Catalytic Decoupling of Quantum Information

Christian Majenz, Mario Berta, Frédéric Dupuis, Renato Renner, and Matthias Christandl

Phys. Rev. Lett. **118**, 080503 — Published 23 February 2017

DOI: 10.1103/PhysRevLett.118.080503

Catalytic Decoupling of Quantum Information

Christian Majenz,[1,*] Mario Berta,[2] Frédéric Dupuis,[3] Renato Renner,[4] and Matthias Christandl[1]

[1] *Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, DK-2100 Copenhagen Ø.*
[2] *Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA 91125, USA.*
[3] *Faculty of Informatics, Masaryk University, Brno, Czech Republic.*
[4] *Institute for Theoretical Physics, ETH Zurich, 8093 Zürich, Switzerland.*

(Dated: January 9, 2017)

The decoupling technique is a fundamental tool in quantum information theory with applications ranging from thermodynamics to many-body physics and black hole radiation, whereby a quantum system is decoupled from another one by discarding an appropriately chosen part of it. Here we introduce catalytic decoupling, i.e., decoupling with the help of an independent system. Thereby we remove a restriction on the standard decoupling notion and present a tight characterization in terms of the max-mutual information. The novel notion unifies various tasks, and leads to a resource theory of decoupling.

Introduction. Erasing correlations between quantum systems via local operations, decoupling, is a task that was first studied in the context of quantum information theory [1] (see [2] for an introductory tutorial). It serves as a building block for a variety of tasks in quantum information and quantum cryptography. In particular, decoupling has been crucial for understanding how to distribute quantum information between different parties [3–7] and for understanding how to send quantum information over noisy quantum channels [8–11], as well as randomness extraction [12]. The concept is, however, also very useful in physics (as, e.g., outlined in [13]). Applications range from quantum thermodynamics [14–16], to the study of black hole radiation [17–19], and solid state physics [20].

Standard decoupling. The basic idea behind decoupling is the following: If a mixed bipartite quantum state ϱ_{AE} is only weakly correlated, then it should suffice to erase a small part of A to approximately decouple A from E, i.e., to get an approximate product state (see Figure 1a). More precisely, we say that a bipartite quantum state ϱ_{AE} is ε-decoupled by the partial trace map $\mathcal{T}_{A\to A_1}(\cdot) = \mathrm{Tr}_{A_2}[\cdot]$ with $A = A_1A_2$ if there exists a unitary operation U_A such that,

$$\min_{\omega_{A_1}\otimes\omega_E} P\big(\mathcal{T}_{A\to A_1}(U_A\varrho_{AE}U_A^\dagger), \omega_{A_1}\otimes\omega_E\big) \leq \varepsilon, \qquad (1)$$

where the minimum is over all product quantum states $\omega_{A_1}\otimes\omega_E$, and $P(\beta,\gamma) := \big(1 - \|\sqrt{\beta}\sqrt{\gamma}\|_1^2\big)^{1/2}$ denotes the purified distance [21]. The A_1-system is called the decoupled system and the A_2-system the remainder system – when trying to decouple A from E, we succeed on A_1, and A_2 is the remainder we fail to decouple. The fundamental question that we want to discuss is how large we have to choose the remainder system A_2 in order to achieve ε-decoupling. We denote the minimal remainder system size, i.e., the logarithm of the minimal remainder system dimension, for ε-decoupling A from E in a state ϱ_{AE} by $R^\varepsilon(A;E)_\varrho$. For a formal definition of $R^\varepsilon(A;E)_\varrho$ see Supplemental Definition 18.

Converse. We first show quite naturally that $R^\varepsilon(A;E)_\varrho$ has to be at least of the size of the smooth max-mutual information $I^\varepsilon_{\max}(E:A)_\varrho$ present in the initial state ϱ_{AE}. This measure is defined as [11],

$$I^\varepsilon_{\max}(E;A)_\varrho := \min_{\bar\varrho} I_{\max}(E;A)_{\bar\varrho} \quad \text{with} \qquad (2)$$

$$I_{\max}(E;A)_{\bar\varrho} := \log\min\left\{\mathrm{Tr}\sigma_A | \sigma_A\otimes\bar\varrho_E \geq \bar\varrho_{AE}\right\}, \qquad (3)$$

where the minimum in (2) is over all bipartite quantum states with $P(\varrho_{AE},\bar\varrho_{AE}) \leq \varepsilon$ [22], and the minimum in (3) is over all $\sigma_A \geq 0$. We note that the definition of the smooth max-information is a priori not symmetric in $A:E$. However, we have [23],

$$I^\varepsilon_{\max}(E;A)_\varrho \approx I^\varepsilon_{\max}(A;E)_\varrho, \qquad (4)$$

where $\approx$ stands for equality up to terms $\mathcal{O}(\log(1/\varepsilon))$. For the converse we exploit that the smooth max-mutual information is invariant under local unitary operations and that it has the so-called non-locking property (see [24] about information locking). That is, just like the quantum mutual information it fulfills the inequality [11, Lemma B.12],

$$I^\varepsilon_{\max}(E;A_1A_2)_\varrho \leq I^\varepsilon_{\max}(E;A_1)_\varrho + 2\log|A_2|, \qquad (5)$$

where $|A_2|$ denotes the dimension of A_2. Since the final state is a product state, its smooth max-mutual information $I^\varepsilon_{\max}(E;A_1)_{\omega\otimes\omega}$ becomes zero. This means that in order to erase the initial correlations $I^\varepsilon_{\max}(E;A)_\varrho$ we need at least a remainder system of size [25],

$$R^\varepsilon(A;E)_\varrho \geq \frac{1}{2}I^\varepsilon_{\max}(E;A)_\varrho. \qquad (6)$$

Previous works. Most of the aforementioned decoupling references only give good achievability bounds for states of the form $\varrho_{A^nE^n} = \varrho_{AE}^{\otimes n}$ in the asymptotic limit $n \to \infty$. Whereas this setting is relevant in quantum Shannon theory, it is often a severe restriction for applications in physics. For typical physical situations (e.g., in thermodynamics), there is usually not even a natural decomposition of a large system in n subsystems. A notable exception concerning achievability results is reference [13], where the authors show that

$$R^{\varepsilon}(A;E)_{\varrho} \lesssim \frac{1}{2}\Big(H_{\max}^{\varepsilon'}(A)_{\varrho} - H_{\min}^{\varepsilon'}(A|E)_{\varrho}\Big) \text{ with } \varepsilon' = \frac{\varepsilon}{5}, \tag{7}$$

where $\lesssim$ means up to terms $\mathcal{O}(\log(1/\varepsilon))$ here. (We give a proof of this particular statement in the supplemental material). Here, $H_{\max}^{\varepsilon}$ and $H_{\min}^{\varepsilon}$ denote the smooth conditional max- and min-entropy whose exact definitions can be found in the supplemental material (or see the textbook [21]). In fact, the results from [13] show that not only decoupling in the sense of (1) is achieved, but moreover that the decoupled system is also randomized. That is, there exists a quantum state ω_E and a unitary operation U_A such that Equation (1), with $\omega_{A_1} = 1_{A_1}/|A_1|$ and where 1_{A_1} denotes the identity matrix on A_1.

It turns out that there can be an arbitrarily big gap between the converse (6) and the achievability result (7). This is best seen for an example with trivial system E, where the corresponding max-mutual information converse bound becomes zero. In that case the achievability bound (7) reduces to the difference between the smooth max- and min-entropy and it is known that this can become roughly as big as $\log|A|$ (we provide an explicit example in the supplemental material). In order to achieve the converse from (6) we propose in the following a generalized notion of decoupling.

Catalytic decoupling. A natural question to ask at this point is if decoupling can be achieved more efficiently in the presence of an already uncorrelated ancilla system (see Figure 1). Formally, we say that a bipartite quantum state ϱ_{AE} is ε-decoupled catalytically by the ancilla state $\varrho_{A'}$ and the partial trace map $\mathcal{T}_{\bar{A}\to A_1}(\cdot) = \mathrm{Tr}_{A_2}[\cdot]$ with $\bar{A} \equiv AA' \cong A_1A_2$ if there exists unitary operation $U_{\bar{A}}$ such that,

$$\min_{\omega_{A_1}\otimes\omega_E} P\big(\mathcal{T}_{\bar{A}\to A_1}(U_{\bar{A}}\varrho_{\bar{A}E}U_{\bar{A}}^{\dagger}), \omega_{A_1}\otimes\omega_E\big) \le \varepsilon \tag{8}$$

$$\text{where} \quad \varrho_{\bar{A}E} = \varrho_{AE}\otimes\varrho_{A'}. \tag{9}$$

Again, we call the A_1-system the decoupled system and the A_2-system the remainder system. The term catalytic means that the share of the initially uncorrelated ancilla system A', that becomes part of the decoupled system A_1, stays decoupled (see Figure 1).

Now, we are interested in the minimal size of the remainder system A_2 in order to achieve ε-decoupling catalytically. We denote the minimal remainder system size for catalytically decoupling A from E in a state ϱ_{AE} by $R_c^{\varepsilon}(A;E)_{\varrho}$. For a formal definition of $R_c^{\varepsilon}(A;E)_{\varrho}$ see Supplemental Definition 19. Clearly, we have $R_c^{\varepsilon}(A;E)_{\varrho} \le R^{\varepsilon}(A;E)_{\varrho}$, as we can always choose a trivial ancilla. Moreover, since appending with an ancilla does not change the smooth max-mutual information (see supplemental material), the same converse as in (6) still holds.

One may analyze decoupling using a resource-theoretic approach, treating decoupled systems as a resource. A quantum system A coupled to the environment E can yield a decoupled system A_1 of a certain size through standard decoupling. That is, in the resource theory language of [26] we have $\langle\varrho_{AE}\rangle \ge_{\varepsilon} (\log|A| - R^{\varepsilon}(A;E)_{\varrho})[d]$. Here, $x[d]$ denotes x decoupled qubits and $\ge_{\varepsilon}$ stands for up to error ε (see also [27]), while the set of free operations is given by the unitary operations [28]. Now, our novel paradigm makes use of the possibility that if we already have decoupled qubits, then we are able to decouple a larger system [29],

$$\langle\varrho_{AE}\rangle + n[d] \ge_{\varepsilon} \big(n + \log|A| - R_c^{\varepsilon}(A;E)_{\varrho}\big)\,[d] \quad \text{for } n \text{ large enough.} \tag{10}$$

Note, however, that this inequality is only proved for *specific* initial and final decoupled states used in the presented decoupling protocols.

Tight achievability. In contrast to standard decoupling as in (1), catalytic decoupling can be achieved with a remainder system size that is essentially equal to the smooth max-mutual information.

Theorem 1 (Catalytic decoupling). *For any bipartite quantum state ϱ_{AE} and $0 < \delta \le \varepsilon \le 1$ we have:*

$$R_c^{\varepsilon}(A;E)_{\varrho} \lesssim \frac{1}{2} I_{\max}^{\varepsilon-\delta}(E;A)_{\varrho} \tag{11}$$

where $\lesssim$ stands for smaller or equal up to terms $\mathcal{O}(\log\log|A| + \log(1/\delta))$. We also have the converse

$$R_c^{\varepsilon}(A;E)_{\varrho} \ge \frac{1}{2} I_{\max}^{\varepsilon}(E:A)_{\varrho}. \tag{12}$$

Note that the converse comes from Equation (6).

In fact, we not only show that catalytic decoupling in the sense of (8) is achieved, but moreover that the decoupled system ends up in the marginal of the original state:

$$P\big(\varrho_{A_1E}, \varrho_{A_1}\otimes\omega_E\big) \le \varepsilon \quad \text{for some quantum state } \omega_E. \tag{13}$$

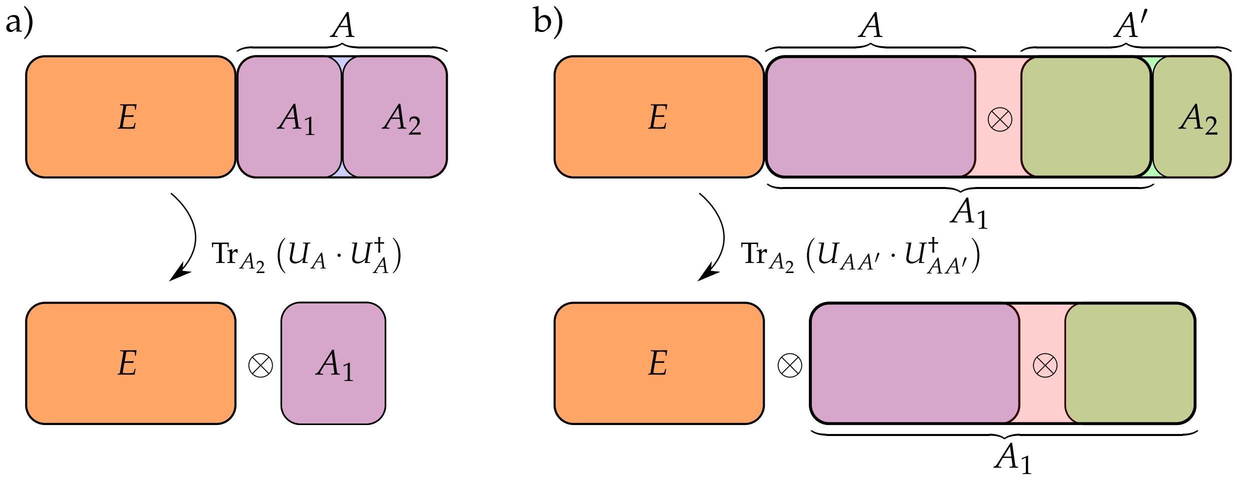
a)
A
E
A_1
A_2
$\mathrm{Tr}_{A_2}\left(U_A \cdot U_A^\dagger\right)$
E
⊗
A_1
b)
A
A'
E
⊗
A_2
A_1
$\mathrm{Tr}_{A_2}\left(U_{AA'} \cdot U_{AA'}^\dagger\right)$
E
⊗
⊗
A_1

FIG. 1. Schematic representation of a) standard and b) catalytic decoupling: tracing out a system A_2 leaves the remaining state decoupled. While there is no ancilla for standard decoupling as in a), catalytic decoupling as in b) allows to make use of an additional, already decoupled system A'. The basic question is how large we have to choose the system A_2 such that the remaining system A_1 is decoupled from E.

In particular, and in contrast to the standard decoupling results leading to (7), our catalytic decoupling scheme does not randomize the decoupled system but leaves it invariant (up to the approximation error ε). We can even choose $A_1 = AA_1'$ such that the decoupled system contains the marginal of the input state (A) (plus part of the catalyst, A_1').

In the supplemental material we give two conceptually different proofs for Theorem 1. The first proof is based on the standard decoupling techniques from [11, 13] combined with the use of embezzling entangled quantum states [30]. For (11) this yields a difference of size at most $\log\log|A| + \mathcal{O}(\log(1/\delta))$ [31]. The second proof is based on the convex splitting technique of Anshu *et al.* [32]. It allows to upper bound the difference in (11) with the tighter bound

$$R_c^\varepsilon(A;E)_\varrho - \frac{1}{2} I_{\max}^{\varepsilon-\delta}(E;A)_\varrho \leq \frac{1}{2}\Big\{\log\log I_{\max}^{\varepsilon-\delta}(E;A)_\varrho\Big\}_+ + \mathcal{O}(\log(1/\delta))\,, \qquad (14)$$

where $\{\cdot\}_+ := \max\{0,\cdot\}$. Moreover, this argument is constructive and hence leads to an explicit scheme for decoupling. This improves on the standard decoupling bounds which are achieved using the probabilistic technique [33] (as, e.g., the previously best known bound (7) from [13]).

Discussion. The achievability result (11) together with the converse (12) establish an operational interpretation of the smooth max-information as twice the minimal size of the remainder system to achieve ε-decoupling. We note that the approximation error as well as the smoothing parameter can be made arbitrarily close in (12) and (11) with only a logarithmic penalty. This enables us to make a statement about the case of many independent copies of a state, the so called i.i.d. setting. Following the information-theoretic arguments outlined in [34] (which in turn are based on ideas from [35, 36]), we find that for states of the form $\varrho_{A^nE^n} = \varrho_{AE}^{\otimes n}$ and large $n \to \infty$,

$$\frac{1}{n} R_c^\varepsilon(A^n;E^n)_{\varrho^{\otimes n}} = \frac{1}{2}\left(I(A:E)_\varrho + \sqrt{\frac{V(A:E)_\varrho}{n}}\,\Phi^{-1}(\varepsilon)\right) + \mathcal{O}\left(\frac{\log n}{n}\right), \qquad (15)$$

with the mutual information $I(A:E)_\varrho = H(A)_\varrho + H(E)_\varrho - H(AE)_\varrho$ featuring the von Neumann entropy $H(A)_\varrho = -\mathrm{Tr}(\varrho_A \log \varrho_A)$, and the mutual information variance $V(A:E)_\varrho$ as well as the cumulative normal distribution function Φ specified in the supplemental material. We note that no such tight (second-order) asymptotic expansion is known for standard decoupling. However, the achievability (7) together with the converse (6) imply that (using the asymptotic equipartition property from [21]),

$$\lim_{n\to\infty} \frac{1}{n} R^\varepsilon(A^n;E^n)_{\varrho^{\otimes n}} = \frac{1}{2} I(A:E)_\varrho \quad \text{for } 0 < \varepsilon < 1. \qquad (16)$$

Thus, we can conclude that catalytic decoupling and standard decoupling become equivalent in the first order rate asymptotically: the mutual information quantifies the minimal size of the remainder system.

Applications. We are now going to illustrate the use of catalytic decoupling with various applications. Groisman *et al.* [37] introduced an operational approach to quantifying the total correlations that are present in a quantum state. In analogy to Landauer's erasure principle [38], they characterize the strength of correlations by the amount of randomness that has to be injected locally to decorrelate the state. This randomizing is done by a random-unitary channel on one of the systems (called local unitary randomizing, A-LUR in [37]):

$$\Lambda(\cdot) = \sum_{i=1}^{N} p_i U_i(\cdot)U_i^\dagger. \tag{17}$$

We say that that the correlations between A and E in a state ϱ_{AE} can be ε-erased by a local mixture of N unitaries on A, if Λ_A ε-decouples A from E. That is, if there exists a quantum channel Λ_A of the form (17) such that

$$\min_{\omega_A\otimes\omega_E} P\left(\Lambda_A(\varrho_{AE}), \omega_A \otimes \omega_E\right) \leq \varepsilon. \tag{18}$$

We denote the logarithm of the minimal number of unitaries needed for ε-erasing the correlations between A and E in a state ϱ_{AE} by $R^\varepsilon_U(A;E)_\varrho$. For a formal definition of $R^\varepsilon_U(A;E)_\varrho$ see Supplemental Definition 20. Groisman *et al.* show that for states of the form $\varrho_{A^nE^n} = \varrho_{AE}^{\otimes n}$ for large $n \to \infty$:

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty} \frac{1}{n} R^\varepsilon_U(A^n;E^n)_{\varrho^{\otimes n}} = I(A:E)_\varrho. \tag{19}$$

In the following we will see that the task of *catalytic* local erasure of correlation becomes equivalent to catalytic decoupling [39]. We therefore define $R^\varepsilon_{U,c}(A;E)_\varrho := \inf R^\varepsilon_U(AA':E)_{\varrho\otimes\sigma}$, where the infimum is taken over all ancilla systems. This quantity is formally defined in Supplemental Definition 20.

Proposition 2 (Erasure of correlations). *For any bipartite quantum state ϱ_{AE} we have $\frac{1}{2}R^\varepsilon_{U,c}(A;E)_\varrho = R^\varepsilon_c(A;E)_\varrho$. Hence, we get*

$$I^\varepsilon_{\max}(E;A)_\varrho \leq R^\varepsilon_{U,c}(A;E)_\varrho \lesssim I^{\varepsilon-\delta}_{\max}(E;A)_\varrho. \tag{20}$$

where $\lesssim$ stands for smaller or equal up to terms $\mathcal{O}(\log\log|A| + \log(1/\delta))$. The same asymptotic expansion as in (15) holds.

This is the generalization of the results in [37] to arbitrary (structureless) states (see also [9, 35, 36]). It gives an alternative operational characterization of the smooth max-mutual information as the the minimal number of unitaries needed for ε-erasing the correlations between A and E. The proof of Proposition 2 proceeds as follows. Suppose we have a way of decoupling A from E with remainder system A_2, and let $|A_2| = 2^k$ for some $k \in \mathbb{N}$. Then, we can think of A_2 as k qubits and erase each of them applying a uniform mixture of the Pauli matrices and the identity. This is a mixture of $4^k = 2^{2k}$ unitaries. Conversely, suppose we have a mixture of $N = 2^{2k}$ unitaries on A that erase the correlations to E. We take the mixed ancilla state $1_{A_1'A_2'}/|A_1'A_2'|$ with $A_i' \cong \mathbb{C}^{2^k}$. Now, we apply the unitaries controlled on an orthonormal basis of maximally entangled states of $A_1'A_2'$. Then, $A_1'A$ are decoupled from E, i.e., we achieved catalytic decoupling with remainder system size $\log|A_2'| = k$ [40].

As a second application we discuss quantum state merging [1] in whose context decoupling was originally introduced [3, 4]. In the communication task of state merging, Alice, Bob and a Referee share initially a pure quantum state ψ_{ABR}. Now Alice has to send her system A to Bob using as little communication as possible. Any catalytic decoupling theorem naturally leads to a quantum state merging protocol. Since the catalytic decoupling theorem is the abstraction of the results on quantum state merging in [11, 32], inserting the bounds from Theorem 1, we recover the following optimal result for the communication cost $q^\varepsilon(A\rangle B)_\varrho$ of merging A to B (up to error $\varepsilon > 0$, see Supplemental Definition 31 for a formal definition).

Proposition 3 (Coherent quantum state merging). *Let ϱ_{ABR} be a pure tripartite quantum state shared between Alice, Bob and a Referee. If Alice and Bob have arbitrary entanglement assistance at hand, then Alice can send her system A to Bob up to error $\varepsilon > 0$ in purified distance using*

$$q^\varepsilon(A\rangle B)_\varrho \lesssim \frac{1}{2} I^{\varepsilon/3}_{\max}(R;A)_\varrho \tag{21}$$

qubits of quantum communication, where $\lesssim$ stands for smaller or equal up to terms $\mathcal{O}(\log\log|A| + \log(1/\delta))$.

We note that in the asymptotic limit standard decoupling is sufficient to obtain,

$$\lim_{n\to\infty} \frac{1}{n} q^\varepsilon(A^n\rangle B^n)_{\varrho^{\otimes n}} = \frac{1}{2} I(R:A)_\varrho, \tag{22}$$

which is optimal [4]. For the general setup there is an issue known as entanglement spread [41], and for the proof of Proposition 3 we make use of catalytic decoupling and Uhlmann's theorem [42]. In the following we present a proof sketch but defer the full argument to the supplemental material. Setting $\delta = \varepsilon/6$ in Theorem 1 shows that there exists an ancilla state $\varrho_{A'}$ and a unitary $U_{AA'\to A_1A_2}$ such that A_1 is $\varepsilon/2$ decoupled from R and

$$\log|A_2| \lesssim \frac{1}{2} I^{\varepsilon/3}_{\max}(R:A)_\varrho \tag{23}$$

Now, Alice and Bob take a pure entangled state $\varrho_{A'B'}$ where Alice's part A' is in state $\varrho_{A'}$, the required ancilla. She applies the unitary $U_{AA'\to A_1A_2}$ and sends A_2 to Bob. The decoupling condition and the triangle inequality for the purified distance imply that $P(\varrho_{A_1R}, \varrho_{A_1}\otimes\varrho_R) \leq \varepsilon$, so by Uhlmann's theorem there exists a unitary $U_{A_2B\to ABB_1}$ acting on Bobs system such that

$$P(U\varrho_{A_1A_2BR}U^\dagger, \varrho_{A_1B_1}\otimes\varrho_{ABR}) \leq \varepsilon, \tag{24}$$

where $\varrho_{A_1B_1}$ is a purification of ϱ_{A_1} and we omitted the subscript of U. This implies that Bob has systems AB after applying U.

Finally, we show in the supplemental material that catalytic decoupling directly implies the achievability bound for quantum state redistribution of Anshu *et al.* [32] (see [43, 44] for alternative bounds).

Extensions. We have analyzed how well the partial trace map $\mathcal{T}_{A\to A_1}(\cdot) = \mathrm{Tr}_{A_2}[\cdot]$ decouples. However, as originally suggested in [13], we can also study quantum channels $\mathcal{T}_{A\to B}(\cdot)$ that add noise in an arbitrary way in order to achieve decoupling. To further clarify the important difference between standard decoupling and catalytic decoupling, as well as to correct the faulty [13, Corollary 4.2], we now give a converse for the decoupling behavior of general quantum channels.

Proposition 4 (Correction of Corollary 4.2 from [13]). *If for a bipartite quantum state ϱ_{AE} and a quantum channel $\mathcal{T}_{A\to B}$,*

$$\int \mathrm{d}U_A P\left(\mathcal{T}_{A\to B}(U_A\varrho_{AE}U_A^\dagger), \mathcal{T}_{A\to B}\left(\frac{1_A}{|A|}\right)\otimes\varrho_E\right) \leq \varepsilon, \tag{25}$$

then we have

$$H_{\min}^{\varepsilon'}(A|E)_\varrho + H_{\max}^{\varepsilon}(A'|B)_\tau \gtrsim 0 \quad \text{with } \varepsilon' = 15\sqrt{\varepsilon}, \tag{26}$$

where $\tau_{A'B} = \mathcal{T}_{A\to B}(\phi^+_{A'A})$ is the Choi-Jamiołkowski state.

In the supplemental material we prove Proposition 4 starting from [13, Theorem 4.1] (from which the faulty [13, Corollary 4.2] was derived). The crucial difference of Proposition 4 to the erroneous version is the assumption that not only decoupling, but decoupling and randomizing is achieved:

$$\mathcal{T}_{A\to B}(\varrho_A)\otimes\varrho_E \quad \text{vs.} \quad \mathcal{T}_{A\to B}\left(\frac{1_A}{|A|}\right)\otimes\varrho_E. \tag{27}$$

For example, a product state $\varrho_{AE} = \varrho_A\otimes\varrho_E$ with ϱ_A pure has $H_{\min}^{\varepsilon'}(A|E)_\varrho = 0$. It is, however, already perfectly decoupled by the identity map on A, which has $H_{\max}^{\varepsilon}(A|B)_\tau \approx -\log|A|$.

In turn, applying the converse bound (26) to the partial trace map $\mathcal{T}_{A\to A_1}(\cdot) = \mathrm{Tr}_{A_2}[\cdot]$ shows that the standard decoupling bound (7) in terms of a difference of smooth max- and min-entropy is natural if we ask for decoupling and randomizing. However, if we are not interested in randomizing but only in decoupling, then our main result about catalytic decoupling (Theorem 1) shows that the smooth max-mutual information is the relevant measure.

Conclusion. In this work we introduced the notion of catalytic decoupling. As our main result we established that the minimal remainder system size for decoupling is given by half the smooth max-mutual information. Moreover, we have shown that catalytic decoupling for general (structureless) states naturally quantifies the resources needed in the erasure of correlation model from [37] and for quantum state merging as in [11]. All of this strengthens the smooth max-mutual information as the one-shot generalization of the quantum mutual information. Finally, given that standard decoupling has already proven useful in various areas of physics (see the references in the introduction), we believe that catalytic decoupling has manifold applications that remain to be explored.

Acknowledgments. We thank Mark M. Wilde for comments on an earlier version of this paper. MC and CM acknowledge financial support from the European Research Council (ERC Grant Agreement no 337603), the Danish Council for Independent Research (Sapere Aude), the Villum Centre of Excellence for the Mathematics of Quantum Theory (QMATH) and the Swiss National Science Foundation (project no PP00P2-150734). MB acknowledges funding by the SNSF through a fellowship, funding by the Institute for Quantum Information and Matter (IQIM), an NSF Physics Frontiers Center (NFS Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028), and funding support form the ARO grant for Research on Quantum Algorithms at the IQIM (W911NF-12-1-0521). FD acknowledges the support of the Czech Science Foundation (GA ČR) project no GA16-22211S and FD and RR acknowledge the support of the EU FP7 under grant agreement no 323970 (RAQUEL).

* majenz@math.ku.dk

[1] M. Horodecki, J. Oppenheim, and A. Winter, Nature **436**, 673 (2005).

[2] P. Hayden, Tutorial QIP Singapore (2011).

[3] M. Horodecki, J. Oppenheim, and A. Winter, Commun. Math. Phys. **269**, 107 (2007).

[4] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, Proc. R. Soc. A **465**, 2537 (2009).

[5] Z. Luo and I. Devetak, IEEE Trans. Inf. Theory **55**, 1331 (20109).

[6] J. T. Yard and I. Devetak, IEEE Trans. Inf. Theory **55**, 5339 (2009).

[7] I. Devetak and J. Yard, Phys. Rev. Lett. **100**, 230501 (2008).

[8] P. Hayden, M. Horodecki, A. Winter, and J. Yard, Open Systems and Information Dynamics **15**, 7 (2008).

[9] F. Dupuis, *The Decoupling Approach to Quantum Information Theory*, Ph.D. thesis, Université de Montréal (2009).

[10] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter, IEEE Trans. Inf. Theory **60**, 2926 (2014).

[11] M. Berta, M. Christandl, and R. Renner, Commun. Math. Phys. **306**, 579 (2011).

[12] M. Berta, O. Fawzi, and S. Wehner, IEEE Trans. Inf. Theory **60**, 1168 (2014).

[13] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, Commun. Math. Phys. **328**, 251 (2014).

[14] L. del Rio, J. Åberg, R. Renner, O. Dahlsten, and V. Vedral, Nature **474**, 61 (2011).

[15] J. Aberg, Nat. Commun. **4**, 1925 (2013).

[16] A. Hutter, *Understanding Thermalization from Decoupling*, Master's thesis, ETH Zurich (2011).

[17] P. Hayden and J. Preskill, J. High Energy Phys. **07**, 120 (2007).

[18] S. L. Braunstein, S. Pirandola, and K. Zyczkowski, Phys. Rev. Lett. **110**, 101301 (2013).

[19] S. L. Braunstein and A. K. Pati, Phys. Rev. Lett. **98**, 080502 (2007).

[20] F. G. Brandão and M. Horodecki, Nat. Phys. **9**, 721 (2013).

[21] M. Tomamichel, *Quantum Information Processing with Finite Resources — Mathematical Foundations* (Springer International Publishing, 2016).

[22] More precisely, this minimum is taken over subnormalized states, see supplemental material, which includes Refs. [45–51].

[23] N. Ciganovic, N. J. Beaudry, and R. Renner, IEEE Trans. Inf. Theory **60**, 1573 (2014).

[24] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004).

[25] Note that $I^{\varepsilon}_{\max}(E;A)$ and $R^{\varepsilon}(A;E)$ are a priori not symmetric, even though the smooth max-mutual information is approximately (as discussed in Equation (4)). Here the chosen quantity gives the cleanest bounds.

[26] I. Devetak, A. Harrow, and A. Winter, IEEE Trans. Inf. Theory **54**, 4587 (2008).

[27] N. Datta and M.-H. Hsieh, New J. Phys. **13**, 093042 (2011).

[28] L. del Rio, L. Kraemer, and R. Renner, preprint arXiv:1511.08818 (2015).

[29] A more careful discussion of this has to include the fact that a large part of the catalyst can be given back unchanged.

[30] W. van Dam and P. Hayden, Phys. Rev. A **67**, 060302 (2003).

[31] The term $\log\log|A|$ can be improved to be logarithmic in the smooth max-information, when accepting a slightly worse leading order term.

[32] A. Anshu, V. K. Devabathini, and R. Jain, preprint arXiv:1410.3031 (2014).

[33] A partial derandomization can be achieved using (approximate) unitary 2-designs [52].

[34] M. Tomamichel and M. Hayashi, IEEE Trans. Inf. Theory **59**, 7693 (2013).

[35] M. Hayashi and H. Nagaoka, IEEE Trans. Inf. Theory **49**, 1753 (2003).

[36] H. Nagaoka and M. Hayashi, IEEE Trans. Inf. Theory **53**, 534 (2007).

[37] B. Groisman, S. Popescu, and A. Winter, Phys. Rev. A **72**, 032317 (2005).

[38] R. Landauer, IBM J. Res. Dev. **5**, 183 (1961).

[39] Also see [37] for a slightly different notion of catalyticity in this context.

[40] A similar argument can be made for arbitrary mixtures of unitaries with a non-uniform probability distribution.

[41] A. W. Harrow, Proc. XVI Int. Cong. Math. Phys **536** (2009).

[42] A. Uhlmann, Ann. Phys. **497**, 524 (1985).

[43] M. Berta, M. Christandl, and D. Touchette, IEEE Trans. Inf. Theory **62**, 1425 (2016).

[44] N. Datta, M.-H. Hsieh, and J. Oppenheim, preprint arXiv:1409.4352 (2014).

[45] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **56**, 4674 (2010).

[46] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge university press, 2010).

[47] R. Renner, *Security of quantum key distribution*, Phd thesis (2005).

[48] R. Renner and S. Wolf, in *Proceedings of the IEEE International Symposium on Information Theory* (2004) pp. 233–233.

[49] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[50] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, arXiv preprint arXiv:1205.5231 (2012).

[51] H. Umegaki, in *Kodai Mathematical Seminar Reports*, Vol. 14 (Department of Mathematics, Tokyo Institute of Technology, 1962) pp. 59–85.

[52] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner, New J. Phys. **15**, 053022 (2013).