosgen and Watrous showed [11, 10] that estimating the distance between two shallow (with depth logarithmic in n) quantum circuits allowing mixed states is PSPACE-hard. This essentially rules out efficient classical or quantum algorithms. Likewise, Janzing, Wocjan, and Beth established QMA-hardness of estimating the distance between two unitary circuits [5]. Ji and Wu [6] strengthened this by showing that this problem remains QMA-hard even if the circuits are *constant-depth* with only *one-dimensional* qubit connectivity. This may come as a surprise since one-dimensional shallow circuits are easy to simulate classically using Matrix Product States [17].

It is important that the no-go results stated above hold only if the distance between quantum circuits has to be estimated with a small *additive error* scaling inverse polynomially with the number of qubits n. Is it possible that some less stringent approximation of the distance can be computed efficiently? In this work, we show that the answer is YES and report linear-time classical algorithms approximating the diamond-norm and the operator-norm distances between constant-depth geometrically-local quantum circuits with a constant *multiplicative error*. Such approximation may be good enough for practical purposes. Note that an estimate of the distance with a constant multiplicative error is informative regardless of how small the distance is. For example, our algorithm can efficiently approximate the distance even if the latter is exponentially small in n. This would be impossible for an algorithm that achieves an additive error approximation scaling inverse polynomially with n.

1.1 Results

We present efficient classical algorithms for estimating the distance from a constant-depth geometrically local circuit to the identity, within a constant multiplicative error. We consider two notions of distance: the diamond norm and operator norm distance measures.

Geometrically-local circuits

We assume our circuits are D-dimensional geometrically local circuits, meaning the following: n qubits are located at cells of a D-dimensional rectangular array. The circuit is composed of single-qubit and two-qubit gates acting on nearest-neighbors cells (cells i and j are called nearest-neighbors if one can go from i to j by changing a single coordinate by ± 1). A depth-h circuit consists of h layers of gates such that within each layer all gates are disjoint.

1.1.1 Diamond-norm identity check

Our main result is in terms of the diamond-norm distance [1].

▶ **Definition 1.** *The diamond-norm distance between U and the identity operation is defined as*

$$\delta(U) = \max_{\rho} \|(U \otimes I)\rho(U^\dagger \otimes I) - \rho\|_1 \tag{1}$$

where $\|\cdot\|_1$ is the trace norm, I is the n-qubit identity, and the maximization is over all $2n$-qubit states ρ.

Operationally, $\delta(U)/2$ is the maximum total variation distance by which the output distribution of any experiment using a single call to U can change if U is replaced by the identity [1, 2].

▶ **Theorem 2** (Diamond-norm identity check algorithm)**.** *Given the description of an n-qubit D-dimensional circuit U of depth h, our algorithm runs in time*

$$T \sim n2^{12(2hD)^D} \tag{2}$$

and outputs a γ such that:

$$\delta(U) \le \gamma \le \alpha\delta(U), \tag{3}$$

where

$$\alpha = \begin{cases} D+1, & \text{if } \delta(U) < 2 \\ 1.16(D+1) & \text{otherwise} \end{cases}. \tag{4}$$

In particular, the runtime is linear in n for any constant circuit depth h and spatial dimension D. We note that achieving an approximation ratio $\alpha = 1+\epsilon$ with $\epsilon = poly(1/n)$ is at least as hard as approximating the distance $\delta(U)$ with an additive error $poly(1/n)$. The latter problem is known to be QMA-hard even in the case of constant-depth 1D circuits [6] which rules out efficient algorithms. An interesting open problem is whether an efficient classical or quantum algorithm can obtain an approximation $\alpha = 1+\epsilon$ for any constant $\epsilon > 0$. If true, this would provide a Polynomial Time Approximation Scheme [16] for the identity check problem.

1.1.2 Phase-sensitive identity check

While the diamond norm captures the worst-case distinguishability of U from the identity, it is insensitive to a global phase. In many quantum algorithms, such as Quantum Phase Estimation [9] or Krylov subspace algorithms [4, 13, 7] this phase matters since the circuit may be applied controlled on ancillary qubits. In such settings, $\delta(U)$ can be small (or even zero) while the operator-norm $\|U - I\|$, the largest singular value of $U - I$, can be large – for example, when $U = e^{i\varphi}I$.

This motivates a phase-sensitive version of the identity check problem where the goal is to estimate the operator-norm distance to within a constant multiplicative factor. We show that this is possible given one additional piece of information: any point t in the *eigenvalue polygon* P_U of U, meaning the convex hull of all the eigenvalues of U (see Figure 1).

▶ **Theorem 3** (Phase-sensitive identity check algorithm)**.** *Given the description of an n-qubit D-dimensional circuit U of depth h, and a point $t \in P_U$, our algorithm runs in time $T \sim n2^{12(2hD)^D}$ and outputs a γ_{op} such that*

$$\|U - I\| \le \gamma_{op} \le \alpha_{op} \|U - I\|. \tag{5}$$

where $\alpha_{op} = 1 + 2\alpha$, for the value of α stated in Theorem 2.

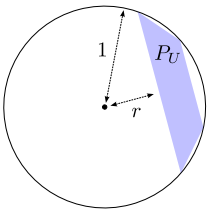

Figure 1 Eigenvalue polygon P_U whose vertices are eigenvalues of U. The diamond-norm distance between U and the identity channel is $\delta(U) = 2\sqrt{1-r^2}$, where r is the distance between P_U and the origin [1]. If P_U does not contain the origin then $\delta(U)$ coincides with the diameter of P_U. Otherwise, $\delta(U) = 2$.

In many cases, efficiently computing some $t \in P_U$ is feasible. If one can efficiently compute $\mathrm{Tr}(\rho U)$ for some n-qubit state ρ, then $\mathrm{Tr}(\rho U) \in P_U$ can serve as the point t required by our phase-sensitive algorithm. This is because the diagonal elements of ρ in the eigenbasis of U is a probability distribution, making $\mathrm{Tr}(\rho U) \in P_U$ a convex combination of U's eigenvalues. Such efficient computability of $\mathrm{Tr}(\rho U)$ holds in several natural cases:

- **1D Shallow cirucits:** If U is a 1D shallow circuit, one can choose ρ as an arbitrary product state. Since U is a Matrix Product Operator with a bond dimension $2^{O(h)}$ one can compute $\mathrm{Tr}(\rho U)$ efficiently using algorithms based on Matrix Product States [12] as long as $h = O(\log n)$. In the 1D case Eqs. (4,3) give $\alpha = 2$ and $\alpha_{op} = 5$ while the runtime of the algorithm is $T \sim n2^{O(h)}$, see Eq. (2).
- **Certain Trotter circuits simulating local Hamiltonian time evolution:** suppose U is a Trotter circuit describing time evolution of a D-dimensional Hamiltonian composed of local Pauli terms $XX + YY$, ZZ, and Z that preserve the Hamming weight. Then the all-zeros state $|0^n\rangle$ is a common eigenvector of each individual gate in U and one can choose ρ as the all-zeros state, that is, $t = \langle 0^n|U|0^n\rangle$. From Eqs. (4,3) one gets $\alpha_{op} = 2D + 3$.

In general, the above gives an efficient algorithm approximating $\|U - I\|$ within a factor $\alpha_{op} = 2D + 3$ for D-dimensional constant-depth circuits provided that one can efficiently find at least one point in the eigenvalue polygon P_U.

1.1.3 Circuit depth – runtime tradeoffs

The exponential runtime dependence on circuit depth limits our algorithm to very shallow circuits. However, it can be extended to deeper circuits U using the divide-and-conquer strategy. Namely, if $U = U_\ell \cdots U_2 U_1$ where each layer U_i has depth $O(1)$, the triangle inequality gives

$$\delta(U) \le \sum_{i=1}^{\ell} \delta(U_i) \le \sum_{i=1}^{\ell} \gamma_i$$

where each γ_i is an upper bound on $\delta(U_i)$ computed by our algorithm. The runtime for computing this upper bound on $\delta(U)$ scales only linearly with the depth of U but we can no longer guarantee that the upper bound is tight within a constant factor. Other tradeoffs between the runtime and the upper bound tightness are discussed in Section 5.

1.2 Open questions and further directions

1. **Improving the approximation ratio** Can an efficient classical or quantum algorithm obtain a multiplicative approximation $\alpha = 1 + \epsilon$ for any constant $\epsilon > 0$? If so, this would provide a Polynomial Time Approximation Scheme [16] for the identity check problem.
2. **Non-geometrically local circuits** Our algorithm scales double-exponentially with the spatial dimension D. Is it possible to remove the dependence on D so that the problem can be efficiently solved for non-geometrically local circuits?
3. **Additive constant error** Ji and Wu show that for constant-depth 1D circuits, solving the identity check problem to within $1/\mathsf{poly}(n)$ additive error is QMA-hard [6]. Is it possible to estimate this efficiently up to constant additive error?
4. **Non-unitary circuits** Our algorithm only considers the case where the circuit consists of unitary gates. Furthermore, one could also ask what is the distance between two quantum *channels*.

1.3 Lower bounds on the distance to the identity

Although this work primarily focuses on computing upper bounds on the distance to the identity, as required for validation of quantum algorithms, efficiently computable lower bounds on the distance are also of interest. Density Matrix Renormalization Group (DMRG) algorithms [12] provide a powerful tool for computing lower bounds on the distance $\delta(U)$ or $\|U - I\|$ for 1D shallow circuits U. Indeed, one can easily check that the squared distance $\|U - I\|^2$ coincides with the largest eigenvalue of a Hamiltonian $H = 2I - U - U^\dagger$. If U is a depth-h 1D circuit then H is a Matrix Product Operator (MPO) with a bond dimension $2^{O(h)}$. In practice, extremal eigenvalues of MPO Hamiltonians with a small bond dimension can be well approximated using DMRG algorithms [12]. However, since DMRG is a variational algorithm, it only provides a lower bound on the distance $\|U - I\|$. To lower bound the diamond-norm distance we use a bound

$$\delta(U) \geq \|U \otimes U^\dagger - I \otimes I\|,$$

with the equality if $\delta(U) < 2$, see Section 2. Thus $\delta(U)^2$ is lower bounded by the maximum eigenvalue of an MPO Hamiltonian $H = 2I \otimes I - U \otimes U^\dagger - U^\dagger \otimes U$ which can in turn be lower bounded using DMRG algorithm. We leave the study of lower bounds based on DMRG algorithms for a future work.

1.4 Paper organization

The rest of the paper is organized as follows. Section 2 describes bounds on the diamond-norm and operator-norm distances $\delta(U)$ and $\|U - I\|$ that can be expressed in terms of commutators between U and certain observables. This section also sketches main ideas behind our algorithm. Section 3 collects some basic facts about shallow quantum circuits and D-dimensional partitions. Section 4 proves a technical lemma which relates the norms of global and local commutators. Our identity check algorithm and its analysis is presented in Section 5. Finally, Section 6 reports a software implementation of our algorithm.

2 Commutator-based bounds

Our identity check algorithm borrows many ideas from the recent breakthrough work by Huang, Liu, et al. [3] on learning shallow quantum circuits. The main ingredients of our algorithm, described below, are bounds on the diamond-norm distance $\delta(U)$ that depend on the norm of commutators between U and certain observables composed of SWAP gates. These bounds and their proof are largely based on Ref. [3].

Consider $2n$ qubits labeled by integers $1,\ldots,2n$. Let W_i be the SWAP gate applied to qubits i and $i+n$. Given a subset $A \subseteq [n]$, define a $2n$-qubit operator

$$W_A = \prod_{i\in A} W_i.$$

By definition, W_A acts non-trivially on $2|A|$ qubits.

▶ **Lemma 4.** *Let $[n] = A_1 \ldots A_m$ be a partition of n qubits into m disjoint subsets and U be a unitary operator acting on n qubits. Define a quantity*

$$\gamma = \sum_{j=1}^{m} \|W_{A_j}(U\otimes I)W_{A_j}(U^\dagger \otimes I) - I\otimes I\|. \tag{6}$$

Then

$$\delta(U) \le \gamma \le m\delta(U) \tag{7}$$

assuming that $\delta(U) < 2$ and

$$\delta(U) \le 1.16\gamma \le 1.16m\delta(U) \tag{8}$$

in the general case.

The quantity γ defined in Eq. (6) or its rescaled version 1.16γ will be the desired estimator of the distance $\delta(U)$. In the next section we show how to choose a partition $[n] = A_1 \ldots A_m$ with $m = D+1$ parts such that each subset A_j is a union of well-separated hypercubes of linear size $O(hD)$ and all commutators $W_{A_j}(U\otimes I)W_{A_j}(U^\dagger\otimes I)$ that appear in Eq. (6) are tensor products of local commutators supported on individual hypercubes. Our construction is based on Ref. [19] which introduced so-called reclusive partitions of the D-dimensional Euclidean space. The key ingredient of our algorithm is an additivity lemma stated in Section 4. This lemma expresses the norm of commutators $\|W_{A_j}(U\otimes I)W_{A_j}(U^\dagger\otimes I) - I\otimes I\|$ in terms of the norm of analogous local commutators supported on individual hypercubes. Each local commutator acts on a subset of at most $O(hD)^D$ qubits and its eigenvalues can be computed by the exact diagonalization. The additivity lemma then provides a linear time algorithm for computing the norm of global commutators $\|W_{A_j}(U\otimes I)W_{A_j}(U^\dagger\otimes I) - I\otimes I\|$ which is all we need to compute the estimator γ defined in Lemma 4.

The next lemma shows that estimation of the operator-norm distance can be reduced to estimation of diamond-norm distance given any point in the eigenvalue polygon of U.

▶ **Lemma 5.** *Let $t \in P_U$ be any point in the eigenvalue polygon of U and α,γ be real numbers such that $\delta(U) \le \gamma \le \alpha\delta(U)$. Then*

$$\gamma_{op} = \gamma + |t-1|$$

obeys

$$\|U-I\| \le \gamma_{op} \le (1+2\alpha)\|U-I\|.$$

In the rest of this section we prove Lemma 4 and 5.

Proof of Lemma 4. Consider first the case $\delta(U) < 2$. We claim that in this case

$$\delta(U) = \|U \otimes U^\dagger - I \otimes I\|. \tag{9}$$

Indeed, since $\delta(U) < 2$, the eigenvalue polygon P_U does not contain the origin and thus $\delta(U)$ coincides with the diameter of P_U, see Fig. 1. Let $\{e^{i\varphi_a}\}_a$ be eigenvalues of U. By definition, P_U is the convex hull of points $\{e^{i\varphi_a}\}_a$. Hence the diameter of P_U coincides with the maximum distance between eigenvalues of U. This shows that

$$\begin{aligned}\delta(U) &= \mathrm{diam}(P_U) = \max_{a,b} |e^{i\varphi_a} - e^{i\varphi_b}| \\ &= \max_{a,b} |e^{i(\varphi_a - \varphi_b)} - 1| \\ &= \|U \otimes U^\dagger - I \otimes I\|.\end{aligned}$$

To get the last equality we noted that $\{e^{i(\varphi_a-\varphi_b)}-1\}_{a,b}$ is the set of eigenvalues of $U\otimes U^\dagger - I\otimes I$.

Let us agree that the tensor product in Eq. (9) separates two n-qubit registers that span qubits $\{1,\ldots,n\}$ and $\{n+1,\ldots,2n\}$. Let $W = \prod_{i=1}^n W_i$ be an operator that swaps the two registers. Since the operator norm is unitarily invariant, Eq. (9) gives

$$\begin{aligned}\delta(U) &= \|(U \otimes U^\dagger - I \otimes I)W\| \\ &= \|(U \otimes I)W(U^\dagger \otimes I) - W\|.\end{aligned} \tag{10}$$

Here we noted that $(I \otimes U^\dagger)W = W(U^\dagger \otimes I)$. The triangle inequality implies that for any unitary operators P_j, Q_j one has

$$\|P_1 P_2 \cdots P_m - Q_1 Q_2 \cdots Q_m\| \le \sum_{j=1}^m \|P_j - Q_j\|. \tag{11}$$

Choosing $P_j = (U \otimes I)W_{A_j}(U^\dagger \otimes I)$, $Q_j = W_{A_j}$, and noting that $W = \prod_{j=1}^m W_{A_j}$ one arrives at

$$\delta(U) \le \sum_{j=1}^m \|(U \otimes I)W_{A_j}(U^\dagger \otimes I) - W_{A_j}\| = \gamma. \tag{12}$$

The last equality uses the fact that W_{A_j} are both hermitian and unitary, which implies $\|O - W_{A_j}\| = \|W_{A_j}O - I\|$ for any operator O. The dual characterization of the diamond-norm [18] gives

$$\delta(U) = \max_{V\,:\,\|V\|\le 1} \|(U \otimes I)V(U^\dagger \otimes I) - V\| \tag{13}$$

where the maximization is over $2n$-qubit operators V. Since $\|W_{A_j}\| = 1$ one infers that

$$\|(U \otimes I)W_{A_j}(U^\dagger \otimes I) - W_{A_j}\| \le \delta(U)$$

for all j and thus $\gamma \le m\delta(U)$. This concludes the proof in the case $\delta(U) < 2$.

Suppose now that $\delta(U) = 2$. Then the eigenvalue polygon P_U contains the origin, see Fig. 1. Let $\{e^{i\varphi_a}\}_a$ be the eigenvalues of U. We claim that there exist eigenvalues $e^{i\varphi_0}, e^{i\varphi_1}$ of U such that the shortest arc length between them is at least $2\pi/3$. Otherwise, all eigenvalues

would lie within an arc of length $2\pi/3$, 1/3 of the unit circle – but this would imply that P_U does not contain the origin. Thus

$$\begin{aligned}\|U \otimes U^\dagger - I \otimes I\| &= \max_{a,b} |e^{i(\varphi_a - \varphi_b)} - 1| && (14)\\ &\geq |e^{i(\varphi_0 - \varphi_1)} - 1| && (15)\\ &\geq |e^{i2\pi/3} - 1| && (16)\\ &= 2\sin(\pi/3) = \sqrt{3}. && (17)\end{aligned}$$

Therefore we have

$$\gamma \geq \|U \otimes U^\dagger - I \otimes I\| \geq \sqrt{3} \tag{18}$$

so

$$\frac{2}{\sqrt{3}}\gamma \geq 2 = \delta(U). \tag{19}$$

Furthermore, our proof of the upper bound $\gamma \leq m\delta(U)$ is unchanged when $\delta(U) = 2$. The desired bound, Eq. (8) follows since $1.16 \geq \frac{2}{\sqrt{3}}$. ◀

Proof of Lemma 5. Let $\{e^{i\varphi_a}\}_a$ be eigenvalues of U and $t = \sum_a p_a e^{i\varphi_a}$, where $p_a \geq 0$ and $\sum_a p_a = 1$. We have

$$\begin{aligned}\|U - I\| &= \|U - tI + tI - I\|\\ &\leq |t-1| + \|\sum_a p_a (U - e^{i\varphi_a} I)\|\\ &\leq |t-1| + \sum_a p_a \|U - e^{i\varphi_a} I\|\\ &\leq |t-1| + \max_a \|U - e^{i\varphi_a} I\|\\ &= |t-1| + \max_{a,b} |e^{i\varphi_a} - e^{i\varphi_b}|\\ &\leq |t-1| + \delta(U) \leq |t-1| + \gamma.\end{aligned}$$

Conversely, it is well known [1] that $\delta(U) \leq 2\|U - I\|$ for any untary U. Thus

$$\begin{aligned}|t-1| + \gamma &= \left|\sum_a p_a (e^{i\varphi_a} - 1)\right| + \gamma\\ &\leq \sum_a p_a |e^{i\varphi_a} - 1| + \alpha\delta(U)\\ &\leq \max_a |e^{i\varphi_a} - 1| + 2\alpha\|U - I\|\\ &= (1 + 2\alpha)\|U - I\|.\end{aligned}$$

◀

3 Lightcones and reclusive partitions

Given a quantum circuit U acting on n qubits, the lightcone $\mathcal{L}(j)$ of a qubit $j \in [n]$ is defined as the set of all output qubits $i \in [n]$ that can be reached by moving through the circuit diagram forward in time starting from the input qubit j. For example, if U is a one-dimensional circuit of depth h then

$$\mathcal{L}(j) \subseteq [j - h, j + h]. \tag{20}$$

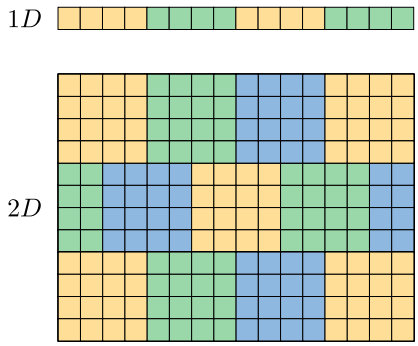

Figure 2 Examples of reclusive partitions for $D = 1, 2$. Qubits are located at cells of a D-dimensional rectangular array. The array is partitioned into $D+1$ sets $A_1, \ldots, A_{D+1}$ such that each set A_j is a disjoint union of D-dimensional cubes of linear size L and the distance between any pair of cubes from the same set A_j is at least L/D. Here $L = 4$. Cubes located near the boundary of the array are truncated. The sets A_1, A_2, A_3 are highlighted in yellow, green, and blue.

For any subset of qubits $S \subseteq [n]$ let $\mathcal{L}(S)$ be the lightcone of S defined as

$$\mathcal{L}(S) = \bigcup_{j \in S} \mathcal{L}(j). \tag{21}$$

We say that a subset of qubits S is the support of an operator O and write $S = \mathrm{supp}(O)$ if O acts trivially on all qubits $j \notin S$. By definition,

$$\mathrm{supp}(UOU^\dagger) \subseteq \mathcal{L}(\mathrm{supp}(O)) \tag{22}$$

for any operator O. Furthermore, $UOU^\dagger = U_{loc} O U_{loc}^\dagger$, where U_{loc} is a "localized" circuit obtained from U by removing all gates acting on qubits outside of the lightcone $\mathcal{L}(\mathrm{supp}(O))$.

Two subsets of qubits S_1 and S_2 are said to be lightcone separated if $\mathcal{L}(S_1) \cap \mathcal{L}(S_2) = \emptyset$. If O_1 and O_2 are operators supported on S_1 and S_2 then $UO_1O_2U^\dagger$ is a product of operators $UO_1U^\dagger$ and $UO_2U^\dagger$ with disjoint supports.

Suppose now that n qubits are located at cells of a D-dimensional rectangular array. We shall consider partitions of the array into D-dimensional cubes known as reclusive partitions [19]. The linear size of each cube in the partition will be chosen as

$$L = 2Dh, \tag{23}$$

where h is the depth of U.

▶ **Lemma 6** (Reclusive Partitions [19]). *One can partition cells of a D-dimensional rectangular array into $D+1$ sets $A_1, \ldots, A_{D+1}$ such that each set A_j is a disjoint union of D-dimensional cubes of linear size L and the distance between any pair of cubes from the same set A_j is at least L/D. The above partition can be constructed efficiently.*

Figure 2 shows examples of 1D and 2D reclusive partitions, see Ref. [19] for the 3D example. We defer the proof of Lemma 6 to Appendix A since it is a simple rephrasing of the results established in [19]. By construction, each cube in the partition contains at most L^D qubits (cubes located near the boundary of the array may be truncated) and any pair of cubes from the same set A_j is lightcone separated due to Eq. (23). Write

$$A_j = A_{j,1} A_{j,2} \ldots A_{j,\ell_j},$$

where ℓ_j is the number of cubes in A_j and $A_{j,p}$ denotes the p-th cube in A_j. By constriction, we have

$$\mathcal{L}(A_{j,p}) \cap \mathcal{L}(A_{j,q}) = \emptyset \quad \text{for all } p \neq q. \tag{24}$$

Since the lightcone of a cube with a linear size L can be enclosed by a cube of linear size $L + 2h$, the number of qubits contained in any lightcone $\mathcal{L}(A_{j,p})$ is bounded as

$$|\mathcal{L}(A_{j,p})| \leq (2h(D+1))^D. \tag{25}$$

Here we used Eq. (23).

Consider the diamond-norm distance $\delta(U)$ and specialize the commutator-based bound of Lemma 4 to the reclusive partition $[n] = A_1 \dots A_{D+1}$. By definition,

$$W_{A_j} = \prod_{p=1}^{\ell_j} W_{A_{j,p}}.$$

Lightcone separation of cubes $A_{j,p}$ implies that operators $(U \otimes I)W_{A_{j,p}}(U^\dagger \otimes I)$ acts on pairwise disjoint subsets of qubits. Thus

$$W_{A_j}(U \otimes I)W_{A_j}(U^\dagger \otimes I) = \prod_{p=1}^{\ell_j} K_{j,p}, \tag{26}$$

where we defined commutators

$$K_{j,p} = W_{A_{j,p}}(U \otimes I)W_{A_{j,p}}(U^\dagger \otimes I).$$

The above shows that $K_{j,p}$ are operators acting on pairwise disjoint subsets of qubits (for a fixed j). Let $U_{j,p}$ be a "localized" circuit obtained from U by replacing all gates acting on at least one qubit outside of the lightcone $\mathcal{L}(A_{j,p})$ with the identity. Then $U_{j,p}$ acts non-trivially only on the lightcone $\mathcal{L}(A_{j,p})$ and

$$K_{j,p} = W_{A_{j,p}}(U_{j,p} \otimes I)W_{A_{j,p}}(U_{j,p}^\dagger \otimes I).$$

The support of $K_{j,p}$ includes all qubits in the left n-qubit register contained in $\mathcal{L}(A_{j,p})$ as well as all qubits in the right n-qubit register contained in $A_{j,p}$. Thus

$$\begin{aligned} |\mathrm{supp}(K_{j,p})| &\leq |\mathcal{L}(A_{j,p})| + |A_{j,p}| \\ &\leq (2h(D+1))^D + (2hD)^D \\ &= (2hD)^D \left[(1+1/D)^D + 1\right] \leq 4(2hD)^D. \end{aligned}$$

Eigenvalues of a unitary operator acting on m qubits can be computed in time $O(2^{3m})$ by the exact diagonalization of a unitary $2^m \times 2^m$ matrix. Thus one can compute all eigenvalues of the commutator $K_{j,p}$ in time

$$T \sim 2^{12(2hD)^D}.$$

In the next section we show that the norm

$$\|W_{A_j}(U \otimes I)W_{A_j}(U^\dagger \otimes I) - I \otimes I\| = \|\prod_{p=1}^{\ell_j} K_{j,p} - I \otimes I\|$$

that appears in the bound of Lemma 4 is a simple function of eigenvalues of individual commutators $K_{j,p}$.

4 Additivity lemma

In this section we show how to compute the norm of commutators that appear in Lemma 4. First, let us introduce some terminology. Let $S^1 = \{z \in \mathbb{CC} : |z| = 1\}$ be the unit circle. If U is a unitary operator, let $\mathsf{eig}(U) \subseteq S^1$ be the set of eigenvalues of U (ignoring multiplicities). Consider $2n$ qubits, a subset $A \subseteq [n]$, and a SWAP operator $W_A = \prod_{i\in A} W_i$ where W_i is the SWAP gate acting on qubits i and $i+n$. Consider a commutator

$$K_A = W_A(U \otimes I)W_A(U^\dagger \otimes I).$$

We claim that $\mathsf{eig}(K_A) = \mathsf{eig}(K_A^\dagger)$. Indeed, $K_A^\dagger = W_A K_A W_A$. Since W_A is both unitary and hermitian, conjugation by W_A does not change the eigenvalue spectrum. Thus eigenvalues of K_A have a form $e^{\pm i\varphi}$ with $0 \le \varphi \le \pi$. For each φ one can choose both positive and negative sign in the exponent. Define a function θ that maps subsets of qubits $A \subseteq [n]$ to real numbers in the interval $[0, \pi]$ such that

$$\theta(A) = \max_{\varphi\in[0,\pi]} \varphi \quad \text{subject to} \quad e^{i\varphi} \in \mathsf{eig}(K_A). \tag{27}$$

Note that $e^{i\theta(A)}$ is the unique eigenvalue of K_A with the maximum distance from 1 and a non-negative imaginary part. Accordingly,

$$\|K_A - I\| = |e^{i\theta(A)} - 1|. \tag{28}$$

We shall need the following simple fact.

▶ **Lemma 7.** *If $\theta(A) \ge \pi/2$ for some subset $A \subseteq [n]$ then $\delta(U) \ge \sqrt{2}$.*

Proof. From $\theta(A) \ge \pi/2$ one infers that K_A has an eigenvalue with a non-positive real part. Since all points on the unit circle within distance less than $\sqrt{2}$ from 1 have a positive real part, one gets $\|K_A - I\| \ge \sqrt{2}$. The dual characterization of the diamond norm [18] gives

$$\begin{aligned}\delta(U) &= \max_{\eta\,:\,\|\eta\|\le 1} \|(U\otimes I)\eta(U^\dagger\otimes I) - \eta\| \\ &\ge \|(U\otimes I)W_A(U^\dagger\otimes I) - W_A\| = \|K_A - I\| \ge \sqrt{2}.\end{aligned}$$

◀

▶ **Definition 8.** *A subset $A \subseteq [n]$ is called good if $\theta(A) < \pi/2$. Otherwise A is called bad.*

The following lemma shows that the function $\theta(A)$ is additive under the union of lightcone-separated subsets, provided that the circuit U is sufficiently close to the identity.

▶ **Lemma 9** (Additivity). *Suppose $A_1, A_2 \subseteq [n]$ are good lightcone-separated subsets. Consider two cases:*
(a) *$\theta(A_1) + \theta(A_2) < \pi/2$,*
(b) *$\theta(A_1) + \theta(A_2) \ge \pi/2$.*
Case (a) implies that the union A_1A_2 is good and

$$\theta(A_1A_2) = \theta(A_1) + \theta(A_2). \tag{29}$$

Case (b) implies that $\delta(U) \ge \sqrt{2}$.

Proof. Define commutators

$$K_p = W_{A_p}(U\otimes I)W_{A_p}(U^\dagger\otimes I)$$

with $p \in \{1,2\}$. Since A_1 and A_2 have lightcone separated, K_1 and K_2 act on disjoint subsets of qubits and thus

$$K_{12} \equiv W_{A_1A_2}(U \otimes I)W_{A_1A_2}(U^\dagger \otimes I) = K_1K_2$$

has the same eigenvalues as the tensor product of K_1 and K_2. In other words,

$$\mathsf{eig}(K_1K_2) = \{z_1z_2 \,:\, z_1 \in \mathsf{eig}(K_1) \quad \text{and} \quad z_2 \in \mathsf{eig}(K_2)\}.$$

By definition, $e^{i\theta(A_p)} \in \mathsf{eig}(K_p)$ for $p = 1, 2$. Thus $e^{i\theta(A_1)+i\theta(A_2)} \in \mathsf{eig}(K_1K_2) = \mathsf{eig}(K_{12})$.

Consider case (a). Let $e^{i\varphi_p} \in \mathsf{eig}(K_p)$ be eigenvalues such that $e^{i\theta(A_1A_2)} = e^{i(\varphi_1+\varphi_2)}$. Then

$$\theta(A_1A_2) = \varphi_1 + \varphi_2 + 2\pi k \tag{30}$$

for some integer k chosen such that $\theta(\sigma_1\sigma_2) \in [0, \pi]$. By definition, $|\varphi_p| \le \theta(A_p)$ and thus

$$|\varphi_1| + |\varphi_2| \le \theta(A_1) + \theta(A_2) < \frac{\pi}{2}.$$

Hence the only integer k in Eq. (30) satisfying $\theta(A_1A_2) \in [0, \pi]$ is $k = 0$, that is, $\theta(A_1A_2) = \varphi_1 + \varphi_2 \le \theta(A_1) + \theta(A_2)$. Conversely, since $e^{i\theta(A_1)+i\theta(A_2)}$ is an eigenvalue of K_{12} and $\theta(A_1) + \theta(A_2) < \pi/2$, one infers that $\theta(A_1A_2) \ge \theta(A_1) + \theta(A_2)$. This proves Eq. (29).

Consider case (b). The same arguments as above show that K_{12} has an eigenvalue $e^{i\varphi}$, where $\varphi = \theta(A_1) + \theta(A_2) \in [\pi/2, \pi)$. Here we used the assumption that both A_1 and A_2 are good, as well as the bound $\theta(A_1) + \theta(A_2) \ge \pi/2$. Hence $\theta(A_1A_2) \ge \pi/2$ and $\delta(U) \ge \sqrt{2}$ by Lemma 7. ◀

By inductive application of the additivity lemma one obtains the following.

▶ **Corollary 10.** *Suppose $A_1, \ldots, A_\ell \subseteq [n]$ are lightcone separated subsets. Let $A = \cup_{p=1}^{\ell} A_p$ be their union and*

$$\varphi = \sum_{p=1}^{\ell} \theta(A_p). \tag{31}$$

Here the angles are added as real numbers (rather than modulo 2π). If $\varphi < \pi/2$ then

$$\|W_A(U \otimes I)W_A(U^\dagger \otimes I) - I\| = |e^{i\varphi} - 1|. \tag{32}$$

If $\varphi \ge \pi/2$ then $\delta(U) \ge \sqrt{2}$.

5 Identity check algorithm

Combining all above ingredients we arrive at the following algorithm for the D-dimensional identity check problem. We first consider the case when the input circuit U is sufficiently close to the identity such that $\delta(U) < 2$. Below we assume that a reclusive partition $[n] = A_1 \ldots A_{D+1}$ of the D-dimensional qubit array has been already computed, see Appendix A for details. We claim that the following algorithm outputs an estimator γ satisfying $\delta(U) \le \gamma \le (D+1)\delta(U)$.

Algorithm 1 Identity check (diamond-norm).

Input: An n-qubit D-dimensional circuit U with $\delta(U) < 2$.
Output: $\gamma \in \mathbb{R}$ satisfying $\delta(U) \leq \gamma \leq (D+1)\delta(U)$.

1: $\gamma \leftarrow 0$
2: **for** $j = 1$ to $D+1$ **do**
3: $\quad \varphi_j \leftarrow 0$
4: $\quad \ell_j \leftarrow$ number of cubes in A_j
5: $\quad$ **for** $p = 1$ to ℓ_j **do**
6: $\quad\quad A_{j,p} \leftarrow p$-th cube in A_j
7: $\quad\quad \varphi_j \leftarrow \varphi_j + \theta(A_{j,p})$
8: $\quad\quad$ **if** $\varphi_j \geq \pi/2$ **then**
9: $\quad\quad\quad$ **return** $\gamma = 2$
10: $\quad\quad$ **end if**
11: $\quad$ **end for**
12: $\quad \gamma \leftarrow \gamma + |e^{i\varphi_j} - 1|$
13: **end for**

Indeed, if line 9 is never reached, Corollary 10 of the additivity lemma imply that the output of the algorithm coincides with the quantity γ defined in Lemma 4 specialized to the reclusive partition. In this case correctness of the algorithm follows directly from Lemma 4. Otherwise, the algorithm outputs $\gamma = 2$, while Corollary 10 implies that $\delta(U) \geq \sqrt{2}$. In this case $\gamma = 2$ satisfies the bounds $\delta(U) \leq \gamma \leq (D+1)\delta(U)$ for $D \geq 1$. We claim that the algorithm runs in time $O(n2^{12(2hD)^D})$. Indeed, the total number of cubes $A_{j,p}$ is $O(n)$. Computing the function $\theta(A_{j,p})$ at line 7 requires eigenvalues of a unitary operator $K_{A_{j,p}}$ acting on at most $4(2hD)^D$ qubits, as discussed in Section 3. This computation takes time $O(2^{12(2hD)^D})$. Hence the total runtime is $O(n2^{12(2hD)^D})$.

Next consider the general case when it is possible that $\delta(U) = 2$. Define our estimator of $\delta(U)$ as 1.16γ, where γ is the output of Algorithm 1. We claim that

$$\delta(U) \leq 1.16\gamma \leq 1.16(D+1)\delta(U). \tag{33}$$

If the algorithm never reaches line 9 then its output coincides with the quantity γ defined in Lemma 4 and Eq. (33) follows directly from Lemma 4, see Eq. (7). Otherwise, if the algorithm reaches line 9, it outputs $\gamma = 2$ while $\delta(U) \geq \sqrt{2}$ due to Corollary 10 of the additivity lemma. In this case the first inequality in Eq. (33) follows from $\delta(U) \leq 2$ and the second inequality becomes $2 \leq (D+1)\delta(U)$ which is true for any $D \geq 1$ since $\delta(U) \geq \sqrt{2}$. The runtime analysis is the same as before.

Since the runtime scales exponentially with the size of cubes $A_{j,p}$, one may wish to choose a partition with smaller cubes even if this negatively impacts the approximation quality. As an extreme case, one can choose each cube $A_{j,p}$ as a single qubit. However ensuring the lightcone separation between cubes in the same subset A_j would require $\approx (4h+1)^D$ subsets A_j instead of $D+1$ subsets [1]. Accordingly, the approximation ratio would become $\alpha = \Omega((4h+1)^D)$ instead of $\alpha = D+1$.

[1] Since any qubit is lightcone separated from all but at most $(1+4h)^D$ other qubits, Vizing's theorem implies that qubits can be partitioned into at most $1+(1+4h)^D$ lightcone separated subsets.

Likewise, we expect that the runtime can be improved at the cost of a worse approximation ratio α by computing the norm of commutators $K_{A_{j,p}} - I$ using a randomized version of the power method [8]. It is known that this method can approximate the operator norm of a matrix of size $2^m \times 2^m$ with a multiplicative error $1+\epsilon$ using $O(m/\epsilon)$ matrix-vector multiplications [8]. In our case, $K_{A_{j,p}}$ is specified by a quantum circuit acting on $m = 4(2hD)^D$ qubits with $poly(m)$ gates, see Section 3. Thus one can implement matrix-vector multiplication for the matrix $K_{A_{j,p}} - I$ in time $poly(m)2^m$. Accordingly, the power method runs in time $poly(m)2^m/\epsilon$, whereas the exact diagonalization of $K_{A_{j,p}} - I$ requires time $\Omega(2^{3m})$.

6 Numerical experiments

In this section, we implement the algorithm described in Section 5 to approximate the distance between identity and a constant-depth circuit U of up to 100 qubits. We consider $U = U_1 U_2^\dagger$, where U_1, U_2 are two different unitaries that both approximate the time evolution $e^{-iH\tau}$ of n qubits under the one-dimensional XY model:

$$H = \sum_{j=1}^{n-1} (X_j X_{j+1} + Y_j Y_{j+1}) .$$

In the limit of small τ, $U = U_1 U_2^\dagger \approx I$ approximate a forward evolution followed by a backward evolution under the same Hamiltonian. Explicitly, U_1 and U_2 are the first-order Trotter approximations with, respectively, an odd-even ordering and an X-Y ordering:

$$U_1 = e^{-i\tau \sum_{\text{odd } j} (X_j X_{j+1} + Y_j Y_{j+1})} e^{-i\tau \sum_{\text{even } j} (X_j X_{j+1} + Y_j Y_{j+1})},$$
$$U_2 = e^{-i\tau \sum_j X_j X_{j+1}} e^{-i\tau \sum_j Y_j Y_{j+1}}.$$

We note that $X_j X_{j+1}$ and $Y_j Y_{j+1}$ are both antisymmetric under the unitary conjugation by the staggered Pauli string $X_1 Y_2 X_3 Y_4 \ldots$. Therefore, the eigenvalues of U comes in complex conjugate pairs which results in a simple relationship between the diamond-norm and the operator-norm distances. Namely, a simple algebra shows that $\delta(U) = 2\sin(\varphi)$, where $\varphi \in [0, \pi/2)$ is defined by $\|U - I\| = |e^{i\varphi} - 1|$. In addition, using a well-known mapping from the XY model to free fermions [15], we can compute this distance exactly, providing a benchmark for our algorithm.

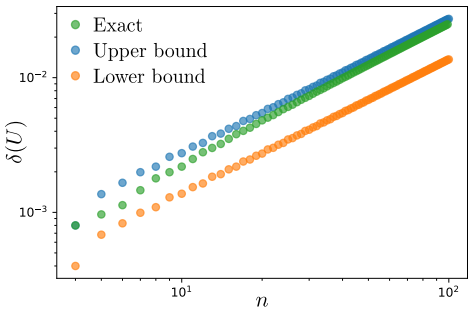

Figure 3 A comparison between the exact diamond-norm distance $\delta(U)$ (green dots) computed by a mapping to free fermions, an upper bound γ computed by Algorithm 1 (blue dots) and the lower bound $\gamma/2$ (orange dots). Both bounds closely capture the exact distance between U and I, demonstrating the scalability of our algorithm.

In Fig. 3, we compare the exact distance $\delta(U)$ against the bounds presented in Lemma 4 for up to 100 qubits at $\tau = 0.01$. For the one-dimensional qubit array, the bounds simplify to $\delta(U) \leq \gamma \leq 2\delta(U)$, where

$$\gamma = \sum_{j=1}^{2} \|W_{A_j}(U \otimes I)W_{A_j}(U^\dagger \otimes I) - I\|. \tag{34}$$

Here, A_1 and A_2 are the qubit partitions illustrated in Fig. 2 with $L = 4$. The lightcone separated construction of A_j and the additivity lemma allow us to efficiently compute the commutator $\|W_{A_j}(U \otimes I)W_{A_j}(U^\dagger \otimes I) - I\|$ for each j. In particular, computing the bounds reduces to finding eigenvalues of operators that are each supported on at most 12 qubits. Additionally, due to the translational invariance of the unitary U, only $O(1)$ such operators are unique, making the complexity of our algorithm independent of the system size.

Both bounds correctly capture the linear dependence of the Trotter error on the system size n, with the upper bound γ approaching the exact $\delta(U)$ in the limit of large n. We note that $\|U - I\|$ and, thus, $\delta(U)$ can also be estimated by finding the maximum eigenvalue of the Hamiltonian $H_U \equiv (U - I)^\dagger(U - I)$. Writing this Hamiltonian as a matrix product operator on a one-dimensional lattice, one can efficiently find a lower bound to its maximum eigenvalue using an algorithm based on the density matrix renormalization group (DMRG). While DMRG does not have a performance guarantee, we find that it produces lower bounds to within 3×10^{-7} of the exact $\delta(U)$ in this example, providing a complementary approach to our algorithm in one dimension. DRMG simulations were performed using the matrix product representation library for Python mpnum [14] with MPS bond dimension $\chi = 20$ and two DMRG sweeps in mpnum.linalg.eig.

References

1. Dorit Aharonov, Alexei Kitaev, and Noam Nisan. Quantum circuits with mixed states. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 20–30, 1998. doi:10.1145/276698.276708.
2. Avraham Ben-Aroya and Amnon Ta-Shma. On the complexity of approximating the diamond norm. *arXiv preprint arXiv:0902.3397*, 2009.
3. Hsin-Yuan Huang, Yunchao Liu, Michael Broughton, Isaac Kim, Anurag Anshu, Zeph Landau, and Jarrod R McClean. Learning shallow quantum circuits. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1343–1351, 2024. doi:10.1145/3618260.3649722.
4. William J Huggins, Joonho Lee, Unpil Baek, Bryan O'Gorman, and K Birgitta Whaley. A non-orthogonal variational quantum eigensolver. *New Journal of Physics*, 22(7):073009, 2020.
5. Dominik Janzing, Pawel Wocjan, and Thomas Beth. "Non-identity-check" is QMA-complete. *International Journal of Quantum Information*, 3(03):463–473, 2005.
6. Zhengfeng Ji and Xiaodi Wu. Non-identity check remains QMA-complete for short circuits. *arXiv preprint arXiv:0906.5416*, 2009.
7. William Kirby, Mario Motta, and Antonio Mezzacapo. Exact and efficient lanczos method on a quantum computer. *Quantum*, 7:1018, 2023. doi:10.22331/Q-2023-05-23-1018.
8. Jacek Kuczyński and Henryk Woźniakowski. Estimating the largest eigenvalue by the power and Lanczos algorithms with a random start. *SIAM journal on matrix analysis and applications*, 13(4):1094–1122, 1992. doi:10.1137/0613066.
9. Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.
10. Bill Rosgen. Distinguishing short quantum computations. *arXiv preprint arXiv:0712.2595*, 2007. arXiv:0712.2595.

11 Bill Rosgen and John Watrous. On the hardness of distinguishing mixed-state quantum computations. In *20th Annual IEEE Conference on Computational Complexity (CCC'05)*, pages 344–354. IEEE, 2005.

12 Ulrich Schollwöck. The density-matrix renormalization group in the age of matrix product states. *Annals of physics*, 326(1):96–192, 2011.

13 Kazuhiro Seki and Seiji Yunoki. Quantum power method by a superposition of time-evolved states. *PRX Quantum*, 2(1):010333, 2021.

14 Daniel Suess and Milan Holzäpfel. mpnum: A matrix product representation library for Python. *Journal of Open Source Software*, 2(20):465, 2017. doi:10.21105/JOSS.00465.

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

16 Vijay V Vazirani. *Approximation algorithms*, volume 1. Springer, 2001.

17 Guifré Vidal. Efficient simulation of one-dimensional quantum many-body systems. *Physical review letters*, 93(4):040502, 2004.

18 John Watrous. Semidefinite programs for completely bounded norms. *arXiv preprint arXiv:0901.4709*, 2009.

19 Jason Vander Woude, Peter Dixon, A Pavan, Jamie Radcliffe, and NV Vinodchandran. Geometry of rounding. *arXiv preprint arXiv:2211.02694*, 2022.

A Proof of Lemma 6

Let A be an upper triangular $D \times D$ matrix with the unit diagonal. In other words, $A_{i,i} = 1$ for all i and $A_{i,j} = 0$ for all $i > j$. Define a lattice $\mathcal{L}_A \subseteq \mathbb{R}^D$ formed by linear combinations of columns of A with integer coefficients. By definition, $p \in \mathcal{L}_A$ iff $p = Ac$ for some integer vector $c \in \mathbb{Z}^D$. For each lattice point $p \in \mathcal{L}_A$ define an open cube $C(p)$ and a closed cube $\overline{C}(p)$ such that p is the cube's corner with the smallest coordinates, that is,

$$C(p) = p + (0,1)^D \quad \text{and} \quad \overline{C}(p) = p + [0,1]^D.$$

The following claim can be interpreted as saying that the cubes $C(p)$ form a partition of the Euclidean space $\mathbb{R}^D$ if one ignores cube's boundaries.

▷ Claim 11. Any point $x \in \mathbb{R}^D$ is contained in at most one open cube $C(p)$. Any point $x \in \mathbb{R}^D$ is contained in at least one closed cube $\overline{C}(p)$.

Proof. Define ℓ_∞ norm of a vector $x \in \mathbb{R}^D$ as

$$\|x\|_\infty = \max_{i=1,\dots,D} |x_i|.$$

Suppose $x \in \mathbb{R}^D$ is contained in cubes $C(p)$ and $C(q)$ for some lattice points $p, q \in \mathcal{L}$. We have to show that $p = q$. Clearly, cubes $C(p)$ and $C(q)$ overlap iff

$$\|p - q\|_\infty < 1. \tag{35}$$

Thus we need to show that Eq. (35) implies $p = q$. Write

$$r = p - q = Ac \tag{36}$$

for some $c \in \mathbb{Z}^D$. Using the upper triangular structure of A and the fact that A has unit diagonal one gets

$$r_i = c_i + \sum_{j=i+1}^{D} A_{i,j} c_j. \tag{37}$$

If $i = D$ then clearly $r_i = c_i$ and thus $|r_i| < 1$ is only possible if $c_i = 0$. If $i = D-1$ then $r_i = c_i + A_{i,D}c_D$. However, we have already showed that $c_D = 0$. Thus $r_i = c_i$ and $|r_i| < 1$ is only possible if $c_i = 0$. Applying the same argument inductively proves that c is the all-zeros vector, that is, Eq. (35) implies $p = q$.

Suppose some vector $x \in \mathbb{R}^D$ is not contained in any closed cube $\overline{C}(p)$. Then $\|x-p\|_\infty > 1$ for all lattice points $p \in \mathcal{L}$. Let us show that this assumption leads to a contradiction. Indeed, set $i = D$. Shift x by an integer linear combination of the i-th column of A to make $|x_i| \le 1$. This is possible since $A_{i,i} = 1$. Next set $i = D-1$. Shift x by an integer linear combination of the i-th column of A to make $|x_i| \le 1$ and $|x_{i+1}| \le 1$. This is possible since $A_{i,i} = 1$ and $A_{i+1,i} = 0$. Applying the same argument inductively shows that shifting x by lattice points one can make $\|x\|_\infty \le 1$. Hence x is contained in the cube $\overline{C}(0^D)$. Equivalently, the original vector x is contained in some cube $\overline{C}(p)$. ◁

Following Ref. [19] we choose

$$A_{i,j} = \begin{cases} 1 & \text{if} \quad i = j, \\ \frac{D-j+1}{D} & \text{if} \quad i < j, \\ 0 & \text{else} \end{cases} \tag{38}$$

for $1 \le i, j \le D$. For example,

$$A = \begin{bmatrix} 1 & 1/2 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad A = \begin{bmatrix} 1 & 2/3 & 1/3 \\ 0 & 1 & 1/3 \\ 0 & 0 & 1 \end{bmatrix}$$

in the case $D = 2$ and $D = 3$ respectively. Below we summarize properties of the corresponding lattice $\mathcal{L}_A$ established in [19].

▶ **Fact 12** (Lemmas 7.15 and 7.19 of [19]). *The ℓ_∞-distance between closed cubes $\overline{C}(p)$ and $\overline{C}(q)$ is either 0 (if these cubes overlap) or at least $1/D$ (if these cubes do not overlap). Here $p, q \in \mathcal{L}_A$ are arbitrary lattice points.*

▶ **Fact 13** (Theorem 7.16 of [19]). *The cubes $\{\overline{C}(p)\}_{p\in\mathcal{L}_A}$ can be colored with $D+1$ colors such that any cube $\overline{C}(p)$ overlaps only with cubes $\overline{C}(q)$ of a different color.*

As a consequence of Facts 1 and 2, the ℓ_∞-distance between any pair of cubes $\overline{C}(p)$ of the same color is at least $1/D$. Rescaling each cube by the factor $L = 2Dh$ and noting that LA is an integer matrix one obtains a partition of $\mathbb{R}^D$ into a disjoin union of D-dimensional cubes $L\overline{C}(p)$ of linear size L such that corners of each cube have integer coordinates, the cubes are colored with $D+1$ colors, and the ℓ_∞-distance between any pair of cubes of the same color is at least L/D.

Finally, embed a D-dimensional rectangular array into $\mathbb{R}^D$ such that each cell of the array is a translation of the cube $(0,1)^D$ by an integer vector. We can now define the desired set of cells A_j as the union of all cells contained in the rescaled cubes $L\overline{C}(p)$ of the j-th color. This concludes the proof of Lemma 6.