Unambiguous quantum state elimination for qubit sequences

Jonathan Crickmore,[1] Ittoop V. Puthoor,[1] Berke Ricketti,[1] Sarah Croke,[2] Mark Hillery,[3] and Erika Andersson[1]

[1]*SUPA, Institute for Photonics and Quantum Sciences, School of Engineering and Physical Sciences,*
Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom
[2]*SUPA, School of Physics and Astronomy, University of Glasgow, Glasgow G12 8QQ, United Kingdom*
[3]*Department of Physics and Astronomy, Hunter College of the City University of New York, New York, New York 10065, USA*
and Graduate Center of the City University of New York, New York, New York 10016, USA

Quantum state elimination measurements tell us what states a quantum system does *not* have. This is different from state discrimination, where one tries to determine what the state of a quantum system is rather than what it is not. Apart from being of fundamental interest, quantum state elimination may find uses in quantum communication and quantum cryptography. We consider unambiguous quantum state elimination for two or more qubits, where each qubit can be in one of two possible states. Optimal measurements for eliminating one and two states out of four two-qubit states are given. We also prove that if we want to maximize the average number of eliminated overall *N*-qubit states, then individual measurements on each qubit are optimal.

I. INTRODUCTION

Quantum measurements more naturally *exclude* states rather than indicate precisely which state a quantum system has. For example, if we make a projective measurement in some basis, then we can rule out any state which is orthogonal to the basis state corresponding to the outcome we obtained. In spite of this, quantum state elimination [1–7] has not been much explored. More attention has been given to quantum state discrimination [8], where one aims to determine what a quantum state is.

Quantum state elimination has already generated significant interest, in the sense that the philosophical argument about the reality of the wave function in Ref. [2] completely relies on the existence of a particular quantum elimination measurement in an entangled basis. Apart from this fundamental interest, quantum state elimination might be useful for applications in quantum information and quantum communication. Examples of this are the communication tasks in Refs. [9–11] and a protocol for quantum oblivious transfer [12]. In 1-out of-2 oblivious transfer, a receiver should receive one out of two bits, with no information about the other. The sender should not know which bit was received. Among other things, in this paper we investigate unambiguously excluding two out of four possible nonorthogonal two-qubit states. If the four states encode two classical bit values, then such a measurement would tell us either the first bit, the second bit, or the XOR of the two bits.

In addition to oblivious transfer, one could envisage novel quantum key distribution schemes employing quantum state elimination. Suppose a sender prepares one of four nonorthogonal states; the recipient excludes two of these, and "reconciliation" means that the recipient tells the sender (using an authenticated but not secret classical channel) whether the first, second, or XOR of the bits was received. This bit value then constitutes the secret key, after privacy amplification. As for the Bennett-Brassard-84 protocol for quantum key distribution, eavesdropping can intuitively be detected if the sender and recipient announce some of the bit values (again using an authenticated channel). The novel feature of such a scheme is that the final bit value cannot be thought of as created at the sender and transmitted to the receiver but is only realized once the receiver's measurement is complete. A similar scheme employing elimination of one among three states has been previously proposed [13] and optimal eavesdropping attacks shown to have counterintuitive features. For example, the optimal attack to maximize the probability that whenever Alice and Bob agree Eve also knows the shared bit is a unitary [14]. Thus, although quantum key distribution is by now very well developed, such schemes are conceptually different and may be of theoretical interest.

In this paper, we consider unambiguous or "error-free" quantum state elimination for qubit sequences. Minimum-error measurements minimize the probability for the result to be wrong, and as a generalization of this, minimum-cost measurements minimize the average cost associated with the result. Unambiguous measurements, on the other hand, never give a wrong result, which is often possible only if the measurement sometimes fails to give a successful result. Minimum-cost and minimum-error state elimination are easily seen to be a special case of minimum-cost measurements, with a suitable cost associated with naming a state that was actually prepared. Moreover, minimum-error state exclusion is equivalent to minimum-error state discrimination among mixtures of the original states [5], and existing results for state discrimination [8] therefore apply.

In contrast, it seems that unambiguous quantum state elimination cannot be usefully re-expressed as unambiguous state discrimination. This makes it particularly interesting to investigate. Here we consider unambiguous state elimination for sequences of qubits. Optimal measurements for eliminating one and two states out of four two-qubit states are given. We also prove that if we want to maximize the average number of eliminated overall N-qubit states, then individual measurements on each qubit are optimal.

The measurements we will consider will often be not just measurements in entangled basis. They will often be generalized quantum measurements, also called positive operator-valued measurements (POVMs) or probability operator measures (POMs) [1,8]. Similarly to projective measurements in some orthonormal basis, generalized measurements are described by a set of Hermitian measurement operators Π_i, where i labels the outcome. The probability of outcome i is $p_i = \text{Tr}(\rho \Pi_i)$, if ρ is the state being measured. In contrast to projective measurements, however, the operators Π_i need not be projectors. They must nevertheless satisfy

$$\Pi_i \geqslant 0 \ \forall \ i, \quad \sum_i \Pi_i = 1. \tag{1}$$

The first of these conditions means that all eigenvalues of Π_i should be positive. This is necessary because probabilities should be non-negative numbers. The second condition means that the sum of the probabilities for all outcomes, including the measurement failing to give the desired information, should be equal to 1. That is, although the measurement is not a projection in an orthonormal basis, the outcomes are nevertheless mutually exclusive in the sense that if one outcome occurs, another one does not occur.

Generalizing the situation in Ref. [2], we will consider states of two or more qubits. Each qubit has one of the states

$$|\pm\theta\rangle = \cos\theta|0\rangle \pm \sin\theta|1\rangle, \tag{2}$$

where $0 \leqslant \theta \leqslant 45°$. The single-qubit states orthogonal to $|\pm\theta\rangle$ are denoted by

$$|\overline{\pm\theta}\rangle = \sin\theta|0\rangle \mp \cos\theta|1\rangle. \tag{3}$$

For two qubits, the four possible states are

$$|+\theta, +\theta\rangle = \cos^2\theta|00\rangle + \sin^2\theta|11\rangle + \cos\theta\sin\theta(|01\rangle + |10\rangle)$$
$$|+\theta, -\theta\rangle = \cos^2\theta|00\rangle - \sin^2\theta|11\rangle - \cos\theta\sin\theta(|01\rangle - |10\rangle)$$
$$|-\theta, +\theta\rangle = \cos^2\theta|00\rangle - \sin^2\theta|11\rangle + \cos\theta\sin\theta(|01\rangle - |10\rangle)$$
$$|-\theta, -\theta\rangle = \cos^2\theta|00\rangle + \sin^2\theta|11\rangle - \cos\theta\sin\theta(|01\rangle + |10\rangle). \tag{4}$$

Pusey, Barrett, and Rudolph [2] mainly considered the scenario with two qubits and $2\theta = 45°$, when a measurement in an entangled basis can unambiguously eliminate one of the four possible states with success probability equal to 1. We will call this the "PBR measurement."

If we for clarity take the two states for each qubit to be $|0\rangle$ and $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ instead of $|\pm\theta\rangle$, then the PBR

measurement basis is given by

$$|\neg(0, 0)\rangle = \frac{1}{\sqrt{2}}(|0, 1\rangle + |1, 0\rangle)$$

$$|\neg(0, +)\rangle = \frac{1}{\sqrt{2}}(|0, -\rangle + |1, +\rangle)$$

$$|\neg(+, 0)\rangle = \frac{1}{\sqrt{2}}(|+, 1\rangle + |-, 0\rangle)$$

$$|\neg(+, +)\rangle = \frac{1}{\sqrt{2}}(|+, -\rangle + |-, +\rangle). \tag{5}$$

If the result $\neg(00)$ is obtained, then the state cannot have been $|00\rangle$, since $|\neg(00)\rangle \perp |00\rangle$, and similarly for the other results.

If one wants to unambiguously eliminate states, but only local measurements on each qubit are allowed, then it is best to perform optimal unambiguous state discrimination on each qubit. Two equiprobable states $|\phi\rangle$ and $|\theta\rangle$ can be unambiguously distinguished with the probability $1 - |\langle\phi|\theta\rangle|$ [15–17], meaning that $|\pm\theta\rangle$ can be distinguished from each other with probability $1 - p_f = 1 - \cos(2\theta)$. One fails to eliminate any state at all iff both measurements fail. This happens with probability p_f^2, which is equal to $1/2$ for $2\theta = 45°$. That is, even if there are no correlations between the two qubits, a measurement in an entangled basis can exclude a single two-qubit state more often than local measurements.

II. ELIMINATING ONE OUT OF FOUR STATES

If $45° < 2\theta \leqslant 90°$, then one can construct a measurement that always eliminates one state, for example, as follows. First, couple each "system" qubit to an ancilla $|\phi\rangle_a$, using a suitable unitary transform V so that $V|\pm\theta\rangle \otimes |\phi\rangle_a = |\pm 22.5°\rangle \otimes |\phi_\pm\rangle_a$. This is possible if we choose $\langle\phi_-|\phi_+\rangle = \sqrt{2}\langle-\theta|\theta\rangle$, which is always possible if $45° \leqslant 2\theta \leqslant 90°$. Then proceed to make the PBR measurement on the "system" qubits. [The measurement basis for $|\pm 22.5°\rangle$ is constructed analogously to that for $|0\rangle, |+\rangle$ in (5).] The ancilla can be discarded or can sometimes be used to unambiguously eliminate more states [18].

When $0° \leqslant 2\theta < 45°$, it is impossible to always eliminate one state. To start with, it can be shown that when ruling out one of four equiprobable two-qubit states, the optimal measurement operators corresponding to successful outcomes obey the same symmetry as the states. The four two-qubit states are transformed into each other when U is applied to the first, second, or both qubits, where $U = |0\rangle\langle 0| - |1\rangle\langle 1|$, with $U^2 = 1$. Then there exists an optimal measurement with the same symmetry,

$$\Pi_{\neg(-+)} = (U_1 \otimes I_2)\Pi_{\neg(++)}(U_1^\dagger \otimes I_2),$$

$$\Pi_{\neg(+-)} = (I_1 \otimes U_2)\Pi_{\neg(++)}(I_1 \otimes U_2^\dagger),$$

$$\Pi_{\neg(--)} = (U_1 \otimes U_2)\Pi_{\neg(++)}(U_1^\dagger \otimes U_2^\dagger), \tag{6}$$

where $U_i = |0\rangle\langle 0| - |1\rangle\langle 1|$ applied to the ith qubit, and I_i is the identity operation for the ith qubit, and we have used the shorthand notation "$++$" for the state $|\theta, \theta\rangle$, "$+-$" for $|\theta, -\theta\rangle$ and so on. To see this, suppose that an optimal measurement strategy has the measurement operators $\widetilde{\Pi}_{\neg(++)}, \widetilde{\Pi}_{\neg(+-)}, \widetilde{\Pi}_{\neg(-+)}, \widetilde{\Pi}_{\neg(--)}$ (in addition to a possible

failure measurement operator $\widetilde{\Pi}_{f,1}$), but that it does not have the symmetry in (6). The measurement with operators

$$\Pi_{\neg(++)} = \tfrac{1}{4}[\widetilde{\Pi}_{\neg(++)} + U_1\widetilde{\Pi}_{\neg(-+)}U_1^\dagger + U_2\widetilde{\Pi}_{\neg(+-)}U_2^\dagger$$
$$+ U_1 \otimes U_2\widetilde{\Pi}_{\neg(--)}U_1^\dagger \otimes U_2^\dagger] \quad (7)$$

and analogously for the other measurement operators, is easily seen to obey the symmetry. If the four states are equiprobable, then it will have the same success probability as the optimal measurement we started from. To show this, let us examine the failure operator for the symmetrized measurement,

$$\Pi_{f,1} = \tfrac{1}{4}(\widetilde{\Pi}_{f,1} + U_1\widetilde{\Pi}_{f,1}U_1^\dagger + U_2\widetilde{\Pi}_{f,1}U_2^\dagger$$
$$+ U_1 \otimes U_2\widetilde{\Pi}_{f,1}fU_1^\dagger \otimes U_2^\dagger). \quad (8)$$

Let us also note that the operation $S(\Pi) = \tfrac{1}{2}(\Pi + U\Pi U^\dagger)$, where $U = |0\rangle\langle0| - |1\rangle\langle1|$ deletes the off-diagonal elements of a 2×2 operator (or density matrix) in the $\{|0\rangle, |1\rangle\}$ basis. This also means that the "symmetrized" $\Pi_{f,1}$ is diagonal in the $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ basis.

The failure probability for the measurement we started with is given by

$$\widetilde{p}_{f,1} = p_{++}p(\widetilde{f}|++) + p_{+-}p(\widetilde{f}|+-) + p_{-+}p(\widetilde{f}|-+)$$
$$+ p_{--}p(\widetilde{f}|--), \quad (9)$$

where p_{++} is the prior probability for state $|\theta,\theta\rangle$ to occur and $p(\widetilde{f}|++)$ is the conditional probability for failing to exclude a state, given that the state was $|\theta,\theta\rangle$, and analogously for the other three states. The failure probability for the symmetrized measurement in (6) is then

$$p_{f,1} = \tfrac{1}{4}(p_{++} + p_{+-} + p_{-+} + p_{--})[p(\widetilde{f}|++)$$
$$+ p(\widetilde{f}|+-) + p(\widetilde{f}|-+) + p(\widetilde{f}|--)]$$
$$= p(\widetilde{f}|++) + p(\widetilde{f}|+-) + p(\widetilde{f}|-+) + p(\widetilde{f}|--). \quad (10)$$

If all four states are equiprobable (or if all four conditional failure probabilities are equal), then this is equal to the failure probability $\widetilde{p}_{f,1}$ of the measurement we started with.

Thus we can without loss of generality assume that an optimal measurement obeys the symmetry if the states are equiprobable and if we allow mixed measurement operators. (A similar construction is possible also in other cases where there is some sort of symmetry among the possible states.)

It can further be shown that in the range $0 \leqslant 2\theta < 45°$, the optimal measurement obeying the symmetry has $\Pi_{\neg(++)} = |X\rangle\langle X|$ for a particular $|X\rangle$, meaning that the other measurement operators also are proportional to pure-state projectors. Consider a strategy which obeys the symmetry but might have mixed measurement operators, with

$$\Pi_{\neg(++)} = \sum_{i=1}^{3} |X_i\rangle\langle X_i|, \quad (11)$$

where

$$|X_i\rangle = \sum_{j,k=0,1} c_{jk}^i |jk\rangle \quad (12)$$

are proportional to the eigenstates of $\Pi_{\neg(++)}$ [we have absorbed the eigenvalues of $\Pi_{\neg(++)}$ into the states in (11)]. The

condition $\langle\theta,\theta|\Pi_{\neg(++)}|\theta,\theta\rangle = 0$, that is, we never incorrectly eliminate a state, reads

$$c_{00}^i \cos^2\theta + (c_{01}^i + c_{10}^i)\sin\theta\cos\theta + c_{11}^i \sin^2\theta = 0 \quad (13)$$

for $i = 1, 2, 3$. The failure operator is

$$\Pi_{f,1} = I - \sum_{jk=+,-}\Pi_{\neg(jk)} = I - 4\sum_{j,k=0,1}\sum_{i=1}^{3}|c_{jk}^i|^2|jk\rangle\langle jk|. \quad (14)$$

Since $\Pi_{f,1} \geqslant 0$, it must hold that $\sum_{i=1}^{3}|c_{jk}^i|^2 \leqslant 1/4$. If the states are equally likely, then the failure probability is

$$p_{f,1} = \frac{1}{4}\sum_{j,k=\pm\theta}\langle j,k|\Pi_{f,1}|j,k\rangle$$
$$= 1 - 4\sum_{i=1}^{3}\big[|c_{00}^i|^2\cos^4\theta + (|c_{01}^i|^2 + |c_{10}^i|^2)\sin^2\theta\cos^2\theta$$
$$+ |c_{11}^i|^2\sin^4\theta\big]. \quad (15)$$

We want to minimize $p_{f,1}$, which means that we want to maximize the sum in the last two lines in the above equation, subject to (13), $\sum_{i=1}^{3}|c_{jk}^i|^2 \leqslant 1/4$, and with $|X_i\rangle$ orthogonal to each other. The coefficient multiplying $\sum_{i=1}^{3}|c_{00}^i|^2$ is the largest. Writing (13) as

$$c_{00}^i = -(c_{01}^i + c_{10}^i)\tan\theta - c_{11}^i\tan^2\theta, \quad (16)$$

and taking into account that for $0 \leqslant 2\theta < 45°$, it holds that $0 \leqslant 2\tan\theta + \tan^2\theta \leqslant 1$, one realizes that in order to maximize the success probability, it is optimal to choose $\Pi_{\neg(++)} = |X_1\rangle\langle X_1|$, with $c_{01}^1 = c_{10}^1 = c_{11}^1 = -1/2$ and $c_{00}^1 = \tan\theta(1 + \tfrac{1}{2}\tan\theta)$, and all other $c_{jk}^i = 0$. The failure operator is then

$$\Pi_{f,1} = [1 - \tan^2\theta(2 + \tan\theta)^2]|0\rangle\langle 0|, \quad (17)$$

and the failure probability is

$$p_{f,1} = [\cos(2\theta) - \sin(2\theta)][1 + \sin(2\theta)]. \quad (18)$$

III. ELIMINATING TWO OUT OF FOUR STATES

It turns out that if θ is large enough, then it becomes possible to eliminate not just one but two out of the four two-qubit states. As we will show, this occurs if $\cos(2\theta) \leqslant \sqrt{2} - 1$, meaning that $2\theta \gtrsim 65.5°$. There are six ways to choose two states out of four. Using the previous shorthand notation "++" for the state $|\theta,\theta\rangle$, "+−" for $|\theta,-\theta\rangle$, and so on, the pairs we can eliminate are

$$\{++, +-\}, \{++, -+\}, \{+-, --\}, \{-+, --\},$$
$$\{+-, -+\}, \{++, --\}. \quad (19)$$

We will label these pairs with the letters A to F in the order they appear above. In the four first pairs, A–D, the state of either the first or the second qubit is the same in both excluded states. That is, eliminating one of the first pairs means determining the state of one of the qubits. For the two last pairs, E and F, we have eliminated the possibility that the two qubits have the same state or that they have different states.

First, let us bound for what range of θ it is possible to unambiguously eliminate two states with success probability 1. Suppose that the prepared state really is $|\theta, \theta\rangle$ but that we only know that it is either $|\theta, \theta\rangle$ or $|-\theta, -\theta\rangle$, with equal prior probabilities. The possible outcomes are now $\{+-, --\}$, $\{-+, --\}$ and $\{+-, -+\}$, with labels C, D, E, plus the "failure" outcome if it occurs. If the outcome is C or D, that is, $\{+-, --\}$ or $\{-+, --\}$, then we have succeeded in unambiguously telling $|\theta, \theta\rangle$ from $|-\theta, -\theta\rangle$. This must occur with a probability at most $1 - \langle -\theta, -\theta|\theta, \theta\rangle = 1 - \cos^2(2\theta)$, meaning that $p(C|++) + p(D|++) \leqslant 1 - \cos^2(2\theta)$ (the conditional success probabilities for optimally distinguishing between two equiprobable states are also equal for both states). Now suppose that the prepared state still is $|\theta, \theta\rangle$, but that we only know that it is either $|\theta, \theta\rangle$ or $|\theta, -\theta\rangle$, again with equal prior probabilities. If the outcome is C or E, $\{+-, --\}$ or $\{+-, -+\}$, then we have succeeded in distinguishing $|\theta, \theta\rangle$ and $|\theta, -\theta\rangle$, which can occur with probability at most $1 - \langle \theta, -\theta|\theta, \theta\rangle = 1 - \cos(2\theta)$, giving $p(C|++) + p(E|++) \leqslant 1 - \cos(2\theta)$. Similarly, if we know that the state is either $|\theta, \theta\rangle$ or $|-\theta, \theta\rangle$, with equal prior probabilities, then the outcomes D and E, $\{-+, --\}$ and $\{+-, -+\}$, can occur with probability at most probability $1 - \cos(2\theta)$, giving $p(D|++) + p(E|++) \leqslant 1 - \cos(2\theta)$. Adding these three inequalities, and assuming that the failure probability is zero, so that $p(C|++) + p(D|++) + p(E|++) = 1$, we obtain

$$2 \leqslant 3 - 2\cos(2\theta) - \cos^2(2\theta) = 4 - [1 + \cos(2\theta)]^2, \quad (20)$$

meaning that $\cos(2\theta) \leqslant \sqrt{2} - 1$ must hold if the measurement never fails.

This bound turns out to be tight. We will now construct a measurement that unambiguously eliminates pairs of states. If $\cos(2\theta) \leqslant \sqrt{2} - 1$, then the success probability is equal to 1; otherwise it is less than 1. Some intuitive assumptions will be made, but by comparison with results in Sec. IV, in particular Eq. (42), it can be seen that the constructed measurement is optimal also when $\cos(2\theta) > \sqrt{2} - 1$.

First, look at E and F, the two last cases in (19). An orthogonal (but un-normalized) basis for the space spanned by the states $|\theta, \theta\rangle$ and $|-\theta, -\theta\rangle$ is given by

$$\{\cos^2\theta|00\rangle + \sin^2\theta|11\rangle, \quad |01\rangle + |10\rangle\}. \quad (21)$$

Similarly, an orthogonal (but un-normalized) basis for the space spanned by the states $|\theta, -\theta\rangle$ and $|-\theta, \theta\rangle$ is

$$\{\cos^2\theta|00\rangle - \sin^2\theta|11\rangle, \quad |01\rangle - |10\rangle\}. \quad (22)$$

Therefore, if some measurement operators are proportional to projectors onto $|\psi_{01}^{\pm}\rangle = |01\rangle \pm |10\rangle$ and $|\psi_{cs}^{\pm}\rangle = \sin^2\theta|00\rangle \pm \cos^2\theta|11\rangle$, then these outcomes would allow us to unambiguously rule out either $\{+-, -+\}$ or $\{++, --\}$. (More generally, such measurement operators could also be proportional to projectors onto superpositions of $|\psi_{01}^{\pm}\rangle$ and $|\psi_{cs}^{\pm}\rangle$, and mixtures of such projectors.)

The sum of all measurement operators, including a possible failure operator, must be the identity operator. If projectors onto the un-normalized states $|01\rangle \pm |10\rangle$ are included among the measurement operators, with the same weight α, then the resulting contribution to the sum of all measurement operators is $2\alpha(|01\rangle\langle01| + |10\rangle\langle10|)$. Similarly, if projectors onto the states $\sin^2\theta|00\rangle \pm \cos^2\theta|11\rangle$ are included among the measurement operators, with the same weight β, then the contribution to the sum of all measurement operators is

$$2\beta(\sin^4\theta|00\rangle\langle00| + \cos^4\theta|11\rangle\langle11|). \quad (23)$$

It holds that $\sin^4\theta \leqslant \cos^4\theta$ if $0 \leqslant \theta \leqslant 45°$. Therefore, to obtain a measurement that *always* eliminates one pair of states, other measurement operators would need to make a greater contribution to $|00\rangle\langle00|$ than to $|11\rangle\langle11|$.

Let us then consider the first four pairs, A–D, in (19). The states in the pair $\{++, +-\}$ span the space $|\theta\rangle\langle\theta| \otimes I_2$, where I_2 is the identity operator on the second qubit. A measurement operator that corresponds to ruling out $\{++, +-\}$ must therefore have the form $|\bar{\theta}\rangle_{11}\langle\bar{\theta}| \otimes \pi_2$, where π_2 is some operator acting on the second qubit. We will choose $\pi_2 \propto |0\rangle_{22}\langle0|$, since we need to make up a "shortfall" in $|00\rangle\langle00|$. Similarly, ruling out the pair $\{++, -+\}$ must correspond to a measurement operator $\pi_1 \otimes |\bar{\theta}\rangle_{22}\langle\bar{\theta}|$, and we will again choose $\pi_1 \propto |0\rangle_{11}\langle0|$. Finally, ruling out the remaining two pairs will correspond to measurement operators proportional to $|\overline{-\theta}, 0\rangle\langle\overline{-\theta}, 0|$ and $|0, \overline{-\theta}\rangle\langle0, \overline{-\theta}|$. It holds that

$$|\bar{\theta}\rangle\langle\bar{\theta}| + |\overline{-\theta}\rangle\langle\overline{-\theta}| = 2\sin^2\theta|0\rangle\langle0| + 2\cos^2\theta|1\rangle\langle1|. \quad (24)$$

Hence, if projectors onto the four states $|\bar{\theta}, 0\rangle$, $|\overline{-\theta}, 0\rangle$, $|0, \bar{\theta}\rangle$, $|0, \overline{-\theta}\rangle$ are all included among the measurement operators with the same weight γ, then the resulting contribution to the sum of all measurement operators is

$$\gamma[4\sin^2\theta|00\rangle\langle00| + 2\cos^2\theta(|01\rangle\langle01| + |10\rangle\langle10|)]. \quad (25)$$

Collecting all contributions to the sum of all measurement operators, the sum is less than or equal to the identity operator if the inequalities

$$2\beta\sin^4\theta + 4\gamma\sin^2\theta \leqslant 1$$
$$2\beta\cos^4\theta \leqslant 1$$
$$2\alpha + 2\gamma\cos^2\theta \leqslant 1 \quad (26)$$

are all satisfied. If equality can be reached in all three inequalities, then the measurement always succeeds in eliminating two states. Evidently, we should choose $\beta = 1/(2\cos^4\theta)$. If the angle θ is large enough, so that $\cos 2\theta \leqslant \sqrt{2} - 1$, then we can satisfy all three inequalities by choosing

$$\gamma = \frac{1 - \tan^4\theta}{4\sin^2\theta}, \quad \alpha = \frac{1}{2} - \gamma\cos^2\theta. \quad (27)$$

If $\cos 2\theta > \sqrt{2} - 1$, then we must instead choose $\gamma = 1/(2\cos^2\theta)$ and $\alpha = 0$ so as not to violate the last inequality in (26). In this case, there will be a failure operator proportional to $|00\rangle\langle00|$,

$$\Pi_{f,2} = [2 - (1 + \tan^2\theta)^2]|00\rangle\langle00|. \quad (28)$$

The failure probability is

$$p_{f,2} = \cos^4\theta[2 - (1 + \tan^2\theta)^2] = 2\cos^4\theta - 1. \quad (29)$$

If $\cos^2\theta = 1/\sqrt{2}$, then $p_{f,2} = 0$ as it should.

The measurement operators for outcomes A–F are given by

$$\Pi_A = \gamma|\overline{\theta}, 0\rangle\langle\overline{\theta}, 0|, \qquad \Pi_B = \gamma|0, \overline{\theta}\rangle\langle0, \overline{\theta}|,$$

$$\Pi_C = \gamma|0, \overline{-\theta}\rangle\langle0, \overline{-\theta}|, \quad \Pi_D = \gamma|\overline{-\theta}, 0\rangle\langle\overline{-\theta}, 0|,$$

$$\Pi_E = \alpha|\psi_{01}^+\rangle\langle\psi_{01}^+| + \beta|\psi_{cs}^+\rangle\langle\psi_{cs}^+|,$$

$$\Pi_F = \alpha|\psi_{01}^-\rangle\langle\psi_{01}^-| + \beta|\psi_{cs}^-\rangle\langle\psi_{cs}^-|, \tag{30}$$

with α, β, and γ given above. In the range $\cos(2\theta) \leqslant \sqrt{2} - 1$, where the success probability is equal to 1, it holds that

$$p_A = p_B = p_C = p_D = \tfrac{1}{2}\cos(2\theta), \quad p_E = p_F = \tfrac{1}{2} - \cos(2\theta), \tag{31}$$

and in the range $\cos(2\theta) > \sqrt{2} - 1$, when the success probability is less than 1, it holds that

$$p_A = p_B = p_C = p_D = \sin^2\theta\cos^2\theta, \quad p_E = p_F = \sin^4\theta. \tag{32}$$

We conjecture that this measurement is optimal for unambiguously eliminating two out of four states also in the range when we cannot do so 100% of the time.

If we rule out that the states of a number of quantum systems are the same, then they must be different and vice versa. Quantum state elimination is therefore related to quantum state comparison [19–21]. As shown in Ref. [19], the optimal success probability for unambiguously determining if two states, each drawn from the set $\{|\theta\rangle, |-\theta\rangle\}$, are the same or different, is $1 - \cos(2\theta) = 2\sin^2\theta$. (The probability for the outcomes "same" and "different" are each half of this.) This is consistent with what we have found here. For the range $\cos(2\theta) \leqslant \sqrt{2} - 1$ where two states are always ruled out, it holds that $p_E + p_F = 1 - 2\cos(2\theta)$. For the range $\cos(2\theta) > \sqrt{2} - 1$, it holds that $p_E + p_F = 2\sin^4\theta$. That is, if we are only interested in whether the states are the same or different, outcomes E and F, then it is possible to obtain these outcomes somewhat more often than when maximizing $p_A + p_B + p_C + p_D + p_E + p_F$.

IV. MAXIMISING THE AVERAGE NUMBER OF ELIMINATED STATES

Let us now consider N qubits, each in the state $|\theta\rangle$ or $|-\theta\rangle$. We will consider a measurement that sometimes eliminates 0, 1, 2 states, and so on, all the way to eliminating all but one of the 2^N states. We will show that if one wants to maximize the average number of eliminated states, then unambiguous measurements on each qubit individually are optimal. First, let us see how many states are excluded in this case. The failure probability for each single-qubit measurement is $p_f = |\langle-\theta|\theta\rangle| = \cos(2\theta)$. The probability that M measurements fail and $N - M$ measurements succeed is then $\binom{N}{M}p_f^M(1 - p_f)^{N-M}$. If M measurements fail, then there are 2^M possible states left, and the average number of states eliminated is

$$\langle S\rangle = 2^N - \sum_{M=0}^{N}\binom{N}{M}p_f^M(1 - p_f)^{N-M}2^M$$

$$= 2^N - [2p_f + (1 - p_f)]^N = 2^N - (1 + p_f)^N. \tag{33}$$

In other words, each single-qubit measurement leaves on average $1 + p_f$ possible states for that qubit, so that the average number of possible states after making all single-qubit measurements is $(1 + p_f)^N$. If $N = 2$, then individual measurements eliminate on average 1.086 states, which is slightly more than the PBR measurement which always eliminates 1 state. We can also easily calculate, e.g., for what combinations of N and θ half of all states will be eliminated on average.

To bound the average number of states that any measurement could unambiguously eliminate, consider using such a measurement to distinguish between the states $|x\rangle$ and $|y\rangle$, where x and $y \in \{0, 2^N - 1\}$ will label two N-qubit states which now occur with probability $1/2$ each. That is, we will use the elimination measurement for a purpose other than for which it might have been optimized. If we exclude $|x\rangle$, then the state must have been $|y\rangle$ and vice versa. No measurement can distinguish between the equiprobable states $|x\rangle$ and $|y\rangle$ more often than with probability $1 - |\langle x|y\rangle| = 1 - p_f^M$ if x and y differ from each other in M positions, where $p_f = \cos(2\theta)$ as before. For any unambiguous elimination measurement it must therefore hold that

$$p(\neg x|y)p(y) + p(\neg y|x)p(x) = \tfrac{1}{2}[p(\neg x|y) + p(\neg y|x)]$$

$$\leqslant 1 - p_f^M, \tag{34}$$

where the left-hand side in the equality gives the probability for the elimination measurement to succeed in distinguishing between $|x\rangle$ and $|y\rangle$, the right-hand side is the optimal success probability, and the prior probabilities for the two states to occur are $p(x) = p(y) = 1/2$.

We will now sum the inequality (34) over all possible x and y (and multiply the sum with $1/2^N$). To start with, for the left-hand side in this sum of inequalities it holds that

$$\sum_{x,y=0}^{2^N-1}\frac{1}{2}[p(\neg x|y) + p(\neg y|x)] = \sum_{x,y=0}^{2^N-1}p(\neg x|y). \tag{35}$$

[Excluding $x = y$ from the sum would make no difference, since we are only considering unambiguous elimination measurements for which $p(\neg x|x) = 0$, and if $x = y$, then $p_f^M = 1$ since x and y differ in no positions.] Moreover, we can write the conditional probability $p(\neg x|y)$ as a sum over probabilities to exclude different sets of states, where each set in this sum contains the state $|x\rangle$. We will denote the possible sets of states by $S_{K,j}$, where K is the number of N-qubit states contained in the set, and j labels the different sets of the same size. Excluding the states in a set $S_{K,j}$ means excluding *only* these states, no more and no less. The outcomes corresponding to excluding different sets $S_{K,j}$ are in this sense mutually exclusive. Also, the sum of all the probabilities for excluding different sets—including the empty one—will be equal to 1, as stated in (1). It then holds that

$$p(\neg x|y) = \sum_{K=1}^{2^N-1}\sum_{j:|x\rangle\in S_{K,j}}p(\neg S_{K,j}|y), \tag{36}$$

where $p(\neg S_{K,j}|y)$ is the probability to exclude the set $S_{K,j}$, given that the state was $|y\rangle$, and we are summing over j such that $S_{K,j}$ contains $|x\rangle$. If we now sum (36) over x, then each set $S_{K,j}$ will occur in this sum K times, once for each state it

contains. It therefore holds that

$$\sum_{x=0}^{2^N-1} p(\neg x|y) = \sum_{K=1}^{2^N-1} K p(\neg K|y), \tag{37}$$

where

$$p(\neg K|y) = \sum_j p(\neg S_{K,j}|y) \tag{38}$$

is the probability to exclude K states, given that the state was y. Now if we use the same state elimination measurement in a different scenario, where each state $|y\rangle$ occurs with the same probability, $p(y) = 1/2^N$, then it holds that

$$\frac{1}{2^N} \sum_{x,y=0}^{2^N-1} p(\neg x|y) = \sum_{K=1}^{2^N-1} \sum_{y=0}^{2^N-1} K p(\neg K|y) p(y)$$

$$= \sum_{K=1}^{2^N-1} K p(\neg K). \tag{39}$$

This is equal to the average number of states eliminated when each N-qubit state $|y\rangle$ occurs with the same probability.

On the right-hand side of the sum of inequality (34) over x and y, p_f appears with different powers. For each $|y\rangle$, there are $\binom{N}{M}$ different states $|x\rangle$ that differ from $|y\rangle$ in M positions, and this will determine the coefficient of each p_f^M. For a given y it therefore holds that

$$\sum_{x=0}^{2^N-1} 1 - p_f^M = 2^N - \sum_{M=0}^{N} \binom{N}{M} p_f^M = 2^N - (1 + p_f)^N. \tag{40}$$

Combining our results for the left-hand side and right-hand side for the sum over x and y of (34), multiplied by $1/2^N$, we obtain

$$\sum_{K=1}^{2^N-1} K p(\neg K) \leqslant 2^N - (1 + p_f)^N. \tag{41}$$

That is, we have obtained a bound on how many states can be eliminated on average, by any measurement, when each N-qubit state appears equally often. As stated above, the left-hand side equals the average number of states which are eliminated. The right-hand side, by comparison with (33), is precisely the number of states that will be eliminated by individual unambiguous measurements. It follows that separate unambiguous measurements on each qubit are optimal; this eliminates the highest possible number of states on average.

Equation (41) can also be used to bound how often measurements that eliminate certain numbers of states can succeed. It is possible that "entangled" measurements eliminate as many states on average as separate unambiguous measurements do, but they cannot do better. For example, consider two qubits with four states in total. It is possible to increase the probability to eliminate two of these states at the expense of lowering the probabilities to eliminate one or three states. But it still has to hold that

$$2p(\neg 2) \leqslant 4 - (1 + p_f)^2 \Leftrightarrow p_f \leqslant \sqrt{4 - 2p(\neg 2)} - 1. \tag{42}$$

Comparing with (29), with $p_f = \cos(2\theta)$, we see that this bound is tight. That is, the optimal entangled six-outcome measurement that eliminates a pair of states as often as possible also eliminates as many states as possible on average.

In general, however, similar bounds do not have to be tight. If we, for example, consider elimination of one state, again for two qubits, then we obtain

$$p(\neg 1) \leqslant 4 - (1 + p_f)^2 \Leftrightarrow p_f \leqslant \sqrt{4 - p(\neg 1)} - 1. \tag{43}$$

If $p(\neg 1) = 1$, then we obtain $p_f \leqslant \sqrt{3} - 1 \approx 0.732$. However, we know that it is possible to deterministically eliminate one state for $45° \leqslant 2\theta \leqslant 90°$, and $\cos(45°) = 1/\sqrt{2} \approx 0.707$, so that the bound from the average number of eliminated states is not tight in this case. Nevertheless, we can generally say that for the probability for eliminating K states, among N qubits, it must hold that

$$K p(\neg K) \leqslant 2^N - (1 + p_f)^N. \tag{44}$$

If we take $K = 2^N - 1$, which corresponds to unambiguous discrimination among all 2^N states, where the optimal success probability is known to be $p[\neg(2^N - 1)] = (1 - p_f)^N$ (the optimal measurement is to perform unambiguous discrimination individually on each qubit, and the overall measurement succeeds if all measurement succeed), then we obtain

$$(2^N - 1)(1 - p_f)^N \leqslant 2^N - (1 + p_f)^N. \tag{45}$$

This inequality is not tight for $N \geqslant 2$ unless $p_f = 0$ or $p_f = 1$, that is, the single-qubit states are orthogonal or identical. The inequality is also tight for $N = 1$, for any p_f, as should be expected; if we consider only one qubit, then the optimal measurement that excludes all but one state of "all qubits" (a single one) is by definition the optimal unambiguous measurement for a single qubit.

To show that the relation otherwise is not tight, consider the function

$$g(p_f) = 2^N - (1 + p_f)^N - (2^N - 1)(1 - p_f)^N. \tag{46}$$

We have

$$g'(p_f) = N[(2^N - 1)(1 - p_f)^{N-1} - (1 + p_f)^{N-1}], \tag{47}$$

which is equal to zero when $(1 + p_f)^{N-1} = (2^N - 1)(1 - p_f)^{N-1}$. Inserting this into the expression for $g(p_f)$, we find the extremal value

$$g(p_f) = 2^N - 2(1 + p_f)^{N-1}, \tag{48}$$

which is strictly greater than 0 [unless $N = 1$ or $p_f = 1$, in which case we already know that inequality is satisfied in (45)]. Since

$$g''(p_f) = -N(N - 1)[(2^N - 1)(1 - p_f)^{N-2} + (1 + p_f)^{N-2}]$$

$$\leqslant 0, \tag{49}$$

the extremal value is a maximum for the function $g(p_f)$. It follows that the inequality in (45) is not tight unless $N = 1$, $p_f = 0$, or $p_f = 1$.

V. CONCLUSIONS

We have derived unambiguous measurements for eliminating one and two of the four possible two-qubit states in (4) and

established that for N-qubit sequences, where each qubit can be in one of two possible states, individual measurements on each qubit maximize the average number of states eliminated. That is, measurements in an entangled basis cannot exclude more states on average, but they can do as well as local measurements. Quantum state elimination has not been investigated as much as quantum state discrimination but might be useful for applications in quantum communication and quantum information. As outlined in the Introduction, excluding two states out of four has a connection to oblivious transfer and might, for example, be used for quantum key distribution. The result on the average number of states eliminated means, for example, that in any situation (such as a communication protocol) where what matters is to eliminate as many states as possible on average, a measurement in an entangled basis will not give any advantage.

There are many other scenarios one might consider. Pusey *et al.* [2] also showed that for N qubits, each in the state $|\pm\theta\rangle$, then no matter how close to zero θ is, it becomes possible to eliminate one of the 2^N N-qubit states with unit probability if N is large enough. This requires a measurement in an entangled basis. Another possibility is to have more than two possible states for each quantum system, meaning that each quantum system can also be more than two dimensional. Some examples of this are considered in a related paper [22], where group theory is used to construct quantum state elimination measurements.

[1] S. M. Barnett, *Quantum Information* (Oxford University Press, Oxford, 2009), pp. 103–104.

[2] M. Pusey, J. Barrett, and T. Rudolph, On the reality of the quantum state, Nat. Phys. **8**, 475 (2012).

[3] C. M. Caves, C. A. Fuchs, and R. Schack, Conditions for compatibility of quantum-state assignments, Phys. Rev. A **66**, 062111 (2002).

[4] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Realization of Quantum Digital Signatures without the Requirement of Quantum Memory, Phys. Rev. Lett. **113**, 040502 (2014).

[5] S. Bandyopadhyay, R. Jain, J. Oppenheim, and C. Perry, Conclusive exclusion of quantum states, Phys. Rev. A **89**, 022336 (2014).

[6] P. Wallden, V. Dunjko, and E. Andersson, Minimum-cost measurements for quantum information, J. Phys. A: Math. Theor. **47**, 125303 (2014).

[7] T. Heinosaari and O. Kerppo, Antidistinguishability of pure quantum states, J. Phys. A: Math. Theor. **51**, 365303 (2018).

[8] S. M. Barnett and S. Croke, Quantum state discrimination, Adv. Opt. Photon. **1**, 238 (2009).

[9] C. Perry, R. Jain, and J. Oppenheim, Communication Tasks with Infinite Quantum-Classical Separation, Phys. Rev. Lett. **115**, 030504 (2015).

[10] T. Heinosaari and O. Kerppo, Communication of partial ignorance with qubits, J. Phys. A: Math. Theor. **52**, 395301 (2019).

[11] V. Havlíček and J. Barrett, Simple communication complexity separation from quantum state antidistinguishability, arXiv:1911.01927.

[12] R. Amiri *et al.* (unpublished).

[13] S. J. D. Phoenix, S. M. Barnett, and A. Chefles, Three-state quantum cryptography, J. Mod. Opt. **47**, 507 (2000).

[14] K. Flatt, S. Croke, and S. M. Barnett, Two-time state formalism for quantum eavesdropping, Phys. Rev. A **98**, 052339 (2018).

[15] I. D. Ivanovic, How to differentiate between non-orthogonal states, Phys. Lett. A **123**, 257 (1987).

[16] D. Dieks, Overlap and distinguishability of quantum states, Phys. Lett. A **126**, 303 (1988).

[17] A. Peres, How to differentiate between non-orthogonal states, Phys. Lett. A **128**, 19 (1988).

[18] J. Crickmore *et al.* (unpublished).

[19] S. M. Barnett, A. Chefles, and I. Jex, Comparison of two unknown pure quantum states, Phys. Lett. A **307**, 189-195 (2003).

[20] A. Chefles, E. Andersson, and I. Jex, Unambiguous comparison of the states of multiple quantum systems, J. Phys. A: Math. Gen. **37**, 7315 (2004).

[21] I. Jex, E. Andersson, and A. Chefles, Comparing the states of many quantum systems, J. Mod. Opt. **51**, 505 (2004).

[22] M. Hillery and E. Andersson, arXiv:2002.02055v1.