JHEP

Published for SISSA by Springer

Received: October 4, 2016
Accepted: December 15, 2016
Published: December 28, 2016

Conditional mutual information of bipartite unitaries and scrambling

Dawei Ding, Patrick Hayden and Michael Walter

Stanford Institute for Theoretical Physics, Department of Physics, Stanford University, 382 Via Pueblo, Stanford, CA 94305, U.S.A.

E-mail: dding@stanford.edu, phayden@stanford.edu, michael.walter@stanford.edu

Abstract: One way to diagnose chaos in bipartite unitary channels is via the tripartite information of the corresponding Choi state, which for certain choices of the subsystems reduces to the negative conditional mutual information (CMI). We study this quantity from a quantum information-theoretic perspective to clarify its role in diagnosing scrambling. When the CMI is zero, we find that the channel has a special normal form consisting of local channels between individual inputs and outputs. However, we find that arbitrarily low CMI does not imply arbitrary proximity to a channel of this form, although it does imply a type of approximate recoverability of one of the inputs. When the CMI is maximal, we find that the residual channel from an individual input to an individual output is completely depolarizing when the other input is maximally mixed. However, we again find that this result is not robust. We also extend some of these results to the multipartite case and to the case of Haar-random pure input states. Finally, we look at the relationship between tripartite information and its Rényi-2 version which is directly related to out-of-time-order correlation functions. In particular, we demonstrate an arbitrarily large gap between the two quantities.

Keywords: Random Systems, AdS-CFT Correspondence, Gauge-gravity correspondence

ArXiv ePrint: 1608.04750

doi:10.1007/JHEP12(2016)145

JHEP12(2016)145

Contents

JHEP12(2016)145

1 Introduction

Recent research in quantum gravity has led to an interest in the scrambling and chaotic properties of many-body quantum systems [1–7]. The simplest model to consider is that of a unitary time evolution, $U_{AB\to CD}$, where A,B and C,D denote fixed bipartitions of past and future time slices of the quantum system, respectively. Typically, $A = C$ and $B = D$, and we merely use different letters to denote the past and future timeslices, but we may also consider two different bipartitions if we want to compare the propagation between different subsystems.

For chaotic dynamics, we expect that the local degrees of freedom A,B will get encoded nonlocally into C, D, i.e., *scrambled*. One way to formalize this intuition, proposed recently in [8], is to consider the *Choi state* dual to U, which is commonly used in quantum information theory to study the properties of quantum channels [9]. For the specific case of bipartite unitaries, the Choi states are used to study the capacity [10–14] and the cost of implementation [15, 16]. In the present context, this is the pure state defined by

$$\rho_{ABCD} = U_{A'B'\to CD}(\Phi^+_{AA'} \otimes \Phi^+_{BB'})U^\dagger_{A'B'\to CD}, \tag{1.1}$$

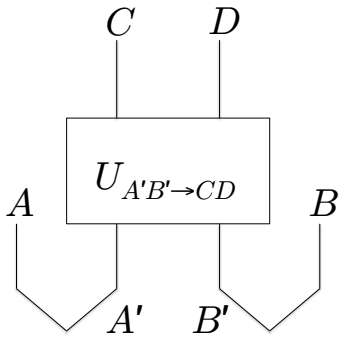

Figure 1. Choi state of a bipartite unitary U.

where $\Phi^+_{AA'}$ and $\Phi^+_{BB'}$ denote maximally entangled states (figure 1), and it allows us to study the past and future subsystems on equal footing. For scrambling unitaries, we expect the local correlations, as measured by the mutual informations $I(A;C) := S(A) + S(C) - S(AC)$ and $I(A;D)$, to be suppressed, while $I(A;CD)$ is necessarily maximal by unitarity. This suggests the *tripartite information*

$$I_3(A;C;D) := I(A;C) + I(A;D) - I(A;CD),$$

or more precisely $-I_3$, as a measure of scrambling in unitary quantum channels. It is easy to verify that the tripartite information does not depend on the choice of three subsystems A,B,C of the four-party pure quantum state ρ_{ABCD}.

The starting point to our investigations is the observation that unitarity implies that the reduced density matrices ρ_{AB} and ρ_{CD} of the Choi state are maximally mixed. It follows that $I(A;B) = I(C;D) = 0$ and hence the negative tripartite information reduces to

$$-I_3 = I(A;B|C), \tag{1.2}$$

where $I(A;B|C) = I(A;BC) - I(A;C)$ is the *conditional mutual information* (CMI).[1] In particular, the tripartite information is never positive as a consequence of the strong subadditivity of the von Neumann entropy:

$$I_3 \leq 0.$$

This is true for an arbitrary unitary time evolution, whether chaotic or not, contrary to previous expectations [8]. Interestingly, $I_3 \leq 0$ is *not* true for general quantum states, but it has recently been proved in a different context, namely as the consequence of the Ryu-Takayanagi formula in holographic systems [17] (cf. [18, 19]) and its tensor network models [20, 21], where it can be interpreted as a consequence of the monogamy of entanglement [22]. Whether there exists a deeper common reason for the negativity of I_3 associated to unitary transformations and the negativity of I_3 of a holographic state remains a tantalizing open question.

[1] Likewise, $-I_3 = I(A;B|D) = I(C;D|A) = I(C;D|B)$. Note that other choices of subsystems might not reduce $-I_3$ to the CMI.

JHEP12(2016)145

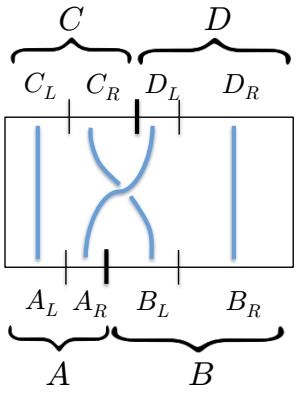

Figure 2. Any bipartite unitary with $I_3 = 0$ is a 'criss-cross channel' of the form (1.3), routing the quantum information from the input to the output subsystems.

In this paper, we aim to clarify the meaning of the tripartite information from the perspective of quantum information theory, based on the connection established above. We are particularly interested in the extreme cases, where the tripartite information attains its minimal or maximal values. We say that U is *minimally I_3-scrambling* if $I_3 = 0$ and *maximally I_3-scrambling* if it attains its maximally negative value.

We start in section 2 by considering the case of minimal I_3-scrambling. Our first result shows that any such unitary has the following special form:

$$U_{AB\to CD} = U_{A_L\to C_L} \otimes U_{A_R\to D_L} \otimes U_{B_L\to C_R} \otimes U_{B_R\to D_R}, \tag{1.3}$$

for some decomposition $A = A_L \otimes A_R$ and likewise for B, C, D (see figure 2 for an illustration). That is, the unitary can be decomposed into, in general, four smaller unitaries which locally route the quantum information between the input and output subsystems. Such a 'criss-cross channel' exactly matches our intuition of what a non-scrambling process should look like. This result can also be interpreted as maximizing simultaneously achievable rates of communication between the input and output subsystems: for example, we have that

$$R_{A\to C} + R_{A\to D} = Q_{A\to CD}, \tag{1.4}$$

where we write $R_{A\to C}$ and $R_{A\to D}$ for the simultaneously achievable (one-shot, zero-error) quantum communication rates from A to C and D, respectively, and $Q_{A\to CD}$ for the quantum capacity from A to CD, which by unitarity is always equal to $\log|A|$, the Hilbert space dimension of A. Note that logarithms in this paper are base 2, in accordance to the convention in quantum information. Lastly, our result can also be translated into a statement about the recoverability of the systems from partial information — for the purposes of recovering the quantum information from input A given output D, access to the other input subsystem B does not help.

It is interesting to ask to what extent the above statements can be generalized to the case where $I_3 \approx 0$. The latter result can be readily generalized to the approximate case using a recent result in quantum information theory [23], which asserts that we can find a

JHEP12(2016)145

quantum operation $\mathcal{R}_{D\to BD}$ independent of the state at A such that we can approximately recover ρ_{ABD} from ρ_{AD}. On the other hand, we show that (1.3) is not robust in the following, strongest possible sense: we explicitly construct a family of unitary quantum channels such that I_3 is arbitrarily close to zero, while their distance from any unitary of the form (1.3) is lower-bounded by a positive constant. Our construction implies that any robust version of (1.3) must necessarily depend on the Hilbert space dimension.

From the perspective of quantum information theory, our results complement the non-robustness result in [24, 25] that provide examples of tripartite states with vanishing conditional mutual information but non-vanishing trace distance to any quantum Markov chain state, that is, a state with a special normal form equivalent to having zero CMI. Here, on the other hand, we find a tripartite state with vanishing CMI *and* trace distance, but still with non-vanishing diamond norm to any quantum Markov chain state when the states are viewed as reduced Choi states of bipartite unitaries. This provides further evidence for the nonrobustness of normal forms for quantum Markov chains.

In section 3 we then consider the other extreme case, where the tripartite information I_3 is maximally negative. This can be achieved by, e.g., perfect tensors [20], also known as absolutely maximally entangled states [26, 27], such as those obtained by the random construction of [21]. Here, we give an explicit construction similar to that of [28] in the case $A = B = C = D$, which works in arbitrary odd dimensions. We also show that maximally scrambling unitaries do not exist if all the systems are qubits.

Now suppose that U is maximally I_3-scrambling and, for concreteness, that the dimension of A is the smallest among the four subsystems, so that $I_3 = -2\log|A|$. Then the residual channels $\mathcal{N}_{A\to C}$ and $\mathcal{N}_{A\to D}$, obtained by fixing a maximally mixed state τ_B into B, applying the unitary, and tracing out either D or C, are completely depolarizing.[2] In other words, we cannot locally route any information from A to C or D, while we still have $R_{A\to CD} = \log|A|$ by unitarity. This characterization nicely complements (1.3) and (1.4). It also complements the recovery interpretation: with only D, we can recover none of the information from A, but with BD we can recover all of it. However, we again find that we need to be cautious when generalizing this result to the approximate case: we construct a unitary such that I_3 is arbitrarily close to being maximally negative, but whose residual channel $\mathcal{N}_{A\to C}$ is bounded away from the completely depolarizing channel.

In section 4, we consider general values of I_3, again using the connection (1.2) to the conditional mutual information. The latter has an operational interpretation in the task of quantum state redistribution. More precisely, given a quantum state ρ_{ACD} with purification ρ_{ABCD}, if one party possesses AC and another party D, the former can send A to the latter using at an optimal rate of $\frac{1}{2}I(A;B|D) = -\frac{1}{2}I_3$ qubits [29]. This is intuitive: given that a strongly scrambling unitary will delocalize information from the inputs, we indeed expect that a larger number of qubits should be required to transfer systems. We show that this is consistent with our main results for minimal and maximal I_3-scrambling and give simple protocols that achieve the given qubit rate. Note that it is also possible to

[2] This is true only when the input on B is fixed to be maximally mixed. In general, there may be some correlations between A and C or D.

JHEP12(2016)145

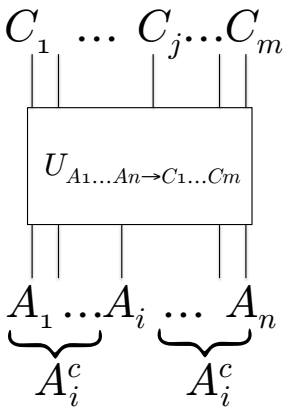

Figure 3. A multiple input and multiple output (MIMO) unitary.

do similar analyses using other operational interpretations of CMI such as in the tasks of state deconstruction and conditional erasure [30].

An appealing feature of the tripartite information is that it is related to *out-of-time-order (OTO) correlators*, an alternative diagnostic of chaos proposed to quantify the analog of the 'butterfly effect' in black holes [3]. OTO correlators can also be measured in various physical systems [31, 32]. An OTO correlator of two local operators $\mathcal{O}_A$ and $\mathcal{O}_C$ is by definition an expectation value of the form

$$\langle \mathcal{O}_C(t)\mathcal{O}_A\mathcal{O}_C(t)\mathcal{O}_A\rangle_\beta = \frac{1}{Z}\operatorname{tr}\left[e^{-\beta H}\mathcal{O}_C(t)\mathcal{O}_A\mathcal{O}_C(t)\mathcal{O}_A\right],$$

where $U = e^{-iHt}$ is the time evolution operator and $\mathcal{O}_C(t) = U^\dagger \mathcal{O}_C U$. We define the *average OTO correlator* between A and C, denoted $|\langle \mathcal{O}_C(t)\mathcal{O}_A\mathcal{O}_C(t)\mathcal{O}_A\rangle_\beta|$, by averaging the above over orthonormal bases of operators on A and C. In the infinite temperature limit, $\beta = 0$, it is known that [8]

$$|\langle \mathcal{O}_C(t)\mathcal{O}_A\mathcal{O}_C(t)\mathcal{O}_A\rangle_{\beta=0}| \times |\langle \mathcal{O}_D(t)\mathcal{O}_A\mathcal{O}_D(t)\mathcal{O}_A\rangle_{\beta=0}| \propto 2^{I_3^{(2)}}.$$

Here, $I_3^{(2)} = S_2(A) + S_2(B) - S_2(AC) - S_2(AD)$ is a variant of the tripartite information[3] defined in terms of the Rényi-2 entropy, $S_2(A) = -\log \operatorname{tr} \rho_A^2$, and the entropies are evaluated on the Choi state of U. Since $I_3^{(2)} \geq I_3$, the butterfly effect as measured by small OTO correlators implies I_3-scrambling. In section 5, we show that the converse is not true: a unitary with almost maximally negative tripartite information can still have large OTO correlators. In fact, we find that the difference $I_3^{(2)} - I_3$ can be arbitrarily large.

Finally, many of the above results can be extended to the multipartite case, as we explain in section 6. Let $U_{A_1\ldots A_n \to C_1\ldots C_m}$ be a *multiple input and multiple output (MIMO) unitary* as shown in figure 3. We show that the natural generalization of minimal I_3-scrambling is to demand that $I_3(A_i; A_i^c; C_j) = 0$ for all i and j, where we write A_i^c for the subset of all input subsystems save for A_i. In this case, the unitary takes the following

[3]Note that we can similarly write $I_3(A; C; D) = -I(C; D|A) = S(A) + S(B) - S(AC) - S(AD)$.

JHEP12(2016)145

form, generalizing our result for the bipartite case:

$$U_{A_1\ldots A_n\to C_1\ldots C_m} = \bigotimes_{i,j} U_{i\to j}, \tag{1.5}$$

where $U_{i\to j}$ is a local unitary mapping input subsystem A_i to output subsystem C_j. We also give an explicit construction of a family of maximally scrambling MIMO unitaries when all systems are of the same large prime dimension.

The nonrobustness of various algebraic characterizations of chaos and scrambling, while undesirable, is one of the central messages of this article. It typically leads to dimensional dependencies, which, in the context of high energy physics where Hilbert spaces are typically high-dimensional, are of particular significance. We believe that this provides good motivation for the development of alternative, more robust characterizations and diagnostics, not only in the present context but also in the study of other quantum information concepts in high energy physics, such as quantum error correction in holographic systems.

2 Minimal scrambling

In this section, we study properties of bipartite unitaries $U_{AB\to CD}$ where $I_3 \approx 0$. We first consider the exact case. Here, our main result is that the unitary has the following normal form:

Theorem 1. *A unitary $U_{AB\to CD}$ is minimally I_3-scrambling, i.e., $I_3 = 0$, if and only if it can be decomposed into a tensor product of local unitaries. That is,*

$$U_{AB\to CD} = U_{A_L\to C_L} \otimes U_{A_R\to D_L} \otimes U_{B_L\to C_R} \otimes U_{B_R\to D_R},$$

with respect to decompositions $A = A_L \otimes A_R$, $B = B_L \otimes B_R$, $C = C_L \otimes C_R$, $D = D_L \otimes D_R$. The dimensions of the subsystems are given by $|A_L| = |C_L| = \frac{1}{2} I(A;C)_U$ etc.

See figure 2 for an illustration. This result is consistent with the notion of scrambling as delocalization of quantum information. To see this, take a minimally I_3-scrambling unitary $U_{AB\to CD}$, and consider the residual channel $\mathcal{N}_{A\to C}[\sigma_A] = \mathrm{tr}_D \left[U_{AB\to CD}(\sigma_A \otimes \sigma_B^0)U_{AB\to CD}^\dagger\right]$ for some choice of state σ_B^0 on B. Then, Theorem 1 implies that

$$\mathcal{N}_{A\to C}[\sigma_A] = U_{A_L\to C_L}\sigma_{A_L}U_{A_L\to C_L}^\dagger \otimes \sigma_{C_R}^0,$$

where $\sigma_{C_R}^0 = U_{B_L\to C_R}\sigma_{B_L}^0 U_{B_L\to C_R}^\dagger$ is independent of the channel input. Hence, for the purposes of quantum information transfer, the residual channel $\mathcal{N}_{A\to C}$ is equivalent to the unitary quantum channel $U_{A_L\to C_L}$. Likewise, $\mathcal{N}_{A\to D}$ is equivalent to the unitary channel $U_{A_R\to D_L}$, while $\mathcal{N}_{A\to CD}$ is equivalent to their tensor product. In particular, the quantum information from A can be perfectly transmitted using local decoders at C and D, independent of the choice of input at B. Thus quantum information is perfectly routed through the system in a completely localized fashion, in agreement with the absence of scrambling.

From the perspective of quantum communication, we may state this as

$$Q_{A\to C} + Q_{A\to D} = Q_{A\to CD} = \log|A|,$$

JHEP12(2016)145

where Q is the quantum capacity of the corresponding channels, i.e., the maximum qubit rate at which quantum communication can be transferred through the channels in the limit of many channel uses and vanishing error (see, e.g., [9] for details). The right-hand side equality is a consequence of unitarity. In fact, we actually get the even stronger result that

$$R_{A\to C} + R_{A\to D} = Q_{A\to CD} = \log|A|$$

where $R_{A\to C}$ and $R_{A\to D}$ are simultaneously achievable, one-shot, zero-error quantum communication rates.

It is important to note that simultaneously achievable rates are different from the individual quantum capacities for general broadcast channels $A \to CD$. The former always satisfy an inequality $R_{A\to C} + R_{A\to D} \leq Q_{A\to CD}$. However, the latter need not. This phenomenon is also found in classical communication capacities. Consider, e.g., the basis-dependent copying channel $A \to CD$ which sends a noiseless copy of A to C and D as $|j\rangle_A \mapsto |j\rangle_C |j\rangle_D$. The individual capacities are $\log d$ but so is the overall capacity. While we cannot make the same construction for quantum capacities due to the no-cloning theorem, we can take advantage of the fact that the product of the dimensions of two subspaces can be greater than the sum to get a gap in quantum capacities as well. Define the unitary

$$U|a\rangle|b\rangle = \begin{cases} |a\rangle|b\rangle & a, b \leq d_0 \text{ or } a, b > d_0 \\ |b\rangle|a\rangle & \text{otherwise} \end{cases}$$

where $d_0 \leq d$. If we fix the input state $\rho_B^0 = |0\rangle\langle 0|$ then the resulting channel sends $|a\rangle \mapsto |a\rangle \otimes |0\rangle$ if $a \leq d_0$, and $|a\rangle \mapsto |0\rangle \otimes |a\rangle$ otherwise. Therefore, $Q_{A\to C} \geq \log d_0$ by coding in the former, d_0-dimensional subspace, while $Q_{A\to D} \geq \log(d - d_0)$ by coding in the latter subspace. Hence the sum of the individual capacities is at least $Q_{A\to C} + Q_{A\to D} = \log d_0(d - d_0) > \log d$ for appropriate d_0. However, $Q_{A\to CD}$ is never larger than $\log|A| = \log d$, so we obtain the inequality $Q_{A\to C} + Q_{A\to D} > Q_{A\to CD}$.

To prove Theorem 1, we first prove the corresponding statement for quantum states with vanishing conditional mutual information:

Proposition 2. *Any pure four-party quantum state ρ_{ABCD} that satisfies the three properties*

1. $I(A;B|C) = 0$,
2. $\rho_{AB} = \tau_{AB}$, *the maximally mixed state on AB, and*
3. $|AB| = |CD|$.

has the form

$$\rho_{ABCD} = \Phi^+_{A_LC_L} \otimes \Phi^+_{A_RD_L} \otimes \Phi^+_{B_LC_R} \otimes \Phi^+_{B_RD_R}$$

where $A = A_L \otimes A_R$, $B = B_L \otimes B_R$, $C = C_L \otimes C_R$, $D = D_L \otimes D_R$, and where the Φ^+ denote maximally entangled states.

Proof. We note that assumptions 2 and 3 together imply that

$$\rho_{CD} = \tau_{CD} \tag{2.1}$$

and so

$$\operatorname{rk} \rho_{ABC} = \operatorname{rk} \tau_D = |D|. \tag{2.2}$$

From [33], we know that if ρ_{ABC} is a quantum state with $I(A;B|C) = 0$ (assumption 1), then we can decompose into sectors $C = \bigoplus_i C_i$ and $C_i = C_{L_i} \otimes C_{R_i}$ such that

$$\rho_{ABC} = \sum_i p_i \, \rho^{(i)}_{AC_{L_i}} \otimes \rho^{(i)}_{BC_{R_i}} \tag{2.3}$$

for some probability distribution p_i and quantum states $\rho^{(i)}_{AC_{L_i}}$, $\rho^{(i)}_{BC_{R_i}}$. Now (2.2) shows that

$$|D| = \sum_i \operatorname{rk} \rho^{(i)}_{AC_{L_i}} \times \operatorname{rk} \rho^{(i)}_{BC_{R_i}}.$$

Thus we can decompose into sectors $D = \bigoplus_i D_i$, $D_i = D_{L_i} \otimes D_{R_i}$ (where $|D_{L_i}| = \operatorname{rk} \rho^{(i)}_{AC_{L_i}}$, etc.) and purify individually to obtain a purification of ρ_{ABC} of the form

$$\sum_i \sqrt{p_i} \, |\eta^{(i)}_{AC_{L_i}D_{L_i}}\rangle \otimes |\xi^{(i)}_{BC_{R_i}D_{R_i}}\rangle \,. \tag{2.4}$$

By Uhlmann's theorem (see, e.g., [9]), the purification in (2.4) only differs by a local unitary on D from the four-party pure state ρ_{ABCD}, which likewise purifies ρ_{ABC}, and hence it suffices to establish the normal form for (2.4). Furthermore, they have the same reduced state on CD, namely, the maximally mixed state (2.1), which is unitarily invariant. Thus:

$$\bigoplus_{i,i'} \sqrt{p_i p_{i'}} \operatorname{tr}_{AB} \left[|\eta^{(i)}_{AC_{L_i}D_{L_i}}\rangle\langle\eta^{(i')}_{AC_{L_{i'}}D_{L_{i'}}}| \otimes |\xi^{(i)}_{BC_{R_i}D_{R_i}}\rangle\langle\xi^{(i')}_{BC_{R_{i'}}D_{R_{i'}}}| \right] = \tau_{CD} \,. \tag{2.5}$$

We may think of the left-hand side as a big block matrix with respect to $\bigoplus_{i,j} C_i \otimes D_j$ which is only supported on blocks where $i = j$. The right-hand side on the other hand is supported on all blocks $C_i \otimes D_j$. Thus (2.5) can only be true if there is only a single sector (and hence no pair with $i \neq j$). Suppressing the index i, this means that, in fact, $C = C_L \otimes C_R$ and $D = D_L \otimes D_R$, so that (2.3) becomes

$$\rho_{ABC} = \rho_{AC_L} \otimes \rho_{BC_R}$$

and its purification (2.4) reads

$$|\eta_{AC_LD_L}\rangle \otimes |\xi_{BC_RD_R}\rangle \,. \tag{2.6}$$

Moreover, (2.5) becomes

$$\eta_{C_LD_L} \otimes \xi_{C_RD_R} = \tau_{CD},$$

and so both $\eta_{C_LD_L} = \tau_{C_LD_L}$ and $\xi_{C_RD_R} = \tau_{C_RD_R}$ are maximally mixed. In particular,

$$|A| \geq |C_LD_L|, \quad |B| \geq |C_RD_R|$$

JHEP12(2016)145

by the Schmidt decomposition. But $|AB| = |CD|$ by assumption 3, thus in fact

$$|A| = |C_L D_L|, \quad |B| = |C_R D_R|.$$

Thus $|\eta_{AC_L D_L}\rangle$ is maximally entangled between A and $C_L D_L$, and $|\xi_{BC_R D_R}\rangle$ is maximally entangled between B and $C_R D_R$. If we decompose $A = A_L \otimes A_R$ and $B = B_L \otimes B_R$ with $|A_L| = |C_L|$, $|A_R| = |D_L|$, etc., then we have another purification of $\eta_{C_L D_L} \otimes \xi_{C_R D_R}$, given by a tensor product of maximally entangled states:

$$\big(|\Phi^+_{A_L C_L}\rangle \otimes |\Phi^+_{A_R D_L}\rangle\big) \otimes \big(|\Phi^+_{B_L C_R}\rangle \otimes |\Phi^+_{B_R D_R}\rangle\big). \tag{2.7}$$

Thus, by another application of Uhlmann's theorem there exist local unitaries on A,B that transform (2.6) into (2.7). Absorbing all local unitaries into the tensor product decompositions, we obtain the desired result. □

The normal form in Theorem 1 follows now readily from Proposition 2, since the Choi state ρ_{ABCD} associated with the unitary $U_{AB\to CD}$ satisfies all three assumptions of the proposition. The formula for the dimensions of the subsystems A_L etc. follows directly from the normal form. For the converse, we observe that $-I_3 = I(C;D|A) = S(AC) + S(AD) - S(A) - S(B)$, where $\rho_{AC} = \Phi^+_{A_L C_L} \otimes \tau_{A_R} \otimes \tau_{C_R}$ and similarly for ρ_{AD}. Hence, $S(AC) = \log|A_R C_R| = \log|A_R B_L|$ and $S(AD) = \log|A_L D_R| = \log|A_L B_R|$, while $S(A) = \log|A|$ and $S(B) = \log|B|$. So, $S(AC) + S(AD) = \log|AB| = S(A) + S(B)$, which implies that $I(C;D|A) = 0$.

Theorem 1 does not appear to directly generalize to isometries $V_{AB\to CD}$. For example, consider the three-party GHZ state $|\mathrm{GHZ}\rangle_{ACD} = (|000\rangle + |111\rangle)/\sqrt{2}$, which is the Choi state of the isometry mapping $|0\rangle \mapsto |00\rangle$ and $|1\rangle \mapsto |11\rangle$. This is a special case of an isometry $V_{AB\to CD}$ where B is trivial, and $I_3(A;C;D)$ is zero, just as for any tripartite pure state. However, the GHZ state is clearly not of the form in Proposition 2, even if we allow for maximally entangled states between C, D. This can be seen by the fact that tracing out any one of the A, C, D in the GHZ state gives a separable state, which is impossible for a triple of maximally entangled states unless they are all trivial.

It is well-established in quantum information literature that the conditional information can be operationally interpreted in terms of the recoverability of quantum information for tripartite quantum states [23, 34]. See also [35–38]. In particular, it is known that, for any quantum state ρ_{ABD},

$$\|\rho_{ABD} - \mathcal{R}_{D\to BD}(\rho_{AD})\|_1 \leq 2\sqrt{1 - e^{-I(A;B|D)/2}},$$

where $\|X\|_1 := \mathrm{tr}\sqrt{X^\dagger X}$ is the *trace norm* and $\mathcal{R}_{D\to BD}$ a quantum channel that only depends on ρ_{BD} [23]. Applied to the Choi state of a bipartite unitary $U_{AB\to CD}$ with $-I_3 \leq \varepsilon$, we therefore obtain a *recovery map* with

$$\|\rho_{ABD} - \mathcal{R}_{D\to BD}(\rho_{AD})\|_1 \leq \sqrt{2\varepsilon}. \tag{2.8}$$

This is immediate from Theorem 1 when $I_3 = 0$. This recovery property of the state from local information is in stark contrast with the maximally scrambling case, such as in the model of black hole evaporation from [1], and we discuss this in more detail on p. 14.

JHEP12(2016)145

In contrast to the interpretation in terms of recovery maps, Theorem 1 itself is not robust in the sense that there exist unitaries for which I_3 is arbitrarily close to zero, while their distance to any unitary of the form of Theorem 1 stays bounded away from zero. Here, we measure distance using the *diamond norm* between two quantum channels $\mathcal{N}$ and $\mathcal{M}$,

$$\|\mathcal{N} - \mathcal{M}\|_\diamond = \max_n \max_{\rho_{AR}} \|\big(\mathrm{id}_R \otimes \mathcal{N}_{A\to B} - \mathrm{id}_R \otimes \mathcal{M}_{A\to B}\big)(\rho)\|_1, \tag{2.9}$$

where we optimize over all states ρ on AR, with R an auxiliary n-dimensional Hilbert space ($n = |A|$ is sufficient). As the trace distance quantifies how well one can experimentally distinguish quantum states [39], the diamond norm is a natural measure of how well one can distinguish two quantum channels even with an auxiliary system.

Our construction is explicit and goes as follows. We choose $A = B = C = D = \mathbb{C}^d$ and define a bipartite unitary U_d that is maximally I_3-scrambling on some subspace and the identity otherwise. More precisely,

$$U_d |a\rangle |b\rangle = \begin{cases} U_S |a\rangle |b\rangle & 0 \le a, b < d_S \\ |a\rangle |b\rangle & \text{otherwise} \end{cases} \tag{2.10}$$

for some $d_S \le d$, where U_S is a bipartite unitary $A_S B_S \to C_S D_S$ that is maximally I_3-scrambling, i.e., $I_3 = -2 \log d_S$, with A_S the subspace spanned by the first d_S basis vectors of A, etc. We prove the existence of such unitaries for arbitrary odd dimension d_S in section 3 below. Then we have the following result:

Proposition 3. *Let d_S be an odd constant. Then the bipartite unitaries U_d defined in (2.10) satisfy*

$$\lim_{d\to\infty} I_3(A;B;C)_{U_d} = 0.$$

However,

$$\liminf_{d\to\infty} \inf_{U_0} \|U_d - U_0\|_\diamond \ge 1 > 0,$$

where the infimum is over all unitaries U_0 with vanishing tripartite information.

That is, by making U_d I_3-scrambling on a subspace whose relative size goes to zero for large d, we can make the triparite information go to zero while still leaving a nonzero subspace that is I_3-scrambling, thereby keeping the diamond norm finitely bounded from zero. It is also interesting to note that the Choi state of U_d converges to that of the identity channel, a quantum Markov chain state, in trace distance, while the channel itself does not converge to the identity nor any minimally I_3-scrambling unitary in diamond norm.

On the other hand, we note that in terms of simultaneous local one-shot quantum capacities of U_d, $\lim_{d\to\infty} Q_{A\to CD} - (R_{A\to C} + R_{A\to D}) = 0$. Indeed, by coding in the complementary subspace of A_S, $R_{A\to C} \ge \log(d - d_S)$ can be achieved. Asymptotically, this goes like $\log d$, since

$$\lim_{d\to\infty} \log d - \log\big(d - d_S\big) = -\lim_{d\to\infty} \log\Big(1 - \frac{d_S}{d}\Big) = 0.$$

JHEP12(2016)145

Thus, since $R_{A\to D} \geq 0$, $\lim_{d\to\infty} Q_{A\to CD} - (R_{A\to C} + R_{A\to D}) \leq 0$. The other inequality is trivial, so we have equality. Hence, one might be tempted to interpret I_3 as the difference between the sum of the simultaneous local quantum capacities $A \to C, D$ and the maximum possible value $\log|A|$, which is true in this example for the limit of large d. For finite d, however, we can find examples where this interpretation fails.

The interpretation can be partially salvaged, however, by considering instead entanglement-assisted classical communication with random codes generated using maximally entangled states while fixing the input to B to be maximally mixed. This follows from the observation

$$I_3 = I(A;C) + I(A;D) - I(A;CD) = I(A;C) + I(A;D) - 2\log|A| \tag{2.11}$$

and the fact that the entanglement-assisted classical communication rate of a channel $\mathcal{N}_{A\to C}$ using such a code is given by the mutual information $I(A;C)$ of its Choi state [40, 41]. Since the mutual information $I(A;CD) = 2\log|A|$ is as large as it can be, it is not just an achievable rate but in fact the capacity of the $A \to CD$ channel. Equation (2.11) therefore states that the sum of the two entanglement-assisted achievable rates is bounded above by the entanglement-assisted capacity.

Proposition 3 is a consequence of the following technical estimates proved in appendix A:

Lemma 4. *Consider the unitaries U_d from (2.10) and their Choi states $\rho_{ABCD,d}$. Then,*

$$\|\rho_{ABCD,d} - \Phi^+_{AC} \otimes \Phi^+_{BD}\|_1 \leq 4\,\frac{d_S}{d} \tag{2.12}$$

and

$$\inf_{U_0} \|U_d - U_0\|_\diamond \geq 1 - \frac{2 + 2\log d_S}{\log d} \tag{2.13}$$

where the infimum is over all unitaries U_0 with vanishing tripartite information.

Indeed, (2.12) implies that the difference between the subsystem entropies vanishes in the limit of large d. This follows from the Fannes-Audenaert inequality [42, 43], which asserts that, for any two quantum states ρ and σ on a D-dimensional Hilbert space,

$$|S(\rho) - S(\sigma)| \leq T\log(D-1) + h(T), \tag{2.14}$$

where $T = \frac{1}{2}\|\rho - \sigma\|_1$ and $h(T) = -T\log T - (1-T)\log(1-T)$ is the binary entropy function, which can be upper bounded as $h(T) \leq 2\sqrt{T}$. But $\Phi^+_{AC} \otimes \Phi^+_{BD}$ is the Choi state of the identity channel, which has zero tripartite information. Hence the tripartite information $I(A;B;C)_{U_d}$ goes to zero in the limit of large d. In the same limit, the right-hand side of (2.13) converges to 1. This concludes the proof of Proposition 3.

JHEP12(2016)145

3 Maximal scrambling

We now consider the opposite extreme where $I_3 \approx -2 \log \min\{|A|, \ldots, |D|\}$ and compare it to the results we obtained in the minimally I_3-scrambling case. Note that this is the most negative value it can take since

$$\begin{aligned} I_3 &= -I(A;B|C) = S(C) + S(ABC) - S(AC) - S(BC) \\ &= S(C) + S(D) - S(AC) - S(AD) \\ &= I(A;C) + I(A;D) - 2S(A) \\ &= I(A;C) + I(A;D) - 2\log|A| \\ &\geq -2\log|A| \end{aligned} \tag{3.1}$$

since the mutual information is always nonnegative. A similar inequality holds for the other subsystems.

We first discuss the existence of maximally I_3-scrambling unitaries in the case where $A = B = C = D = \mathbb{C}^d$. Clearly, $I_3 = -2\log d$ if and only if any bipartite subsystem is maximally mixed, i.e., if $S(AB) = S(AC) = \cdots = 2\log d$. Such unitaries are precisely four-party perfect tensors, i.e., tensors that are unitary from any bipartition to the complement, as pointed out in [8]. This establishes the existence of maximally I_3-scrambling unitaries in sufficiently large prime dimension d, since a stabilizer state chosen at random will be a perfect tensor with high probability [21]. On the other hand, the following explicit construction achieves the same for any odd dimension d:

$$U_S |i\rangle_A |j\rangle_B = |i+j\rangle_C |i-j\rangle_D , \tag{3.2}$$

where all arithmetic is modulo d. We require d to be odd so that U_S is unitary. It can be readily verified that $I_3 = -2\log d$. We note that (3.2) is a straightforward generalization of the three-qutrit code from [28]. It is interesting to observe that U_S^2 is minimally I_3-scrambling. In this sense, a unitary that is maximally I_3-scrambling can still have a very small recurrence time.

The relationship to quantum error correcting codes can also be used to argue that there exists no maximally I_3-scrambling unitary for qubits ($d = 2$). Indeed, assume that such a unitary $U_{AB\to CD}$ exists and consider the isometry $V_{A\to BCD} := U_{AB'\to CD} |\Phi^+_{BB'}\rangle$ obtained by inputting one half of a maximally entangled state into B. Then the perfect tensor property implies that we can correct for the erasure of any one of the output qubits B, C and D. In other words, $V_{A\to BCD}$ would be a code for the qubit erasure channel of length 3. But this is ruled out by [44]. Hence, such a U does not exist.

We return to the general setup, where the dimensions of the systems $A, \ldots, D$ need not be equal, and consider the consequences of a unitary being maximally I_3-scrambling. In particular, we consider the residual channels from a single input to a single output. Then, we expect the channels residual channels $A \to C$ etc. to be noisy since quantum information should be delocalized. Indeed, we find:

JHEP12(2016)145

Proposition 5. *Let $U_{AB\to CD}$ be a maximally I_3-scrambling unitary and ρ_{ABCD} its Choi state. If either A or C have the smallest dimension among the four subsystems then ρ_{AC} is maximally mixed and $I(A;C)=0$.*

As a consequence, the residual channel $\mathcal{N}_{A\to C}[\sigma_A]=\mathrm{tr}_D[U(\sigma_A\otimes\tau_B)U^\dagger]$ corresponding to the maximally mixed input on B is completely depolarizing, i.e., its channel output is the maximally mixed state τ_C for any input state σ_A.[4]

Proof. If the dimension of A is smallest, maximal I_3-scrambling means that $I_3=-2\log|A|$. Thus it follows from (3.1) that $I(A;C)=I(A;D)=0$, since the mutual information is always nonnegative. Similarly, if C is smallest then we have $I_3=-2\log|C|$, which implies that $I(A;C)=I(B;C)=0$.

In either case, we thus find that $I(A;C)=0$ and hence that $\rho_{AC}=\rho_A\otimes\rho_C=\tau_{AC}$, since both ρ_A and ρ_C are maximally mixed. To see that this implies the second claim, we note that ρ_{AC} is the Choi state of the residual channel $\mathcal{N}_{A\to C}$. Hence, $\mathcal{N}_{A'\to C}[\Phi^+_{AA'}]=\tau_{AC}$ and therefore $\mathcal{N}_{A\to C}[\sigma_A]=\tau_C$ for any input state σ_A. □

Completely depolarizing channels have zero capacity of any kind, in agreement with our expectation that the quantum information at A gets fully delocalized for maximally mixed input at B. In appendix D we show that if $|D|\gg|AC|$ then $\rho_{AC}\approx\tau_{AC}$ for typical input states on B. Moreover, if $|D|\gg|AC|^2$ then the residual channel $\mathcal{N}_{A\to C}$ is typically entanglement-breaking, in which case it still has zero quantum capacity.

In general, there exist input states on B such that the corresponding residual channel $A\to C$ can still be used for communication. For example, consider the unitary defined in (3.2). If we fix the input on B to a computational basis state $|0\rangle$, then

$$\mathcal{N}_{A\to C}[\rho_A]=\mathrm{tr}_D\left[U_S(\rho_A\otimes|0\rangle\langle 0|)U_S^\dagger\right]=\sum_i\langle i|\rho_A|i\rangle\,|i\rangle\langle i|_C\,.$$

Hence, the residual channel is the completely dephasing channel, which has maximal classical capacity. If we instead fix the input on B to be in the state $\frac{1}{\sqrt{3}}(|0\rangle+\sqrt{2}\,|1\rangle)$ and consider the $d=3$ case, we obtain a residual channel $A\to C$ with positive quantum capacity. To see this, we use the fact that the coherent information of a channel is a lower bound on the quantum capacity [45–47]:

$$Q(\mathcal{N}_{A\to C})\geq I(\mathcal{N}_{A\to C})\equiv\max_{\varphi_{RA}}I(R\rangle C)_{\mathcal{N}(\varphi)}\tag{3.3}$$

where $I(R\rangle C)\equiv S(C)-S(RC)$ is the *coherent information*. If we choose the input state $|\varphi\rangle_{RA}=\frac{1}{\sqrt{3}}(|00\rangle+\sqrt{2}\,|11\rangle)$, we obtain $I(R\rangle C)=\frac{12}{9}-\frac{5}{9}\log 5>0$.

We can also interpret Proposition 5 from the perspective of recovery of quantum information. If we assume that the dimension of A is smallest then both residual channels $A\to C$ and $A\to D$ are completely depolarizing. Given only D, none of the quantum information at A can be recovered, while if we supplement it with B, perfect recovery is possible. More precisely, we can transfer entanglement from A to BD perfectly. This follows from

[4] Dually, $\mathcal{N}_{B\to C}[\sigma_B]=\mathrm{tr}_D[U(\sigma_A^0\otimes\sigma_B)U^\dagger]$ maps $\tau_B\mapsto\tau_C$ for *any* choice of input state σ_A^0 at A.

JHEP12(2016)145

the fact that ρ_{ABCD} and $\Phi^+_{AA'} \otimes \Phi^+_{CC'}$ both purify the reduced state $\rho_{AC} = \tau_A \otimes \tau_C$, which by Uhlmann's theorem implies the existence of a decoding operation $\mathcal{D}_{BD\to A'}$.

One of the motivations for studying scrambling unitaries comes from black hole physics. The preceding interpretation applies naturally to the model of black hole evaporation in [1] and was also discussed in [8]. We can schematically model black hole evaporation by a bipartite unitary time evolution where A is half of a Bell pair whose other half A' enters the black hole at time t_0, B is the Hawking radiation emitted before t_0, assumed to be maximally entangled with the black hole B at t_0, C is the state of the remaining black hole at a later time t_1, and D is the Hawking radiation emitted in the interval $[t_0, t_1]$. All indications are that black holes are highly scrambling [1–3, 6]. If we assume that they are maximally I_3-scrambling then we find that A' cannot be recovered from the late-time Hawking radiation D alone, while it would be possible when also given the old Hawking radiation B. In contrast, if the process were minimally I_3-scrambling then someone without knowledge of quantum state at A and with only the new Hawking radiation D could apply a local operation $\mathcal{R}_{D\to BD}$ to approximately recover the old Hawking radiation, so that the overall tripartite state $\mathcal{R}_{D\to BD}(\rho_{AD})$ is close to ρ_{ABD} (eq. (2.8)).

Lastly, we consider the approximate case, where $I_3 \approx -2\log\min\{|A|, \ldots, |D|\}$. For concreteness, we assume that the dimension of system A is smallest among all four subsystems and $I_3 = -2\log|A| + \varepsilon$. Then, $I(A;D) \leq \varepsilon$ as a consequence of (3.1) (cf. the proof of Proposition 5). Using Pinsker's inequality, this implies that $\|\rho_{AD} - \tau_A \otimes \tau_D\|_1 \leq \sqrt{2\ln(2)\varepsilon}$. In particular, if we put one half of a maximally entangled state into the residual channel $A \to D$, then the resulting state is close to being completely uncorrelated. Likewise, $\rho_{AC} \approx \tau_A \otimes \tau_C$, and hence ρ_{ABCD} and $\Phi^+_{AA'} \otimes \Phi^+_{CC'}$ still purify approximately the same state. It follows, again by Uhlmann's theorem, that there still exists a quantum operation $\mathcal{D}_{BC\to A'}$ such that $\mathcal{D}_{BD\to A'}[\rho_{ABD}] \approx \Phi^+_{AA'}$. In this sense, the recovery interpretation described above can be made robust.

On the other hand, the stronger conclusion of Proposition 5 is not robust in the sense that we can find unitaries such that the negative tripartite information goes to its maximal value, while the diamond norm (2.9) between the residual channel $\mathcal{N}_{A\to C}$ and the completely depolarizing channel remains finite. Furthermore, we find that there are such unitaries with nonvanishing one-shot zero-error quantum capacity. That is, a unitary can be arbitrarily close to being maximally I_3-scrambling even though its residual channel can still transmit quantum information perfectly at a nonvanishing rate. The sequence of unitaries we use is again (2.10),

$$U_d |a\rangle |b\rangle = \begin{cases} U_S |a\rangle |b\rangle & 0 \leq a, b < d_S \\ |a\rangle |b\rangle & \text{otherwise,} \end{cases},$$

except this time d_S will be large. We still require that $d_S = d - d_0$ is odd, so that the existence of a maximally I_3-scrambling unitary U_S is guaranteed. Then we can then establish the following result:

JHEP12(2016)145

Proposition 6. *Let d_0 be a constant and consider the family of unitaries U_d for odd $d_S = d - d_0$. Then,*

$$\lim_{d\to\infty} \left(I_3(A;B;C)_{U_d} + 2\log d\right) = 0, \tag{3.4}$$

while the residual channels $\mathcal{N}_{A\to C,d}[\sigma_A] = \mathrm{tr}_D[U_d(\sigma_A \otimes \tau_B)U_d^\dagger]$ have bounded distance away from the completely depolarizing channel $\Delta_{A\to C}$:

$$\lim_{d\to\infty} \|\mathcal{N}_{A\to C} - \Delta_{A\to C}\|_\diamond = 2 > 0. \tag{3.5}$$

Moreover, their one-shot zero-error quantum capacities $Q_{A\to C,d}$ can be lower bounded as

$$Q_{A\to C,d} \geq \log d_0 > 0. \tag{3.6}$$

To establish Proposition 6, we first note that the last bound (3.6) is immediate, since we can code perfectly using the d_0-dimensional subspaces. The first two bounds, (3.4) and (3.5), follow from the following lemma, proved in appendix B, together with the Fannes-Audenaert inequality (2.14) that we similarly used to establish Proposition 3.

Lemma 7. *Consider the unitaries U_d from (2.10) and their Choi states $\rho_{ABCD,d}$. Then $\rho_{AD,d}$ is maximally mixed, and*

$$\|\rho_{AC,d} - \tau_{AC}\|_1 \leq 8\frac{d_0}{d},$$

where $d_0 = d - d_S$. On the other hand, if $d_S < d$ then

$$\|\mathcal{N}_{A\to C} - \Delta_{A\to C}\|_\diamond \geq 2 - \frac{2}{d}.$$

4 Tripartite information and state redistribution

We now briefly discuss the meaning of general values of the tripartite information. Naturally, we would like to look for operational interpretations that hold in general. Using the equivalence between tripartite information and conditional mutual information, (1.2), one such interpretation is given by the task of *quantum state redistribution*, in which a party holding two quantum systems is to transfer one of the systems to a party holding one [29]. Specifically, given many copies of a quantum state ρ_{ACD} with purification ρ_{ABCD}, a party with AC can transmit A to a party with D using a rate of $\frac{1}{2}I(A;B|D)$ qubits of communication, $\frac{1}{2}I(A;C) - \frac{1}{2}I(A;D)$ ebits (i.e., shared Bell pairs of maximally entangled qubits) and no classical communication. Conversely, $\frac{1}{2}I(A;B|D)$ is the minimum rate of quantum communication required by any state redistribution protocol. This is consistent with the intuition of scrambling — a strongly scrambling unitary will delocalize the information from the inputs so that observers at individual outputs have little knowledge of the inputs. Hence, a large number of qubits should be required to transmit this information.

We can cross-check this intuition with our main results in the minimally and maximally scrambling cases and give explicit protocols in each case. For the minimally I_3-scrambling case, we cross-check Theorem 1 by applying this result to the reduced Choi state ρ_{ACD} of

JHEP12(2016)145

the unitary. Using the above result, to transfer A from AC to D, we shouldn't need any communication and consume $\log \frac{|A_L|}{|A_R|}$ ebits, where we are using the notation of Theorem 1. This is consistent with our result as we can prepare $|\Phi_{A_R D_L}\rangle$ locally. Thus, we only need to consume $\log|A_L|$ ebits to transmit A_L. However, we can use the $\log|A_R|$ pre-existing ebits to transmit A_L for a net ebit cost of $\log \frac{|A_L|}{|A_R|}$. No communication was done, so our qubit and bit costs are indeed zero.

In the maximally I_3-scrambling case, we can cross-check with Proposition 5. In the case where A is the smallest system, [29] states that we should need $\log|A|$ qubits, zero ebits, and zero bits. This is achieved by the trivial protocol that transfers A to D over a quantum channel, in agreement with our result.

5 Tripartite information and OTO correlators

An important property of the definition of scrambling using the tripartite information is that it can be related to scrambling as measured by out-of-time-order (OTO) correlators, as explained in the introduction. Specifically, we recall the following formula for the product of average OTO correlators,

$$|\langle \mathcal{O}_C(t)\mathcal{O}_A\mathcal{O}_C(t)\mathcal{O}_A\rangle_{\beta=0}| \times |\langle \mathcal{O}_D(t)\mathcal{O}_A\mathcal{O}_D(t)\mathcal{O}_A\rangle_{\beta=0}| \propto 2^{I_3^{(2)}},$$

where

$$I_3^{(2)} = S_2(A) + S_2(B) - S_2(AC) - S_2(AD) = \log|A| + \log|B| - S_2(AC) - S_2(AD) \tag{5.1}$$

is a Rényi-2 version of the tripartite information, defined in terms of the *Rényi-2 entropy* $S_2(\rho) = -\log \operatorname{tr} \rho^2$ instead of the von Neumann entropy. Since $S_2(\rho) \leq S(\rho)$ for any quantum state ρ, one obtains that $I_3^{(2)} \geq I_3$. Thus the 'butterfly effect' as measured by small OTO correlators implies I_3-scrambling [8].

However, the converse of this statement is not true. That is, a I_3-scrambling bipartite unitary can nevertheless have high OTO correlators. One example of this is again given by the family of unitaries U_d defined in (2.10), where we find an arbitrarily large gap between I_3 and $I_3^{(2)}$.

Proposition 8. *Consider the unitaries U_d defined in (2.10) and choose $d_0 \sim \sqrt[4]{d}$. Then*

$$I_3^{(2)}(A;B;C)_{U_d} - I_3(A;B;C)_{U_d} \gtrsim \frac{1}{2}\log d,$$

in the limit of large d.

This is proved by explicit calculation in appendix C, where we find that for sufficiently large d,

$$I_3^{(2)}(A;B;C)_{U_d} \geq -\frac{3}{2}\log d. \tag{5.2}$$

On the other hand, $I_3(A;B;C)_{U_d} \sim -2\log d$ as a consequence of eqs. (2.12) and (2.14). Together this establishes Proposition 8.

JHEP12(2016)145

This large separation can be understood by the fact that we have large individual OTO correlators. To see this, it is useful to choose bases of local Hermitian operators, $\operatorname{tr} \mathcal{O}_{D,i}\mathcal{O}_{D,j} = d\delta_{i,j}$ etc., that are adapted to the scrambling and nonscrambling subspaces. Indeed, we can write

$$U_d = U_S \oplus I_{\bar{S}},$$

where U_S is the maximally I_3-scrambling unitary acting on $A_S B_S = C_S D_S$ and $I_{\bar{S}}$ the identity operator on the complement $\overline{C_S D_S} = C_S D_0 \oplus C_0 D_S \oplus C_0 D_0$. Hence, if $\mathcal{O}_{D,i}$ is an operator that only acts on D_0, it will commute with U_d, so that $\mathcal{O}_{D,i}(t) = \mathcal{O}_{D,i}$. In this case, it follows that, for any local operator $\mathcal{O}_A$ on A,

$$\langle \mathcal{O}_{D,i}(t)\mathcal{O}_A\mathcal{O}_{D,i}(t)\mathcal{O}_A\rangle_{\beta=0} = \langle \mathcal{O}_{D,i}\mathcal{O}_A\mathcal{O}_{D,i}\mathcal{O}_A\rangle_{\beta=0} = \frac{1}{d}\operatorname{tr}\mathcal{O}_{D,i}^2 \times \frac{1}{d}\operatorname{tr}\mathcal{O}_{A,i}^2 = 1.$$

Furthermore, the number of such pairs of maximally correlated operators will be increasing without bound as $d \to \infty$.

6 Multipartite generalizations

The main results for the minimal and maximal cases above can be generalized to the multipartite setting. However, it is not clear, a priori, how to extend the definition of I_3-scrambling to the MIMO case. In the following, we will justify defining I_3-scrambling for *multiple input and multiple output (MIMO) unitaries* $U_{A_1\ldots A_n\to C_1\ldots C_m}$ using tripartite informations of the form

$$-I_3(A_i; A_i^c; C_j) = I(A_i; A_i^c|C_j) = I(C_j; C_j^c|A_i),$$

where A_i^c is the subset of all input subsystems save for A_i and C_j^c the subset of all output subsystems except for C_j (figure 3). The equalities follow from the bipartite case, (1.2), if we partition the Choi state of U into the four subsystems A_i, A_i^c, C_j, C_j^c.

Minimal scrambling

We define a *minimally I_3-scrambling* MIMO unitary to be a unitary $U_{A_1\ldots A_n\to C_1\ldots C_m}$ such that

$$I_3(A_i; A_i^c; C_j) = 0$$

for all i, j. Again, we find that such a unitary can be decomposed into a tensor product of local unitaries connecting individual inputs and outputs, generalizing Theorem 1:

Theorem 9. *Let $U_{A_1\ldots A_n\to C_1\ldots C_m}$ be a MIMO unitary. Then U is minimally I_3-scrambling if and only if it is of the form*

$$U_{A_1\ldots A_n\to C_1\ldots C_m} = \bigotimes_{i,j} U_{i\to j}$$

with respect to decompositions $A_i = \bigotimes_{j=1}^m A_{i\to j}$ for $i = 1,\ldots,n$, $C_j = \bigotimes_{i=1}^n C_{i\to j}$ for $j = 1,\ldots,m$ and unitaries $U_{i\to j}\colon A_{i\to j} \to C_{i\to j}$ for i, j.

JHEP12(2016)145

We will prove Theorem 9 by viewing the MIMO unitary as a bipartite unitary where we group inputs and outputs. This will then allow us to iteratively apply Theorem 1 to decompose the MIMO unitary piece by piece. We will first peel off all the unitaries for a single input and then repeat for all other inputs. To do so, we need to show that we can decompose a MIMO unitary into a local unitary and a residual MIMO unitary such that A_1 and C_1 have zero mutual information on the residual unitary and such that the residual MIMO unitary is still minimally I_3-scrambling:

Lemma 10. *Let $U_{A_1\dots A_n\to C_1\dots C_m}$ be a minimally I_3-scrambling MIMO unitary. Then there exist decompositions $A_1 = A_{1\to 1}\otimes A_1'$, $C_1 = C_{1\to 1}\otimes C_1'$ and unitaries $U_{1\to 1}\colon A_{1\to 1}\to C_{1\to 1}$, $U'_{A_1'A_2\dots A_n\to C_1'C_2\dots C_m}$ such that*

$$U_{A_1\dots A_n\to C_1\dots C_m} = U_{1\to 1}\otimes U'_{A_1'A_2\dots A_n\to C_1'C_2\dots C_m}.$$

Here, U' is a minimally I_3-scrambling MIMO unitary that satisfies $I(A_1';C_1')_{U'} = 0$.

Proof. We apply Theorem 1 with $A = A_1$, $B = A_2\dots A_n$ and $C = C_1$ and $D = C_2\dots C_m$. Thus we obtain that

$$U_{AB\to CD} = U_{A_L\to C_L}\otimes\big(U_{A_R\to D_L}\otimes U_{B_L\to C_R}\otimes U_{B_R\to D_R}\big). \tag{6.1}$$

If we define $A_{1\to 1} := A_L$, $A_1' := A_R$, $C_{1\to 1} := C_L$, $C_1' := C_R$, $U_{1\to 1} := U_{A_L\to C_L}$ and U' as the tensor product of the three unitaries on the right-hand side then we obtain a decomposition as in the statement of the lemma.

That U' is still minimally I_3-scrambling follows from the fact local unitaries $U_{1\to 1}$ and the overall unitary U have zero tripartite information, in addition to the additivity of von Neumann entropy for tensor product states (cf. [19, 22]). And the statement about the mutual information holds because $I(A_R;C_R)_{U'} = 0$ by direct inspection of the normal form (6.1). □

By iteratively applying Lemma 10, we find decompositions $A_1 = \bigotimes_{j=1}^m A_{1\to j}\otimes A_1'$ and $C_j = C_{1\to j}\otimes C_j'$ such that U factors into a tensor product

$$U_{A_1\dots A_n\to C_1\dots C_m} = \bigotimes_{j=1}^m U_{1\to j}\otimes U'_{A_1'A_2\dots A_n\to C_1'\dots C_m'}$$

of local unitaries $U_{1\to j}\colon A_{1\to j}\to C_{1\to j}$ with a residual unitary U'. The latter is minimally I_3-scrambling and moreover satisfies $I(A_1';C_j')_{U'} = 0$ for all j (using monotonicity of the mutual information). However, we also need to make sure that this process will consume all of A_1. This is a consequence of the following lemma, applied to the residual unitary U'.

Lemma 11. *Let $U_{A_1\dots A_n\to C_1\dots C_m}$ be a minimally I_3-scrambling MIMO unitary with $I(A_1;C_j) = 0$ for $j = 1,\dots,m$. Then the system A_1 is trivial.*

JHEP12(2016)145

Proof. First note that, for all $j = 1, \ldots, m$,

$$\begin{aligned} 0 &= I_3(A_1; A_1^c; C_j) = I(A_1; A_1^c|C_j) \\ &= S(A_1C_j) + S(A_1^cC_j) - S(C_j) - S(A_1A_1^cC_j) \\ &= S(A_1C_j) + S(A_1C_j^c) - S(C_j) - S(C_j^c) \\ &= S(A_1) + S(A_1C_j^c) - S(C_j^c), \end{aligned} \tag{6.2}$$

where the last equality follows from the assumption that $I(A_1; C_j) = 0$. This implies the following recursion formula:

$$\begin{aligned} &S(A_1C_j \ldots C_m) - S(C_j \ldots C_m) \\ &\quad = S(A_1C_j \ldots C_m) + S(A_1C_j^c) - S(C_j \ldots C_m) - S(C_j^c) + S(A_1) \\ &\quad \geq S(A_1C_1 \ldots C_m) + S(A_1C_{j+1} \ldots C_m) - S(C_j \ldots C_m) - S(C_j^c) + S(A_1) \\ &\quad = S(A_1C_{j+1} \ldots C_m) - S(C_{j+1} \ldots C_m) - S(C_j) - S(C_j^c) + S(A_1) + S(A_1^c) \\ &\quad = S(A_1C_{j+1} \ldots C_m) - S(C_{j+1} \ldots C_m)\,. \end{aligned}$$

The first equality holds by plugging in (6.2), the inequality is strong subadditivity, and the last two follow by using that the reduced state $\rho_{C_1 \ldots C_m}$ is maximally mixed by unitarity. If we start with (6.2) for $j = 1$ and successively apply the recursion formula, we obtain

$$\begin{aligned} 0 &= S(A_1) + S(A_1C_2 \ldots C_m) - S(C_2 \ldots C_m) \\ &\geq S(A_1) + S(A_1C_3 \ldots C_m) - S(C_3 \ldots C_m) \\ &\geq \cdots \geq 2S(A_1). \end{aligned}$$

We conclude that $\log|A_1| = S(A_1) = 0$. □

The above considerations thus allow us to completely peel off A_1 from the MIMO unitary, leaving a minimally I_3-scrambling MIMO unitary on the other inputs. We have thus proved the following lemma:

Lemma 12. *Let $U_{A_1 \ldots A_n \to C_1 \ldots C_m}$ be a minimally I_3-scrambling MIMO unitary. Then there exist decompositions $A_1 = \bigotimes_{j=1}^m A_{1\to j}$ and $C_j = C_{1\to j} \otimes C_j'$ for $j = 1, \ldots, m$, as well as unitaries $U_{1\to j}\colon A_{1\to j} \to C_{1\to j}$ for $j = 1, \ldots, m$ and $U'_{A_2 \ldots A_n \to C_1' \ldots C_m'}$, such that*

$$U_{A_1 \ldots A_n \to C_1 \ldots C_m} = \bigotimes_{j=1}^n U_{1\to j} \otimes U'_{A_2 \ldots A_n \to C_1' \ldots C_m'}.$$

Moreover, U' is again a minimally I_3-scrambling MIMO unitary.

Theorem 9 now follows by applying Lemma 12 inductively to A_1, A_2, etc. After n steps, there are no A-systems left. Since the residual operator U' is a unitary, the corresponding C_j' likewise have to be trivial. We thus obtain the desired normal form. To see that, conversely, any MIMO unitary of the given normal form is minimally I_3-scrambling follows directly from the corresponding statement in Theorem 1, applied to the bipartitions A_i, A_i^c and C_j, C_j^c. This concludes the proof of Theorem 9.

JHEP12(2016)145

Maximal scrambling

On the other end, we define a *maximally I_3-scrambling* MIMO unitary as one that satisfies

$$I_3(A_i; A_i^c; C_j) = -2 \log \min\{|A_i|, |A_i^c|, |C_j|, |C_j^c|\}$$

for all i, j. Applying Proposition 5 to the bipartition A_i, A_i^c, C_j, C_j^c, we conclude that the residual channels $\mathcal{N}_{A_i \to C_j}$ are completely depolarizing whenever A_i or C_j is the smallest system (e.g., if all systems have the same dimension, as in a typical many-body scenario). We note that if the average OTO correlators between A_i, C_j and A_i, C_j^c are minimal for each i and j, then the MIMO unitary is maximally I_3-scrambling.

By an explicit construction similar to that of eq. (3.2), we can establish that maximally I_3-scrambling MIMO unitaries exist for arbitrarily large values of d.

Proposition 13. *Let $A_1 = \cdots = A_n = C_1 = \cdots = C_n = \mathbb{C}^d$, where $d > n + 1$ is a prime. Let M_n be the following $n \times n$ matrix,*

$$M_n = I_n + E_n = \begin{bmatrix} 2 & 1 & \dots & 1 \\ 1 & 2 & \dots & 1 \\ & & \ddots & \\ 1 & 1 & \dots & 2 \end{bmatrix}, \tag{6.3}$$

where I_n is the identity matrix and E_n the matrix of ones. Then $U_{d,n} |\vec{x}\rangle = |M_n \vec{x}\rangle$ defines a maximally I_3-scrambling MIMO unitary. Here we write $|\vec{x}\rangle = |x_1\rangle \dots |x_n\rangle$, and all arithmetic is modulo d.

We prove this by showing that the following three criteria on a matrix M are together sufficient to ensure that $U_M |\vec{x}\rangle = |M\vec{x}\rangle$ is maximally I_3-scrambling:

1. M is an invertible matrix modulo d.
2. If we replace any row of M by any elementary row (i.e., a row with all 0's except for a single entry occupied by a 1) then the resulting matrix is still invertible modulo d.
3. All entries of M are invertible modulo d.

We then show that M_n defined in (6.3) satisfies these conditions when $d > n+1$ and is prime. The detailed proof is given in appendix E. It is an interesting open question to determine sufficient and necessary conditions on the dimensions for maximally I_3-scrambling MIMO unitaries to exist [26].

Acknowledgments

We thank Sepehr Nezami and Beni Yoshida for helpful discussions. The authors gratefully acknowledge support from the Simons Foundation, including the It from Qubit Collaboration, as well as CIFAR and the Air Force Office of Scientific Research. DD acknowledges funding by a Stanford Graduate Fellowship.

JHEP12(2016)145

A Nonrobustness in the approximately minimal case

In this appendix we prove Lemma 4, restated here for convenience:

Lemma 4. *Consider the unitaries U_d from (2.10) and their Choi states $\rho_{ABCD,d}$. Then,*

$$\|\rho_{ABCD,d} - \Phi^+_{AC} \otimes \Phi^+_{BD}\|_1 \leq 4\,\frac{d_S}{d} \tag{2.12}$$

and

$$\inf_{U_0} \|U_d - U_0\|_\diamond \geq 1 - \frac{2 + 2\log d_S}{\log d} \tag{2.13}$$

where the infimum is over all unitaries U_0 with vanishing tripartite information.

Proof. Recall that U_d is given by

$$U_d \left|a\right\rangle \left|b\right\rangle = \begin{cases} U_S \left|a\right\rangle \left|b\right\rangle & 0 \leq a, b < d_S \\ \left|a\right\rangle \left|b\right\rangle & \text{otherwise} \end{cases}. \tag{A.1}$$

We prove the first statement. The Choi state $\rho_d = |U_d\rangle\langle U_d|$ of U_d is given by

$$\begin{aligned} |U_d\rangle &= \frac{1}{d} U_{A'B' \to CD,d} \left(\sum_{a,b<d_S} + \sum_{a \geq d_S \vee b \geq d_S} \right) |aa\rangle_{AA'} |bb\rangle_{BB'} \\ &= \frac{d_S}{d} |U_S\rangle_{A_S B_S C_S D_S} + \frac{1}{d} \sum_{a \geq d_S \vee b \geq d_S} |aa\rangle_{AC} |bb\rangle_{BD} \end{aligned} \tag{A.2}$$

where we write $|U_S\rangle$ for the Choi state of the maximally I_3-scrambling unitary U_S. On the other hand,

$$|\Phi^+_{AC}\rangle |\Phi^+_{BD}\rangle = \frac{d_S}{d} |\Phi^+_{A_S C_S}\rangle |\Phi^+_{B_S D_S}\rangle + \frac{1}{d} \sum_{a \geq d_S \vee b \geq d_S} |aa\rangle_{AC} |bb\rangle_{BD}\,.$$

Hence, for small d_S, the overlap between the two Choi states is given by

$$|\langle \Phi^+_{AC} \otimes \Phi^+_{BD} | U_d \rangle| = \left| \frac{d_S^2}{d^2} \langle \Phi^+_{A_S C_S} \otimes \Phi^+_{B_S D_S} | U_S \rangle + \frac{d^2 - d_S^2}{d^2} \right| \geq 1 - 2\frac{d_S^2}{d^2}\,.$$

Using the relationship between trace distance and overlap of pure states [9],

$$\|\rho_{ABCD,d} - \Phi^+_{AC} \otimes \Phi^+_{BD}\|_1 = 2\sqrt{1 - |\langle \Phi^+_{AC} \otimes \Phi^+_{BD} | U_d \rangle|^2} \leq 4\frac{d_S}{d}\,.$$

We have thus established (2.12).

We now prove the second statement. Let U_0 be a minimally I_3-scrambling unitary. By Theorem 1, we can write

$$U_0 = U_{A_L \to C_L} \otimes U_{A_R \to D_L} \otimes U_{B_L \to C_R} \otimes U_{B_R \to D_R}, \tag{A.3}$$

where $A = A_L \otimes A_R$ and similarly for B, C, D. Without loss of generality, $|C_R| \geq |C|^{1/2}$. Otherwise, switch the roles of A, B in the following. We consider a state of the form

$$\sigma_{AB} = \sigma_{A_S} \otimes \tau_B,$$

JHEP12(2016)145

where σ_{A_S} is an arbitrary state on $A_S \subseteq A = A_L \otimes A_R$. We will show that U_d and U_0 lead to reduced density matrices on C with markedly different entropies, implying that U_d, U_0 are well-distinguishable. It is clear from (A.1) and the form of σ_{AB} that $\sigma_C = \mathrm{tr}_D[U_d \sigma_{AB} U_d^\dagger]$ is supported on the subspace C_S, hence

$$S(\sigma_C) \leq \log d_S.$$

On the other hand, using (A.3) we can compute the second reduced state as

$$\begin{aligned}\sigma'_C &= \mathrm{tr}_D[U_0 \sigma_{AB} U_0^\dagger] = \left(U_{A_L \to C_L} \otimes U_{B_L \to C_R}\right) \mathrm{tr}_{A_R B_R}[\sigma_{AB}] \left(U_{A_L \to C_L} \otimes U_{B_L \to C_R}\right)^\dagger \\ &= U_{A_L \to C_L} \, \mathrm{tr}_{A_R}[\sigma_{A_S}] U_{A_L \to C_L} \otimes \tau_{C_R},\end{aligned}$$

and hence that

$$S(\sigma'_C) \geq \log C_R \geq \frac{1}{2} \log d.$$

Thus, using the Fannes-Audenaert inequality (2.14),

$$\frac{1}{2} \log d - \log d_S \leq |S(\sigma_C) - S(\sigma'_C)| \leq \frac{1}{2} \|\sigma_C - \sigma'_C\|_1 \log d + 1,$$

from which it follows that

$$\|\sigma_C - \sigma'_C\|_1 \geq 1 - \frac{2 + 2 \log d_S}{\log d}.$$

Hence, we can bound the trace distance between the output states using monotonicity, which in turn bounds the diamond norm (2.9):

$$\|U - U_0\|_\diamond \geq \|U_d \sigma_{AB} U_d^\dagger - U_0 \sigma_{AB} U_0^\dagger\|_1 \geq \|\sigma_C - \sigma'_C\|_1 \geq 1 - \frac{2 + 2 \log d_S}{\log d}.$$

This establishes (2.13). □

B Nonrobustness in the approximately maximal case

In this appendix we prove Lemma 7, restated again for convenience.

Lemma 7. *Consider the unitaries U_d from (2.10) and their Choi states $\rho_{ABCD,d}$. Then $\rho_{AD,d}$ is maximally mixed, and*

$$\|\rho_{AC,d} - \tau_{AC}\|_1 \leq 8 \frac{d_0}{d},$$

where $d_0 = d - d_S$. On the other hand, if $d_S < d$ then

$$\|\mathcal{N}_{A \to C} - \Delta_{A \to C}\|_\diamond \geq 2 - \frac{2}{d}.$$

Proof. We start with the formula in (A.2) for the Choi state of U_d, which can be written as

$$\begin{aligned}|U_d\rangle = \frac{d_S}{d} |U_S\rangle_{A_S B_S C_S D_S} + \frac{d_0}{d} |\Phi^+_{A_0 C_0}\rangle \otimes |\Phi^+_{B_0 D_0}\rangle \\ + \frac{\sqrt{d_S d_0}}{d} |\Phi^+_{A_S C_S}\rangle \otimes |\Phi^+_{B_0 D_0}\rangle + \frac{\sqrt{d_S d_0}}{d} |\Phi^+_{A_0 C_0}\rangle \otimes |\Phi^+_{B_S D_S}\rangle\end{aligned}$$

JHEP12(2016)145

where $A = A_S \oplus A_0$ etc. with A_S, B_S, etc. the d_S-dimensional subspaces on which the maximally I_3-scrambling unitary U_S acts, and $|U_S\rangle$ the Choi state of the latter.

We first compute the reduced density matrix $\rho_{AD,d}$. There are no cross-terms, hence

$$\rho_{AD,d} = \frac{d_S^2}{d^2}\tau_{A_S D_S} + \frac{d_0^2}{d^2}\tau_{A_0 D_0} + \frac{d_0 d_S}{d^2}\tau_{A_S D_0} + \frac{d_0 d_S}{d^2}\tau_{A_0 D_S} = \tau_{AD}$$

as desired. Here, we have used that U_S is maximally I_3-scrambling and hence its reduced state on $A_S D_S$ is maximally mixed.

We now compute the reduced density matrix $\rho_{AC,d}$. For this, we split the matrix into blocks according to the decomposition $AC = A_S C_S \oplus A_0 C_0 \oplus A_S C_0 \oplus A_0 C_S$. Then there are four nonzero blocks,

$$\rho_{AC,d} = \left[\begin{array}{c|c|c|c} \rho_{SS} & \rho_{S0} & 0 & 0 \\ \hline \rho_{S0}^\dagger & \rho_{00} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right], \tag{B.1}$$

where

$$\begin{aligned} \rho_{SS} &= \frac{d_S^2}{d^2}\tau_{A_S C_S} + \frac{d_0 d_S}{d^2}\Phi^+_{A_S C_S}, \\ \rho_{00} &= \frac{d_0 d_S}{d^2}\Phi^+_{A_0 C_0} + \frac{d_0^2}{d^2}\Phi^+_{A_0 C_0} = \frac{d_0}{d}\Phi^+_{A_0 C_0}, \\ \rho_{S0} &= \frac{\sqrt{d_0 d_S}}{d^2}\,|\Psi_{A_S C_S}\rangle\langle\Phi^+_{A_0 C_0}|\,, \end{aligned} \tag{B.2}$$

where we have introduced

$$|\Psi_{A_S C_S}\rangle = |\theta_{A_S C_S}\rangle + d_0\,|\Phi^+_{A_S C_S}\rangle\,,$$

where $|\theta_{A_S C_S}\rangle = d_S\,\langle\Phi^+_{B_S D_S}|U_{S,A_S B_S C_S D_S}\rangle$. This is a unit vector:

$$\langle\theta|\theta\rangle = d_S^2\,\mathrm{tr}\,\Phi^+_{B_S D_S}\tau_{B_S D_S} = 1,$$

since U_S is maximally I_3-scrambling and so its Choi state on $B_S D_S$ is maximally mixed. It follows that

$$\|\rho_{S0}\|_1 = \mathrm{tr}\sqrt{\rho_{S0}\rho_{S0}^\dagger} = \frac{\sqrt{d_0 d_S}}{d^2}\|\Psi_{A_S C_S}\| \le \frac{\sqrt{d_0 d_S}}{d^2}(1+d_0) \le 2\frac{d_0}{d}\,.$$

Therefore, using $\tau_{AC} = \frac{d_S^2}{d^2}\tau_{A_S C_S} + \frac{d^2 - d_S^2}{d^2}\tau'$, where τ' is a maximally mixed state on the complement of $A_S C_S$,

$$\begin{aligned} \|\rho_{AC,d} - \tau_{AC}\|_1 &= \|\frac{d_0 d_S}{d^2}\Phi^+_{A_S C_S} + \rho_{00} + \rho_{S0} + \rho_{S0}^\dagger - \frac{d^2 - d_S^2}{d^2}\tau'\|_1 \\ &\le \frac{d_0 d_S}{d^2} + \frac{d_0}{d} + 4\frac{d_0}{d} + \frac{d^2 - d_S^2}{d^2} \le 8\frac{d_0}{d}. \end{aligned}$$

At last, we show that the residual channel $\mathcal{N}_{A\to C}$ for U_d is bounded away from the completely depolarizing channel $\Delta_{A\to C}$ in the diamond norm. For this, it suffices to compare their action on a state orthogonal to the scrambling subspace A_S, so that $\mathcal{N}_{A\to C}$ acts by the identity. The d-th computational basis state $|d-1\rangle$ is such a state:

$$\left\|\mathcal{N}_{A\to C} - \Delta_{A\to C}\right\|_\diamond \ge \left\||d-1\rangle\langle d-1|_C - \tau_C\right\|_1 = 2 - \frac{2}{d}. \qquad \square$$

C Calculation of the Rényi-2 tripartite information

In this appendix we verify (5.2), the lower bound for the Rényi-2 tripartite information of the unitary U_d defined in (2.10). Let $\rho_{ABCD,d}$ denote its Choi state. In Lemma 7, we have shown that $\rho_{AD,d}$ is maximally mixed. Hence the Rényi-2 tripartite information (5.1) reduces to

$$I_3^{(2)} = -S_2(AC) = \log \operatorname{tr} \rho_{AC,d}^2.$$

Now, it follows from (B.1) that

$$\rho_{AC,d}^2 = \left[\begin{array}{c|c} \rho_{SS}^2 + \rho_{S0}\rho_{S0}^\dagger & * \\ \hline * & \rho_{00}^2 + \rho_{S0}^\dagger \rho_{S0} \end{array}\right],$$

where we omitted zero rows and did not specify the off-diagonal blocks, which are irrelevant to our calculation. Using (B.2), we find

$$\operatorname{tr} \rho_{AC,d}^2 \geq \operatorname{tr} \rho_{SS}^2 + \operatorname{tr} \rho_{00}^2 = \frac{d_S^2}{d^4} + 2\frac{d_0 d_S}{d^4} + \frac{d_0^2 d_S^2}{d^4} + \frac{d_0^2}{d^2} \geq \frac{d_0^2 d_S^2}{d^4} = \frac{1}{d^2}\frac{d_S^2}{d^2} d_0^2.$$

Hence, if we choose $d_0 \sim \sqrt[4]{d}$ then $\log d_0 \sim \frac{1}{4}\log d$, thus

$$I_3^{(2)} = \log \operatorname{tr} \rho_{AC,d}^2 \geq -2\log d + 2\log\left(1 - \frac{d_0}{d}\right) + \log d_0^2 \gtrsim -\frac{3}{2}\log d.$$

D Maximal scrambling and typical inputs

In Proposition 5 we found that the residual channel $\mathcal{N}_{A\to C}$ for maximally mixed input on B is completely depolarizing. In other words, its Choi state is maximally mixed, $\mathcal{N}_{A'\to C}[\Phi_{AA'}^+] = \tau_A \otimes \tau_C$. Under certain conditions this is approximately true also for *typical* input states on B:

Proposition 14. *Let $U_{AB\to CD}$ be a maximally I_3-scrambling unitary and σ_B a Haar-random pure state. Let $\widetilde{\mathcal{N}}_{A\to C}[\sigma_A] = \operatorname{tr}_D[U(\sigma_A \otimes \sigma_B)U^\dagger]$ denote the corresponding residual channel from A to C, and $\widetilde{\rho}_{AC} := \widetilde{\mathcal{N}}_{A'\to C}[\Phi_{AA'}^+]$ its Choi state. Then,*

$$\Pr(\|\widetilde{\rho}_{AC} - \tau_{AC}\|_1 \leq \varepsilon) \geq 1 - \frac{|A||C|}{\varepsilon^2 |D|}.$$

Proof. Let us write ρ_{ABCD} for the Choi state of $U_{AB\to CD}$. For a Haar-random pure state, $\mathbb{E}[\sigma_B] = \tau_B$. Hence, the average Choi state is maximally mixed, $\mathbb{E}[\widetilde{\rho}_{AC}] = \rho_{AC} = \tau_{AC}$.

We now bound the mean square deviation. For this, let $\|X\|_2 := \sqrt{\operatorname{tr} X^\dagger X}$ denote the 2-norm. Then:

$$\mathbb{E}[\|\widetilde{\rho}_{AC} - \tau_{AC}\|_2^2] = \mathbb{E}[\operatorname{tr} \widetilde{\rho}_{AC}^2] - \operatorname{tr} \tau_{AC}^2.$$

We calculate the first term using the swap trick:

$$\operatorname{tr} \widetilde{\rho}_{AC}^2 = \operatorname{tr}(\widetilde{\rho}_{AC} \otimes \widetilde{\rho}_{AC}) F_{AC} = \operatorname{tr} U_{A'B\to CD}^{\otimes 2} (\Phi_{AA'}^{+\otimes 2} \otimes \sigma_B^{\otimes 2}) U_{A'B\to CD}^{\dagger\otimes 2} F_{AC},$$

JHEP12(2016)145

where F_{AC} denotes the swap operator that exchanges the two copies of AC. The second moment of a Haar-random state is given by $\mathbb{E}[\sigma_B^{\otimes 2}] = \frac{1}{|B|(|B|+1)}(I + F_B)$ where I is the identity and F_B the swap operator on the two copies of B. Thus:

$$\begin{aligned}\mathbb{E}[\operatorname{tr} \widetilde{\rho}_{AC}^2] = &\frac{1}{|B|(|B|+1)} \operatorname{tr} U_{A'B\to CD}^{\otimes 2} \Phi_{AA'}^{+\otimes 2} U_{A'B\to CD}^{\dagger\otimes 2} F_{AC} \\ &+ \frac{1}{|B|(|B|+1)} \operatorname{tr} U_{A'B\to CD}^{\otimes 2} \Phi_{AA'}^{+\otimes 2} F_B U_{A'B\to CD}^{\dagger\otimes 2} F_{AC}.\end{aligned}$$

The first term can be bounded as

$$\begin{aligned}&\frac{1}{|B|(|B|+1)} \operatorname{tr} U_{A'B\to CD}^{\otimes 2} \Phi_{AA'}^{+\otimes 2} U_{A'B\to CD}^{\dagger\otimes 2} F_{AC} \\ &\quad= \frac{|B|^2}{|B|(|B|+1)} \operatorname{tr} U_{A'B\to CD}^{\otimes 2} (\Phi_{AA'}^{+\otimes 2} \otimes \tau_B^{\otimes 2}) U_{A'B\to CD}^{\dagger\otimes 2} F_{AC} \\ &\quad= \frac{|B|^2}{|B|(|B|+1)} \operatorname{tr} \tau_{AC}^2 \leq \operatorname{tr} \tau_{AC}^2,\end{aligned}$$

where the last equality follows since the Choi state of U is maximally mixed on AC. For the second term, we compute

$$\begin{aligned}&\frac{1}{|B|(|B|+1)} \operatorname{tr} U_{A'B\to CD}^{\otimes 2} \Phi_{AA'}^{+\otimes 2} F_B U_{A'B\to CD}^{\dagger\otimes 2} F_{AC} \\ &\quad= \frac{|B|^2}{|B|(|B|+1)} \operatorname{tr} U_{A'B'\to CD}^{\otimes 2} (\Phi_{AA'}^{+\otimes 2} \otimes \tau_{B'}^{\otimes 2}) F_{B'} U_{A'B'\to CD}^{\dagger\otimes 2} F_{AC} \\ &\quad= \frac{|B|^2}{|B|(|B|+1)} \operatorname{tr} U_{A'B'\to CD}^{\otimes 2} (\Phi_{AA'}^{+\otimes 2} \otimes \Phi_{BB'}^{+\otimes 2}) U_{A'B'\to CD}^{\dagger\otimes 2} F_{ABC} \\ &\quad= \frac{|B|^2}{|B|(|B|+1)} \operatorname{tr} \rho_{ABC}^2 \leq \operatorname{tr} \rho_D^2 = \frac{1}{|D|}.\end{aligned}$$

In the first step, we have relabeled B to B' and inserted two copies of the maximally mixed state $\tau_{B'}$; in the second, we have extended the maximally mixed states to maximally entangled states $\Phi_{BB'}^+$ and teleported the swap operator from the B' systems to the B systems; in the third step, we have recognized the Choi state of U and undone the swap trick; and in the last we have used that ρ_D is maximally mixed. Together, we obtain the following bound on the mean square deviation:

$$\mathbb{E}[\|\widetilde{\rho}_{AC} - \tau_{AC}\|_2^2] \leq \frac{1}{|D|}.$$

By the Cauchy-Schwarz inequality, $\|X\|_1^2 \leq |A||C| \, \|X\|_2^2$, we get

$$\mathbb{E}[\|\widetilde{\rho}_{AC} - \tau_{AC}\|_1^2] \leq \frac{|A||C|}{|D|}.$$

Now Markov's inequality gives

$$\Pr(\|\widetilde{\rho}_{AC} - \tau_{AC}\|_1 \geq \varepsilon) = \Pr(\|\widetilde{\rho}_{AC} - \tau_{AC}\|_1^2 \geq \varepsilon^2) \leq \frac{\mathbb{E}[\|\widetilde{\rho}_{AC} - \tau_{AC}\|_1^2]}{\varepsilon^2} \leq \frac{|A||C|}{\varepsilon^2 |D|},$$

and we obtain the desired bound:

$$\Pr(\|\widetilde{\rho}_{AC} - \tau_{AC}\|_1 \leq \varepsilon) \geq 1 - \frac{|A||C|}{\varepsilon^2 |D|}. \qquad \square$$

JHEP12(2016)145

The fact that we need $|A||C| \ll |D|$ is intuitive: for any realization of the random pure state σ_B, the state $\widetilde{\rho}_{ACD} = U_{A'B\to CD}\,|\Phi^+_{AA'}\rangle \otimes |\sigma_B\rangle$ is a purification of ρ_{AC}. Thus, if ρ_{AC} is to be maximally mixed then we clearly need that $|A||C| \leq |D|$, since otherwise the Schmidt rank cannot be $|A||C|$.

One natural scenario to apply Proposition 14 is to the toy model of black hole evaporation discussed on p. 14 (with D and C interchanged). If A is small (e.g., a qubit) and the initial black hole B is in a typical pure state, the Hawking radiation emitted at later times D is decoupled from A if D is much smaller than the post-evaporation black hole C [1]. The only assumption necessary about the dynamics is that the black hole be maximally I_3-scrambling.

Another natural scenario to apply Proposition 14 is in the context of maximally I_3-scrambling MIMO unitaries as discussed in section 6. Here, $|A_i||C_j|$ is usually much smaller than $|C_j^c|$. Hence, if we input a random pure state into A_i^c and half of a maximally entangled state into A_i, then with high probability the reduced state on A_iC_j is close to being maximally mixed. We can make a even stronger statement by demanding

$$\|\widetilde{\rho}_{A_iC_j} - \tau_{A_iC_j}\|_2 \leq \frac{1}{|A_i||C_j|},$$

which by [48] would imply that $\widetilde{\rho}_{A_iC_j}$ is separable. By Choi-Jamiołkowski, this means $\mathcal{N}^{\sigma_{A_i^c}}_{A_i'\to C_j}$ is entanglement-breaking. Using Proposition 14 the probability of this is at least $1 - |A_i|^2|C_j|^2/|C_j^c|$. In the case where all systems are of size d,

$$\frac{|A_i|^2|C_j|^2}{|C_j^c|} = \frac{1}{d^{n-5}},$$

which vanishes for large n or d.

E Existence of maximally scrambling MIMO unitaries

In this appendix we prove Proposition 13. As discussed in section 6, we first consider the case where M_n is replaced by an arbitrary $n \times n$ matrix M and identify sufficient conditions for the corresponding unitary $U_M\,|\vec{x}\rangle = |M\vec{x}\rangle$ to be maximally I_3-scrambling. First, it is clear that U_M is unitary if and only if M is invertible modulo d. We then consider the Choi state of U_M,

$$\rho_{AC} = \frac{1}{d^n}\sum_{\vec{x},\vec{y}} |\vec{x}\rangle\langle\vec{y}|_A \otimes |M\vec{x}\rangle\langle M\vec{y}|_C\,,$$

where we write $A = A_1 \ldots A_n$ and $C = C_1 \ldots C_n$. We now compute the reduced state $\rho_{A_i^cC_j}$. The partial trace over A_i forces $x_i = y_i$, and the partial trace over C_j^c forces $M\vec{x} = M\vec{y}$, except for the j-th entry. Assuming that matrix we obtain by replacing the j-th row of M with the elementary row e_i is invertible modulo d, this implies that $\vec{x} = \vec{y}$. Hence,

$$\rho_{A_i^cC_j} = \frac{1}{d^n}\sum_{\vec{x}} |\vec{x}'\rangle\langle\vec{x}'|_{A_i^c} \otimes |(M\vec{x})_j\rangle\langle(M\vec{x})_j|_{C_j}\,,$$

JHEP12(2016)145

where $\vec{x}'$ is $\vec{x}$ with the i-th entry omitted and $(M\vec{x})_j$ denotes the j-th entry of $M\vec{x}$. First summing over $\vec{x}'$ and then over all options for x_i, we get

$$\rho_{A_i^c C_j} = \frac{1}{d^{n-1}} \sum_{\vec{x}'} |\vec{x}'\rangle\langle\vec{x}'|_{A_i^c} \otimes \frac{1}{d} \sum_{x_i} |(M\vec{x})_j\rangle\langle(M\vec{x})_j|_{C_j} .$$

Assuming the matrix element M_{ji} is invertible modulo d, the right-hand side sum is over all basis states, for any fixed choice of $\vec{x}'$. Thus:

$$\rho_{A_i^c C_j} = \frac{1}{d^{n-1}} \sum_{\vec{x}'} |\vec{x}'\rangle\langle\vec{x}'|_{A_i^c} \otimes \tau_{C_j} = \tau_{A_i^c C_j}.$$

If we replace i by some $k \neq i$ then we also find that

$$\rho_{A_i C_j} = \mathrm{tr}_{A_k^c \setminus A_i}[\rho_{A_k^c C_j}] = \tau_{A_i C_j}.$$

Together, we obtain that

$$I_3(A_i; A_i^c; C_j) = -I(A_i; A_i^c|C_j) = -2\log d,$$

as desired. Hence, it is sufficient for M to satisfy the following three criteria so that U_M is maximally I_3-scrambling:

1. M is an invertible matrix modulo d.

2. If we replace any row of M by any elementary row then the resulting matrix is still invertible modulo d.

3. All entries of M are invertible modulo d.

Now we show that M_n defined in (6.3) satisfies these conditions when $d > n+1$ and is prime. Recall that

$$M_n = \begin{bmatrix} 2 & 1 & \dots & 1 \\ 1 & 2 & \dots & 1 \\ & & \ddots & \\ 1 & 1 & \dots & 2 \end{bmatrix}.$$

The third condition is obvious, since both 1 and 2 are invertible modulo d. For the first condition, we note that $n+1$ is invertible modulo d. Hence the following matrix is well-defined and easily checked to be the inverse of M_n:

$$M_n^{-1} = -(n+1)^{-1} \begin{bmatrix} -n & 1 & \dots & 1 \\ 1 & -n & \dots & 1 \\ & & \ddots & \\ 1 & 1 & \dots & -n \end{bmatrix}.$$

JHEP12(2016)145

It remains to verify the second criterion. If we replace the j-th row by an elementary row e_i, we obtain a matrix of the form

$$N_n = \begin{bmatrix} 2 & 1 & \dots & 1 & 1 \\ 1 & 2 & \dots & 1 & 1 \\ & & \dots & & \\ 0 & \dots & 1 & \dots & 0 \\ & & \dots & & \\ 1 & 1 & \dots & 1 & 2 \end{bmatrix}.$$

We can calculate the determinant by cofactor expanding along the elementary row. If $i = j$ then we obtain that $\det N_n = \pm \det M_{n-1}$, which is nonzero by the preceding. Otherwise, if $i \neq j$ then find that $\det N_n$ is up to sign equal to the determinant of the following $(n-1) \times (n-1)$ matrix,

$$N'_{n-1} = \begin{bmatrix} 2 & 1 & \dots & 1 & 1 \\ 1 & 2 & \dots & 1 & 1 \\ & & \dots & & \\ 1 & \dots & 1 & \dots & 1 \\ & & \dots & & \\ 1 & 1 & \dots & 1 & 2 \end{bmatrix},$$

which looks like M_{n-1} except that a 2 is replaced by a 1. We can use determinant-preserving row operations to reduce this matrix to

$$\begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \dots & & \\ 1 & \dots & 1 & \dots & 1 \\ & & \dots & & \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix},$$

which has determinant one. This concludes the proof of Proposition 13.

References

[1] P. Hayden and J. Preskill, *Black holes as mirrors: Quantum information in random subsystems*, *JHEP* **09** (2007) 120 [arXiv:0708.4025] [INSPIRE].

[2] Y. Sekino and L. Susskind, *Fast Scramblers*, *JHEP* **10** (2008) 065 [arXiv:0808.2096] [INSPIRE].

[3] S.H. Shenker and D. Stanford, *Black holes and the butterfly effect*, *JHEP* **03** (2014) 067 [arXiv:1306.0622] [INSPIRE].

JHEP12(2016)145

[4] S.H. Shenker and D. Stanford, *Multiple Shocks*, *JHEP* **12** (2014) 046 [arXiv:1312.3296] [INSPIRE].

[5] A. Kitaev, *Hidden correlations in the Hawking radiation and thermal noise*, talk given at *Fundamental Physics Prize Symposium*, 10 November 2014.

[6] D.A. Roberts and D. Stanford, *Two-dimensional conformal field theory and the butterfly effect*, *Phys. Rev. Lett.* **115** (2015) 131603 [arXiv:1412.5123] [INSPIRE].

[7] J. Maldacena, S.H. Shenker and D. Stanford, *A bound on chaos*, *JHEP* **08** (2016) 106 [arXiv:1503.01409] [INSPIRE].

[8] P. Hosur, X.-L. Qi, D.A. Roberts and B. Yoshida, *Chaos in quantum channels*, *JHEP* **02** (2016) 004 [arXiv:1511.04021] [INSPIRE].

[9] M.M. Wilde, *Quantum information theory*. Cambridge University Press (2013).

[10] C.H. Bennett, A.W. Harrow, D.W. Leung and J.A. Smolin, *On the capacities of bipartite Hamiltonians and unitary gates*, *IEEE Trans. Inf. Theory* **49** (2003) 1895 [quant-ph/0205057].

[11] A. Harrow, *Coherent communication of classical messages*, *Phys. Rev. Lett.* **92** (2004) 097902 [quant-ph/0307091].

[12] A.W. Harrow and P.W. Shor, *Time reversal and exchange symmetries of unitary gate capacities*, *IEEE Trans. Inf. Theory* **56** (2010) 462 [quant-ph/0511219].

[13] D.W. Berry, *Lower bounds for communication capacities of two-qudit unitary operations*, *Phys. Rev.* **A 76** (2007) 062302 [arXiv:0704.2066].

[14] A.W. Harrow and D.W. Leung, *A communication-efficient nonlocal measurement with application to communication complexity and bipartite gate capacities*, *IEEE Trans. Inf. Theory* **57** (2011) 5504 [arXiv:0803.3066].

[15] E. Wakakuwa, A. Soeda and M. Murao, *A coding theorem for bipartite unitaries in distributed quantum computation*, *IEEE Int. Symp. Inf. Theory* (2015) 705, [arXiv:1505.04352].

[16] E. Wakakuwa, A. Soeda and M. Murao, *The cost of randomness for converting a tripartite quantum state to be approximately recoverable*, arXiv:1512.06920.

[17] P. Hayden, M. Headrick and A. Maloney, *Holographic Mutual Information is Monogamous*, *Phys. Rev.* **D 87** (2013) 046003 [arXiv:1107.2940] [INSPIRE].

[18] V. Balasubramanian, P. Hayden, A. Maloney, D. Marolf and S.F. Ross, *Multiboundary Wormholes and Holographic Entanglement*, *Class. Quant. Grav.* **31** (2014) 185015 [arXiv:1406.2663] [INSPIRE].

[19] N. Bao, S. Nezami, H. Ooguri, B. Stoica, J. Sully and M. Walter, *The Holographic Entropy Cone*, *JHEP* **09** (2015) 130 [arXiv:1505.07839] [INSPIRE].

[20] F. Pastawski, B. Yoshida, D. Harlow and J. Preskill, *Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence*, *JHEP* **06** (2015) 149 [arXiv:1503.06237] [INSPIRE].

[21] P. Hayden, S. Nezami, X.-L. Qi, N. Thomas, M. Walter and Z. Yang, *Holographic duality from random tensor networks*, *JHEP* **11** (2016) 009 [arXiv:1601.01694] [INSPIRE].

[22] S. Nezami and M. Walter, *Multipartite Entanglement in Stabilizer Tensor Networks*, arXiv:1608.02595 [INSPIRE].

JHEP12(2016)145

[23] D. Sutter, O. Fawzi and R. Renner, *Universal recovery map for approximate Markov chains*, *Proc. the Roy. Soc. Lond.* **A 472** (2016) 20150623 [arXiv:1504.07251].

[24] B. Ibinson, N. Linden and A. Winter, *Robustness of quantum Markov chains*, *Commun. Math. Phys.* **277** (2008) 289 [quant-ph/0611057].

[25] M. Christandl, N. Schuch and A. Winter, *Entanglement of the antisymmetric state*, *Phys. Rev. Lett.* **104** (2010) 240405 [arXiv:0910.4151].

[26] D. Goyeneche, D. Alsina, J.I. Latorre, A. Riera and K. Życzkowski, *Absolutely maximally entangled states, combinatorial designs and multiunitary matrices*, *Phys. Rev.* **A 92** (2015) 032316 [arXiv:1506.08857] [INSPIRE].

[27] W. Helwig, W. Cui, A. Riera, J.I. Latorre and H.-K. Lo, *Absolute Maximal Entanglement and Quantum Secret Sharing*, *Phys. Rev.* **A 86** (2012) 052335 [arXiv:1204.2289] [INSPIRE].

[28] A. Keet, B. Fortescue, D. Markham and B.C. Sanders, *Quantum secret sharing with qudit graph states*, *Phys. Rev.* **A 82** (2010) 062315 [arXiv:1004.4619].

[29] I. Devetak and J. Yard, *Exact cost of redistributing multipartite quantum states*, *Phys. Rev. Lett.* **100** (2008) 230501 [quant-ph/0612050].

[30] M. Berta, F. G. Brandao, C. Majenz and M.M. Wilde, *Deconstruction and conditional erasure of quantum correlations*, arXiv:1609.06994.

[31] B. Swingle, G. Bentsen, M. Schleier-Smith and P. Hayden, *Measuring the scrambling of quantum information*, *Phys. Rev.* **A 94** (2016) 040302 [arXiv:1602.06271] [INSPIRE].

[32] N.Y. Yao et al., *Interferometric Approach to Probing Fast Scrambling*, arXiv:1607.01801 [INSPIRE].

[33] P. Hayden, R. Jozsa, D. Petz and A. Winter, *Structure of states which satisfy strong subadditivity of quantum entropy with equality*, *Commun. Math. Phys.* **246** (2004) 359 [quant-ph/0304007].

[34] O. Fawzi and R. Renner, *Quantum conditional mutual information and approximate Markov chains*, *Commun. Math. Phys.* **340** (2015) 575 [arXiv:1410.0664].

[35] K. Li and A. Winter, *Squashed entanglement, k-extendibility, quantum Markov chains, and recovery maps*, arXiv:1410.4184.

[36] I.H. Kim, *Application of conditional independence to gapped quantum many-body systems*, (2013), http://www.physics.usyd.edu.au/quantum/Coogee2013/Presentations/Kim.pdf.

[37] L. Zhang, *Conditional mutual information and commutator*, *Int. J. Theor. Phys.* **52** (2013) 2112 [arXiv:1212.5023].

[38] M. Berta, K.P. Seshadreesan and M.M. Wilde, *Rényi generalizations of the conditional quantum mutual information*, *J. Math. Phys.* **56** (2015) 022205 [arXiv:1403.6102] [INSPIRE].

[39] C.W. Helstrom, *Quantum detection and estimation theory*, *J. Stat. Phys.* **1** (1969) 231.

[40] C.H. Bennett, P.W. Shor, J.A. Smolin, B.M. Terhal and A.V. Thapliyal, *Entanglement-assisted classical capacity of noisy quantum channels*, *Phys. Rev. Lett.* **83** (1999) 3081 [quant-ph/9904023] [INSPIRE].

[41] C.H. Bennett, P.W. Shor, J.A. Smolin and A.V. Thapliyal, *Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem*, *IEEE Trans. Inf. Theory* **48** (2002) 2637, [quant-ph/0106052].

JHEP12(2016)145

[42] M. Fannes, *A continuity property of the entropy density for spin lattice systems*, *Commun. Math. Phys.* **31** (1973) 291.

[43] K.M. Audenaert, *A sharp continuity estimate for the von Neumann entropy*, *J. Phys.* **A 40** (2007) 8127 [quant-ph/0610146].

[44] M. Grassl, T. Beth and T. Pellizzari, *Codes for the quantum erasure channel*, *Phys. Rev.* **A 56** (1997) 33 [quant-ph/9610042] [INSPIRE].

[45] S. Lloyd, *The capacity of the noisy quantum channel*, *SCIENCE* (1996) [quant-ph/9604015] [INSPIRE].

[46] P.W. Shor, *The quantum channel capacity and coherent information*, in *MSRI Workshop on Quantum Computation*, (2002).

[47] I. Devetak, *The private classical capacity and quantum capacity of a quantum channel*, *IEEE Trans. Inf. Theory* **51** (2005) 44 [quant-ph/0304127].

[48] L. Gurvits and H. Barnum, *Largest separable balls around the maximally mixed bipartite quantum state*, *Phys. Rev.* **A 66** (2002) 062311 [quant-ph/0204159].

JHEP12(2016)145