Retrodiction of Generalised Measurement Outcomes

Anthony Chefles
Department of Physical Sciences, University of Hertfordshire, Hatfield AL10 9AB, Hertfordshire, UK

Masahide Sasaki
Communications Research Laboratory, Koganei, Tokyo 184-8795, Japan

If a generalised measurement is performed on a quantum system and we do not know the outcome, are we able to retrodict it with a second measurement? We obtain a necessary and sufficient condition for perfect retrodiction of the outcome of a known generalised measurement, given the final state, for an arbitrary initial state. From this, we deduce that, when the input and output Hilbert spaces have equal (finite) dimension, it is impossible to perfectly retrodict the outcome of any fine-grained measurement (where each POVM element corresponds to a single Kraus operator) for all initial states unless the measurement is unitarily equivalent to a projective measurement. It also enables us to show that every POVM can be realised in such a way that perfect outcome retrodiction is possible for an arbitrary initial state when the number of outcomes does not exceed the output Hilbert space dimension. We then consider the situation where the initial state is not arbitrary, though it may be entangled, and describe the conditions under which unambiguous outcome retrodiction is possible for a fine-grained generalised measurement. We find that this is possible for some states if the Kraus operators are linearly independent. This condition is also necessary when the Kraus operators are non-singular. From this, we deduce that every trace-preserving quantum operation is associated with a generalised measurement whose outcome is unambiguously retrodictable for some initial state, and also that a set of unitary operators can be unambiguously discriminated iff they are linearly independent. We then examine the issue of unambiguous outcome retrodiction without entanglement. This has important connections with the theory of locally linearly dependent and locally linearly independent operators.

PACS numbers: 03.65.Bz, 03.67.-a, 03.67.Hk

I. INTRODUCTION

One of the most contentious issues in the development of quantum mechanics was, and continues to be, the measurement process. The fact that measurement appears explicitly in the quantum formalism represents a significant break with the implicit assumption in classical mechanics that all quantities which enter into the description of the state of a physical system are observable and that the measurement process requires no special treatment. It does in quantum mechanics. Among the consequences of the nature of the quantum measurement process as expounded by, for example, von Neumann, are indeterminism, the impossibility of measuring the state of a quantum system and uncertainty relations.

However, the projective measurements introduced by von Neumann and defined in full generality by Lüders do retain one significant feature of classical physics. This is the property of repeatability. Simply stated, if we perform such a measurement on a quantum system twice, and if we are able to reverse any evolution of the state between the measurements, then the outcome of the second measurement will be the same as that of the first.

Subsequent developments in quantum measurement theory have shown that the combination of projective measurements with unitary interactions leads to a broader range of state transformations and information-acquisition procedures. These, which are known as quantum operations and generalised measurements respectively, are closely related to each other.

The statistical properties of a generalised measurement are determined by a set of positive operators forming a positive, operator-valued measure (POVM). Generalised measurements enable one to acquire certain kinds of information about quantum states which are unobtainable using only projective measurements, especially if the possible initial states are non-orthogonal. However, they do have some disadvantages. One is the fact that they do not possess the aforementioned repeatability property of projective measurements. The repeatability of these measurements is independent of the initial state, which may be arbitrary and unknown. It enables us to predict not only the outcome of a future repetition of the measurement, but also the future post-measurement state, provided that there is no irreversible evolution between the measurements. Furthermore, these predictions will be fulfilled with unit probability.

As well as enabling us to predict the outcome of an identical measurement, repeatability also enables us to retrodict the outcome of a projective measurement and also the post-measurement state, given that we know which observable was measured and again, in the absence
of subsequent irreversible evolution.

The fact that the repeatability of projective measurements has so many aspects and consequences suggests that, while these may not all hold for generalised measurements, some vestiges of repeatability could be made to hold for these measurements in some circumstances if we are willing to sacrifice others. This is the issue we investigate in this paper. The particular aspect of the repeatability of projective measurements we would like to retain is outcome retrodictability. As one might expect, when this is possible, the measurement which carries out the retrodiction will, in general, differ from the original measurement in this wider context.

It is well-established that the implementation of a generalised measurement will often involve a projective measurement on an extended space \([\mathcal{H}_1 \otimes \mathcal{H}_2, \mathcal{H}_1 \otimes \mathcal{H}_2]\), for example, a projective measurement on a Cartesian product (Naimark) extension or a unitary-projection scheme on a direct, or tensor product extension. However, it is typically the case that we do not have access to this extension, which is assumed to be the case throughout this paper. When we address the issue of measurement outcome retrodictability, the retrodiction operators will act only on the space of system post-measurement states and not on such an extension. We shall, however, allow for the possibility that the space of post-measurement states differs from that of the preparation states whenever making this distinction is necessary for a fully general analysis.

We should also emphasise the distinction between the idea of retrodicting the outcome of a generalised measurement and the formalism of retrodictive quantum mechanics. The latter was proposed originally by Aharonov and coworkers\(^{[9]}\) and has recently been extended and applied in numerous interesting ways by Barnett and coworkers\(^{[10]}\). In retrodictive quantum mechanics, the aim is to use accessible measurement data to retrodict the initial state of a quantum system. The retrodicted information is then quantum information. In the present context, although a measurement has been carried out, the result is not accessible and it is this classical measurement result that we aim to retrodict.

Our motivation for focusing on this particular aspect of repeatability is as follows: if we know the result of a known measurement then in practical situations we would seldom have any reason to carry it out again. The issue of repeatability, or non-repeatability, will be important in situations when a measurement has been performed and the result has been lost or otherwise made inaccessible to us. If we do not know the measurement result then, in the most favourable scenario, we will have access to the final state. This is a mixture of the post-measurement states corresponding to the various possible outcomes weighted by their respective probabilities. When we do have access to the system following the measurement, which we shall assume to be the case, we will be concerned with how its state has been transformed by the measurement process. If the initial state is represented by a density operator \(\rho\), then the final state will be obtained by a completely positive, linear, trace-preserving (CPLTP) map \(\Phi : \rho \rightarrow \Phi(\rho)\).

In projective measurements, repeatability and thus perfect outcome retrodiction are possible for an arbitrary, unknown, initial state. At the outset, we make a distinction between two kinds of generalised measurement: fine-grained and coarse-grained measurements. These correspond, respectively, to situations where each POVM element is related to a single, or multiple Kraus transformation operators. The former is clearly a special case of the latter. Section II is devoted to the examination of perfect outcome retrodiction, that is, deterministic, error-free retrodiction of the outcome of a known generalised measurement. We derive a necessary and sufficient condition for such perfect retrodiction to be possible for an arbitrary initial state and show that there is no advantage to be gained if the initial state, though arbitrary, is known. The remainder of this section is devoted to unravelling some implications of this condition. We show that it implies that, when the input and output Hilbert spaces have equal dimension, the only fine-grained measurements with perfectly retrodictable outcomes for arbitrary initial states are those which are unitarily equivalent to projective measurements. However, we also show that there exists a large class of coarse-grained generalised measurements which are highly dissimilar to projective measurements for which perfect outcome retrodiction, with an arbitrary initial state, is possible. We show that a necessary and sufficient condition for a particular POVM to have an associated, typically coarse-grained, generalised measurement whose outcome is perfectly retrodictable for all initial states is that the number of outcomes does not exceed the dimension of the output Hilbert space of the system. We also show how such measurements can be realised in terms of the unitary-projection picture of generalised measurements.

In section III we drop the condition of perfect retrodiction and require instead that the outcome can be retrodicted, unambiguously, with some probability instead. We also, for the most part, drop the condition that the initial state may be arbitrary, and require only that the outcome is retrodictable for at least one known, initial state. We focus on fine-grained measurements and allow for the possibility of the system being initially entangled with an additional, ancillary system. We show that, when such entanglement is permitted, the measurement operations for which this is possible are closely related to the ‘canonical’ representations of general quantum operations, first studied by Choi\(^{[11]}\). These canonical representations have linearly independent Kraus operators. We find that a general sufficient and, for ‘finite-strength’ measurements\(^{[1]}\), which, in the fine-grained case, have non-singular Kraus operators, necessary condition for unambiguous retrodiction of the outcome of a fine-grained generalised measurement for some, possibly entangled, initial state is that the Kraus operators are linearly independent. Every CPLTP map has a Choi canonical representation, and so every trace-preserving quantum opera-
tion has an associated, fine-grained, generalised measurement amenable to unambiguous outcome retrodiction. A further consequence of our analysis, relating to unitary operator discrimination, is that a necessary and sufficient condition for unambiguous discrimination among a set of unitary operators is that they are linearly independent.

We finally examine the issue of unambiguous outcome retrodiction without entanglement. We focus on finite-strength, fine-grained measurements. For such measurements, we find that a necessary and sufficient condition for unambiguous outcome retrodiction for some non-entangled initial pure state is that the Kraus operators are not locally linearly dependent. We use this, together with some results recently obtained by Šemrl and coworkers relating to locally linearly dependent operators, to explore the relationship between unambiguous outcome retrodiction without entanglement and local linear dependence. We then explore the possibility of unambiguous outcome retrodiction for every initial, pure, separable state. For fine-grained, finite-strength measurements, we find that this is possible only when the Kraus operators are locally linearly independent.

II. PERFECT OUTCOME RETRODICTIO

FOR ARBITRARY INITIAL STATES

Consider a quantum system $Q$. Its initial state lies in a Hilbert space which we will denote by $H_Q$. Except where explicitly stated otherwise, this will have finite dimension $D_Q$. A generalised measurement $M_Q$ is carried out on this system. We assume that the number of possible outcomes of this measurement is also finite and shall denote this by $N$.

The possible outcomes of the measurement $M_Q$ will be labelled by the index $k \in \{1, \ldots, N\}$. Associated with the $k$th outcome is a linear, positive, quantum detection operator, or positive operator-valued measure (POVM) element $\Pi_k : H_Q \rightarrow H_Q$. These satisfy

$$\sum_{k=1}^{N} \Pi_k = 1_Q,$$  \hspace{1cm} (2.1)

where $1_Q$ is the identity operator on $H_Q$. The probability of outcome $k$ when the initial state is described by the density operator $\rho$ is

$$P(k|\rho) = \text{Tr}(\Pi_k \rho).$$  \hspace{1cm} (2.2)

Suppose that the measurement $M_Q$ is carried out on $Q$ and that the outcome is withhold from us. We do, nevertheless, have access to the final state of the system. On the basis of this, can we retrodict the measurement outcome?

To proceed, we must account for the manner in which the state of the system is transformed by the measurement process. Let $H_Q$ be the Hilbert space of post-measurement states. These definitions enable us to allow for the possibility that the initially prepared system and the system corresponding to the space of post-measurement states, which will subsequently be subjected to a retrodiction attempt, may be different. For example, the initial state may be that of an atom, yet the final state that of an electromagnetic field mode. However, for the sake of notational convenience, we shall denote both the initially prepared system and the final, interrogated system by the symbol $Q$, as it will be clear from the context which system is being referred to.

We distinguish between two kinds of generalised measurement. We will refer to these as fine-grained measurements and coarse-grained measurements. In a fine-grained measurement, corresponding to each detection operator $\Pi_k$, there is a single Kraus operator $A_k : H_Q \rightarrow H_Q$ such that

$$\Pi_k = A_k^\dagger A_k$$  \hspace{1cm} (2.3)

and the final, normalised state of the system when the outcome is $k$ is given by the transformation

$$\rho \rightarrow \rho_k = \frac{A_k \rho A_k^\dagger}{P(k|\rho)}.$$  \hspace{1cm} (2.4)

In a coarse-grained measurement, corresponding to the operator $\Pi_k$, there is a set of $R$ Kraus operators $A_{kr}$, where $r \in \{1, \ldots, R\}$, some of which may be zero, such that

$$\Pi_k = \sum_{r=1}^{R} A_{kr}^\dagger A_{kr}.$$  \hspace{1cm} (2.5)

The final, normalised state of the system when the outcome is $k$ is given by the transformation

$$\rho \rightarrow \rho_k = \frac{\sum_{r=1}^{R} A_{kr} \rho A_{kr}^\dagger}{P(k|\rho)}$$  \hspace{1cm} (2.6)

where, in both cases, $P(k|\rho)$ is given by Eq. (2.2). We can easily see from these definitions that fine-grained measurements are a special case of coarse-grained measurements.

Given the post-measurement system, to retrodict the measurement outcome we must be able to distinguish between the $k$ possible post-measurement states $\rho_k$. We will say that the retrodiction is perfect if the probability of error is zero and the retrodiction is deterministic, i.e., the probability of the attempt at retrodiction giving an inconclusive result is also zero. Perfect retrodiction will be possible only if the $\rho_k$ are orthogonal, that is

$$\text{Tr}(\rho_{k'} \rho_k) = \text{Tr}(\rho_k^2) \delta_{kk'},$$  \hspace{1cm} (2.7)

or equivalently, that

$$\rho_{k'} \rho_k = \rho_k^2 \delta_{kk'}.$$  \hspace{1cm} (2.8)

Even if, for every initial state $\rho$, the final states $\rho_k$ are orthogonal, it could be the case that a different measurement is required to distinguish between the final states.
for each initial state. So, it would appear that there are two distinct cases to consider when examining the issue of whether the outcome of a generalised measurement can be perfectly retrodicted for an arbitrary initial state, corresponding to whether the initial state is known or unknown. The former case is clearly at least as favourable as the latter, since in the former there is the possibility of tailoring the retrodicting measurement to suit the possible final states, and by implication the initial state, which we cannot do in the latter case. It follows that if perfect retrodiction of the outcome of a generalised measurement $\mathcal{M}_Q$ is possible for an arbitrary, known, initial state, then it is also possible if the initial state is unknown. The following theorem gives a necessary and sufficient condition for perfect outcome retrodiction for all initial states, and moreover shows that there is, in fact, no advantage to be gained when the initial state, though arbitrary, is known.

**Theorem 1** A quantum system $Q$ is initially prepared in the state $|\psi\rangle\in\mathcal{H}_Q$. A generalised measurement $\mathcal{M}_Q$ with $N$ POVM elements $\Pi_k$ and Kraus operators $A_{kr}$ satisfying Eq. (2.5) is carried out on $Q$. The Hilbert space of the post-measurement states $\mathcal{H}_Q$ has dimension $D_Q$. A necessary and sufficient condition for the outcome of $\mathcal{M}_Q$ to be perfectly retrodictable for every initial state $|\psi\rangle\in\mathcal{H}_Q$ is

$$A_{kr}^\dagger A_{kr} = \delta_{kk'}A_{kr}^\dagger A_{kr}, \quad (2.9)$$

for all $r, r'\in\{1, \ldots, R\}$ and irrespective of whether or not $|\psi\rangle$ is known.

**Proof.** We will prove this theorem by establishing the necessity of condition (2.9) when the initial state is arbitrary and known. Subsequently, we will show that this condition is sufficient when the initial state is arbitrary and unknown. Thus, knowing the state confers no benefits in the context of this problem. To prove necessity, we will make use of the unnormalised final density operators

$$\tilde{\rho}_k = \sum_{r=1}^{R} A_{kr}|\psi\rangle\langle\psi| A_{kr}^\dagger. \quad (2.10)$$

We do this to avoid unnecessary complications which arise when the probability of one of the outcomes is zero. When this is so, the corresponding unnormalised final density operator will also be zero, but shall see that this causes no problems.

From Eq. (2.7), we see that the necessary condition for perfect outcome retrodiction given the initial state $|\psi\rangle$ is

$$\text{Tr}(\tilde{\rho}_{k'}\tilde{\rho}_k) = 0, \quad (2.11)$$

when $k\neq k'$ and for all $|\psi\rangle\in\mathcal{H}_Q$. This is the sole condition for perfect retrodictability we will impose in order to establish the necessity of Eq. (2.9). It says that the final states are orthogonal, which must be true if we can distinguish between them perfectly (using a projective measurement.) We do not require that the same distinguishing measurement is suitable for all initial states, so we take the initial state to be known, and assume that the appropriate distinguishing measurement can always be carried out.

Substituting (2.10) into (2.11), we find that

$$\text{Tr} \left( \sum_{r, r'=1}^{R} A_{kr'}|\psi\rangle\langle\psi| A_{kr'}^\dagger A_{kr}|\psi\rangle A_{kr}^\dagger \right),$$

$$= \sum_{r, r'=1}^{R} |\langle\psi| A_{kr'}^\dagger A_{kr}|\psi\rangle|^2 = 0, \quad (2.12)$$

for $k\neq k'$. From this, we see that

$$\langle\psi| A_{kr'}^\dagger A_{kr}|\psi\rangle = \delta_{kk'}\langle\psi| A_{kr'}^\dagger A_{kr}|\psi\rangle,$$

$$\Rightarrow \langle\psi| A_{kr'}^\dagger A_{kr} - \delta_{kk'}A_{kr'}^\dagger A_{kr'} |\psi\rangle = 0 \quad (2.13)$$

for all $r, r'\in\{1, \ldots, R\}$ and all $|\psi\rangle\in\mathcal{H}_Q$, which implies Eq. (2.9). This proves necessity.

We now prove that Eq. (2.9) is a sufficient condition for perfect outcome retrodiction when the initial state is both arbitrary and unknown. We show that there exists a projective measurement which is independent of the initial state and can be used to distinguish perfectly between the post-measurement states $\rho_k$. Consider the following subspaces of $\mathcal{H}_Q$:

$$\tilde{\mathcal{H}}_{Qk} = \text{span} \left\{ |\phi\rangle\in\mathcal{H}_Q : \langle\phi| \left( \sum_{r=1}^{R} A_{kr} A_{kr}^\dagger \right) |\phi\rangle > 0 \right\}, \quad (2.14)$$

that is, $\tilde{\mathcal{H}}_{Qk}$ is the support of the operator $\sum_{r} A_{kr} A_{kr}^\dagger : \mathcal{H}_Q\rightarrow\tilde{\mathcal{H}}_{Qk}$. Let $P_k : \mathcal{H}_Q\rightarrow\tilde{\mathcal{H}}_{Qk}$ be the projector onto $\tilde{\mathcal{H}}_{Qk}$. We will prove that when Eq. (2.9) is satisfied, these projectors are orthogonal and form a projective measurement which can always be used to distinguish perfectly between the post-$\mathcal{M}_Q$ states.

To show that they form a projective measurement, define

$$G_k = \sum_{r=1}^{R} A_{kr} A_{kr}^\dagger. \quad (2.15)$$

Eq. (2.9) implies that

$$G_k G_{k'} = \delta_{kk'} G_{k}^2. \quad (2.16)$$

It follows from this, and the positivity of the $G_k$, that, when $k\neq k'$, every eigenvector of $G_k$ corresponding to a non-zero eigenvalue is orthogonal to every eigenvector of $G_{k'}$ corresponding to a non-zero eigenvalue. Let $\mathcal{H}_G$ be the support of the operator $\sum_{kr} A_{kr} A_{kr}^\dagger$, having dimension $D_G$. It follows from Eq. (2.16) that $\mathcal{H}_G$ has an orthonormal basis $\{|g_j\rangle\}$ in terms of which we can write

$$G_k = \sum_{j=1}^{D_G} g_{jk}|g_j\rangle\langle g_j|, \quad (2.17)$$
where
\[ g_{jk}g_{j'k'} = \delta_{kk'}g_{jk}g_{j'k'} \forall j, j'. \] (2.18)

It follows from Eq. (2.17) that
\[ P_k = \sum_{j:j_k \neq 0} |g_j\rangle\langle g_j|. \] (2.19)

Making use of Eq. (2.18), we see that these projectors are orthogonal, i.e.
\[ P_k P_{k'} = \delta_{kk'} P_k. \] (2.20)

They are also complete on the space \( \tilde{H}_Q \). To prove that a projective measurement based on these projectors can distinguish perfectly between the \( \rho_k \), we make use of the fact that the support of \( \tilde{\rho}_k \) is a subspace of \( \tilde{H}_Q_k \). To prove this, we make use of the fact that the positivity of 1\( _Q - \rho \) implies that
\[ \tilde{\rho}_k \leq G_k. \] (2.21)

In other words,
\[ \langle \phi|\tilde{\rho}_k|\phi\rangle \leq \langle \phi|G_k|\phi\rangle \forall|\phi\rangle \in \tilde{H}_Q. \] (2.22)

Hence, every state \( |\phi\rangle \) which is in the support of \( \tilde{\rho}_k \) is also in \( \tilde{H}_Q k \), the support of \( G_k \). Furthermore, for any final state \( \rho_k \) with non-zero outcome probability, the support of \( \rho_k \) is the same as that of \( \tilde{\rho}_k \). The fact that the subspaces \( \tilde{H}_Q_k \) are orthogonal can thus be perfectly distinguished using a projective measurement on the space \( \tilde{H}_Q \) based on the projectors \( P_k \) enables us to distinguish between the states \( \rho_k \) with the same projective measurement, irrespective of the initial state \( |\psi\rangle \). This completes the proof. \( \square \)

The fact that (2.19) is a sufficient condition for perfect outcome retrodiction when \( |\psi\rangle \) is an arbitrary, unknown pure state \( |\psi\rangle \) can easily be seen to imply that it is also sufficient when the initial state is an arbitrary mixed state \( \rho \).

Theorem 1 implies the following for fine-grained measurements:

**Theorem 2** A quantum system \( Q \) is initially prepared in the state \( |\psi\rangle \in H_Q \). A fine-grained generalised measurement \( M_Q \) is carried out on \( Q \). If \( D_Q = D_Q \), the outcome of \( M_Q \) is perfectly retrodictible for all \( |\psi\rangle \in H_Q \), irrespective of whether or not \( |\psi\rangle \) is known, if and only if \( M_Q \) is a projective measurement followed by a unitary transformation from \( H_Q \) to \( H_Q \), that is
\[ \Pi_k \Pi_k = \delta_{kk} \Pi_k, \] (2.23)

where each POVM element is related to its corresponding Kraus operator in the following way:
\[ A_k = U \Pi_k. \] (2.24)

and \( U \) is a unitary transformation from \( H_Q \) to \( \tilde{H}_Q \).

**Proof.** For a fine-grained measurement, we see that it follows from Eq. (2.9) that a necessary and sufficient condition for perfect outcome retrodiction with an arbitrary, known or unknown, initial state \( |\psi\rangle \in H_Q \) is
\[ A^\dagger_{j'} A_k = \delta_{kk'} A^\dagger_{j'} A_k. \] (2.25)

Sufficiency is easily proven. When Eqs. (2.23) and (2.24) are satisfied, we see that
\[ A^\dagger_{j'} A_k = \Pi_k \Pi_k = \delta_{kk'} A^\dagger_{j'} A_k. \] This proves sufficiency. To prove necessity, we notice that, for fine-grained measurements, Eqs. (2.3) and (2.9) imply
\[ A^\dagger_{k'} A_k = \Pi_k \delta_{kk'}. \] (2.26)

If we sum both sides of this with respect to \( k \) and \( k' \), and make use of the resolution of the identity (2.1), we find that
\[ \left( \sum_{k'=1}^N A^\dagger_{k'} \right) \left( \sum_{k=1}^N A_k \right) = 1_Q, \] (2.27)

which implies that \( \sum_{k=1}^N A_k \) is an isometry, which, if \( D_Q = D_Q \), is necessarily unitary. We will write
\[ \sum_{k=1}^N A_k = U. \] (2.28)

Summing both sides of Eq. (2.26) over \( k' \), and making use of the adjoint of Eq. (2.28), we obtain
\[ A_k = U \Pi_k. \] (2.29)

Substituting this into Eq. (2.26) gives
\[ \Pi_k \Pi_k = \Pi_k \delta_{kk'}. \] (2.30)

So, the POVM elements of the measurement \( M_Q \) form a set of orthogonal projectors. Thus, if perfect retrodiction of the outcome of a fine-grained measurement is possible for every initial state, even if the actual state is known, then when the input and output Hilbert spaces have the same dimension, the measurement is a projective measurement followed by a unitary transformation. This completes the proof. \( \square \)

It is natural to examine in more detail the issue of outcome retrodictability for more general, coarse-grained measurements. As we shall see, there do exist coarse-grained measurements which are highly dissimilar to projective measurements for which perfect outcome retrodiction is possible. Prior to showing this, we make the following observation which will put our findings in context. The statistical properties of a generalised measurement are determined solely by the POVM elements \( \Pi_k \). These operators can always be decomposed in the manner of (2.5). This decomposition is non-unique, so a POVM with elements \( \Pi_k \) defines an equivalence class \( \mathcal{E}((\Pi_k)) \).
of measurements, each element of which corresponds to a particular coarse-grained operator-sum decomposition of the form (2.6) with fine-grained decompositions being special cases. Having these ideas in mind, we can ask the following question: under what circumstances does the equivalence class associated with a particular POVM contain a generalised measurement whose outcome is perfectly retrodictable for an arbitrary pure initial state? For generalised measurements with a finite number of outcomes, this is answered by the following theorem:

**Theorem 3** Let \( \mathcal{E}(\{\Pi_k\}) \) be the equivalence class of generalised measurements associated with a particular POVM with \( N < \infty \) elements \( \Pi_k \), where these operators act on the Hilbert space \( \mathcal{H}_Q \) of a quantum system \( Q \). This space has dimension \( D_Q \). The Hilbert space of the post-measurement states, \( \mathcal{H}_{\tilde{Q}} \), has dimension \( \tilde{D}_Q \). A necessary and sufficient condition for the existence of a measurement \( \mathcal{M}_{Q} \in \mathcal{E}(\{\Pi_k\}) \) whose outcome is perfectly retrodictable for an arbitrary pure initial state is

\[
N \leq \tilde{D}_Q. \tag{2.31}
\]

**Proof.** To prove necessity we make use of the fact that for every generalised measurement with \( N < \infty \) outcomes, there exists a state vector \( |\psi\rangle \in \mathcal{H}_Q \) such that \( P(k|\psi) > 0 \ \forall \ k \in \{1, \ldots, N\} \). To see why this is so, let \( K_k \) be the kernel of \( \Pi_k \). None of the \( \Pi_k \) are equal to the zero operator, so the space \( K_k \) is at most \( D_Q - 1 \) dimensional. It follows that if there is no vector \( |\psi\rangle \in \mathcal{H}_Q \) such that \( \langle \psi|\Pi_k|\psi\rangle > 0 \ \forall \ k \in \{1, \ldots, N\} \), then every \( |\psi\rangle \in \mathcal{H}_Q \) is an element of at least one of the \( K_k \). We conclude that \( \mathcal{H}_Q = \cup_{k=1}^{N} K_k \). This statement, that the \( D_Q \) dimensional Hilbert space \( \mathcal{H}_Q \) is the union of a finite set of Hilbert spaces of strictly lower dimension, is clearly false. For example, a two dimensional plane is not the union of a finite set of one dimensional rays. Hence, for each generalised measurement with a finite number of potential outcomes, there exists a pure initial state for which all of these outcomes have non-zero probability of occurrence.

Suppose that \( Q \) is initially prepared such a state. The final state corresponding to the \( k \)th outcome is \( \rho_k \). If Eq. (2.31) is not satisfied, then the number of final states will exceed the dimension \( \tilde{D}_Q \) of \( \mathcal{H}_{\tilde{Q}} \). To retrodict the outcome of the measurement perfectly, we must be able to distinguish between the states \( \rho_k \) perfectly. The supports of these states must be orthogonal, which is clearly impossible if their number exceeds the dimension of \( \mathcal{H}_Q \). This proves necessity.

We will prove sufficiency constructively, which is to say that we will explicitly derive a measurement in the equivalence class corresponding to any POVM which satisfies Eq. (2.31) for which the outcome is perfectly retrodictable for an arbitrary pure initial state. To begin, we write the \( \Pi_k \) in spectral decomposition form

\[
\Pi_k = \sum_{r=1}^{D_Q} \pi_{kr} |\pi_{kr}\rangle \langle \pi_{kr}|, \tag{2.32}
\]

where the \( \pi_{kr} \) are real and non-negative and, for each \( k \), the set \( \{|\pi_{kr}\rangle\} \) is an orthonormal basis for \( \mathcal{H}_{\tilde{Q}} \). We require a set of Kraus operators \( A_{kr} : \mathcal{H}_{\tilde{Q}} \to \mathcal{H}_{\tilde{Q}} \) satisfying

\[
\Pi_k = \sum_{r=1}^{D_Q} A_{kr}^\dagger A_{kr}, \tag{2.33}
\]

for the \( \Pi_k \) defined by Eq. (2.32) and which satisfy the perfect retrodiction condition in Eq. (2.9). To this end, consider

\[
A_{kr} = \sqrt{\pi_{kr}} |x_k\rangle \langle \pi_{kr}|, \tag{2.34}
\]

where the set \( \{|x_k\rangle\} \) is any set of \( N \) orthonormal states in \( \mathcal{H}_{\tilde{Q}} \). Notice that this construction is possible only if (2.31) is satisfied. The orthonormality of the \( |x_k\rangle \) implies that the \( A_{kr} \) satisfy the perfect outcome retrodictability condition Eq. (2.9). One can also easily verify that they are related to the \( \Pi_k \) in Eq. (2.33) through Eq. (2.34). This completes the proof.\[\square\]

The foregoing discussion has been somewhat abstract. It would be helpful to have a concrete physical understanding of how these measurements can be implemented. Generalised measurements are commonly understood as resulting from a unitary interaction with an ancillary system, followed by a projective measurement on the latter. For \( D_Q = D_Q \), we shall see how to form a unitary-projection implementation of any POVM which satisfies Eq. (2.31) whose outcome is perfectly retrodictable given what we shall shortly refer to as a standard implementation.

We begin with the following well-known fact about generalised measurements, as described, for example, by Kraus\[14\]. Suppose that we have a POVM \( \Pi_k \), with \( k \in \{1, \ldots, D_Q\} \) which we wish to measure. This POVM may be factorised as

\[
\Pi_k = B_k^\dagger B_k, \tag{2.35}
\]

for some operators \( B_k : \mathcal{H}_Q \to \tilde{\mathcal{H}}_Q \). Let us introduce a \( D_Q \) dimensional ancilla \( A_1 \) with Hilbert space \( \mathcal{H}_{A_1} \), initially prepared in the state \( |\chi\rangle \). For any operators \( B_k \) satisfying Eq. (2.35) and the resolution of the identity (2.1), there exists a unitary transformation \( U_{Q,A_1} : \mathcal{H}_{\tilde{Q}} \otimes \mathcal{H}_{A_1} \to \mathcal{H}_{\tilde{Q}} \otimes \mathcal{H}_{A_1} \) such that

\[
U_{Q,A_1} |\psi\rangle \otimes |\chi\rangle_{A_1} = \sum_{k=1}^{D_Q} (B_k|\psi\rangle) \otimes |x_k\rangle_{A_1}, \tag{2.36}
\]

where the \( \{|x_k\rangle\} \) is an orthonormal basis set for \( \mathcal{H}_{A_1} \). A measurement on \( A_1 \) in this basis, yielding the result \( k \), transforms the state of \( Q \) from \( |\psi\rangle \) into \( B_k|\psi\rangle / \sqrt{P(k|\psi)} \), with probability \( P(k|\psi) = \langle \psi|\Pi_k|\psi\rangle \). We will refer to this construction as a standard implementation of a POVM.

To obtain from this measurement a perfectly retrodictable one which is also in the equivalence class of the
same POVM, we introduce a further ancilla \( A_2 \) with \( D_Q \) dimensional Hilbert space \( \mathcal{H}_{A_2} \), also initially prepared in the state \( |\chi\rangle \). Following the action of \( U_{QA} \), we apply a unitary copying transformation on \( A_1,A_2 \) which perfectly copies the orthogonal states \( |x_k\rangle \), that is,
\[
\text{COPY}_{A_1,A_2} |x_k\rangle_{A_1} \otimes |\chi\rangle_{A_2} = |x_k\rangle_{A_1} \otimes |x_k\rangle_{A_2}.
\]
(2.37)
Since \( \tilde{D}_Q = D_Q \), we can carry out the SWAP operation on \( QA_1 \), which exchanges the states of these two systems. The entire unitary interaction between \( Q \) and the ancilla \( A_1,A_2 \) is then
\[
\text{SWAP}_{Q,A_1} \text{COPY}_{A_1,A_2} U_{QA_1} |\psi\rangle_Q \otimes |\chi\rangle_{A_1} \otimes |\chi\rangle_{A_2} = \sum_{k=1}^{D_Q} |x_k\rangle_Q \otimes (B_k|\psi\rangle)_{A_1} \otimes |x_k\rangle_{A_2}.
\]
(2.38)
Following this unitary interaction, we carry out a projective measurement on \( A_1,A_2 \), with the projection operators
\[
P_k = 1_{A_1} \otimes (|x_k\rangle \langle x_k|)_{A_2}.
\]
(2.39)
The probability \( P(k|\psi) \) of the \( k \)th outcome is easily shown to be \( \langle \psi|P_k|\psi\rangle \). The final state of \( Q \) is obtained by tracing the entire final state over the ancilla. If we write
\[
V = \text{SWAP}_{Q,A_1} \text{COPY}_{A_1,A_2} U_{QA_1},
\]
(2.40)
where \( V \) is clearly unitary, then when outcome \( k \) is obtained for the measurement based on the projects \( P_k \) in Eq. (2.39), the state of \( Q \) is transformed by the following completely positive, linear, trace non-increasing map:
\[
\Phi_k(\rho_Q) = \text{Tr}_{A_1A_2} \left( P_k V (\rho_Q \otimes |\chi\rangle_{A_1} \langle \chi|_{A_2}) V^\dagger \right),
\]
(2.41)
So, there is a one-to-one correspondence between the measurement outcomes and the orthonormal states \( |x_k\rangle \). This implies that the result of the measurement is perfectly retrodictable for an arbitrary initial quantum state.

It is often helpful to make use of the fact that every measurement \( M_Q \) on a quantum system \( Q \) by examining the final state when the initial state is arbitrary. Here we impose the less stringent condition that for some known, initial state, the outcome can always be retrodicted, unambiguously, which is to say with zero probability of error, with some some non-zero probability instead. We allow for the possibility that the retrodiction attempt gives an inconclusive result.

The issues that we discuss in this subsection are insensitive to the dimension \( D_Q \) of \( \mathcal{H}_Q \), provided that \( D_Q \geq D_Q \). For maximum generality, we should assume, and take advantage of the fact that \( Q \) can be initially entangled with some ancillary system \( A \), with corresponding Hilbert space \( \mathcal{H}_A \) having finite dimension \( D_A \). These systems are initially prepared in a joint state with corresponding density operator \( \rho_{QA} \). The measurement \( M_Q \) is carried out on \( Q \). For the sake of simplicity, we will consider only fine-grained measurements. Here, the final, normalised state corresponding to outcome \( k \) is obtained by the transformation
\[
\rho_{QA} \rightarrow \rho_{QA,k} = \frac{(A_k \otimes 1_A) \rho_{QA} (A_k^\dagger \otimes 1_A)}{P(k|\rho_{QA})}.
\]
(3.1)
Our aim is to retrodict the outcome of the measurement \( M_Q \) by distinguishing between the states \( \rho_{QA,k} \). To do this, we must perform a second measurement \( M_{QA} \) on \( QA \). This will be tailored so that its outcome matches that of \( M_Q \) as closely as possible. As we are interested in situations where the outcome is retrodicted unambiguously, the measurement \( M_{QA} \) will have \( N+1 \) outcomes: \( N \) of these correspond to the possible outcomes of \( M_Q \) and a further signals the failure of the retrodiction attempt, making this result inconclusive. So, we may represent this measurement by an \( N+1 \)-element POVM \( (\Xi_0,\Xi_1,\ldots,\Xi_N) \) for which
\[
\sum_{k=0}^{N} \Xi_k = 1_{QA}.
\]
(3.2)
The condition for error-free unambiguous outcome retrodiction may be written as
\[
\text{Tr}(\Xi_{k'} \rho_{QA,k}) = \text{Tr}(\Xi_k \rho_{QA,k}) \delta_{kk'},
\]
(3.3)
for \( k,k' \in \{1,\ldots,N\} \). The probability that the retrodiction attempt gives an inconclusive result is
\[
P(?|\rho_{QA}) = \text{Tr} \left( \Xi_0 \sum_{k=0}^{N} (A_k \otimes 1_A) \rho_{QA} (A_k^\dagger \otimes 1_A) \right).
\]
(3.4)
Under what conditions does there exist an initial state $\rho_{QA}$ for which the outcome of the fine-grained measurement $M_Q$ is unambiguously retrodictable? To address this question, we may, without loss of generality take the initial state to be a pure state $\rho_{QA} = |\psi_{QA}\rangle\langle\psi_{QA}|$, since any mixed state can be purified by considering a sufficiently large ancilla $A$. The Schmidt decomposition theorem implies that we can always take the dimensionality of $H_A$ to be at most $D_Q$. We will now prove

**Theorem 4** A sufficient condition for the existence of an initial state $|\psi_{QA}\rangle \in H_{QA}$ for which the outcome of a fine-grained measurement $M_Q$ is unambiguously retrodictable is that the corresponding Kraus operators are linearly independent. When this is the case, the outcome of $M_Q$ is unambiguously retrodictable for any known $|\psi_{QA}\rangle \in H_{QA}$ with maximum Schmidt rank. When the Kraus operators are non-singular, linear independence is also a necessary condition for the existence of an initial state $|\psi_{QA}\rangle \in H_{QA}$ for which the outcome of $M_Q$ can be unambiguously retrodicted.

**Proof.** We will first prove necessity for non-singular Kraus operators. Consider the final states

$$\rho_{QA}(\lambda) = \sum_{j=1}^{D_Q} c_j |\psi_{QA}^j\rangle\langle\psi_{QA}^j|_A,$$

where $(\{x_j\})$ is an orthonormal basis for $H_Q$ and $(\{y_j\})$ is an orthonormal subset of $H_A$. When outcome $k$ is obtained, the post-measurement state is

$$\rho_{QA}(\lambda) = \sum_{j=1}^{D_Q} c_j^2 |\psi_{QA}\rangle_{QA} \langle\psi_{QA}|_A.$$

where the probability of outcome $k$ is

$$P(k|\psi_{QA}) = \sum_{j=1}^{D_Q} c_j^2 \langle x_j | \Pi_k | x_j \rangle.$$

We will assume that $|\psi_{QA}\rangle$ has maximum Schmidt rank, that is, that all of the $c_j$ are non-zero. For any initial state with this property, all of the outcome probabilities $P(k|\psi_{QA})$ are non-zero, even if some of the $A_k$ are singular. To prove this, let $c > 0$ be the smallest of the $|c_j|$. Then $P(k|\psi_{QA}) \geq c^2 \sum_{j=1}^{D_Q} \langle x_j | \Pi_k | x_j \rangle = c^2 \text{Tr}(\Pi_k)$. The $\Pi_k$ are positive operators, which, while not necessarily being positive definite, are nevertheless non-zero. Hence, $\text{Tr}(\Pi_k) > 0 \forall k \in \{1, \ldots, N\}$. From this, it follows that $P(k|\psi_{QA}) > 0 \forall k \in \{1, \ldots, N\}$.

Suppose now that unambiguous outcome retrodiction is impossible, that is, that the final states $|\psi_{QA}\rangle$ are linearly dependent. There would then exist coefficients $\alpha_k$, not all of which are zero, such that

$$\sum_{k=1}^{N} \alpha_k |\psi_{QA}\rangle = 0.$$  \hspace{1cm} (3.9)

If we again let $\beta_k = \alpha_k P(k|\psi_{QA})^{-1/2}$, then we see that these are not all zero and that, with the help of Eq. (3.7), this linear dependence condition can be written as

$$\sum_{k=1}^{N} \beta_k \sum_{j=1}^{D_Q} c_j\langle A_k | x_j \rangle\langle y_j | A \rangle = 0.$$  \hspace{1cm} (10.10)

Taking the partial inner product of this with $\langle y_j |$ and dividing the result by $c_j$, we find

$$\sum_{k=1}^{N} \beta_k A_k | x_j \rangle = 0 \forall j.$$  \hspace{1cm} (11.11)

Finally, we make use of the completeness of the $|x_j\rangle$ and see that this, when combined with Eq. (11.11), gives

$$\sum_{k=1}^{N} \beta_k A_k = \sum_{k=1}^{N} \beta_k A_k \sum_{j=1}^{D_Q} |x_j\rangle \langle x_j| = 0.$$  \hspace{1cm} (12.12)

that is, the $A_k$ must be linearly dependent. So, for an initial state which is pure with maximum Schmidt rank, if the final states are unambiguously distinguishable, which is to say that they are linearly dependent, then the Kraus operators are also linearly dependent. This completes the proof. \hspace{1cm} $\square$

This theorem has some interesting consequences that we shall now describe. The first is in relation to general quantum operations. These are described by completely positive, linear, trace non-increasing maps $\rho \rightarrow \Phi(\rho) = \sum_{k=1}^{N} A_k \rho A_k^{\dagger}$, where $\sum_{k=1}^{N} A_k^{\dagger} A_k \leq I_Q$. In a well-known theorem, Choi\cite{choi} showed that every such map has an operator-sum decomposition in terms of linearly independent Kraus operators $A_k$. Combining this fact with Theorem 4, we see that for each trace-preserving quantum operation $\Phi$, there exists a fine-grained generalised measurement whose Kraus operators form an operator-sum decomposition of $\Phi$ and whose outcome is unambiguously
retrodiction for all pure initial states with maximum Schmidt rank.

A second consequence of this theorem relates to the problem of distinguishing between unitary operators. Childs et al. [14] and Acín [17] have addressed the problem of distinguishing between a pair of unitary operators. Theorem 4 enables us to say something about the more general problem of distinguishing between $N$ unitary operators.

The problem is this: a quantum system $Q$ and an ancilla $A$ are initially prepared in the possibly entangled state $\rho_{QA}$. With probability $p_k$, $Q$ is subjected to one of the $N$ unitary operators $U_k$. The entire state undergoes the transformation

$$\rho_{QA} \rightarrow \rho_{QA,k} = (U_k \otimes 1_A) \rho_{QA} (U_k^\dagger \otimes 1_A),$$  \hspace{1cm} (3.13)

with probability $p_k$. The aim is to determine which unitary operator has been applied. This is done by distinguishing between the final states $\rho_{QA,k}$.

Comparison of Eq. (3.13) with Eq. (3.1) shows that this procedure can be regarded as a particular example of retrodiction of the outcome of a fine-grained generalised measurement, specifically one which has the Kraus operators

$$A_k = \sqrt{p_k} U_k.$$ \hspace{1cm} (3.14)

Clearly, when all of the $p_k$ are non-zero, then linear independence of the $A_k$ is equivalent to that of the $U_k$. It follows from this and the non-singularity of unitary operators that a necessary and sufficient condition for being able to unambiguously discriminate between $N$ unitary operators $U_k$ for some, possibly entangled, initial state is that they are linearly independent.

Theorem 4 gives a special status to generalised measurements with non-singular Kraus operators. Measurements of this kind might appear to be somewhat artificial constructions. After all, neither projective measurements nor many of the optimal generalised measurements for the various kinds of state discrimination have this property. However, it has recently been suggested by Fuchs and Jacobs [34] that such measurements may, in practice, be the rule rather than the exception. They argue that a measurement for which a particular outcome is impossible to achieve for some initial state is an idealisation that would require infinite resources to implement (infinite precision in tuning interactions, timings etc.) Accordingly, realistic, finite-strength measurements do not possess this property and have non-singular POVM elements or equivalently, for fine-grained measurements, Kraus operators.

Of course, this reasoning also applies to the measurement which retrodicts the outcome of $M_Q$. Unambiguous outcome retrodiction will, in general, require that the Kraus operators of the retrodicting measurement are highly singular. While, for the reasons given above, this is difficult, even impossible to achieve in practice, there are, as far as we are aware, no fundamental limitations on how well these idealised measurements can be approximately implemented. Finite-strength measurements will have a special status with regard to unambiguous outcome retrodiction if the measurement whose outcome we are trying to retrodict is not as strong as the retrodicting measurement.

It should also be noted that when some of the Kraus operators are singular, linear independence is not, in general, a necessary condition for unambiguous outcome retrodiction for some initial state. As a counter-example, consider the case of $\mathcal{H}_Q$ being three dimensional and spanned by the orthonormal vectors $|x\rangle$, $|y\rangle$ and $|z\rangle$. Consider now a fine-grained measurement with the singular, linearly dependent Kraus operators

$$A_1 = \frac{|x\rangle \langle x|}{\sqrt{2}},$$ \hspace{1cm} (3.15)
$$A_2 = \frac{|y\rangle \langle y|}{\sqrt{2}},$$ \hspace{1cm} (3.16)
$$A_3 = |z\rangle \langle z|,$$ \hspace{1cm} (3.17)
$$A_4 = \frac{|x\rangle \langle x| + |y\rangle \langle y|}{\sqrt{2}}.$$ \hspace{1cm} (3.18)

If the initial state is $|z\rangle$, then we know a priori that the only possible outcome is ‘3’, so knowing that this state was prepared enables us to perfectly retrodict the outcome without having access to the measurement record.

B. Without entanglement

The final issue we shall investigate is unambiguous outcome retrodiction without entanglement. For the sake of simplicity, we again confine our attention to fine-grained measurements. When $Q$ is initially prepared in the pure state $|\psi\rangle$, then the final state corresponding to the $k$th outcome is, up to a phase

$$|\psi_k\rangle = \frac{A_k|\psi\rangle}{\sqrt{P(k|\psi)}},$$ \hspace{1cm} (3.19)

when the probability $P(k|\psi)$ of the $k$th outcome is non-zero. Unambiguous retrodiction of the outcome of $M_Q$ with the initial state $|\psi\rangle$ is possible only if the final states which have non-zero probability are linearly independent. Actually, in what follows it will, for reasons that will become apparent, be more convenient to enquire as to when unambiguous retrodiction is impossible for every initial state in $\mathcal{H}_Q$. Let $\sigma(\psi)$ be the subset of $\{1, \ldots, N\}$ for which $A_k|\psi\rangle \neq 0$ when $k \in \sigma(\psi)$. Then unambiguous retrodiction of the outcome of $M_Q$ is impossible for every pure initial state $|\psi\rangle \in \mathcal{H}_Q$ iff there exist coefficients $\alpha_k(\psi)$, not all of which are zero for $k \in \sigma(\psi)$, such that

$$\left( \sum_{k \in \sigma(\psi)} \alpha_k(\psi)A_k \right)|\psi\rangle = 0,$$ \hspace{1cm} (3.20)
for all $|\psi\rangle \in \mathcal{H}_Q$, which is to say iff the possible final states are linearly dependent for all initial states. In particular, for a finite-strength measurement, the $A_k$ are non-singular and so $\sigma(|\psi\rangle) = \{1, \ldots, N\}$. In this case, the impossibility condition is that for each $|\psi\rangle \in \mathcal{H}_Q$, there exist coefficients $\alpha_k(\psi)$, not all of which are zero, such that

$$
\left( \sum_{k=1}^{N} \alpha_k(\psi) A_k \right) |\psi\rangle = 0.
$$

(3.21)

Operators $A_k$ with this property are said to be **locally linearly dependent**.

Locally linearly dependent sets of operators have been investigated in detail by Šemrl and coworkers [12–13]. Notice that local linear dependence is weaker than linear dependence, which is the special case of the $\alpha_k$ being independent of $|\psi\rangle$.

Equivalently, it is necessary, though not sufficient for a set of operators to be locally independent to not be locally linearly dependent. Consequently, it is sufficient for the outcome of a finite-strength, fine-grained measurement to be unambiguously retrodictable for a single unentangled state for it to be unambiguously retrodictable for all maximum Schmidt rank entangled states, but not vice versa. Consider, for example, the four, non-singular, Pauli operators $(1, \sigma_x, \sigma_y, \sigma_z)$. Though linearly independent, these operators are locally linearly dependent. So, as far as pure states are concerned, an entangled initial state is required to unambiguously determine which operator has been implemented, as in dense coding [13]. More generally, the non-singularity of unitary operators implies that a necessary and sufficient condition for a set of unitary operators to be unambiguously distinguishable with a pure, non-entangled initial state is that they are not locally linearly dependent.

Having made the distinction between linear dependence and local linear dependence, which is responsible for the fact that there exist finite-strength measurements whose outcomes are unambiguously retrodictable for some entangled but no unentangled, pure, initial states, one particular question forces itself upon us: given that the outcome of a measurement is unambiguously retrodictable with an entangled, pure initial state, what subsidiary conditions must the measurement satisfy for its outcome to be unambiguously retrodictable for some non-entangled, pure initial state? For finite-strength measurements, this question is equivalent to: under what conditions is a linearly independent set of Kraus operators, subject, of course, to the resolution of the identity, not a locally linearly dependent set?

The problem of determining when a linearly independent set of operators is not a locally linearly dependent set has been solved for the special cases $N = 2, 3$ [12]. The solutions for $N \geq 4$ are not known at this time. Progress has, however, been made with regard to this problem. It has been shown by Brešar and Šemrl [12] that the solution for arbitrary $N$ can be deduced from that of the problem of classifying the maximal vector spaces of $N \times N$ matrices with zero determinant. However, this is also currently unknown.

We will examine here the solution for $N = 2$ and unravel its implications. Here, we are considering a finite-strength measurement with two outcomes having corresponding Kraus operators $A_1$ and $A_2$. Brešar and Šemrl [12] have shown that the following two statements are equivalent:

(i) $A_1$ and $A_2$ are locally linearly dependent.

(ii) (a) $A_1$ and $A_2$ are linearly dependent or (b) there exists a vector $|\phi\rangle \in \mathcal{H}_Q$ such that $\text{span}\{A_1|\psi\rangle : |\psi\rangle \in \mathcal{H}_Q\} = \text{span}\{A_2|\psi\rangle : |\psi\rangle \in \mathcal{H}_Q\} = \mathcal{H}_\phi$, where $\mathcal{H}_\phi$ is the one-dimensional subspace of $\mathcal{H}_Q$ spanned by $|\phi\rangle$.

It follows that if $A_1$ and $A_2$ are linearly independent and also locally linearly dependent, then condition (ii) must be satisfied. This condition, when combined with the resolution of the identity, implies that $D_Q = 2$ and that $\mathcal{H}_Q$ has an orthonormal basis $\{|x\rangle, |y\rangle\}$ such that

$$
A_1 = |\phi\rangle \langle x|,
$$

(3.22)

$$
A_2 = |\phi\rangle \langle y|.
$$

(3.23)

These operators are clearly singular. It follows that for every two-outcome, fine-grained, finite strength measurement, if the Kraus operators are not locally dependent, then they are not locally linearly dependent either. So, for such measurements, if the outcome can be unambiguously retrodicted for some entangled initial state, then it can also be unambiguously retrodicted for some non-entangled initial pure state.

Let us conclude with an examination of the possibility of unambiguous outcome retrodiction for all initial states $|\psi\rangle \in \mathcal{H}_Q$. For a finite-strength, fine-grained measurement, the necessary and sufficient condition for this to be possible is that for every pure, initial state, the set of $N$ pure, post-measurement states is a linearly independent set. Formally, this requirement can be expressed as

$$
\left( \sum_{k=1}^{N} \alpha_k A_k \right) |\psi\rangle \neq 0,
$$

(3.24)

for all non-zero $|\psi\rangle \in \mathcal{H}_Q$ and all complex coefficients $\alpha_k$ unless $\alpha_k = 0 \forall k \in \{1, \ldots, N\}$. A set of operators $A_k$ with this property can be said to be **locally linearly independent**. Local linear dependence and local linear independence are not, like linear dependence and independence, complementary concepts. For example, no set of two Pauli operators is either locally linearly dependent or locally linearly independent.

Local linear independence is a considerably stronger condition than linear independence. So strong, in fact, that if $\mathcal{H}_Q$ and $\mathcal{H}_Q$ are finite dimensional and $D_Q \leq D_Q$, then it cannot be satisfied (except in the trivial case of
the equality and a single, non-singular operator.) It is easy to see that locally linearly independent operators must be non-singular, so that this condition cannot be satisfied if \( D_Q < D_Q \). To prove that it cannot be satisfied when \( D_Q = D_Q \) either, we make use of the fact that any subset of a locally linearly independent set must also be locally linearly independent. Let us then consider just two operators, \( A_1 \) and \( A_2 \). These operators must be non-singular. This implies, in the finite dimensional case, that if \( D_Q = D_Q \), they must have unique left and right inverses.

Given that \( A_1 \) and \( A_2 \) are non-singular, it follows that \( A_1^{-1}A_2 \) must also be non-singular. It then has \( D_Q \) linearly independent eigenvectors with non-zero eigenvalues. Let \( \lambda \neq 0 \) be an eigenvalue of \( A_1^{-1}A_2 \) with corresponding eigenvector \( |\psi\rangle \). Now consider

\[
A_1^{-1}(-\lambda A_1 + A_2)|\psi\rangle = (-\lambda + \lambda)|\psi\rangle = 0. \tag{3.25}
\]

Operating throughout this equation with \( A_1 \), we find that

\[
(-\lambda A_1 + A_2)|\psi\rangle = 0, \tag{3.26}
\]

and so the operators \( A_1 \) and \( A_2 \) cannot be locally linearly independent. From this, it follows that, for finite dimensional quantum systems, if the dimension of the output Hilbert space does not exceed that of the input Hilbert space, then fine-grained measurements with locally linearly independent Kraus operators are impossible. However, one can devise examples of such measurements for finite dimensional quantum systems if the dimension of the output Hilbert space does not exceed that of the input Hilbert space. Let \( D_Q = 2 \) and \( D_Q = 4 \). Also, let \( \{|x_1\rangle, |x_2\rangle\} \) and \( \{|\tilde{x}_1\rangle, |\tilde{x}_2\rangle, |\tilde{x}_3\rangle, |\tilde{x}_4\rangle\} \) be orthonormal basis sets for \( \mathcal{H}_Q \) and \( \mathcal{H}_Q \) respectively. Consider now a two-outcome, fine-grained measurement whose Kraus operators have the following matrix representations in these bases:

\[
A_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \tag{3.27}
\]

that is, the row-\( j \), column-\( k \) element of \( A_k \) is \( \langle \tilde{x}_j | A_k | x_k \rangle \).

One can easily verify that \( A_1^\dagger A_1 + A_2^\dagger A_2 = I_Q \), and so these operators constitute a fine-grained measurement. To prove that they are locally linearly independent, let us write an arbitrary pure initial state in \( \mathcal{H}_Q \) as \( |\psi\rangle = c_1|x_1\rangle + c_2|x_2\rangle \). Then,

\[
(\alpha_1 A_1 + \alpha_2 A_2)|\psi\rangle = \frac{c_1(\alpha_1|x_1\rangle + \alpha_2|\tilde{x}_2\rangle) + c_2(\alpha_1|\tilde{x}_3\rangle + \alpha_2|\tilde{x}_4\rangle)}{\sqrt{2}} \tag{3.28}
\]

As a consequence of the orthonormality of the \( |\tilde{x}_j\rangle \), when either or both \( c_1 \) and \( c_2 \) are non-zero, this expression is never equal to the zero vector unless \( \alpha_1 \) and \( \alpha_2 \) are equal to 0. Hence, the operators \( A_1 \) and \( A_2 \) are locally linearly independent. In fact, these operators satisfy the condition in Eq. (2.9) for perfect operators for an arbitrary initial state condition in \( \mathcal{H}_Q \).

There also exist interesting examples of measurements with locally linearly independent Kraus operators on infinite dimensional quantum systems. Consider a bosonic mode with Hilbert space spanned by the orthonormal occupation number states \( |n\rangle \), \( n = 0, 1, 2, \ldots \). Now consider a two-outcome generalised measurement with the Kraus operators \( A_1 = \mu \sum_{n=0}^{\infty} (|n+1\rangle\langle n| \) and \( A_2 = \sqrt{1 - |\mu|^2} \sum_{n=0}^{\infty} |n\rangle\langle n| \), where \( 0 < |\mu| < 1 \). It is a simple matter to show that \( A_1^\dagger A_1 + A_2^\dagger A_2 = \sum_{n=0}^{\infty} |n\rangle\langle n| = 1 \), so that these operators do indeed form a fine-grained generalised measurement. To show that these operators are locally linearly independent, let the initial state of the system be the pure state \( |\psi\rangle = \sum_{n=0}^{\infty} c_n|n\rangle \), where at least one of the \( c_n \) is non-zero. The operators \( A_1 \) and \( A_2 \) will be locally linearly independent if, for every such state, and for every pair of complex coefficients \( \alpha_1 \) and \( \alpha_2 \), at least one of which is non-zero,

\[
(\alpha_1 A_1 + \alpha_2 A_2)|\psi\rangle \neq 0. \tag{3.29}
\]

To show that this is so, let \( n_0 \) be the smallest value of \( n \) for which \( c_n \neq 0 \). It follows then that \( \langle n_0|A_1|\psi\rangle = 0 \) and

\[
\langle n_0|A_2|\psi\rangle = \sqrt{1 - |\mu|^2} c_{n_0}. \quad \text{Hence,}
\]

\[
\langle n_0|(\alpha_1 A_1 + \alpha_2 A_2)|\psi\rangle = \alpha_2 \sqrt{1 - |\mu|^2} c_{n_0} \tag{3.30}
\]

which is non-zero for non-zero \( \alpha_2 \), implying that when \( \alpha_2 \neq 0 \), (3.29) is satisfied. To show that it is also satisfied when \( \alpha_2 = 0 \), we simply make use of the fact that if this were not the case, then we would have \( A_1|\psi\rangle = 0 \), which is not true. We can see this, for example, by making use of the fact that \( \langle n_0 + 1|A_1|\psi\rangle = \mu c_{n_0} \neq 0 \).

The key property which makes the operators \( A_1 \) and \( A_2 \) defined above a locally linearly independent set is the fact that \( A_1 \) has no eigenvalues/eigenvectors. In fact, it is straightforward to prove that, for any pair of non-singular operators \( A_1 \) and \( A_2 \), if \( A_2 \) is proportional to the identity, then local linear independence of \( A_1 \) and \( A_2 \) is equivalent to the condition that \( A_1 \) has no eigenvalues/eigenvectors.

**Discussion**

In this paper, we have addressed the following problem: suppose that a generalised measurement has been carried out on a quantum system. We do not know the outcome of the measurement. We do, however, know which measurement has been carried out and have access to the system following the measurement. We are free to interrogate the final state in any way which is physically possible. Our aim is to devise a suitable ‘retrodicting’ measurement which will reveal the outcome of the first measurement.
This task is simple if the initial measurement is a projective measurement; if there no irreversible evolution following this measurement, then we can simply reverse any evolution that occurs and perform the same measurement again. Generalised measurements do not, however, possess the repeatability property which is responsible for the straightforward nature of outcome retrodiction for projective measurements. In section II, we derived a necessary and sufficient condition on the Kraus transformations operators for the outcome of a generalised measurement to be perfectly retrodictable for an arbitrary initial state. We also showed that there is no advantage to be gained if the initial state, though arbitrary, is known.

When the input and output Hilbert spaces have the same dimension, the only fine-grained measurements which satisfy this condition are projective measurements, possibly followed by an outcome-independent unitary transformation. We also showed that every POVM can be realised by a measurement whose outcome is perfectly retrodictable for all initial states if the number of outcomes does not exceed the output Hilbert space dimension. We also described an algorithm by which such an implementation can be constructed using a standard implementation. This essentially involves swapping the information contained in the measuring apparatus and the system following the measurement.

We then addressed the problem of unambiguously retrodicting the outcome of a generalised measurement, with zero probability of error but with a possible non-zero probability of the retrodiction attempt giving an inconclusive result. We addressed this issue in section III, focusing on fine-grained measurements. The fact that only linearly independent pure, final states can be unambiguously discriminated places constraints on the Kraus operators of such measurements. We showed that if entanglement with an ancillary system is possible, then a sufficient and, for finite-strength measurements, necessary condition is that the Kraus operators are linearly independent. This result has interesting connections with a theorem due to Choi and also with the problem of unambiguously discriminating between unitary operators.

When the initial state is pure and entanglement is not permitted, we have shown that the issue of unambiguous outcome retrodiction is closely related to the concepts of operator local linear dependence and local linear independence. While being interesting in their own right, our demonstration that these concepts are relevant to quantum measurement theory gives a further incentive to explore them.

Acknowledgements

We would like to thank Peter Šemrl and Leo Livshits for helpful correspondence and Stephen M. Barnett for illuminating discussions about retrodiction. We also thank Osamu Hirota, Jerry Finkelstein and Paul Busch for suggesting helpful clarifications. This work was supported by the UK Engineering and Physical Sciences Research Council and by the British Council.

[1] Even in classical mechanics, this assumption seems to be invalid. See A. Peres, Quantum Theory: Concepts and Methods, (Kluwer Academic, Dordrecht, 1995).
[2] J. von Neumann, Mathematical Foundations of Quantum Mechanics (Princeton University Press, Princeton, 1955).
[3] G. Lüders, Ann. der Phys. 8 322 (1951).
[4] A. S. Holevo, Prob. Peredachi Inform. 9 No. 2 31 (1973).
[5] C. W. Helstrom, Quantum Detection and Estimation Theory (Academic Press, New York, 1976).
[6] A. Chefdes, Contemp. Phys. 41 401 (2000).
[7] A. Chefdes, Phys. Lett. A 239 339 (1998).
[8] Y. Aharonov, P. G. Bergman and J. L. Lebowitz, Phys. Rev. 134 B1410 (1964); Y. Aharonov and D. Z. Albert, Phys. Rev. D29 223 (1984); Y. Aharonov and D. Z. Albert, Phys. Rev. D29 228 (1984); Y. Aharonov and L. Vaidman, J. Phys. A: Math. Gen. 24 2315 (1991).
[9] S. M. Barnett, D. T. Pegg and J. Jeffers, J. Mod. Opt 47 1779 (2000); S. M. Barnett, D. T. Pegg, J. Jeffers and O. Jedrzkiewicz, J. Phys. B: At. Mol. Opt. Phys. 33 3047 (2000); S. M. Barnett, D. T. Pegg, J. Jeffers and O. Jedrzkiewicz, Phys. Rev. A 62 022313 (2000); S. M. Barnett, D. T. Pegg, J. Jeffers and O. Jedrzkiewicz, Phys. Rev. Lett 86 2455 (2001).
[10] M.-D. Choi, Linear Algebra Appl. 10 285 (1975).
[11] C. A. Fuchs and K. Jacobs, Phys. Rev. A 63 062305 (2001).
[12] M. Bresar and P. Šemrl, Trans. Amer. Math. Soc. 351 1257 (1999).
[13] R. Meshulam and P. Šemrl, Pacific. J. Math. 203 411 (2002).
[14] K. Kraus, States, Effects and Operations: Fundamental Notions of Quantum Theory, (Springer-Verlag, Berlin Heidelberg, 1983).
[15] This is not, in general, true for measurements which have an infinite number of potential outcomes. Consider, for example, the POVM with elements Π(φ) = const.×⟨φ|φ⟩, where |φ⟩ varies over all normalised states |φ⟩∈H and the resolution of the identity is formed by integration with respect to the appropriate Haar measure and with an appropriate choice of the multiplicative constant. Clearly, for any particular state |χ⟩, we can find a state |φ⟩ which is orthogonal to it. It follows that we have P(φ|χ⟩ = ⟨χ|Π(φ)|χ⟩ = 0.
[16] A. M. Childs, J. Preskill and J. Renes, J. Mod. Opt. 47 155 (2000).
[17] A. Acín, Phys. Rev. Lett. 87 177901 (2001).
[18] C. H. Bennett and S. Wiesner, Phys. Rev. Lett. 69 2881 (1992).
[19] If (α1|A1 + α2|A2)|ψ⟩ = 0, then α1≠0 and |A1|ψ⟩ = −(α2/α1)√1−|μ|2|ψ⟩ and so |ψ⟩ is an eigenvector of A1 with eigenvalue −(α2/α1)√1−|μ|2. Conversely, if
$A_1|\psi\rangle = \lambda|\psi\rangle$ then $[A_1 - (\frac{\lambda}{\sqrt{1 - |\mu|^2}})A_2]|\psi\rangle = 0$ and so $A_1$ and $A_2$ are not locally linearly independent.