

Implementing Unitary 2-Designs Using Random Diagonal-unitary Matrices

Yoshifumi Nakata^{*1}, Christoph Hirche^{†1}, Ciara Morgan¹, and Andreas Winter²

- 1 Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstrasse 2, 30167 Hannover, Germany
{yoshifumi.nakata,christoph.hirche,ciara.morgan}@itp.uni-hannover.de
- 2 ICREA & Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain
andreas.winter@uab.cat

Abstract

Unitary 2-designs are random unitary matrices which, in contrast to their Haar-distributed counterparts, have been shown to be efficiently realized by quantum circuits. Most notably, unitary 2-designs are known to achieve decoupling, a fundamental primitive of paramount importance in quantum Shannon theory. Here we prove that unitary 2-designs can be implemented approximately using random diagonal-unitaries.

1998 ACM Subject Classification H.1.1 Systems and Information Theory

Keywords and phrases Unitary 2-designs, commuting quantum circuits

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.191

1 Introduction

With coherent implementations of quantum circuits becoming a reality, the question of the practical realization of protocols in quantum information science has been a particular focus of the field in recent years. Indeed, quantum information theory itself is concerned with the evolution of quantum systems and decoupling represents one of the most fundamental primitives [1, 2, 3, 4]. Moreover, this protocol characterizes the conditions under which two, initially correlated, quantum systems will decohere completely, after evolution and the protocol itself is achieved using so-called Haar random unitaries [5, 6].

While Haar random unitaries are a powerful theoretical tool, the number of gates required to achieve their implementation grows exponentially in the system size. Unitary designs represent finite approximations of Haar random unitaries and, unitary 2-designs in particular, have been shown to efficiently achieve the decoupling protocol [7]. Moreover, unitary designs and the analysis of their performance have been widely studied [8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]. Unitary 2-designs have been shown to be achieved using Clifford circuits [8, 9] and random quantum circuits [12, 13, 14, 15] and among the most notable of results is the recent breakthrough of Cleve *et al.* [18] demonstrating a “near linear” implementation of an exact unitary 2-design.

* Now at: Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan – nakata@qi.t.u-tokyo.ac.jp.

† Now at: Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain – christoph.hirche@uab.cat.



© Yoshifumi Nakata, Christoph Hirche, Ciara Morgan, and Andreas Winter; licensed under Creative Commons License CC-BY

10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015).

Editors: Salman Beigi and Robert König; pp. 191–205

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

This motivates the question of how simply unitary 2-designs can be achieved. In this paper we show that unitary 2-designs can be realized to arbitrary precision by random diagonal-unitaries. Along with theoretical interest, the significance of this result lies in its simple implementation. Indeed, a quantum circuit for the implementation consists of repeating single-qubit phase gates, the controlled- Z gates, and the Hadamard gates. The first two parts are commuting, and they can be applied, in principle, simultaneously. Moreover, the depth of the non-commuting part, i.e. the Hadamard gates, is $O(1)$. These features of our implementation leads to a vast reduction in the execution time of the overall circuit. This work also provides a concrete application of commuting quantum circuits. Little is known about their concrete applications [19, 20] though they are known to provide a quantum advantage in computational tasks [21, 22]. The present authors have also shown that the decoupling theorem can be achieved by random-diagonal unitaries [23].

The article is organised as follows. We begin by introducing the necessary definitions and notation in Section 2. The main results are presented in Section 3, with the statement that unitary 2-designs can be achieved using random diagonal-unitary matrices given by Theorem 5 and the implementation given by Corollary 6. Proofs of the main results are presented in Section 4, along with statements of the necessary lemmas. Indeed, Lemma 8 is of particular importance in our analysis.

2 Preliminaries

2.1 Notation

We consider a system composed of N qubits and denote by \mathcal{H} , the corresponding Hilbert space and by $d = 2^N$ the dimension of \mathcal{H} . The set of bounded operators and states on \mathcal{H} are denoted by $\mathcal{B}(\mathcal{H})$ and $\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{B}(\mathcal{H}) | \rho \geq 0, \text{tr}\rho = 1\}$, respectively.

We will make use of various norms throughout the article, defined as follows. The p -norm of $X \in \mathcal{B}(\mathcal{H})$ is defined by $\|X\|_p := (\text{tr}|X|^p)^{1/p}$ for $p \geq 1$. For a superoperator $\mathcal{C} : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$, we use a family of superoperator norms $\|\mathcal{C}\|_{q \rightarrow p}$ ($q, p \geq 1$) and the diamond norm [24] defined by

$$\|\mathcal{C}\|_{q \rightarrow p} = \sup_{X \neq 0} \frac{\|\mathcal{C}(X)\|_p}{\|X\|_q}, \quad \|\mathcal{C}\|_{\diamond} := \sup_k \|\mathcal{C} \otimes \text{id}_k\|_{1 \rightarrow 1}, \quad (1)$$

respectively, where id_k is the identity map acting on a Hilbert space of dimension k . Note that it is known that $k \leq d$ is sufficient to obtain the diamond norm [24].

2.2 Random unitary matrices and their t -designs

We begin with the definition of random unitary matrices, before discussing their role in quantum information science, leading to the definition of unitary t -designs and approximations.

► **Definition 1** (Haar random unitary matrices [25]). Let $\mathcal{U}(d)$ be the unitary group of degree d , and denote the Haar measure (i.e. the unique unitarily invariant probability measure, thus often called uniform distribution) on $\mathcal{U}(d)$ by $\mathbb{H}_{\mathcal{U}(d)}$. A *Haar random unitary matrix* U is a $\mathcal{U}(d)$ -valued random variable distributed according to the Haar measure, $U \sim \mathbb{H}_{\mathcal{U}(d)}$.

► **Definition 2** (Random \mathbf{X} - and \mathbf{Z} -diagonal-unitary matrices [19]). Let $\mathcal{D}_{W,\text{diag}}$ be the set of unitary matrices diagonal in the Pauli- W basis $\{|n\rangle_W\}_{n=0}^{d-1}$ ($W = X, Z$), given by $\{\sum_{n=0}^{d-1} e^{i\varphi_n} |n\rangle\langle n|_W : \varphi_n \in [0, 2\pi) \text{ for } n \in [0, \dots, d-1]\}$. Let \mathbb{D}_W denote a probability

measure on it induced by a uniform probability measure on its parameter space $[0, 2\pi)^d$. A *random W -diagonal-unitary matrix* D^W is a $\mathcal{D}_{W,\text{diag}}$ -valued random variable distributed according to D_W , $D^W \sim D_W$.

The random unitary matrices, defined above, have been applied to a wide variety of problems in quantum information science (see e.g. [16] for a summary) and have been used to investigate typical properties in physical systems [26, 27, 28, 29]. However, they cannot be efficiently implemented by quantum circuits, since the number of random numbers needed for the implementation scales exponentially with the number of qubits in the system. This fact has led to the investigation of their approximation, that is, to the definition and performance analysis of *unitary t -designs* [8, 9, 10, 11, 12, 13, 14, 16, 15, 17, 18].

Indeed, a unitary t -design is a random variable taking values in the unitary group that simulate, up to the t th order, the statistical moments of a given random unitary matrix. To define a unitary t -design for a random unitary matrix U , let $\mathcal{G}_U^{(t)}(X)$ be a superoperator given by $\mathcal{G}_U^{(t)}(X) := \mathbb{E}_U[U^{\otimes t} X U^{\dagger \otimes t}]$ for any $X \in \mathcal{B}(\mathcal{H}^{\otimes t})$, where \mathbb{E}_U represents an expectation over U . Then, an ϵ -approximate unitary t -design is defined as follows.

► **Definition 3** (ϵ -approximate unitary t -designs [9, 14]). A random unitary matrix $U \in \mathcal{U}(d)$ is called an ϵ -approximate unitary t -design if $\|\mathcal{G}_U^{(t)} - \mathcal{G}_{U_H}^{(t)}\|_\diamond \leq \epsilon$, where U_H is a Haar random unitary matrix.

► **Definition 4** (ϵ -approximate diagonal-unitary t -designs [19]). A random diagonal-unitary matrix $U \in \mathcal{D}_{W,\text{diag}}$ ($W = X, Z$) is called an ϵ -approximate W -diagonal-unitary t -design if $\|\mathcal{G}_U^{(t)} - \mathcal{G}_{D^W}^{(t)}\|_\diamond \leq \epsilon$, where D^W is a random W -diagonal unitary matrix.

In these definitions, the designs are called *exact* when $\epsilon = 0$. Note that there are various definitions of ϵ -approximate unitary t -designs, a summary of which can be found in Ref. [16]. Most definitions are equivalent in the sense that, if U is an ϵ -approximate unitary t -design in one definition, it is also an ϵ' -approximate unitary t -design in other definitions for $\epsilon' = \text{poly}(d^t)\epsilon$.

3 Main results

3.1 A unitary 2-design by random diagonal-unitary matrices

We study an implementation of a unitary 2-design using random diagonal-unitary matrices. We alternately apply independent random Z - and X -diagonal-unitary matrices, and show that this strategy approaches a unitary 2-design, after a number of repetitions ℓ . A random unitary matrix obtained by this process is given by

$$D[\ell] := D_{\ell+1}^Z D_\ell^X D_\ell^Z \cdots D_2^X D_2^Z D_1^X D_1^Z. \quad (2)$$

where D_i^W are independent W -diagonal-unitary matrices ($i = 1, \dots, \ell + 1$, $W = X, Z$). The $D[\ell]$ can, equivalently, be expressed as

$$D[\ell] = \prod_{i=\ell}^1 D_i'^Z D_i^X D_i^Z, \quad (3)$$

where all random diagonal-unitary matrices are taken independently. We will use this particular expression of $D[\ell]$ in the remainder of the article.

Note that, since a random X -diagonal-unitary matrix can be obtained by conjugating a random Z -diagonal-unitary matrix by Hadamard gates, $D[\ell]$ can equivalently be expressed as

$$D[\ell] = D_{2\ell+1}^Z \prod_{i=2\ell}^1 (H^{\otimes N} D_i^Z), \quad (4)$$

where $H^{\otimes N}$ is the tensor product of N Hadamard gates acting on all N qubits. From this point of view, the Hadamard gates are the only non-commuting part of $D[\ell]$. We will use this expression when we consider an efficient implementation of $D[\ell]$ in Subsection 3.2.

Our main result shows that $D[\ell]$ quickly approaches a unitary 2-design with increasing ℓ . The formal statement is given by Theorem 5 below.

► **Theorem 5** ($D[\ell]$ is an approximate unitary 2-design). *A random unitary matrix $D[\ell]$, acting on N qubits, is an ϵ -approximate unitary 2-design for $\ell \geq 2 + \frac{1}{N}(1 + \log 1/\epsilon)$. Conversely, $D[\ell]$ cannot be an ϵ -approximate unitary 2-design if $\ell \leq \frac{1}{N} \log 1/\epsilon$.*

► **Remark.** The significance of Theorem 5 lies in the efficiency of its implementation. Moreover, since a random unitary matrix $D[\ell]$ can be separated into commuting (random Z -diagonal-unitary matrices) and non-commuting (the Hadamard gates) parts, and the number of non-commuting gates for the implementation scales linearly with the system size, this construction of an approximate unitary 2-design has a simple practical implementation. We expand upon this point in the following subsection.

3.2 Implementation of $D[\ell]$ by a quantum circuit

We show that a unitary 2-design achieved by $D[\ell]$ can be efficiently implemented by a quantum circuit. We do so by only considering a random Z -diagonal-unitary matrix D^Z , since $D[\ell]$ is composed simply of D^Z along with Hadamard matrices.

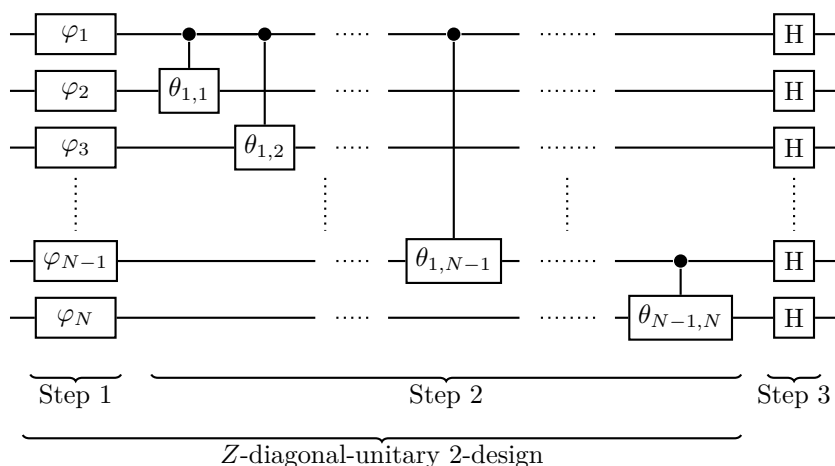
Since the exact implementation of D^Z is not efficient, we replace it by a random diagonal unitary matrix that is efficiently implementable. As we only need the second moments of D^Z for the implementation of a unitary 2-design, this is achieved by an exact Z -diagonal-unitary 2-design. An efficient implementation of an exact Z -diagonal-unitary t -design by a diagonal quantum circuit for any $t \in \mathbf{N}$ is provided in Ref. [30]. As its corollary, an exact Z -diagonal-unitary 2-design is implemented in the following way.

► **Corollary 6** (Exact implementation of Z -diagonal-unitary 2-designs). *An exact Z -diagonal-unitary 2-design is obtained by applying single-qubit phase gates $\text{diag}\{1, e^{i\varphi_k}\}$ on all qubits, where each phase φ_k is randomly and independently chosen from $\{0, 2\pi/3, 4\pi/3\}$ with $k \in [1, \dots, N]$, followed by probabilistic applications of the controlled- Z gate on every pair of qubits, where each controlled- Z gate is applied with probability $1/2$.*

Using this implementation, an approximate unitary 2-design can be implemented by repeating the following three steps (see also Fig. 1):

1. Apply single-qubit phase gates $\text{diag}(1, e^{i\varphi})$, which are diagonal in the Pauli- Z basis, with $\varphi \in \{0, 2\pi/3, 4\pi/3\}$ a random phase on all qubits.
2. Apply the controlled-phase gates $\text{diag}(1, 1, 1, e^{i\theta})$, diagonal in the Pauli- Z basis, with a random phase $\theta \in \{0, \pi\}$ on all pairs of qubits.
3. Apply the Hadamard gates on all qubits.

Note that the two-qubit phase gate, applied in the second step, is equivalent to a random application of the controlled- Z gate with probability $1/2$ in Corollary 6, since θ is randomly



■ **Figure 1** The figure depicts a building block of the quantum circuit that implements a unitary 2-design according to $D[\ell]$, given by Eq. (4). All the gates in the implementation of a Z -diagonal-unitary 2-design are diagonal in the Pauli- Z basis and, hence, can be applied simultaneously. One- and two-qubit gates in the first and the second step are given by $\text{diag}(1, e^{i\varphi_k})$ and $\text{diag}(1, 1, 1, e^{i\theta_{l,r}})$, respectively. The phases φ_k ($k = 1, \dots, N$) and $\theta_{l,r}$ ($l, r = 1, \dots, N, l \neq r$) are chosen from $\{0, 2\pi/3, 4\pi/3\}$ and $\{0, \pi\}$, respectively, uniformly at random. The one-qubit gates H represent the Hadamard gates.

chosen from $\{0, \pi\}$. We conclude from Theorem 5 and Corollary 6 that an ϵ -approximate unitary 2-design can be implemented with at most $3N(N + \frac{1}{2} \log 1/\epsilon) + O(N)$ one- or two-qubit gates, most of which are commuting. Numerical evidence for this observation has previously been found in Ref. [12, 13]

In terms of the number of gates, this implementation is as efficient as most of the previously known implementations of a unitary 2-design [9, 8, 14], but is not as efficient as a recently discovered near-linear construction of an exact unitary 2-design [18]. Our implementation of a unitary 2-design has another merit in view of commutativity of the gates, resulting in an instant property of the circuit in the sense that all the commuting parts of the circuit can be, in principle, applied simultaneously. In many physical systems for a quantum circuit, quantum gates are implemented by adding external electromagnetic fields [31]. If the circuit is composed of non-commuting gates, each field implementing a quantum gate should be applied in sequence, which results in a relatively long implementation time. In contrast, no ordering is imposed for commuting circuits and all the fields can be applied at once. Since our construction of a unitary 2-design uses a quantum circuit, where only the non-commuting part is the third step and is depth one, the practical time of our implementation is drastically reduced compared to the implementations using non-commuting gates scattered over the circuits. This also results in a robust implementation. Hence, our construction of a unitary 2-design may be preferable to other constructions from an experimental point of view.

This construction is also preferable for measurement-based quantum computation (MBQC) [32, 33]. In MBQC, computation is performed by single-qubit measurements on a certain type of multi-partite entangled pure states, known as cluster states. The measurement basis for implementing quantum gates, with the exception of Clifford gates, depends on the outcomes of previous measurements. This adaptivity of measurement basis in MBQC makes it challenging to experimentally perform. When we implement a unitary 2-design by $D[\ell]$ in MBQC, adaptive measurements are not necessary since all the gates are either

commuting (the first and the second steps) or Clifford (the third step). The implementation is also uniform in the sense that it is invariant under permutations of qubits. Hence, a unitary 2-design is obtained by simple MBQC where all the qubits in a cluster state can be simultaneously measured in prefixed bases.

4 Proofs

4.1 Auxiliary lemmas

In the following we provide the lemmas needed in the proof of Theorem 5. We begin by introducing some additional notation.

We denote the Pauli- Z and Pauli- X bases by $\{|i\rangle\}_{i=0,\dots,d-1}$ and $\{|\alpha\rangle\}_{\alpha=0,\dots,d-1}$, respectively. That is, the Pauli- Z basis is always labelled by Latin alphabets and the Pauli- X basis by Greek ones. We also denote the coefficients of $|\alpha\rangle$ in the basis of $\{|i\rangle\}$ by α_i/\sqrt{d} , namely, $\alpha_i = \sqrt{d}\langle i|\alpha\rangle$. Similarly, we define $i_\alpha := \sqrt{d}\langle \alpha|i\rangle$. Note that they are always ± 1 , and $\alpha_i = i_\alpha$. We also use the following quantity f_{kl}^{ij} ;

$$f_{kl}^{ij} = \frac{2}{d^3} \left(\sum_{\alpha=0}^{d-1} \alpha_i \alpha_j \alpha_k \alpha_l \right)^2. \quad (5)$$

The f_{kl}^{ij} satisfy the following relations (see Appendix A for the proof).

► **Lemma 7.** *The quantity f_{kl}^{ij} is in $\{0, 2/d\}$ and satisfies $f_{kl}^{ij} = f_{ij}^{kl}$, $\sum_{i>j} f_{kl}^{ij} = 1$ and $\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = f_{kl}^{ij}$.*

We use several operators in $\mathcal{B}(\mathcal{H}^{\otimes 2})$. First, we denote by \mathbb{I} , \mathbb{F} , \mathbb{L}_Z , and \mathbb{L}_X , the identity operator, the swap operator defined by $\sum_{i,j} |ij\rangle\langle ji|$, $\mathbb{L}_Z := \sum_i |ii\rangle\langle ii|$, and $\mathbb{L}_X := \sum_\alpha |\alpha\alpha\rangle\langle \alpha\alpha|$, respectively. The operator \mathbb{L}_W is defined in the Pauli- W basis and is dependent on the basis. We also denote by P_{sym} and P_{anti} the projection operators onto the symmetric and antisymmetric subspaces of $\mathcal{H}^{\otimes 2}$, which are equal to $(\mathbb{I} + \mathbb{F})/2$ and $(\mathbb{I} - \mathbb{F})/2$, respectively. Using these operators, we define states Π_{sym} , Π_{anti} , and Λ_W ($W = X, Z$), which are given by $P_{\text{sym}}/\text{tr}P_{\text{sym}}$, $P_{\text{anti}}/\text{tr}P_{\text{anti}}$, and $\mathbb{L}_W/\text{tr}\mathbb{L}_W$, respectively. The normalization factors are given by

$$\text{tr}P_{\text{sym}} = \frac{d(d+1)}{2}, \quad \text{tr}P_{\text{anti}} = \frac{d(d-1)}{2}, \quad \text{tr}\mathbb{L}_W = d. \quad (6)$$

The main part of the proof is concerned with the completely-positive and trace-preserving (CPTP) map \mathcal{R} from $\mathcal{B}(\mathcal{H}^{\otimes 2})$ to itself defined by $\mathcal{R} = \mathcal{G}_{D^Z}^{(2)} \circ \mathcal{G}_{D^X}^{(2)} \circ \mathcal{G}_U^{(2)}$, where $\mathcal{G}_U^{(2)}$ for a random unitary matrix U is defined in Subsection 2.

► **Lemma 8.** *Let B be the basis in $\mathcal{H}^{\otimes 2}$ given by $\{|ii\rangle\}_{i=0}^{d-1} \cup \{|\phi_{ij}\rangle\}_{i>j} \cup \{|\psi_{ij}\rangle\}_{i>j}$, where $|\phi_{ij}\rangle := \frac{1}{\sqrt{2}}(|ij\rangle + |ji\rangle)$ and $|\psi_{ij}\rangle := \frac{1}{\sqrt{2}}(|ij\rangle - |ji\rangle)$. Then, for all $|p\rangle \neq |q\rangle \in B$ and all integers ℓ , it holds $\mathcal{R}^\ell(|p\rangle\langle q|) = 0$, and*

$$\mathcal{R}^\ell(|ii\rangle\langle ii|) = (1 - d^{-2\ell})\Pi_{\text{sym}} + d^{-2\ell}\Lambda_Z \quad (7)$$

$$\mathcal{R}^\ell(|\phi_{ij}\rangle\langle \phi_{ij}|) = a_\ell \Pi_{\text{sym}} + b_\ell \Lambda_Z + d^{-\ell} \sum_{k>l} f_{kl}^{ij} |\phi_{kl}\rangle\langle \phi_{kl}| \quad (8)$$

$$\mathcal{R}^\ell(|\psi_{ij}\rangle\langle \psi_{ij}|) = (1 - d^{-\ell})\Pi_{\text{anti}} + d^{-\ell} \sum_{k>l} f_{kl}^{ij} |\psi_{kl}\rangle\langle \psi_{kl}|, \quad (9)$$

where

$$a_\ell = 1 - \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell}(d-1)}, \quad (10)$$

$$b_\ell = 2 \frac{d^\ell - 1}{d^{2\ell}(d-1)}. \quad (11)$$

Proof. We first investigate $\mathcal{R}(|ii\rangle\langle kk|)$, $\mathcal{R}(|\phi_{ij}\rangle\langle\phi_{kl}|)$, and $\mathcal{R}(|\psi_{ij}\rangle\langle\psi_{kl}|)$ ($i > j$ and $k > l$). As each input state is in the Pauli-Z basis, we obtain

$$\mathcal{R}(|ii\rangle\langle kk|) = \delta_{ik} \mathcal{G}_{DZ}^{(2)} \circ \mathcal{G}_{DX}^{(2)}(|ii\rangle\langle ii|) \quad (12)$$

$$\mathcal{R}(|\phi_{ij}\rangle\langle\phi_{kl}|) = \delta_{ik} \delta_{jl} \mathcal{G}_{DZ}^{(2)} \circ \mathcal{G}_{DX}^{(2)}(|\phi_{ij}\rangle\langle\phi_{ij}|) \quad (13)$$

$$\mathcal{R}(|\psi_{ij}\rangle\langle\psi_{kl}|) = \delta_{ik} \delta_{jl} \mathcal{G}_{DZ}^{(2)} \circ \mathcal{G}_{DX}^{(2)}(|\psi_{ij}\rangle\langle\psi_{ij}|). \quad (14)$$

Using the relation $\mathcal{G}_{DX}^{(2)}(|ii\rangle\langle ii|) = \frac{1}{d^2}(\mathbb{I} + \mathbb{F} - \mathbb{L}_X)$, and \mathbb{I} and \mathbb{F} are invariant under $\mathcal{G}_{DZ}^{(2)}$, the $\mathcal{R}(|ii\rangle\langle kk|)$ is calculated to be

$$\mathcal{R}(|ii\rangle\langle kk|) = \frac{1}{d^2} \delta_{ik} \left[\left(1 - \frac{1}{d}\right)(\mathbb{I} + \mathbb{F}) + \frac{1}{d} \mathbb{L}_Z \right]. \quad (15)$$

Note that this implies that $\mathcal{R}(|ii\rangle\langle ii|)$ is independent of i . For $\mathcal{R}(|\phi_{ij}\rangle\langle\phi_{kl}|)$ and $\mathcal{R}(|\psi_{ij}\rangle\langle\psi_{kl}|)$, simple calculations lead to

$$\mathcal{G}_{DX}^{(2)}(|ij\rangle\langle ij|) = \frac{1}{d^2} \left(\mathbb{I} + \sum_{\alpha, \beta} \alpha_i \alpha_j \beta_i \beta_j |\alpha\beta\rangle\langle\beta\alpha| - \mathbb{L}_X \right) \quad (16)$$

$$\mathcal{G}_{DX}^{(2)}(|ij\rangle\langle ji|) = \frac{1}{d^2} \left(\sum_{\alpha, \beta} \alpha_i \alpha_j \beta_i \beta_j |\alpha\beta\rangle\langle\alpha\beta| + \mathbb{F} - \mathbb{L}_X \right), \quad (17)$$

and similar relations for $\mathcal{G}_{DZ}^{(2)}(|\alpha\beta\rangle\langle\alpha\beta|)$ and $\mathcal{G}_{DZ}^{(2)}(|\alpha\beta\rangle\langle\beta\alpha|)$. Hence, we obtain

$$\mathcal{R}(|\phi_{ij}\rangle\langle\phi_{kl}|) = \frac{1}{d^2} \delta_{ik} \delta_{jl} \left[\left(1 - \frac{2}{d}\right)(\mathbb{I} + \mathbb{F}) + \frac{2}{d} \mathbb{L}_Z + d \sum_{s>t} f_{st}^{ij} |\phi_{st}\rangle\langle\phi_{st}| \right] \quad (18)$$

$$\mathcal{R}(|\psi_{ij}\rangle\langle\psi_{kl}|) = \frac{1}{d^2} \delta_{ik} \delta_{jl} \left[\mathbb{I} - \mathbb{F} + d \sum_{s>t} f_{st}^{ij} |\psi_{st}\rangle\langle\psi_{st}| \right], \quad (19)$$

where we use, e.g. $\alpha_i = i_\alpha$ for the derivation.

We next show that other terms, such as $\mathcal{R}(|\phi_{ij}\rangle\langle kk|)$, $\mathcal{R}(|\psi_{ij}\rangle\langle kk|)$, $\mathcal{R}(|\phi_{ij}\rangle\langle\psi_{kl}|)$ and their conjugates, are zero. Amongst these terms, all except $\mathcal{R}(|\phi_{ij}\rangle\langle\psi_{ij}|)$ and its conjugate vanish after the first application of $\mathcal{G}_{DZ}^{(2)}$. For $\mathcal{R}(|\phi_{ij}\rangle\langle\psi_{ij}|)$, $\mathcal{R}(|\phi_{ij}\rangle\langle\psi_{ij}|) = \mathcal{G}_{DZ}^{(2)} \circ \mathcal{G}_{DX}^{(2)}(|\phi_{ij}\rangle\langle\psi_{ij}|)$, since $|\phi_{ij}\rangle\langle\psi_{ij}|$ is not changed by $\mathcal{G}_{DZ}^{(2)}$. The $\mathcal{G}_{DX}^{(2)}(|\phi_{ij}\rangle\langle\psi_{ij}|)$ term is expanded to be

$$\mathcal{G}_{DX}^{(2)}(|\phi_{ij}\rangle\langle\psi_{ij}|) = \frac{1}{2} \left(\mathcal{G}_{DX}^{(2)}(|ij\rangle\langle ij|) - \mathcal{G}_{DX}^{(2)}(|ij\rangle\langle ji|) + \mathcal{G}_{DX}^{(2)}(|ji\rangle\langle ij|) - \mathcal{G}_{DX}^{(2)}(|ji\rangle\langle ji|) \right) \quad (20)$$

This is calculated using Eqs. (16) and (17). As the right hand sides of both Eqs. (16) and (17) are invariant under the exchange of i and j , $\mathcal{G}_{DX}^{(2)}(|\phi_{ij}\rangle\langle\psi_{ij}|)$ is zero, which implies $\mathcal{R}(|\phi_{ij}\rangle\langle\psi_{ij}|) = \mathcal{R}(|\psi_{ij}\rangle\langle\phi_{ij}|) = 0$.

Finally, we investigate $\mathcal{R}^\ell(|ii\rangle\langle ii|)$, $\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|)$, and $\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|)$. Since we have

$$\mathcal{R}(\mathbb{L}_Z) = \frac{1}{d} \left[\left(1 - \frac{1}{d}\right)(\mathbb{I} + \mathbb{F}) + \frac{1}{d} \mathbb{L}_Z \right], \quad (21)$$

from Eq. (15), $\mathcal{R}(\mathbb{I}) = \mathbb{I}$, and $\mathcal{R}(\mathbb{F}) = \mathbb{F}$, it is observed from Eq. (15) that $\mathcal{R}^\ell(|ii\rangle\langle ii|)$ is a linear combination of $\mathbb{I} + \mathbb{F}$ and \mathbb{L}_Z . Using this fact, it is straightforward to obtain

$$\mathcal{R}^\ell(|ii\rangle\langle ii|) = \frac{1 - d^{-2\ell}}{d(d+1)}(\mathbb{I} + \mathbb{F}) + d^{-2\ell-1}\mathbb{L}_Z, \quad (22)$$

which is rewritten, in terms of $\Pi_{\text{sym}} = \frac{1}{d(d+1)}(\mathbb{I} + \mathbb{F})$ and $\Lambda_Z = \frac{1}{d}\mathbb{L}_Z$, as

$$\mathcal{R}^\ell(|ii\rangle\langle ii|) = (1 - d^{-2\ell})\Pi_{\text{sym}} + d^{-2\ell}\Lambda_Z. \quad (23)$$

Similarly, $\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|)$ ($\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|)$) is given by a linear combination of $\mathbb{I} + \mathbb{F}$, \mathbb{L}_Z , and $\sum_{s>t} f_{st}^{ij} |\phi_{st}\rangle\langle\phi_{st}|$ ($\mathbb{I} - \mathbb{F}$ and $\sum_{s>t} f_{st}^{ij} |\psi_{st}\rangle\langle\psi_{st}|$). This can be seen to hold, since

$$\mathcal{R}\left(\sum_{s>t} f_{st}^{ij} |\phi_{st}\rangle\langle\phi_{st}|\right) = \frac{1}{d^2} \left[\left(1 - \frac{2}{d}\right)(\mathbb{I} + \mathbb{F}) + \frac{2}{d}\mathbb{L}_Z \right] + \frac{1}{d} \sum_{s>t} \sum_{k>l} f_{st}^{ij} f_{kl}^{st} |\phi_{kl}\rangle\langle\phi_{kl}| \quad (24)$$

$$= \frac{1}{d^2} \left[\left(1 - \frac{2}{d}\right)(\mathbb{I} + \mathbb{F}) + \frac{2}{d}\mathbb{L}_Z \right] + \frac{1}{d} \sum_{k>l} f_{kl}^{ij} |\phi_{kl}\rangle\langle\phi_{kl}|, \quad (25)$$

where we have used $\sum_{s>t} f_{st}^{kl} = 1$ and $\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = f_{kl}^{ij}$ due to Lemma 7, and similarly

$$\mathcal{R}\left(\sum_{s>t} f_{st}^{ij} |\psi_{st}\rangle\langle\psi_{st}|\right) = \frac{1}{d^2}(\mathbb{I} - \mathbb{F}) + \frac{1}{d} \sum_{k>l} f_{kl}^{ij} |\psi_{kl}\rangle\langle\psi_{kl}|. \quad (26)$$

Hence, to obtain $\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|)$ and $\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|)$, we set

$$\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|) = a_\ell^{(+)}(\mathbb{I} + \mathbb{F}) + b_\ell^{(+)}\mathbb{L}_Z + c_\ell^{(+)} \sum_{k>l} f_{kl}^{ij} |\phi_{kl}\rangle\langle\phi_{kl}| \quad (27)$$

$$\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|) = a_\ell^{(-)}(\mathbb{I} - \mathbb{F}) + c_\ell^{(-)} \sum_{k>l} f_{kl}^{ij} |\psi_{kl}\rangle\langle\psi_{kl}|, \quad (28)$$

and derive the coefficients using their recurrence relations. From Eqs. (18) and (19), the coefficients for $n = 1$ are given by

$$a_1^{(+)} = \frac{1}{d^2} \left(1 - \frac{2}{d}\right), \quad b_1^{(+)} = \frac{2}{d^3}, \quad c_1^{(+)} = \frac{1}{d}, \quad (29)$$

$$a_1^{(-)} = \frac{1}{d^2}, \quad c_1^{(-)} = \frac{1}{d}. \quad (30)$$

From Eqs. (18), (19), (25), and (26), recurrence relations for $a_\ell^{(\pm)}$, $b_\ell^{(+)}$, and $c_\ell^{(\pm)}$ are given by

$$a_{\ell+1}^{(+)} = a_\ell^{(+)} + \frac{1}{d} \left(1 - \frac{1}{d}\right) b_\ell^{(+)} + \frac{1}{d^2} \left(1 - \frac{2}{d}\right) c_\ell^{(+)}, \quad b_{\ell+1}^{(+)} = \frac{b_\ell^{(+)}}{d^2} + \frac{2c_\ell^{(+)}}{d^3}, \quad c_{\ell+1}^{(+)} = \frac{c_\ell^{(+)}}{d}, \quad (31)$$

and

$$a_{\ell+1}^{(-)} = a_\ell^{(+)} + \frac{c_\ell^{(-)}}{d^2}, \quad c_{\ell+1}^{(-)} = \frac{c_\ell^{(-)}}{d}. \quad (32)$$

Solving these relations, we obtain

$$a_\ell^{(+)} = \frac{1}{d(d+1)} - \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell+1}(d^2 - 1)}, \quad b_\ell^{(+)} = \frac{2(d^\ell - 1)}{d^{2\ell+1}(d - 1)}, \quad c_\ell^{(+)} = d^{-\ell}, \quad (33)$$

and

$$a_\ell^{(-)} = \frac{1 - d^{-\ell}}{d(d-1)}, \quad c_\ell^{(-)} = d^{-\ell}. \quad (34)$$

Thus, we have

$$\mathcal{R}^\ell(|\phi_{ij}\rangle\langle\phi_{ij}|) = \left(1 - \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell}(d-1)}\right) \Pi_{\text{sym}} + 2 \frac{d^\ell - 1}{d^{2\ell}(d-1)} \Lambda_Z + \frac{1}{d^\ell} \sum_{k>l} f_{kl}^{ij} |\phi_{kl}\rangle\langle\phi_{kl}| \quad (35)$$

$$\mathcal{R}^\ell(|\psi_{ij}\rangle\langle\psi_{ij}|) = \left(1 - \frac{1}{d^\ell}\right) \Pi_{\text{anti}} + \frac{1}{d^\ell} \sum_{k>l} f_{kl}^{ij} |\psi_{kl}\rangle\langle\psi_{kl}|. \quad (36)$$

This concludes the proof. \blacktriangleleft

We will also make use of upper and lower bounds of the diamond norm, in terms of a superoperator norm.

► **Lemma 9.** *Let \mathcal{C} be a linear map from $\mathcal{B}(\mathcal{H})$ ($\dim\mathcal{H} = D$) to $\mathcal{B}(\mathcal{H}')$ ($\dim\mathcal{H}' = D'$). Then,*

$$\|\mathcal{C}\|_{1 \rightarrow 1} \leq \|\mathcal{C}\|_\diamond \leq \sqrt{DD'} \|\mathcal{C}\|_{1 \rightarrow 1}. \quad (37)$$

Lemma 9 is a well-known relation (see, e.g. [16]). Nevertheless, for the sake of completeness, we present a proof below.

Proof. The first inequality holds by definition. To show the second inequality, we use a property of a superoperator norm $\|\mathcal{E}\|_{1 \rightarrow 2}$ such that, for any map \mathcal{E} acting on $\mathcal{B}(\mathcal{H}_K)$ where \mathcal{H}_K is a K -dimensional Hilbert space, $\|\mathcal{E} \otimes \text{id}_k\|_{1 \rightarrow 2} = \|\mathcal{E}\|_{1 \rightarrow 2}$ for $k \in \mathbf{N}$ [34]. It also satisfies the following chain of inequalities $\|\mathcal{E}\|_{1 \rightarrow 2} \leq \|\mathcal{E}\|_{1 \rightarrow 1} \leq \sqrt{K} \|\mathcal{E}\|_{1 \rightarrow 2}$ due to $\|X\|_2 \leq \|X\|_1 \leq \sqrt{K} \|X\|_2$ for $X \in \mathcal{B}(\mathcal{H}_K)$. Using these relations, we obtain

$$\|\mathcal{C}\|_\diamond = \|\mathcal{C} \otimes \text{id}_D\|_{1 \rightarrow 1} \leq \sqrt{DD'} \|\mathcal{C} \otimes \text{id}_D\|_{1 \rightarrow 2} = \sqrt{DD'} \|\mathcal{C}\|_{1 \rightarrow 2} \leq \sqrt{DD'} \|\mathcal{C}\|_{1 \rightarrow 1}. \quad (38)$$

\blacktriangleleft

4.2 Proof of the main result

Proof. Now we can prove Theorem 5. To this end, we investigate $\|\mathcal{G}_{D[\ell]}^{(2)} - \mathcal{G}_{U_H}^{(2)}\|_{1 \rightarrow 1}$, where U_H is a Haar random unitary matrix. In terms of the operators $\rho \in \mathcal{B}(\mathcal{H}^{\otimes 2})$ satisfying $\|\rho\|_1 = 1$, it is given by

$$\sup_{\substack{\rho \in \mathcal{B}(\mathcal{H}^{\otimes 2}) \\ \|\rho\|_1 = 1}} \|\mathcal{G}_{D[\ell]}^{(2)}(\rho) - \mathcal{G}_{U_H}^{(2)}(\rho)\|_1. \quad (39)$$

Note that ρ may be assumed to be Hermitian, but not necessarily positive semidefinite.

Due to Schur-Weyl duality [35], the latter term $\mathcal{G}_{U_H}^{(2)}(\rho)$ is given by

$$\mathcal{G}_{U_H}^{(2)}(\rho) = (\text{tr} P_{\text{sym}} \rho) \Pi_{\text{sym}} + (\text{tr} P_{\text{anti}} \rho) \Pi_{\text{anti}}. \quad (40)$$

On the other hand, the former term $\mathcal{G}_{D[\ell]}^{(2)}(\rho)$ is equal to $\mathcal{R}^\ell(\rho)$ since

$$\mathcal{G}_{D[\ell]}^{(2)}(\rho) = \mathbb{E}_{D[\ell]}[(D[\ell])^{\otimes 2} \rho (D[\ell])^{\dagger \otimes 2}] \quad (41)$$

$$= \prod_{i=\ell}^1 \mathbb{E}_{D_i^Z} \mathbb{E}_{D_i^X} \mathbb{E}_{D_i^Z} [(U_i^Z D_i^X D_i^Z)^{\otimes 2} \rho (D_i^Z D_i^X D_i^Z)^{\dagger \otimes 2}] \quad (42)$$

$$= \left(\mathcal{G}_{D^Z}^{(2)} \circ \mathcal{G}_{D^X}^{(2)} \circ \mathcal{G}_{D^Z}^{(2)} \right)^\ell(\rho) \quad (43)$$

$$= \mathcal{R}^\ell(\rho), \quad (44)$$

where the second line is obtained using the fact that the random diagonal-unitary matrices are independent.

Due to Lemma 8, for all $\rho \in \mathcal{B}(\mathcal{H}^{\otimes 2})$, we have

$$\begin{aligned} \mathcal{R}^\ell(\rho) &= ((1 - d^{-2\ell})s_0 + a_\ell s_1) \Pi_{\text{sym}} + (d^{-2\ell}s_0 + b_\ell s_1) \Lambda_Z + (1 - d^{-\ell})s_2 \Pi_{\text{anti}} \\ &\quad + d^{-\ell} \sum_{i>j} \sum_{k>l} f_{kl}^{ij} (\rho_{\phi_{ij}} |\phi_{kl}\rangle\langle\phi_{kl}| + \rho_{\psi_{ij}} |\psi_{kl}\rangle\langle\psi_{kl}|), \end{aligned} \quad (45)$$

where a_ℓ and b_ℓ are given by Lemma 8, $\rho_{\phi_{ij}} = \text{tr} \rho |\phi_{ij}\rangle\langle\phi_{ij}|$, $\rho_{\psi_{ij}} = \text{tr} \rho |\psi_{ij}\rangle\langle\psi_{ij}|$, $s_0 = \text{tr} \rho \mathbb{L}_Z$, $s_1 = \text{tr} \rho (P_{\text{sym}} - \mathbb{L}_Z)$, and $s_2 = \text{tr} \rho P_{\text{anti}}$. Using $\text{tr} P_{\text{sym}} \rho = s_0 + s_1$, this leads to

$$\begin{aligned} \mathcal{G}_{U_H}^{(2)}(\rho) - \mathcal{G}_{D[\ell]}^{(2)}(\rho) &= (d^{-2\ell}s_0 + (1 - a_\ell)s_1) \Pi_{\text{sym}} - (d^{-2\ell}s_0 + b_\ell s_1) \Lambda_Z + d^{-\ell}s_2 \Pi_{\text{anti}} \\ &\quad - d^{-\ell} \sum_{i>j} \sum_{k>l} f_{kl}^{ij} (\rho_{\phi_{ij}} |\phi_{kl}\rangle\langle\phi_{kl}| + \rho_{\psi_{ij}} |\psi_{kl}\rangle\langle\psi_{kl}|). \end{aligned} \quad (46)$$

Since $\Pi_{\text{sym}} = \frac{2}{d(d+1)} (\sum_i |ii\rangle\langle ii| + \sum_{i>j} |\phi_{ij}\rangle\langle\phi_{ij}|)$, $\Pi_{\text{anti}} = \frac{2}{d(d-1)} \sum_{i>j} |\psi_{ij}\rangle\langle\psi_{ij}|$, and $\Lambda_Z = \frac{1}{d} \sum_i |ii\rangle\langle ii|$, Eq. (46) is already diagonal in the basis $B = \{|ii\rangle\}_{i=0}^{d-1} \cup \{|\phi_{ij}\rangle\}_{i>j} \cup \{|\psi_{ij}\rangle\}_{i>j}$. Thus, its 1-norm is exactly calculated to be

$$\begin{aligned} \|\mathcal{G}_{U_H}^{(2)}(\rho) - \mathcal{G}_{D[\ell]}^{(2)}(\rho)\|_1 &= d \left| \frac{2}{d(d+1)} (d^{-2\ell}s_0 + (1 - a_\ell)s_1) - \frac{1}{d} (d^{-2\ell}s_0 + b_\ell s_1) \right| \\ &\quad + \sum_{k>l} \left(\left| \frac{2}{d(d+1)} (d^{-2\ell}s_0 + (1 - a_\ell)s_1) - d^{-\ell} \sum_{i>j} f_{kl}^{ij} \rho_{\phi_{ij}} \right| + \left| \frac{2}{d(d-1)} d^{-\ell}s_2 - d^{-\ell} \sum_{i>j} f_{kl}^{ij} \rho_{\psi_{ij}} \right| \right). \end{aligned} \quad (47)$$

The first term in Eq. (47) is simply equal to $\frac{|2s_1 - (d-1)s_0|}{d^{2\ell}(d+1)}$, which is smaller than or equal to $\frac{2|s_1| + (d-1)|s_0|}{d^{2\ell}(d+1)}$ due to the triangle inequality. In the following, we evaluate upper and lower bounds of the second and the third terms.

The second term is bounded from above, again due to the triangle inequality, by

$$\sum_{k>l} \left(\frac{2}{d(d+1)} (d^{-2\ell}|s_0| + |1 - a_\ell||s_1|) + d^{-\ell} \sum_{i>j} f_{kl}^{ij} |\rho_{\phi_{ij}}| \right), \quad (48)$$

where we have used the fact that f_{kl}^{ij} is non-negative. Substituting a_ℓ and using Lemma 7, i.e., $\sum_{k>l} f_{kl}^{ij} = 1$, it is bounded from above by

$$\frac{(d-1)|\text{tr} \rho \mathbb{L}_Z|}{d^{2\ell}(d+1)} + \frac{(d^{\ell+1} + d^\ell - 2)|\text{tr} \rho (P_{\text{sym}} - \mathbb{L}_Z)|}{d^{2\ell}(d+1)} + \frac{1}{d^\ell} \text{tr} |\rho| (P_{\text{sym}} - \mathbb{L}_Z). \quad (49)$$

Similarly, an upper bound of the third term in Eq. (47) is given by $\frac{1}{d^\ell}(|\text{tr}\rho P_{\text{anti}}| + \text{tr}|\rho|P_{\text{anti}})$.

From these upper bounds, an upper bound of $\|\mathcal{G}_{D[\ell]}^{(2)}(\rho) - \mathcal{G}_{U_H}^{(2)}(\rho)\|_1$ is given as follows, using $|s_0| = |\text{tr}\rho\mathbb{L}_Z| \leq \text{tr}|\rho|\mathbb{L}_Z$, $|s_1| = |\text{tr}\rho(P_{\text{sym}} - \mathbb{L}_Z)| \leq \text{tr}|\rho|(P_{\text{sym}} - \mathbb{L}_Z)$, $|s_2| = |\text{tr}\rho P_{\text{anti}}| \leq \text{tr}|\rho|P_{\text{anti}}$, and $P_{\text{sym}} + P_{\text{anti}} = \mathbb{I}$,

$$\|\mathcal{G}_{D[\ell]}^{(2)}(\rho) - \mathcal{G}_{U_H}^{(2)}(\rho)\|_1 \leq \frac{2(d-1)}{d^{2\ell}(d+1)}\text{tr}|\rho|\mathbb{L}_Z + \frac{2}{d^\ell}\text{tr}|\rho|(\mathbb{I} - \mathbb{L}_Z), \quad (50)$$

where we dropped the negative term $-\frac{2}{d^{2\ell}(d+1)}|\text{tr}\rho(P_{\text{sym}} - \mathbb{L}_Z)|$. Denoting $\text{tr}|\rho|\mathbb{L}_Z$ and $\text{tr}|\rho|(\mathbb{I} - \mathbb{L}_Z)$ by p_0 and p_1 , respectively, we have

$$\|\mathcal{G}_{D[\ell]}^{(2)}(\rho) - \mathcal{G}_{U_H}^{(2)}(\rho)\|_1 \leq \frac{2(d-1)}{d^{2\ell}(d+1)}p_0 + \frac{2}{d^\ell}p_1. \quad (51)$$

From this, we obtain an upper bound of $\sup_{\rho \in \mathcal{B}(\mathcal{H}^{\otimes 2}), \|\rho\|_1=1} \|\mathcal{G}_{D[\ell]}^{(2)}(\rho) - \mathcal{G}_{U_H}^{(2)}(\rho)\|_1$. Since $\|\rho\|_1 = 1$ implies that p_0 and p_1 satisfy $p_0 + p_1 = 1$, and they are positive by definition, Eq. (51) is a convex sum of $\frac{2(d-1)}{d^{2\ell}(d+1)}$ and $\frac{2}{d^\ell}$, where the latter is larger than the former. Hence, the supremum is given by $(p_0, p_1) = (0, 1)$, resulting in

$$\sup_{\rho \in \mathcal{B}(\mathcal{H}^{\otimes 2}), \|\rho\|_1=1} \|\mathcal{G}_{D[\ell]}^{(2)}(\rho) - \mathcal{G}_{U_H}^{(2)}(\rho)\|_1 \leq \frac{2}{d^\ell}. \quad (52)$$

A lower bound of $\sup_{\rho \in \mathcal{B}(\mathcal{H}^{\otimes 2}), \|\rho\|_1=1} \|\mathcal{G}_{D[\ell]}^{(2)}(\rho) - \mathcal{G}_{U_H}^{(2)}(\rho)\|_1$ is obtained by substituting a specific instance of ρ given by $\Phi_{i_0j_0} := |\phi_{i_0j_0}\rangle\langle\phi_{i_0j_0}|$ ($i_0 > j_0$), which gives

$$\|\mathcal{G}_{D[\ell]}^{(2)}(\Phi_{i_0j_0}) - \mathcal{G}_{U_H}^{(2)}(\Phi_{i_0j_0})\|_1 = \frac{2}{d^{2\ell}(d+1)} + \sum_{k>l} \left| \frac{2}{d(d+1)} \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell}(d-1)} - \frac{1}{d^\ell} f_{kl}^{i_0j_0} \right|, \quad (53)$$

from Eq. (47). Since $f_{kl}^{i_0j_0}$ satisfies $f_{kl}^{i_0j_0} = 0, 2/d$ for any $k > l$ and $\sum_{k>l} f_{kl}^{i_0j_0} = 1$ from Lemma 7, the number of (k, l) ($k > l$) for which $f_{kl}^{i_0j_0}$ is nonzero is $d/2$. Due to this fact, we can exactly calculate Eq. (53) as follows:

$$\begin{aligned} \|\mathcal{G}_{D[\ell]}^{(2)}(\Phi_{i_0j_0}) - \mathcal{G}_{U_H}^{(2)}(\Phi_{i_0j_0})\|_1 &= \frac{2}{d^{2\ell}(d+1)} + \frac{d}{2} \left| \frac{2}{d(d+1)} \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell}(d-1)} - \frac{2}{d^{\ell+1}} \right| \\ &\quad + \left(\frac{d(d-1)}{2} - \frac{d}{2} \right) \frac{2}{d(d+1)} \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell}(d-1)}, \end{aligned} \quad (54)$$

which is simplified to be

$$\|\mathcal{G}_{D[\ell]}^{(2)}(\Phi_{i_0j_0}) - \mathcal{G}_{U_H}^{(2)}(\Phi_{i_0j_0})\|_1 = \frac{2}{d^\ell} - 2 \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell}(d^2 - 1)}. \quad (55)$$

Hence, we obtain

$$\sup_{\rho \in \mathcal{B}(\mathcal{H}^{\otimes 2}), \|\rho\|_1=1} \|\mathcal{G}_{D[\ell]}^{(2)}(\rho) - \mathcal{G}_{U_H}^{(2)}(\rho)\|_1 \geq \frac{2}{d^\ell} - 2 \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell}(d^2 - 1)} \geq \frac{2}{d^\ell} \left[1 - \frac{2d}{d^2 - 1} \right]. \quad (56)$$

From these bounds, we obtain, using Lemma 9, upper and lower bounds of $\mathcal{G}_{D[\ell]}^{(2)} - \mathcal{G}_{U_H}^{(2)}$ in terms of the diamond norm,

$$\frac{2}{d^\ell} - 2 \frac{d^{\ell+1} + d^\ell - 2}{d^{2\ell}(d^2 - 1)} \leq \|\mathcal{G}_{D[\ell]}^{(2)} - \mathcal{G}_{U_H}^{(2)}\|_\diamond \leq \frac{2}{d^{\ell-2}}. \quad (57)$$

This implies that $D[\ell]$ is not an ϵ -approximate unitary 2-design if $\ell \leq \frac{\log \epsilon^{-1}}{N}$, as the lower bound in Eq. (57) is strictly greater than $1/d^\ell$ if $d > 3$, and is an ϵ -approximate unitary 2-design if $\ell \geq 2 + \frac{1 + \log \epsilon^{-1}}{N}$, and concludes the proof. \blacktriangleleft

5 Conclusion

We have proven that an approximate unitary 2-design can be achieved by alternately applying independent random Z - and X -diagonal unitary matrices. We have shown that one iteration of random Z - and X -diagonal unitary matrices is not sufficient, but it rapidly converges to an ϵ -approximate unitary 2-design after a number of iterations. We have also provided an implementation of our construction by a quantum circuit composed of $O(N(N + \log 1/\epsilon))$ one- or two-qubit gates, most of which are diagonal in the Pauli- Z basis. This implementation is, in terms of the number of gates, as efficient as many of other constructions using the Clifford circuits and random quantum circuits. An advantage unique to our implementation is its simple form. As the diagonal part can be applied simultaneously and the non-commuting part is depth $O(1)$, the practical time for the implementation will be vastly reduced compared to other implementations. Further applications of random diagonal-unitary matrices for decoupling can be found in Ref. [23].

Acknowledgements. The authors are grateful to Reinhard F. Werner and Omar Fawzi for interesting and fruitful discussions. YN is a JSPS Research Fellow and is partially supported by JSPS Postdoctoral Fellowships for Research Abroad. CM acknowledge support from the EU grants SIQS and QFTCMPS and by the cluster of excellence EXC 201 Quantum Engineering and Space-Time Research. CH and AW are supported by the Spanish MINECO, project FIS2013-40627-P, as well as by the Generalitat de Catalunya, CIRIT project no. 2014 SGR 966. AW is further supported by the European Commission (STREP “RAQUEL”), the European Research Council (Advanced Grant “IRQUAT”) and the Spanish MINECO, project FIS2008-01236, with the support of FEDER funds.

References

- 1 P. Hayden, M. Horodecki, A. Winter, and J. Yard. A decoupling approach to the quantum capacity. *Open Syst. Inf. Dyn.*, 15:7, 2008.
- 2 A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter. The mother of all protocols : Restructuring quantum information’s family tree. *Proc. R. Soc. A*, 465:2537, 2009.
- 3 N. Datta and M.-H. Hsieh. The apex of the family tree of protocols : optimal rates and resource inequalities. *New J. Phys.*, 13:093042, 2011.
- 4 C. Hirche and C. Morgan. Efficient achievability for quantum protocols using decoupling theorems. In *Proc. 2014 IEEE Int. Symp. Info. Theory*, page 536, 2014.
- 5 F. Dupuis. *The decoupling approach to quantum information theory*. PhD thesis, Université de Montréal, 2010. arXiv:1004.1641.
- 6 F. Dupuis, M. Berta, J. Wullschleger, and R. Renner. One-shot decoupling. *Commun. Math. Phys.*, 328:251, 2014.
- 7 O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner. Decoupling with unitary approximate two-designs. *New J. Phys.*, 15:053022, 2013.
- 8 D. P. DiVincenzo, D. W. Leung, and B. M. Terhal. Quantum data hiding. *IEEE Trans. Inf. Theory*, 48:580, 2002.
- 9 C. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A*, 80:012304, 2009.
- 10 G. Tóth and J. J. García-Ripoll. Efficient algorithm for multiqubit twirling for ensemble quantum computation. *Phys. Rev. A*, 75(4):042311, 2007.
- 11 D. Gross, K. Audenaert, and J. Eisert. Evenly distributed unitaries: On the structure of unitary designs. *J. of Math. Phys.*, 48(5):052104, 2007.

- 12 W. G. Brown, Y. S. Weinstein, and L. Viola. Quantum pseudorandomness from cluster-state quantum computation. *Phys. Rev. A*, 77(4):040303(R), 2008.
- 13 Y. S. Weinstein, W. G. Brown, and L. Viola. Parameters of pseudorandom quantum circuits. *Phys. Rev. A*, 78(5):052332, 2008.
- 14 A. W. Harrow and R. A. Low. Random quantum circuits are approximate 2-designs. *Commun. Math. Phys.*, 291:257, 2009.
- 15 I. T. Diniz and D. Jonathan. Comment on “Random quantum circuits are approximate 2-designs”. *Commun. Math. Phys.*, 304:281, 2011.
- 16 R. A. Low. *Pseudo-randomness and learning in quantum computation*. PhD thesis, University of Bristol, 2010. arXiv:1006.5227.
- 17 F. G. S. L. Brandao, A. W. Harrow, and M. Horodecki. Local random quantum circuits are approximate polynomial-designs, 2012. arXiv: 1208.0692.
- 18 R. Cleve, D. Leung, L. Liu, and C. Wang. Near-linear constructions of exact unitary 2-designs, 2015. arXiv:1501.04592.
- 19 Y. Nakata and M. Mura0. Diagonal-unitary 2-designs and their implementations by quantum circuits. *Int. J. Quant. Inf.*, 11:1350062, 2013.
- 20 Y. Nakata and M. Mura0. Diagonal quantum circuits: their computational power and applications. *Eur. Phys. J. Plus*, 129:152, 2014.
- 21 D. J. Shepherd and M. J. Bremner. Temporally unstructured quantum computation. *Proc. R. Soc. A*, 465:1413, 2009.
- 22 M. J. Bremner, R. Jozsa, and D. J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proc. R. Soc. A*, 467(2126):459, 2011.
- 23 Y. Nakata, C. Hirche, C. Morgan, and A. Winter, 2015. In preparation.
- 24 A. Kitaev, A. Shen, and M. Vyalı. *Classical and Quantum Computation*. American Mathematical Society Boston, MA, USA, 2002.
- 25 M. L. Mehta. *Random Matrices*. Academic Press, Amsterdam San Diego Oxford London, 1990.
- 26 S. Popescu, A. J. Short, and A. Winter. Entanglement and the foundations of statistical mechanics. *Nature Physics*, 2:754, 2006.
- 27 P. Hayden and J. Preskill. Black holes as mirrors : quantum information in random subsystems. *J. High Energy Phys.*, 9:120, 2007.
- 28 Y. Nakata, P. S. Turner, and M. Mura0. Phase-random states: Ensembles of states with fixed amplitudes and uniformly distributed phases in a fixed basis. *Phys. Rev. A*, 86(1):012301, 2012.
- 29 L. del Rio, A. Hutter, R. Renner, and S. Wehner. Relative thermalization, 2014. arXiv:1401.7997.
- 30 Y. Nakata, M. Koashi, and M. Mura0. Generating a state t-design by diagonal quantum circuits. *New J. Phys.*, 16:053043, 2014.
- 31 N. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.
- 32 R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188, 2001.
- 33 R. Raussendorf, D. E. Browne, and H. J. Briegel. Measurement-based quantum computation with cluster states. *Phys. Rev. A*, 68:022312, 2003.
- 34 J. Watrous. Notes on super-operator norms induced by Schatten norms, 2004. arXiv:quant-ph/0411077.
- 35 R. Goodman and N. R. Wallach. *Representations and Invariants of the Classical Groups*. Cambridge University Press, Cambridge, UK, 1999.

A Proof of Lemma 7

Proof. The statement $f_{kl}^{ij} = f_{ij}^{kl}$ follows from the definition of f_{kl}^{ij} . We first show that f_{kl}^{ij} is either 0 or $2/d$. As f_{kl}^{ij} is defined by $f_{kl}^{ij} = \frac{2}{d^3} \left(\sum_{\alpha=0}^{d-1} \alpha_i \alpha_j \alpha_k \alpha_l \right)^2$, we investigate $\sum_{\alpha=0}^{d-1} \alpha_i \alpha_j \alpha_k \alpha_l$. This is invariant even if Pauli X is applied on the m -th qubit for any $m \in [1, \dots, N]$, which we denote by X_m , since

$$\sum_{\alpha=0}^{d-1} \alpha_i \alpha_j \alpha_k \alpha_l = d^2 \sum_{\alpha=0}^{d-1} \langle \alpha | i \rangle \langle \alpha | j \rangle \langle \alpha | k \rangle \langle \alpha | l \rangle \quad (58)$$

$$= d^2 \sum_{\alpha=0}^{d-1} \langle \alpha | X_m | i \rangle \langle \alpha | X_m | j \rangle \langle \alpha | X_m | k \rangle \langle \alpha | X_m | l \rangle. \quad (59)$$

This is due to $\langle \alpha | X_m = \pm \langle \alpha |$. Hence, we assume $|i\rangle = |0\rangle^{\otimes N}$ without loss of generality, resulting in $\alpha_i = 1$ for all α . The $\sum_{\alpha=0}^{d-1} \alpha_j \alpha_k \alpha_l$ still has another invariance, that is,

$$\sum_{\alpha=0}^{d-1} \alpha_j \alpha_k \alpha_l = d\sqrt{d} \sum_{\alpha=0}^{d-1} \langle \alpha | j \rangle \langle \alpha | k \rangle \langle \alpha | l \rangle \quad (60)$$

$$= d\sqrt{d} \sum_{\alpha=0}^{d-1} \langle \alpha | Z_m | j \rangle \langle \alpha | Z_m | k \rangle \langle \alpha | Z_m | l \rangle, \quad (61)$$

due to the summation over all α , where Z_m is the Pauli- Z operator acting on the m -th qubit. We then assume $\alpha_j = 1$ for $j = 0, \dots, d/2 - 1$ and $\alpha_j = -1$ for $j = d/2, \dots, d - 1$ without loss of generality. This leads to

$$\sum_{\alpha=0}^{d-1} \alpha_i \alpha_j \alpha_k \alpha_l = \left(\sum_{\alpha=0}^{d/2-1} - \sum_{\alpha=d/2}^{d-1} \right) \alpha_k \alpha_l. \quad (62)$$

Denoting $|\alpha\rangle$ by $|\alpha^1 \alpha^2 \dots \alpha^N\rangle$ ($\alpha^m = \pm$), where $|\pm\rangle$ are the eigenbasis of the Pauli- X with eigenvalues ± 1 , respectively, and similarly denoting $|k\rangle$ and $|l\rangle$ in binary such as $|k_1 \dots k_N\rangle$ ($k_m = 0, 1$), $(\sum_{\alpha=0}^{d/2-1} - \sum_{\alpha=d/2}^{d-1}) \alpha_k \alpha_l$ is rewritten as

$$\sum_{\alpha_2, \dots, \alpha_N = \pm} \left(\langle + | k_1 \rangle \langle + | l_1 \rangle \langle \alpha_2 \dots \alpha_N | k_1 \dots k_N \rangle \langle \alpha_2 \dots \alpha_N | l_1 \dots l_N \rangle \right. \\ \left. - \langle - | k_1 \rangle \langle - | l_1 \rangle \langle \alpha_2 \dots \alpha_N | k_1 \dots k_N \rangle \langle \alpha_2 \dots \alpha_N | l_1 \dots l_N \rangle \right). \quad (63)$$

When $k_1 = l_1$, this is simply zero. When $k_1 \neq l_1$, this is equal to $2^N = d$. Thus, $f_{ij}^{kl} \in \{0, 2/d\}$.

We next show $\sum_{k>l} f_{kl}^{ij} = 1$ for any $i > j$.

$$\sum_{k>l} f_{kl}^{ij} = \frac{2}{d^3} \sum_{k>l} \left(\sum_{\alpha} \alpha_i \alpha_j \alpha_k \alpha_l \right)^2 \quad (64)$$

$$= \frac{1}{d^3} \sum_{\alpha, \beta} \alpha_i \alpha_j \beta_i \beta_j \left(\sum_{k,l} \alpha_k \alpha_l \beta_k \beta_l - \sum_k \alpha_k^2 \beta_k^2 \right). \quad (65)$$

As $\sum_k \alpha_k^2 \beta_k^2 = d$ due to $\alpha_k = \pm 1$, we obtain

$$\frac{1}{d^3} \sum_{\alpha, \beta} \alpha_i \alpha_j \beta_i \beta_j \sum_k \alpha_k^2 \beta_k^2 = \frac{1}{d^2} \sum_{\alpha, \beta} \alpha_i \alpha_j \beta_i \beta_j \quad (66)$$

$$= \left(\sum_{\alpha} \langle i | \alpha \rangle \langle \alpha | j \rangle \right)^2 \quad (67)$$

$$= 0, \quad (68)$$

where we used that $i \neq j$ for the last line. Hence,

$$\sum_{k>l} f_{kl}^{ij} = \frac{1}{d^3} \sum_{\alpha, \beta} \alpha_i \alpha_j \beta_i \beta_j \left(\sum_k \alpha_k \beta_k \right)^2. \quad (69)$$

As $\sum_k \alpha_k \beta_k$ is given by $\frac{1}{d^2} \sum_k |\alpha\rangle \langle k| |k\rangle \langle \beta| = \frac{1}{d^2} \delta_{\alpha, \beta}$, we obtain

$$\sum_{k>l} f_{kl}^{ij} = \frac{1}{d} \sum_{\alpha, \beta} \alpha_i \alpha_j \beta_i \beta_j \delta_{\alpha, \beta} = 1. \quad (70)$$

We finally show $\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = f_{kl}^{ij}$. To this end, we define a set Ξ_{ij} for $i > j$ by $\Xi_{ij} := \{(s, t) | s, t \in \{1, \dots, N\}, s > t, f_{st}^{ij} = \frac{2}{d}\}$. Since $f_{kl}^{ij} \in \{0, 2/d\}$ and $\sum_{k>l} f_{kl}^{ij} = 1$ for any $i > j$, the number of elements in Ξ_{ij} , denoted by $|\Xi_{ij}|$, is $d/2$. Due to the definition of f_{st}^{ij} , Ξ_{ij} is also given in terms of α_i 's by $\Xi_{ij} = \{(s, t) | s, t \in \{1, \dots, N\}, s > t, \forall \alpha \in [0, \dots, d-1], \alpha_s \alpha_t = \alpha_i \alpha_j\}$. From this, it is observed that $\forall i > j$ and $\forall k > l$, Ξ_{ij} is either equal to Ξ_{kl} or has no intersection with Ξ_{kl} , i.e. $\Xi_{ij} \cap \Xi_{kl} = \emptyset$.

In terms of Ξ_{ij} , $f_{ij}^{kl} = \frac{2}{d} \delta_{kl \in \Xi_{ij}}$, where $\delta_{kl \in \Xi_{ij}} = 1$ if $(k, l) \in \Xi_{ij}$ and 0 otherwise. Note that, as $f_{ij}^{kl} = f_{kl}^{ij}$, $\delta_{kl \in \Xi_{ij}} = \delta_{ij \in \Xi_{kl}}$. Using this notation, we have

$$\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = \left(\frac{2}{d} \right)^2 \sum_{s>t} \delta_{st \in \Xi_{kl}} \delta_{st \in \Xi_{ij}} \quad (71)$$

$$= \left(\frac{2}{d} \right)^2 \sum_{s>t} \delta_{st \in \Xi_{kl} \cap \Xi_{ij}}. \quad (72)$$

When $\Xi_{kl} = \Xi_{ij}$, this is equal to $\frac{2}{d}$ as $|\Xi_{kl}| = d/2$. In this case, $f_{ij}^{kl} = \frac{2}{d} \delta_{kl \in \Xi_{ij}} = \frac{2}{d}$ since $(k, l) \in \Xi_{kl} = \Xi_{ij}$, implying $\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = f_{ij}^{kl}$. When $\Xi_{kl} \cap \Xi_{ij} = \emptyset$, Eq. (72) is equal to zero, and f_{ij}^{kl} is also zero by definition. Hence, $\sum_{s>t} f_{st}^{ij} f_{kl}^{st} = f_{ij}^{kl}$ holds even in this case. Since Ξ_{ij} is either Ξ_{kl} or satisfies $\Xi_{ij} \cap \Xi_{kl} = \emptyset$, this concludes the proof. \blacktriangleleft