Ann. Henri Poincaré 23 (2022), 3331–3390

1424-0637/22/093331-60
published online April 1, 2022
https://doi.org/10.1007/s00023-022-01175-z

Annales Henri Poincaré

"Interaction-Free" Channel Discrimination

Markus Hasenöhrl and Michael M. Wolf

Abstract. In this work, we investigate the question of which objects can be discriminated by totally "interaction-free" measurements. To this end, we interpret the Elitzur–Vaidman bomb-tester experiment as a quantum channel discrimination problem and generalize the notion of "interaction-free" measurement to arbitrary quantum channels. Our main result is a necessary and sufficient criterion for when it is possible or impossible to discriminate quantum channels in an "interaction-free" manner (i.e., such that the discrimination error probability and the "interaction" probability can be made arbitrarily small). For the case where our condition holds, we devise an explicit protocol with the property that both probabilities approach zero with an increasing number of channel uses, N. More specifically, the "interaction" probability in our protocol decays as $\frac{1}{N}$ and we show that this rate is the optimal achievable one. Furthermore, our protocol only needs at most one ancillary qubit and might thus be implementable in near-term experiments. For the case where our condition does not hold, we prove an inequality that quantifies the trade-off between the error probability and the "interaction" probability.

Contents

1. Introduction

In 1993, Elitzur and Vaidman proposed their famous bomb-tester experiment [1] to demonstrate that the arguably most intriguing property of quantum theory—superposition—can be exploited to detect an ultra-sensitive bomb in a black-box, in such a way that there is a non-vanishing probability that the bomb will not explode. Only two years later, Kwiat et al. [2] showed how to employ another fundamental phenomenon—the quantum Zeno effect [3]—to boost the probability that the bomb will not explode as close to 1 as one pleases. These powerful ideas found applications in "interaction-free" imaging [4,5], counterfactual quantum computation [6,7], counterfactual communication [8] and cryptography [9], and even complexity theory [10]. Despite the great success, it became apparent that the aforementioned techniques, which we will generically call "interaction-free" measurements, are subject to some fundamental limitations. Notably, it is impossible to learn the outcome of a decision problem solved by a quantum computer [7] without "running" the computer in at least one of the two cases, and two optically semi-transparent objects cannot be discriminated in such a way that no photon gets absorbed [11,12].

Despite the results mentioned above, there seems to be no framework and analysis sufficiently general to pinpoint which objects can or cannot be discriminated perfectly by "interaction-free" measurements. Encouraged by recent results that generalize the quantum Zeno effect [13–16], we aim to remedy these shortcomings. To this end, we interpret the Elitzur–Vaidman bomb-tester experiment as a quantum channel discrimination problem and generalize the notion of "interaction-free" measurement to quantum channels via two slightly different, but in the end largely equivalent models. The theory of quantum supermaps [17] then provides the right framework to consider all possible (causally ordered) discrimination strategies, allowing us to decide when it is possible or impossible to discriminate two channels in an "interaction-free" manner.

Organization of the Paper This article is structured as follows: In the remainder of this section, we review the bomb-tester experiment in its versions by Elitzur and Vaidman and by Kwait et al. We also try to convey the idea of how the general model should look. Armed with this rough understanding, we will be able to state and discuss the major results of this work in Sect. 2. In

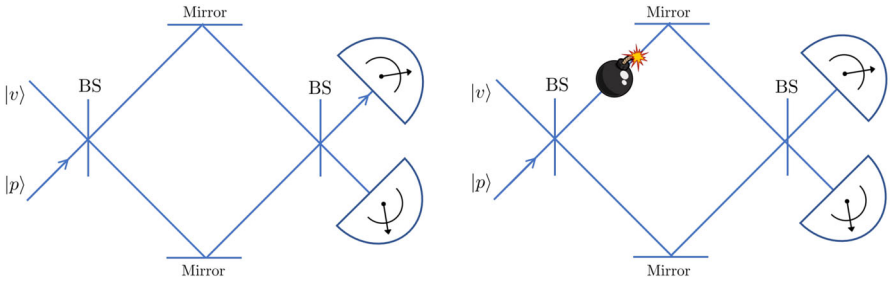

FIGURE 1. Elitzur–Vaidman bomb-tester experiment

Sect. 3, we give a detailed derivation of our model. Our main result, a characterization of what is possible and impossible to do with "interaction-free" measurements, is the combination of two pillars: a no-go theorem, in the form of an inequality, that tells us when it is impossible to discriminate two channels in an "interaction-free" manner; and a protocol that discriminates two channels in those cases that are not touched by the no-go theorem. A quantitative treatment of this protocol is given in Sect. 4, while the main content of Sect. 5 is the no-go theorem. Also in Sect. 5, we prove fundamental limits for the achievable decay rate of the "interaction" probability.

The Bomb-Tester Experiment In the following, we briefly review the bomb-tester experiment in its original version by Elitzur and Vaidman and its iterative version by Kwiat et al. Suppose you have a box and you have been told that inside of this box there is an ultra-sensitive bomb. By ultra-sensitive, we mean that the bomb will explode even if only one photon hits it. As you do not trust the deliverer, you want to check if there is a bomb inside the box. For some reason, the only way to obtain information about the content of the box is by shining light through it. Doing so, however, might trigger the bomb, which is what we want to avoid. If photons were classical particles our task seems to be an impossible one.[1] To circumvent this problem, Elizur and Vaidman proposed to put the box into the upper arm of a Mach–Zehnder interferometer, as depicted in Fig. 1. If we work only with a single photon, then this proposal can be stated abstractly as follows: The Hilbert space of the problem is $\mathcal{H} = \mathcal{H}_U \otimes \mathcal{H}_L$, where $\mathcal{H}_U = \mathcal{H}_L = \operatorname{span}\{v, p\}$ are the Hilbert spaces associated with the upper and lower arm, and the orthogonal unit vectors v and p denote the vacuum and one-photon states, respectively. The 50/50 beamsplitter (BS) can be modeled as a unitary transformation U, defined by

$$\begin{aligned} Uv \otimes v &= v \otimes v, \\ Up \otimes v &= \cos(\theta)\, v \otimes p + \sin(\theta)\, p \otimes v, \\ Uv \otimes p &= -\sin(\theta)\, v \otimes p + \cos(\theta)\, p \otimes v, \end{aligned} \tag{1.1}$$

[1] Note that one needs to be careful about the notion of classicality, since the bomb-tester experiment allows for a formulation in terms of Spekkens toy models [18,19].

where $\theta = 45°$. Suppose we start with a photon in the lower input, then the initial state is $s_0 := |v \otimes p\rangle\langle v \otimes p|$. There are two cases to analyze. On the one hand, if there is no bomb in the box, then the two beamsplitters rotate the state by 90°. Hence, the photon ends up in the upper output. On the other hand, if there is a bomb in the box, then the bomb acts as a measurement device in the upper path. There are three possible outcomes of the experiment. The first possibility is that the photon takes the upper path and thus causes the bomb to explode. This happens with a probability of 50%. If the bomb does not explode, then, by the measurement postulate, the state of the system is still s_0. Since the second beamsplitter has a 50/50 splitting ratio, the probability that we measure the photon in the upper output equals the probability that we measure the photon in the lower output, i.e., the probability for each of them is 25%. The important point here is that in 25% of the cases the photon ends up in the lower path. In that case, we can conclude that there is a bomb in the box, but the bomb has not been triggered. However, we only get this result in 25% of the cases.

Kwiat et al.'s Iterative Version To increase the efficiency of this protocol, the crucial idea is to feed the output back to the input, (thus, to let the photon go through the box many times) and to adjust the splitting ratio of the beamsplitters sensibly (see [2] for the experimental realization). The easiest way to analyze this proposal is to think of the feedback loop in a "rolled out" way. That is, we look at this proposal as if we had N copies of the Mach–Zehnder interferometer (where N is the number of times we let the photon go through the box), in each of which the box is in the upper arm (see Fig. 2).

We further choose the angle $\theta := \frac{90°}{N}$ in (1.1), which defines the action of the beamsplitters. Let us analyze this protocol: If there is no bomb in the box and the photon starts in the lower path, then the photon travels through N beamsplitters, each of which rotates the state by an angle of $\frac{90°}{N}$. So overall the state is rotated by 90°, which means that the photon will be in the upper output. For the case where there is a bomb in the box, let us calculate the probability that the photon always takes the lower path and therefore does not hit the bomb. For each of the beamsplitters, if the photon is in the lower path before the beamsplitter, then the probability that the photon will be in the lower path after the beamsplitter is given by $\cos^2(\theta)$. Since the bomb can be viewed as a measurement device, the probability that the photon always takes the lower path is simply the product of the probabilities at each beamsplitter. Hence, $P(\text{always lower path}) = \cos^{2N}(\theta)$. For $N \to \infty$, we have

$$\cos^{2N}(\theta) = \left(1 - \frac{\pi^2}{8N^2} + \mathcal{O}(N^{-4})\right)^{2N} = 1 - \frac{\pi^2}{4N} + \mathcal{O}(N^{-2}) \xrightarrow{N\to\infty} 1.$$

This simple calculation has the remarkable consequence that (when N is large enough) the photon will always end up in the lower path and the bomb will not explode. Since the photon will always end up in the upper path if there is no bomb in the box, this protocol enables us to tell (with probability approaching 1) whether there is a bomb in the box, while simultaneously ensuring that the bomb will not be triggered.

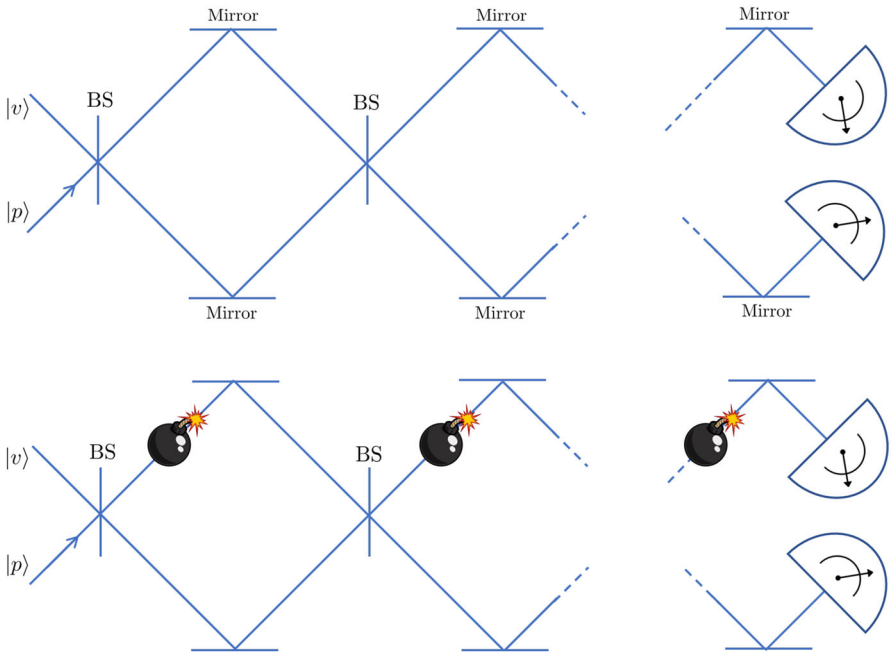

FIGURE 2. Kwiat et al.'s version of the bomb-tester experiment

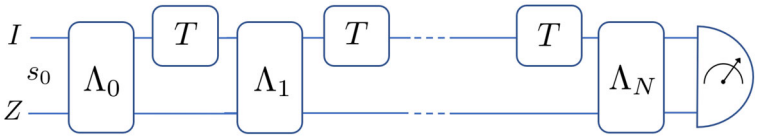

FIGURE 3. N-step discrimination strategy

Interpretation as a Channel Discrimination Problem We have seen in the previous paragraph how to discriminate between a completely transparent object (empty box) and an opaque object (bomb) such that the probability that a photon gets absorbed by the opaque object can be made as small as one pleases. This problem can be reinterpreted as a channel discrimination problem as follows: The channel corresponding to the transparent object is simply the identity channel ($T_{\text{empty}} := \text{id}$), while the action of the opaque object can be identified with the channel[2] $T_{\text{bomb}} : \mathcal{B}_1(\mathcal{H}_U) \to \mathcal{B}_1(\mathcal{H}_U)$, defined by

$$T_{\text{bomb}}(\cdot) = \text{tr}\,[\cdot]\,|v\rangle\langle v|.$$

[2] $\mathcal{B}_1(\mathcal{H})$ denotes the set of traceclass operators on the Hilbert space $\mathcal{H}$ and $\mathcal{S}(\mathcal{H})$ denotes the set of density operators.

According to the theory of quantum combs,[3] the most general (causally ordered) strategy to discriminate channels is given by the sequential scheme, depicted in Fig. 3. That is, if the channels to be discriminated act on the system I (I for interaction), then the most general discrimination strategy[4] allowed by quantum theory can be described as follows: First, we choose an ancillary system Z (which might be arbitrarily large) and an initial state $s_0 \in \mathcal{S}(\mathcal{H}_I \otimes \mathcal{H}_Z)$. Then, we can apply a channel[5] $\Lambda_0 : \mathcal{B}_1(\mathcal{H}_I \otimes \mathcal{H}_Z) \to \mathcal{B}_1(\mathcal{H}_I \otimes \mathcal{H}_Z)$ to s_0. Afterwards, the unknown channel is applied to the system (i.e., if $T : \mathcal{B}_1(\mathcal{H}_I) \to \mathcal{B}_1(\mathcal{H}_I)$ is the unknown channel, then its application transforms the state $\Lambda_0(s_0)$ to $(T \otimes \mathrm{id})(\Lambda_0(s_0)))$. Then, we can transform the system by applying a channel $\Lambda_1 : \mathcal{B}_1(\mathcal{H}_I \otimes \mathcal{H}_Z) \to \mathcal{B}_1(\mathcal{H}_I \otimes \mathcal{H}_Z)$. Afterwards, we apply the unknown channel again, followed by an application of a channel $\Lambda_2 : \mathcal{B}_1(\mathcal{H}_I \otimes \mathcal{H}_Z) \to \mathcal{B}_1(\mathcal{H}_I \otimes \mathcal{H}_Z)$. We repeat this process N times overall. In the end, our system is in a state $\rho_N^T \in \mathcal{S}(\mathcal{H}_I \otimes \mathcal{H}_Z)$, which depends on T. Hence, by measuring we can obtain information about the identity of T. Kwiat et al.'s protocol can be integrated in this formalism as follows: We identify the upper path with the system I and the lower path with the system Z and choose $s_0 := |v \otimes p\rangle\langle v \otimes p|$. For $0 \leq i \leq N-1$, the channels Λ_i are defined by $\Lambda_i(\cdot) := U \cdot U^\dagger =: \hat{U}(\cdot)$, with $\theta = \frac{90^\circ}{N}$ and we set $\Lambda_N := \mathrm{id}$. It is then easy to calculate that

$$\begin{aligned} \rho_N^{T_{\mathrm{empty}}} &= \hat{U}^N(|v \otimes p\rangle\langle v \otimes p|) = |p \otimes v\rangle\langle p \otimes v|, \\ \rho_N^{T_{\mathrm{bomb}}} &= \Big((T_{\mathrm{bomb}} \otimes \mathrm{id}) \circ \hat{U}\Big)^N (|v \otimes p\rangle\langle v \otimes p|) \\ &= \cos^{2N}(\theta)|v \otimes p\rangle\langle v \otimes p| + (1 - \cos^{2N}(\theta))|p \otimes v\rangle\langle v \otimes v|, \end{aligned} \tag{1.2}$$

where $\rho_N^{T_{\mathrm{empty}}}$ and $\rho_N^{T_{\mathrm{bomb}}}$ denote the output states of the protocol when the unknown channel is T_{empty} or T_{bomb}. An interesting aspect of the expressions (1.2) is that one can read off the results of the last paragraph, since the states are orthogonal and since the probability that the bomb explodes is simply given by the coefficient of $|v \otimes v\rangle\langle v \otimes v|$. To abstract from the bomb-tester experiment, we want to allow for arbitrary quantum channels and for arbitrary discrimination strategies (Fig. 3). In this more general setting, the concept of the output state does not change. What is not a priori clear is what it means that something was "interaction-free". Since we want to allow for arbitrary strategies (for example, involving many photons in arbitrary superpositions), the output state does not, in general, contain the information if an interaction occurred. Therefore, we need to model separately what "interaction-free" means for general discrimination strategies. A derivation of such a model based on some axioms takes some effort. We will, therefore, postpone this discussion until Sect. 3. For now, let us just describe the essential constituents. First, for the notion of "interaction-free" to have any meaning, there needs to be some

[3] Quantum combs: also known as quantum supermaps, quantum strategies, ...

[4] This includes in particular coherent evolution, the use of entanglement, measurements, adaptive strategies, channels used in parallel, ...

[5] Of course, the application of Λ_0 is redundant, since one could choose s_0 differently. Allowing to apply Λ_0, however, will simplify the notation.

way not to interact with the object in the box. We will thus assume, in analogy to the bomb-tester experiment, the existence of a *vacuum state*. That is, we assume that for the channels under consideration, there exists a pure state $|v\rangle\langle v| \in \mathcal{S}(\mathcal{H}_I)$ such that $|v\rangle\langle v|$ gets mapped to a pure state by the channel and that if the channel is applied to $|v\rangle\langle v|$, then there is no "interaction" with the object in the box. This concept is formalized by the notion of a channel with vacuum.

Definition 1.1 (*Channel with vacuum*). A channel with vacuum $v \in \mathcal{H}$ is a channel $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ together with a unit vector $v \in \mathcal{H}$ such that $T(|v\rangle\langle v|)$ is pure. The unit vector v is called the *vacuum*, and the state $|v\rangle\langle v| \in \mathcal{S}(\mathcal{H})$ is called the vacuum state.

The notion of an object in the box already suggests that we should look at the given channel in the open system picture. To this end, we imagine a Demon sitting in the box and trying to figure out if something else than the vacuum was sent through the box. To do so, we allow the Demon to access the object in the box. In more mathematical terms, the Demon has full access to the output of the conjugate channel [20]. An important implicit assumption underlying the discussion above is that the channels we look at can be applied several times (which means that the channel does not change)—a Markovianity assumption. Given just this Markovianity assumption, it is possible to determine the probability that, for a certain discrimination strategy, the Demon will find out if at any point during the execution of the strategy, the channel was applied to something else than the vacuum state. We will call this probability the *"interaction" probability* (see Definition 3.3), denoted by $P_I^T(D)$, where T denotes the channel and D the discrimination strategy. The central notion of *discrimination in an "interaction-free" manner*, as formalized in Definition 3.4, is then defined by demanding that the discrimination error probability as well as the "interaction" probability can be made arbitrarily small simultaneously. We finish this section by formalizing the notion of a discrimination strategy[6] and by fixing the notation.

Definition 1.2 (*Discrimination strategy*). An N-step discrimination strategy is a tuple $(\mathcal{H}, \mathcal{H}_Z, \mathcal{H}_i, \mathcal{H}_o, s_0, \Lambda)$, where $\mathcal{H}$, $\mathcal{H}_Z$, $\mathcal{H}_i$, and $\mathcal{H}_o$ are Hilbert spaces, $s_0 \in \mathcal{S}(\mathcal{H}_i)$ is the initial state and $\Lambda := \{\Lambda_0, \Lambda_1, \ldots, \Lambda_N\}$ is a set of channels, with $\Lambda_0 : \mathcal{B}_1(\mathcal{H}_i) \to \mathcal{B}_1(\mathcal{H} \otimes \mathcal{H}_Z)$, $\Lambda_n : \mathcal{B}_1(\mathcal{H} \otimes \mathcal{H}_Z) \to \mathcal{B}_1(\mathcal{H} \otimes \mathcal{H}_Z)$ for $1 \leq n \leq N-1$, and $\Lambda_N : \mathcal{B}_1(\mathcal{H} \otimes \mathcal{H}_Z) \to \mathcal{B}_1(H_o)$.
An N-step discrimination strategy induces the *intermediate state map* $\rho : \mathcal{B}(\mathcal{B}_1(\mathcal{H})) \times \{0, 1, 2, \ldots, N\} \to \mathcal{B}_1(\mathcal{H} \otimes \mathcal{H}_Z) \cup \mathcal{B}_1(\mathcal{H}_o)$, defined by

$$\begin{aligned} \rho(T, 0) &= \Lambda_0(s_0), \\ \rho(T, n) &= \Lambda_n \circ (T \otimes \mathrm{id}) \circ \rho(T, n-1), \text{ for } 1 \leq n \leq N. \end{aligned} \tag{1.3}$$

We will always write[7] ρ_n^T for $\rho(T, n)$ and omit $\mathcal{H}_i$ and $\mathcal{H}_o$ if $\mathcal{H}_i = \mathcal{H}_o = \mathcal{H} \otimes \mathcal{H}_Z$.

[6] Note that in this definition, we allow the input and output spaces to be different from $\mathcal{H} \otimes \mathcal{H}_Z$. This is solely for notational flexibility and has no physical significance.
[7] The superscript should not be confused with the transpose.

Notation Throughout, $\mathcal{H}$ (with some subscript) denotes a separable complex Hilbert space and in this paragraph, $\mathcal{X}$ and $\mathcal{Y}$ are Banach spaces. The range of a map $f : \mathcal{X} \to \mathcal{Y}$ is denoted by $\mathrm{ran}(f) := \{f(x) \,|\, x \in \mathcal{X}\}$. The kernel of f is $\ker(f) := \{x \in \mathcal{X} \,|\, f(x) = 0\}$. The dual space $\mathcal{X}^*$ of $\mathcal{X}$ is the set of bounded linear functionals on $\mathcal{X}$. The orthogonal complement of a linear subspace $\mathcal{V} \subseteq \mathcal{H}$ is denoted by $\mathcal{V}^\perp$. The open ϵ-ball around $x_0 \in \mathcal{X}$ is defined by $B_\epsilon(x_0) := \{x \in \mathcal{X} \,|\, \|x - x_0\| < \epsilon\}$ and the closed δ-disc around $z_0 \in \mathbb{C}$ is denoted by $\mathbb{D}_\delta(z_0) := \{z \in \mathbb{C} \,|\, |z - z_0| \leq \delta\}$.

The Banach space of bounded linear operators $\mathcal{X} \to \mathcal{X}$ is denoted by $\mathcal{B}(\mathcal{X})$. The space of trace-class operators $\mathcal{B}_1(\mathcal{H})$ becomes a Banach space with trace-norm $\|\cdot\|_1 := \mathrm{tr}\,[|\cdot|]$. For $A \in \mathcal{B}(\mathcal{H})$, the adjoint is denoted by $A^\dagger$ and the support of A is defined by $\mathrm{supp}(A) := \ker(A)^\perp$. If $A^\dagger = A$, then A is called self-adjoint. A is called positive semi-definite, sometimes denoted by $A \geq 0$, if A is self-adjoint and $\langle\psi|A\psi\rangle \geq 0$ for all $\psi \in \mathcal{H}$. For a closed subspace $\mathcal{V} \subseteq \mathcal{H}$, we denote (in a slight abuse of notation) by $\mathcal{B}(\mathcal{V}) \subseteq \mathcal{B}(\mathcal{H})$ the bounded linear operators with range and support in $\mathcal{V}$ and by $\mathcal{B}_1(\mathcal{V})$ the trace-class operators with range and support in $\mathcal{V}$.

A linear operator $T \in \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ is called a quantum operation if it is completely positive and trace non-increasing. If T is in addition trace-preserving, then T is called a (quantum) channel. If a quantum channel T is written in the form $T(\cdot) = \mathrm{tr}_E\left[V \cdot V^\dagger\right]$, where $V : \mathcal{H} \to \mathcal{H}_E \otimes \mathcal{H}$ is an isometry and where tr_E is the partial trace, then V is called a Stinespring isometry. The set of (quantum) states on $\mathcal{H}$ is given by $\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{B}_1(\mathcal{H}) \,|\, \rho \geq 0, \mathrm{tr}\,[\rho] = 1\}$. The identity channel is denoted by id and the unit matrix by $\mathbb{1}$. For positive semi-definite trace-class operators ρ and σ, the fidelity is defined by $\sqrt{F}(\rho, \sigma) := \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1$.

For $B \in \mathcal{B}(\mathcal{X})$, the resolvent set is $\rho(B) := \{z \in \mathbb{C} \,|\, z - B \text{ is invertible}\}$ and the spectrum is $\sigma(B) := \mathbb{C} \setminus \rho(B)$. The discrete spectrum of B is the subset of isolated points of $\sigma(B)$ such that the corresponding Riesz projection has finite rank.

2. Results

To state and discuss our main results, we need one more concept, which is similar to that of a decoherence-free subspace.[8]

Definition 2.1 (*Isometric subspace*). Let $\mathcal{V}$ be a closed linear subspace of a Hilbert space $\mathcal{H}$. A channel $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ is said to be *isometric on* $\mathcal{V}$ if there exists an isometry $V : \mathcal{V} \to \mathcal{H}$, such that[9]

$$T|_{\mathcal{B}_1(\mathcal{V})}(\cdot) = V \cdot V^\dagger. \tag{2.1}$$

If T is isometric on $\mathcal{V}$, we call $\mathcal{V}$ an *isometric subspace* w.r.t. T.

[8] An isometric subspace is a decoherence-free subspace if the range of the isometry is $\mathcal{V}$.

[9] $T|_{\mathcal{B}_1(\mathcal{V})}$ denotes the restriction of T to the bounded linear operators with range and support in $\mathcal{V}$.

The significance of channels that are isometric on $\mathcal{V}$ is that they are the analogue to the identity channel in the bomb-tester case. To see why, note that $T|_{\mathcal{B}_1(\mathcal{V})}$ satisfies the Knill–Laflamme error-correcting conditions [21]. Hence, by composing $T|_{\mathcal{B}_1(\mathcal{V})}$ with an appropriate channel, we obtain the identity channel on $\mathcal{B}_1(\mathcal{V})$. Furthermore, as Lemma 3.10 proves in a language adapted to our model, the output of the conjugate channel of T will be the same for all $\rho \in \mathcal{B}_1(\mathcal{V})$. In particular, if we have $v \in \mathcal{V}$, where v is the vacuum, then even though $\rho \in \mathcal{B}_1(\mathcal{V})$ might be different from $|v\rangle\langle v|$, the Demon (having access to the conjugate channel only) has no chance of telling that something other than the vacuum has been sent through the box.

We are now ready to state our main result, which is an easy to check necessary and sufficient criterion that tells us when it is possible (or impossible) to discriminate two quantum channels in an "interaction-free" manner.

Theorem 2.2 (Main result). *Let* $\dim(\mathcal{H}) < \infty$. *Two channels* $T_A, T_B : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *with vacuum* $v \in \mathcal{H}$ *can be discriminated in an "interaction-free" manner if and only if there exists a subspace* $\mathcal{V} \subseteq \mathcal{H}$ *with the following three properties:*

1. $v \in \mathcal{V}$.
2. *At least one of the two channels is isometric on* $\mathcal{V}$.
3. $T_A|_{\mathcal{B}(\mathcal{V})} \neq T_B|_{\mathcal{B}(\mathcal{V})}$.

Note that the central notion "discrimination in an 'interaction-free' manner" has only been defined informally in the paragraph following Definition 1.1. The formal definition, as well as the one for the "interaction" probability, can be found in Sect. 3.3, after a derivation of the mathematical form of these quantities from first principles in Sect. 3.1.

Remark 2.3. At first glance it may seem to be hard to check whether such a subspace exists. This is not so, as one only needs to consider two candidates for $\mathcal{V}$, the so-called maximal vacuum subspaces $\mathcal{V}_{T_A}$ and $\mathcal{V}_{T_B}$, which we define and study in 3.9 and 3.10.

Theorem 2.2 is a direct consequence of two results: a protocol to discriminate two channels and a no-go theorem. We discuss these cases separately in the following two subsections.

2.1. The Constructive Case

We consider the case where our main theorem says that we can discriminate the two channels in an "interaction-free" manner. That is, where there is a subspace $\mathcal{V}$, such that $\mathcal{V}$ contains the vacuum and one of the two channels is isometric on $\mathcal{V}$ and $T_A|_{\mathcal{B}(\mathcal{V})} \neq T_B|_{\mathcal{B}(\mathcal{V})}$. For this case, we propose a protocol (see Sect. 4) that can discriminate two channels in an "interaction-free" manner. We will discuss the properties of this protocol in the following. It turns out that one does not need complete information about the two channels to perform the discrimination task. To account for this, we consider the more general task, where we want to know to which one of two known, disjoint, sets of channels the unknown channel belongs. Of course, Theorem 2.2 puts some restrictions

on how these sets may look like. Specifically, we consider the following: Given a channel T with vacuum $v \in \mathcal{V}$ that is isometric on $\mathcal{V}$, we take as our first set (a subset of) the set of channels that equal T if we restrict their domains to $\mathcal{B}_1(\mathcal{V})$. The second set is less restricted in that we only assume that all channels must be channels with (the same) vacuum v and that the restrictions to $\mathcal{B}_1(\mathcal{V})$ must not equal $T|_{\mathcal{B}_1(\mathcal{V})}$. It will then turn out that under these conditions, these two sets can be discriminated in an "interaction-free" manner. Roughly speaking, this tells us that we can test whether the unknown channel is T or some other channel, whose identity is unknown. Putting it yet another way, if the identity channel is interpreted as an empty box and every other channel as a non-empty box, then our result says that one can always find out (in an "interaction-free" manner) if there is something or nothing in the box. Before we state this in mathematical terms, we need to define the *discrimination error probability* for two sets.

Definition 2.4 (*Error probability*). Let $\mathcal{C}_A, \mathcal{C}_B \subseteq \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ be two sets of channels. For an N-step discrimination strategy D and a two-valued POVM $\Pi = \{\pi_A, \pi_B\}$, the *discrimination error probability* is defined by

$$P_e(D,\Pi) := \frac{1}{2}\left[\sup_{T\in\mathcal{C}_A} \operatorname{tr}\left[\pi_B \rho_N^T\right] + \sup_{T\in\mathcal{C}_B} \operatorname{tr}\left[\pi_A \rho_N^T\right]\right]. \tag{2.2}$$

Theorem 2.5 (Discrimination strategy). *For* $\dim(\mathcal{H}) < \infty$*, let* $\mathcal{C}_A, \mathcal{C}_B \subseteq \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ *be two closed sets of channels and* $\mathcal{V}$ *be a subspace of* $\mathcal{H}$*, such that*

1. *For all* $T \in \mathcal{C}_A \cup \mathcal{C}_B$*,* T *is a channel with vacuum* $v \in \mathcal{V}$*.*
2. *For all* $T \in \mathcal{C}_A$*,* T *is isometric on* $\mathcal{V}$*.*
3. *The set* $\mathcal{C}_A|_{\mathcal{B}_1(\mathcal{V})} := \left\{T|_{\mathcal{B}_1(\mathcal{V})} \,\middle|\, T \in \mathcal{C}_A\right\}$ *contains exactly one element.*
4. $\mathcal{C}_A|_{\mathcal{B}_1(\mathcal{V})}$ *and* $\mathcal{C}_B|_{\mathcal{B}_1(\mathcal{V})} := \left\{T|_{\mathcal{B}_1(\mathcal{V})} \,\middle|\, T \in \mathcal{C}_B\right\}$ *are disjoint.*

Then there exist a constant C*, and for every* $N \in \mathbb{N}$*, an* N*-step discrimination strategy* D *and a two-valued POVM* Π*, such that*

$$P_e(D,\Pi) \leq \frac{C}{N^2}, \tag{2.3}$$

$$P_I^{T_A}(D) = 0 \quad \text{and} \quad P_I^{T_B}(D) \leq \frac{C}{N}, \tag{2.4}$$

for all $T_A \in \mathcal{C}_A$ *and all* $T_B \in \mathcal{C}_B$*, where* P_I *denotes the "interaction" probability. Thus, the sets* $\mathcal{C}_A$ *and* $\mathcal{C}_B$ *can be discriminated in an "interaction-free" manner.*

Remark 2.6. The strategy we propose that has the properties stated in Theorem 2.5 only requires one ancillary qubit system in the worst-case scenario (as does the Kwiat et al. protocol) and might thus be implementable in the near future. We also show that one cannot get rid of the ancillary qubit in a naive way.

Remark 2.7. Although Theorem 2.5 is formulated for finite-dimensional spaces, a key part of the proof works also in infinite-dimensional spaces (Theorems 4.5 and 4.6).

Remark 2.8. For two channels T_A and T_B with vacuum $v \in \mathcal{H}$, we can define the sets $\mathcal{C}_A := \{T_A\}$ and $\mathcal{C}_B := \{T_B\}$. If there is a subspace $\mathcal{V}$ such that the Conditions 1-3 in the main theorem are fulfilled (and, w.l.o.g, T_A is isometric on $\mathcal{V}$), then clearly $\mathcal{C}_A$ and $\mathcal{C}_B$ satisfy the hypothesis of Theorem 2.5 and thus T_A and T_B can be discriminated in an "interaction-free" manner. This proves the direct part of Theorem 2.2.

Given the result of Theorem 2.5, it is natural to ask whether the bounds on the error probability and the "interaction" probability have the optimal dependence on N. This is clearly not the case for the error probability, as is already evident from the bomb-tester experiment. For the "interaction" probability, we were able to show (under a mild condition on $\mathcal{C}_A$ and $\mathcal{C}_B$) that N^{-1} is indeed the best possible rate. We state this as a meta theorem (see Theorem 5.9).

Theorem. *Subject to a condition stated in Theorem 5.9, there exists a constant* $C > 0$ *such that*

$$\max(P_I^{T_A}(D), P_I^{T_B}(D)) \geq C \frac{(1 - 2P_e(D, \Pi))^4}{N}, \tag{2.5}$$

for all N*-step discrimination strategies* D *and all two-valued POVM's* Π.

The result above cannot hold unconditionally. If there is a subspace $\mathcal{V}$ such that $v \in \mathcal{V}$, and *both* channels are isometric on $\mathcal{V}$ and $T_A|_{\mathcal{B}(\mathcal{V})} \neq T_B|_{\mathcal{B}(\mathcal{V})}$, then we can restrict ourselves to probing the channel only with states in $\rho \in \mathcal{B}_1(\mathcal{V})$. Since the Demon cannot tell the difference between these states, the "interaction" probability is zero and the remaining problem is to discriminate two isometric channels. This problem can be solved with discrimination error probability equal to zero, in a finite number of steps [22]. We were unable to show that the case described above is the only one where the N^{-1}-rule can be violated, but this seems plausible.

2.2. The No-Go Case

In this section, we consider the case for which our main theorem tells us that "interaction-free" channel discrimination is impossible; that is, if there exists no subspace satisfying all three properties of Theorem 2.2. In this case the channels T_A and T_B must be such that whenever there is a subspace $\mathcal{V}$ that contains the vacuum and on which at least one of the two channels is isometric, then the two channels must necessarily be the same on that subspace.[10] In this case, we were able to establish the following theorem that shows that there is a trade-off between the error probability and the "interaction" probability, in the sense that not both of them can go to zero simultaneously.

[10] Unfortunately, this case seems to be the generic case. Indeed, on physical grounds (think of two semi-transparent objects) it is reasonable to assume that for both channels, the only isometric subspace that contains the vacuum is simply span$\{v\}$ and that $|v\rangle\langle v|$ is a fixed point.

Theorem 2.9 (No-go theorem). *For* $\dim(\mathcal{H}) < \infty$, *let* $T_A, T_B : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *be two channels with vacuum* $v \in \mathcal{H}$. *Suppose that no subspace satisfies the properties 1, 2, and 3 of Theorem 2.2 simultaneously.*

Then, there exists a constant $C > 0$, *such that*

$$(1 - 2P_e(D, \Pi))^2 \leq C \max(P_I^{T_A}(D), P_I^{T_B}(D)), \tag{2.6}$$

for all finite-dimensional N*-step discrimination strategies* D *and all two-valued POVMs,* Π. *Hence,* T_A *and* T_B *cannot be discriminated in an "interaction-free" manner.*

Clearly, this implies the converse in Theorem 2.2.

As a by-product, we obtained an inequality for the fidelity, which might be of independent interest.

Proposition 2.10. *For* $\dim(\mathcal{H}) < \infty$, *let* $T_A^{\downarrow}, T_B^{\downarrow} : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *be quantum operations and let* $\mathcal{V}$ *be a subspace of* $\mathcal{H}$ *such that* $T_A^{\downarrow}|_{\mathcal{B}_1(\mathcal{V})} = T_B^{\downarrow}|_{\mathcal{B}_1(\mathcal{V})}$ *and* $T_A^{\downarrow}|_{\mathcal{B}_1(\mathcal{V})}$ *is trace-preserving. Then,*

$$\sqrt{F}(T_A^{\downarrow}(\rho), T_B^{\downarrow}(\sigma)) \geq \sqrt{F}(\rho, \sigma) - 2\sqrt{F}(P^{\perp}\rho P^{\perp}, P^{\perp}\sigma P^{\perp}), \tag{2.7}$$

for all $\rho, \sigma \geq 0$, *where* $P^{\perp}$ *is the orthogonal projection onto* $\mathcal{V}^{\perp}$.

3. The Models

In this section, we propose two different, but in the end largely equivalent models that generalize the notion of "interaction-free" measurement to quantum channels. Since the sequential scheme, given in Fig. 3, is the most general causally ordered strategy allowed in quantum theory [17], it suffices to define our notions for this kind of strategy. In both models, we assume the validity of Fig. 3. That is, we assume that the unknown channel T does not change during the execution of the discrimination strategy—the Markovianity assumption. This is a relatively weak assumption, since we are in control of the duration between the individual channel invocations. This section consists of four subsections. In the first two subsections, we derive our two models. The third subsection summarizes the former two by properly defining the quantities of merit and thereby setting the stage for a rigorous analysis in the later sections. In the fourth subsection, we compare the two models by deriving some elementary properties, which will be used later on.

3.1. The "Interaction" Model

In our first model, we interpret the term "interaction-free" in an information-theoretic way. That is, we imagine a Demon sitting in the box trying to figure out, if we interacted with the interior of the box. In more technical terms, this means that the Demon has full access to the output of the conjugate channel. Since our task would be trivially infeasible otherwise, there must be a way not to interact with the box. Therefore, we only consider channels with vacuum. That is, we assume that for all channels under consideration there exists a distinguished pure state, the *vacuum state*, $|v\rangle\langle v|$. This state is assumed

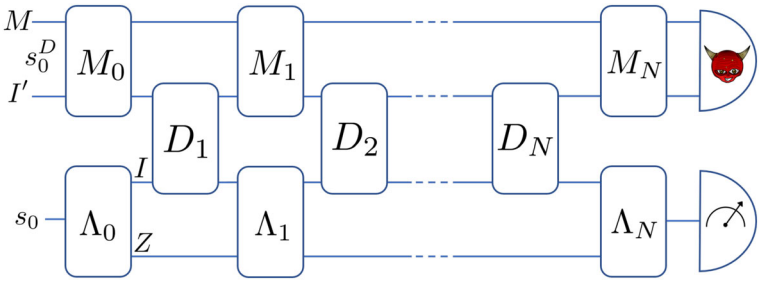

FIGURE 4. General scenario

to have the following two important properties: First, if the vacuum state is sent through the channel, then the Demon concludes that no interaction has occurred. Second, we assume that the channels under consideration map the vacuum state to a pure state. This assumption is physically reasonable as it means that the state of the probe system does not become entangled with the Demon's system. If in contrast, the probe system becomes entangled with the Demon's system, then there must have been an interaction and the term "interaction-free" measurement would be inappropriate. We should mention, however, that the transmission model, which we are going to describe in the next section does not use the ""vacuum maps to pure state"" assumption. This comes at the cost that the transmission functional is no longer a property of a channel (as the "interaction" functional will turn out to be) but rather an object that has to be modeled separately. Together, these two assumptions yield the definition of a channel with vacuum (Definition 1.1). For a given channel T with vacuum $v \in \mathcal{H}_I$ and an N-step discrimination strategy $D = (\mathcal{H}_I, \mathcal{H}_Z, \mathcal{H}_i, \mathcal{H}_o, s_0, \Lambda)$, we want to define the *"interaction" probability* $P_I^T(D)$ as the probability that the Demon in the box encounters that, during the execution of D, something other than the vacuum state was sent through the channel. To define this probability, we need to specify how the Demon can obtain information about what was sent through the channel.

A natural way to model this is by assuming that for each of the N channel-uses (indexed by n) in the discrimination strategy, the Demon is allowed to implement the channel T via a channel $D_n : \mathcal{B}_1(\mathcal{H}_{I'} \otimes \mathcal{H}_I) \to \mathcal{B}_1(\mathcal{H}_{I'} \otimes \mathcal{H}_I)$, where $\mathcal{H}_{I'}$ is the Hilbert space associated with a system I', which the Demon controls. We further allow the Demon to keep an arbitrarily large memory system M (with Hilbert space $\mathcal{H}_M$) which he can manipulate freely (i.e., he can choose the channels M_n, defined below). The most general (causally ordered) scheme that can be obtained from the above description is depicted in Fig. 4. Mathematically, the Demon's strategy is completely determined by an initial state $s_0^D \in \mathcal{S}(\mathcal{H}_M \otimes \mathcal{H}_{I'})$ and channels $M_0, M_1, \ldots, M_N : \mathcal{B}_1(\mathcal{H}_M \otimes \mathcal{H}_{I'}) \to \mathcal{B}_1(\mathcal{H}_M \otimes \mathcal{H}_{I'})$ and $D_1, D_2, \ldots, D_N : \mathcal{B}_1(\mathcal{H}_{I'} \otimes \mathcal{H}_I) \to \mathcal{B}_1(\mathcal{H}_{I'} \otimes \mathcal{H}_I)$. Given this data, the scheme in Fig. 4 produces the output (or final) state $\rho_F \in$

$\mathcal{S}(\mathcal{H}_M \otimes \mathcal{H}_{I'} \otimes \mathcal{H}_o)$, defined by

$$\rho_F := (M_N \otimes \Lambda_N)(\mathrm{id} \otimes D_N \otimes \mathrm{id}) \dots (M_1 \otimes \Lambda_1)(\mathrm{id} \otimes D_1 \otimes \mathrm{id})(M_0 \otimes \Lambda_0)(\chi_0),$$

where $\chi_0 := s_0^D \otimes s_0$. In the end, the Demon will measure his system $(M + I')$ and decide, based on the measurement outcome, if an interaction has occurred. The "interaction" probability is then the probability that he detects such an interaction if he chooses his strategy optimally within the given constraints.

Before we can analyze what the Demon's optimal strategy is, we need to formulate mathematically the assumption that D_n implements T, and that T must be independent of the Demon's strategy (Markovianity). Precisely, we assume that D_n must be such that if the Demon's system (I') and I are uncorrelated, then the action on the system I must be independent of the state of the system I'. In formulas, we assume that

$$\mathrm{tr}_{I'} [D_n(\rho_{I'} \otimes \rho_I)] = T(\rho_I) \tag{3.1}$$

for all $\rho_{I'} \in \mathcal{S}(\mathcal{H}_{I'})$, $\rho_I \in \mathcal{S}(\mathcal{H}_I)$, and $n \in \{1, 2, \dots, N\}$. We note that (3.1) is exactly the definition of a semicausal channel, as introduced in [23]. A structure theorem by Eggeling et al. [24] tells us that semi-causal channels are semi-localizable. That is, D_n can be written in the form:

$$D_n(\rho_{I'I}) = \mathrm{tr}_{E_n} \left[(X_n \otimes \mathrm{id}_I)(\mathrm{id}_{I'} \otimes \hat{V}_n)(\rho_{I'I}) \right],$$

where $\hat{V}_n : \mathcal{B}_1(\mathcal{H}_I) \to \mathcal{B}_1(\mathcal{H}_{E_n} \otimes \mathcal{H}_I)$, defined by $\hat{V}_n(\cdot) = V_n \cdot V_n^\dagger$ is the quantum channel associated with a Stinespring isometry $V_n : \mathcal{H}_I \to \mathcal{H}_{E_n} \otimes \mathcal{H}_I$ of T and $X_n : \mathcal{B}_1(\mathcal{H}_{I'} \otimes \mathcal{H}_{E_n}) \to \mathcal{B}_1(\mathcal{H}_{I'} \otimes \mathcal{H}_{E_n})$ is some channel. To proceed further in our search for the Demon's optimal strategy, we make a few simplifying observations and definitions. First, the unitary freedom in the Stinespring dilation $\hat{V}_n$ can be absorbed into the channel X_i. We can therefore assume, without loss of generality, that $\mathcal{H}_{E_1} = \mathcal{H}_{E_2} = \dots = \mathcal{H}_{E_N} =: \mathcal{H}_E$ and $\hat{V}_1 = \hat{V}_2 = \dots = \hat{V}_N =: \hat{V}$. Second, for $\rho \in \mathcal{S}(\mathcal{H}_M \otimes \mathcal{H}_{I'} \otimes \mathcal{H}_I)$, we have

$$(M_n \otimes \mathrm{id}_I) D_n(\rho) = \mathrm{tr}_{E_n} \left[([(M_n \otimes \mathrm{id}_{E_n})(\mathrm{id}_M \otimes X_n)] \otimes \mathrm{id}_I)(\mathrm{id}_{MI'} \otimes \hat{V}_n)(\rho) \right],$$

which motivates the definition $\underline{X}_n := (M_n \otimes \mathrm{id}_{E_n})(\mathrm{id}_M \otimes X_n)$. In the following, we adopt the convention that if some channel acts trivially on a tensor factor (i.e., as the identity), then we omit these tensor factors in the notation (e.g., $\underline{X}_i \otimes \mathrm{id}_I$ becomes just $\underline{X}_i$). With the newly introduced notation, it follows from the definition of σ_F that the state the Demon obtains is

$$\mathrm{tr}_{IZ} [\rho_F] = \mathrm{tr}_{IZ} \Lambda_N \mathrm{tr}_{E_N} \underline{X}_N \hat{V}_N \Lambda_{N-1} \mathrm{tr}_{E_{N-1}} \underline{X}_{N-1} \dots \Lambda_1 \mathrm{tr}_{E_1} \underline{X}_1 \hat{V}_1 M_0 \Lambda_0(\chi_0).$$

We can commute the $\underline{X}_i$s and tr_{E_i}s to the left. Thus, upon defining the channel $\Gamma : \mathcal{B}_1(\mathcal{H}_{E_N} \otimes \mathcal{H}_{E_{N-1}} \otimes \dots \otimes \mathcal{H}_{E_1}) \to \mathcal{B}_1(\mathcal{H}_M \otimes \mathcal{H}_{I'})$ by

$$\Gamma(\rho) = \mathrm{tr}_{E_N} \underline{X}_N \mathrm{tr}_{E_{N-1}} \underline{X}_{N-1} \dots \mathrm{tr}_{E_1} \underline{X}_1 M_0(s_0^D \otimes \rho),$$

we have

$$\mathrm{tr}_{IZ} [\rho_F] = \Gamma(\mathrm{tr}_{IZ} \Lambda_N \hat{V}_N \Lambda_{N-1} \hat{V}_{N-1} \dots \Lambda_1 \hat{V}_1 \Lambda_0(s_0)).$$

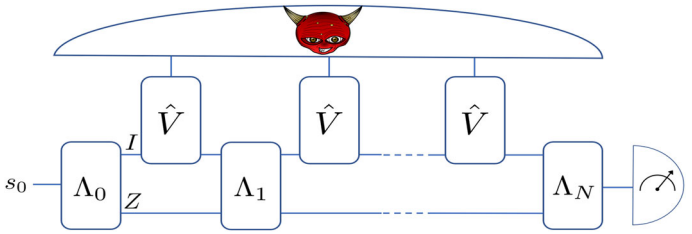

FIGURE 5. Scenario when the Demon's strategy is optimal

To decide if the channel was ever applied to a state different from the vacuum state, the Demon measures his state with a two-valued POVM, $\{Q_1, Q_2\}$. By convention, he will conclude that an interaction occurred (something other than the vacuum was sent through) if the event corresponding to Q_2 occurs. If the state sent through the channel is always the vacuum state, then the Demon's final state is

$$\Gamma(\left[\mathrm{tr}_I\left[V|v\rangle\langle v|V^\dagger\right]\right]^{\otimes N}),$$

where the tensor power is in the space $\mathcal{H}_{E_N} \otimes \mathcal{H}_{E_{N-1}} \otimes \cdots \otimes \mathcal{H}_{E_1}$. Since the Demon must not report an interaction, if the state was always the vacuum state, we demand

$$0 = \mathrm{tr}\left[Q_2\Gamma(\left[\mathrm{tr}_I\left[V|v\rangle\langle v|V^\dagger\right]\right]^{\otimes N})\right] = \mathrm{tr}\left[\Gamma^*(Q_2)\left[\mathrm{tr}_I\left[V|v\rangle\langle v|V^\dagger\right]\right]^{\otimes N}\right],$$

where Γ^* denotes the channel Γ in the Heisenberg picture. Clearly, if $\Gamma^*(Q_2) = \mathbb{1}^{\otimes N} - P_v^{\otimes N}$, where P_v is the orthogonal projection onto the support of $\mathrm{tr}_I\left[V|v\rangle\langle v|V^\dagger\right]$, then this requirement is fulfilled. Since we want to choose the optimal strategy the Demon can pursue, we want to set $\Gamma^*(Q_2) := \mathbb{1}^{\otimes N} - P_v^{\otimes N}$. We can always choose Γ and Q_2 to satisfy the last equation, because this corresponds to the strategy where the Demon simply stores all the states he obtains from the Stinespring dilation in each round. This justifies the graphical representation in Fig. 5. Since we defined the "interaction" probability to be the probability that the Demon concludes that an interaction occurred (if he acts optimally), we have

$$P_I^T(D) := \mathrm{tr}\left[(\mathbb{1}^{\otimes N} - P_v^{\otimes N})\,\mathrm{tr}_{IZ}\hat{V}_N\Lambda_{N-1}\hat{V}_{N-1}\ldots\Lambda_1\hat{V}_1(\rho_0^T)\right], \tag{3.2}$$

where $\rho_0^T := \Lambda_0(s_0)$ is the first intermediate state. We remark that the definition of $P_I^T(D)$ does not depend on the particular choice of the Stinespring dilation, since the unitary freedom in the Stinespring isometries is compensated by the equal and opposite freedom in P_v.

We can simplify this expression a bit. We define $P_v^\perp := \mathbb{1} - P_v$ and note that

$$\mathbb{1}^{\otimes N} - P_v^{\otimes N} = \sum_{n=0}^{N-1} \mathbb{1}^{\otimes N-n-1} \otimes P_v^\perp \otimes P_v^{\otimes n},$$

$$P_v^{\perp} \otimes P_v^{\otimes K} = \prod_{j=0}^{K-1} P_v^{\perp} \otimes \mathbb{1}^{\otimes j} \otimes P_v \otimes \mathbb{1}^{\otimes K-j-1}.$$

Using these two expressions and (several times) that Λ_n is trace-preserving, we obtain our final version for $P_I^T(D)$,

$$\begin{aligned}
P_I^T(D) &= \sum_{n=0}^{N-1} \mathrm{tr}\left[\mathbb{1}^{\otimes N-n-1} \otimes P_v^{\perp} \otimes P_v^{\otimes n}\ \mathrm{tr}_{IZ}\hat{V}_N \Lambda_{N-1}\hat{V}_{N-1}\ldots\Lambda_1\hat{V}_1(\rho_0^T)\right] \\
&= \sum_{n=0}^{N-1} \mathrm{tr}\left[P_v^{\perp} \otimes P_v^{\otimes n}\ \mathrm{tr}_{IZ}\hat{V}_{n+1}\Lambda_n\hat{V}_n\ldots\Lambda_1\hat{V}_1(\rho_0^T)\right] \\
&= \sum_{n=0}^{N-1} \mathrm{tr}\left[P_v^{\perp}\mathrm{tr}_{IZ}(\hat{V}_{n+1}(\Lambda_n(\mathrm{tr}_{E_i}((P_v\otimes\mathbb{1})\hat{V}_n(..\mathrm{tr}_{E_1}((P_v\otimes\mathbb{1})\hat{V}_1(\rho_0^T)..)\right] \\
&= \sum_{n=0}^{N-1} \mathrm{tr}\left[P_v^{\perp}\mathrm{tr}_I\hat{V}(\mathrm{tr}_Z(\Lambda_i T^{\downarrow}\Lambda_{n-1}T^{\downarrow}\ldots\Lambda_1 T^{\downarrow}(\rho_0^T)))\right] \\
&= \sum_{n=0}^{N-1} \mathrm{tr}\left[P_v^{\perp}\mathrm{tr}_I\hat{V}(\mathrm{tr}_Z\left[\rho_n^{T^{\downarrow}}\right])\right].
\end{aligned}$$

In the second to last line, we defined $T^{\downarrow}(\cdot) = \mathrm{tr}_E\left[(P_v\otimes\mathbb{1})V\cdot V^{\dagger}\right]$ and $\rho_n^{T^{\downarrow}}$ is determined by the intermediate state map. We have thus succeeded in our goal to define the "interaction" probability.

Remark 3.1. It is immediate from (3.2) that an alternative expression for $P_I^T(D)$ is given by

$$P_I^T(D) = 1 - \mathrm{tr}\left[\rho_N^{T^{\downarrow}}\right]. \tag{3.3}$$

There are two reasons to prefer the lengthy version derived above. First, it makes the connection between the "interaction" model and the transmission model (defined below) explicit and thus allows us to treat these points of view on an equal footing. Second, it suggests to approach the problem by looking at the inputs of the individual channel uses, which turns out to be fruitful.

3.2. The Transmission Model

In our second model, we think of an interaction as something that does damage to the system in the box. As a guiding example, we think of a biological system—say a body cell. For the sake of argument, assume that we want to use high-energetic radiation (e.g., X-ray) to resolve the inner structure of the cell. Of course, radiation might damage the cell, which is usually undesirable. A reasonable measure for how much damage has been done to a cell seems to be the number of X-ray photons that were absorbed by the cell. In other words, the damage is quantified by the amount of energy that got *transmitted* from the probe system (X-ray) to the interior of the box (biological cell). Furthermore, if the cell is exposed to radiation several times, then the damage measure should be the sum of the number of photons that were absorbed each

time. Let us now abstract away from this example. Assume that the system in the box is modeled quantum mechanically on a Hilbert space $\mathcal{H}_E$ and that the probe system is modeled on $\mathcal{H}_I$. Assume that initially the system E is in the state $\rho_E \in \mathcal{S}(\mathcal{H}_E)$. If we probe the system with a state $\rho_I \in \mathcal{S}(\mathcal{H}_I)$, then the combined evolution is described by a (not necessarily unitary) channel $U : \mathcal{B}_1(\mathcal{H}_E \otimes \mathcal{H}_I) \to \mathcal{B}_1(\mathcal{H}_E \otimes \mathcal{H}_I)$. Thus, the state of the combined system after the evolution is given by

$$\rho'_{EI} = U(\rho_E \otimes \rho_I).$$

Now assume that, in analogy to the number of absorbed photons in the example above, there is some physical quantity (an observable) that got transmitted from the probe system to the interior of the box by the above process, and that this quantity is related to the damage done to the object in the box. We further assume that the process above can only cause damage and cannot repair the system in the box. Thus, the observable must be a positive semi-definite operator Θ on the Hilbert space $\mathcal{H}_E$. Hence, for a single shot experiment, the important object is the positive linear functional $\mathfrak{t} : \mathcal{B}_1(\mathcal{H}_I) \to \mathbb{C}$, defined by

$$\mathfrak{t}(\rho_I) = \operatorname{tr}\left[\Theta \operatorname{tr}_I \left[U(\rho_E \otimes \rho_I)\right]\right].$$

For a general N-step discrimination strategy D (with intermediate state map ρ), we assume that the transmitted quantity is extensive. Since the state of the part of the probe system that interacts with the interior of the box in the nth step is given by $\operatorname{tr}_Z\left[\rho_n^T\right]$ (T is the channel defined by $T(\rho_I) = \operatorname{tr}_E\left[U(\rho_E \otimes \rho_I)\right]$), a good definition for the *total transmission* $\mathfrak{T}_T(D)$ is

$$\mathfrak{T}_T(D) := \sum_{n=0}^{N-1} \mathfrak{t}_T\left(\operatorname{tr}_Z\left[\rho_n^T\right]\right).$$

We raise this to a principle by assuming that for every channel T we have a positive linear functional $\mathfrak{t}_T$, which we call the *transmission functional*, that models the damage done to the object. The total transmission then plays the same role for the transmission model as the "interaction" probability does for the "interaction" model.

3.3. Formal Definition

We cast the principles developed in the last sections into formal definitions.

Definition 3.2 (*"Interaction" functional*). Let $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be a channel with vacuum $v \in \mathcal{H}$ and let $V : \mathcal{H} \to \mathcal{H}_E \otimes \mathcal{H}$ be any Stinespring isometry of T. The positive linear functional $\mathfrak{i}_T : \mathcal{B}_1(\mathcal{H}) \to \mathbb{C}$, defined by

$$\mathfrak{i}_T(\cdot) := \operatorname{tr}\left[P_v^{\perp} \operatorname{tr}_{\mathcal{H}}\left[V \cdot V^{\dagger}\right]\right], \tag{3.4}$$

is called the *"interaction" functional* of T, where $P_v^{\perp}$ is the orthogonal projection onto the kernel of $\operatorname{tr}_{\mathcal{H}}\left[V|v\rangle\langle v|V^{\dagger}\right]$.

Definition 3.3 (*"Interaction" probability*). Let $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be a channel with vacuum $v \in \mathcal{H}$ and let $D = (\mathcal{H}, \mathcal{H}_Z, \mathcal{H}_i, \mathcal{H}_o, s_0, \Lambda)$ be an N-step discrimination strategy. The *"interaction" probability* is defined by

$$P_I^T(D) := \sum_{n=0}^{N-1} \mathfrak{i}_T \left(\mathrm{tr}_Z \left[\rho_n^{T^\downarrow} \right] \right), \tag{3.5}$$

where the quantum operation $T^\downarrow : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ is defined by

$$T^\downarrow(\cdot) = \mathrm{tr}_E \left[(P_v \otimes \mathbb{1}) V \cdot V^\dagger \right], \tag{3.6}$$

and where $V : \mathcal{H} \to \mathcal{H}_E \otimes \mathcal{H}$ is any Stinespring isometry of T and P_v is the orthogonal projection onto the support of $\mathrm{tr}_{\mathcal{H}} \left[V|v\rangle\langle v|V^\dagger \right]$.

Definition 3.4 *("Interaction-free" discrimination).* Let $v \in \mathcal{H}$ and $\mathcal{C}_A, \mathcal{C}_B \subseteq \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ be two sets of channels such that for all $T \in \mathcal{C}_A \cup \mathcal{C}_B$, T is a channel with vacuum v. We say that $\mathcal{C}_A$ and $\mathcal{C}_B$ can be *discriminated in an "interaction-free" manner* if for every $\epsilon, \delta > 0$ there exists an N-step discrimination strategy D and a two-valued POVM Π such that

$$P_e(D, \Pi) < \epsilon \quad \text{and} \quad P_I^T(D) < \delta, \tag{3.7}$$

for all $T \in \mathcal{C}_A \cup \mathcal{C}_B$.

Definition 3.5 (*Channel with transmission functional*). A *channel with transmission functional* $\mathfrak{t}_T$ is a channel $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ together with a positive linear functional $\mathfrak{t}_T \in (\mathcal{B}_1(\mathcal{H}))^*$. We call $\mathfrak{t}_T$ the *transmission functional*.

Definition 3.6 *(Total transmission)* Let $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be a channel with transmission functional $\mathfrak{t}_T$. For an N-step discrimination strategy $D = (\mathcal{H}, \mathcal{H}_Z, \mathcal{H}_i, \mathcal{H}_o, s_0, \Lambda)$, the *total transmission* is defined by

$$\mathfrak{T}_T(D) := \sum_{n=0}^{N-1} \mathfrak{t}_T \left(\mathrm{tr}_Z \left[\rho_n^T \right] \right). \tag{3.8}$$

Definition 3.7 *(Transmission-free discrimination).* Let $\mathcal{C}_A, \mathcal{C}_B \subseteq \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ be two sets of channels such that for all $T \in \mathcal{C}_A \cup \mathcal{C}_B$, T is a channel with transmission functional $\mathfrak{t}_T$. We say that $\mathcal{C}_A$ and $\mathcal{C}_B$ can be *discriminated in a transmission-free manner* if for every $\epsilon, \delta > 0$ there exists an N-step discrimination strategy D and a two-valued POVM Π such that

$$P_e(D, \Pi) < \epsilon \quad \text{and} \quad \mathfrak{T}_T(D) < \delta, \tag{3.9}$$

for all $T \in \mathcal{C}_A \cup \mathcal{C}_B$.

3.4. Comparison of the Models and Elementary Properties

In this section, we clarify the relation between the transmission model and the "interaction" model. As a rule of thumb, the transmission model can be thought of as a generalization of the "interaction" model. Since we admit arbitrary positive linear functionals as transmission functionals, we have a much greater flexibility when modeling. For example, one could decide that out of the two objects to be discriminated, it does not matter (or is even desirable) if

the second one gets destroyed. We should therefore set the transmission functional of the second channel to zero. This is something that is not possible in the "interaction" model. On the other hand, the advantage of the "interaction" model is that the "interaction" probability has a very clear interpretation and that the "interaction" functional is an intrinsic property of the channel. For the relation between these models, we note the following lemma.

Lemma 3.8. *Let $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be a channel with vacuum $v \in \mathcal{H}$ and let $\mathfrak{i}_T$ be its "interaction" functional. If we interpret T as a channel with transmission functional $\mathfrak{i}_T$, then*

$$P_I^T(D) \leq \mathfrak{T}_T(D), \tag{3.10}$$

for all N-step discrimination strategies D.

Proof. Immediate from the definition, since (by induction) $\rho_i^{T^\downarrow} \leq \rho_i^T$. □

The insight that should be gained from this lemma is that if we want to prove that a certain discrimination task can be done in an "interaction-free" or in a transmission-free manner, then it suffices to tackle the problem in the transmission model. Thus, the results in Sect. 4 will be formulated in terms of the transmission model. On the other hand, if we want to prove a no-go theorem, then it is sufficient to work in the "interaction" model. At this point, there is a little detail that we do not want to hide, which is that it is possible that certain discrimination tasks can be performed with less resources, if one works in the "interaction" model and not in the transmission model. We will not investigate this possibility any further. We close this section by introducing the concept of a *maximal vacuum subspace*.

Definition 3.9 (*Maximal vacuum subspace*). Let $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be a channel with vacuum $v \in \mathcal{H}$ and let $V : \mathcal{H} \to \mathcal{H}_E \otimes \mathcal{H}$ be any Stinespring isometry of T. The subspace $\mathcal{V}_T$ of $\mathcal{H}$, defined by[11]

$$\mathcal{V}_T := V^{-1}\left[\mathrm{supp}(\mathrm{tr}_{\mathcal{H}}\left[V|v\rangle\langle v|V^\dagger\right]) \otimes \mathcal{H}\right], \tag{3.11}$$

is called the *maximal vacuum subspace* of T.

Lemma 3.10 (Properties of maximal vacuum subspaces). *For $\dim(\mathcal{H}) < \infty$, let $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be a channel with vacuum $v \in \mathcal{H}$. The maximal vacuum subspace $\mathcal{V}_T$ has the following properties:*

1. *$v \in \mathcal{V}_T$.*
2. *T is isometric on $\mathcal{V}_T$.*
3. *If T is isometric on a subspace $\mathcal{V}' \subseteq \mathcal{H}$, then either $\mathcal{V}_T \cap \mathcal{V}' = \{0\}$ or $\mathcal{V}' \subseteq \mathcal{V}_T$.*
4. *$\mathcal{V}_T$ is the union of all subspaces that contain v and on which T is isometric.*
5. *There exists a constant $C_T > 0$ such that $\mathfrak{i}_T(\rho) \geq C_T \mathrm{tr}\left[P^\perp \rho\right]$ for all $\rho \geq 0$, where $P^\perp$ is the projection onto $\mathcal{V}_T^\perp$.*

[11] $V^{-1}[\cdot]$ denotes the preimage operation.

6. *For all $\rho \geq 0$, we have $\mathrm{i}_T(\rho) \leq \mathrm{tr}\left[P^\perp \rho\right]$, where $P^\perp$ is the projection onto $\mathcal{V}_T^\perp$.*

Remark 3.11. The Claims 1–4 and 6 remain true if one lifts the assumption that $\mathcal{H}$ is finite-dimensional. Claim 5, however, would then be wrong.

Proof. We start with the following observation: Let $V : \mathcal{H} \to \mathcal{H}_E \otimes \mathcal{H}$ be any Stinespring isometry of T. Since $T(|v\rangle\langle v|)$ is pure, Vv must be a tensor product. Thus, there are two unit vectors $v' \in \mathcal{H}$ and $e \in \mathcal{H}_E$ such that

$$Vv = e \otimes v'.$$

Hence, $\mathrm{tr}_{\mathcal{H}}\left[V|v\rangle\langle v|V^\dagger\right] = |e\rangle\langle e|$ and

$$\mathrm{supp}(\mathrm{tr}_{\mathcal{H}}\left[V|v\rangle\langle v|V^\dagger\right]) = \mathrm{span}\{e\}. \tag{3.12}$$

(1) Clearly, $Vv \in \mathrm{supp}(\mathrm{tr}_{\mathcal{H}}\left[V|v\rangle\langle v|V^\dagger\right]) \otimes \mathcal{H}$. Thus, $v \in V^{-1}\left[Vv\right] \subseteq \mathcal{V}_T$.
(2) For $\phi \in \mathcal{V}_T$, we have $V\phi = e \otimes \psi_\phi$ for a uniquely defined $\psi_\phi \in \mathcal{H}$. We define $U : \mathcal{V}_T \to \mathcal{H}$ by $U\phi := \psi_\phi$. It is easy to check that U is an isometry and that $T(|\phi\rangle\langle\phi|) = U|\phi\rangle\langle\phi|U^\dagger$. Since this holds for all $\phi \in \mathcal{V}_T$, T is isometric on $\mathcal{V}_T$.
(3) Suppose that T is isometric on $\mathcal{V}'$, with isometry $U' : \mathcal{V}' \to \mathcal{H}$. If $\dim(\mathcal{V}') \leq 1$ then the claim is trivially true. So we can assume that $\dim(\mathcal{V}') \geq 2$. Let v_1 and v_2 be two orthogonal unit vectors in $\mathcal{V}'$. By assumption,

$$T(|v_i\rangle\langle v_i|) = \mathrm{tr}_E\left[V|v_i\rangle\langle v_i|V^\dagger\right] = U'|v_i\rangle\langle v_i|U'^\dagger,$$

for $i \in \{1,2\}$. As $U'|v_i\rangle\langle v_i|U'^\dagger$ is pure, there exists a pair of unit vectors $e_1, e_2 \in \mathcal{H}_E$ such that $Vv_i = e_i \otimes U'v_i$. By linearity, we have

$$\begin{aligned}
0 &= T(|v_1+v_2\rangle\langle v_1+v_2|) - \mathrm{tr}_E\left[V|v_1+v_2\rangle\langle v_1+v_2|V^\dagger\right] \\
&= U'|v_1+v_2\rangle\langle v_1+v_2|U'^\dagger - U'|v_1\rangle\langle v_1|U'^\dagger \\
&\quad - \langle e_2|e_1\rangle U'|v_1\rangle\langle v_2|U'^\dagger - \langle e_1|e_2\rangle U'|v_2\rangle\langle v_1|U'^\dagger - U'|v_2\rangle\langle v_2|U'^\dagger \\
&= (1-\langle e_2|e_1\rangle)U'|v_1\rangle\langle v_2|U'^\dagger + (1-\langle e_1|e_2\rangle)U'|v_2\rangle\langle v_1|U'^\dagger.
\end{aligned}$$

This can only be true if $\langle e_1|e_2\rangle = 1$, which is true only if $e_1 = e_2$. Thus, by transitivity, there is a unit vector $e' \in \mathcal{H}_E$ such that $Vv' = e' \otimes U'v'$ for all $v' \in \mathcal{V}'$. With the definition of U in the proof of 2, we also have $V\phi = e \otimes U\phi$ for all $\phi \in \mathcal{V}_T$. Assume that $\mathcal{V}_T \cap \mathcal{V}' \neq \{0\}$. For a unit vector $\hat{v} \in \mathcal{V}_T \cap \mathcal{V}'$, the Cauchy–Schwarz inequality yields

$$\begin{aligned}
1 = |\langle\hat{v}|\hat{v}\rangle| &= |\langle V\hat{v}|V\hat{v}\rangle| = |\langle e'|e\rangle|\,|\langle U'\hat{v}|U\hat{v}\rangle| \\
&\leq |\langle e'|e\rangle|\,\|U'\hat{v}\|\,\|U\hat{v}\| = |\langle e'|e\rangle| \leq \|e'\|\,\|e\| = 1.
\end{aligned}$$

Hence, the Cauchy–Schwarz inequality is satisfied with equality, which implies that the vectors e and e' differ only by a phase factor. In particular, $\mathrm{span}\{e\} = \mathrm{span}\{e'\}$. Using (3.12), we have for any $v' \in \mathcal{V}'$ that $Vv' = e' \otimes U'v' \in \mathrm{supp}(\mathrm{tr}_{\mathcal{H}}\left[V|v\rangle\langle v|V^\dagger\right]) \otimes \mathcal{H}$. Consequently, $v' \in \mathcal{V}_T$. As v' was arbitrary, this proves $\mathcal{V}' \subseteq \mathcal{V}_T$ as claimed.
4) If an isometric subspace $\mathcal{V}'$ contains v, then (by 1) the intersection with $\mathcal{V}_T$ is non-trivial. Thus, (by 3) $\mathcal{V}'$ is a subspace of $\mathcal{V}_T$. Hence, $\mathcal{V}_T$ contains all isometric subspaces and the claim follows as (by 2) $\mathcal{V}_T$ is isometric itself.

The following consideration is needed in the proof of 5 as well as in the proof of 6. We define the projections $\hat{P} := P_v \otimes \mathbb{1}$ and $\hat{P}^\perp := \mathbb{1} - \hat{P}$, where $P_v := |v\rangle\langle v|$. We further denote by P, the orthogonal projection onto $\mathcal{V}_T$ and define $P^\perp := \mathbb{1} - P$. In the following, let $\rho \geq 0$. By definition, we have

$$\begin{aligned}
\mathfrak{i}_T(\rho) &= \operatorname{tr}\left[P_v^\perp \operatorname{tr}_{\mathcal{H}}\left[V\rho V^\dagger\right]\right] \\
&= \operatorname{tr}\left[\hat{P}^\perp V\rho V^\dagger\right] \\
&= \operatorname{tr}\left[\hat{P}^\perp VP\rho PV^\dagger\right] + \operatorname{tr}\left[\hat{P}^\perp VP\rho P^\perp V^\dagger\right] \\
&\quad + \operatorname{tr}\left[\hat{P}^\perp VP^\perp \rho PV^\dagger\right] + \operatorname{tr}\left[\hat{P}^\perp VP^\perp \rho P^\perp V^\dagger\right].
\end{aligned}$$

By definition, if $\psi \in \mathcal{V}_T$, then $\hat{P}^\perp V\psi = 0$. Thus, $\hat{P}^\perp VP = 0$ as an operator. Hence, all summands except the last one vanish. Thus, we have

$$\mathfrak{i}_T(\rho) = \operatorname{tr}\left[\hat{P}^\perp VP^\perp \rho P^\perp V^\dagger\right] = \operatorname{tr}\left[V^\dagger \hat{P}^\perp VP^\perp \rho P^\perp\right]. \tag{3.13}$$

We can now prove 5. To this end, note that if $\operatorname{tr}\left[P^\perp \rho P^\perp\right] = 0$, then the claim follows trivially. Otherwise, $\frac{P^\perp \rho P^\perp}{\operatorname{tr}[P^\perp \rho P^\perp]}$ is a density matrix and the spectral theorem implies that

$$\frac{P^\perp \rho P^\perp}{\operatorname{tr}\left[P^\perp \rho P^\perp\right]} = \sum_i p_i |\psi_i^\perp\rangle\langle\psi_i^\perp|,$$

with $p_i \geq 0$, $\sum_i p_i = 1$ and $\psi_i^\perp \in \mathcal{V}_T^\perp$. By convexity, we have

$$\begin{aligned}
\operatorname{tr}\left[\hat{P}^\perp VP^\perp \rho P^\perp V^\dagger\right] &= \operatorname{tr}\left[P^\perp \rho\right] \operatorname{tr}\left[\hat{P}^\perp V \frac{P^\perp \rho P^\perp}{\operatorname{tr}\left[P^\perp \rho P^\perp\right]} V^\dagger\right] \\
&\geq \operatorname{tr}\left[P^\perp \rho\right] \inf_{\substack{\psi^\perp \in \mathcal{V}_T^\perp \\ \|\psi^\perp\| = 1}} \operatorname{tr}\left[\hat{P}^\perp V|\psi^\perp\rangle\langle\psi^\perp|V^\dagger\right].
\end{aligned}$$

If the infimum is strictly positive, then this is the C_T we are looking for. To see that this is indeed the case, note that the set $\{\psi^\perp \in \mathcal{V}_T^\perp \mid \|\psi^\perp\| = 1\}$ is compact. Thus, the infimum is actually a minimum. Assume for the sake of contradiction that $\operatorname{tr}\left[\hat{P}^\perp V|\psi^\perp\rangle\langle\psi^\perp|V^\dagger\right] = 0$, for some unit vector $\psi^\perp \in \mathcal{V}_T^\perp$. Then $\langle \hat{P}^\perp V\psi^\perp | \hat{P}^\perp V\psi^\perp\rangle = 0$ and consequently $\hat{P}^\perp V\psi^\perp = 0$. Hence, $V\psi^\perp \in \operatorname{supp}(\operatorname{tr}_{\mathcal{H}}\left[V|v\rangle\langle v|V^\dagger\right]) \otimes \mathcal{H}$ and $\psi^\perp \in \mathcal{V}_T$. As this is a contradiction, the claim follows.

To prove 6, we use Hölder's inequality for Schatten norms. Applying this inequality to the RHS of (3.13) yields

$$\mathfrak{i}_T(\rho) \leq \left\|V^\dagger \hat{P}^\perp V\right\|_\infty \left\|P^\perp \rho P^\perp\right\|_1 = \operatorname{tr}\left[P^\perp \rho\right].$$

The last equality follows, since $V^\dagger \hat{P}^\perp V$ is an orthogonal projection (and thus has norm 1) and since $P^\perp \rho P^\perp \geq 0$. This proves the claim. □

Remark 3.12. Since by the previous theorem, every subspace that is isometric w.r.t. T and contains the vacuum is contained in $\mathcal{V}_T$, checking the conditions in Theorem 2.2 reduces to checking whether

$$T_A|_{\mathcal{B}(\mathcal{V}_{T_A})} \neq T_B|_{\mathcal{B}(\mathcal{V}_{T_A})} \quad \text{or} \quad T_A|_{\mathcal{B}(\mathcal{V}_{T_B})} \neq T_B|_{\mathcal{B}(\mathcal{V}_{T_B})}. \tag{3.14}$$

This can be done efficiently, since $\mathcal{V}_{T_A}$ and $\mathcal{V}_{T_B}$ can be computed by simple linear algebraic methods.

4. The Discrimination Protocol

The main goal of this section is to prove Theorem 2.5. This is done in two steps. At first, we show how to discriminate between the identity channel and a compact set of channels, where some additional conditions are imposed on the channels under consideration. In particular, we obtain the following theorem.

Theorem 4.1. *For* $\dim(\mathcal{H}) < \infty$*, let* $\mathcal{C} \subseteq \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ *be a closed set of channels and let* $v \in \mathcal{H}$ *be a unit vector such that for all* $T \in \mathcal{C}$*, the state* $|v\rangle\langle v|$ *is the only state that is a fixed point of* T*. Then, there exists a constant* C *and for every* $N \in \mathbb{N}$ *an* N*-step discrimination strategy* D *and a two-valued POVM* Π *such that*

$$P_e(D, \Pi) \leq \frac{C}{N^2}, \tag{4.1}$$

where the discrimination error probability is w.r.t the sets $\{\mathrm{id}\}$ *and* $\mathcal{C}$*. Furthermore, if* $T \in \mathcal{C}$ *is a channel with transmission functional* $\mathfrak{t}_T$ *and* $\mathfrak{t}_T(|v\rangle\langle v|) = 0$*, then the total transmission* $\mathfrak{T}_T(D)$ *is bounded by*

$$\mathfrak{T}_T(D) \leq \frac{C\,\|\mathfrak{t}_T\|}{N}. \tag{4.2}$$

In particular, if $\mathfrak{t}_{\mathrm{id}} = 0$ *and for all* $T \in \mathcal{C}$*,* T *is a channel with transmission functional* $\mathfrak{t}_T$*, with* $\mathfrak{t}_T(|v\rangle\langle v|) = 0$*; and if* $\sup_{T\in\mathcal{C}} \|\mathfrak{t}_T\| < \infty$*, then the sets* $\{\mathrm{id}\}$ *and* $\mathcal{C}$ *can be discriminated in a transmission-free manner.*

Proof. This statement is a direct consequence of Theorem 4.10 and the discussion in the paragraph "Description of the discrimination strategy." □

The second step then is to show how to reduce the general case to Theorem 4.1. This is the main content of Sect. 4.2, in which we also prove Theorem 2.5.

4.1. Empty or Not?

In this section we study a special case of the general discrimination task. That is, we study the case where we want to discriminate between the identity channel (empty box) and a compact set of channels $\mathcal{C} \subseteq \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$, which does not contain the identity channel. We show that under some conditions on the spectrum of the channels in $\mathcal{C}$ and on the transmission functionals, a Kwiat et al.-like strategy suffices to perform the task in a transmission-free manner, even if the underlying Hilbert space is infinite-dimensional. In the finite-dimensional case, our considerations reduce to Theorem 4.1. Before we

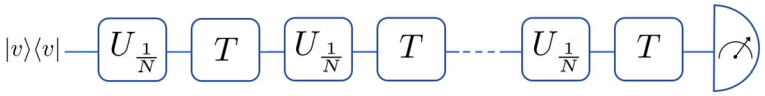

FIGURE 6. General form of a Kwiat et al.-like strategy

go into detail on what we mean by a Kwiat et al.-like strategy, we give an overview of the additional conditions we impose on the channels in $\mathcal{C}$.

Outline of the Assumptions Our first assumption is that there is a pure state $|v\rangle\langle v| \in \mathcal{S}(\mathcal{H})$ (vacuum) that is a fixed point of all channels in $\mathcal{C}$ and that the transmission functionals satisfy $\mathfrak{t}_T(|v\rangle\langle v|) = 0$ for all $T \in \mathcal{C}$. As a remark, note that if there were no state $\rho \in \mathcal{S}(\mathcal{H})$, with $\mathfrak{t}_T(\rho) = 0$ for all $T \in \mathcal{C}$, then, of course, the discrimination task is impossible. On the other hand, if there exists such a state ρ, then, by the spectral theorem and the linearity and positivity of $\mathfrak{t}_T$, there exists a pure state $\rho_v \in \mathcal{S}(\mathcal{H})$, with $\mathfrak{t}_T(\rho_v) = 0$ for all $T \in \mathcal{C}$. But then, if ρ_v is not a fixed point of T, the discrimination task becomes trivial. Thus, assuming a pure fixed point for the current setting is not a strong assumption.

Our second assumption is that all channels in $\mathcal{C}$ have a spectral gap. That is, if we exclude 1 from the spectrum of T, then the remaining part must be contained in a disk of radius less than 1 (remember that since T is a channel, its spectral radius is 1 and 1 is part of the spectrum). In Remark 4.11, we show that the spectral gap assumption cannot be waived completely if a Kwiat et al.-like protocol (defined below) should succeed.

Our third assumption is that the spectral gap assumption is compatible in a certain sense with the discrimination strategy. Expression (4.9) in the statement of Theorem 4.5 makes this statement precise. A sufficient condition for the compatibility assumption to be fulfilled (given our second assumption) is that 1 is a simple eigenvalue of every channel in $\mathcal{C}$. This is the content of Theorem 4.6. Furthermore, in the finite-dimensional case our second assumption is automatically fulfilled (given our first assumption) if 1 is a simple eigenvalue of every channel in $\mathcal{C}$. This is the content of Theorem 4.10.

Our fourth assumption concerns the relation between the channels in $\mathcal{C}$ and their associated transmission functionals. Note that the definition of a transmission functional (Definition 3.5) does not impose such a relation. For our current purpose, however, this is problematic since $\sup_{T\in\mathcal{C}} \|\mathfrak{t}_T\|$ may be infinite. We will thus assume that $\sup_{T\in\mathcal{C}} \|\mathfrak{t}_T\|$ is finite. This is a very mild assumption, since it is implied if $\mathfrak{t}_T$ depends continuously on T (which is very reasonable on physical grounds). Furthermore, note that if $\mathfrak{t}_T$ is an "interaction" functional, then, as a consequence of Claim 6 in Lemma 3.10, we have $\sup_{T\in\mathcal{C}} \|\mathfrak{t}_T\| \leq 1$.

Description of the Discrimination Strategy The next step is to design a strategy that allows us to discriminate between the identity channel and $\mathcal{C}$. An important factor in designing a strategy is the amount of resources that are needed to implement it. To this end, we show that only a bare minimum is

required. Let $H \in \mathcal{B}(\mathcal{H})$ be a self-adjoint operator such that v is not an eigenvector of e^{-iH}. In other words, we assume that $C_H := \left|\langle v|e^{-iH}v\rangle\right|$ is strictly less than 1. Then, our strategy is to repeat the N-step discrimination strategy, depicted in Fig. 6, a total of K times. More precisely, upon defining the 1-parameter family of channels $U_t : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ by $U_t(\cdot) = e^{-iHt} \cdot e^{iHt}$, the discrimination strategy is given by the initial state $s_0 := |v\rangle\langle v|$ and the set of channels Λ, with $\Lambda_i := U_{\frac{1}{N}}$ for $0 \leq i \leq N-1$ and $\Lambda_N := \mathrm{id}$. After each execution of the discrimination strategy, we perform a measurement described by the two-valued POVM $\{P^\perp, |v\rangle\langle v|\}$, where $P^\perp := \mathbb{1} - |v\rangle\langle v|$. If all K outcomes correspond to the second event, then we decide that the unknown channel is in $\mathcal{C}$ and if otherwise we decide that the unknown channel is the identity. Of course, this protocol can be cast into the form of an NK-step discrimination strategy by using an ancillary system and the principle of deferred measurement (see [25], p. 186). We call this strategy $D_{H,N,K}$. By Definition 2.4, the error probability is then given by

$$P_e(D_{H,N,K}, \Pi) = \frac{1}{2}\left(\mathrm{tr}\left[|v\rangle\langle v|\rho_N^{\mathrm{id}}\right]^K + \sup_{T\in\mathcal{C}}\left\{\mathrm{tr}\left[P^\perp\rho_N^T\right]\sum_{k=0}^{K-1}\mathrm{tr}\left[|v\rangle\langle v|\rho_N^T\right]^k\right\}\right),$$

where ρ is the intermediate state map and where Π denotes the measurement scheme described above. Explicitly, we have

$$\rho_N^{\mathrm{id}} = U_{\frac{1}{N}}^N(|v\rangle\langle v|) = e^{-iH}|v\rangle\langle v|e^{iH} \quad \text{and} \quad \rho_N^T = (T \circ U_{\frac{1}{N}})^N(|v\rangle\langle v|).$$

In general, this leads to the estimate

$$P_e(D_{H,N,K}, \Pi) \leq \frac{1}{2}\left(C_H^{2K} + K\sup_{T\in\mathcal{C}}\mathrm{tr}\left[P^\perp\rho_N^T\right]\right). \tag{4.3}$$

Now suppose that $P_M := \sup_{T\in\mathcal{C}}\mathrm{tr}\left[P^\perp\rho_N^T\right]$ approaches zero as $N \to \infty$ (we show this below). Then, for given $\epsilon > 0$, we can choose $K := \left\lceil \frac{\ln(\epsilon)}{\ln(C_H)} \right\rceil$ and N such that $KP_M < \epsilon$. It follows from (4.3) that $P_e(D_{H,N,K}, \Pi) < \epsilon$. In other words, $P_e(D_{H,N,K}, \Pi)$ approaches zero if and only if P_M does. Furthermore, for a channel $T \in \mathcal{C}$, the total transmission is given by

$$\mathfrak{T}_T(D_{H,N,K}) = K\sum_{n=0}^{N-1}\mathfrak{t}_T\left(\rho_n^T\right) = K\mathfrak{T}_T(D_{H,N,1}).$$

Thus, also $\mathfrak{T}_T(D_{H,N,K})$ approaches zero if and only if $\mathfrak{T}_T(D_{H,N,1})$ does. In addition to that, we could always choose H such that $\langle v|e^{-iH}v\rangle = 0$. In that case, it suffices to set $K = 1$, which yields the simple expression

$$P_e(D_{H,N,1}, \Pi) = \frac{1}{2}\mathrm{tr}\left[P^\perp(T \circ U_{\frac{1}{N}})^N(|v\rangle\langle v|)\right],$$

for the error probability. Hence, in order to find a strategy that discriminates between the identity channel and the set $\mathcal{C}$, we only need to show that the quantities P_M and $\sup_{T\in\mathcal{C}}\mathfrak{T}_T(D_{H,N,1})$ approach zero for $N \to \infty$. Moreover, since $\mathfrak{t}_T$ can be written in the form $\mathfrak{t}_T(\cdot) = \mathrm{tr}\left[\Theta_T\cdot\right]$ for some positive semi-definite operator $\Theta_T \in \mathcal{B}(\mathcal{H})$ and since, by assumption $\mathfrak{t}_T(|v\rangle\langle v|) = 0$, we can

conclude that for $\rho \geq 0$,

$$\mathfrak{t}_T(\rho) \leq \|\mathfrak{t}_T\| \operatorname{tr}\left[P^\perp \rho\right].$$

The important conclusion that we draw from the discussion above is that in order to prove Theorem 4.1, it suffices to show (under the hypotheses of Theorem 4.1) that for any self-adjoint $H \in \mathcal{B}(\mathcal{H})$, there is a constant C such that the inequalities

$$\operatorname{tr}\left[P^\perp (T \circ U_{\frac{1}{N}})^N(|v\rangle\langle v|)\right] \leq \frac{C}{N^2}, \tag{4.4}$$

$$\operatorname{tr}\left[P^\perp \sum_{n=0}^{N-1} (U_{\frac{1}{N}} \circ T)^n(|v\rangle\langle v|)\right] \leq \frac{C}{N}, \tag{4.5}$$

hold for all $N \in \mathbb{N}$. This is precisely the statement of Theorem 4.10. Taking the validity of Theorem 4.10 for granted, we conclude that Theorem 4.1 holds.

Technical Theorems The remainder of this section is devoted to the proof of Theorem 4.10 and its infinite-dimensional versions. The following lemmas serve this purpose.

Lemma 4.2 ([26], p. 202). *Let $T \in \mathcal{B}(\mathcal{H})$, let $z \in \mathbb{C}$ be in the unbounded component of the resolvent $\rho(T)$, and let X be a closed invariant subspace of T. Then, X is an invariant subspace of $(z - T)^{-1}$.*

Lemma 4.3. *Let $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be a channel such that 1 is in the discrete spectrum of T. Then, for any $n \in \mathbb{N}$ and any (rectifiable) path inside the resolvent set of T that encloses 1, and separates 1 from $\sigma(T) \setminus \{1\}$, we have*

$$\frac{1}{2\pi i} \oint_{\Gamma_1} \frac{z^n}{z - T} \, \mathrm{d}z = \frac{1}{2\pi i} \oint_{\Gamma_1} \frac{1}{z - T} \, \mathrm{d}z. \tag{4.6}$$

Proof. See "Appendix A". □

Lemma 4.4 (Invariant subspace lemma). *Let $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be a channel, where $\mathcal{H}$ can be finite or infinite dimensional. Let $v \in \mathcal{H}$ be such that $|v\rangle\langle v|$ is a fixed point of T and set $V_v := \operatorname{span}\{v\}$. Then, the subspaces*

$$\mathcal{B}_{v\perp} := \left\{|v\rangle\langle\phi| \,\middle|\, \phi \in V_v^\perp\right\}, \tag{4.7}$$

$$\mathcal{B}_{\perp v} := \left\{|\phi\rangle\langle v| \,\middle|\, \phi \in V_v^\perp\right\}, \tag{4.8}$$

are invariant under T.

Proof. We prove that $\mathcal{B}_{v\perp}$ is invariant. The invariance of $\mathcal{B}_{\perp v}$ follows as T is Hermiticity-preserving. Let $\{K_i\}$ be a set of (non-zero) Kraus-operators of T. By assumption we have

$$|v\rangle\langle v| = T(|v\rangle\langle v|) = \sum_i \operatorname{tr}\left[K_i^\dagger K_i\right] \frac{K_i|v\rangle\langle v|K_i^\dagger}{\operatorname{tr}\left[K_i^\dagger K_i\right]},$$

where the series converges in trace norm. As the pure state $|v\rangle\langle v|$ is an extreme point of the closed and convex set of quantum states and the RHS is a convex

combination of states, we must have that $K_i|v\rangle\langle v|K_i^\dagger$ is proportional to $|v\rangle\langle v|$. Henceforth, v is an eigenvector of K_i for all i. We denote the corresponding eigenvalue by λ_i. So for $\psi \in V_v^\perp$, we get

$$T(|v\rangle\langle\psi|) = \sum_i K_i|v\rangle\langle\psi|K_i^\dagger = |v\rangle\langle\phi|,$$

where $\phi = \sum_i \overline{\lambda_i} K_i\,\psi$. As T is trace-preserving, we have

$$0 = \operatorname{tr}\left[|v\rangle\langle\phi|\right] = \operatorname{tr}\left[T(|v\rangle\langle\psi|)\right] = \operatorname{tr}\left[|v\rangle\langle\phi|\right] = \langle\phi|v\rangle.$$

Hence, $\phi \in V_v^\perp$. This proves the claim. □

The following theorem is the main technical result. In fact, everything else in this section can (to some extent) be regarded as a corollary to this theorem.

Theorem 4.5. *Let $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be a channel such that 1 is in the discrete spectrum of T, and let $v \in \mathcal{H}$ be a unit vector such that $|v\rangle\langle v|$ is a fixed point of T. Furthermore, let $H \in \mathcal{B}(\mathcal{H})$ be self-adjoint, $\tau > 0$ and $0 < \delta < 1$ such that*

$$\sigma(U_t \circ T) \subseteq \mathbb{D}_{1-\delta}(0) \cup \{1\}, \tag{4.9}$$

for $0 \le t \le \tau$, where $U_t : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ is defined by $U_t(\cdot) := e^{-iHt} \cdot e^{iHt}$. Then, the inequalities

$$\operatorname{tr}\left[P^\perp\,(T \circ U_{\frac{1}{N}})^N(|v\rangle\langle v|)\right] \le \frac{C}{N^2}, \tag{4.10}$$

$$\operatorname{tr}\left[P^\perp \sum_{n=0}^{N-1} (U_{\frac{1}{N}} \circ T)^n(|v\rangle\langle v|)\right] \le \frac{C}{N}, \tag{4.11}$$

hold for all $N \in \mathbb{N}$. Here, $P^\perp := \mathbb{1} - |v\rangle\langle v|$ and

$$C := \max\left\{\tau^{-2},\ 18\delta^{-1}\,\|H\|^2_{\mathcal{B}(\mathcal{H})} \max_{\substack{0\le t\le\tau \\ z\in\Gamma}} \left\|(z-T)^{-1}\right\| \left\|(z-U_tT)^{-1}\right\|\right\} < \infty,$$

where $\Gamma := \left\{z \in \mathbb{C} \,\middle|\, |z| = 1 - \frac{\delta}{2}\right\} \cup \left\{z \in \mathbb{C} \,\middle|\, |z-1| = \frac{\delta}{2}\right\}$.

Proof. We need to calculate the quantities (4.10) and (4.11). To do so, we employ the holomorphic functional calculus. For $0 \le t \le \tau$ and $n \in \mathbb{N}$, we have

$$(U_tT)^n = \frac{1}{2\pi i} \oint_{|z-1|=\frac{\delta}{2}} \frac{z^n}{z - U_tT}\,\mathrm{d}z + \frac{1}{2\pi i} \oint_{|z|=1-\frac{\delta}{2}} \frac{z^n}{z - U_tT}\,\mathrm{d}z \tag{4.12}$$

$$= \frac{1}{2\pi i} \oint_{|z-1|=\frac{\delta}{2}} \frac{1}{z - U_tT}\,\mathrm{d}z + \frac{1}{2\pi i} \oint_{|z|=1-\frac{\delta}{2}} \frac{z^n}{z - U_tT}\,\mathrm{d}z, \tag{4.13}$$

where we used Lemma 4.3 to obtain the second line. Under the trace, we can (crudely) estimate this term as follows:

$$\begin{aligned}\left|\mathrm{tr}\left[P^{\perp}(U_tT)^n(|v\rangle\langle v|)\right]\right| &\leq \frac{\delta}{2}\max_{|z-1|=\frac{\delta}{2}}\left|\mathrm{tr}\left[P^{\perp}\frac{1}{z-U_tT}(|v\rangle\langle v|)\right]\right| \\ &\quad+\left(1-\frac{\delta}{2}\right)^{n+1}\max_{|z|=1-\frac{\delta}{2}}\left|\mathrm{tr}\left[P^{\perp}\frac{1}{z-U_tT}(|v\rangle\langle v|)\right]\right| \\ &\leq \max_{z\in\Gamma}\left|\mathrm{tr}\left[P^{\perp}\frac{1}{z-U_tT}(|v\rangle\langle v|)\right]\right|. \end{aligned} \tag{4.14}$$

In everything that follows, we assume that $z \in \Gamma$. To proceed, we need two auxiliary calculations. First, we use the second resolvent identity ([27], p. 84) twice to obtain

$$\begin{aligned}\frac{1}{z-U_tT} &= \frac{1}{z-T}+\frac{1}{z-T}(U_t-\mathrm{id})\frac{T}{z-T} \\ &\quad+\frac{1}{z-U_tT}(U_t-\mathrm{id})\frac{T}{z-T}(U_t-\mathrm{id})\frac{T}{z-T}.\end{aligned} \tag{4.15}$$

Second, an elementary application of Taylor's formula yields

$$\|U_t-\mathrm{id}\| \leq 2\,\|H\|_{\mathcal{B}(\mathcal{H})}\,t, \tag{4.16}$$

$$(U_t-\mathrm{id})(\rho) = i[\rho,H]t+\mathfrak{U}t^2, \tag{4.17}$$

with $||\mathfrak{U}|| \leq 2\,\|H\|^2_{\mathcal{B}(\mathcal{H})}$. When looking at (4.15), it is clear that the summands are of zeroth, first and second order in t, as $t \to 0$. The crucial step is to show that under the trace, the second term is $\mathcal{O}(t^2)$. Using (4.17), we get

$$\begin{aligned}\frac{1}{z-T}(U_t-\mathrm{id})\frac{T}{z-T}(|v\rangle\langle v|) &= \frac{1}{z-1}\frac{1}{z-T}(U_t-\mathrm{id})(|v\rangle\langle v|) \\ &= \frac{it}{z-1}\frac{1}{z-T}(|v\rangle\langle Hv|-|Hv\rangle\langle v|) \\ &\quad+\frac{t^2}{z-1}\frac{1}{z-T}(\mathfrak{U}(|v\rangle\langle v|)).\end{aligned} \tag{4.18}$$

It is easily verified, using the self-adjointness of H, that $|v\rangle\langle Hv|-|Hv\rangle\langle v| = |v\rangle\langle\phi|-|\phi\rangle\langle v|$, with $\phi := (H-\langle v|Hv\rangle)v$. Clearly, $\langle\phi|v\rangle = 0$. Thus, $|\phi\rangle\langle v| \in \mathcal{B}_{\perp v}$ and $|v\rangle\langle\phi| \in \mathcal{B}_{v\perp}$, where $\mathcal{B}_{\perp v}$ and $\mathcal{B}_{v\perp}$ are both invariant subspaces of T (by Lemma 4.4). As z is in the unbounded component of the resolvent set of T, Lemma 4.2 implies that also $(z-T)^{-1}(|\phi\rangle\langle v|) \in \mathcal{B}_{\perp v}$ and $(z-T)^{-1}(|v\rangle\langle\phi|) \in \mathcal{B}_{v\perp}$. Thus, the first term in (4.18) vanishes under the trace, and we get

$$\left|\mathrm{tr}\left[P^{\perp}(4.18)\right]\right| \leq t^2\frac{2\,\|H\|^2_{\mathcal{B}(\mathcal{H})}}{|z-1|}\left\|(z-T)^{-1}\right\|. \tag{4.19}$$

So under the trace, this term is indeed quadratic in t. For the other two terms in (4.15), we have

$$\left|\mathrm{tr}\left[P^{\perp}\frac{1}{z-T}(|v\rangle\langle v|)\right]\right| = \frac{1}{|z-1|}\mathrm{tr}\left[P^{\perp}|v\rangle\langle v|\right] = 0 \tag{4.20}$$

and

$$\begin{aligned}
&\left|\mathrm{tr}\left[P^{\perp}\,\frac{1}{z-U_tT}(U_t-\mathrm{id})\frac{T}{z-T}(U_t-\mathrm{id})\frac{T}{z-T}(|v\rangle\langle v|)\right]\right| \\
&\quad\leq \frac{1}{|z-1|}\left\|(z-U_tT)^{-1}\right\|\|U_t-\mathrm{id}\|^2\left\|\frac{T}{z-T}\right\| \\
&\quad\leq t^2\frac{4\,\|H\|^2_{\mathcal{B}(\mathcal{H})}}{|z-1|}\left\|(z-U_tT)^{-1}\right\|\left\|(z-T)^{-1}\right\|, \qquad (4.21)
\end{aligned}$$

where we used the estimate (4.16) and $\|T\| = 1$ to obtain the last line. We can now use the results obtained in (4.19), (4.20), and (4.21) to estimate the quantity of interest, (4.14). We have

$$\begin{aligned}
(4.14) &\leq 2t^2\,\|H\|^2_{\mathcal{B}(\mathcal{H})}\max_{z\in\Gamma}\frac{\left\|(z-T)^{-1}\right\|\left(1+2\left\|(z-U_tT)^{-1}\right\|\right)}{|z-1|} \\
&\leq t^2\left(18\delta^{-1}\,\|H\|^2_{\mathcal{B}(\mathcal{H})}\max_{\substack{0\leq t'\leq\tau\\ z\in\Gamma}}\left\|(z-T)^{-1}\right\|\left\|(z-U_{t'}T)^{-1}\right\|\right) \\
&=: t^2C_0. \qquad (4.22)
\end{aligned}$$

To obtain the second estimate, we used $\max_{z\in\Gamma}|z-1|^{-1} = 2\delta^{-1}$ and $\left\|(z-U_tT)^{-1}\right\| \geq \|(z-U_tT)\|^{-1} \geq (|z|+1)^{-1} \geq \frac{2}{5}$. Equation (4.22) is a bound for $t \leq \tau$. To prove the theorem, we need a bound for all $t \geq 0$. To this end, we note that $\mathrm{tr}\left[P^{\perp}(U_tT)^n(|v\rangle\langle v|)\right] \leq 1$, since the expression represents a probability. We further define $C := \max(\tau^{-2}, C_0)$. If $t \leq \tau$, then by Eq. (4.22),

$$\mathrm{tr}\left[P^{\perp}(U_tT)^n(|v\rangle\langle v|)\right] \leq t^2C_0 \leq Ct^2.$$

And if $t > \tau$, then

$$\mathrm{tr}\left[P^{\perp}(U_tT)^n(|v\rangle\langle v|)\right] \leq 1 \leq \frac{t^2}{\tau^2} \leq Ct^2.$$

Hence,

$$\mathrm{tr}\left[P^{\perp}(U_tT)^n(|v\rangle\langle v|)\right] \leq Ct^2,$$

for all $t \geq 0$. This is a bound independent of n. Inequality (4.11) is then easily obtained by setting $t := \frac{1}{N}$ and summing over all n, which yields an additional factor N. It remains to show inequality (4.10), in which U_t and T have switched order. Since $|v\rangle\langle v|$ is a fixed point of T, we have $\mathrm{tr}\left[P^{\perp}(TU_t)^N(|v\rangle\langle v|)\right] = \mathrm{tr}\left[P^{\perp}T(U_tT)^N(|v\rangle\langle v|)\right]$. We set $\rho := (U_tT)^N(|v\rangle\langle v|)$ and $\phi := P^{\perp}\rho v$ and write

$$\rho = \langle v|\rho v\rangle|v\rangle\langle v| + |v\rangle\langle\phi| + |\phi\rangle\langle v| + P^{\perp}\rho P^{\perp}.$$

Clearly, $|v\rangle\langle\phi| \in \mathcal{B}_{v\perp}$ and $|\phi\rangle\langle v| \in \mathcal{B}_{\perp v}$. Hence, by Lemma 4.4, we have $T(|v\rangle\langle\phi|) \in \mathcal{B}_{v\perp}$ and $T(|\phi\rangle\langle v|) \in \mathcal{B}_{\perp v}$. Thus,

$$\mathrm{tr}\left[P^{\perp}T(\rho)\right] = \mathrm{tr}\left[P^{\perp}T(P^{\perp}\rho P^{\perp})\right] \leq \mathrm{tr}\left[T(P^{\perp}\rho P^{\perp})\right] = \mathrm{tr}\left[P^{\perp}\rho\right].$$

Hence,

$$\operatorname{tr}\left[P^{\perp}(TU_t)^N(|v\rangle\langle v|)\right] \leq \frac{C}{N^2}.$$

This finishes the proof. □

Theorem 4.6. *Let $\mathcal{C} \subseteq \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ be a compact set of channels, and let $v \in \mathcal{H}$ be a unit vector. Assume that*

1. *For all $T \in \mathcal{C}$, the quantity*
$$r_T := \sup_{z \in \sigma(T)\setminus\{1\}} |z|$$
is strictly less than 1. In other words, the spectral gap is nonzero.
2. *For each $T \in \mathcal{C}$, the state $|v\rangle\langle v|$ is a fixed point of T.*
3. *For all $T \in \mathcal{C}$, the algebraic multiplicity[12] of the isolated point $1 \in \sigma(T)$ is 1. In other words, 1 is a simple eigenvalue.*

Furthermore, let $H \in \mathcal{B}(\mathcal{H})$ be self-adjoint and $U_t : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be defined by $U_t(\cdot) = e^{-iHt} \cdot e^{iHt}$. Then, there exists a constant $C_{\mathcal{C}} < \infty$, such that

$$\operatorname{tr}\left[P^{\perp}\left(T \circ U_{\frac{1}{N}}\right)^N(|v\rangle\langle v|)\right] \leq \frac{C_{\mathcal{C}}\,\|H\|^2_{\mathcal{B}(\mathcal{H})}}{N^2}, \tag{4.23}$$

$$\operatorname{tr}\left[P^{\perp}\sum_{n=0}^{N-1}\left(U_{\frac{1}{N}} \circ T\right)^n(|v\rangle\langle v|)\right] \leq \frac{C_{\mathcal{C}}\,\|H\|^2_{\mathcal{B}(\mathcal{H})}}{N}, \tag{4.24}$$

for all $N \in \mathbb{N}$, where $P^{\perp} := \mathbb{1} - |v\rangle\langle v|$.

Remark 4.7. The distinctive feature of the preceding theorems is the N^{-2} bound in (4.23). It seems that such a bound cannot be obtained directly from the results in [13–16], because those results are of the form $\left(U_{\frac{1}{N}} \circ T\right)^N \approx \mathcal{P} + \mathcal{O}(\frac{1}{N})$ for $N \to \infty$, where $\mathcal{P}$ denotes the spectral projection on the eigenspace with eigenvalue 1.

Proof. The basic strategy is to reduce the claim to an application of Theorem 4.5. To this end, we basically need to show that Conditions 1–3 imply that condition (4.9) can be satisfied uniformly, i.e., that there exist $\tau > 0$ and $0 < \delta < 1$ such that (4.9) is satisfied for all $T \in \mathcal{C}$. The main tool to show this is the upper semi-continuity of the spectrum. To use that property, we import the following two theorems.

Theorem 4.8 ([28], p. 208). *For a Banach space $\mathcal{X}$, let $T, S \in \mathcal{B}(\mathcal{X})$, and let Γ be a compact subset of the resolvent set $\rho(T)$.*

If $\|T - S\| < \min_{z\in\Gamma} \left\|(z - T)^{-1}\right\|^{-1}$, then $\Gamma \subseteq \rho(S)$. Furthermore, for any open set $V \subseteq \mathbb{C}$, with $\sigma(T) \subset V$, there exists $\gamma > 0$, such that $\sigma(S) \subseteq V$ whenever $\|S - T\| < \gamma$.

[12] For an isolated point $\lambda \in \sigma(T)$, the algebraic multiplicity is the dimension of the range of the spectral projection.

Theorem 4.9 ([29], p. 67). *For a Banach space $\mathcal{X}$, let $P, Q \in \mathcal{B}(\mathcal{X})$ be bounded projections with $\|P - Q\| < 1$. Then, there exists an invertible operator $A \in \mathcal{B}(\mathcal{X})$, such that $Q = APA^{-1}$. In particular* $\mathrm{ran}(P)$ *and* $\mathrm{ran}(Q)$ *are isomorphic.*

To start, we show that not only $r_T < 1$ for all $T \in \mathcal{C}$, but that $\sup_{T\in\mathcal{C}} r_T < 1$. To this end, we show that the function $r : \mathcal{C} \to \mathbb{R},\ T \mapsto r_T$ is upper semi-continuous. That is, we need to show that for every $T \in \mathcal{C}$ and every $\epsilon > 0$, there is a set $U \subseteq \mathcal{C}$, which is open in the relative topology on $\mathcal{C}$, such that $r_S \leq r_T + \epsilon$ for all $S \in U$. For fixed T and $\epsilon > 0$, define $\epsilon' := \min(\epsilon, \frac{1-r_T}{3})$ and the open set $V_{\epsilon'} := B_{r_T+\epsilon'}(0) \cup B_{\epsilon'}(1) \subseteq \mathbb{C}$. By construction, $\sigma(T) \subseteq V_{\epsilon'}$. Thus, Theorem 4.8 implies that there exists $\gamma > 0$ such that $\sigma(S) \subseteq V_{\epsilon'}$ for all $S \in B_\gamma(T)$. Thus, for $S \in B_\gamma(T)$ the projection P_S onto the spectral subspace associated with the spectral subset $\sigma(S) \cap B_{\epsilon'}(1)$ is given by

$$P_S := \frac{1}{2\pi i} \oint_{|z-1|=\frac{1-r_T}{2}} \frac{1}{z - T_n}\,\mathrm{d}z = P_T + \frac{1}{2\pi i} \oint_{|z-1|=\frac{1-r_T}{2}} \frac{1}{z-S}(S-T)\frac{1}{z-T}\,\mathrm{d}z,$$

where we used the second resolvent identity to obtain the last equation. A standard estimate yields

$$\|P_S - P_T\| \leq \frac{1-r_T}{2}\,\|S-T\| \max_{|z-1|=\frac{1-r_T}{2}} \left\{ \left\|(z-S)^{-1}\right\| \left\|(z-T)^{-1}\right\| \right\}.$$

Since the set $S_0 := \overline{B_{\frac{\gamma}{2}}(T)} \cap \mathcal{C}$ is compact, the constant

$$C_0 := \max_{\substack{|z-1|=\frac{1-r_T}{2} \\ S\in S_0}} \left\{ \left\|(z-S)^{-1}\right\| \left\|(z-T)^{-1}\right\| \right\}$$

is finite. We set $\gamma' := \min\{\frac{\gamma}{2}, \frac{1}{(1-r_T)C_0}\}$ and $U := B_{\gamma'}(T) \cap \mathcal{C}$. By construction, U is open in the relative topology on $\mathcal{C}$ and we have $\sigma(S) \subseteq V_{\epsilon'}$ and $\|P_S - P_T\| \leq \frac{1}{2} < 1$ for all $S \in U$. By Assumption 3, $\mathrm{ran}(P_T)$ is 1-dimensional. Thus, by Theorem 4.9, also $\mathrm{ran}(P_S)$ is one-dimensional, for $S \in U$. Thus, there can be only one point in $\sigma(S) \cap B_{\epsilon'}(1)$, and this point must be 1, as 1 is in the spectrum of every channel. Hence, for $S \in U$, we have $\sigma(S) \setminus \{1\} \subseteq B_{r_T+\epsilon'}(0)$. So $r(S) = r_S \leq r_T + \epsilon' \leq r_T + \epsilon = r(T) + \epsilon$. In other words, r is upper semi-continuous. The upper semi-continuous function r assumes its maximum on the compact set $\mathcal{C}$. This maximum cannot be equal to 1, as this would contradict Assumption 1. Thus $\max_{T\in\mathcal{C}} r_T < 1$, as claimed.
In preparation for the application of Theorem 4.5, we define the joint spectral gap

$$\delta_J := 1 - \max_{T\in\mathcal{C}} r(T). \tag{4.25}$$

We have $0 < \delta_J < 1$ and

$$\sigma(T) \subseteq \mathbb{D}_{1-\delta_J}(0) \cup \{1\},$$

for all $T \in \mathcal{C}$. We define $\Gamma := \mathbb{D}_{1+\frac{\delta_J}{3}}(0) \setminus (B_{\frac{\delta_J}{3}}(1) \cup B_{1-\frac{2\delta_J}{3}}(0))$, which is a compact subset of $\rho(T)$ for all $T \in \mathcal{C}$, and we set

$$\tau := \frac{1}{7\|H\|_{\mathcal{B}(\mathcal{H})}} \min_{\substack{T\in\mathcal{C}\\ z\in\Gamma}} \left\|(z-T)^{-1}\right\|^{-2},$$

which is nonzero, as the minimization is over a strictly positive function on a compact set. For this particular choice of τ, we show that

$$\sigma(U_t T) \subseteq D_{1-\frac{2\delta_J}{3}}(0) \cup \{1\}$$

for $0 \leq t \leq \tau$ and then use Theorem 4.5. From now on, let $0 \leq t \leq \tau$ and $T \in \mathcal{C}$. Using the Taylor estimate (4.16) and the definition of τ yields

$$\begin{aligned}\|T - U_t T\| &\leq \|U_t - \mathrm{id}\|\,\|T\| \leq 2\|H\|_{\mathcal{B}(\mathcal{H})}\, t \\ &\leq \frac{2}{7} \min_{\substack{T\in\mathcal{C}\\ z\in\Gamma}} \left\|(z-T)^{-1}\right\|^{-2}. \end{aligned} \tag{4.26}$$

This inequality has two important implications. First, for $z \in \Gamma$ we have $\left\|(z-T)^{-1}\right\|^{-1} \leq \|z - T\| \leq |z|+1 \leq \frac{7}{3}$. Hence, (4.26) $< \min_{\substack{T\in\mathcal{C}\\ z\in\Gamma}} \left\|(z-T)^{-1}\right\|^{-1}$ and we can apply Theorem 4.8, which tells us that $\Gamma \subseteq \rho(U_t T)$ for all $T \in \mathcal{C}$ and $0 \leq t \leq \tau$. Equivalently,

$$\sigma(U_t T) \subseteq \mathbb{D}_{1-\frac{2\delta_J}{3}}(0) \cup \mathbb{D}_{\frac{\delta_J}{3}}(1).$$

Thus, we only have to show that $\sigma(U_t T) \cap \mathbb{D}_{\frac{\delta_J}{3}}(1) = \{1\}$.

Second, $\left\|(U_t T - T)(z-T)^{-1}\right\| \leq \frac{2}{7} \min_{\substack{T\in\mathcal{C}\\ z\in\Gamma}} \left\|(z-T)^{-1}\right\|^{-1} \leq \frac{2}{3}$. Thus, the series

$$\frac{1}{z-T} \sum_{k=0}^{\infty} \left[(U_t T - T)(z-T)^{-1}\right]^k = (z - U_t T)^{-1}$$

converges. A term-by-term estimate yields

$$\left\|(z-U_t T)^{-1}\right\| \leq 3\left\|(z-T)^{-1}\right\|, \tag{4.27}$$

Let $P_t := \frac{1}{2\pi i} \oint_{|z-1|=\frac{\delta_J}{3}} \frac{1}{z-U_t T}\,\mathrm{d}z$ be the spectral projection, then

$$\begin{aligned}\|P_t - P_0\| &= \left\| \frac{1}{2\pi i} \oint_{|z-1|=\frac{\delta_J}{3}} \frac{1}{z-U_t T} - \frac{1}{z-T}\,\mathrm{d}z \right\| \\ &\leq \frac{\delta_J}{3} \max_{|z-1|=\frac{\delta_J}{3}} \left\|(z-U_t T)^{-1} - (z-T)^{-1}\right\| \\ &= \frac{\delta_J}{3} \max_{|z-1|=\frac{\delta_J}{3}} \left\|(z-U_t T)^{-1}(U_t T - T)(z-T)^{-1}\right\| \\ &\leq \delta_J \|U_t T - T\| \max_{z\in\Gamma} \left\|(z-T)^{-1}\right\|^2 \end{aligned}$$

$$\leq \frac{2\delta_J}{7} < 1,$$

where we used the second resolvent identity to obtain the third line, (4.27) for the fourth line and (4.26) for the fifth line. Hence, by Theorem 4.9, the dimension of $\mathrm{ran}(P_t)$ equals the dimension of $\mathrm{ran}(P_0)$ for all $0 \leq t \leq \tau$, and the latter dimension is 1. Thus, $\sigma(U_t T) \cap \mathbb{D}_{\frac{\delta_J}{3}}(1)$ contains exactly one point, which must be 1, as $U_t T$ is a channel. In conclusion, we have

$$\sigma(U_t T) \subseteq \mathbb{D}_{1-\delta}(0) \cup \{1\},$$

for all $T \in \mathcal{C}$ and $0 \leq t \leq \tau$, with $\delta := \frac{2\delta_J}{3}$. Finally, a direct application of Theorem 4.5 proves the claim. We can also get an explicit bound for $C_{\mathcal{C}}$. To this end, we need to bound the constant that appears in Theorem 4.5. We have

$$\tau^{-2} = 49 \|H\|^2_{\mathcal{B}(\mathcal{H})} \max_{\substack{T\in\mathcal{C}\\ z\in\Gamma}} \left\|(z-T)^{-1}\right\|^4$$

and, by (4.27), the second term can be bounded by

$$36\delta_J^{-1} \|H\|^2_{\mathcal{B}(\mathcal{H})} \max_{\substack{T\in\mathcal{C}\\ z\in\Gamma}} \left\|(z-T)^{-1}\right\|^2. \tag{4.28}$$

Furthermore, by the spectral mapping theorem, the spectral radius of $(z-T)^{-1}$ is given by $(\inf_{s\in\sigma(T)} \|z-s\|)^{-1} = (\mathrm{dist}(z,\sigma(T)))^{-1}$. Since the norm of any operator is an upper bound for the spectral radius, we have

$$\max_{\substack{T\in\mathcal{C}\\ z\in\Gamma}} \left\|(z-T)^{-1}\right\| \geq \max_{\substack{T\in\mathcal{C}\\ z\in\Gamma}} \left\{\mathrm{dist}(z,\sigma(T))^{-1}\right\} \geq 3\delta_J^{-1} \geq 3.$$

By applying this bound to (4.28), we see that $\tau^{-2} \geq$ (4.28). Thus, we can choose

$$C_{\mathcal{C}} := 49 \max_{\substack{T\in\mathcal{C}\\ z\in\Gamma}} \left\|(z-T)^{-1}\right\|^4 < \infty. \tag{4.29}$$

□

Theorem 4.10. *For $\dim(\mathcal{H}) < \infty$, let $\mathcal{C}$ be a closed set of channels $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ and let $v \in \mathcal{H}$ be a unit vector such that for every $T \in \mathcal{C}$, the state $|v\rangle\langle v|$ is the only state that is a fixed point of T.*

Furthermore, let $H \in \mathcal{B}(\mathcal{H})$ be self-adjoint and $U_t : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be defined by $U_t(\cdot) = e^{-iHt} \cdot e^{iHt}$. Then, there exists a constant $C_{\mathcal{C}} < \infty$, such that for all $N \in \mathbb{N}$,

$$\mathrm{tr}\left[P^{\perp} (T \circ U_{\frac{1}{N}})^N (|v\rangle\langle v|)\right] \leq \frac{C_{\mathcal{C}} \|H\|^2_{\mathcal{B}(\mathcal{H})}}{N^2} \tag{4.30}$$

$$\mathrm{tr}\left[P^{\perp} \sum_{n=0}^{N-1} (U_{\frac{1}{N}} \circ T)^n (|v\rangle\langle v|)\right] \leq \frac{C_{\mathcal{C}} \|H\|^2_{\mathcal{B}(\mathcal{H})}}{N}, \tag{4.31}$$

where $P^{\perp} := \mathbb{1} - |v\rangle\langle v|$.

Proof. The claim follows from Theorem 4.6 and from results by Burgarth and Giovannetti [30]. In particular, in their terminology, a channel T is called *ergodic* if there is a unique state that is a fixed point of T. And (according to Theorem 7 in [30]), T is called *mixing* if 1 is the only eigenvalue with modulus 1 and the eigenvalue 1 is simple. Thus, in particular, if T is mixing, then the spectral gap is nonzero. Theorem 8 in [30] says that ergodic channels are mixing if the unique state that is a fixed point is pure. By assumption, every $T \in \mathcal{C}$ is ergodic and the only state that is a fixed point is the pure state $|v\rangle\langle v|$. Thus, all $T \in \mathcal{C}$ are mixing and the conditions in Theorem 4.6 are automatically satisfied. This proves the claim. □

Remark 4.11. In the previous theorem, it is important that $|v\rangle\langle v|$ is the only state that is a fixed point. To demonstrate this, we define the Hamiltonian on a qubit system, $\mathcal{H}_Q := \operatorname{span}\{v, q_1\}$, as $H := \frac{\pi}{2}\sigma_y$, where σ_y is the Pauli matrix.[13] So, $U_t(\cdot) := e^{-iHt} \cdot e^{iHt}$. The channel $T : \mathcal{B}_1(\mathcal{H}_Q) \to \mathcal{B}_1(\mathcal{H}_Q)$ is then defined by

$$T(\cdot) := \operatorname{tr}\left[|v\rangle\langle v| \cdot\right] |v\rangle\langle v| + \operatorname{tr}\left[|q_1\rangle\langle q_1| \cdot\right] |q_1\rangle\langle q_1|.$$

It is not hard to verify by induction that

$$(U_{\frac{1}{N}} \circ T)^n = U_{\frac{1}{N}} \left(\frac{1}{2}(1 + \cos^n(2\theta))|v\rangle\langle v| + \frac{1}{2}(1 - \cos^n(2\theta))|q_1\rangle\langle q_1| \right),$$

where $\theta := \frac{\pi}{2N}$. The formula for the sum of the geometric progression yields

$$\sum_{n=0}^{N-1} (U_{\frac{1}{N}} \circ T)^n(|v\rangle\langle v|) = U_{\frac{1}{N}} \left(\frac{1}{2}\left(N + \lambda\right)|v\rangle\langle v| + \frac{1}{2}\left(N - \lambda\right)|q_1\rangle\langle q_1| \right),$$

with $\lambda := \frac{1-\cos^N(2\theta)}{2\sin^2(\theta)}$. It is an exercise in elementary calculus (or a query in your favorite computer algebra system) to show that

$$\lim_{N\to\infty} (N - \lambda) = \frac{\pi^2}{4}. \tag{4.32}$$

Since $U_{\frac{1}{N}} \to \mathrm{id}$, when $N \to \infty$, it follows that the quantity on the RHS of (4.31) does not vanish as $N \to \infty$. In particular, our example shows that the Kwiat et al.-like protocol cannot be applied naively. Thus, the reduction process described in the next section is needed in some cases.

Remark 4.12. If the channel in Theorem 4.10 is a qubit channel ($\mathcal{H} = \operatorname{span}\{v, p\}$), then one can determine the precise asymptotics in a rather tedious calculation.

[13] In coordinates, $\sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $e^{-iHt} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$, with $\theta := \frac{\pi t}{2}$

We only state the result, which is that if $H := \frac{\pi}{2}\sigma_y$, then

$$\lim_{N\to\infty} N^2 \mathrm{tr}\left[P^\perp \left(T \circ U_{\frac{1}{N}}\right)^N (|v\rangle\langle v|)\right] = \lim_{N\to\infty} N \mathrm{tr}\left[P^\perp \sum_{n=0}^{N-1} (U_{\frac{1}{N}} \circ T)^n (|v\rangle\langle v|)\right] = \frac{\pi^2}{4} \frac{1-|\tau_0|^2}{(1-\tau)\,|1-\tau_0|^2}, \tag{4.33}$$

where $\tau := \mathrm{tr}\left[P^\perp T(P^\perp)\right]$ and $\tau_0 := \mathrm{tr}\left[|p\rangle\langle v|\, T(|v\rangle\langle p|)\right]$.
This result contains as a special case the result for semi-transparent objects [31,32].

Remark 4.13. It is a direct consequence of the results in the next section that the N^{-1} form of the bound is optimal.

4.2. The Reduction Protocol

In this section, in which we assume that all Hilbert spaces are finite-dimensional, we want to transform our given channel in such a way that the Kwiat et al.-like strategy, which was described in the previous section, can be applied. The general idea is that instead of inserting the unknown channel directly into the circuit of Fig. 6, we preprocess and postprocess the states that go in and out of the channel. In other words, we replace the channel T in Fig. 6 by the construction that is depicted on the RHS of Fig. 7. In Fig. 7, $\mathcal{H}_Q$ and $\mathcal{H}_A$ are Hilbert spaces and $R_0 : \mathcal{B}_1(\mathcal{H}_Q) \to \mathcal{B}_1(\mathcal{H}\otimes\mathcal{H}_A)$ and $R_0' : \mathcal{B}_1(\mathcal{H}\otimes\mathcal{H}_A) \to \mathcal{B}_1(\mathcal{H}_Q)$ are channels. The resulting transformation can be viewed as a map $R : \mathcal{B}(\mathcal{B}_1(\mathcal{H})) \to \mathcal{B}(\mathcal{B}_1(\mathcal{H}_Q))$, defined by $R(T) := R_0'(T\otimes \mathrm{id})R_0$. Maps of this kind are usually called superchannels [33]. Clearly, if T is a channel with transmission functional $\mathfrak{t}_T$, then $R(T)$ is a channel with transmission functional $\mathfrak{t}_{R(T)} := \mathfrak{t}_T \circ \mathrm{tr}_A \circ R_0$. We say that the superchannel R transforms the transmission functional $\mathfrak{t}_T$ to $\mathfrak{t}_{R(T)}$. For consistency reasons, we also remark the following: As is shown in [33], for any superchannel $S : \mathcal{B}(\mathcal{B}_1(\mathcal{H})) \to \mathcal{B}(\mathcal{B}_1(\mathcal{H}_Q))$, there exists a Hilbert space $\mathcal{H}_{A'}$ and channels $S_0 : \mathcal{B}_1(\mathcal{H}_Q) \to \mathcal{B}_1(\mathcal{H}\otimes\mathcal{H}_{A'})$ and $S_0' : \mathcal{B}_1(\mathcal{H}\otimes\mathcal{H}_{A'}) \to \mathcal{B}_1(\mathcal{H}_Q)$ such that $S(T) = S_0'(T\otimes\mathrm{id})S_0$ for all $T \in \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$. Of course, the choice of $\mathcal{H}_{A'}$, S_0, and S_0' is not unique. The transformation of the transmission functional, however, is unique. To see this, assume that we apply S to the map T_B, defined by $T_B(\cdot) = \mathrm{tr}\,[B\,\cdot\,]\,\rho_0$, where $\rho_0 \in \mathcal{S}(\mathcal{H})$ and $B \in \mathcal{B}(\mathcal{H})$ are arbitrary. Since S_0' is trace-preserving, we have for $\sigma \in \mathcal{B}(\mathcal{H}_Q)$, that $\mathrm{tr}\,[S(T)(\sigma)] = \mathrm{tr}\,[(T\otimes\mathrm{id})S_0(\sigma)] = \mathrm{tr}\,[B\mathrm{tr}_{A'}\,[S_0(\sigma)]]$. Since B and σ were arbitrary, it follows that $\mathrm{tr}_{A'}\circ S_0$ is independent of the choice of $\mathcal{H}_{A'}$, S_0, and S_0'. Hence, the transformation of the transmission functional is independent of the particular implementation of a superchannel. Formally, the replacement described above yields a transformation of the discrimination strategy. That is, given a discrimination strategy $D = (\mathcal{H}_Q, \mathcal{H}_Z, \mathcal{H}_i, \mathcal{H}_o, s_0, \Lambda)$, with $\Lambda = \{\Lambda_1, \Lambda_2, \ldots, \Lambda_N\}$, then we obtain the transformed discrimination strategy $D^R := (\mathcal{H}, \mathcal{H}_A\otimes\mathcal{H}_Z, \mathcal{H}_i, \mathcal{H}_o, s_0, \Lambda_R)$, with $\Lambda_0^R := (R_0\otimes \mathrm{id}_Z)\Lambda_0$, $\Lambda_N^R := \Lambda_N(R_0'\otimes\mathrm{id}_Z)$, and $\Lambda_n^R := (R_0\otimes\mathrm{id}_Z)\Lambda_n(R_0'\otimes\mathrm{id}_Z)$, for $1 \le n \le N-1$.

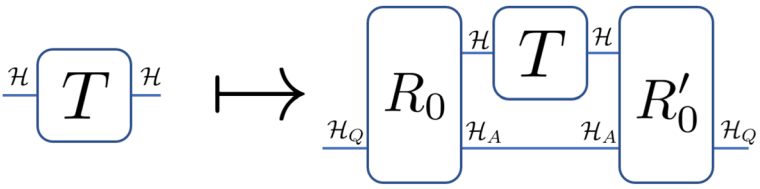

FIGURE 7. General transformation scheme: a superchannel

The task of this section is to show the existence of a superchannel such that the general discrimination task reduces to the one described in the last section. It will be evident from the proof of the following theorem that such a superchannel can be implemented by using only one ancillary qubit and classical resources. Furthermore, we show in Remark 4.18 that in general the implementation of such a superchannel is impossible without using an ancillary qubit.

Theorem 4.14 (Reduction superchannel). *For* $\dim(\mathcal{H}) < \infty$, *let* $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *be a channel and let* $\mathcal{V} \subseteq \mathcal{H}$ *be a subspace such that* T *is isometric on* $\mathcal{V}$. *Furthermore, let* $v \in \mathcal{V}$ *be a unit vector. Then, there exists a two-dimensional Hilbert space* $\mathcal{H}_Q$, *with orthonormal basis* $\{q_0, q_1\}$ *and a superchannel* $R : \mathcal{B}(\mathcal{B}_1(\mathcal{H})) \to \mathcal{B}(\mathcal{B}_1(\mathcal{H}_Q))$ *with the following properties:*

1. *If* $T' \in \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ *satisfies* $T|_{\mathcal{B}_1(\mathcal{V})} = T'|_{\mathcal{B}_1(\mathcal{V})}$, *then* $R(T') = \mathrm{id}$.
2. *If* $T' \in \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ *is a channel such that* $T|_{\mathcal{B}_1(\mathcal{V})} \neq T'|_{\mathcal{B}_1(\mathcal{V})}$, *then the only state that is a fixed point of* $R(T')$, *is* $|q_0\rangle\langle q_0|$.
3. *If* $T' \in \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ *is a channel with transmission functional* $\mathfrak{t}_{T'}$ *and* $\mathfrak{t}_T(|v\rangle\langle v|) = 0$, *then the transformed transmission functional* $\mathfrak{t}_{R(T')}$ *is given by*

$$\mathfrak{t}_{R(T')}(\cdot) = \begin{cases} \frac{1}{2}\mathfrak{t}_{T'}(\frac{P^\perp}{d-1})\mathrm{tr}\left[|q_1\rangle\langle q_1|\,\cdot\right] & \text{if } d > 1 \\ 0 & \text{if } d = 1 \end{cases}, \tag{4.34}$$

where $d := \dim(\mathcal{V})$ *and where* $P^\perp$ *denotes the orthogonal projection onto* $\{\psi \in \mathcal{V} \,|\, \langle\psi|v\rangle = 0\}$.

Before we prove the theorem, let us explore its consequences. First, we establish the analog of Theorem 2.5 for the transmission functional model.

Corollary 4.15. *For* $\dim(\mathcal{H}) < \infty$, *let* $\mathcal{C}_A, \mathcal{C}_B \subseteq \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ *be two closed sets of channels. Furthermore, let* $\mathcal{V}$ *be a subspace of* $\mathcal{H}$ *and let* $v \in \mathcal{V}$ *be a unit vector such that*

1. *For all* $T \in \mathcal{C}_A \cup \mathcal{C}_B$, T *is a channel with transmission functional* $\mathfrak{t}_T$.
2. *For all* $T \in \mathcal{C}_A$, T *is isometric on* $\mathcal{V}$.
3. *For all* $T \in \mathcal{C}_A$, $\mathfrak{t}_T|_{\mathcal{B}_1(\mathcal{V})} = 0$.
4. *For all* $T \in \mathcal{C}_B$, $\mathfrak{t}_T(|v\rangle\langle v|) = 0$.
5. $\sup_{T\in\mathcal{C}_B} \left\|\mathfrak{t}_T|_{\mathcal{B}_1(\mathcal{V})}\right\| < \infty$
6. *The set* $\mathcal{C}_A|_{\mathcal{B}_1(\mathcal{V})} := \left\{T|_{\mathcal{B}_1(\mathcal{V})} \,\middle|\, T \in \mathcal{C}_A\right\}$ *contains exactly one element.*
7. $\mathcal{C}_A|_{\mathcal{B}_1(\mathcal{V})}$ *and* $\mathcal{C}_B|_{\mathcal{B}_1(\mathcal{V})} := \left\{T|_{\mathcal{B}_1(\mathcal{V})} \,\middle|\, T \in \mathcal{C}_B\right\}$ *are disjoint.*

Then, there exist a constant C and for every $N \in \mathbb{N}$, an N-step discrimination strategy D and a two-valued POVM Π such that

$$P_e(D,\Pi) \leq \frac{C}{N^2}, \tag{4.35}$$

$$\mathfrak{T}_{T_A}(D) = 0 \quad \text{and} \quad \mathfrak{T}_{T_B}(D) \leq \frac{C}{N}, \tag{4.36}$$

for all $T_A \in \mathcal{C}_A$ and all $T_B \in \mathcal{C}_B$, where the discrimination error probability is w.r.t. the sets $\mathcal{C}_A$ and $\mathcal{C}_B$. Hence, the sets $\mathcal{C}_A$ and $\mathcal{C}_B$ can be discriminated in a transmission-free manner.

Proof. We combine Theorems 4.1 and 4.14. Let us fix some $T_A \in \mathcal{C}_A$. From Theorem 4.14 (with $T = T_A$), we obtain the map R, with the properties (1), (2), and (3). We want to apply Theorem 4.1 with $\mathcal{C} := R(\mathcal{C}_B)$. Since $\mathcal{C}_B$ is (as a closed subset of the compact set of channels) compact and R is continuous, $\mathcal{C}$ is compact and hence closed. Furthermore, since by Assumption 7, the sets $\mathcal{C}_A|_{\mathcal{B}_1(\mathcal{V})}$ and $\mathcal{C}_B|_{\mathcal{B}_1(\mathcal{V})}$ are disjoint, we have $T'|_{\mathcal{B}_1(\mathcal{V})} \neq T_A|_{\mathcal{B}_1(\mathcal{V})}$ for all $T' \in \mathcal{C}_B$. Hence, property (2) implies that for all $T \in \mathcal{C}$, the state $|q_0\rangle\langle q_0|$ is the only state that is a fixed point of T. In particular, $\mathrm{id} \notin \mathcal{C}$. Furthermore, Assumption 6 implies that $T'|_{\mathcal{B}_1(\mathcal{V})} = T_A|_{\mathcal{B}_1(\mathcal{V})}$, for all $T' \in \mathcal{C}_A$. Hence, by property (1), $R(\mathcal{C}_\mathcal{A}) = \{\mathrm{id}\}$. Thus, Theorem 4.1 yields a discrimination strategy $\tilde{D}$ and a two-valued POVM such that $P_e(\tilde{D},\Pi) \leq \tilde{C}N^{-2}$, for some constant $\tilde{C}$. By construction, $P_e(\tilde{D},\Pi)$ is the discrimination probability w.r.t. the sets $\mathcal{C}$ and $\{\mathrm{id}\}$, but since we have for $T' \in \mathcal{C}_A \cup \mathcal{C}_B$ that $R(T') \in \{\mathrm{id}\}$ iff $T' \in \mathcal{C}_A$ and $R(T') \in \mathcal{C}$ iff $R(T') \in \mathcal{C}_B$, it follows that $P_e(\tilde{D}^R,\Pi) = P_e(\tilde{D},\Pi)$, where $\tilde{D}^R$ is the transformed discrimination strategy, as defined in the main text. For $T' \in \mathcal{C}_A$, condition 3 and property (3) imply that the transformed transmission functional $\mathfrak{t}_{R(T')} = 0$. Thus, $\mathfrak{T}_{T'}(\tilde{D}^R) = 0$. Furthermore, for $T' \in \mathcal{C}_B$ with transmission functional $\mathfrak{t}_{T'}$, property (3) implies that the norm of the transformed transmission functional satisfies $\left\|\mathfrak{t}_{R(T')}\right\| = \frac{1}{2}\mathfrak{t}_{T'}\left(\frac{P^\perp}{d-1}\right) \leq \frac{1}{2}\left\|\mathfrak{t}_{T'}|_{\mathcal{B}_1(\mathcal{V})}\right\|$. Since we have $\mathfrak{T}_{T'}(\tilde{D}^R) = \mathfrak{T}_{R(T')}(\tilde{D})$, Theorem 4.1 implies that $\mathfrak{T}_{T'}(D^R) \leq \frac{\tilde{C}\left\|\mathfrak{t}_{T'}|_{\mathcal{B}_1(\mathcal{V})}\right\|}{2N}$. We finish the proof by identifying D with $\tilde{D}^R$ and defining

$$C := \max\left[\tilde{C}, \frac{\tilde{C}}{2}\sup_{T' \in \mathcal{C}_B}\left\|\mathfrak{t}_{T'}|_{\mathcal{B}_1(\mathcal{V})}\right\|\right] < \infty. \tag{4.37}$$

□

As a direct consequence of the previous result, we get the validity of Theorem 2.5.

Proof. (Theorem 2.5) We interpret every channel T with "interaction" functional $\mathfrak{i}_T$ as channel with transmission functional $\mathfrak{i}_T$. By Lemma 3.8, it suffices to check Conditions 1-7 of Corollary 4.15. 1, 2, 6, and 7 follow by assumption and 3, 4, and 5 follow directly from Lemma 3.10 (6). □

The remainder of this section is devoted to the proof of Theorem 4.14. We show that the transformation depicted in Fig. 8 has the desired properties. We

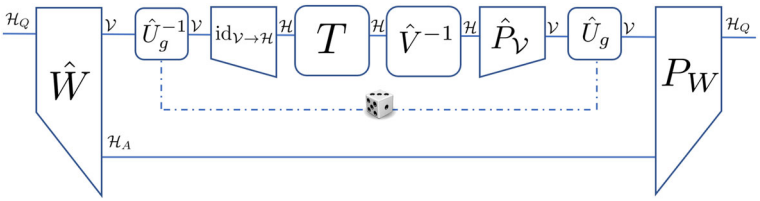

FIGURE 8. The reduction superchannel for $\dim(\mathcal{V}) > 1$

define this superchannel precisely in the proof of Theorem 4.14. An important part is the so-called twirling operation, which we study here for a special group.

Lemma 4.16 (Twirling). *For $2 \leq d := \dim(\mathcal{H}) < \infty$, let $v \in \mathcal{H}$ be a unit vector and set $V_v := \mathrm{span}\{v\}$. We define the group*

$$G := \left\{ g = \mathbb{1}_{V_v} \oplus U_g \in \mathcal{B}(V_v \oplus V_v^\perp) \,\middle|\, U_g \in \mathcal{B}(V_v^\perp) \text{ is unitary} \right\} \tag{4.38}$$

and the twirling superchannel $S : \mathcal{B}(\mathcal{B}_1(\mathcal{H})) \to \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ by

$$S(T) = \int \hat{U}_g \circ T \circ \hat{U}_g^{-1} \, \mathrm{d}\mu_G(g), \tag{4.39}$$

where μ_G is the Haar measure on G and $\hat{U}_g : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ is the quantum channel obtained by conjugation with the group element $g \in G$, i.e., $\hat{U}_g(\cdot) = g \cdot g^{-1}$. Then, the following statements hold.

- *Let $\psi \in V_v^\perp$ be any unit vector and $\phi := \frac{1}{\sqrt{2}}(v + \psi)$. If $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ is a channel and $|\phi\rangle\langle\phi|$ is a fixed point of $S(T)$, then $T = \mathrm{id}$. Conversely, $S(\mathrm{id}) = \mathrm{id}$ and thus $|\phi\rangle\langle\phi|$ is a fixed point of $S(\mathrm{id})$.*
- *For a functional $\mathfrak{t} : \mathcal{B}_1(\mathcal{H}) \to \mathbb{C}$, we have*

$$\int \mathfrak{t} \circ \hat{U}_g^{-1} \, \mathrm{d}\mu_G(g) = \mathfrak{t}\left(\frac{P^\perp}{d-1}\right) \mathrm{tr}\left[P^\perp \cdot\right] + \mathfrak{t}(|v\rangle\langle v|) \, \mathrm{tr}\left[|v\rangle\langle v| \cdot\right]. \tag{4.40}$$

Remark 4.17. The integration over the Haar measure can be replaced by a unitary t-design [34]. We can thus implement the superchannel S without using an ancillary quantum system.

Proof. We start by showing that the range of S is spanned by the following seven operators:

$$\begin{aligned}
&\mathrm{tr}\left[|v\rangle\langle v| \cdot\right] |v\rangle\langle v|, && \mathrm{tr}\left[P^\perp \cdot\right] |v\rangle\langle v|, && \mathrm{tr}\left[|v\rangle\langle v| \cdot\right] \frac{P^\perp}{d-1}, \\
&\mathrm{tr}\left[P^\perp \cdot\right] \frac{P^\perp}{d-1}, && P^\perp \cdot |v\rangle\langle v|, && |v\rangle\langle v| \cdot P^\perp, \\
& && && P^\perp \cdot P^\perp - \mathrm{tr}\left[P^\perp \cdot\right] \frac{P^\perp}{d-1}.
\end{aligned} \tag{4.41}$$

Using the definition of the Haar measure, we obtain that the range of S consists of precisely those operators $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ that commute with $\hat{U}_g$ for all $g \in G$. We calculate the commutant on the level of Choi matrices. To this end,

we identify $\mathcal{B}_1(\mathcal{H})$ with $\mathcal{H}\otimes\mathcal{H}$ via the Choi isomorphism ($|h_i\rangle\langle h_j| \leftrightarrow h_i\otimes h_j$), where $h_0, h_1, \dots h_{d-1}$ is an orthonormal basis of $\mathcal{H}$ such that $h_0 = v$. The operator corresponding to $\hat{U}_g$ is $g\otimes\overline{g}$, where the complex conjugation is w.r.t the aforementioned basis. We can rewrite this operator as:

$$\begin{aligned} g\otimes\overline{g} &= (\mathbb{1}_{V_v}\oplus U_g)\otimes(\mathbb{1}_{V_v}\oplus\overline{U}_g)\\ &= (\mathbb{1}_{V_v}\otimes\mathbb{1}_{V_v})\oplus(\mathbb{1}_{V_v}\otimes\overline{U}_g)\oplus(U_g\otimes\mathbb{1}_{V_v})\oplus(U_g\otimes\overline{U}_g). \end{aligned}$$

The maps $g\mapsto\mathbb{1}_{V_v}\otimes\mathbb{1}_{V_v}$, $g\mapsto\mathbb{1}_{V_v}\oplus\overline{U}_g$, and $g\mapsto U_g\otimes\mathbb{1}_{V_v}$ are inequivalent irreducible representations of G. If $d=2$, the representation $g\mapsto(U_g\otimes\overline{U}_g)$ is the trivial 1-dimensional representation. A simple consequence of Schur's lemma is that the commutant then is $2^2+1^2+1^2=6$ dimensional (see [35], p. 60 for the dimension formula). For $d=2$, the span of the operators in (4.41) is also 6-dimensional ($P^\perp\cdot P^\perp - \mathrm{tr}\left[P^\perp\cdot\right]\frac{P^\perp}{d-1}=0$). So in this case, we have proven the claim. If $d\geq 3$, then the representation $g\mapsto(U_g\otimes\overline{U}_g)$ is the direct sum of the trivial 1-dimensional representation and an irreducible $((d-1)^2-1)$-dimensional representation (see [36]). Hence, the dimension of the commutant is $2^2+1^2+1^2+1^2=7$. Also, the dimension of the span of the operators in (4.41) is 7-dimensional. This proves that the range of S is indeed given by the span of the operators in (4.41).

For our first claim, we clearly have $S(\mathrm{id})=\mathrm{id}$. Conversely, let T be a channel such that $|\phi\rangle\langle\phi|$ is a fixed point of $S(T)$. Let $\alpha_1,\alpha_2,\dots,\alpha_7$ be the coefficients of an expansion of $S(T)$ in terms of the operators in (4.41). Note that for $d=2$, this expansion is not unique but can be made that way by demanding $\alpha_7:=1$. As $|\phi\rangle\langle\phi|$ is a fixed point of $S(T)$, we have

$$\begin{aligned} |\phi\rangle\langle\phi| &= \frac{1}{2}\left(|v\rangle\langle v| + |v\rangle\langle\psi| + |\psi\rangle\langle v| + |\psi\rangle\langle\psi|\right)\\ &= S(T)(|\phi\rangle\langle\phi|)\\ &= \frac{1}{2}\Bigg((\alpha_1+\alpha_2)|v\rangle\langle v| + (\alpha_3+\alpha_4-\alpha_7)\frac{P^\perp}{d-1} + \alpha_5|\psi\rangle\langle v| + \alpha_6|v\rangle\langle\psi|\\ &\qquad + \alpha_7|\psi\rangle\langle\psi|\Bigg). \end{aligned}$$

By comparing the second and the last expression, it follows that $\alpha_1+\alpha_2=1$ and $\alpha_5=\alpha_6=1$. If $d=2$, then $P^\perp=|\psi\rangle\langle\psi|$ and $\alpha_3+\alpha_4=1$. Otherwise, we have $\alpha_7=1$ and $\alpha_3+\alpha_4-\alpha_7=0$, hence also $\alpha_3+\alpha_4=1$. Furthermore,

$$\begin{aligned} S(T)(|v\rangle\langle v|) &= \alpha_1|v\rangle\langle v| + \alpha_3\frac{P^\perp}{d-1},\\ S(T)(|\psi\rangle\langle\psi|) &= \alpha_2|v\rangle\langle v| + (\alpha_4-\alpha_7)\frac{P^\perp}{d-1} + \alpha_7|\psi\rangle\langle\psi|. \end{aligned} \tag{4.42}$$

As $S(T)$ is trace-preserving, we obtain $\alpha_1+\alpha_3=1$ and $\alpha_3+\alpha_4=1$. Our equations imply that $\alpha_2=1-\alpha_1, \alpha_3=1-\alpha_1$, and $\alpha_4=\alpha_1$. Positivity of $S(T)$ in (4.42) implies that $\alpha_1\geq 0$ and $\alpha_3\geq 0$. Thus, $0\leq\alpha_1\leq 1$. We want to show that complete positivity of $S(T)$ even implies $\alpha_1=1$. To this end, we

define $\mathcal{H}_A := \mathrm{span}\{v, \psi\}$ and $\Omega^+, \Omega^- \in \mathcal{H}_A \otimes \mathcal{H}$ by

$$\Omega^+ := v \otimes v + \psi \otimes \psi, \qquad \Omega^- := v \otimes v - \psi \otimes \psi.$$

As $S(T)$ is completely positive, we have

$$\begin{aligned}
0 &\leq \langle \Omega^- | (\mathrm{id}_A \otimes S(T))(|\Omega^+\rangle\langle\Omega^+|)\ \Omega^- \rangle \\
&= \langle \Omega^- | \left(|v\rangle\langle v| \otimes \left(\alpha_1 |v\rangle\langle v| + (1-\alpha_1)\frac{P^\perp}{d-1} \right) \right)\ \Omega^- \rangle \\
&\quad + \langle \Omega^- | \left(|\psi\rangle\langle v| \otimes |\psi\rangle\langle v| \right)\ \Omega^- \rangle + \langle \Omega^- | \left(|v\rangle\langle\psi| \otimes |v\rangle\langle\psi| \right)\ \Omega^- \rangle \\
&\quad + \langle \Omega^- | \left(|\psi\rangle\langle\psi| \otimes \left((1-\alpha_1)|v\rangle\langle v| + \alpha_1 \frac{P^\perp}{d-1} + |\psi\rangle\langle\psi| - \frac{P^\perp}{d-1} \right) \right)\ \Omega^- \rangle \\
&= \alpha_1 - 2 + \frac{\alpha_1 - 1}{d-1} + 1 \\
&= d\frac{\alpha_1 - 1}{d-1}.
\end{aligned}$$

Thus, $\alpha_1 \geq 1$. This further implies that $\alpha_1 = 1, \alpha_2 = 0, \alpha_3 = 0$, and $\alpha_4 = 1$. Together with the earlier result that $\alpha_5 = \alpha_6 = \alpha_7 = 1$, we obtain

$$\begin{aligned}
S(T) = \mathrm{tr}\left[|v\rangle\langle v| \cdot\right] |v\rangle\langle v| + \mathrm{tr}\left[P^\perp \cdot\right] \frac{P^\perp}{d-1} + P^\perp \cdot |v\rangle\langle v| + |v\rangle\langle v| \cdot P^\perp \\
+ P^\perp \cdot P^\perp - \mathrm{tr}\left[P^\perp \cdot\right] \frac{P^\perp}{d-1} \\
= \mathrm{id}.
\end{aligned}$$

Thus, we have shown that if $|\phi\rangle\langle\phi|$ is a fixed point of $S(T)$, then $S(T) = \mathrm{id}$. To see that this also implies that $T = \mathrm{id}$, we note that $S(T)$ is a convex combination of the channels $\hat{U}_g \circ T \circ \hat{U}_g^{-1}$. But as the identity is an extremal element of the convex set of quantum channels, $\hat{U}_g \circ T \circ \hat{U}_g^{-1}$ must be proportional to the identity μ_G-almost everywhere. In particular, $\hat{U}_g \circ T \circ \hat{U}_g^{-1} = \mathrm{id}$, for some $g \in G$. Thus, $T = \mathrm{id}$. This proves the first claim.

It remains to prove the second claim. For $\mathfrak{t}(\cdot) = \mathrm{tr}\left[L \cdot\right]$ and $\rho \in \mathcal{B}_1(\mathcal{H})$, we have

$$S'(\mathfrak{t})(\rho) := \int \mathfrak{t} \circ \hat{U}_g^{-1}(\rho)\, \mathrm{d}\mu_G(g) = \mathrm{tr}\left[\int gLg^{-1}\, \mathrm{d}\mu_G(g)\ \rho \right].$$

By the definition of the Haar measure, the integral must commute with all $g \in G$. The representation $g \mapsto \mathbb{1}_{V_v} \oplus U_g$ is the sum of two inequivalent irreducible representations of G. Thus, the commutant is 2-dimensional. It is easy to check that $P^\perp$ and $|v\rangle\langle v|$ are in the commutant. Thus,

$$\int gLg^{-1}\, \mathrm{d}\mu_G(g) = \lambda_1 P^\perp + \lambda_2 |v\rangle\langle v|,$$

for some $\lambda_1, \lambda_2 \in \mathbb{C}$. Therefore, we can write

$$S'(\mathfrak{t})(\rho) = \lambda_1 \mathrm{tr}\left[P^\perp \rho\right] + \lambda_2 \mathrm{tr}\left[|v\rangle\langle v|\rho\right].$$

Substituting $P^\perp$ and $|v\rangle\langle v|$ for ρ yields $\lambda_1 = (d-1)^{-1} S'(\mathfrak{t})(P^\perp)$ and $\lambda_2 = S'(\mathfrak{t})(|v\rangle\langle v|)$. As $P^\perp$ and $|v\rangle\langle v|$ commute with all $g \in G$, we have

$$S'(\mathfrak{t})(P^\perp) = \mathfrak{t}\left(\int g^{-1} P^\perp g \, \mathrm{d}\mu_G(g)\right) = \mathfrak{t}(P^\perp),$$
$$S'(\mathfrak{t})(|v\rangle\langle v|) = \mathfrak{t}\left(\int g^{-1} |v\rangle\langle v| g \, \mathrm{d}\mu_G(g)\right) = \mathfrak{t}(|v\rangle\langle v|).$$

We plug this into (4.43) and obtain the desired result, Eq. (4.40). Thus, we have proven our last claim. □

We are now ready to prove Theorem 4.14.

Proof. As already mentioned, the proof consists of an explicit construction of the superchannel R. The construction is depicted in Fig. 8. We start by defining the components of this circuit from left to right. For the definition of the first component, we define $\mathcal{H}_A$ to be a two-dimensional Hilbert space with orthonormal basis $\{a_0, a_1\}$. The channel $\hat{W} : \mathcal{B}_1(\mathcal{H}_Q) \to \mathcal{B}_1(\mathcal{V} \otimes \mathcal{H}_A)$ is defined by $\hat{W}(\cdot) = W \cdot W^\dagger$, with isometry $W : \mathcal{H}_Q \to \mathcal{V} \otimes \mathcal{H}_A$ defined by

$$Wq_0 = v \otimes a_0,$$
$$Wq_1 = \begin{cases} \frac{1}{\sqrt{2}}(v+\psi) \otimes a_1, & \text{if } \dim(\mathcal{V}) > 1 \\ v \otimes a_1, & \text{if } \dim(\mathcal{V}) = 1 \end{cases},$$

where $\psi \in \mathcal{V}$ is any unit vector that is orthogonal to v. This channel is designed in order to exhibit the second conclusion of Lemma 4.16.

The second component is the twirling operation $S : \mathcal{B}(\mathcal{B}_1(\mathcal{V})) \to \mathcal{B}(\mathcal{B}_1(\mathcal{V}))$, which is a superchannel on its own and which we only define for $\dim(\mathcal{V}) > 1$. This operation is depicted by the two unitary channels $\hat{U}_g$ and $\hat{U}_g^{-1}$ connected by a dashed line and acts as

$$S(\cdot) := \int \hat{U}_g \circ (\cdot) \circ \hat{U}_g^{-1} \, \mathrm{d}\mu_G(g), \tag{4.43}$$

where μ_G is the Haar measure on the compact group G, defined by (cf. Lemma 4.16)

$$G := \left\{ g = \mathbb{1}_{V_v} \oplus U_g \in \mathcal{B}(V_v \oplus V_v^\perp) \,\middle|\, U_g \in \mathcal{B}(V_v^\perp) \text{ is unitary} \right\},$$

with $V_v := \mathrm{span}\{v\}$. The channels $\hat{U}_g, \hat{U}_g^{-1} : \mathcal{B}_1(\mathcal{V}) \to \mathcal{B}_1(\mathcal{V})$ are defined by

$$\hat{U}_g(\cdot) := (\mathbb{1}_{V_v} \oplus U_g)(\cdot)(\mathbb{1}_{V_v} \oplus U_g^\dagger) \quad \text{and} \quad \hat{U}_g^{-1}(\cdot) := (\mathbb{1}_{V_v} \oplus U_g^\dagger)(\cdot)(\mathbb{1}_{V_v} \oplus U_g).$$

The channel $\mathrm{id}_{\mathcal{V}\to\mathcal{H}} : \mathcal{B}_1(\mathcal{V}) \to \mathcal{B}_1(\mathcal{H}), \rho \mapsto \rho$ embeds $\mathcal{B}_1(\mathcal{V})$ into $\mathcal{B}_1(\mathcal{H})$.

To define the channel $\hat{V}^{-1} : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$, we use that by assumption, T is isometric on $\mathcal{V}$. This means that there exists an isometry $\tilde{V} : \mathcal{V} \to \mathcal{H}$ such that $T|_{\mathcal{B}_1(\mathcal{V})}(\cdot) = \tilde{V} \cdot \tilde{V}^\dagger$. This isometry can be extended (in a non-unique way) to a unitary and therefore invertible operation $V : \mathcal{H} \to \mathcal{H}$. We then define

$$\hat{V}^{-1}(\cdot) := V^\dagger \cdot V.$$

We define the channel $\hat{P}_{\mathcal{V}} : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{V})$ by

$$\hat{P}_{\mathcal{V}}(\cdot) := P_{\mathcal{V}} \cdot P_{\mathcal{V}}^\dagger + \operatorname{tr}\left[(\mathbb{1} - P_{\mathcal{V}}^\dagger P_{\mathcal{V}})(\cdot)\right] |v\rangle\langle v|,$$

where $P_{\mathcal{V}} : \mathcal{H} \to \mathcal{V}$ is the orthogonal projection onto $\mathcal{V}$. To finish the channel definitions, we define the channel $P_W : \mathcal{B}_1(\mathcal{V} \otimes \mathcal{H}_A) \to \mathcal{B}_1(\mathcal{H}_Q)$ by

$$P_W(\cdot) := W^\dagger \cdot W + \operatorname{tr}\left[(\mathbb{1} - WW^\dagger)(\cdot)\right] |q_0\rangle\langle q_0|.$$

We can now define the superchannel R. If $\dim(\mathcal{V}) > 1$, we define

$$R(\cdot) := P_W \circ \left(\left[\int \hat{U}_g \circ \hat{P}_{\mathcal{V}} \circ \hat{V}^{-1} \circ (\cdot) \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}} \circ \hat{U}_g^{-1} \, \mathrm{d}\mu_G(g)\right] \otimes \mathrm{id}_A\right) \circ \hat{W}, \tag{4.44}$$

and if $\dim(\mathcal{V}) = 1$, we define

$$R(\cdot) := P_W \circ \hat{V}^{-1} \circ (\cdot) \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}} \circ \hat{W}. \tag{4.45}$$

With the definition in place, it only remains to show that the superchannel R has the claimed properties. To prove the first claim, let $T' \in \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ such that $T|_{\mathcal{B}_1(\mathcal{V})} = T'|_{\mathcal{B}_1(\mathcal{V})}$. For $\dim(\mathcal{V}) > 1$, we use that by construction $\hat{V}^{-1} \circ T'|_{\mathcal{B}_1(\mathcal{V})} = \mathrm{id}_{\mathcal{V}}$ and that operators in $\mathcal{B}_1(\mathcal{V})$ are fixed points of $P_{\mathcal{V}}$. We get

$$\begin{aligned} R(T') &= P_W \circ \left(\left[\int \hat{U}_g \circ \mathrm{id}_{\mathcal{V}} \circ \hat{U}_g^{-1} \, \mathrm{d}\mu_G(g)\right] \otimes \mathrm{id}_A\right) \circ \hat{W} \\ &= P_W \circ \hat{W} \\ &= \mathrm{id}_Q. \end{aligned}$$

By means of a similar argument, it follows that the claim also holds for $\dim(\mathcal{V}) = 1$. To prove the second claim, we start by showing that $|q_0\rangle\langle q_0|$ is a fixed point of $R(T')$, for every channel T'. For $\dim(\mathcal{V}) > 1$, we have

$$\begin{aligned} R(T')(|q_0\rangle\langle q_0|) &= P_W \circ \left(S(\hat{P}_{\mathcal{V}} \circ \hat{V}^{-1} \circ T' \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}}) \otimes \mathrm{id}_A\right) \circ W(|q_0\rangle\langle q_0|) \\ &= P_W \left(S(\hat{P}_{\mathcal{V}} \circ \hat{V}^{-1} \circ T' \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}})(|v\rangle\langle v|) \otimes |a_0\rangle\langle a_0|\right) \\ &= |q_0\rangle\langle q_0|, \end{aligned}$$

where the last line follows as P_W maps every state of the form $\sigma \otimes |a_0\rangle\langle a_0|$ to $|q_0\rangle\langle q_0|$. An analogous argument yields that $|q_0\rangle\langle q_0|$ is also a fixed point of $R(T')$ if $\dim(\mathcal{V}) = 1$. Conversely, assume that $T' \in \mathcal{B}(\mathcal{B}_1(\mathcal{H}))$ is a channel such that $T|_{\mathcal{B}_1(\mathcal{V})} \neq T'|_{\mathcal{B}_1(\mathcal{V})}$ and $\rho \in \mathcal{S}(\mathcal{H}_Q)$ is a fixed point of $R(T')$. We prove that $\rho = |q_0\rangle\langle q_0|$. We do so by first showing that if $\rho \neq |q_0\rangle\langle q_0|$, then $|q_1\rangle\langle q_1|$ is also a fixed point of $R(T')$, which will lead to a contradiction. By part 1 of the theorem, $|q_0\rangle\langle q_0|$ is a fixed point of $R(T')$. Hence, Lemma 4.4 implies that $\operatorname{span}\{|q_0\rangle\langle q_1|\}$ and $\operatorname{span}\{|q_1\rangle\langle q_0|\}$ are invariant subspaces of $R(T')$. Thus,

$$\langle q_0 | R(T')(|q_0\rangle\langle q_1|)\, q_0\rangle = \langle q_0 | R(T')(|q_1\rangle\langle q_0|)\, q_0\rangle = 0.$$

We then have

$$\begin{aligned}\langle q_0|\rho\, q_0\rangle &= \langle q_0|R(T')(\rho)\, q_0\rangle \\ &= \sum_{i,j=0}^{1} \langle q_i|\rho\, q_j\rangle\langle q_0|R(T')(|q_i\rangle\langle q_j|)\, q_0\rangle \\ &= \sum_{i=0}^{1} \langle q_i|\rho\, q_i\rangle\langle q_0|R(T')(|q_i\rangle\langle q_i|)\, q_0\rangle \\ &= \langle q_0|\rho\, q_0\rangle + \langle q_1|\rho\, q_1\rangle\langle q_0|R(T')(|q_1\rangle\langle q_1|)\, q_0\rangle.\end{aligned}$$

Hence,

$$\langle q_1|\rho\, q_1\rangle\langle q_0|R(T')(|q_1\rangle\langle q_1|)\, q_0\rangle = 0.$$

If $\langle q_1|\rho\, q_1\rangle = 0$, then positivity of ρ implies that $\rho = |q_0\rangle\langle q_0|$, which contradicts the assumption that $\rho \neq |q_0\rangle\langle q_0|$. It follows that

$$\langle q_0|R(T')(|q_1\rangle\langle q_1|)\, q_0\rangle = 0.$$

Positivity of $R(T')(\rho)$ yields $R(T')(|q_1\rangle\langle q_1|) = |q_1\rangle\langle q_1|$, which shows that $|q_1\rangle\langle q_1|$ is a fixed point of $R(T')$. We now show that this leads to a contradiction. With the abbreviations $\tilde{S} := S(\hat{P}_{\mathcal{V}} \circ \hat{V}^{-1} \circ T' \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}})$ and $\phi := \frac{1}{\sqrt{2}}(v+\psi)$, we get

$$\begin{aligned}|q_1\rangle\langle q_1| &= R(T')(|q_1\rangle\langle q_1|) \\ &= P_W\left(\tilde{S}(|\phi\rangle\langle\phi|) \otimes |a_1\rangle\langle a_1|\right) \\ &= \mathrm{tr}\left[|\phi\rangle\langle\phi|\, \tilde{S}(|\phi\rangle\langle\phi|)\right] |q_1\rangle\langle q_1| + \mathrm{tr}\left[(\mathbb{1} - WW^\dagger)\, \tilde{S}(|\phi\rangle\langle\phi|)\right] |q_0\rangle\langle q_0|.\end{aligned}$$

Comparing the last with the first line implies that $\mathrm{tr}\left[|\phi\rangle\langle\phi|\, \tilde{S}(|\phi\rangle\langle\phi|)\right] = 1$. We observe the latter equation says that the Cauchy–Schwarz inequality (w.r.t. the Hilbert–Schmidt inner product) is satisfied with equality. Thus, $\tilde{S}(|\phi\rangle\langle\phi|) = |\phi\rangle\langle\phi|$. Lemma 4.16 then implies

$$\hat{P}_{\mathcal{V}} \circ \hat{V}^{-1} \circ T' \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}} = \mathrm{id}_{\mathcal{V}}.$$

Note that $P_{\mathcal{V}}$ is the sum of the two completely positive trace non-increasing maps, $P_1(\cdot) := P_{\mathcal{V}} \cdot P_{\mathcal{V}}$ and $P_2(\cdot) := \mathrm{tr}\left[(\mathbb{1} - P_{\mathcal{V}}^\dagger P_{\mathcal{V}})(\cdot)\right] |v\rangle\langle v|$. Thus, with the appropriate normalization, the extremal point of the convex set of completely positive maps, $\mathrm{id}_{\mathcal{V}}$, can be written as a convex combination of $P_i \circ \hat{V}^{-1} \circ T' \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}}$. Thus,

$$\hat{V}^{-1} \circ T' \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}} = \mathrm{id}_{\mathcal{V}\to\mathcal{H}}. \tag{4.46}$$

As $\hat{V}^{-1}$ is invertible and $T' \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}}$, identity (4.46) is equivalent to

$$T'|_{\mathcal{B}_1(\mathcal{V})} = \hat{V}|_{\mathcal{B}_1(\mathcal{V})}.$$

By construction of $\hat{V}$, the RHS equals $T|_{\mathcal{B}_1(\mathcal{V})}$. But this contradicts the assumption that $T|_{\mathcal{B}_1(\mathcal{V})} \neq T'|_{\mathcal{B}_1(\mathcal{V})}$. Thus, $|q_1\rangle\langle q_1|$ cannot be a fixed point of $R(T')$. Consequently, $\rho = |q_0\rangle\langle q_0|$, which proves that $|q_0\rangle\langle q_0|$ is the only state

that is a fixed point of $R(T')$. This proves the second claim. To prove the third claim, we must calculate how our protocol transforms the transmission functional. For $\dim(\mathcal{V}) = 1$, we get directly from the definition (4.45) that $\mathfrak{t}_{R(T)}(\cdot) = \mathrm{tr}\,[\cdot]\,\mathfrak{t}_T(|v\rangle\langle v|) = 0$. For $\dim(\mathcal{V}) > 1$, the transmission functional $\mathfrak{t}_T$ transforms to $\mathfrak{t}_{R(T)}$, given by

$$\mathfrak{t}_{R(T)} := \int \mathfrak{t}_T \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}} \circ \hat{U}_g^{-1} \circ \mathrm{tr}_A \circ \hat{W}\, \mathrm{d}\mu_G(g). \tag{4.47}$$

To evaluate (4.47), we use (4.40) and get

$$\mathfrak{t}_{R(T)}(\cdot) = \mathfrak{t}_T \circ \mathrm{id}_{\mathcal{V}\to\mathcal{H}} \left(\frac{P^\perp}{d-1}\right) \mathrm{tr}\left[P^\perp \mathrm{tr}_A\left[\hat{W}(\cdot)\right]\right].$$

A direct calculation then yields the claim. □

Remark 4.18. With our protocol, we achieved a transformation from channels on $\mathcal{H}$ to qubit channels with certain properties. This was achieved by using classical communication and one ancillary qubit. To demonstrate that our implementation of this transformation uses the quantum resources in the most economic way possible, we show that in general one cannot use only classical communication to implement a transformation which has the desired properties. To this end, we consider the following procedure. First, we use an instrument to transform the state and to obtain classical information. Then, we apply the channel, which should be transformed. Afterwards, we apply some quantum channel, where the choice of the channel may depend on the classical information that we obtained in the first step. Our instrument described by a collection of nonzero quantum operations $I_1, I_2, \ldots, I_N$, such that $\sum_i I_i$ is trace-preserving. We denote the associated channels that are applied in the last step by $\Lambda_1, \Lambda_2, \ldots, \Lambda_N$. Our protocol then implements the following transformation:

$$T \mapsto \sum_i \Lambda_i \circ T \circ I_i. \tag{4.48}$$

Assume that the channel T of the Theorem 4.14 is the identity and $\dim(\mathcal{H}) = \dim(\mathcal{V}) = 2$. Our first requirement is that $\mathrm{id} \mapsto \mathrm{id}$. Thus,

$$\mathrm{id} = \sum_i \Lambda_i \circ I_i. \tag{4.49}$$

Since id is an extreme point of the convex set of quantum operations, there must be non-negative coefficients $p_1, p_2, \ldots, p_N$, such that

$$\Lambda_i \circ I_i = p_i \cdot \mathrm{id}, \text{ for } i = 1, 2, \ldots, N. \tag{4.50}$$

This implies that Λ_i and I_i must be proportional to a unitary conjugation, i.e., $\Lambda_i(\cdot) = U_i^\dagger \cdot U_i$ and $I_i(\cdot) = p_i U_i \cdot U_i^\dagger$, for some unitary operator U_i. Our second requirement is that (since $\mathcal{V} = \mathcal{H}$) every channel except id must be transformed to a state whose only fixed point is $|q_0\rangle\langle q_0| =: P_0$. In particular,

for the pinching channel, defined by $T_P(\cdot) = P_0 \cdot P_0 + P_1 \cdot P_1$, with $P_1 := \mathbb{1} - P_0$, we have

$$P_0 = \sum_i \sum_{j=0}^{1} p_i (U_i^\dagger P_j U_i) P_0 (U_i^\dagger P_j U_i). \tag{4.51}$$

Since P_0 is an extremal point of the convex set $\{\rho \geq 0 \,|\, \mathrm{tr}\,[\rho] \leq 1\}$, we get that

$$(U_i^\dagger P_j U_i) P_0 (U_i^\dagger P_j U_i) = \lambda_{ij} P_0, \tag{4.52}$$

for some $\lambda_{ij} \geq 0$. From this, we conclude that either $U_i^\dagger P_j U_i = P_0$ or $U_i^\dagger P_j U_i = P_1$. But then the application of the transformed channel to P_1 yields

$$\sum_i \sum_{j=0}^{1} p_i (U_i^\dagger P_j U_i) P_1 (U_i^\dagger P_j U_i) = P_1. \tag{4.53}$$

Thus, P_0 is not the only state that is a fixed point of the transformed channel. Hence, to achieve our transformation, an ancillary system is needed.

5. No-Go Results

In this section, we consider the case for which we claimed in our main theorem that it is impossible to discriminate two channels in an "interaction-free" manner. There are two major results in this section: Theorem 5.7 which claims an inequality between the error probability and the "interaction" probability; and Theorem 5.9, which claims that, under a certain condition, the best achievable rate (in terms of the number of channel uses, N) for the "interaction" probability is proportional to N^{-1}. Both theorems are consequences of our main technical results: Propositions 5.2 and 5.3. The proof techniques for these results are inspired by the techniques used in two papers by Mitchison, Massar, and Pironio [11,12], who proved an analogous no-go result for the special case of a semitransparent object. Before we state the first proposition, we define a quantity that will appear as proportionality constant in the results of this section. As this may seem complicated, we want to stress that in all relevant cases, $C_{\mathcal{V},\mathcal{W}}^{(T_A^\downarrow, T_B^\downarrow)}$ can be bounded by 2.

Definition 5.1. For $\dim(\mathcal{H}) < \infty$, let $T_A^\downarrow, T_B^\downarrow : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be two linear maps, let $\mathcal{V}$ be a linear subspace of $\mathcal{H}$, and let $\mathcal{W} = \{\mathcal{W}_1, \mathcal{W}_2, \ldots, \mathcal{W}_K\}$ be a collection of mutually orthogonal subspaces of $\mathcal{V}^\perp$ with the property that $\mathcal{V}^\perp = \mathcal{W}_1 \oplus \mathcal{W}_2 \oplus \cdots \oplus \mathcal{W}_K$. Furthermore, let P and $P_1, P_2, \ldots, P_K$ be the orthogonal projections onto $\mathcal{V}$ and $\mathcal{W}_1, \mathcal{W}_2, \ldots \mathcal{W}_K$.

We define the quantity $C_{\mathcal{V},\mathcal{W}}^{(T_A^\downarrow, T_B^\downarrow)}$ to be the infimum of the (possibly empty) set of real numbers r with the property that there exists a finite-dimensional Hilbert space $\mathcal{H}_E$, isometries $V_A, V_B : \mathcal{H} \to \mathcal{H}_E \otimes \mathcal{H}$, and orthogonal projections $P_A, P_B : \mathcal{H}_E \to \mathcal{H}_E$ such that[14]

$$r = \max_{1 \leq k \leq K} \left\| P_k ({V_A}^\dagger (P_A P_B \otimes \mathbb{1}) V_B - \mathbb{1}) P_k \right\|, \tag{5.1a}$$

[14] $\|\cdot\|$ is the operator norm on $\mathcal{B}(\mathcal{H})$.

$$V_A P = V_B P, \tag{5.1b}$$

$$T_X^{\downarrow}(\cdot) = \mathrm{tr}_E \left[(P_X \otimes \mathbb{1}) V_X \cdot V_X^{\dagger} \right], \tag{5.1c}$$

for $X \in \{A, B\}$.

We are now ready to state the first important proposition, which establishes, for a single channel use, an uncertainty relation between the "information-gain" (RHS of (5.2)) about the identity of the channel (is it T_A or T_B?) and a quantity that depends on the probability that if we would measure the input states, we would find that they are supported in the orthogonal complement of a subspace $\mathcal{V}$. Later on, this subspace will be chosen to be a maximum vacuum subspace.

Proposition 5.2 (Information-interaction tradeoff). *For* $\dim(\mathcal{H}) < \infty$, *let* $T_A^{\downarrow}$, $T_B^{\downarrow} : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *be quantum operations and let* $\mathcal{V}$ *be a subspace of* $\mathcal{H}$ *such that* $T_A^{\downarrow}|_{\mathcal{B}_1(\mathcal{V})}$ *is trace-preserving and* $T_A^{\downarrow}|_{\mathcal{B}_1(\mathcal{V})} = T_B^{\downarrow}|_{\mathcal{B}_1(\mathcal{V})}$. *Let* $\mathcal{W} = \{\mathcal{W}_1, \mathcal{W}_2, \ldots, \mathcal{W}_K\}$ *be a collection of mutually orthogonal subspaces of* $\mathcal{V}^{\perp}$, *such that* $\mathcal{V}^{\perp} = \mathcal{W}_1 \oplus \mathcal{W}_2 \oplus \cdots \oplus \mathcal{W}_K$. *Denote the orthogonal projections onto these subspaces by* $P_1, P_2, \ldots, P_K$. *Then,* $C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \leq 2$ *and*

$$\sqrt{F}(\rho, \sigma) - \sqrt{F}(T_A^{\downarrow}(\rho), T_B^{\downarrow}(\sigma)) \leq C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \sum_{k=1}^{K} \sqrt{\mathrm{tr}\,[P_k \rho]\,\mathrm{tr}\,[P_k \sigma]}, \tag{5.2}$$

for all $\rho, \sigma \geq 0$.

Before proving the proposition, let us remark that Proposition 2.10 is a direct consequence thereof.

Proof. (Proposition 2.10) This follows directly from the fact that the fidelity can be characterized in terms of the minimum over measurements of expressions of the form given on the RHS of (5.2) (see [25], p. 412). □

Proof. (Proposition 5.2) We first establish that $C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \leq 2$. Let P, $P^{\perp}$ be the orthogonal projections onto $\mathcal{V}$ and $\mathcal{V}^{\perp}$. By applying the triangular inequality and the sub-multiplicativity of the operator norm to the definition of $C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})}$, it follows that if there exist $\mathcal{H}_E, V_A, V_B, P_A$, and P_B with the properties of Definition 5.1, then $C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \leq 2$. Therefore, we start our proof by showing the existence of the aforementioned quantities. It is a basic property of completely positive trace non-increasing maps (see [25], p. 365) that there exist finite-dimensional Hilbert spaces $\mathcal{H}_{E_A}$ and $\mathcal{H}_{E_B}$, isometries $\tilde{V}_A : \mathcal{H} \to \mathcal{H}_{E_A} \otimes \mathcal{H}$ and $\tilde{V}_B : \mathcal{H} \to \mathcal{H}_{E_B} \otimes \mathcal{H}$, and orthogonal projections $\tilde{P}_A : \mathcal{H}_{E_A} \to \mathcal{H}_{E_A}$ and $\tilde{P}_B : \mathcal{H}_{E_B} \to \mathcal{H}_{E_B}$, such that $T_A^{\downarrow}(\cdot) = \mathrm{tr}_{E_A} \left[(\tilde{P}_A \otimes \mathbb{1}) \tilde{V}_A \cdot \tilde{V}_A^{\dagger} \right]$ and $T_B^{\downarrow}(\cdot) = \mathrm{tr}_{E_B} \left[(\tilde{P}_B \otimes \mathbb{1}) \tilde{V}_B \cdot \tilde{V}_B^{\dagger} \right]$. By enlarging the smaller of the two ancillary Hilbert spaces and identifying two orthonormal basis, we can achieve that $\mathcal{H}_{E_A}$ and $\mathcal{H}_{E_B}$ are the same space, $\mathcal{H}_E$. By assumption, $T_A|_{\mathcal{B}_1(\mathcal{V})}$ and $T_B|_{\mathcal{B}_1(\mathcal{V})}$ are trace-preserving. It follows that $(\tilde{P}_A \otimes \mathbb{1})\tilde{V}_A|_{\mathcal{V}}$ and $(\tilde{P}_A \otimes \mathbb{1})\tilde{V}_B|_{\mathcal{V}}$ are isometries and

thus $(\tilde{P}_A \otimes \mathbb{1})\tilde{V}_A|_{\mathcal{V}} = \tilde{V}_A|_{\mathcal{V}}$ and $(\tilde{P}_B \otimes \mathbb{1})\tilde{V}_B|_{\mathcal{V}} = \tilde{V}_B|_{\mathcal{V}}$. Hence, $\tilde{V}_A|_{\mathcal{V}}$ and $\tilde{V}_B|_{\mathcal{V}}$ are Stinespring isometries of the same channel and thus are related by a unitary operator on $\mathcal{H}_E$. Precisely, there exists a unitary operator $W : \mathcal{H}_E \to \mathcal{H}_E$ such that $\tilde{V}_B|_{\mathcal{V}} = (W \otimes \mathbb{1})\tilde{V}_A|_{\mathcal{V}}$. Equivalently, $\tilde{V}_B P = (W \otimes \mathbb{1})\tilde{V}_A P$. It is then easy to verify that the operators $V_A := (W \otimes \mathbb{1})\tilde{V}_A$, $V_B := \tilde{V}_B$ and $P_A := W\tilde{P}_A W^{-1}, P_B := \tilde{P}_B$ satisfy the requirements (5.1c) and (5.1b). In particular, we have

$$(P_A \otimes \mathbb{1})V_A P = V_A P = V_B P = (P_B \otimes \mathbb{1})V_B P. \tag{5.3}$$

This finishes the proof of the first part of the proposition. For the second part, we fix V_A, V_B, P_A, and P_B such that the Conditions (5.1c) and (5.1b) are satisfied. In particular, this implies that (5.3) holds. To prove the inequality, we proceed as follows: for two positive operators $\rho, \sigma \geq 0$, Uhlmann's theorem implies that there exists a finite-dimensional Hilbert space $\mathcal{H}_Q$ and two vectors $\psi, \phi \in \mathcal{H}_Q \otimes \mathcal{H}$ (purifications) such that $\mathrm{tr}_Q\,[|\psi\rangle\langle\psi|] = \rho$ and $\mathrm{tr}_Q\,[|\phi\rangle\langle\phi|] = \sigma$ and $\sqrt{F}(\rho,\sigma) = |\langle\psi|\phi\rangle|$. We further note that $(\mathbb{1}_Q \otimes (P_A \otimes \mathbb{1})V_A)|\psi\rangle$ and $(\mathbb{1}_Q \otimes (P_B \otimes \mathbb{1})V_B)|\phi\rangle$ are purifications of $T_A^{\downarrow}(\rho)$ and $T_B^{\downarrow}(\sigma)$. Hence, Uhlmann's theorem implies that

$$\sqrt{F}(T_A^{\downarrow}(\rho), T_B^{\downarrow}(\sigma)) \geq |\langle(\mathbb{1}_{\mathcal{Q}} \otimes (P_A \otimes \mathbb{1})V_A)\psi|(\mathbb{1}_{\mathcal{Q}} \otimes (P_B \otimes \mathbb{1})V_B)\phi\rangle|\,. \tag{5.4}$$

By inserting $\mathbb{1}_{\mathcal{Q}} \otimes P + \mathbb{1}_{\mathcal{Q}} \otimes P^{\perp}$ (which is equal to the identity) and expanding the scalar product, we obtain

$$\begin{aligned}
\text{RHS of (5.4)} = {} & |\langle(\mathbb{1}_Q \otimes (P_A \otimes \mathbb{1})V_A P)\psi|(\mathbb{1}_Q \otimes (P_B \otimes \mathbb{1})V_B P)\phi\rangle && \text{(5.5a)}\\
& + \langle(\mathbb{1}_Q \otimes (P_A \otimes \mathbb{1})V_A P^{\perp})\psi|(\mathbb{1}_Q \otimes (P_B \otimes \mathbb{1})V_B P)\phi\rangle && \text{(5.5b)}\\
& + \langle(\mathbb{1}_Q \otimes (P_A \otimes \mathbb{1})V_A P)\psi|(\mathbb{1}_Q \otimes (P_B \otimes \mathbb{1})V_B P^{\perp})\phi\rangle && \text{(5.5c)}\\
& + \langle(\mathbb{1}_Q \otimes (P_A \otimes \mathbb{1})V_A P^{\perp})\psi|(\mathbb{1}_Q \otimes (P_B \otimes \mathbb{1})V_B P^{\perp})\phi\rangle|. && \text{(5.5d)}
\end{aligned}$$

It is not hard to see from (5.3) that the terms (5.5b) and (5.5c) vanish. Explicitly, we have

$$\begin{aligned}
\text{(5.5b)} &= \langle(\mathbb{1}_Q \otimes (P_A \otimes \mathbb{1})V_A P^{\perp})\psi|(\mathbb{1}_Q \otimes (P_B \otimes \mathbb{1})V_B P)\phi\rangle\\
&= \langle(\mathbb{1}_Q \otimes (P_A \otimes \mathbb{1})V_A P^{\perp})\psi|(\mathbb{1}_Q \otimes (P_A \otimes \mathbb{1})V_A P)\phi\rangle\\
&= \langle(\mathbb{1}_Q \otimes V_A P^{\perp})\psi|(\mathbb{1}_Q \otimes (P_A \otimes \mathbb{1})V_A P)\phi\rangle\\
&= \langle(\mathbb{1}_Q \otimes V_A P^{\perp})\psi|(\mathbb{1}_Q \otimes V_A P)\phi\rangle\\
&= \langle\psi|(\mathbb{1}_Q \otimes P^{\perp}P)\phi\rangle\\
&= 0,
\end{aligned}$$

and similarly for (5.5c). Adding and subtracting $\langle(\mathbb{1}_Q \otimes P^{\perp})\psi|(\mathbb{1}_Q \otimes P^{\perp})\phi\rangle$ and using the inverse triangular inequality yields

$$\begin{aligned}
\text{(5.5)} \geq {} & |\langle(\mathbb{1}_Q \otimes P)\psi|(\mathbb{1}_Q \otimes P)\phi\rangle + \langle(\mathbb{1}_Q \otimes P^{\perp})\psi|(\mathbb{1}_Q \otimes P^{\perp})\phi\rangle|\\
& - |\langle(\mathbb{1}_Q \otimes (P_A \otimes \mathbb{1})V_A P^{\perp})\psi|(\mathbb{1}_Q \otimes (P_B \otimes \mathbb{1})V_B P^{\perp})\phi\rangle && \text{(5.6)}\\
& - \langle(\mathbb{1}_Q \otimes P^{\perp})\psi|(\mathbb{1}_Q \otimes P^{\perp})\phi\rangle|.
\end{aligned}$$

We further use $P^\perp P = 0$ (thus $\sqrt{F}(\rho,\sigma) = |\langle(\mathbb{1}_Q \otimes P)\psi|(\mathbb{1}_Q \otimes P)\phi\rangle + \langle(\mathbb{1}_Q \otimes P^\perp)\psi|(\mathbb{1}_Q \otimes P^\perp)\phi\rangle|$) and some rearrangement to arrive at

$$(5.6) = \sqrt{F}(\rho,\sigma) - |\langle(\mathbb{1}_Q \otimes P^\perp)\psi|(\mathbb{1}_Q \otimes P^\perp(V_A^\dagger(P_A P_B \otimes \mathbb{1})V_B - \mathbb{1})P^\perp)\phi\rangle|. \tag{5.7}$$

As by assumption, $P^\perp = \sum_k P_k$ and $P_k P_l = 0$ for $k \neq l$, we get

$$\begin{aligned}(5.7) &\geq \sqrt{F}(\rho,\sigma) - \sum_{k=1}^{K} |\langle(\mathbb{1}_Q \otimes P_k)\psi|(\mathbb{1}_Q \otimes P_k(V_A^\dagger(P_A P_B \otimes \mathbb{1})V_B - \mathbb{1})P_k)\phi\rangle| \\ &\geq \sqrt{F}(\rho,\sigma) - \sum_{k=1}^{K} \Big\{ \Big\| P_k(V_A^\dagger(P_A P_B \otimes \mathbb{1})V_B - \mathbb{1})P_k \Big\| \\ &\qquad \|(\mathbb{1}_Q \otimes P_k)\psi\| \, \|(\mathbb{1}_Q \otimes P_k)\phi\| \Big\} \\ &= \sqrt{F}(\rho,\sigma) - \sum_{k=1}^{K} \Big\| P_k(V_A^\dagger(P_A P_B \otimes \mathbb{1})V_B - \mathbb{1})P_k \Big\| \sqrt{\operatorname{tr}[P_k\rho]\operatorname{tr}[P_k\sigma]},\end{aligned} \tag{5.8}$$

where we used the Cauchy–Schwarz inequality and the sub-multiplicativity of the matrix norm to get from the first to the second line. For the last line, we used

$$\begin{aligned}\|\mathbb{1}_Q \otimes P_k\psi\|^2 &= \langle\psi|(\mathbb{1}_Q \otimes P_k)\psi\rangle = \operatorname{tr}[(\mathbb{1}_Q \otimes P_k)|\psi\rangle\langle\psi|] = \operatorname{tr}[P_k \operatorname{tr}_Q[|\psi\rangle\langle\psi|]] \\ &= \operatorname{tr}[P_k\rho]\,.\end{aligned}$$

As the only constraints that V_A, V_B, P_A, P_B, and $\mathcal{H}_E$ have to satisfy are the ones of Definition 5.1, we conclude that

$$(5.8) \geq \sqrt{F}(\rho,\sigma) - C_{\mathcal{V},\mathcal{W}}^{(T_A^\downarrow, T_B^\downarrow)} \sum_{k=1}^{K} \sqrt{\operatorname{tr}[P_k\rho]\operatorname{tr}[P_k\sigma]}.$$

This proves the claim. □

Proposition 5.2 does not allow for ancillary systems. In the following proposition, which is an iterated refinement of the preceding one, we show that this problem can be solved by applying Proposition 5.2 to $T^\downarrow \otimes \mathrm{id}$.

Proposition 5.3 (Technical no-go theorem). *For* $\dim(\mathcal{H}) < \infty$, *let* $T_A^\downarrow, T_B^\downarrow : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *be two completely positive trace non-increasing maps. Let* $\mathcal{V}$ *be a subspace of* $\mathcal{H}$ *such that* $T_A^\downarrow|_{\mathcal{B}_1(\mathcal{V})}$ *is trace-preserving and* $T_A^\downarrow|_{\mathcal{B}_1(\mathcal{V})} = T_B^\downarrow|_{\mathcal{B}_1(\mathcal{V})}$. *Let* $\mathcal{W} = \{\mathcal{W}_1, \mathcal{W}_2, \ldots, \mathcal{W}_K\}$ *be a collection of mutually orthogonal subspaces of* $\mathcal{V}^\perp$, *such that* $\mathcal{V}^\perp = \mathcal{W}_1 \oplus \mathcal{W}_2 \oplus \cdots \oplus \mathcal{W}_K$. *We denote the orthogonal projections onto these subspaces by* $P_1, P_2, \ldots, P_K$. *Furthermore, let* $T_A, T_B : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *be completely positive maps such that* $T_A - T_A^\downarrow$ *and* $T_B - T_B^\downarrow$ *are also completely positive. Then, for every finite-dimensional* N*-step discrimination*

strategy $D = (\mathcal{H}, \mathcal{H}_Z, s_0, \Lambda)$*, we have*

$$1 - \sqrt{F}(\rho_N^{T_A}, \rho_N^{T_B}) \leq C_{\mathcal{V},\mathcal{W}}^{(T_A^\downarrow, T_B^\downarrow)} \sum_{i=0}^{N-1} \sum_{k=1}^{K} \sqrt{\mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{T_A^\downarrow}\right]\right] \cdot \mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{T_B^\downarrow}\right]\right]}, \tag{5.9}$$

where ρ *is the intermediate state map of* D*. Furthermore,* $C_{\mathcal{V},\mathcal{W}}^{(T_A^\downarrow, T_B^\downarrow)} \leq 2$*.*

Corollary 5.4. *For* $\dim(\mathcal{H}) < \infty$*, let* $T_A^\downarrow, T_B^\downarrow : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *be two completely positive trace non-increasing maps. Let* $\mathcal{V}$ *be a subspace of* $\mathcal{H}$ *such that* $T_A^\downarrow|_{\mathcal{B}_1(\mathcal{V})}$ *is trace-preserving and* $T_A^\downarrow|_{\mathcal{B}_1(\mathcal{V})} = T_B^\downarrow|_{\mathcal{B}_1(\mathcal{V})}$*. Then,*

$$1 - \sqrt{F}(\rho_N^{T_A}, \rho_N^{T_B}) \leq C_{\mathcal{V},\mathcal{W}}^{(T_A^\downarrow, T_B^\downarrow)} \sum_{i=0}^{N-1} \sum_{k=1}^{K} \sqrt{\mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{T_A^\downarrow}\right]\right] \cdot \mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{T_B^\downarrow}\right]\right]}. \tag{5.10}$$

Proof. To reduce the overhead in notation, we define $\rho_i := \rho_i^{T_A}$, $\rho_i^\downarrow := \rho_i^{T_A^\downarrow}$ and $\sigma_i := \rho_i^{T_B}$, $\sigma_i^\downarrow := \rho_i^{T_B^\downarrow}$. We start to prove the proposition by showing that

$$1 - \sqrt{F}(\rho_N, \sigma_N) \leq 1 - \sqrt{F}(\rho_N^\downarrow, \sigma_N^\downarrow). \tag{5.11}$$

This inequality follows from the strong concavity of the fidelity and the observation that $\rho_N - \rho_N^\downarrow \geq 0$ and $\sigma_N - \sigma_N^\downarrow \geq 0$. The latter statement follows inductively, as $\rho_0 - \rho_0^\downarrow = 0 \geq 0$ and

$$\begin{aligned}
\rho_{i+1} - \rho_{i+1}^\downarrow &= \Lambda_i((T_A \otimes \mathrm{id})(\rho_i) - (T_A^\downarrow \otimes \mathrm{id})(\rho_i^\downarrow)) \\
&= \Lambda_i((T_A \otimes \mathrm{id})(\rho_i - \rho_i^\downarrow) + ((T_A - T_A^\downarrow) \otimes \mathrm{id})(\rho_i^\downarrow)) \\
&\geq 0.
\end{aligned}$$

The last line follows, as by induction $\rho_i - \rho_i^\downarrow \geq 0$ and $T_A - T_A^\downarrow$ is, by assumption, completely positive. Replacing ρ by σ and A by B in the argument above shows that also $\sigma_N - \sigma_N^\downarrow \geq 0$. We write $\Delta\rho := \rho_N - \rho_N^\downarrow$ and $\Delta\sigma := \sigma_N - \sigma_N^\downarrow$ and use the strong concavity (see [25], p. 414) and the non-negativity of the fidelity, to obtain the following inequality:

$$\begin{aligned}
\sqrt{F}(\rho_N, \sigma_N) &= \sqrt{F}(\rho_N^\downarrow + \Delta\rho, \sigma_N^\downarrow + \Delta\sigma) \\
&\geq \sqrt{F}(\rho_N^\downarrow, \sigma_N^\downarrow) + \sqrt{F}(\Delta\rho, \Delta\sigma) \\
&\geq \sqrt{F}(\rho_N^\downarrow, \sigma_N^\downarrow),
\end{aligned}$$

which is equivalent to (5.11). To prove (5.9), it remains to show that

$$1 - \sqrt{F}(\rho_N^\downarrow, \sigma_N^\downarrow) \leq C_{\mathcal{V},\mathcal{W}}^{(T_A^\downarrow, T_B^\downarrow)} \sum_{i=0}^{N-1} \sum_{k=0}^{K} \sqrt{\mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^\downarrow\right]\right] \cdot \mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\sigma_i^\downarrow\right]\right]}. \tag{5.12}$$

To this end, notice that if $T_A^\downarrow|_{\mathcal{B}_1(\mathcal{V})} = T_B^\downarrow|_{\mathcal{B}_1(\mathcal{V})}$, then $(T_A^\downarrow \otimes \mathrm{id})|_{\mathcal{B}_1(\mathcal{V}\otimes\mathcal{H}_Z)} = (T_B^\downarrow \otimes \mathrm{id})|_{\mathcal{B}_1(\mathcal{V}\otimes\mathcal{H}_Z)}$. Hence, $T_A' := (T_A^\downarrow \otimes \mathrm{id})$, $T_B' := (T_B^\downarrow \otimes \mathrm{id})$, $\mathcal{V}' := \mathcal{V} \otimes \mathcal{H}_Z$ and

$\mathcal{W}' := \{\mathcal{W}_1 \otimes \mathcal{H}_Z, \ldots, \mathcal{W}_K \otimes \mathcal{H}_Z\}$ satisfy the assumptions of Proposition 5.2. Furthermore, as the fidelity is non-decreasing under the action of the channel Λ_i (see [25], p. 414), we have

$$\begin{aligned}\sqrt{F}(\rho_i^{\downarrow}, \sigma_i^{\downarrow}) - \sqrt{F}(\rho_{i+1}^{\downarrow}, \sigma_{i+1}^{\downarrow}) &= \sqrt{F}(\rho_i^{\downarrow}, \sigma_i^{\downarrow}) - \sqrt{F}(\Lambda_i \circ T'_A(\rho_i^{\downarrow}), \Lambda_i \circ T'_B(\sigma_i^{\downarrow})) \\ &\leq \sqrt{F}(\rho_i^{\downarrow}, \sigma_i^{\downarrow}) - \sqrt{F}(T'_A(\rho_i^{\downarrow}), T'_B(\sigma_i^{\downarrow})).\end{aligned}$$

We want to apply Proposition 5.2 to the RHS of this expression. To do this correctly, we should notice that the projections, appearing in (5.2), project onto $\mathcal{W}_k \otimes \mathcal{H}_Z$, and hence are equal to $P_k \otimes \mathbb{1}$. Also, if V_A, V_B, P_A, and P_B satisfy Conditions (5.1b) and (5.1c), then $V_A \otimes \mathbb{1}, V_B \otimes \mathbb{1}, P_A \otimes \mathbb{1}$, and $P_B \otimes \mathbb{1}$ satisfy the Conditions (5.1b) and (5.1c) for T'_A and T'_B. If we plug this into (5.1a) and use that in general $\|X \otimes \mathbb{1}\| = \|X\|$, we obtain

$$C_{\mathcal{V}',\mathcal{W}'}^{(T_A^{\downarrow} \otimes \mathrm{id}, T_B^{\downarrow} \otimes \mathrm{id})} \leq C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})}.$$

Using these observations, we get

$$\begin{aligned}\sqrt{F}(\rho_i^{\downarrow}, \sigma_i^{\downarrow}) - \sqrt{F}(\rho_{i+1}^{\downarrow}, \sigma_{i+1}^{\downarrow}) &\leq C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \sum_{k=1}^{K} \sqrt{\mathrm{tr}\left[(P_k \otimes \mathbb{1})\rho_i^{\downarrow}\right] \mathrm{tr}\left[(P_k \otimes \mathbb{1})\sigma_i^{\downarrow}\right]} \\ &= C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \sum_{k=1}^{K} \sqrt{\mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{\downarrow}\right]\right] \mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\sigma_i^{\downarrow}\right]\right]}.\end{aligned}$$

Equivalently,

$$\sqrt{F}(\rho_{i+1}^{\downarrow}, \sigma_{i+1}^{\downarrow}) \geq \sqrt{F}(\rho_i^{\downarrow}, \sigma_i^{\downarrow}) - C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \sum_{k=1}^{K} \sqrt{\mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{\downarrow}\right]\right] \mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\sigma_i^{\downarrow}\right]\right]}.$$

If we iterate this inequality, we obtain

$$\sqrt{F}(\rho_N^{\downarrow}, \sigma_N^{\downarrow}) \geq \sqrt{F}(\rho_0^{\downarrow}, \sigma_0^{\downarrow}) - C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \sum_{i=0}^{N-1} \sum_{k=1}^{K} \sqrt{\mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{\downarrow}\right]\right] \mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\sigma_i^{\downarrow}\right]\right]}.$$

Using $\sqrt{F}(\rho_0^{\downarrow}, \sigma_0^{\downarrow}) = \sqrt{F}(s_0, s_0) = 1$ and some rearrangement establishes (5.12) and completes the proof of the theorem. □

To connect this technical result with the main results of this section, we need two auxiliary lemmas.

Lemma 5.5. *For* $\dim(\mathcal{H}) < \infty$*, let* $T_A, T_B : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *be two channels and let* D *be a finite-dimensional* N*-step discrimination strategy and* Π *be a two-valued POVM. Then,*

$$\frac{(1 - 2P_e(D, \Pi))^2}{2} \leq 1 - \sqrt{F}(\rho_N^{T_A}, \rho_N^{T_B}), \tag{5.13}$$

where ρ *is the intermediate state map of* D*.*

Proof. By definition,

$$P_e(D, \Pi) = \frac{1}{2}\left[\mathrm{tr}\left[\pi_B \rho_N^{T_A}\right] + \mathrm{tr}\left[\pi_A \rho_N^{T_B}\right]\right]. \tag{5.14}$$

If we minimize over the possible two-valued POVMs Π', the famous Holevo-Helstrom formula reads

$$P_e^m(D) := \min_{\Pi'} P_e(D,\Pi') = \frac{1}{2}\left[1 - \frac{1}{2}\left\|\rho_N^{T_A} - \rho_N^{T_B}\right\|_1\right].$$

Since $0 \leq P_e(D,\Pi) \leq \frac{1}{2}$, we have $1 - 2P_e(D,\Pi) \geq 0$. Thus,

$$\frac{(1-2P_e(D,\Pi))^2}{2} \leq \frac{(1-2P_e^m(D))^2}{2}. \tag{5.15}$$

By the Fuchs–van de Graaf inequality (see [25], p. 416),

$$\frac{1}{2}\left\|\rho - \sigma\right\|_1 \leq \sqrt{1 - \sqrt{F}(\rho,\sigma)^2}.$$

Thus,

$$\begin{aligned}\frac{(1-2P_e^m(D))^2}{2} &= \frac{\left(\frac{1}{2}\left\|\rho_N^{T_A} - \rho_N^{T_B}\right\|_1\right)^2}{2} \\ &\leq \frac{1 - \sqrt{F}(\rho_N^{T_A},\rho_N^{T_B})^2}{2} \\ &= (1 - \sqrt{F}(\rho_N^{T_A},\rho_N^{T_B}))\frac{1 + \sqrt{F}(\rho_N^{T_A},\rho_N^{T_B})}{2} \\ &\leq 1 - \sqrt{F}(\rho_N^{T_A},\rho_N^{T_B}).\end{aligned}$$

Together with (5.15), this proves the claim. □

Lemma 5.6. *For $\dim(\mathcal{H}) < \infty$, let $T_A, T_B : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be two channels with vacuum $v \in \mathcal{H}$. Let $\mathcal{V}_{T_A}$ and $\mathcal{V}_{T_B}$ be the respective maximal vacuum subspaces and let $T_A^{\downarrow}$ and $T_B^{\downarrow}$ be as in Definition 3.3 (Eq. 3.6). Furthermore, let $\mathcal{V}$ be a subspace such that $v \in \mathcal{V}$ and $\mathcal{V} \subseteq \mathcal{V}_{T_A} \cap \mathcal{V}_{T_B}$. Let $\mathcal{W} = \{\mathcal{W}_1, \mathcal{W}_2, \ldots, \mathcal{W}_K\}$ be a collection of mutually orthogonal subspaces of $\mathcal{V}^{\perp}$, such that $\mathcal{V}^{\perp} = \mathcal{W}_1 \oplus \mathcal{W}_2 \oplus \cdots \oplus \mathcal{W}_K$. Denote the orthogonal projections onto these subspaces by $P_1, P_2, \ldots, P_K$. Then,*

$$\frac{(1-2P_e(D,\Pi))^2}{2} \leq C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow},T_B^{\downarrow})} \sum_{i=0}^{N-1}\sum_{k=1}^{K}\sqrt{\mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{T_A^{\downarrow}}\right]\right]\cdot \mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{T_B^{\downarrow}}\right]\right]}, \tag{5.16}$$

for all finite-dimensional N-step discrimination strategies $D = (\mathcal{H}, \mathcal{H}_Z, s_0, \Lambda)$ and all two-valued POVMs, Π.

Proof. By Lemma 5.5, we have for any finite-dimensional N-step discrimination strategy D and any two-valued POVM, Π, that

$$\frac{(1-2P_e(D,\Pi))^2}{2} \leq 1 - \sqrt{F}(\rho_N^{T_A},\rho_N^{T_B}). \tag{5.17}$$

We want to apply Proposition 5.3 to the RHS of this inequality. To this end, we have to define the quantities appearing in that proposition. We identify $T_A, T_B, \mathcal{V}$, and $\mathcal{W}$ with the objects that bear the same name. In the following let $X \in \{A, B\}$. We define $T_X^{\downarrow}$ as in Definition 3.3 and need to check that

$T_X - T_X^{\downarrow}$ is completely positive and that $T_X^{\downarrow}|_{\mathcal{B}_1(\mathcal{V})}$ is trace-preserving. To this end, we fix a Stinespring isometry $V_X : \mathcal{H} \to \mathcal{H}_E \otimes \mathcal{H}$ of T_X. Then, $T_X^{\downarrow}$ is defined by

$$T_X^{\downarrow}(\cdot) = \mathrm{tr}_E \left[(P_v^{(X)} \otimes \mathbb{1}) V_X \cdot V_X^{\dagger} \right],$$

where $P_v^{(X)}$ is the projection onto the support of $\mathrm{tr}_{\mathcal{H}} \left[V_X |v\rangle\langle v| V_X^{\dagger} \right]$. It follows immediately from this expression that $T_X - T_X^{\downarrow}$ is completely positive. To see that $T_X^{\downarrow}|_{\mathcal{B}_1(\mathcal{V}_{T_X})}$ is trace-preserving, note that by Definition 3.9

$$\mathcal{V}_{T_X} = V_X^{-1} \left[\mathrm{supp}(\mathrm{tr}_{\mathcal{H}} \left[V_X |v\rangle\langle v| V_X^{\dagger} \right]) \otimes \mathcal{H} \right].$$

Thus, for any[15] $\rho \in \mathcal{B}_1(\mathcal{V}_{T_X})$,

$$V_X \rho V_X^{\dagger} \in \mathcal{B}_1(\mathrm{supp}(\mathrm{tr}_{\mathcal{H}} \left[V_X |v\rangle\langle v| V_X^{\dagger} \right]) \otimes \mathcal{H}).$$

As $P_v^{(X)} \otimes \mathbb{1}$ is the projection onto $\mathrm{supp}(\mathrm{tr}_{\mathcal{H}} \left[V_X |v\rangle\langle v| V_X^{\dagger} \right]) \otimes \mathcal{H}$, we have

$$T_X^{\downarrow}|_{\mathcal{B}_1(\mathcal{V}_{T_X})}(\cdot) = \mathrm{tr}_E \left[(P_v^{(X)} \otimes \mathbb{1}) V_X \cdot V_X^{\dagger} \right] = \mathrm{tr}_E \left[V_X \cdot V_X^{\dagger} \right] = T_X|_{\mathcal{B}_1(\mathcal{V}_{T_X})}(\cdot).$$

Thus, $T_X^{\downarrow}|_{\mathcal{B}_1(\mathcal{V}_{T_X})}$ is trace-preserving, as $T_X|_{\mathcal{B}_1(\mathcal{V}_{T_X})}$ is. As $\mathcal{V}$ is a subspace of $\mathcal{V}_{T_X}$, also $T_X^{\downarrow}|_{\mathcal{B}_1(\mathcal{V})}$ is trace-preserving. This is what we have claimed. As all assumptions are satisfied, we can invoke Proposition 5.3, which directly yields the desired inequality. □

The next result has already been stated in the results section.

Theorem 5.7 (No-go theorem). *For* $\dim(\mathcal{H}) < \infty$, *let* $T_A, T_B : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *be two channels with vacuum* $v \in \mathcal{H}$. *If there exists no subspace* $\mathcal{V} \subseteq \mathcal{H}$ *such that* $v \in \mathcal{V}$, *at least one of the channels* T_A *or* T_B *is isometric on* $\mathcal{V}$ *and* $T_A|_{\mathcal{B}_1(\mathcal{V})} \neq T_B|_{\mathcal{B}_1(\mathcal{V})}$, *then there exists a constant* $C < \infty$, *such that*

$$(1 - 2P_e(D, \Pi))^2 \leq C \sqrt{P_I^{T_A}(D) \cdot P_I^{T_B}(D)} \leq C \max(P_I^{T_A}(D), P_I^{T_B}(D)), \tag{5.18}$$

for all finite-dimensional N*-step discrimination strategies* D *and all two-valued POVMs,* Π. *Hence,* T_A *and* T_B *cannot be discriminated in an "interaction-free" manner.*

Remark 5.8. The assumption "The statement that T_A or T_B is isometric on a subspace $\mathcal{V}$, with $v \in \mathcal{V}$, already implies that $T_A|_{\mathcal{B}_1(\mathcal{V})} = T_B|_{\mathcal{B}_1(\mathcal{V})}$" can be rephrased in two equivalent ways. The first one is that the Conditions 1, 2, and 3 in the Main Theorem (Sect. 2) cannot be fulfilled simultaneously. The second reformulation is that for the maximum vacuum subspaces $\mathcal{V}_{T_A}$ and $\mathcal{V}_{T_B}$, we have $\mathcal{V}_{T_A} = \mathcal{V}_{T_B}$ and $T_A|_{\mathcal{B}_1(\mathcal{V}_{T_A})} = T_B|_{\mathcal{B}_1(\mathcal{V}_{T_B})}$. The equivalence follows directly from the characterization of maximal vacuum subspaces in

[15] Remember that for a subspace $\mathcal{V}_0 \subseteq \mathcal{H}$, the operators in $\mathcal{B}_1(\mathcal{V}_0)$ are those that can be written in the form $\sum_{i,j} \alpha_{ij} |\psi_i\rangle\langle\psi_i|$, with $\alpha_{ij} \in \mathbb{C}$ and $\psi_i \in \mathcal{V}_0$.

Lemma 3.10 4. This second reformulation is not only important in the proof, but also if one wants to check this criterion, as $\mathcal{V}_{T_A}$ and $\mathcal{V}_{T_B}$ are efficiently computable directly from Definition 3.9.

Proof. We use the second characterization in Remark 5.8. That is, $\mathcal{V}_{T_A} = \mathcal{V}_{T_B}$ and $T_A|_{\mathcal{B}_1(\mathcal{V}_{T_A})} = T_B|_{\mathcal{B}_1(\mathcal{V}_{T_B})}$. We set $\mathcal{V} := \mathcal{V}_{T_A}$ and let $T_A^{\downarrow}$ and $T_B^{\downarrow}$ be as in Definition 3.3. Furthermore, we define $\mathcal{W} := \{\mathcal{W}_1\}$, with $\mathcal{W}_1 := \mathcal{V}^{\perp}$. Then, by Lemma 5.6, we have

$$(1-2P_e(D,\Pi))^2 \leq 2C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow},T_B^{\downarrow})} \sum_{i=0}^{N-1} \sqrt{\mathrm{tr}\left[P^{\perp}\mathrm{tr}_Z\left[\rho_i^{T_A^{\downarrow}}\right]\right]\cdot \mathrm{tr}\left[P^{\perp}\mathrm{tr}_Z\left[\rho_i^{T_B^{\downarrow}}\right]\right]}, \tag{5.19}$$

where $P^{\perp}$ is the orthogonal projection onto $\mathcal{W}_1 = \mathcal{V}^{\perp}$. As $\mathcal{V}$ is the maximum vacuum subspace of T_A and T_B, Lemma 3.10 5 implies that for $X \in \{A,B\}$, there is a constant $C_{T_X} > 0$ such that $\mathfrak{i}_{T_X}(\rho) \geq C_{T_X}\mathrm{tr}\left[P^{\perp}\rho\right]$ for all $\rho \geq 0$. As $\mathrm{tr}_Z\left[\rho_i^{T_X^{\downarrow}}\right] \geq 0$, we get

$$\begin{aligned}
(5.19) &\leq \frac{2C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow},T_B^{\downarrow})}}{\sqrt{C_{T_A}C_{T_B}}} \sum_{i=0}^{N-1} \sqrt{\mathfrak{i}_{T_A}\left(\mathrm{tr}_Z\left[\rho_i^{T_A^{\downarrow}}\right]\right)\,\mathfrak{i}_{T_B}\left(\mathrm{tr}_Z\left[\rho_i^{T_B^{\downarrow}}\right]\right)} \\
&\leq \frac{2C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow},T_B^{\downarrow})}}{\sqrt{C_{T_A}C_{T_B}}} \sqrt{\left(\sum_{i=0}^{N-1}\mathfrak{i}_{T_A}\left(\mathrm{tr}_Z\left[\rho_i^{T_A^{\downarrow}}\right]\right)\right)\left(\sum_{i=0}^{N-1}\mathfrak{i}_{T_B}\left(\mathrm{tr}_Z\left[\rho_i^{T_B^{\downarrow}}\right]\right)\right)} \\
&= \frac{2C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow},T_B^{\downarrow})}}{\sqrt{C_{T_A}C_{T_B}}} \sqrt{P_I^{T_A}(D)\cdot P_I^{T_B}(D)},
\end{aligned}$$

where we used the Cauchy–Schwarz inequality (on $\mathbb{C}^N$) to obtain the second line and the definition of the "interaction" probability in the last line. We note that the last inequality in the statement of the theorem is trivial. Thus, by setting $C := \frac{2C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow},T_B^{\downarrow})}}{\sqrt{C_{T_A}C_{T_B}}}$, we have proven the claim. □

The following theorem is the technical version of the result stated in the results section.

Theorem 5.9 (Rate limit theorem). *For $\dim(\mathcal{H}) < \infty$, let $T_A, T_B : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ be two channels with vacuum $v \in \mathcal{H}$. Let $\mathcal{V}_{T_A}$ and $\mathcal{V}_{T_B}$ be the respective maximal vacuum subspace of T_A and T_B. Set $\mathcal{V} := \mathcal{V}_{T_A} \cap \mathcal{V}_{T_B}$. Suppose that $T_A|_{\mathcal{B}_1(\mathcal{V})} = T_B|_{\mathcal{B}_1(\mathcal{V})}$ and that $\mathcal{V}^{\perp} \cap \mathcal{V}_{T_A}$ and $\mathcal{V}^{\perp} \cap \mathcal{V}_{T_B}$ are orthogonal. Then there exists a constant $C > 0$ such that*

$$\max(P_I^{T_A}(D), P_I^{T_B}(D)) \geq C\,\frac{(1-2P_e(D,\Pi))^4}{N}, \tag{5.20}$$

for all finite-dimensional N-step discrimination strategies D, and any two-valued POVM Π.

Proof. The proof is similar to the one of the no-go theorem. Let $T_A^{\downarrow}$ and $T_B^{\downarrow}$ be as in Definition 3.3 and set $\mathcal{V} := \mathcal{V}_{T_A} \cap \mathcal{V}_{T_B}$. Furthermore, define $\mathcal{W} := \{\mathcal{W}_1, \mathcal{W}_2, \mathcal{W}_3\}$ with $\mathcal{W}_1 := \mathcal{V}^{\perp} \cap \mathcal{V}_{T_A}$, $\mathcal{W}_2 := \mathcal{V}^{\perp} \cap \mathcal{V}_{T_B}$ and $\mathcal{W}_3 := (\mathcal{W}_1 \oplus \mathcal{W}_2)^{\perp} \cap \mathcal{V}^{\perp}$. Clearly, $\mathcal{W}_1, \mathcal{W}_2$, and $\mathcal{W}_3$ are mutually orthogonal and their direct sum is $\mathcal{V}^{\perp}$. Furthermore, $\mathcal{W}_2 \oplus \mathcal{W}_3 = \mathcal{V}_{T_A}^{\perp}$ and $\mathcal{W}_1 \oplus \mathcal{W}_3 = \mathcal{V}_{T_B}^{\perp}$. Thus, by Lemma 5.6, we have

$$(1 - 2P_e(D, \Pi))^2 \leq 2C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \sum_{i=0}^{N-1} \sum_{k=1}^{3} \sqrt{\mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{T_A^{\downarrow}}\right]\right] \cdot \mathrm{tr}\left[P_k \mathrm{tr}_Z\left[\rho_i^{T_B^{\downarrow}}\right]\right]}, \tag{5.21}$$

where for $k \in \{1, 2, 3\}$, P_k is the orthogonal projection onto $\mathcal{W}_k$. Using the Cauchy–Schwarz inequality (on $\mathbb{C}^3$), and the fact that probabilities are less than one, and afterwards the Cauchy–Schwarz inequality on $\mathbb{C}^N$, we get

$$\begin{aligned}(5.21) &\leq \sqrt{12} C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \sum_{i=0}^{N-1} \sqrt{\mathrm{tr}\left[(P_2 + P_3)\mathrm{tr}_Z\left[\rho_i^{T_A^{\downarrow}}\right]\right] + \mathrm{tr}\left[(P_1 + P_3)\mathrm{tr}_Z\left[\rho_i^{T_B^{\downarrow}}\right]\right]} \\ &\leq \sqrt{12N} C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \sqrt{\sum_{i=0}^{N-1} \mathrm{tr}\left[P_{\mathcal{V}_{T_A}}^{\perp} \mathrm{tr}_Z\left[\rho_i^{T_A^{\downarrow}}\right]\right] + \mathrm{tr}\left[P_{\mathcal{V}_{T_B}}^{\perp} \mathrm{tr}_Z\left[\rho_i^{T_B^{\downarrow}}\right]\right]},\end{aligned} \tag{5.22}$$

where $P_{\mathcal{V}_{T_A}}^{\perp}$ and $P_{\mathcal{V}_{T_B}}^{\perp}$ are the projections onto $\mathcal{V}_{T_A}^{\perp}$ and $\mathcal{V}_{T_B}^{\perp}$. Lemma 3.10, 5 implies that for $X \in \{A, B\}$, there is a constant $C_{T_X} > 0$ such that $\mathfrak{i}_{T_X}(\rho) \geq C_{T_X} \mathrm{tr}\left[P_{\mathcal{V}_{T_X}}^{\perp} \rho\right]$ for all $\rho \geq 0$. As $\mathrm{tr}_Z\left[\rho_i^{T_X^{\downarrow}}\right] \geq 0$, we get

$$\begin{aligned}(5.22) &\leq \sqrt{12N} C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \sqrt{C_{T_A}^{-1} \sum_{i=0}^{N-1} \mathfrak{i}_{T_A}\left(\mathrm{tr}_Z\left[\rho_i^{T_A^{\downarrow}}\right]\right) + C_{T_B}^{-1} \sum_{i=0}^{N-1} \mathfrak{i}_{T_B}\left(\mathrm{tr}_Z\left[\rho_i^{T_B^{\downarrow}}\right]\right)} \\ &\leq C_{\mathcal{V}}^{(T_A^{\downarrow}, T_B^{\downarrow})} \sqrt{\frac{24}{\min(C_{T_A}, C_{T_B})}} \sqrt{N \max(P_I^{T_A}(D), P_I^{T_B}(D))}.\end{aligned}$$

Taking the square and defining $C := \frac{\min(C_{T_A}, C_{T_B})}{24 C_{\mathcal{V},\mathcal{W}}^{(T_A^{\downarrow}, T_B^{\downarrow})^2}}$ proves the claim. □

6. Related Work

In this section we compare our setup and results to selected other works in the literature.[16] We start with a detailed comparison with the work on counterfactual computation (CFC) by Mitchison and Josza [7]. CFC aims to determine the outcome of a quantum computation without switching on the computer. Expressed in a language closer to ours, CFC aims to discriminate (counterfactually, the term analogous to "interaction-free") between two unitaries U_0 and

[16] Although we tried to make the discussion as self-contained as possible, this section is intended for the reader who is at last partially familiar with the referenced works.

U_1 defined on a bipartite system $\mathcal{H}_O \otimes \mathcal{H}_S$ (where "O" stands for output and "S" for switch).

Before defining what counterfactual means, we need to discuss the allowed discrimination strategies. Here, it is allowed to use the unknown unitary many times while performing unitary operations and measurements in between. It is also allowed to add an ancillary system $\mathcal{H}_Z$ of arbitrary size and to let the unitary operations act on the space $\mathcal{H}_O \otimes \mathcal{H}_S \otimes \mathcal{H}_Z$. This implies that measurements can be deferred until the unknown unitary was applied for the last time. Thus, if the unknown unitary U_r, $r \in \{0,1\}$ is used N times, the initial state is $\psi_I \in \mathcal{H}_O \otimes \mathcal{H}_S \otimes \mathcal{H}_Z$ and the intermediary unitaries are $V_1, V_2, \ldots, V_{N-1} \in \mathcal{B}(\mathcal{H}_O \otimes \mathcal{H}_S \otimes \mathcal{H}_Z)$, then the ($r$-dependent) state before the final measurement is

$$\psi_F^r = (U_r \otimes \mathbb{1}_Z) V_{N-1} (U_r \otimes \mathbb{1}_Z) V_{N-2} \cdots (U_r \otimes \mathbb{1}_Z) V_1 (U_r \otimes \mathbb{1}_Z) \psi_I. \tag{6.1}$$

In preparation for defining the term counterfactual, one assumes that for each $r \in \{0,1\}$ we can split the switch space into two orthogonal spaces $\mathcal{H}_S = \mathcal{H}_S^{r,\mathrm{off}} \oplus \mathcal{H}_S^{r,\mathrm{on}}$, called the off and on subspaces, respectively. The interpretation here is that if we apply U_r to a state in $\mathcal{H}_O \otimes \mathcal{H}_S^{r,\mathrm{off}}$, then the computer does not run. Consistent with this interpretation, it is also assumed that

$$U_r \psi = \psi, \text{ for all } \psi \in \mathcal{H}_O \otimes \mathcal{H}_S^{r,\mathrm{off}}. \tag{6.2}$$

One then introduces a decomposition into so-called histories. To this end, one imagines that after each application of U_r a measurement was performed, projecting either onto $\mathcal{H}_O \otimes \mathcal{H}_S^{r,\mathrm{off}} \otimes \mathcal{H}_Z$ or onto $\mathcal{H}_O \otimes \mathcal{H}_S^{r,\mathrm{on}} \otimes \mathcal{H}_Z$. We denote the corresponding projections by P_{off}^r and P_{on}^r. On can then decompose ψ_F^r as:

$$\begin{aligned} \psi_F^r &= \sum_{h \in \{\mathrm{on},\mathrm{off}\}^N} v_h^r, \text{ with} \\ v_h^r &= P_{h_N}^r (U_r \otimes \mathbb{1}_Z) V_{N-1} \cdots P_{h_2}^r (U_r \otimes \mathbb{1}_Z) V_1 P_{h_1}^r (U_r \otimes \mathbb{1}_Z) \psi_I. \end{aligned} \tag{6.3}$$

Each of the on/off sequences h in (6.3) is called a history.

Suppose we perform a projective measurement on the final state with possible outcomes $m \in \{1, 2, \ldots, M\}$ and associated projections $\{Q_1, Q_2, \ldots, Q_M\}$. Mitchison and Josza (Definition 5.1 in [7]) then define an outcome m to be a *counterfactual outcome of type* $r \in \{0,1\}$, if

1. $Q_m v_h^r = 0$, if h is not the all-off history,
2. $Q_m \psi_F^{1-r} = 0$.

The first condition says that the only history consistent with the outcome m must be the all-off history and the second condition demands that the outcome m can only occur if the unknown unitary is U_r (and not U_{1-r}).

Now, how does CFC relate to "interaction-free" channel discrimination? First, one can interpret "interaction-free" channel discrimination in terms of CFC after some modifications, as follows. Consider a channel T with vacuum $v \in \mathcal{H}_I$, given by $T(\cdot) = \mathrm{tr}_E \left[V \cdot V^\dagger \right]$. In Sect. 3.1, we determined that the Demon's optimal strategy is to perform a two-outcome measurement on E (with corresponding projections P_v and $P_v^\perp$). After extending V to a unitary

U, we can interpret the whole space $\mathcal{H}_E \otimes \mathcal{H}_I$ as the switch space $\mathcal{H}_S$ and set $\mathcal{H}_O := \mathbb{C}$. A natural way to introduce the splitting of $\mathcal{H}_S$ into on and off subspace is then to define $\mathcal{H}_S^{\text{off}} = \text{range}(P_v) \otimes \mathcal{H}_I$ and $\mathcal{H}_S^{on} = \text{range}(P_v^{\perp}) \otimes \mathcal{H}_I$. Note, however, that this definition does not satisfy (6.2).[17] A violation of assumption (6.2) does not prevent us from defining histories, nor does it interfere with the definition of a counterfactual outcome as above. So, one might consider broadening the definition of CFC by dropping it. However, upon close investigation one finds that (the proofs of) all theorems in [7] rely crucially on that assumption. In any case, even after dropping that assumption, the definition of a counterfactual outcome above is still too restrictive to fully cover "interaction-free" channel discrimination, since we do not require that the "interaction" probability or the error probability are exactly zero (as demanded by CFC) but rather that they can be made arbitrarily small. This requires a probabilistic modification of the definition of a counterfactual outcome, such as the one suggested in the discussion section in [7]. We therefore conclude that "interaction-free" channel discrimination is consistent with a sufficiently broadened definition of CFC. Unfortunately, however, we do not think that this point of view has any important direct implications for the feasibility of the "interaction-free" channel discrimination task. The main reasons for this belief are that even after reformulation into the language of CFC, the allowed discrimination strategies differ considerably and that the only result in [7] that goes beyond the qubit case is that the number of insertions of U_r must tend to infinity for an optimal success probability.[18]

What about implications of our results for CFC? We believe that a conceptual weakness of CFC is that there are (in general) no observable consequences—in the sense that (the surroundings of) the apparatus changes—regardless of whether a computation was performed counterfactually or not. This is so because the imagined measurements after each application of the unknown unitary are not actually performed. We think that the question about a change of (the surroundings of) the apparatus is the relevant one for technical applications, which is our main focus. If one demands that the imaginary measurements are actually performed, then CFC becomes a special case of "interaction-free" channel discrimination by assigning to the unitary $U_r \in \mathcal{B}(\mathcal{H}_O \otimes \mathcal{H}_S)$ the channel $T_r : \mathcal{B}(\mathcal{H}_O \otimes \mathcal{H}_S)$ given by

$$T_r(\rho) = (\mathbb{1}_O \otimes P_S^{r,\text{off}})U\rho U^\dagger(\mathbb{1}_O \otimes P_S^{r,\text{off}}) + (\mathbb{1}_O \otimes P_S^{r,\text{on}})U\rho U^\dagger(\mathbb{1}_O \otimes P_S^{r,\text{on}}), \tag{6.4}$$

for all $\rho \in \mathcal{B}_1(\mathcal{H}_O \otimes \mathcal{H}_S)$, where $P_S^{r,\text{off}}$ and $P_S^{r,\text{on}}$ are the projections according to the splitting of $\mathcal{H}_S$ into on and off subspace. It follows from (6.2) that T_r

[17] For example, if U is defined on $\mathbb{C}^2 \otimes \mathbb{C}^2$ by $U|00\rangle = |00\rangle, U|01\rangle = \frac{1}{\sqrt{2}}(|01\rangle + \langle 10|), U|10\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle), U|11\rangle = |11\rangle$ and $|0\rangle$ is the vacuum, then $P_v = |0\rangle\langle 0|$. However, the corresponding off subspace $\mathcal{H}_S^{\text{off}} = \text{span}\{|00\rangle, |01\rangle\}$ is not even left invariant by U.

[18] Note that this conclusion does not apply to all cases of our setting, since the number of applications for a perfect discrimination of two unitaries is finite.

is a channel with vacuum, where the vacuum can be taken to be any vector in $\mathcal{H}_O \otimes \mathcal{H}_S^{r,\text{off}}$. Hence, our results apply to this setting.

From our technological point of view, some interpretational discussions in the literature can be avoided. For example, in [37], Hosten et. al claimed that they could discriminate counterfactually between four unitaries associated with the result of a Grover search. We agree with [38,39] that the proposal in [37] does not constitute a CFC for all possible outcomes in the sense of [7]. However, from the point of view of our model, this is a rather artificial debate. Since a unitarily evolving system does not interact with its surroundings (the Demon), there is no way to tell whether a computation has been performed or not by looking at the surroundings. In that sense, the task in [37] was (as every other discrimination task involving only unitary operations) performed in an "interaction-free" manner.

A work with a title similar to ours is "Interaction-free measurement as quantum channel discrimination" by Zhou and Yung [32]. The objective of their work was to determine if the Kwiat et. al protocol for detecting a semi-transparent object can be enhanced by using an entangled initial state. The study was conducted by employing tools from quantum channel theory, but no attempts were made to generalize the notion of "interaction-free" measurements. Generalizing this notion, however, is the main focus of the present work.

7. Conclusion and Open Problems

In our work, we have characterized when it is possible and impossible to discriminate quantum channels in an "interaction-free" manner. This answers the question, what can be done perfectly with "interaction-free" measurements. However, there are still some open questions. One question that is in direct succession of our work is, under which conditions two channels can be discriminated such that the "interaction" probability decays faster than N^{-1}. Another question would ask for a more quantitative treatment, i.e., even though one might not be able to discriminate two channels in an "interaction-free" manner, there still might be a significant quantum advantage over classical strategies. A related question suggested to us by an anonymous reviewer is what kind of information about the discriminator's strategy the Demon can obtain. In this context, we showed that the Demon cannot distinguish (under our conditions) between a strategy that always sends the vacuum through the channels and our proposed one. However, the more general question remains open. A big question concerns the influence of noise and decoherence. We note that noise may influence what can or cannot be done in both directions, since the noise can also be on the Demon's side and hence make his detection skills weaker. Before the no-go results for semitransparent objects were established [11,12], one anticipated application of "interaction-free" measurement was to eliminate the exposure of humans to radiation in medical applications such as X-ray scans. This is not possible. However, our no-go theorem does not touch

the case of asymmetric "interaction-free" discrimination. That is, we may allow that one of the two objects to be discriminated gets destroyed (for example, by simply setting its transmission functional to zero). This might even be a desirable effect. For example, in a medical context, we would love to design a procedure such that a tumor gets destroyed, while the healthy tissue stays intact.

Acknowledgements

M.H. was supported by the Bavarian excellence network ENB via the International PhD Programme of Excellence *Exploring Quantum Matter* (EXQM). M.M.W. acknowledges funding by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy EXC-2111 390814868.

Funding Information Open Access funding enabled and organized by Projekt DEAL.

Appendix A.

Lemma A.1 (Semi-simplicity of the peripheral spectrum). *Let* $T : \mathcal{B}_1(\mathcal{H}) \to \mathcal{B}_1(\mathcal{H})$ *be a channel such that* 1 *is in the discrete spectrum of* T*. Then, for any* $n \in \mathbb{N}$ *and any (rectifiable) path inside the resolvent set of* T *that encloses* 1*, and separates* 1 *from* $\sigma(T) \setminus \{1\}$*, we have*

$$\frac{1}{2\pi i} \oint_{\Gamma_1} \frac{z^n}{z - T} \, \mathrm{d}z = \frac{1}{2\pi i} \oint_{\Gamma_1} \frac{1}{z - T} \, \mathrm{d}z. \tag{A.1}$$

Proof. For brevity, we denote the Riesz-Projection on the RHS of (A.1) by P. As 1 is in the discrete spectrum of T, Corollary 2.3.6 in [29] says that $TP = \frac{1}{2\pi i} \oint_{\Gamma_1} \frac{z}{z-T} \, \mathrm{d}z = P + N$, where N is a nilpotent operator that commutes

with P. Hence $T = P+N+T_0$, where $T_0 := (\mathrm{id}-P)T(\mathrm{id}-P)$. By the analytic functional calculus, we have

$$(P+N)^n = \left(\frac{1}{2\pi i}\oint_{\Gamma_1} \frac{z}{z-T}\,\mathrm{d}z\right)^n = \frac{1}{2\pi i}\oint_{\Gamma_1} \frac{z^n}{z-T}\,\mathrm{d}z.$$

If $N = 0$, then the claim follows, since P is a projection ($P^n = P$). To this end, assume that $N \neq 0$. Since N is nilpotent, there exists an integer D such that $N^D \neq 0$ and $N^{D+1} = 0$. As $N \neq 0$, we have $D \geq 1$. Choose $\rho \in \mathcal{B}_1(\mathcal{H})$ such that $N^D(\rho) \neq 0$ and $P(\rho) = \rho$. Note that $PT_0 = T_0P = 0$. Thus, $T^n(\rho) = (P+N)^n(\rho) + T_0^n(\rho) = (P+N)^n(\rho)$. In particular, since T is a channel, $\|T^n\| = 1$ and thus

$$\|(P+N)^n(\rho)\| \leq \|\rho\|\,. \tag{A.2}$$

For $n \geq D$, we have

$$(P+N)^n(\rho) = \sum_{i=0}^{D} \binom{n}{i} N^i(\rho).$$

Furthermore, the vectors $\rho, N(\rho), N^2(\rho), \ldots N^D(\rho)$ are linearly independent. The coordinate function of $N(\rho)$ is $\binom{n}{1}$, which is unbounded for $n \to \infty$. Since the coordinate function can be extended to a continuous linear functional on $\mathcal{B}_1(\mathcal{H})$ (Hahn–Banach), the unboundedness contradicts (A.2). Hence, $N = 0$. □

References

[1] Elitzur, A.C., Vaidman, L.: Quantum mechanical interaction-free measurements. Found. Phys. **23**, 987–997 (1993)

[2] Kwiat, P., Weinfurter, H., Herzog, T., Zeilinger, A., Kasevich, M.A.: Interaction-free measurement. Phys. Rev. Lett. **74**, 4763–4766 (1995)

[3] Misra, B., Sudarshan, E.C.G.: The zeno's paradox in quantum theory. J. Math. Phys. **18**(4), 756–763 (1977)

[4] White, A.G., Mitchell, J.R., Nairz, O., Kwiat, P.G.: "Interaction-free" imaging. Phys. Rev. A **58**, 605–613 (1998)

[5] Putnam, W.P., Yanik, M.F.: Noninvasive electron microscopy with interaction-free quantum measurements. Phys. Rev. A **80**, 040902 (2009)

[6] Jozsa, R.: Quantum effects in algorithms. In: Williams, C.P. (ed.) Quantum Computing and Quantum Communications, pp. 103–112. Springer, Berlin (1999)

[7] Mitchison, G., Jozsa, R.: Counterfactual computation. Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. **457**(2009), 1175–1193 (2001)

[8] Salih, H., Li, Z.-H., Al-Amri, M., Zubairy, M.S.: Protocol for direct counterfactual quantum communication. Phys. Rev. Lett. **110**, 170502 (2013)

[9] Noh, T.-G.: Counterfactual quantum cryptography. Phys. Rev. Lett. **103**, 230501 (2009)

[10] Lin, C.Y.-Y., Lin, H.-H.: Upper bounds on quantum query complexity inspired by the Elitzur–Vaidman bomb tester. In: Zuckerman, D. (ed.) 30th Conference on Computational Complexity (CCC 2015), Vol. 33 of Leibniz International Proceedings in Informatics (LIPIcs), (Dagstuhl, Germany), pp. 537–566. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik (2015)

[11] Mitchison, G., Massar, S.: Absorption-free discrimination between semitransparent objects. Phys. Rev. A **63**, 032105 (2001)

[12] Massar, S., Mitchison, G., Pironio, S.: Minimal absorption measurements. Phys. Rev. A **64**, 062303 (2001)

[13] Möbus, T., Wolf, M.M.: Quantum zeno effect generalized. J. Math. Phys. **60**(5), 052201 (2019)

[14] Burgarth, D., Facchi, P., Nakazato, H., Pascazio, S., Yuasa, K.: Generalized adiabatic theorem and strong-coupling limits. Quantum **3**, 152 (2019)

[15] Burgarth, D., Facchi, P., Nakazato, H., Pascazio, S., Yuasa, K.: Quantum zeno dynamics from general quantum operations. Quantum **4**, 289 (2020)

[16] Barankai, N., Zimborás, Z.: Generalized quantum zeno dynamics and ergodic means (2018). arXiv:1811.02509

[17] Chiribella, G., D'Ariano, G.M., Perinotti, P.: Theoretical framework for quantum networks. Phys. Rev. A **80**, 022339 (2009)

[18] Spekkens, R.W.: Evidence for the epistemic view of quantum states: a toy theory. Phys. Rev. A **75**, 032110 (2007)

[19] Spekkens, R.W., Elliot, M., Leife, M.: Reassessing claims of nonclassicality for quantum interference phenomena. PIRSA:16060102 see, https://pirsa.org (2016)

[20] King, C., Matsumoto, K., Nathanson, M., Ruskai, M.B.: Properties of conjugate channels with applications to additivity and multiplicativity Markov Process. Relat. Fields **13**(2), 391–423 (2007)

[21] Knill, E., Laflamme, R., Viola, L.: Theory of quantum error correction for general noise. Phys. Rev. Lett. **84**, 2525–2528 (2000)

[22] Acín, A.: Statistical distinguishability between unitary operations. Phys. Rev. Lett. **87**, 177901 (2001)

[23] Beckman, D., Gottesman, D., Nielsen, M.A., Preskill, J.: Causal and localizable quantum operations. Phys. Rev. A **64**, 052309 (2001)

[24] Eggeling, T., Schlingemann, D., Werner, R.F.: Semicausal operations are semilocalizable. Europhys. Lett. (EPL) **57**, 782–788 (2002)

[25] Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)

[26] Abramovich, Y., Aliprantis, C.: Problems in Operator Theory. No. v. 2 in Graduate Studies in Mathematics. American Mathematical Society, Providence (2002)

[27] Borthwick, D.: Spectral Theory: Basic Concepts and Applications. Graduate Texts in Mathematics. Springer, Berlin (2020)

[28] Kato, T.: Perturbation Theory for Linear Operators, 2nd edn. Grundlehren Math. Wiss. Springer, Berlin (1976)

[29] Simon, B.: Operator Theory. American Mathematical Society, Providence (2015)

[30] Burgarth, D., Giovannetti, V.: The generalized Lyapunov theorem and its application to quantum channels. New J. Phys. **9**, 150 (2007)

[31] Azuma, H.: Interaction-free measurement with an imperfect absorber. Phys. Rev. A **74**, 054301 (2006)

[32] Zhou, Y., Yung, M.-H.: Interaction-free measurement as quantum channel discrimination. Phys. Rev. A **96**, 062129 (2017)

[33] Chiribella, G., D'Ariano, G.M., Perinotti, P.: Transforming quantum operations: quantum supermaps. EPL (Europhys. Lett.) **83**, 30004 (2008)

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

[35] Sternberg, S.: Group Theory and Physics. Cambridge University Press, Cambridge (1995)

[36] Vollbrecht, K.G.H., Werner, R.F.: Entanglement measures under symmetry. Phys. Rev. A **64**, 062307 (2001)

[37] Hosten, O., Rakher, M., Barreiro, J., Peters, N., Kwiat, P.: Counterfactual quantum computation through quantum interrogation. Nature **439**, 949–52 (2006)

[38] Vaidman, L.: Impossibility of the counterfactual computation for all possible outcomes. Phys. Rev. Lett. **98**(16), 160403 (2007)

[39] Mitchison, G., Jozsa, R.: The limits of counterfactual computation. arXiv:quant-ph/0606092 (2007)

Markus Hasenöhrl and Michael M. Wolf
Department of Mathematics
Technical University of Munich
Garching
Germany
e-mail: m.hasenoehrl@tum.de;
m.wolf@tum.de

and

Munich Center for Quantum Science and Technology (MCQST)
Munich
Germany

and

Zentrum Mathematik
Garching Forschungszentrum
Boltzmannstr. 3
85748 Garching bei München
Germany

Communicated by Matthias Christandl.

Received: January 25, 2021.

Accepted: March 10, 2022.