

# Rapid purification of quantum systems by measuring in a feedback-controlled unbiased basis

Joshua Combes,<sup>1,2</sup> Howard M. Wiseman,<sup>1,2</sup> Kurt Jacobs,<sup>3</sup> and Anthony J. O'Connor<sup>4</sup>

<sup>1</sup>*Centre for Quantum Computer Technology, Australia*

<sup>2</sup>*Centre for Quantum Dynamics, Griffith University, Brisbane, Queensland 4111, Australia*

<sup>3</sup>*Department of Physics, University of Massachusetts at Boston, 100 Morrissey Blvd, Boston, MA 02125, USA*

<sup>4</sup>*School of Biomolecular and Physical Sciences, Griffith University, Brisbane, Queensland 4111, Australia*

(Dated: November 30, 2010)

Rapid-purification by feedback — specifically, reducing the mean impurity faster than by measurement alone — can be achieved by choosing the eigenbasis of the density matrix to be unbiased relative to the measurement basis. Here we further examine the protocol introduced by Combes and Jacobs [Phys. Rev. Lett. **96**, 010504 (2006)] involving continuous measurement of the observable  $J_z$  for a  $D$ -dimensional system. We rigorously re-derive the lower bound  $(2/3)(D+1)$  on the achievable speed-up factor, and also an upper bound, namely  $D^2/2$ , for all feedback protocols that use measurements in unbiased bases. Finally we extend our results to  $n$  independent measurements on a register of  $n$  qubits, and derive an upper bound on the achievable speed-up factor that scales linearly with  $n$ .

PACS numbers: 03.67.-a, 02.30.Yy, 02.50.-r, 89.70.-a

## I. INTRODUCTION

Many quantum information processing (QIP) tasks require pure states as a resource [1]. Preparation of pure states may be a bottleneck in certain physical implementations of some QIP protocols (*e.g.* solid state systems). In these systems measurement can not be treated as instantaneous [2–5], and are often slow compared to the timescale for unitary operations [6]. In such systems, a projective measurement is approached only in the limit of long measurement times, by integrating the measured current [7]. There are demonstrable advantages associated with using the dynamics of the measured current to perform read-out or state estimation [7]. Technology is approaching the point where it can implement useful feedback protocols [8–15]. Thus it makes sense to consider combining continuous measurement with quantum feedback [16] to control the purification process. Our goal is to increase the rate at which these systems can be purified in order to alleviate the bottleneck identified above. We note that, by the addition of a unitary at the end of the measurement process, rapid purification is identical with rapid state preparation [17–19].

The Von-Neumann entropy,  $S(\rho) = -\text{Tr}[\rho \log \rho]$ , for a quantum state  $\rho$  is a natural choice for characterizing a procedure that purifies and/or cools the state of a quantum system. Unfortunately, the von Neumann entropy is not an easy quantity with which to perform calculations. Because of this the linear entropy, given by  $L(t) = 1 - \text{Tr}[\rho(t)^2]$ , is often used to make the calculations more tractable. In this paper we use the linear entropy, also known as the *impurity*, to characterize the purification process. Since unitary operations on a quantum system leave the eigenvalues of the density matrix unchanged, in order to reduce the entropy of a system it must be allowed to interact with a bath. It is this interaction which enables, and is common to, all purification

and cooling procedures.

Until recently the majority of work in the field of state-purification had been based on what we will term ‘open-loop’ control methods, such as algorithmic cooling [20] or dissipation engineering [21]. In this approach the bath remains unmeasured or the results of the measurements are forgotten. As a result the system evolves according to a deterministic master equation, such as

$$d\rho = dt\mathcal{L}[\ell]\rho \equiv -idt[H(t), \rho] + 2\gamma dt\mathcal{D}[\ell]\rho, \quad (1)$$

where  $\mathcal{D}[A]\rho \equiv A\rho A^\dagger - \frac{1}{2}(A^\dagger A\rho + \rho A^\dagger A)$  [16],  $H(t)$  is the system Hamiltonian,  $\ell$  is a lowering operator and  $\gamma$  is a relaxation rate. Consequently the control signals or interactions are not conditioned on measurement results, and thus can be completely determined prior to the cooling process. Cooling can be thought of as a version of *purification* in which the final state is also the ground state for the system.

In measurement-based purification schemes the bath must be measured. In this case the system can be purified without control fields, provided the system observable coupled to the bath has no degenerate eigenvalues, by measurement alone. The change to an observer’s state of knowledge of an individual system after a weak measurement of the system observable  $X$  is described by the stochastic master equation (SME) [22, 23]

$$d\rho = dt\mathcal{L}_c[X]\rho \equiv 2\gamma dt\mathcal{D}[X]\rho + \sqrt{2\gamma}dW\mathcal{H}[X]\rho, \quad (2)$$

where  $\mathcal{H}[A]\rho \equiv A\rho + \rho A^\dagger - \text{Tr}[(A^\dagger + A)\rho]\rho$  [16], and  $dW$  is the increment of a Wiener noise process [24]. It should be noted that we have moved to a frame that has enabled us to factor out the Hamiltonian evolution. The *measurement strength*,  $\gamma$ , determines the rate at which information is extracted, and thus the rate at which the system is projected onto a single eigenstate of  $X$  [25, 26]. (This means for times  $\tau \gg \gamma^{-1}$  we may say that we have

performed a projective measurement of the observable  $X$ .) The measurement result in a small time interval  $[t, t + dt)$  is

$$dR = \sqrt{4\gamma}\langle X(t) \rangle dt + dW(t), \quad (3)$$

where  $dW$  is the same Wiener noise process that appears in Eq.(2), and  $\langle X(t) \rangle = \text{Tr}[X\rho(t)]$ . We will denote the continuous measurement record obtained by the observer integrated up until time  $t$  as  $R(t) = \int_0^t dR(t')$ .

Conceptually a continuous measurement is a sequence of weak measurements, in the limit where the strength of the measurements tends to zero and the repetition rate tends to infinity [16, 22, 23, 27]. Feedback, if thought about in the framework of a sequence of weak measurements, amounts to the ability to perform a unitary operation in-between each measurement [27]. While unitary operations by themselves do not change the entropy of a system, the average *reduction* in the linear entropy caused by a measurement depends not only on the measurement but also on the prior state of the system. Feedback protocols that increase the rate of purification usually involve choosing the applied unitary after each weak measurement so as to increase the entropy reduction generated by the *next* weak measurement [3, 17–19, 28–43].

Here we consider rapid purification feedback protocols that apply unitary operations to continually keep the eigenbasis of the density matrix unbiased with respect to the basis of the observable being measured,  $X$ . (Two bases of a  $D$ -dimensional system are unbiased with respect to each other if the inner product of every vector of the first basis with every vector of the second basis is equal to  $1/\sqrt{D}$ .) We will refer to this class of feedback protocols as “unbiased-basis” (UBB) feedback protocols. Specifically, the goal of these protocols is to increase the rate at which the *average* linear entropy of the system,  $\langle L(t) \rangle$ , decreases as a function of time. The average here is taken over all possible trajectories (measurement records) for the evolution of the system under the measurement (and feedback). For a single qubit, the UBB protocol is optimal [18, 30, 43]. UBB protocols were first examined for systems of arbitrary dimension in [31]. The purpose of the present work is to clarify and extend the results in [31], as well as to derive upper and lower bounds on the performance of UBB protocols when applied to registers of qubits.

In Section II we review rapid purification for a single qubit. Section III discusses previous results on qudit feedback in an unbiased-basis. And Section IV provides a unified formalism to derive both the upper and lower bound on purification for any UBB feedback on a qudit. Finally, we derive upper and lower bounds for UBB protocols applied to a register of qubits in Section V, and conclude with a discussion of the results.

## II. RAPID PURIFICATION FOR A SINGLE QUBIT

In this section we review the UBB protocol for a single qubit (originally presented in [30]). For a single qubit the UBB protocol is optimal – a non-rigorous proof of this is given in [30], and a rigorous proof is given in [18] and confirmed in Ref. [43]. It is not presently known whether UBB protocols are optimal for systems of higher dimension.

To calculate the factor by which a feedback protocol speeds up the purification of a system we divide the time it takes the feedback protocol to achieve a given value of  $\langle L(t) \rangle$  by the time it takes a measurement in the absence of feedback to achieve this value [49]. In both cases we start the system in the maximally mixed state. We will refer to a measurement acting without feedback as a *bare* measurement [44].

### A. Purification from Measurement Alone

We will perform our analysis keeping the dimension of the system arbitrary, for later convenience. Consider a quantum system of dimension  $D$  initially in the maximally mixed state  $\rho(0) = \mathbf{I}/D$ , where  $\mathbf{I}$  is the  $D \times D$  identity matrix. It is possible to obtain a closed form expression for the linear entropy as a function of the measurement record by using the linear trajectory formulation of continuous measurements [16, 45, 46] (for a simple introduction see [22]). This involves solving the linear version of the SME, which produces an unnormalized density matrix. The linear version of the SME in Eq. (2) is

$$d\tilde{\rho} = dt\tilde{\mathcal{L}}_c[X]\tilde{\rho} \equiv 2\gamma dt\mathcal{D}[X]\tilde{\rho} + \sqrt{2\gamma}dR\tilde{\mathcal{H}}[X]\tilde{\rho}. \quad (4)$$

Here  $\tilde{\mathcal{H}}[A]\rho \equiv A\rho + \rho A^\dagger$ , and the tilde over  $\rho$  denotes the lack of normalization at all but the initial time. Because the initial state is  $\tilde{\rho} = \rho(0) = \mathbf{I}/D$ , the density matrix commutes with  $X$  at all times, and this makes obtaining the solution simple. This solution is [22]

$$\tilde{\rho}(R, t) = \exp(-4\gamma X^2 t) \exp(2\sqrt{2\gamma}XR(t))\mathbf{I}/D, \quad (5)$$

where, as before,  $R(t)$  is the integrated measurement record. For a qubit, for which  $D = 2$ , we take the observable to be  $X = J_z = \sigma_z/2$ . The solution becomes

$$\tilde{\rho}(R, t) = \frac{e^{-\gamma t}}{2} \begin{pmatrix} e^{\sqrt{2\gamma}R} & 0 \\ 0 & e^{-\sqrt{2\gamma}R} \end{pmatrix}. \quad (6)$$

(Here we have dropped the time-dependence of  $R$  for compactness.)

The final normalized density matrix  $\rho(R, t)$  is given by dividing  $\tilde{\rho}(R, t)$  by its norm,  $\mathcal{N} = \text{Tr}[\tilde{\rho}(R, t)]$ . The probability density that we obtain the state  $\rho(R, t)$  at time  $t$ , is given by  $\mathcal{P}(R, t) = \mathcal{N} \exp(-R^2/2t)/\sqrt{2\pi t}$ . The average

impurity of the final state is thus given by averaging the impurity  $L[\rho(R, t)]$  over the probability density  $\mathcal{P}(R, t)$ . For a single qubit this gives

$$\langle L(t) \rangle = \frac{e^{-\gamma t}}{\sqrt{8\pi t}} \int_{-\infty}^{+\infty} \frac{e^{-R^2/2t}}{\cosh(\sqrt{2\gamma}R)} dR. \quad (7)$$

While this integral has no analytic solution (to our knowledge), we can obtain the behavior in the long-time limit by noting that the integral contains two multiplied distributions. The distribution in the numerator is broad compared to the distribution in the denominator for  $t \gg \gamma^{-1}$ . Thus in this long time (LT) limit, the integral can be approximated by  $\int_{-\infty}^{\infty} dR / \cosh(\sqrt{2\gamma}R) = \pi / \sqrt{2\gamma}$ , and we have

$$\langle L(t) \rangle_{\text{LT}} = \frac{\pi e^{-\gamma t}}{\sqrt{16\pi\gamma t}}. \quad (8)$$

The key result is that the impurity for a bare continuous measurement scales asymptotically as  $e^{-\gamma t}$ .

We note that recently Jordan and Korotkov [3] generalized Eq. (7) for an arbitrary initial state,  $\rho_0 = \rho(0) = \frac{1}{2}(\mathbf{I} + x\sigma_x + y\sigma_y + z\sigma_z)$ . Using linear trajectory theory as above one can show that the impurity decays as

$$\langle L(t) \rangle = \frac{e^{-\gamma t} L(\rho_0)}{\sqrt{2\pi t}} \int_{-\infty}^{+\infty} \frac{e^{-R^2/2t} dR}{\cosh(\sqrt{2\gamma}R) + z_0 \sinh(\sqrt{2\gamma}R)}, \quad (9)$$

where  $z_0 = \text{Tr}[\sigma_z \rho(0)]$ . The asymptotic expression is

$$\langle L(t) \rangle_{\text{LT}} = \frac{\pi e^{-\gamma t}}{\sqrt{16\pi\gamma t}} \frac{2L(\rho_0)}{\sqrt{1 - z_0^2}}. \quad (10)$$

## B. Purification Using Feedback

For the initial state  $\rho(0) = \mathbf{I}/2$ , the measurement dynamics is symmetric with respect to rotations about the  $z$ -axis. Because of this we lose nothing by restricting our feedback protocol to rotations about the  $y$  axis at some rate  $\alpha(t)$ . The SME for this situation is

$$d\rho = -idt[\alpha(t)J_y, \rho] + dt\mathcal{L}_c[J_z]\rho(t). \quad (11)$$

To simplify the calculations we assume that  $\alpha(t)$  can be arbitrarily large compared to the measurement strength  $\gamma$ . This means that we can consider the action of the control in each infinitesimal time-interval,  $[t, t + dt)$ , as a unitary that generates a rotation through any desired angle. This unitary is therefore of the form

$$U_t \equiv U(t + dt, t) = \exp\{-i\alpha(t)J_y dt\}. \quad (12)$$

In this case the state following an infinitesimal time-step consisting of measurement and feedback is

$$\begin{aligned} \rho_{\text{fb}}(t + dt) &= U_t\{\rho(t) + d\rho(t)\}U_t^\dagger \\ &= U_t\{\rho(t) + dt\mathcal{L}_c[J_z]\rho(t)\}U_t^\dagger. \end{aligned} \quad (13)$$

Note that up to a unitary transformation, which has no effect on the purity, this is equivalent to having the feedback change the measurement basis:

$$\rho_{\text{fb}}(t + dt) = \rho(t) + dt\mathcal{L}_c[\tilde{X}(t)]\rho(t), \quad (14)$$

where  $\tilde{X}(t + dt) = U_t\tilde{X}(t)U_t^\dagger$  and  $\tilde{X}(0) = J_z$ . This is a Heisenberg picture with respect to the control unitary. In what follows we will always assume, for the sake of simplicity, that the feedback changes the measurement basis, rather than the state of the system.

To derive an expression for  $\langle L(t) \rangle$ , we begin by examining the first-order change in the linear entropy. This is

$$\begin{aligned} dL &= d[1 - \text{Tr}[\rho^2]] = -\text{Tr}[d(\rho^2)] \\ &= -\text{Tr}[2\rho d\rho + (d\rho)^2]. \end{aligned} \quad (15)$$

Here we must keep the second-order term in  $d\rho$ , because  $\rho(t)$  is stochastic, and  $(dW)^2 = dt$  [24]. From Eq. (2), with  $X$  replaced by  $\tilde{X}$ , the change in impurity is thus

$$\begin{aligned} dL &= -8\gamma dt\{\text{Tr}[\rho\tilde{X}\rho\tilde{X}] - 2\text{Tr}[\tilde{X}\rho]\text{Tr}[\tilde{X}\rho^2] \\ &\quad + \text{Tr}[\rho\tilde{X}]^2\text{Tr}[\rho^2]\} \\ &\quad - 4\sqrt{2\gamma}dW\{\text{Tr}[\tilde{X}\rho^2] - \text{Tr}[\rho\tilde{X}]\text{Tr}[\rho^2]\}. \end{aligned} \quad (16)$$

To obtain the greatest decrease in impurity in each time interval  $[t, t + dt)$ , we must now optimize over all unitaries  $U_t$  to obtain the locally optimal  $\tilde{X}(t)$ . It was shown in [30] that for a single qubit this is achieved by choosing the eigenbasis of  $\tilde{X}$  to be *unbiased* with respect to the eigenbasis of  $\rho$ . Each infinitesimal measurement disturbs this unbiased relationship, and thus feedback is required to maintain it. Since the disturbance to the basis of  $\rho$  is proportional to  $dW$  (rather than  $dt$ ), to keep the bases *perfectly* unbiased requires that  $\alpha(t)$  be arbitrarily large.

If the bases of  $\tilde{X}(t)$  and  $\rho(t)$  are unbiased, then the bases of  $\tilde{X}(t)$  and  $\rho(t + dt)$  will only be infinitesimally biased, so that the necessary feedback unitary  $U(t, t + dt)$  will be infinitesimally different from  $\mathbf{I}$ . This is required for physically reasonable feedback. Mathematically, however, it is simpler to imagine the case where  $\rho(t)$  is diagonal in the  $J_z$  basis. In this case,  $\tilde{X}(t)$  will be obtainable from  $J_z$  by a finite unitary rotation.

We choose  $\tilde{X} = J_x$ , so that the unitary that transforms  $X$  to  $\tilde{X}$  via  $\tilde{X} = TJ_zT^\dagger$ , is

$$T \equiv \exp\left(i\frac{\pi}{2}J_y\right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}. \quad (17)$$

One can show that if  $\tilde{X}$  is traceless, and unbiased with respect to  $\rho$ , then regardless of the dimension  $\text{Tr}[\tilde{X}\rho] = 0$  and  $\text{Tr}[\tilde{X}\rho^2] = 0$  (the derivation is given in Appendix A). This considerably simplifies the expression for  $dL$ , which is now

$$dL = -8\gamma\text{Tr}[\tilde{X}\rho\tilde{X}\rho] dt. \quad (18)$$

For a single qubit it turns out that  $\text{Tr}[\check{X}\rho\check{X}\rho] = L/4$  and we obtain the very simple equation

$$dL = -2\gamma dt L. \quad (19)$$

Evolution of the impurity is thus deterministic, and is given by

$$L(t) = e^{-2\gamma t} L(0). \quad (20)$$

Note that the evolution of  $L$  is only perfectly deterministic under the assumption that the observable  $\check{X}$  is perfectly unbiased with respect to the density matrix. In the long-time limit we obtain the speedup factor from Eqs. (8) and (20). Denoting the time taken by a bare measurement to reach a given value of  $L$  as  $t_{\text{bare}}$ , and that for the feedback protocol as  $t_{\text{fb}}$ , we equate  $L(t_{\text{fb}}) = L(t_{\text{bare}})$  and solve for the ratio  $t_{\text{fb}}/t_{\text{bare}}$ . Doing so gives

$$\frac{t_{\text{fb}}}{t_{\text{bare}}} = \frac{1}{S} = \frac{1}{2} + \frac{\ln \sqrt{16\pi\gamma t_{\text{bare}}}}{2\gamma t_{\text{bare}}} - \frac{\ln 2\pi}{2\gamma t_{\text{bare}}}. \quad (21)$$

For sufficiently large  $t_{\text{bare}}$  (equivalently, a sufficiently small target impurity) the second and third terms are insignificant, and we obtain

$$S = \frac{t_{\text{bare}}}{t_{\text{fb}}} = 2. \quad (22)$$

Numerical calculations show that for shorter times (higher target impurities) the speedup factor is always less than this. Thus the largest possible speedup for a single qubit is a factor of 2.

### III. QUDIT PURIFICATION USING FEEDBACK

#### A. Purification from Measurement Alone

To analyze UBB feedback protocols for  $D$ -dimensional systems, we will need the asymptotic evolution of the impurity for a bare measurement of  $J_z$  for arbitrary  $D$ . In [31] it was shown only that at long times  $L \sim e^{-\gamma t}$ . A more detailed analysis, to be presented elsewhere [47], shows that the asymptotic behavior is

$$\langle L_2(t) \rangle_{\text{LT}} = \frac{2(D-1)}{D} \frac{\pi e^{-\gamma t}}{\sqrt{16\gamma t\pi}}. \quad (23)$$

Interestingly this is merely the expression for a single qubit, Eq. (7), multiplied by a factor that depends on the dimension of the system.

#### B. The UBB protocol

In this section we examine the generalization of the qubit rapid purification algorithm to  $D$ -dimensional systems (qudits), which was first proposed in [31]. Recall

that an UBB protocol for a  $D$  dimensional system involves using feedback to continually adjust the measured observable  $\check{X}(t)$  so that its eigenbasis remains unbiased with respect to the density matrix. Note that for these protocols we require only a single basis that is unbiased with respect to  $\rho$  — we do not require a complete set of mutually unbiased bases.

The change in the impurity in a single infinitesimal time-step is once again given by Eq.(18):

$$dL = -8\gamma \text{Tr}[\check{X}\rho\check{X}\rho] dt. \quad (24)$$

However, in this case the right-hand side is no longer a simple function of  $L$ . Further, the evolution of  $L$  need no longer be deterministic;  $L$  is now coupled to other functions of  $\rho$ , and these will still evolve stochastically. It will be useful in what follows to write the right-hand side explicitly in terms of the matrix elements of  $\check{X}$  in the elementary basis (the eigenbasis of  $\rho$ ). Denoting this basis as  $\{|i\rangle\}$ ,  $i = 1, \dots, N$ , we have

$$dL = -8\gamma dt \sum_{i,j} |\check{X}_{i,j}|^2 \lambda_i \lambda_j. \quad (25)$$

where  $\lambda_j$  is the eigenvalue of  $\rho$  associated with the eigenstate  $|j\rangle$ .

In [31] a lower bound was derived on the performance of UBB protocols, by considering a protocol in which simultaneous measurements are made of all observables that can be obtained from  $\check{X}$  by permuting the basis vectors. This was possible because the evolution of  $L$  under this protocol can be solved. Under the  $D!$  simultaneous measurements, the total change in  $L$ ,  $dL_{\text{tot}}$ , is simply the sum of the  $dL$ 's due to each measurement:

$$dL_{\text{tot}} = -\frac{8\gamma dt}{D!} \sum_{m=1}^{D!} \text{Tr}[\check{X}_m^\dagger \rho \check{X}_m^\dagger \rho] \quad (26)$$

where the  $\check{X}_m = P_m^\dagger \check{X} P_m$  are  $D!$  permutations of the operator  $\check{X}$ . Since at least one of the observables  $\check{X}_m$  in the sum in Eq.(26) must give a  $dL$  that is at least as large as the average over all the  $\check{X}_m$ , the performance of this protocol is a lower bound on the performance of protocols that employ a single optimized observable  $\check{X}(t)$ . An intricate calculation [31] shows that Eq. (26) can then be rewritten in a remarkably simple way:

$$dL_{\text{tot}} = -8\gamma dt \frac{(D-2)!}{D!} \text{Tr}[X^2] L. \quad (27)$$

In Appendix B we give a new, and much more detailed, proof of the process to obtain the relation in Eq.(27) from Eq. (26), and in Sec. V we will use this to obtain a lower bound on UBB protocols for a register of qubits. When  $X = J_z$ ,  $\text{Tr}[X^2] = \text{Tr}[J_z^2] = D(D^2-1)/12$ , and Eq. (27) becomes

$$dL_{\text{LB}} = -\frac{2}{3}\gamma t(D+1)L. \quad (28)$$

The subscript LB indicates that this increment is a lower bound on  $|dL|$  for any unbiased basis feedback, that is  $|dL_{\text{LB}}| \leq |dL[\rho]|$ .

#### IV. UPPER AND LOWER BOUNDS FOR RAPID PURIFICATION USING UBB FEEDBACK

We now introduce a new method to determine the lower bound obtained in [31], Eq. (28) here, and a similar method that allows us to obtain an upper bound.

The lower bound in Ref.[31] was obtained by averaging over all permutations  $P_m$  of the measured observable. We now note that this procedure renders  $\langle dL \rangle$  invariant to such permutations. In light of this, and by analogy with the technique employed in Ref. [41], we introduce a density matrix for which  $dL$  is invariant under the permutations  $P_m$ :

$$\rho_F = \text{diag} \left( 1 - \Delta, \frac{\Delta}{D-1}, \frac{\Delta}{D-1}, \dots, \frac{\Delta}{D-1} \right). \quad (29)$$

We call this the ‘‘flat state’’, as it has one large eigenvalue and the remaining eigenvalues are equal in magnitude (‘‘flat’’). For any  $D$ -dimensional state  $\rho$ , with an impurity  $L[\rho]$ , we can always find a  $\Delta$  so that  $L[\rho_F] = L[\rho]$ .

Intuitively the state in which  $dL$  is *most* sensitive to permutations for a fixed value of  $L$  is

$$\rho_2 = \text{diag}(1 - \Delta', \Delta', 0, \dots, 0). \quad (30)$$

We will refer to this state as the ‘‘binary’’ distribution. Once again, for a given  $\rho$  we can always find a  $\Delta'$  so that  $L[\rho_2] = L[\rho]$ .

We now derive upper and lower bounds on UBB protocols by showing that when  $L[\rho] = L[\rho_F] = L[\rho_2]$ , and when each of these three density matrices have a permutation applied that maximizes  $dL$ ,

$$|\langle dL[\rho_F] \rangle| \leq |\langle dL[\rho] \rangle| \leq |\langle dL[\rho_2] \rangle|. \quad (31)$$

##### A. The Lower Bound via the flat distribution

In Sec. III we showed that the lower bound on the change in impurity is  $dL_{\text{LB}} = -\frac{2}{3}\gamma t(D+1)L$ . That is,  $|dL_{\text{LB}}| \leq |dL(\rho)|$ . Now we show that  $dL_{\text{LB}} = dL(\rho_F)$ . We first note that the impurity of  $\rho_F$  can be written as

$$L[\rho_F] = (D-1) \left[ \frac{2\Delta(1-\Delta)}{D-1} + (D-2) \frac{\Delta^2}{(D-1)^2} \right]. \quad (32)$$

Equation (32) will enable us to factor out the impurity in the following working. Substituting  $\rho_F$  into Eq. (25) to calculate  $dL(\rho_F)$  (or  $dL_F$  in shorthand notation) and then writing  $dL_F$  in the form of Eq. (32) we have

$$dL_F = -8\gamma dt \left( \frac{2\Delta(1-\Delta)}{(D-1)} \sum_{r \neq p} |\check{X}_{rp}|^2 + \frac{\Delta^2}{(D-1)^2} \sum_{r \neq p, c \neq p} |\check{X}_{rc}|^2 \right), \quad (33)$$

where the largest eigenvalue  $1 - \Delta$  is associated with some particular eigenstate  $|p\rangle$ . It is easy to see that  $dL_F$  is invariant under the transformation  $dL[\rho_F] = dL(P_m^\dagger \rho_F P_m)$  for all the  $D!$  permutations  $P_m$  labeled by  $m$ . The permutation invariance of  $\rho_F$  already implies that  $dL(\rho_F) = (1/D!) \sum_{m=1}^{D!} dL(P_m^\dagger \rho_F P_m) = dL_{\text{tot}} = dL_{\text{LB}}$ . Nevertheless we pursue the simplification of Eq. (33) by noting that for any unbiased-basis

$$\sum_{r \neq p} |\check{X}_{rp}|^2 = (D+1)(D-1)/12, \quad (34)$$

as shown in Appendix C. From this it follows that

$$\sum_{r \neq p, c \neq p} |\check{X}_{rc}|^2 = \frac{D+1}{12} (D-1)(D-2). \quad (35)$$

Thus it is possible to write Eq. (33) so that it has the same form as Eq. (32), simplifying the resulting expression gives:

$$dL_F = -8\gamma dt \frac{(D+1)}{12} L[\rho_F] = -\frac{2}{3}(D+1)\gamma dt L(t). \quad (36)$$

It should be noted that technically we have not independently rederived the lower bound in Eq. (28); rather we have shown that for all unbiased bases and for all possible permutations  $P_m$  of  $\rho_F$ 's basis and for all impurities  $dL_{\text{LB}} = dL_F$ .

##### B. The Upper Bound via the binary distribution

We now show that  $|dL[\rho]| \leq |dL[\rho_2]|$ . Substituting  $\rho_2$  in to Eq. (25) gives  $dL_2 = -8\gamma dt [2(1-\Delta')\Delta' |\check{X}_{r,c}|^2]$ . This expression is sensitive to the arrangement of the eigenvalues of  $\rho_2$ ; accordingly  $dL[\rho_2] \neq dL(P_m^\dagger \rho_2 P_m)$  for most permutations. The impurity for  $\rho_2$  can be written as

$$L[\rho_2] = 2(1-\Delta')\Delta' = L[\rho] = \sum_{r \neq c, c \neq r} \lambda_r \lambda_c. \quad (37)$$

Using these relations we find for the optimal permutation that  $dL(\rho_2) = -8\gamma dt [2(1-\Delta')\Delta' \max_{mn} |\check{X}_{mn}|^2] = -8\gamma dt \max_{mn} |\check{X}_{mn}|^2 L[\rho]$ . To prove  $|dL(\rho)| \leq |dL(\rho_2)|$  we need to prove that

$$\sum_{r,c} \lambda_r \lambda_c |\check{X}_{rc}|^2 \leq \sum_{r,c} \lambda_r \lambda_c \max_{mn} |\check{X}_{mn}|^2. \quad (38)$$

This is trivially true since all the  $\lambda_i$ 's are positive. All that remains is to bound the  $\max_{mn} |\check{X}_{mn}|^2$  in any unbiased-basis.

A general unitary that transforms the basis  $|k\rangle$  to an unbiased-basis is  $T|n\rangle = \sum_{-j}^j \frac{1}{\sqrt{D}} \exp(i\phi_k^{(n)})|k\rangle$ . It is possible to rewrite  $|\check{X}_{mn}|^2$  as  $|\check{X}_{mn}|^2 = |\langle m|T^\dagger J_z T|n\rangle|^2$

so that

$$\begin{aligned} \max_{mn} |\tilde{X}_{mn}|^2 &\leq \max_{\{\phi_k^{(n)}\}, \{\theta_k^{(m)}\}} \frac{1}{D^2} \left| \sum_{k=-j}^j e^{i(\phi_k^{(n)} - \theta_k^{(m)})} k \right|^2 \\ &\leq \frac{1}{D^2} \left| \sum_{k=-j}^j k \right|^2. \end{aligned} \quad (39)$$

For even  $D$  Eq. (39) evaluates to  $D^2/16$ ; for odd  $D$  it evaluates to  $D^2/16 - 1/8 + 1/(16D^2)$ . For large  $D$  (say  $D > 5$ ),  $D^2/16$  is a good approximation for both even and odd  $D$ . To find the lower bound on the decrease in impurity it is important to remember that two matrix elements contribute to the sum:  $\max_{m,n} |\tilde{X}_{mn}|^2 \lambda_m \lambda_n$ , and  $\max_{m,n} |\tilde{X}_{nm}|^2 \lambda_n \lambda_m$ . For large  $D$  the impurity under the two eigenvalue distribution is then

$$dL_2 \leq -8\gamma dt \frac{D^2}{16} 2\lambda_0 \lambda_1 = -\gamma dt \frac{D^2}{2} L_2(t). \quad (40)$$

The dependance for this matrix element is only on the dimension of the system. Thus the speed-up upper bound for any unbiased-basis feedback is

$$S_2 \leq \frac{D^2}{2}, \quad (41)$$

for  $D \gg 1$  and  $t \gg \gamma^{-1}$ .

## V. A REGISTER OF QUBITS

We now generalize UBB feedback protocols to the case of a register of  $n$  qubits, where each qubit is independently and continuously measured. Instead of one observable  $X$ , we now have  $n$ , given by  $X^{(r)} = I^{(1)} \otimes I^{(2)} \otimes \dots \otimes \sigma_z^{(r)} \dots \otimes I^{(n)}$ , where  $r$  labels the  $r$ th qubit. The SME describing such a measurement is

$$d\rho = \sum_r 2\kappa dt \mathcal{D} \left[ X^{(r)} \right] \rho + \sqrt{2\kappa} dW^{(r)} \mathcal{H} \left[ X^{(r)} \right] \rho. \quad (42)$$

The combined state of the  $n$  qubits exists in a  $D = 2^n$  dimensional Hilbert space.

### A. Purification from Measurement Alone

In this section we will not analyse the no-feedback case to the same level of rigor as we did in section II A, but rather, we rely upon the intuition gained from that analysis. For simplicity, consider first a two-qubit register with uncorrelated qubits. The state of the system is  $\rho = \rho_1 \otimes \rho_2$ . The impurity for such a state is

$$L^{(2)} = 1 - \text{Tr} \left[ (\rho_1 \otimes \rho_2)^2 \right] = 1 - \text{Tr} \left[ \rho_1^2 \right] \text{Tr} \left[ \rho_2^2 \right], \quad (43)$$

where the superscript “(2)” on  $L$  signifies the number of qubits in the register. For very pure states it is natural

to parameterize the eigenvalues of the  $r$ th qubit,  $\rho_r$ , as  $\{\lambda_0^r = 1 - \Delta_r, \lambda_1^r = \Delta_r\}$  where the convention that  $\Delta_r \ll 1$  still holds. To first order in  $\Delta$  we have

$$L^{(2)} = 1 - (1 - 2\Delta_1)(1 - 2\Delta_2) \sim 2(\Delta_2 + \Delta_1). \quad (44)$$

Because the qubits are initially uncorrelated, and are independently monitored, it is reasonable to assume that  $\Delta_1$  and  $\Delta_2$  are of the same order, so  $L^{(2)} \sim 2(2\Delta)$ . When  $\Delta \ll 1$  then  $L = 2(1 - \Delta)\Delta \approx 2\Delta$  so  $L^{(2)} \approx 2L$ . At long times, for  $n$  qubits we expect that

$$\langle L^{(n)} \rangle_{\text{LT}} \sim n \langle L^{(1)} \rangle_{\text{LT}}. \quad (45)$$

We can verify this using the analytic expression for qubit impurity, Eq. (7). Recalling that the purity may be written as  $P = 1 - L$ , we have  $\langle P^{(n)} \rangle = \langle P^{(1)} \rangle^n$ , so

$$\langle L^{(n)}(t) \rangle = 1 - \left( 1 - \frac{e^{-4\kappa t}}{\sqrt{8\pi t}} \int_{-\infty}^{\infty} \frac{e^{-R^2/(2t)} dR}{\cosh(\sqrt{8\kappa R})} \right)^n. \quad (46)$$

Using the long-time expression for a qubit, Eq. (8), we obtain a long-time analytical expression for  $L$  in the absence of feedback for a register of  $n$  qubits

$$\langle L^{(n)}(t) \rangle_{\text{LT}} \sim 1 - \left( 1 - \frac{n\pi e^{-4\kappa t}}{\sqrt{64\pi\gamma t}} \right) = \frac{n\pi e^{-4\kappa t}}{8\sqrt{\pi\kappa t}}. \quad (47)$$

To compare this expression to the qubit expression, Eq. (8),  $n$  is set to 1 and  $\kappa = \frac{1}{4}\gamma$ .

### B. Lower bound for purification using UBB feedback on a register of qubits

The change in impurity for a register of qubits in an unbiased basis is

$$dL = -8\kappa dt \sum_{r=1}^n \text{Tr} \left[ \tilde{X}^{(r)} \rho \tilde{X}^{(r)} \rho \right] \quad (48)$$

$$= -8\kappa dt \sum_{r=1}^n \sum_{i,j=0}^{(D-1)} |\tilde{X}_{i,j}^{(r)}|^2 \lambda_i \lambda_j. \quad (49)$$

Using  $\rho_F$  to calculate the lower bound for a UBB protocol in a register appears to be difficult. Instead we will derive the lower bound using the same method presented in Appendix B. To do this we will again introduce the feedback in the Heisenberg picture so that  $\tilde{X}^{(r,m)} = P_m T X^{(r)} T^\dagger P_m^\dagger$ . As before the  $T$ 's are conditional unitaries that introduce the unbiasedness (between  $\rho$  and  $X^{(r)}$ ) and the  $P_m$ 's also retain their meaning as permutations. For a register being measured in a basis that is unbiased with respect to the logical basis, with a randomly changing permutation, the change in impurity is

$$dL = \sum_{r=1}^n \sum_{m=1}^{D!} -8\kappa dt \text{Tr} \left[ \tilde{X}^{(r,m)} \rho \tilde{X}^{(r,m)} \rho \right]$$

where  $D = 2^n - 1$ . After performing a similar procedure to the one found in Appendix B we find

$$dL = -8\kappa dt n D(D-2)! L(t). \quad (50)$$

Thus we find the impurity of the state undergoing feedback of the above form decreases as

$$L^{(n)}(t) = e^{-8\kappa nt/(D-1)} L(0). \quad (51)$$

The asymptotic speed-up factor is

$$S = \frac{2n}{D-1}. \quad (52)$$

For  $n = 1$  (i.e. a qubit) the speed-up factor  $S$  is  $S = 2$ , which agrees with the result from Ref. [30]. When  $n = 2$ , the speed-up is  $S = 4/3$ . This is comparable to the speed-up found for the locally optimal rapid measurement (RM) protocol in [41] where the predicted speed-up in the long-time limit was  $S_{\text{RM}} \approx 1.4$ . (The feedback in the rapid measurement protocol permutes the eigenvalues of  $\rho$  in the logical basis to decrease a different measure of impurity. Thus at all times the state eigenbasis and the measurement basis commute.) Unfortunately when  $n = 3$ ,  $S = 6/7$ , which is a slow-down. This slow-down trend continues for all  $n \geq 3$ , and for large  $n$  the slow-down is  $\sim n2^{-n+1}$ .

One can interpret Eq. (52) as a lower bound on an UBB algorithm for a register of qubits in much the same way as we did in Section III B. Equation (52) may also be interpreted as an all-permutation deterministic purification protocol, although it is only useful in a two qubit register.

### C. Upper bound for purification using UBB feedback on a register of qubits

As before it is possible to rewrite  $|\check{X}_{mn}^{(r)}\rangle$  as  $|\check{X}_{mn}^{(r)}\rangle = |\langle m|T^\dagger X^{(r)} T|n\rangle|$  so that

$$\max_{mn} |\check{X}_{mn}^{(r)}| \leq \max_{\{\varphi_k\}} \frac{1}{D} \left| \sum_{k=0}^{D-1} e^{i\varphi_k} (-1)^{f(k,r)} \right|, \quad (53)$$

where  $f(k, r)$  is a function that appropriately determines the sign of the diagonal elements of  $X^{(r)}$ . Thus

$$\max_{mn} |\check{X}_{mn}| \leq 1, \quad (54)$$

and

$$dL_2^{(n)} \leq -8\kappa dt \sum_{r=1}^n L(t) = -8\kappa dt n L(t).$$

At long times the speed-up upper bound for any UBB feedback in a register is

$$S_2 \leq 2n. \quad (55)$$

By substituting in  $n = 1$  we regain the result of Ref. [30]. At present it is unclear if the bound in Eq. (55) is tight. One reason why we expect this bound not to be tight comes from the upper bound on the rapid measurement protocol of Ref. [41]. The upper bound was shown to be  $n$  and numerical results indicated it was  $S_{\text{RM}} = 0.718n$ , which is significantly less than the upper bound.

## VI. DISCUSSION

For a qudit we have bounded the speed-up in purification for any unbiased basis feedback by  $\frac{2}{3}(D+1) \leq S \leq D^2/2$ . Prior to this work only the lower bound was known for the qudit. In Ref. [19] it was shown that by applying a unitary, chosen at random from the unitary group  $\mathfrak{U}(D)$ , to a qudit during the measurement process (random feedback) one could attain  $S = \frac{2}{3}D$  asymptotically. This suggests UBB feedback is unnecessary for a speed-up  $O(D)$ , although it remains an open question whether the actual speed-up for UBB protocols is  $O(D)$  or  $O(D^2)$ .

We also examined UBB feedback applied to a register of  $n$  qubits. We have shown that the speed-up in purification is bounded by  $2n/(2^n - 1) \leq S \leq 2n$ . Prior to this work there were no results for purification of a register of qubits using UBB feedback.

Unlike the rapid measurement (RM) protocols of [41] the UBB protocols presented in this paper are not locally optimized in time for decreasing  $dL$ . Additionally it is not clear if UBB protocols allow one to obtain information about the preparation procedure, unlike RM protocols which may be used for state estimation.

In the future we plan to investigate locally optimal protocols for the impurity (and other measures of mixedness), and examine rapid purification using a particular unbiased basis. Also, very recently Ruskov *et al.* [48] have considered monitoring a single qubit in three unbiased bases simultaneously. The relation between their work and ours remains to be explored.

*Acknowledgements:* The authors thank Andy Chia and Andrew Scott for helpful discussions. JC and HMW are supported by the Australian Research Council (FF0458313 and CE0348250). KJ is supported by the National Science Foundation, under Project No. PHY-0902906.

### Appendix A: Proof that $\check{X}_{ii} = 0$

For a traceless operator  $X$ , which is diagonal in the computational basis, we can find a transformation  $T$  that will make it unbiased with respect to the computational basis. The transformation has the form  $\check{X} = T X T^\dagger$

$$\check{X}_{il} = \sum_{j,k=1}^D T_{ij} X_{jk} T_{kl}^\dagger.$$

Now we wish to examine the diagonal elements. Being mindful of the fact that  $T_{rs}^\dagger = T_{sr}^*$  we have

$$\check{X}_{ii} = \sum_{j,k=1}^D T_{ij} X_{jk} T_{ki}^\dagger = \sum_{j,k=1}^D T_{ij} X_{jk} T_{ik}^* = \sum_{j,k=1}^D T_{ij} T_{ik}^* X_{jk}.$$

Using the fact that  $X$  is diagonal gives the expression

$$\check{X}_{ii} = \sum_{j=1}^D T_{ij} T_{ij}^* X_{jj}. \quad (\text{A1})$$

Unbiasedness means that  $T_{ij} T_{ij}^* = 1/D$  so that

$$\check{X}_{ii} = \frac{1}{D} \sum_{j=1}^D X_{jj}. \quad (\text{A2})$$

Recalling that  $X$  is traceless, we thus have  $\check{X}_{ii} = 0$ .

### Appendix B: Proof of Eq. (26)

Denote eigenvalues and eigenvectors of  $\rho$  in the basis which diagonalizes  $\rho$  as  $\rho|i\rangle = \lambda_i|i\rangle$ . Define  $X$  as a Hermitian operator that is diagonal in this eigenbasis, and  $\check{X} = T X T^\dagger$  as a transformed version of  $X$  that is unbiased with respect to this eigenbasis. Now define  $P_m$ , for  $m = 1, \dots, D!$ , to be the  $D!$  operators that give each of the possible permutations of the eigenbasis  $|i\rangle$ : for example,  $P_m|i\rangle = |m(i)\rangle$  labels a particular permutation of the basis  $|i\rangle$ , while  $P_m^\dagger|i\rangle = |m^{-1}(i)\rangle$  is an inverse permutation to  $m$ . Note that  $P_m^\dagger P_m|i\rangle = P_m P_m^\dagger|i\rangle = |i\rangle$ . Starting with Eqn. 26 one may write

$$\begin{aligned} S &= \sum_{m=1}^{D!} \text{Tr} [P_m \check{X} P_m^\dagger \rho P_m \check{X} P_m^\dagger \rho] \\ &= \sum_{m=1}^{D!} \sum_{i=1}^D \langle i | \check{X} P_m^\dagger \rho P_m \check{X} P_m^\dagger \rho P_m | i \rangle. \end{aligned} \quad (\text{B1})$$

Consider the action of the permutation operators and the state on the basis  $|i\rangle$

$$P_m^\dagger \rho P_m |i\rangle = P_m^\dagger \rho |m(i)\rangle = \lambda_{m(i)} P_m^\dagger |m(i)\rangle = \lambda_{m(i)} |i\rangle. \quad (\text{B2})$$

Using the notation  $\check{X}|i\rangle = |\check{X}i\rangle$ , we thus have

$$S = \sum_{m=1}^{D!} \sum_{i=1}^D \lambda_{m(i)} \langle \check{X}i | P_m^\dagger \rho P_m | \check{X}i \rangle. \quad (\text{B3})$$

Now we use the completeness of the basis ( $\langle a|b\rangle =$

$\sum_j \langle a|(|j\rangle\langle j|)|b\rangle$ ) so that

$$S = \sum_{m=1}^{D!} \sum_{i,j=1}^D \lambda_{m(i)} \langle \check{X}i|j\rangle \langle j| P_m^\dagger \rho P_m | \check{X}i \rangle \quad (\text{B4})$$

$$= \sum_{m=1}^{D!} \sum_{i,j=1}^D \lambda_{m(i)} \lambda_{m(j)} \langle \check{X}i|j\rangle \langle j| \check{X}i \rangle \quad (\text{B5})$$

$$= \sum_{m=1}^{D!} \sum_{i,j=1}^D \lambda_{m(i)} \lambda_{m(j)} |\langle \check{X}i|j\rangle|^2. \quad (\text{B6})$$

Next we wish to sum over the  $m$  label, which represents permutations of the basis. First we define

$$C_{ij} = |\langle \check{X}i|j\rangle|^2 \sum_{m=1}^{D!} \lambda_{m(i)} \lambda_{m(j)}, \quad (\text{B7})$$

so that  $S = \sum_{ij} C_{ij}$ . Suppose  $i = j$ , then

$$C_{ii} = |\langle \check{X}i|i\rangle|^2 \sum_{m=1}^{D!} \lambda_{m(i)}^2. \quad (\text{B8})$$

There are  $(D-1)!$  permutations that take  $i \rightarrow p$  for a fixed  $p \in [1, 2, \dots, D]$ , so

$$C_{ii} = |\langle \check{X}i|i\rangle|^2 (D-1)! \sum_{p=1}^D \lambda_p^2 = |\langle \check{X}i|i\rangle|^2 (D-1)! \text{Tr} [\rho^2]. \quad (\text{B9})$$

Now consider the case where  $i \neq j$ . Take any pair  $q \neq p$  and look for permutations that take  $i \rightarrow p$ ,  $j \rightarrow q$ . There are  $(D-2)!$  of these permutations:

$$C_{ij} = |\langle \check{X}i|j\rangle|^2 (D-2)! \sum_{p \neq q} \lambda_p \lambda_q. \quad (\text{B10})$$

Now examine  $\sum_{p \neq q} \lambda_p \lambda_q$  term:

$$\begin{aligned} \left( \sum_p \lambda_p \right)^2 &= \left( \sum_p \lambda_p \right) \left( \sum_q \lambda_q \right) \\ &= \sum_p \lambda_p^2 + \sum_{p \neq q} \lambda_p \lambda_q \\ (\text{Tr} [\rho])^2 &= \text{Tr} [\rho^2] + \sum_{p \neq q} \lambda_p \lambda_q. \end{aligned} \quad (\text{B11})$$

As  $\rho$  is normalized we find  $\sum_{p \neq q} \lambda_p \lambda_q = 1 - \text{Tr} [\rho^2]$ . The simplified expression for Eq. (B1), so far, is

$$\begin{aligned} S &= \sum_i C_{ii} + \sum_{i,j \neq i} C_{ij} \\ &= \sum_i (D-1)! \text{Tr} [\rho] |\langle \check{X}i|i\rangle|^2 \\ &\quad + \sum_{i,j \neq i} (D-2)! (1 - \text{Tr} [\rho^2]) |\langle \check{X}i|j\rangle|^2. \end{aligned} \quad (\text{B12})$$

Now we simplify the expression  $\sum_{i \neq j} |\langle \check{X}i|j \rangle|^2$ . Using the Parseval relation for a vector  $\Psi$ ,  $\langle \Psi|\Psi \rangle = \sum_{j=1}^D |\langle \Psi|j \rangle|^2$ , we find

$$\begin{aligned} \sum_{j=1}^D |\langle \check{X}i|j \rangle|^2 &= \sum_{j \neq i} |\langle \check{X}i|j \rangle|^2 + \sum_{j=i} |\langle \check{X}i|i \rangle|^2 \\ \langle \check{X}i|\check{X}i \rangle &= \sum_{j \neq i} |\langle \check{X}i|j \rangle|^2 + \langle \check{X}i|i \rangle^2, \end{aligned} \quad (\text{B13})$$

i.e.  $\sum_{j \neq i} |\langle \check{X}i|j \rangle|^2 = \langle \check{X}i|\check{X}i \rangle - \langle \check{X}i|i \rangle^2$ . The total expression is now

$$\begin{aligned} S &= \sum_i^D (D-1)! \text{Tr}[\rho] |\langle \check{X}i|i \rangle|^2 \\ &+ (D-2)!(1 - \text{Tr}[\rho^2]) \sum_{i=1}^D (\langle \check{X}i|\check{X}i \rangle - \langle \check{X}i|i \rangle^2). \end{aligned} \quad (\text{B14})$$

Massaging the  $\sum_{i=1}^D \langle \check{X}i|\check{X}i \rangle$  term gives

$$\sum_{i=1}^D \langle \check{X}i|\check{X}i \rangle = \sum_{i=1}^D \langle i|\check{X}^\dagger \check{X}|i \rangle = \text{Tr}[\check{X}^2].$$

Recall that  $\check{X} = TXT^\dagger$ , thus  $\text{Tr}[\check{X}^\dagger \check{X}] = \text{Tr}[(TXT^\dagger)^\dagger TXT^\dagger] = \text{Tr}[X^2]$ .

Now we examine the  $\sum_{i=1}^D \langle \check{X}i|i \rangle^2$  term. The eigenvectors and eigenvalues of  $\check{X}$  are  $\check{X}|\Psi_b \rangle = x_b |\Psi_b \rangle$  and  $\langle i|\Psi_b \rangle = 1/\sqrt{D}$  by way of their unbiasedness. By inserting the identity we have

$$\begin{aligned} \langle \check{X}i|i \rangle &= \sum_b \langle \check{X}i|\Psi_b \rangle \langle \Psi_b|i \rangle \\ &= \frac{1}{\sqrt{D}} \sum_b \langle i|\check{X}|\Psi_b \rangle \\ &= \frac{1}{\sqrt{D}} \sum_b x_b \langle i|\Psi_b \rangle \\ &= \frac{1}{D} \sum_b x_b = \text{Tr}[\check{X}]/D, \end{aligned} \quad (\text{B15})$$

so  $\sum_{i=1}^D \langle \check{X}i|i \rangle^2 = \text{Tr}[\check{X}]^2/D^2$ . The total expression is

$$\begin{aligned} S &= (D-1)! \text{Tr}[\rho] \text{Tr}[\check{X}]^2/D^2 \\ &+ (D-2)!(1 - \text{Tr}[\rho^2]) (\text{Tr}[\check{X}^2] - \text{Tr}[\check{X}]^2/D^2). \end{aligned} \quad (\text{B16})$$

Finally, recalling from Appendix A that  $\check{X}$  is traceless, we have

$$S = (D-2)! \text{Tr}[\check{X}^2] (1 - \text{Tr}[\rho^2]) \quad (\text{B17})$$

as required.

### Appendix C: Proof of Eq. (34)

Recall that  $\sum_{r \neq 0}^D |\check{X}_{r0}|^2 = \sum_{r=0}^D |\check{X}_{r0}|^2$  as  $|\check{X}_{ii}| = 0$ . So,

$$\langle k|\check{X}^\dagger \check{X}|k \rangle = \langle k|(UJ_z U^\dagger)^\dagger UJ_z U^\dagger|k \rangle = \langle k|UJ_z^2 U^\dagger|k \rangle.$$

Now insert the identity

$$\begin{aligned} \langle k|\check{X}^\dagger \check{X}|k \rangle &= \sum_{l,m} \langle k|U|l \rangle \langle l|J_z^2|m \rangle \langle m|U^\dagger|k \rangle \\ &= \sum_{l,m} \langle k|U|l \rangle \langle l|J_z^2|m \rangle \langle m|U^\dagger|k \rangle. \end{aligned} \quad (\text{C1})$$

The matrix  $J_z^2$  is diagonal, so

$$\begin{aligned} \langle k|\check{X}^\dagger \check{X}|k \rangle &= \sum_l \langle l|J_z^2|l \rangle \langle k|U|l \rangle \langle l|U^\dagger|k \rangle \\ &= \sum_l \langle l|J_z^2|l \rangle |\langle k|U|l \rangle|^2 \\ &= \frac{1}{D} \sum_l \langle l|J_z^2|l \rangle = \frac{D^2 - 1}{12}. \end{aligned} \quad (\text{C2})$$

- [1] e.g. criteria number two of D. P. DiVincenzo, *Fortschritte der Physik* **48**, 771 (2000).
- [2] N. P. Oxtoby, P. Warszawski, H. M. Wiseman, He-Bi Sun and R. E. S. Polkinghorne, *Phys. Rev. B* **71**, 165317 (2005).
- [3] A. N. Jordan and A. N. Korotkov, *Phys. Rev. B* **74**, 085307 (2006).
- [4] N. P. Oxtoby, H. M. Wiseman and He-Bi. Sun, *Phys. Rev. B* **74**, 045328 (2006).
- [5] N. P. Oxtoby, J. Gambetta and H. M. Wiseman, *Phys. Rev. B* **77**, 125304 (2008).
- [6] J. R. Petta *et al.*, *Science* **309**, 2180 (2005).
- [7] J. Gambetta, W. A. Braff, A. Wallraff, S. M. Girvin and

- R. J. Schoelkopf, *Phys. Rev. A*, **76**, 012325, (2007).
- [8] A. Kubanek, M. Koch, C. Sames, A. Ourjoumteev, P. W. H. Pinkse, K. Murr and G. Rempe, *Nature*, **462**, 898 (2009).
- [9] N. V. Morrow, S. K. Dutta, and G. Raithel, *Phys. Rev. Lett.* **88**, 093003 (2002).
- [10] T. Fischer, P. Maunz, P. W. H. Pinkse, T. Puppe, and G. Rempe, *Phys. Rev. Lett.* **88**, 163002 (2002).
- [11] M. A. Armen, J. K. Au, J. K. Stockton, A. C. Doherty, and H. Mabuchi, *Phys. Rev. Lett.*, **89**, 133602 (2002)
- [12] J. E. Reiner, W. P. Smith, L. A. Orozco, H. M. Wiseman, and J. Gambetta, *Phys. Rev. A.*, **70**, 023819, (2004)
- [13] P. Bushev, *et al.*, *Phys. Rev. Lett.* **96**, 043003 (2006).

- [14] S. Chaudhury, S. Merkel, T. Herr, A. Silberfarb, I. H. Deutsch, and P. S. Jessen, *Phys. Rev. Lett.* **99**, 163002 (2007)
- [15] R.L. Cook, P.J. Martin, and J.M. Geremia, *Nature* **446**, 774 (2007).
- [16] H. M. Wiseman and G. J. Milburn, *Quantum Measurement and control*, (CUP, Cambridge, 2010).
- [17] K. Jacobs, *Proc. SPIE-Int. Soc. Opt. Eng.* **5468**, 355 (2004).
- [18] H. M. Wiseman and L. Bouten, *Quant. Inf. Proc.* **7**, 71 (2008).
- [19] J. Combes, H. M. Wiseman, A. J. Scott, *Phys. Rev. A* **81**, 020301(R) (2010).
- [20] See, e.g. D. J. Tannor and A. Bartana, *J. Phys. Chem. A* **103**, 10359-10363 (1999); P. O. Boykin, T. Mor, V. Roychowdhury, F. Vatan, and R. Vrijen, *Proc. Natl. Acad. Sci. USA* **99**, 3388 (2002); S.E. Sklarz, D.J. Tannor and N. Khaneja, *Phys. Rev. A* **69**, 053408 (2004).
- [21] F. Verstraete, M. Wolf and J. Ignacio Cirac, *Nat. Phys.*, **5**, 633 (2009); B. Kraus *et al.*, *Phys. Rev. A*, **78**, 042307 (2008); S. G. Schirmer and Xiaoting Wang, *Phys. Rev. A* **81**, 062306 (2010).
- [22] K. Jacobs and D. Steck, *Contemp. Phys.* **47**, 279 (2006).
- [23] T. A. Brun, *Am. J. Phys.* **70**, 719 (2002).
- [24] K. Jacobs, *Stochastic Processes for Physicists* (CUP, Cambridge, 2010).
- [25] John K. Stockton, Ramon van Handel and Hideo Mabuchi, *Phys. Rev. A*, **70**, 022106 (2004).
- [26] R. van Handel, J. K. Stockton and H. Mabuchi, *IEEE Trans. on Automatic Control*, **50**, 768 (2005).
- [27] C. M. Caves and G. J. Milburn, *Phys. Rev. A* **36**, 5543 (1987).
- [28] C. A. Fuchs and K. Jacobs, *Phys. Rev. A*, **63**, 062305 (2001).
- [29] A. C. Doherty, K. Jacobs and G. Jungman, *Phys. Rev. A*, **63**, 062306 (2001).
- [30] K. Jacobs, *Phys. Rev. A* **67**, 030301(R) (2003).
- [31] J. Combes and K. Jacobs, *Phys. Rev. Lett.* **96**, 010504 (2006).
- [32] H. M. Wiseman and J. F. Ralph, *New J. Phys.*, **8**, 90 (2006).
- [33] J. F. Ralph, E. J. Griffith, C. D. Hill and T. D. Clark, *Proc. SPIE-Int. Soc. Opt. Eng.*, **6244**, 624403 (2006).
- [34] K. Jacobs, *Quantum Inf. Comput.* **7**, 127 (2007).
- [35] E. J. Griffith and C. D. Hill and J. F. Ralph and H. M. Wiseman and K. Jacobs, *Phys. Rev. B*, **75**, 014511 (2007).
- [36] C. Hill and J. Ralph, *New J. Phys.*, **9**, 151 (2007).
- [37] K. Jacobs and A. P. Lund, *Phys. Rev. Lett.*, **99**, 020501 (2007).
- [38] A. Chiruvelli and K. Jacobs, *Phys. Rev. A*, **77**, 012102, (2008).
- [39] C. Hill and J. Ralph, *Phys. Rev. A*, **77**, 014305, (2008).
- [40] A. Shabani and K. Jacobs, *Phys. Rev. Lett.*, **101**, 230403 (2008).
- [41] J. Combes, H. M. Wiseman and K. Jacobs, *Phys. Rev. Lett.*, **100**, 160503 (2008).
- [42] J. Li and K. Jacobs, *Quantum Inf. Comput.* **9**, 395 (2009).
- [43] V. P. Belavkin and A. Negretti and K. Mølmer, *Phys. Rev. A*, **79**, 022123 (2009).
- [44] K. Jacobs, *Phys. Rev. A* **72**, 044101 (2005).
- [45] H. M. Wiseman, *Quantum Semiclass. Opt.* **8**, 205 (1996).
- [46] K. Jacobs and P. L. Knight, *Phys. Rev. A*. **57**, 2301 (1998).
- [47] J. Combes and H. M. Wiseman, in preparation.
- [48] R. Ruskov, A. N. Korotkov, K. Mølmer, e-print arXiv:1006.2013 (2010).
- [49] Another natural optimization would be to minimize the average time it takes for a qubit to reach a fixed purity; for details see Refs. [32, 41].