New Journal of Physics
The open access journal for physics

Decoupling with unitary approximate two-designs

Oleg Szehr[1,2,5], Frédéric Dupuis[2,3], Marco Tomamichel[2,4] and Renato Renner[2]

[1] Zentrum Mathematik, Technische Universität München, D-85748 Garching, Germany
[2] Institute for Theoretical Physics, ETH Zurich, CH-8093 Zurich, Switzerland
[3] Department of Computer Science, Aarhus University, DK-8200 Aarhus N, Denmark
[4] Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore
E-mail: o.dim.qit@googlemail.com

New Journal of Physics **15** (2013) 053022 (20pp)
Received 27 February 2013
Published 15 May 2013
Online at http://www.njp.org/
doi:10.1088/1367-2630/15/5/053022

Abstract. Consider a bipartite system, of which one subsystem, A, undergoes a physical evolution separated from the other subsystem, R. One may ask under which conditions this evolution destroys all initial correlations between the subsystems A and R, i.e. *decouples* the subsystems. A quantitative answer to this question is provided by *decoupling theorems*, which have been developed recently in the area of quantum information theory. This paper builds on preceding work, which shows that decoupling is achieved if the evolution on A consists of a typical unitary, chosen with respect to the Haar measure, followed by a process that adds sufficient decoherence. Here, we prove a generalized decoupling theorem for the case where the unitary is chosen from an approximate two-design. A main implication of this result is that decoupling is physical, in the sense that it occurs already for short sequences of random two-body interactions, which can be modeled as efficient circuits. Our decoupling result is independent of the dimension of the R system, which shows that approximate two-designs are appropriate for decoupling even if the dimension of this system is large.

[5] Author to whom any correspondence should be addressed.

Contents

1. Introduction

Consider a joint quantum system, consisting of subsystems A and R. We say that A is *decoupled* from R if the joint state τ_{AR} has product form $\tau_A \otimes \tau_R$. Operationally, this means that the probability distributions obtained upon measuring the A and R systems are statistically independent. In this work, we are interested in processes acting locally on system A, which may initially be correlated to R, such that A ends up being decoupled from R.

Processes that decouple a system A from R play an important role in various information theoretic applications. Examples abound in the area of quantum Shannon theory: state merging [23] and state transfer [20]. Other important theorems, such as the best known achievable rates for sending quantum information through a quantum channel [21], can be proven concisely via decoupling. Moreover, arguments referring to decoupling have been used in a physical context and, for example, deepened our insight into the black hole information paradox [22] and the role of negative conditional entropies in thermodynamics [10].

In [13], a decoupling theorem has been derived that generalizes the previous decoupling theorems used in the aforementioned work. There one considers a situation where a subsystem A of a joint system AR undergoes an evolution while R is left unchanged. The mapping describing the evolution of A is conceptually split into two parts: a unitary followed by an arbitrary trace-preserving and completely positive map $\mathcal{T} = \mathcal{T}_{A\to B}$. The decoupling theorem of [13] (see also [14]) states that if an initial state ρ_{AR} and a process $\mathcal{T}$ are fixed and the unitary is taken either from the Haar measure or from a two-design [9], then the expected distance of the resulting state from a decoupled state is bounded in terms of entropic quantities

$$\mathop{\mathbb{E}}_{\mathbb{U}} \|\mathcal{T}((U_A\otimes\mathbb{1}_R)\rho_{AR}(U_A\otimes\mathbb{1}_R)^\dagger) - \omega_B \otimes \rho_R\|_1 \leqslant 2^{-\frac{1}{2}H_{\min}(A'|B)_\omega - \frac{1}{2}H_{\min}(A|R)_\rho}.$$

Here the operator ω only depends on the map $\mathcal{T}_{A\to B}$ and, in particular, is independent of the chosen input state, ρ_{AR}. The min-entropy, $H_{\min}(A|R)_\rho$ (cf definition 1 below), quantifies the uncertainty an observer with access to R has about the A subsystem prior to the decoupling operation. The quantity $H_{\min}(A'|B)_\omega$ measures how well the mapping $\mathcal{T}_{A\to B}$ conserves correlations. It quantifies the uncertainty of an observer with access to the output subsystem B about a copy A' of the input state space, after the map $\mathcal{T}_{A\to B}$ is applied to a maximally entangled state on AA'. The min-entropy can be seen as a generalization of the well-known von Neumann entropy in the following sense. If a smoothed version of the min-entropy (cf definition 2) is evaluated for n identical copies of the same state then in the asymptotic limit of large n it reduces to the von Neumann entropy (cf equation (2)). Thus an important special case of the above relation arises when we consider the limit of a large number of identical copies of states, ρ_{AR}, and channels, $\mathcal{T}_{A\to B}$, applied to them. In this scenario the subsystems decouple if

$$H(A'|B)_\omega + H(A|R)_\rho > 0$$

holds for the conditional von Neumann entropies of ω and ρ. Roughly, this inequality establishes a condition on the correlation in the initial state ρ_{AR} and the 'decoupling power' of the map $\mathcal{T}_{A\to B}$, which is sufficient for decoupling. Suppose, for instance, that ρ_{AR} contains strong quantum correlations such that $H(A|R)_\rho$ is negative, then decoupling occurs if $\mathcal{T}_{A\to B}$ can destroy this correlation, that is $H(A'|B)_\omega$ is large enough for the above to hold. (See [29] for a general introduction of negative conditional entropies and [10] for their meaning in thermodynamics. A detailed discussion of sufficiency and necessity of the above condition for decoupling can be found in [14].)

Often $\mathcal{T}_{A\to B}$ is chosen in a specific way. For example, in order to obtain the fully quantum Slepian–Wolf (FQSW) theorem [20], it suffices to consider the case where $\mathcal{T}_{A\to B}$ is the partial trace. Another special case is state merging [23], where $\mathcal{T}_{A\to B}$ represents a measurement of the A system. In the FQSW scenario, the above inequality is known to be tight [20].

In this paper, we analyze whether decoupling occurs in a typical physical process. For this purpose, we generalize the decoupling theorem above to the case when the random unitary is taken from an *approximate* two-design instead of a two-design. Our discussion of approximate two-designs is motivated by the fact that as opposed to exact two-designs, such as the Clifford group [12, 15, 18], approximate two-designs emerge in various realistic models of physical systems. In particular, approximate two-designs can be used to model a typical quantum mechanical evolution of an A subsystem that is governed by two-particle interactions. More precisely, we follow the lines of [19] and model the internal dynamics of the A subsystem in terms of a random quantum circuit and address the question of how well these dynamics decouple. We show that the quality of decoupling does not depend on the dimensions of the channel output B and the reference system R and prove that decoupling is physical, in the sense that it occurs already for short sequences of random two-body interactions even if R is large[6]. Moreover, our decoupling results open the door to a more efficient implementation of operational tasks such as state transfer and state merging, since one might expect good approximate two-designs to outperform exact two-designs in terms of circuit complexity[7].

We note that the result achieved here has a (semi-) classical analogue, which is used, for instance, in quantum cryptography for a task called *privacy amplification*. Here the system A is a classical random variable that is correlated with a quantum memory, R, held by an adversary.

[6] Note that it follows straight from continuity that approximate two-designs can be used for decoupling with an error depending on the approximation and the dimension of the physical system. However, in a physical scenario the dimensions of the channel output B and the reference system R can be large or unknown, which motivates the more elaborate analysis we provide in this paper.

[7] Note that the circuit complexity of the exact two-design given by the Clifford group is quadratic, as shown in [18].

The goal is to extract randomness from A which is private, i.e. uncorrelated to the adversary's data R. This can be achieved by two-universal hash functions [5], which replace the unitary two-design used in the decoupling theorem [33]. An extension to *almost* two-universal hash functions is already known in this classical scenario [36]. Our work can be seen as a fully quantum version of this result.

In this paper, we consider finite-dimensional systems only. However, the analogous task of privacy amplification described above has recently been extended to the case where the adversary holds an infinite-dimensional system [16] or a general von Neumann algebra of observables [2]. The fact that our decoupling results do not involve the dimension of the system held by the adversary (and the dimension of the channel output) suggests that a similar generalization is also possible for decoupling.

The remainder of the paper is organized as follows. In section 2, we introduce the mathematical framework used to derive our main technical results, which are presented in section 3. Finally, in section 4, we apply our results to analyze decoupling in a physical context.

2. Preliminaries

2.1. Notation

Let $\mathcal{H}$ be a finite-dimensional, complex Hilbert space. The set of linear operators on $\mathcal{H}$ will be denoted by $\mathcal{L}(\mathcal{H})$, the set of Hermitian operators by $\mathcal{L}^\dagger(\mathcal{H})$ and the set of positive-semidefinite operators is given by $\mathcal{P}(\mathcal{H})$. The set of quantum states is given by $\mathcal{S}_=(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) \mid \operatorname{tr}\rho = 1\}$ and the set of subnormalized quantum states is $\mathcal{S}_\leqslant(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) \mid \operatorname{tr}\rho \leqslant 1\}$. For the Lie group of unitary matrices, we write $\mathbb{U}$. A subscript letter following some mathematical object denotes the physical system to which it belongs. However, when it is clear which systems are described we might drop the subscripts to shorten the notation.

Bipartite systems AB are represented by a tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B =: \mathcal{H}_{AB}$. We will denote by $\mathbb{1}_A$ the identity operator on $\mathcal{H}_A$ and by $\pi_A := \mathbb{1}_A/d_A$ the completely mixed state on A, where $d_A = \dim \mathcal{H}_A$. Linear maps from $\mathcal{L}(\mathcal{H}_A)$ to $\mathcal{L}(\mathcal{H}_B)$ will be denoted by calligraphic letters, e.g. $\mathcal{T}_{A\to B}$. Quantum operations are in one-to-one correspondence with the trace preserving completely positive maps (TPCPMs). The TPCPM we will encounter most often is the partial trace (over the system B), denoted $\operatorname{tr}_B(\cdot)$, which is defined to be the adjoint mapping of $\mathcal{T}_{A\to AB}(\xi_A) = \xi_A \otimes \mathbb{1}_B$ for $\xi_A \in \mathcal{L}^\dagger(\mathcal{H}_A)$ with respect to the Schmidt scalar product $\langle A, B\rangle := \operatorname{tr}(A^\dagger B)$. This means $\operatorname{tr}((\xi_A \otimes \mathbb{1}_B)\zeta_{AB}) = \operatorname{tr}(\xi_A \operatorname{tr}_B(\zeta_{AB}))$ for any $\zeta_{AB} \in \mathcal{L}^\dagger(\mathcal{H}_{AB})$. Given a multipartite state ξ_{AB}, we write $\xi_A := \operatorname{tr}_B \xi_{AB}$ for the reduced density operator on A and $\xi_B := \operatorname{tr}_A \xi_{AB}$, respectively, on B.

For isomorphic $\mathcal{H}_A$ and $\mathcal{H}_{A'}$, we denote by $\Phi_{AA'}$ the completely entangled state on AA', i.e. $\Phi_{AA'} := |\Phi\rangle\langle\Phi|_{AA'}$, where $|\Phi\rangle_{AA'} := \sum_i |i\rangle_A \otimes |i\rangle_{A'}/\sqrt{d_A}$ and $\{|i\rangle_A\}$ and $\{|i\rangle_{A'}\}$ form orthonormal bases. The swap operator $\mathcal{F}$ on the bipartite space $\mathcal{H}_{AA'}$ is defined as $\mathcal{F} := \sum_{i,j} |i\rangle\langle j|_A \otimes |j\rangle\langle i|_{A'}$. It is not difficult to verify [1, 4] that this operator satisfies $\operatorname{tr}(MN) = \operatorname{tr}((M \otimes N)\mathcal{F})$ for any $M, N \in \mathcal{L}(\mathcal{H}_A)$. We refer to this observation as the *swap trick*. The Choi–Jamiołkowski representation [6, 25] of $\mathcal{T}_{A\to B} \in \operatorname{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_B))$ is given by the operator $\omega_{A'B} := (\mathcal{T}_{A\to B} \otimes \mathcal{I}_{A'})(\Phi_{AA'})$. Here, $\mathcal{I}_{A'}$ denotes the operator identity on A', which we will only write explicitly if it is not clear from the context.

For any operator in $\xi \in \mathcal{L}(\mathcal{H})$, we denote by $\|\xi\|_1$, $\|\xi\|_2$ and $\|\xi\|_\infty$ the Schatten one-, two- and ∞-norms of ξ, respectively. These norms are invariant under conjugation with unitaries and satisfy $\|\xi\|_\infty \leqslant \|\xi\|_2 \leqslant \|\xi\|_1$. We will furthermore use that, for any $A, B, C \in \mathcal{L}(\mathcal{H})$ and any Schatten norm $\|\cdot\|$, it holds that $\|ABC\| \leqslant \|A\|_\infty \|B\| \|C\|_\infty$ (see e.g. [3]).

The metric induced on $\mathcal{L}(\mathcal{H})$ via the Schatten one-norm is $D(\rho, \sigma) := \|\rho - \sigma\|_1$. Another measure of distance on $\mathcal{P}(\mathcal{H})$ is the fidelity, $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$. We also require a norm for linear maps $\mathcal{T}_{A\to B}$ from $\mathcal{L}(\mathcal{H}_A)$ to $\mathcal{L}(\mathcal{H}_B)$. Given such a map, its diamond norm is defined to be [26]

$$\|\mathcal{T}_{A\to B}\|_\diamond := \sup_{\mathcal{H}_R} \max_{\rho_{AR}\in\mathcal{L}(\mathcal{H}_{AR})} \frac{\|\mathcal{T}_{A\to B}(\rho_{AR})\|_1}{\|\rho_{AR}\|_1}.$$

Note that the diamond norm is the dual of the well-known norm of complete boundedness [30].

2.2. *Smooth entropies*

Entropies are used to quantify the uncertainty an observer has about a quantum state. Moreover, conditional entropies quantify the uncertainty of an observer about one subsystem of a bipartite state when he has access to another subsystem. The most commonly used quantity is the von Neumann entropy. Given a state $\rho_{AB} \in \mathcal{S}_=(\mathcal{H}_{AB})$, we denote by $H(A|B)_\rho := H(\rho_{AB}) - H(\rho_B)$ the von Neumann entropy of A conditioned on B.

While the von Neumann entropy is appropriate for analyzing processes involving a large number of copies of an identical system, the smooth min-entropy is the relevant quantity when a single system is considered [32]. Its definition is based on the following quantity.

Definition 1 (Min-entropy [32])**.** Let $\rho_{AB} \in \mathcal{S}_\leqslant(\mathcal{H}_{AB})$, then the min-entropy of A conditioned on B of ρ_{AB} is defined as

$$H_{\min}(A|B)_\rho := \max_{\sigma_B\in\mathcal{S}_=(\mathcal{H}_B)} \sup\{\lambda \in \mathbb{R} \mid \rho_{AB} \leqslant 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B\}.$$

More precisely, the smooth conditional min-entropy is defined as the largest conditional min-entropy one can obtain within a distance of at most ε from ρ. Here closeness is measured with respect to the *purified distance*, $P(\rho, \sigma)$, which is defined to be

$$P(\rho, \sigma) := \sqrt{1 - \bar{F}(\rho, \sigma)^2},$$

where $\bar{F}(\rho, \sigma)$ is the *generalized fidelity*; $\bar{F}(\rho, \sigma) := F(\rho, \sigma) + \sqrt{(1 - \operatorname{tr}\rho)(1 - \operatorname{tr}\sigma)}$ for $\rho, \sigma \in \mathcal{S}_\leqslant(\mathcal{H})$. In [34], it is shown that P constitutes a metric on $\mathcal{S}_\leqslant(\mathcal{H})$ and the following inequalities are derived:

$$\tfrac{1}{2}\|\rho - \sigma\|_1 + \tfrac{1}{2}|\operatorname{tr}\rho - \operatorname{tr}\sigma| \leqslant P(\rho, \sigma) \leqslant \sqrt{\|\rho - \sigma\|_1 + |\operatorname{tr}\rho - \operatorname{tr}\sigma|}. \tag{1}$$

We say that ρ is ε-close to $\tilde{\rho}$, denoted by $\tilde{\rho} \approx_\varepsilon \rho$ if $P(\rho, \tilde{\rho}) \leqslant \varepsilon$.

Definition 2 (Smooth min-entropy [32, 34])**.** Let $\varepsilon \geqslant 0$ and let $\rho_{AB} \in \mathcal{S}_\leqslant(\mathcal{H}_{AB})$ with $\sqrt{\operatorname{tr}\rho} > \varepsilon$, then the ε-smooth min-entropy of A conditioned on B of ρ_{AB} is defined as

$$H^\varepsilon_{\min}(A|B)_\rho = \max_{\tilde{\rho}} H_{\min}(A|B)_{\tilde{\rho}},$$

where we maximize over all $\tilde{\rho} \approx_\varepsilon \rho$.

The fully quantum asymptotic equipartition property (QAEP) states that in the limit of an infinite number of identical states the smooth min-entropy converges to the von Neumann entropy [35]: let $\rho_{AB} \in \mathcal{S}_{=}(\mathcal{H}_{AB})$, then

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_{\min}^{\varepsilon}(A^n|B^n)_{\rho^{\otimes n}} = H(A|B)_{\rho}. \tag{2}$$

In that sense, the smooth conditional min-entropy can be seen as a one-shot generalization of the von Neumann entropy.

2.3. Approximate two-designs and quantum circuits

Heuristically, a unitary two-design is a finite subset $\mathcal{D}$ of $\mathbb{U}$ that has the property that averaging any polynomial of degree 2 over $\mathcal{D}$ gives the same result as integrating this polynomial over $\mathbb{U}$ with respect to the Haar measure, dU.

Definition 3 (Unitary δ-approximate two-design [8, 9, 19])**.** Let $\mathcal{D} = \{(p_i, U_i)\}_{i=1,\dots,n}$ be a set of pairs, where the U_i are unitary matrices on a Hilbert space $\mathcal{H}$ and the $p_i \geqslant 0$ with $\sum_i p_i = 1$ are probabilities. We define the maps

$$\mathcal{G}_W(\rho) := \sum_i p_i U_i^{\otimes 2}\rho(U_i^{\dagger})^{\otimes 2} \quad \text{and} \quad \mathcal{G}_H(\rho) := \int_{\mathbb{U}} U^{\otimes 2}\rho(U^{\dagger})^{\otimes 2}\,\mathrm{d}U$$

for $\rho \in \mathcal{L}(\mathcal{H}^{\otimes 2})$. The set $\mathcal{D}$ is called a unitary two-design if $\mathcal{G}_W = \mathcal{G}_H$. Furthermore, $\mathcal{D}$ is called a δ-approximate unitary two-design if $\|\mathcal{G}_W - \mathcal{G}_H\|_{\diamond} \leqslant \delta$.

We will denote an integral over the unitary group with respect to the normalized Haar measure by $\mathbb{E}_{\mathbb{U}}(\cdot)$ and an average over a unitary approximate two-design by $\mathbb{E}_{\mathcal{D}}(\cdot)$ for notational convenience.

For the applications that we are interested in, the most relevant approximate designs are generated by random quantum circuits [19]. A quantum circuit is a set of wires on which gates are applied. Each wire corresponds to a qubit evolving in time, and each gate on the wire corresponds to some unitary operation being applied to the qubit. A k-qubit gate is given by an element of $\mathbb{U}(2^k)$. For us it will be sufficient to think of the circuit as a sequence of unitaries that are applied in a certain order: $W = W_t \cdot \ldots \cdot W_2 \cdot W_1$, where we call t the time of the circuit. We call a set of gates *universal* for n qubits if any operation that can be performed on n qubits can be approximated to arbitrary precision using operations from the universal gate set only.

3. Decoupling with δ-approximate unitary two-designs

We prove a decoupling theorem which applies to the general case where the evolution is described by a unitary chosen from a δ-approximate two-design followed by an arbitrary physical process.

Theorem 1 (Decoupling with δ-approximate unitary two-designs)**.** *Let $\rho_{AR} \in \mathcal{S}_{\leqslant}(\mathcal{H}_{AR})$ be a subnormalized density operator and let $\mathcal{T}_{A\to B}$ be a linear map with Choi–Jamiołkowski representation $\omega_{A'B} \in \mathcal{S}_{\leqslant}(\mathcal{H}_{BA'})$, then*

$$\mathop{\mathbb{E}}_{\mathcal{D}}\|\mathcal{T}((U_A\otimes \mathbb{1}_R)\,\rho_{AR}\,(U_A^{\dagger}\otimes\mathbb{1}_R)) - \omega_B\otimes\rho_R\|_1 \leqslant \sqrt{1+4\delta d_A^4}\,2^{-\frac{1}{2}(H_{\min}(A'|B)_{\omega}+\,H_{\min}(A|R)_{\rho})},$$

where $\mathcal{D}$ constitutes a δ-approximate two-design.

Remark 1. It should be noted that the factor d_A^4 in the above formula can be compensated for by making δ accordingly small. See section 4 for a specific example, where the approximate two-design is created by a random circuit.

Remark 2. Since the above decoupling formula does not involve the dimension factors d_B and d_R a δ-approximate two-design (with fixed δ) yields decoupling even if one of these factors is intractably large.

Note that theorem 1 does not follow straight from a simple argument based on continuity. If exact two-designs work in the sense of decoupling, one expects that δ-approximate two-designs should work approximately. The error due to approximation depends on δ and, due to norm equivalence (compare also lemma 2.2.14 in [28]), the dimension of the expression in the norm above. However, the upper bound of theorem 1 does not involve the dimensions of the systems B and R. Hence, it allows for the conclusion that decoupling can occur in a physical scenario, where the evolution of the A subsystem is modeled as a (short) quantum circuit and the reference system R potentially is large (see section 4). We also remark that in the particular case of a perfect two-design, the proof of theorem 1 includes a shorter derivation of the decoupling theorem for perfect two-designs as opposed to the original proof in [13, 14] (see section 3.2).

The rest of this section is structured in four subsections. First, we prove a lemma that quantifies decoupling in terms of Schatten two-norms. Then, in section 3.2, we derive the decoupling formula for perfect two-designs using that lemma (see theorem 2). Section 3.3 is devoted to the derivation and analysis of the decoupling formula for general δ-approximate two-designs (see theorem 1). And lastly, in section 3.4 we reformulate the upper bound given by the decoupling formula for δ-approximate two-designs in terms of smooth conditional min-entropies (see theorem 3). This enables us to make statements about independent, identically distributed states via the QAEP, equation (2).

3.1. Decoupling with Schatten two-norms

For a map $\mathcal{T} \in \mathrm{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_B))$ with Choi–Jamiołkowski representation $\omega_{A'B} \in \mathcal{L}^\dagger(\mathcal{H}_{BA'})$ and an operator $\rho_{AR} \in \mathcal{L}^\dagger(\mathcal{H}_{AR})$, we prove that

$$\mathop{\mathbb{E}}_{\mathbb{U}} \left\| \mathcal{T}((U_A \otimes \mathbb{1}_R)\, \rho_{AR}\, (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_B \otimes \rho_R \right\|_2^2$$

$$= \frac{d_A^2}{d_A^2 - 1} \left\| \rho_{AR} - \pi_A \otimes \rho_R \right\|_2^2 \left\| \omega_{A'B} - \pi_{A'} \otimes \omega_B \right\|_2^2. \tag{3}$$

For our application and the proof of (3) it is convenient to reformulate the argument of the expectation value in a more symmetric way. We introduce the map $\mathcal{E}_{\tilde{A}\to R}$, which we define to be the unique Choi–Jamiołkowski preimage of the state ρ_{AR}, i.e. $\mathcal{E}_{\tilde{A}\to R}(\Phi_{A\tilde{A}}) = \rho_{AR}$, where $\tilde{A}$ is just a copy of A. Note that $\mathcal{E}$ is not trace preserving in general. We can write for any unitary U_A:

$$\mathcal{T}((U_A \otimes \mathbb{1}_R)\, \rho_{AR}\, (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_B \otimes \rho_R$$

$$= (\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}})\, \Phi_{A\tilde{A}}\, (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}})) - (\mathcal{T} \otimes \mathcal{E})(\pi_A \otimes \pi_{\tilde{A}}) \tag{4}$$

$$= (\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}})\, \xi_{A\tilde{A}}\, (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}})), \tag{5}$$

where we have introduced the *decoupling operator* $\xi_{A\tilde{A}} := \Phi_{A\tilde{A}} - \pi_A \otimes \pi_{\tilde{A}}$. Equation (4) uses the fact that an arbitrary map acting exclusively on the A subsystem of $\Phi_{A\tilde{A}}$ commutes with any map that only acts on $\tilde{A}$. In equation (5), the linearity of the maps is used. Analogously, one has that

$$\mathcal{E}(\xi_{A\tilde{A}}) = \rho_{AR} - \pi_A \otimes \rho_R, \quad \mathcal{T}(\xi_{A\tilde{A}}) = \omega_{\tilde{A}B} - \pi_{\tilde{A}} \otimes \omega_B.$$

Thus the stated result, equation (3), can be rewritten equivalently in terms of the decoupling operator.

Lemma 1. *Let* $\xi_{A\tilde{A}} = \Phi_{A\tilde{A}} - \pi_A \otimes \pi_{\tilde{A}}$ *and let* $\mathcal{T}_{A\to B} \in \mathrm{Hom}(\mathcal{L}(\mathcal{H}_A), \mathcal{L}(\mathcal{H}_B))$ *and* $\mathcal{E}_{\tilde{A}\to R} \in \mathrm{Hom}(\mathcal{L}(\mathcal{H}_{\tilde{A}}), \mathcal{L}(\mathcal{H}_R))$ *be linear maps that preserve hermiticity, then*

$$\underset{\mathbb{U}}{\mathbb{E}} \left\| (\mathcal{T}\otimes\mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}})\, \xi_{A\tilde{A}}\, (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}})) \right\|_2^2 = \frac{d_A^2}{d_A^2 - 1} \left\| \mathcal{E}(\xi_{A\tilde{A}}) \right\|_2^2 \left\| \mathcal{T}(\xi_{A\tilde{A}}) \right\|_2^2.$$

Proof. We have that

$$\underset{\mathbb{U}}{\mathbb{E}} \left\| (\mathcal{T}\otimes\mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}})\, \xi_{A\tilde{A}}\, (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}})) \right\|_2^2 = \underset{\mathbb{U}}{\mathbb{E}}\, \mathrm{tr} \left((\mathcal{T}\otimes\mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}})\, \xi_{A\tilde{A}}\, (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}}))^2 \right)$$

$$= \underset{\mathbb{U}}{\mathbb{E}}\, \mathrm{tr} \left((\mathcal{T}\otimes\mathcal{E})^{\otimes 2} \left((U_A \otimes \mathbb{1}_{\tilde{A}})^{\otimes 2} (\xi_{A\tilde{A}})^{\otimes 2} (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}})^{\otimes 2} \right) \mathcal{F}_{BR} \right) \tag{6}$$

$$= \underset{\mathbb{U}}{\mathbb{E}}\, \mathrm{tr} \left(\left((U_A \otimes \mathbb{1}_{\tilde{A}})^{\otimes 2} (\xi_{A\tilde{A}})^{\otimes 2} (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}})^{\otimes 2} \right) (\mathcal{T}^\dagger)^{\otimes 2}[\mathcal{F}_B] \otimes (\mathcal{E}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right). \tag{7}$$

We introduced two further copies A' and $\tilde{A}'$ of A when using the swap trick in equation (6), i.e. $(\xi_{A\tilde{A}})^{\otimes 2} = \xi_{A\tilde{A}} \otimes \xi_{A'\tilde{A}'}$. In equation (7), we used the definition of the adjoint of the mapping $(\mathcal{T}\otimes\mathcal{E})^{\otimes 2}$ with respect to the Schmidt scalar product. We have from [13, lemma 3.4] that

$$\underset{\mathbb{U}}{\mathbb{E}} \left((U_A)^{\dagger\otimes 2} (\mathcal{T}^\dagger)^{\otimes 2} (\mathcal{F}_B) (U_A)^{\otimes 2} \right) = \alpha \mathbb{1}_{AA'} + \beta \mathcal{F}_A$$

with the coefficients α and β satisfying

$$\alpha = \mathrm{tr}(\omega_B^2) \left(\frac{d_A^2 - \frac{d_A\, \mathrm{tr}(\omega_{A'B}^2)}{\mathrm{tr}(\omega_B^2)}}{d_A^2 - 1} \right) \quad \text{and} \quad \beta = \mathrm{tr}(\omega_{A'B}^2) \left(\frac{d_A^2 - \frac{d_A\, \mathrm{tr}(\omega_B^2)}{\mathrm{tr}(\omega_{A'B}^2)}}{d_A^2 - 1} \right).$$

Similar integrals were evaluated in the context of decoupling already in [23]. Using the above we obtain

$$\underset{\mathbb{U}}{\mathbb{E}} \left\| (\mathcal{T}\otimes\mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}})\, \xi_{A\tilde{A}}\, (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}})) \right\|_2^2 = \mathrm{tr} \left((\xi_{A\tilde{A}})^{\otimes 2} \{\alpha \mathbb{1}_{AA'} + \beta \mathcal{F}_A\} \otimes (\mathcal{E}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right)$$

$$= \beta\, \mathrm{tr} \left((\xi_{A\tilde{A}})^{\otimes 2} \mathcal{F}_A \otimes (\mathcal{E}^\dagger)^{\otimes 2}[\mathcal{F}_R] \right) \tag{8}$$

$$= \beta \left\| \mathcal{E}(\xi_{A\tilde{A}}) \right\|_2^2. \tag{9}$$

In equation (8), we used that tracing out one of the subsystems A, $\tilde{A}$ of $\xi_{A\tilde{A}}$ gives the zero state. The last line above makes use of the definition of the adjoint of $\mathcal{E}$, the swap trick and the definition of the Schatten two-norm. Rewriting β we find that

$$\begin{aligned}\beta &= \mathrm{tr}(\omega_{A'B}^2)\left(\frac{d_A^2 - \frac{d_A\,\mathrm{tr}(\omega_B^2)}{\mathrm{tr}(\omega_{A'B}^2)}}{d_A^2-1}\right)\\ &= \frac{d_A^2}{d_A^2-1}\left\|\mathcal{T}(\xi_{A\tilde{A}})\right\|_2^2. \end{aligned}\tag{10}$$

Substituting this into equation (9) yields

$$\mathop{\mathbb{E}}_{\mathbb{U}}\left\|(\mathcal{T}\otimes\mathcal{E})((U_A\otimes\mathbb{1}_{\tilde{A}})\,\xi_{A\tilde{A}}\,(U_A^\dagger\otimes\mathbb{1}_{\tilde{A}}))\right\|_2^2 = \frac{d_A^2}{d_A^2-1}\left\|\mathcal{T}(\xi_{A\tilde{A}})\right\|_2^2\left\|\mathcal{E}(\xi_{A\tilde{A}})\right\|_2^2,$$

which proves the lemma. □

3.2. *Decoupling with perfect two-designs*

In this section, we show two additional lemmas that we require for the derivation of our main result, theorem 1. Taking these lemmas together with lemma 1, we also obtain a concise derivation of the decoupling theorem for the Haar measure (cf theorem 2).

Lemma 2. *Let $\xi_{BR}\in\mathcal{L}^\dagger(\mathcal{H}_{BR})$ and let $\lambda_{BR}\in\mathcal{S}_=(\mathcal{H}_{BR})$ be invertible. Then*

$$\|\xi_{BR}\|_1 \leqslant \|\lambda_{BR}^{-\frac{1}{4}}\,\xi_{BR}\,\lambda_{BR}^{-\frac{1}{4}}\|_2.$$

Proof. The lemma follows from an application of the Hölder-type inequality $\|ABC\|_1 \leqslant \left\||A|^4\right\|_1^{\frac{1}{4}}\left\||B|^2\right\|_1^{\frac{1}{2}}\left\||C|^4\right\|_1^{\frac{1}{4}}$ (see, e.g. [3]), with $A=C=(\lambda_{BR})^{\frac{1}{4}}$ and $B=\lambda_{BR}^{-\frac{1}{4}}\,\xi_{BR}\,\lambda_{BR}^{-\frac{1}{4}}$. □

Lemma 3. *For any $\xi_{AR}\in\mathcal{S}_\leqslant(\mathcal{H}_{AR})$ there is $\zeta_R\in\mathcal{S}_=(\mathcal{H}_R)$ with*

$$\frac{1}{\mathrm{tr}[\xi_{AR}]}\mathrm{tr}\left(((\mathbb{1}_A\otimes\zeta_R^{-1/2})\xi_{AR})^2\right)\leqslant 2^{-H_{\min}(A|R)_\xi}.$$

Proof. Choose ζ_R such that it saturates the bound in the definition of the $H_{\min}$-entropy. Without loss of generality ζ_R is invertible (otherwise, redefine R such that it corresponds to the support of ρ_{AR}). Then

$$\xi_{AR}\leqslant 2^{-H_{\min}(A|R)_\xi}\mathbb{1}_A\otimes\zeta_R$$

which implies that there is ζ_R with

$$\sqrt{\xi_{AR}}\,(\mathbb{1}_A\otimes\zeta_R^{-\frac{1}{2}})\xi_{AR}(\mathbb{1}_A\otimes\zeta_R^{-\frac{1}{2}})\,\sqrt{\xi_{AR}}\leqslant 2^{-H_{\min}(A|R)_\xi}\,\xi_{AR}.\tag{11}$$

Taking the trace on both sides of (11) proves lemma 3. □

Before proving our main theorem, it will be useful for the sake of completeness to first state and prove the decoupling theorem of [13] in the formulation which is given in [14]:

Theorem 2 (Decoupling theorem [13].)**.** *Let* $\rho_{AR} \in \mathcal{S}_{\leqslant}(\mathcal{H}_{AR})$ *be a subnormalized density operator and let* $\mathcal{T}_{A\to B}$ *be a linear map with Choi–Jamiołkowski representation* $\omega_{A'B} \in \mathcal{S}_{\leqslant}(\mathcal{H}_{BA'})$*, then*

$$\mathop{\mathbb{E}}_{\mathbb{U}} \|\mathcal{T}((U_A \otimes \mathbb{1}_R)\, \rho_{AR}\, (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_B \otimes \rho_R\|_1 \leqslant 2^{-\frac{1}{2}H_{\min}(A'|B)_\omega - \frac{1}{2}H_{\min}(A|R)_\rho}.$$

Proof. Note first that for a proof of theorem 2 it suffices to show that

$$\mathop{\mathbb{E}}_{\mathbb{U}} \|\mathcal{T}((U_A \otimes \mathbb{1}_R)\, \rho_{AR}\, (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_B \otimes \rho_R\|_1^2 \leqslant 2^{-H_{\min}(A'|B)_\omega - H_{\min}(A|R)_\rho} \tag{12}$$

holds and to apply the Jensen inequality. To prove equation (12), we work with the integrand in terms of the decoupling operator (lemma 1). We use lemma 2 to bound the Schatten one-norm of the integrand with the Schatten two-norm. Introducing the positive and normalized operators σ_B and ζ_R, we have

$$\begin{aligned}&\left\|(\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}})\, \xi_{A\tilde{A}}\, (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}}))\right\|_1 \\ &\quad \leqslant \left\|(\sigma_B \otimes \zeta_R)^{-\frac{1}{4}} \left((\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}})\, \xi_{A\tilde{A}}\, (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}}))\right) (\sigma_B \otimes \zeta_R)^{-\frac{1}{4}}\right\|_2.\end{aligned}$$

One can abbreviate the notation using the completely positive maps $\tilde{\mathcal{T}}_{A\to B}$ and $\tilde{\mathcal{E}}_{\tilde{A}\to R}$ defining

$$\tilde{\mathcal{T}}(\tau_{A\tilde{A}}) := (\sigma_B \otimes \mathbb{1}_{\tilde{A}})^{-1/4}\mathcal{T}(\tau_{A\tilde{A}})(\sigma_B \otimes \mathbb{1}_{\tilde{A}})^{-1/4} \quad \forall\, \tau_{A\tilde{A}} \in \mathcal{L}(\mathcal{H}_{A\tilde{A}}), \tag{13}$$

$$\tilde{\mathcal{E}}(\tau_{A\tilde{A}}) := (\mathbb{1}_A \otimes \zeta_R)^{-1/4}\mathcal{E}(\tau_{A\tilde{A}})(\mathbb{1}_A \otimes \zeta_R)^{-1/4} \quad \forall\, \tau_{A\tilde{A}} \in \mathcal{L}(\mathcal{H}_{A\tilde{A}}), \tag{14}$$

and $\tilde{\omega}_{A'B} := \tilde{\mathcal{T}}(\Phi_{AA'}),\ \tilde{\rho}_{AR} := \tilde{\mathcal{E}}(\Phi_{A\tilde{A}})$, which yields

$$\begin{aligned}\mathop{\mathbb{E}}_{\mathbb{U}} \left\|(\mathcal{T} \otimes \mathcal{E})((U_A \otimes \mathbb{1}_{\tilde{A}})\, \xi_{A\tilde{A}}\, (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}}))\right\|_1^2 &\leqslant \mathop{\mathbb{E}}_{\mathbb{U}} \left\|(\tilde{\mathcal{T}} \otimes \tilde{\mathcal{E}})((U_A \otimes \mathbb{1}_{\tilde{A}})\, \xi_{A\tilde{A}}\, (U_A^\dagger \otimes \mathbb{1}_{\tilde{A}}))\right\|_2^2 \\ &= \frac{d_A^2}{d_A^2 - 1} \left\|\tilde{\mathcal{T}}(\xi_{A\tilde{A}})\right\|_2^2 \left\|\tilde{\mathcal{E}}(\xi_{A\tilde{A}})\right\|_2^2.\end{aligned} \tag{15}$$

By equation (10) we have that

$$\begin{aligned}\frac{d_A^2}{d_A^2 - 1} \left\|\tilde{\mathcal{T}}(\xi_{A\tilde{A}})\right\|_2^2 \left\|\tilde{\mathcal{E}}(\xi_{A\tilde{A}})\right\|_2^2 &= \left(1 - \frac{1}{d_A^2}\right) \mathrm{tr}(\tilde{\omega}_{A'B}^2)\, \mathrm{tr}(\tilde{\rho}_{AR}^2) \left(\frac{d_A^2 - \frac{d_A\, \mathrm{tr}(\tilde{\omega}_B^2)}{\mathrm{tr}(\tilde{\omega}_{A'B}^2)}}{d_A^2 - 1}\right) \left(\frac{d_A^2 - \frac{d_A\, \mathrm{tr}(\tilde{\rho}_R^2)}{\mathrm{tr}(\tilde{\rho}_{AR}^2)}}{d_A^2 - 1}\right) \\ &\leqslant \frac{1}{\mathrm{tr}[\omega_{A'B}]} \mathrm{tr}(\tilde{\omega}_{A'B}^2)\, \frac{1}{\mathrm{tr}[\rho_{AR}]} \mathrm{tr}(\tilde{\rho}_{AR}^2).\end{aligned} \tag{16}$$

In equation (16) we used the Cauchy–Schwarz inequality (lemma 3.5 in [13]) to infer that both bracket terms are smaller than one. The derivation is valid for any positive and normalized operators σ_B and ζ_R, therefore one can choose $\hat{\sigma}_B$ and $\hat{\zeta}_R$ such that they minimize the expression in (16). An application of lemma 3 then shows that

$$\mathop{\mathbb{E}}_{\mathbb{U}} \left\|\mathcal{T}((U_A \otimes \mathbb{1}_R)\, \rho_{AR}\, (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_B \otimes \rho_R\right\|_1^2 \leqslant 2^{-H_{\min}(A'|B)_\omega - H_{\min}(A|R)_\rho}.$$

□

3.3. Decoupling with δ-approximate two-designs

This section is devoted to a proof of the core theorem of this paper:

Proof of theorem 1. Due to the Jensen inequality it suffices to show that

$$\mathop{\mathbb{E}}_{\mathcal{D}} \|\mathcal{T}((U_A\otimes \mathbb{1}_R)\,\rho_{AR}\,(U_A^\dagger\otimes\mathbb{1}_R)) - \omega_B\otimes\rho_R\|_1^2 \leqslant \left(1+4\delta d_A^4\right)\, 2^{-H_{\min}(A'|B)_\omega - H_{\min}(A|R)_\rho} \tag{17}$$

holds. To prove (17), we proceed in a similar fashion to our proof of theorem 2. As before, we introduce the map $\mathcal{E}_{\tilde A\to B}$ which we define to be the unique Choi–Jamiołkowski preimage of ρ_{AR} and the state $\xi_{A\tilde A} = \Phi_{A\tilde A} - \pi_A\otimes\pi_{\tilde A}$ and write for any unitary:

$$\mathcal{T}((U_A\otimes\mathbb{1}_R)\rho_{AR}(U_A^\dagger\otimes\mathbb{1}_R)) - \omega_B\otimes\rho_R = (\mathcal{T}\otimes\mathcal{E})((U_A\otimes\mathbb{1}_{\tilde A})\xi_{A\tilde A}(U_A^\dagger\otimes\mathbb{1}_{\tilde A})).$$

To upper bound the left-hand side of (17), we apply lemma 2. We introduce positive, normalized operators σ_B and ζ_R and the maps $\tilde{\mathcal{T}}$ and $\tilde{\mathcal{E}}$ as defined in equations (13) and (14), respectively, and find

$$\begin{aligned}\mathop{\mathbb{E}}_{\mathcal{D}} \left\|(\mathcal{T}\otimes\mathcal{E})((U_A\otimes\mathbb{1}_{\tilde A})\,\xi_{A\tilde A}\,(U_A^\dagger\otimes\mathbb{1}_{\tilde A}))\right\|_1^2 &\leqslant \mathop{\mathbb{E}}_{\mathcal{D}} \left\|(\tilde{\mathcal{T}}\otimes\tilde{\mathcal{E}})((U_A\otimes\mathbb{1}_{\tilde A})\,\xi_{A\tilde A}\,(U_A^\dagger\otimes\mathbb{1}_{\tilde A}))\right\|_2^2 \\ &= \mathop{\mathbb{E}}_{\mathcal{D}} \operatorname{tr}\left((\tilde{\mathcal{T}}\otimes\tilde{\mathcal{E}})((U_A\otimes\mathbb{1}_{\tilde A})\,\xi_{A\tilde A}\,(U_A^\dagger\otimes\mathbb{1}_{\tilde A}))\right).\end{aligned}$$

Applying the swap trick and using the definitions of the adjoint mappings of $\tilde{\mathcal{T}}$ and $\tilde{\mathcal{E}}$ gives

$$\begin{aligned}&\mathop{\mathbb{E}}_{\mathcal{D}} \operatorname{tr}\left((\tilde{\mathcal{T}}\otimes\tilde{\mathcal{E}})((U_A\otimes\mathbb{1}_{\tilde A})\,\xi_{A\tilde A}\,(U_A^\dagger\otimes\mathbb{1}_{\tilde A}))^2\right) \\ &\qquad = \mathop{\mathbb{E}}_{\mathcal{D}} \operatorname{tr}\left(\left((U_A\otimes\mathbb{1}_{\tilde A})^{\otimes 2}\,(\xi_{A\tilde A})^{\otimes 2}\,(U_A^\dagger\otimes\mathbb{1}_{\tilde A})^{\otimes 2}\right)(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\otimes(\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right).\end{aligned}$$

With the relations

$$\begin{aligned}\mathop{\mathbb{E}}_{\mathcal{D}}\left((U_A^{\otimes 2}\otimes\mathbb{1}_{\tilde A}^{\otimes 2})\,(\xi_{A\tilde A})^{\otimes 2}\,((U_A^\dagger)^{\otimes 2}\otimes\mathbb{1}_{\tilde A}^{\otimes 2})\right) &= (\mathcal{G}_W\otimes\mathcal{I}_{\tilde A\tilde A'})(\xi_{A\tilde A}^{\otimes 2}), \\ \mathop{\mathbb{E}}_{\mathbb{U}}\left((U_A^{\otimes 2}\otimes\mathbb{1}_{\tilde A}^{\otimes 2})\,(\xi_{A\tilde A})^{\otimes 2}\,((U_A^\dagger)^{\otimes 2}\otimes\mathbb{1}_{\tilde A}^{\otimes 2})\right) &= (\mathcal{G}_H\otimes\mathcal{I}_{\tilde A\tilde A'})(\xi_{A\tilde A}^{\otimes 2}),\end{aligned}$$

we have

$$\begin{aligned}&\operatorname{tr}\left(\mathop{\mathbb{E}}_{\mathcal{D}}\left((U_A^{\otimes 2}\otimes\mathbb{1}_{\tilde A}^{\otimes 2})\,(\xi_{A\tilde A})^{\otimes 2}\,((U_A^\dagger)^{\otimes 2}\otimes\mathbb{1}_{\tilde A}^{\otimes 2})\right)(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\otimes(\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right) \\ &\qquad = \operatorname{tr}\left(\left((\mathcal{G}_W\otimes\mathcal{I}_{\tilde A\tilde A'})(\xi_{A\tilde A}^{\otimes 2}) - \left(\mathcal{G}_H\otimes\mathcal{I}_{\tilde A\tilde A'}\right)(\xi_{A\tilde A}^{\otimes 2})\right)(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\otimes(\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right) \\ &\qquad\quad + \operatorname{tr}\left(\left(\mathcal{G}_H\otimes\mathcal{I}_{\tilde A\tilde A'}\right)(\xi_{A\tilde A}^{\otimes 2})\;(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\otimes(\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right).\end{aligned} \tag{18}$$

For now we fix our attention on the first term of equation (18). Bounding this term gives

$$\begin{aligned}&\left\|\left((\mathcal{G}_W\otimes\mathcal{I}_{\tilde A\tilde A'})(\xi_{A\tilde A}^{\otimes 2}) - \left(\mathcal{G}_H\otimes\mathcal{I}_{\tilde A\tilde A'}\right)(\xi_{A\tilde A}^{\otimes 2})\right)(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\otimes(\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right\|_1 \\ &\qquad \leqslant \left\|\left(\mathcal{G}_W\otimes\mathcal{I}_{\tilde A\tilde A'} - \mathcal{G}_H\otimes\mathcal{I}_{\tilde A\tilde A'}\right)(\xi_{A\tilde A}^{\otimes 2})\right\|_1\left\|(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\right\|_\infty\left\|(\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right\|_\infty \\ &\qquad \leqslant \|\mathcal{G}_W - \mathcal{G}_H\|_\diamond\left\|\xi_{A\tilde A}^{\otimes 2}\right\|_1\left\|(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\right\|_\infty\left\|(\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right\|_\infty \\ &\qquad \leqslant 4\delta\left\|(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\right\|_\infty\left\|(\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right\|_\infty,\end{aligned} \tag{19}$$

where inequality (19) uses the explicit form of $\xi_{A\tilde{A}} = \Phi_{A\tilde{A}} - \pi_A \otimes \pi_{\tilde{A}}$ and the definition of the δ-approximate two-design. In the following steps, we upper bound the term $\|(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\|_\infty$. Let $P^+_{AA'}$ be the projector corresponding to the biggest absolute eigenvalue of $(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]$. The ∞-norm can then be rewritten as

$$\left\|(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\right\|_\infty = \left|\mathrm{tr}\left((\tilde{\mathcal{T}})^{\otimes 2}[P^+_{AA'}]\mathcal{F}_B\right)\right|. \tag{20}$$

To be able to apply the swap trick, we decompose $P^+_{AA'}$ into some basis: $P^+_{AA'} = \sum_{i,j} c_{ij}\sigma^i_A \otimes \sigma^j_{A'}$. Without loss of generality, we choose the coefficients c_{ij} to be real. This gives

$$\mathrm{tr}\left((\tilde{\mathcal{T}})^{\otimes 2}[P^+_{AA'}]\mathcal{F}_B\right) = \sum_{i,j} c_{ij}\mathrm{tr}\left(\tilde{\mathcal{T}}(\sigma^i_A)\tilde{\mathcal{T}}(\sigma^j_{A'})\right). \tag{21}$$

We rewrite $\tilde{\mathcal{T}}(\sigma^i_A)$ using the Choi–Jamiołkowski representation of $\tilde{\mathcal{T}}$

$$\begin{aligned}\sum_{i,j} c_{ij}\mathrm{tr}\left((\tilde{\mathcal{T}}(\sigma^i_A)\tilde{\mathcal{T}}(\sigma^j_{A'}))\right) &= d_A^2 \sum_{i,j} c_{ij}\mathrm{tr}\left(\mathrm{tr}_A\left(\tilde{\omega}_{AB}\left(\mathbb{1}_B \otimes (\sigma^i_A)^\mathsf{T}\right)\right)\mathrm{tr}_{A'}\left(\tilde{\omega}_{A'B}\left(\mathbb{1}_B \otimes (\sigma^j_{A'})^\mathsf{T}\right)\right)\right)\\ &= d_A^2\mathrm{tr}\left((\mathbb{1}_{A'} \otimes \tilde{\omega}_{AB})(\mathbb{1}_A \otimes \tilde{\omega}_{A'B})(\mathbb{1}_B \otimes (P^+_{AA'})^\mathsf{T})\right).\end{aligned} \tag{22}$$

To obtain an upper bound for equation (22), we apply the following lemma 4. □

Lemma 4. *Let $\omega_{AB} \in \mathcal{L}^\dagger(\mathcal{H}_{AB})$, $\omega_{A'B} \in \mathcal{L}^\dagger(\mathcal{H}_{A'B})$ and let $\rho_{AA'} \in \mathcal{L}^\dagger(\mathcal{H}_{AA'})$, then*

$$|\mathrm{tr}\left((\mathbb{1}_{A'} \otimes \omega_{AB})(\mathbb{1}_A \otimes \omega_{A'B})(\mathbb{1}_B \otimes \rho_{AA'})\right)| \leqslant \mathrm{tr}\left(\omega^2_{AB}\right)\sqrt{\mathrm{tr}\left(\rho^2_{AA'}\right)}.$$

The proof of this lemma will be given after concluding the proof of theorem 1. We use the fact that $(P^+_{AA'})^\mathsf{T}$ is a rank one projector and obtain

$$\mathrm{tr}\left((\mathbb{1}_{A'} \otimes \tilde{\omega}_{AB})(\mathbb{1}_A \otimes \tilde{\omega}_{A'B})(\mathbb{1}_B \otimes (P^+_{AA'})^\mathsf{T})\right) \leqslant \mathrm{tr}\left(\tilde{\omega}^2_{A'B}\right). \tag{23}$$

This gives the bound

$$\left\|(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B]\right\|_\infty \leqslant d_A^2\mathrm{tr}\left(\tilde{\omega}^2_{A'B}\right).$$

And identically we find that

$$\left\|(\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right\|_\infty \leqslant d_A^2\mathrm{tr}\left(\tilde{\rho}^2_{AR}\right).$$

Thus we obtain the desired bound for the first term of (18) using (19):

$$\begin{aligned}&\left\|\left((\mathcal{G}_W \otimes \mathcal{I}_{\tilde{A}\tilde{A}'})(\xi^{\otimes 2}_{A\tilde{A}}) - \left(\mathcal{G}_H \otimes \mathcal{I}_{\tilde{A}\tilde{A}'}\right)(\xi^{\otimes 2}_{A\tilde{A}})\right)(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right\|_1\\ &\quad\leqslant 4\delta d_A^4 \frac{1}{\mathrm{tr}[\omega_{A'B}]}\mathrm{tr}\left(\tilde{\omega}^2_{A'B}\right)\frac{1}{\mathrm{tr}[\rho_{AR}]}\mathrm{tr}\left(\tilde{\rho}^2_{AR}\right).\end{aligned} \tag{24}$$

The only thing left is to evaluate the second term of (18), but this term was already calculated as a part of the proof of the decoupling theorem. It equals the term on the right-hand side of (15) and can be bounded using (16):

$$\mathrm{tr}\left(\left(\mathcal{G}_H \otimes \mathcal{I}_{\tilde{A}\tilde{A}'}\right)(\xi^{\otimes 2}_{A\tilde{A}})(\tilde{\mathcal{T}}^\dagger)^{\otimes 2}[\mathcal{F}_B] \otimes (\tilde{\mathcal{E}}^\dagger)^{\otimes 2}[\mathcal{F}_R]\right) \leqslant \frac{1}{\mathrm{tr}[\omega_{A'B}]}\mathrm{tr}\left(\tilde{\omega}^2_{A'B}\right)\frac{1}{\mathrm{tr}[\rho_{AR}]}\mathrm{tr}\left(\tilde{\rho}^2_{AR}\right). \tag{25}$$

An application of lemma 3 on (24) and (25) gives

$$\mathop{\mathbb{E}}_{\mathcal{D}} \|\mathcal{T}((U_A \otimes \mathbb{1}_R)\, \rho_{AR}\, (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_B \otimes \rho_R\|_1^2 \leqslant \left(1 + 4\delta d_A^4\right) 2^{-H_{\min}(A'|B)_\omega - H_{\min}(A|R)_\rho}$$

which proves (17) and thus concludes the proof of the decoupling theorem with approximate two-designs.

Proof of lemma 4. We introduce a basis $\{\sigma_A^i\}_i$ for $\mathcal{L}^\dagger(\mathcal{H}_A)$ and a basis $\{\sigma_B^i\}_i$ for $\mathcal{L}^\dagger(\mathcal{H}_B)$. Moreover, we choose them to be orthonormal with respect to the Schmidt scalar product (i.e. $\mathrm{tr}(\sigma_A^i \sigma_A^j) = \delta_{ij}$ and likewise for the B system). Hence, the product operators $\{\sigma_A^i \otimes \sigma_B^j\}_{i,j}$ also form an orthonormal basis for $\mathcal{L}^\dagger(\mathcal{H}_{AB})$ with respect to the Schmidt scalar product:

$$\mathrm{tr}\left((\sigma_A^i \otimes \sigma_B^j)\,(\sigma_A^k \otimes \sigma_B^l)\right) = \mathrm{tr}\left(\sigma_A^i \sigma_A^k\right) \cdot \mathrm{tr}\left(\sigma_B^j \sigma_B^l\right) = \delta_{ik}\delta_{jl}.$$

We write the operators ω_{AB}, $\omega_{A'B}$ and $\rho_{AA'}$ in that basis:

$$\omega_{AB} := \sum_{i,j} a_{ij} \sigma_A^i \otimes \sigma_B^j, \quad a_{ij} := \mathrm{tr}\left((\sigma_A^i \otimes \sigma_B^j)\, \omega_{AB}\right),$$

$$\omega_{A'B} := \sum_{i,j} a_{ij} \sigma_{A'}^i \otimes \sigma_B^j, \quad a_{ij} := \mathrm{tr}\left((\sigma_{A'}^i \otimes \sigma_B^j)\, \omega_{A'B}\right),$$

$$\rho_{AA'} := \sum_{i,j} c_{ij} \sigma_A^i \otimes \sigma_{A'}^j, \quad c_{ij} := \mathrm{tr}\left((\sigma_A^i \otimes \sigma_{A'}^j)\, \rho_{AA'}\right).$$

Since all matrices in the above statements are Hermitian, the coefficients a_{ij} and c_{ij} are real. Moreover, the coefficients in the expansion of ω_{AB} and $\omega_{A'B}$ are the same, because the corresponding matrices are the same. Substituting the expansions into the left-hand side of the lemma gives

$$\begin{aligned}
&\mathrm{tr}\left((\mathbb{1}_{A'} \otimes \omega_{AB})\,(\mathbb{1}_A \otimes \omega_{A'B})\,(\mathbb{1}_B \otimes \rho_{AA'})\right)\\
&\quad= \sum_{i,j,k,l,m,n} a_{ij}a_{kl}c_{mn}\mathrm{tr}\left((\mathbb{1}_{A'} \otimes \sigma_A^i \otimes \sigma_B^j)\,(\mathbb{1}_A \otimes \sigma_{A'}^k \otimes \sigma_B^l)\,(\mathbb{1}_B \otimes \sigma_A^m \otimes \sigma_{A'}^n)\right)\\
&\quad= \sum_{i,j,k,l,m,n} a_{ij}a_{kl}c_{mn}\mathrm{tr}\left(\sigma_A^i \sigma_A^m\right)\mathrm{tr}\left(\sigma_{A'}^k \sigma_{A'}^n\right)\mathrm{tr}\left(\sigma_B^j \sigma_B^l\right)\\
&\quad= \sum_{i,j,k,l,m,n} a_{ij}a_{kl}c_{mn}\delta_{im}\delta_{kn}\delta_{jl}\\
&\quad= \sum_{i,j,k} a_{ij}a_{kj}c_{ik}.
\end{aligned} \tag{26}$$

We now introduce the matrices $A := (a_{ij})$ and $C := (c_{ij})$ and use equation (26) to find that

$$\begin{aligned}
|\mathrm{tr}\left((\mathbb{1}_{A'} \otimes \omega_{AB})\,(\mathbb{1}_A \otimes \omega_{A'B})\,(\mathbb{1}_B \otimes \rho_{AA'})\right)| &= \left|\mathrm{tr}\left(A^\dagger C A\right)\right|\\
&\leqslant \left\|AA^\dagger\right\|_1 \|C\|_\infty\\
&\leqslant \mathrm{tr}\left(AA^\dagger\right)\|C\|_2.
\end{aligned} \tag{27}$$

We calculate the Schatten two-norm of C using that $\|C\|_2{}^2 = \sum_{ij} |c_{ij}|^2$ ([3]) and the explicit formula for the c_{ij}:

$$\begin{aligned}
\|C\|_2{}^2 &= \sum_{ij} |c_{ij}|^2 \\
&= \sum_{ij} \mathrm{tr}\left((\sigma_A^i \otimes \sigma_{A'}^j)\, \rho_{AA'} \right) \mathrm{tr}\left((\sigma_A^i \otimes \sigma_{A'}^j)\, \rho_{AA'} \right) \\
&= \mathrm{tr}\left(\left(\sum_{ij} \mathrm{tr}\left(\sigma_A^i \otimes \sigma_{A'}^j \rho_{AA'} \right) \sigma_A^i \otimes \sigma_{A'}^j \right) \rho_{AA'} \right) \\
&= \mathrm{tr}\left(\rho_{AA'}^2 \right).
\end{aligned} \tag{28}$$

The trace term in (27) can be calculated similarly. We use the explicit formula for the coefficients:

$$\begin{aligned}
\mathrm{tr}\left(AA^\dagger \right) &= \sum_{ij} a_{ij} a_{ij} \\
&= \sum_{ij} \mathrm{tr}\left((\sigma_{A'}^i \otimes \sigma_B^j)\, \omega_{A'B} \right) \mathrm{tr}\left((\sigma_{A'}^i \otimes \sigma_B^j)\, \omega_{A'B} \right) \\
&= \mathrm{tr}\left(\left(\sum_{ij} \mathrm{tr}\left(\sigma_{A'}^i \otimes \sigma_B^j \omega_{A'B} \right) \sigma_{A'}^i \otimes \sigma_B^j \right) \omega_{A'B} \right) \\
&= \mathrm{tr}\left(\omega_{A'B}^2 \right).
\end{aligned} \tag{29}$$

Taking (28) together with (29) and substituting them into (27) concludes the proof of lemma 4. □

3.4. A smoothed decoupling formula for approximate two-designs

In order to achieve a tighter bound in the decoupling formula for approximate two-designs (theorem 1), we now introduce a modified upper bound stated in terms of *smooth* conditional min-entropies (see definition 2). We refer to [14] for a discussion of the optimality of decoupling in terms of these quantities. The smooth conditional min-entropy has the additional advantage that it reduces to the von Neumann entropy in the important special case where the state is a tensor product of many identical states, as shown by the fully quantum asymptotic equipartition theorem (see equation (2)).

Theorem 3 (Smoothed decoupling formula for δ-approximate two-designs). *Let $\rho_{AR} \in \mathcal{S}_\leqslant(\mathcal{H}_{AR})$ be a subnormalized density operator and let $\mathcal{T}_{A\to B}$ be a linear map with Choi–Jamiołkowski representation $\omega_{A'B} \in \mathcal{S}_\leqslant(\mathcal{H}_{BA'})$ and let ε be such that* $\min\{\sqrt{\mathrm{tr}(\rho)}, \sqrt{\mathrm{tr}(\omega)}\} > \varepsilon \geqslant 0$. *Then*

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathcal{D}} \left\| \mathcal{T}((U_A \otimes \mathbb{1}_R)\rho_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) - \omega_B \otimes \rho_R \right\|_1 \\
&\qquad \leqslant \sqrt{1 + 4\delta d_A^4}\, 2^{-\frac{1}{2} H_{\min}^\varepsilon(A'|B)_\omega - \frac{1}{2} H_{\min}^\varepsilon(A|R)_\rho} + 8 d_A \delta\, \varepsilon + 12\varepsilon,
\end{aligned}$$

where $\mathcal{D}$ constitutes a δ-approximate two-design.

Proof. Let $\hat{\omega}_{A'B} \in \mathcal{S}_{\leqslant}(\mathcal{H}_{A'B})$ be the state that saturates the bound in the definition of $H^{\varepsilon}_{\min}$, i.e. $P(\omega_{A'B}, \hat{\omega}_{A'B}) \leqslant \varepsilon$ and $H_{\min}(A'|B)_{\hat{\omega}} = H^{\varepsilon}_{\min}(A'|B)_{\omega}$. Analogously $\hat{\rho}_{AR}$ is defined to be an operator with $P(\hat{\rho}_{AR}, \rho_{AR}) \leqslant \varepsilon$ and $H_{\min}(A|R)_{\hat{\rho}} = H^{\varepsilon}_{\min}(A|R)_{\rho}$.

Using inequality (1), we find that

$$\left\|\omega_{A'B} - \hat{\omega}_{A'B}\right\|_1 \leqslant 2\varepsilon, \quad \left\|\rho_{AR} - \hat{\rho}_{AR}\right\|_1 \leqslant 2\varepsilon. \tag{30}$$

We decompose $\hat{\omega} - \omega$ and $\hat{\rho} - \rho$ into positive operators with orthogonal support writing

$$\hat{\omega} - \omega = \Delta_+ - \Delta_-, \quad \hat{\rho} - \rho = \Gamma_+ - \Gamma_-$$

and conclude from (30) that

$$\|\Delta_+\|_1 \leqslant 2\varepsilon, \quad \|\Delta_-\|_1 \leqslant 2\varepsilon, \quad \|\Gamma_+\|_1 \leqslant 2\varepsilon, \quad \|\Gamma_-\|_1 \leqslant 2\varepsilon.$$

Let $\hat{\mathcal{T}}$, $\mathcal{D}_+$ and $\mathcal{D}_-$ be the unique Choi–Jamiołkowski preimages of $\hat{\omega}_{A'B}$, Δ_+ and Δ_- respectively. We apply theorem 1 on $\hat{\rho}$ and $\hat{\omega}$ to find

$$\begin{aligned}\sqrt{1+4\delta d_A^4}\, 2^{-\frac{1}{2} H^{\varepsilon}_{\min}(A'|B)_{\omega} - \frac{1}{2} H^{\varepsilon}_{\min}(A|R)_{\rho}} &= \sqrt{1+4\delta d_A^4}\, 2^{-\frac{1}{2} H_{\min}(A'|B)_{\hat{\omega}} - \frac{1}{2} H_{\min}(A|R)_{\hat{\rho}}} \\ &\geqslant \mathop{\mathbb{E}}_{\mathcal{D}} \left\|\hat{\mathcal{T}}((U_A \otimes \mathbb{1}_R)\, \hat{\rho}_{AR}\, (U_A^\dagger \otimes \mathbb{1}_R)) - \hat{\omega}_B \otimes \hat{\rho}_R\right\|_1.\end{aligned}$$

For any unitary, we have with an application of the triangle inequality

$$\begin{aligned}&\left\|\hat{\mathcal{T}}((U_A \otimes \mathbb{1}_R)\, \hat{\rho}_{AR}\, (U_A^\dagger \otimes \mathbb{1}_R)) - \hat{\omega}_B \otimes \hat{\rho}_R\right\|_1 \\ &\qquad \geqslant \left\|\hat{\mathcal{T}}((U_A \otimes \mathbb{1}_R)\, \hat{\rho}_{AR}\, (U_A^\dagger \otimes \mathbb{1}_R)) - \omega_B \otimes \hat{\rho}_R\right\|_1 - 2\varepsilon.\end{aligned}$$

In the same way $\hat{\rho}_R$ is eliminated from the product term and we obtain in total

$$\begin{aligned}&\left\|\hat{\mathcal{T}}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) - \hat{\omega}_B \otimes \hat{\rho}_R\right\|_1 \\ &\qquad \geqslant \left\|\hat{\mathcal{T}}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) - \omega_B \otimes \rho_R\right\|_1 - 4\varepsilon \\ &\qquad \geqslant \left\|\mathcal{T}((U_A \otimes \mathbb{1}_R)\rho_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) - \omega_B \otimes \rho_R\right\|_1 \\ &\qquad\quad - \left\|\mathcal{T}((U_A \otimes \mathbb{1}_R)\rho_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) - \mathcal{T}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R))\right\|_1 \\ &\qquad\quad - \left\|\hat{\mathcal{T}}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) - \mathcal{T}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R))\right\|_1 - 4\varepsilon.\end{aligned} \tag{31}$$

The first term of equation (31) corresponds to the unsmoothed decoupling formula. For the remaining two terms

$$\mathop{\mathbb{E}}_{\mathcal{D}} \left\|\mathcal{T}((U_A \otimes \mathbb{1}_R)\rho_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) - \mathcal{T}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R))\right\|_1 \tag{32}$$

and

$$\mathop{\mathbb{E}}_{\mathcal{D}} \left\|\hat{\mathcal{T}}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) - \mathcal{T}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R))\right\|_1, \tag{33}$$

we need to find upper bounds. We treat them separately beginning with the first one. To perform the calculation we write $\hat{\rho} - \rho = \Gamma_+ - \Gamma_-$ and use the linearity of $\mathcal{T}$. We obtain

$$\begin{align}
&\underset{\mathcal{D}}{\mathbb{E}} \left\| \mathcal{T}((U_A \otimes \mathbb{1}_R)\rho_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) - \mathcal{T}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) \right\|_1 \nonumber\\
&\qquad\leqslant \sum_{a\in\{+,-\}} \underset{\mathcal{D}}{\mathbb{E}} \left\| \mathcal{T}((U_A \otimes \mathbb{1}_R)\Gamma_a(U_A^\dagger \otimes \mathbb{1}_R)) \right\|_1 \nonumber\\
&\qquad= \sum_{a\in\{+,-\}} \mathrm{tr}\left(\mathcal{T}\left(\left(\underset{\mathcal{D}}{\mathbb{E}} - \underset{\mathbb{U}}{\mathbb{E}}\right)\left((U_A \otimes \mathbb{1}_R)\Gamma_a(U_A^\dagger \otimes \mathbb{1}_R)\right)\right)\right) \nonumber\\
&\qquad\quad + \sum_{a\in\{+,-\}} \mathrm{tr}\left(\mathcal{T}\left(\underset{\mathbb{U}}{\mathbb{E}}\left((U_A \otimes \mathbb{1}_R)\Gamma_a(U_A^\dagger \otimes \mathbb{1}_R)\right)\right)\right) \nonumber\\
&\qquad\leqslant \sum_{a\in\{+,-\}} \left\|\left(\underset{\mathcal{D}}{\mathbb{E}} - \underset{\mathbb{U}}{\mathbb{E}}\right)\left((U_A \otimes \mathbb{1}_R)\Gamma_a(U_A^\dagger \otimes \mathbb{1}_R)\right)\right\|_1 \left\|\mathcal{T}^\dagger(\mathbb{1}_B)\right\|_\infty \nonumber\\
&\qquad\quad + \sum_{a\in\{+,-\}} \mathrm{tr}\left(\mathcal{T}(\pi_A) \otimes \mathrm{tr}_A\, \Gamma_a\right) \nonumber\\
&\qquad\leqslant \sum_{a\in\{+,-\}} \delta\, \|\Gamma_a\|_1 \left\|\mathcal{T}^\dagger(\mathbb{1}_B)\right\|_\infty + \sum_{a\in\{+,-\}} \mathrm{tr}\,(\omega_{A'B})\mathrm{tr}\,(\Gamma_a) \tag{34}\\
&\qquad\leqslant 4 d_A \delta\varepsilon + 4\varepsilon. \tag{35}
\end{align}$$

Inequality (34) used that an approximate two-design constitutes an approximate one-design automatically. This can be seen straight from the definition by considering states that are given by the identity operator on one of the systems on which the unitaries act. The last inequality (35) can be seen by choosing the eigenvalue of $\mathcal{T}^\dagger(\mathbb{1}_B)$ which is the biggest in absolute value and defining P_A to be the projector corresponding to this eigenvalue. One then has $\left\|\mathcal{T}^\dagger(\mathbb{1}_B)\right\|_\infty \leqslant d_A$.

Bounding the term (33) is done similarly. We decompose $\hat{\mathcal{T}} - \mathcal{T} = \mathcal{D}_+ - \mathcal{D}_-$ in accordance with the decomposition $\hat{\omega} - \omega = \Delta_+ - \Delta_-$. We then obtain

$$\begin{aligned}
&\underset{\mathcal{D}}{\mathbb{E}} \left\| \hat{\mathcal{T}}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) - \mathcal{T}((U_A \otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger \otimes \mathbb{1}_R)) \right\|_1 \\
&\qquad\leqslant \sum_{a\in\{+,-\}} \mathrm{tr}\left(\mathcal{D}_a\left(\underset{\mathcal{D}}{\mathbb{E}}\ (U_A \otimes \mathbb{1}_R)\ \hat{\rho}_{AR}\ (U_A^\dagger \otimes \mathbb{1}_R)\right)\right) \\
&\qquad= \sum_{a\in\{+,-\}} \mathrm{tr}\left(\mathcal{D}_a\left(\left(\underset{\mathcal{D}}{\mathbb{E}} - \underset{\mathbb{U}}{\mathbb{E}}\right)\left((U_A \otimes \mathbb{1}_R)\ \hat{\rho}_{AR}\ (U_A^\dagger \otimes \mathbb{1}_R)\right)\right)\right) \\
&\qquad\quad + \sum_{a\in\{+,-\}} \mathrm{tr}\left(\mathcal{D}_a\left(\underset{\mathbb{U}}{\mathbb{E}}\left((U_A \otimes \mathbb{1}_R)\ \hat{\rho}_{AR}\ (U_A^\dagger \otimes \mathbb{1}_R)\right)\right)\right) \\
&\qquad\leqslant \sum_{a\in\{+,-\}} \left\|\left(\underset{\mathcal{D}}{\mathbb{E}} - \underset{\mathbb{U}}{\mathbb{E}}\right)\left((U_A \otimes \mathbb{1}_R)\ \hat{\rho}_{AR}\ (U_A^\dagger \otimes \mathbb{1}_R)\right)\right\|_1 \left\|\mathcal{D}_a^\dagger(\mathbb{1}_B)\right\|_\infty \\
&\qquad\quad + \sum_{a\in\{+,-\}} \mathrm{tr}\left(\mathcal{D}_a(\pi_A \otimes \hat{\rho}_R)\right)
\end{aligned}$$

$$\begin{aligned}&\leqslant \sum_{a\in\{+,-\}} \delta \,\|\hat{\rho}_{AR}\|_1 \left\|\mathcal{D}_a^\dagger(\mathbb{1}_B)\right\|_\infty + \sum_{a\in\{+,-\}} \operatorname{tr}\left(\Delta_a \otimes \hat{\rho}_R\right)\\ &\leqslant 4d_A\delta\varepsilon + 4\varepsilon. \end{aligned} \tag{36}$$

Combining the expressions (35) and (36) and substituting them into (31), we obtain

$$\begin{aligned}&\mathop{\mathbb{E}}_{\mathcal{D}} \left\|\hat{\mathcal{T}}((U_A\otimes \mathbb{1}_R)\hat{\rho}_{AR}(U_A^\dagger\otimes\mathbb{1}_R)) - \hat{\omega}_B\otimes\hat{\rho}_R\right\|_1\\ &\qquad\qquad \geqslant \mathop{\mathbb{E}}_{\mathcal{D}} \left\|\mathcal{T}((U_A\otimes \mathbb{1}_R)\rho_{AR}(U_A^\dagger\otimes\mathbb{1}_R)) - \omega_B\otimes\rho_R\right\|_1 - 8d_A\delta\varepsilon - 12\varepsilon.\end{aligned}$$

Finally this yields

$$\begin{aligned}&\mathop{\mathbb{E}}_{\mathcal{D}} \left\|\mathcal{T}((U_A\otimes \mathbb{1}_R)\rho_{AR}(U_A^\dagger\otimes\mathbb{1}_R)) - \omega_B\otimes\rho_R\right\|_1\\ &\qquad\qquad \leqslant \sqrt{1+4\delta d_A^4}\, 2^{-\frac{1}{2}H_{\min}^{\varepsilon}(A'|B)_\omega - \frac{1}{2}H_{\min}^{\varepsilon}(A|R)_\rho} + 8d_A\delta\,\varepsilon + 12\varepsilon\end{aligned}$$

which proves the smoothed decoupling formula for δ-approximate two-designs. □

4. Decoupling in physical systems

In this section, we explain how our result can be applied to study a typical evolution of a physical system. Consider, as before, a joint system AR in an initial state ρ_{AR} and assume that the A system consists of a large number of interacting particles. In a physical scenario A might be correlated with a huge, diffuse subsystem of the universe such that R might be much larger than A. The most common type of interaction in nature is a local two-particle interaction. It can be modeled using a two-qubit unitary gate. More generally, one may describe the randomization process induced by the evolution of a many-particle system using a quantum circuit. Such approaches were considered earlier for instance in [7, 19]. The circuit is constructed in the following way: at each step of the circuit, two qubits from A and an element of a universal gate set for $\mathbb{U}(4)$ are chosen uniformly at random. The gate is applied to the qubits and the circuit proceeds to the next step. For a given circuit time t, we consider the set of all possible unitaries the circuit can produce together with the corresponding probabilities. If t goes to infinity this yields the Haar distribution on the whole unitary group [19]. Unfortunately, it turns out that the convergence rate of the random circuit toward the Haar distribution is exponentially slow in the number of qubits of the underlying system [7, 19, 29]. Nevertheless, after a time t that grows polynomially in the number of qubits and logarithmically in $\frac{1}{\delta}$, the above circuit will constitute a δ-approximate two-design.

More precisely, the authors of [19] (theorems 2.9 and 2.10) and [11] derive the following pivotal theorem.

Theorem 4 (Random quantum circuits are approximate two-designs [11, 19])**.** *Let μ be the probability distribution corresponding to any universal gate set on $\mathbb{U}(4)$ and let W be a random circuit on n qubits obtained by drawing t random unitaries according to μ and applying each of them to a random pair of qubits. Then there exists C (and $C = C(\mu)$ only) such that for any $\delta > 0$ and any $t \geqslant C(n^2 + n\log(1/\delta))$, the set of unitaries produced by W together with the corresponding probabilities forms a δ-approximate unitary two-design.*

Following the discussion in [7], we will assume that typical dynamics in nature are given by (short) circuits of the type of theorem 4. We conclude that in our model the possible evolutions of a many qubit system are given by elements of a unitary approximate two-design. Moreover, theorem 4 states that in order to reach a δ-approximate two-design a circuit time $t := C(n^2 + n\log\frac{1}{\delta})$ is sufficient, with C being some constant that only depends on the concrete circuit used.

We can now apply our decoupling theorem for approximate two-designs to infer conditions under which typical processes in nature result in decoupling. In this example, we shall assume that the R system is correlated with a subsystem of A and we are interested in how this correlation behaves under a typical evolution. Hence, we decompose A into two parts: A_S, which identifies the subsystem of interest; and A_E, which corresponds to an environmental system which is uncorrelated with R. Since we are interested in the state of A_S we choose $\mathcal{T}$ to be the partial trace on the environment system: $\mathcal{T}(\rho) = \mathrm{tr}_{A_\mathrm{E}}[\rho]$. Formally, this implies that $H_{\min}(A|R)_\rho \geqslant -\log d_{A_\mathrm{S}}$ and $H_{\min}(A'|E)_\omega \geqslant \log d_{A_\mathrm{E}} - \log d_{A_\mathrm{S}}$ (see lemma 20 in [34]). An application of Markov's inequality to the decoupling formula for approximate two-designs shows that, for any $\epsilon > 0$, one has

$$\Pr_W\left\{\|\mathrm{tr}_{A_\mathrm{E}}\left((W_A \otimes \mathbb{1}_R)\,\rho_{AR}\,(W_A^\dagger \otimes \mathbb{1}_R)\right) - \pi_{A_\mathrm{S}} \otimes \rho_R\|_1 \geqslant \epsilon\right\}$$
$$\leqslant \frac{1}{\epsilon}\frac{d_{A_\mathrm{S}}}{\sqrt{d_{A_\mathrm{E}}}}\sqrt{1 + 4\delta d_A^4}.$$

This implies that if the environment A_E is chosen big enough, decoupling occurs except with small probability. Note, moreover, that the factor d_A^4 does not increase the time that is required until decoupling is reached in a significant way. To reach a $\bar{\delta}$-approximate two-design with $\bar{\delta} := \frac{\delta}{d_A^4}$ it is sufficient to have run the circuit for a time

$$\bar{t} := C\left(n^2 + n\log\left(\frac{2^{4n}}{\delta}\right)\right) = C\left(n^2 + 4n^2 + n\log\left(\frac{1}{\delta}\right)\right).$$

This means that once the circuit has reached a δ-approximate two-design, it suffices to wait only approximately five times longer until it generates a $\bar{\delta}$-approximate two-design. This additional time certainly does not affect our conclusions.

We summarize our discussion with a corollary and give an outlook for possible applications of our results.

Corollary 1. *Given a system A which consists of two subsystems A_S and A_E, assume that A_S is correlated with a reference system R. Furthermore, assume the A system to consist of interacting particles, whose dynamics can be described with the above circuit model. Then if A_E is chosen large enough a typical process reaches decoupling after polynomial time except with small probability.*

In the context of black hole evaporation a result similar to theorem 1 occurs in [22, inequality (5.1)]. However, the validity of this formula is restricted to the approximate two-designs constructed in [9], which share strong additional properties [9, equation (16)]. In the model of [22] it seems reasonable to assume that the approximate two-designs are generated via a random quantum circuit as in corollary 1. Since in general such circuits will not produce the two-designs of [9] our decoupling formula seems more appropriate for the application in [22] than inequality (5.1).

Finally, note that related results concerning the thermalization of subsystems have been derived in [17, 27, 31] and a generalization of these results using the decoupling approach has recently been proposed in [24].

Acknowledgments

The authors thank Mark Wilde for carefully reading the paper and pointing out some mistakes. This work was supported by the Swiss National Science Foundation (SNSF) through the National Centre of Competence in Research 'Quantum Science and Technology' and through grant no. 200020-135048 and by the European Research Council through grant no. 258932.

References

[1] Ando T 1979 Concavity of certain maps on positive definite matrices and applications to Hadamard products *Linear Algebra Appl.* **26** 203–41

[2] Berta M, Furrer F and Scholz V 2011 The smooth entropy formalism on von Neumann algebras. arXiv:1107.5460v1

[3] Bhatia R 1996 *Matrix Analysis* (Berlin: Springer)

[4] Carlen E 2010 *Entropy and the Quantum: Trace Inequalities and Quantum Entropy* (Providence, RI: AMS)

[5] Carter J L and Wegman M N 1979 Universal classes of hash functions *J. Comput. Syst. Sci.* **18** 143–54

[6] Choi M-D 1975 Completely positive linear maps on complex matrices *Linear Algebra Appl.* **10** 285

[7] Dahlsten O, Oliveira R and Plenio M 2007 Emergence of typical entanglement in two-party random processes *J. Phys. A: Math. Theor.* **40** 8081

[8] Dankert C 2005 Efficient simulation of random quantum states and operators *Master's Thesis* University of Waterloo (arXiv:quant-ph/0512217)

[9] Dankert C, Cleve R, Emerson J and Livine E 2009 Exact and approximate unitary 2-designs and their application to fidelity estimation *Phys. Rev.* A **80** 012304

[10] del Rio L, Åberg J, Renner R, Dahlsten O and Vedral V 2011 The thermodynamic meaning of negative entropy *Nature* **474** 61–63

[11] Diniz I and Jonathan D 2011 Comment on 'Random quantum circuits are approximate 2-designs' by A W Harrow and R A Low (*Commun. Math. Phys.* **291** 257–302 (2009)) *Commun. Math. Phys.* **304** 281–93

[12] DiVincenzo D, Leung D and Terhal B 2002 Quantum data hiding *IEEE Trans. Inform. Theory* **48** 580–99

[13] Dupuis F 2009 The decoupling approach to quantum information theory *PhD Thesis* Université de Montréal (arXiv:1004.1641v1 [quant-ph])

[14] Dupuis F, Berta M, Wullschleger J and Renner R 2010 The decoupling theorem arXiv:1012.6044v1

[15] Dür W, Hein M, Cirac J and Briegel H-J 2005 Standard forms of noisy quantum operations via depolarization *Phys. Rev.* A **72** 052326

[16] Furrer F, Aberg J and Renner R 2011 Min- and max-entropy in infinite dimensions *Commun. Math. Phys.* **306** 165–86

[17] Gemmer J, Michel M and Mahler G 2004 *Quantum Thermodynamics* (Berlin: Springer)

[18] Gottesman D 1997 Stabilizer codes and quantum error correction *PhD Thesis* California Institute of Technology (arXiv:quant-ph/9705052)

[19] Harrow A and Low R 2009 Random quantum circuits are approximate 2-designs *Commun. Math. Phys.* **291** 257–302

[20] Hayden P, Abeyesinghe A, Devetak I and Winter A 2006 The mother of all protocols: restructuring quantum information's family tree *Proc. R. Soc. Lond.* A **465** 2537–63

[21] Hayden P, Horodecki M, Yard J and Winter A 2008 A decoupling approach to the quantum capacity *World Sci. J. (OSID)* **15** 7–19

[22] Hayden P and Preskill J 2007 Black holes as mirrors: quantum information in random subsystems *J. High Energy Phys.* JHEP09(2007)120

[23] Horodecki M, Oppenheim J and Winter A 2005 Quantum state merging and negative information *Commun. Math. Phys.* **269** 107–36

[24] Hutter A 2010 The foundations of statistical physics from first principles of quantum mechanics: deriving equipartition from the decoupling approach *Semester Thesis* ETH Zürich

[25] Jamiolkowski A 1972 Linear transformations which preserve trace and positive semidefiniteness of operators *Rep. Math. Phys.* **3** 275–8

[26] Kitaev A 1997 Quantum computations: algorithms and error correction *Russ. Math. Surv.* **52** 1191–249

[27] Lloyd S 1988 Black holes, demons and the loss of coherence *PhD Thesis* The Rockefeller University

[28] Low R 2009 Pseudo-randomness and learning in quantum computation *PhD Thesis* University of Bristol (arXiv:1006.5227v1 [quant-ph])

[29] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[30] Paulsen V I 2002 *Completely Bounded Maps and Operator Algebras* (Cambridge: Cambridge University Press)

[31] Popescu S, Short A and Winter A 2006 Entanglement and the foundations of statistical mechanics *Nature Phys.* **2** 754–8

[32] Renner R 2005 Security of quantum key distribution *PhD Thesis* ETH Zürich (arXiv:quant-ph/0512258v2)

[33] Renner R and König R 2005 Universally composable privacy amplification against quantum adversaries *Proc. TCC* (*Lecture Notes in Computer Science* vol 3378) (Cambridge, MA: Springer) pp 407–25

[34] Tomamichel M, Colbeck R and Renner R 2009 Duality between smooth min- and max-entropies *IEEE Trans. Inform. Theory* **56** 4674–81

[35] Tomamichel M, Colbeck R and Renner R 2009 A fully quantum asymptotic equipartition property *IEEE Trans. Inform. Theory* **55** 5840–7

[36] Tomamichel M, Schaffner C, Smith A and Renner R 2011 Leftover hashing against quantum side information *IEEE Trans. Inform. Theory* **57** 5524–35