Polarization requirements for ensemble implementations of quantum algorithms with a single-bit output

Brandon M. Anderson*
Department of Physics, University of Texas at Dallas, P.O. Box 830688, Richardson, Texas 75083, USA

David Collins†
Department of Physics, Bucknell University, Lewisburg, Pennsylvania 17837, USA
(Received 7 August 2005; published 28 October 2005)

We compare the failure probabilities of ensemble implementations of quantum algorithms which use pseudopure initial states, quantified by their polarization, to those of competing classical probabilistic algorithms. Specifically we consider a class algorithms which require only one bit to output the solution to problems. For large ensemble sizes, we present a general scheme to determine a critical polarization beneath which the quantum algorithm fails with greater probability than its classical competitor. We apply this to the Deutsch-Jozsa algorithm and show that the critical polarization is 86.6%.

DOI: 10.1103/PhysRevA.72.042337 PACS number(s): 03.67.Lx

I. INTRODUCTION

There are two general paradigms for implementing quantum algorithms [1]. In the first, the quantum algorithm is implemented on a single quantum system with the appropriate number of qubits and which can be prepared in a suitable pure state and is amenable to projective measurements. Most quantum algorithms are written with this in mind. In the second paradigm, the algorithm is implemented on an ensemble of of identical, noninteracting quantum computers. This is the situation with conventional room temperature, solution state nuclear magnetic resonance (NMR) implementations, in which case the ensemble consists of approximately 10^{20} molecules [2–8].

In ensemble implementations each ensemble member undergoes the same unitary evolution as its companions and algorithms for the two paradigms are typically most similar in this respect. However, they differ in the initialization and measurement stages. In general an ensemble quantum computer can only be prepared in a mixed state, so that the state of any single ensemble member is not known with certainty. Also, the output from an ensemble quantum computer is an average of individual ensemble member measurement outcomes. The initialization and measurement issues have led to modifications of quantum algorithms for ensemble realizations.

The conventional approach to ensemble quantum computing initializes the ensemble in a pseudopure state, for which various preparation techniques have been proposed [5,6,9–11] and which has the form

$$\hat{\rho}_i = \frac{(1-\varepsilon)}{2^n}\hat{I}^{\otimes n} + \varepsilon|\psi_i\rangle\langle\psi_i|, \tag{1}$$

where n is the number of qubits, $|\psi_i\rangle$ is a known pure state and $0 \leqslant \varepsilon \leqslant 1$ is called the *polarization*. The idea is that under the collection of unitaries required to implement a quantum algorithm, $\hat{U}_{\text{alg}}$, the density operator transforms to

$$\hat{\rho}_{\text{final}} = \frac{(1-\varepsilon)}{2^n}\hat{I}^{\otimes n} + \varepsilon\hat{U}_{\text{alg}}|\psi_i\rangle\langle\psi_i|\hat{U}_{\text{alg}}^{\dagger}$$

$$= \frac{(1-\varepsilon)}{2^n}\hat{I}^{\otimes n} + \varepsilon|\psi_{\text{final}}\rangle\langle\psi_{\text{final}}|, \tag{2}$$

where

$$|\psi_{\text{final}}\rangle := \hat{U}_{\text{alg}}|\psi_i\rangle \tag{3}$$

and this is followed by measuring the expectation value of a traceless observable. The identity component of of $\hat{\rho}_{\text{final}}$ does not contribute to this measurement outcome and it is as though the pure state algorithm represented by $|\psi_i\rangle \rightarrow \hat{U}_{\text{alg}}|\psi_i\rangle$ has been implemented.

Much of the discussion of ensemble quantum computing on pseudopure states has focused on the scaling properties of the polarization with respect to the problem's input size [12] or the presence of entanglement in these [13]. In particular, most pseudopure state preparation schemes result in polarizations which diminish exponentially as the number of qubits increases, thus resulting in exponentially decreasing output signal strength. However, a promising new approach using NMR with parahydrogen induced polarization attains high polarizations and appears to avoid these problems [14].

Here we consider how well an ensemble quantum algorithm, for a given polarization and ensemble size, performs in relation to competing classical probabilistic algorithms. We propose a criterion, considering the ensemble size as one of the resources, for which an ensemble algorithm can be compared fairly to a classical competitor. We then use this to ask, for a certain class of problems, whether there is a critical polarization below which the quantum algorithm fails with greater probability than the classical algorithm.

The remainder of this paper is organized as follows. In Sec. II we provide a general scheme for comparing the per-

*Electronic address: brandona@utdallas.edu
†Author to whom correspondence should be addressed. Electronic address: dcollins@bucknell.edu

formance of ensemble quantum algorithms to their classical counterparts. We only consider algorithms for which the output is obtained after measuring a *single qubit*. In Sec. III we apply the general scheme to the Deutsch-Jozsa algorithm determine the critical polarization below which the quantum algorithm fails with greater probability than a classical random algorithm. Finally, the appendices contain much of the mathematical derivations of various essential results.

II. PERFORMANCE OF ENSEMBLE QUANTUM ALGORITHMS VERSUS CLASSICAL PROBABILISTIC ALGORITHMS

We consider problems which take one of many possible inputs and determine into which of *two possible classes* the input falls. Any classical algorithm to solve one of these could be designed to write the output to one bit; those inputs returning "0" fall into "class 0," and those returning "1" fall into "class 1." We assume that a quantum algorithm exists, which, when applied to a collection of qubits in an appropriate pure initial state, can determine the input class with certainty. It is convenient to split the collection of qubits into a single qubit target register, on which a measurement will reveal the input type, and a remaining n-qubit argument and workspace register as may be required by the algorithm. This quantum analog proceeds as:

$$|\psi_i\rangle \xrightarrow{\hat{U}_{\text{alg}}} \begin{cases} |\phi_0\rangle_{\text{a}}|0\rangle_{\text{t}} & \text{for class 0} \\ |\phi_1\rangle_{\text{a}}|1\rangle_{\text{t}} & \text{for class 1}, \end{cases} \tag{4}$$

where the subscripts denote the argument/workspace and target registers and $|\phi_0\rangle_{\text{a}}$ and $|\phi_1\rangle_{\text{a}}$ are normalized but not necessarily orthogonal argument register states. The input class is revealed following a computational basis measurement on the target qubit.

On an ensemble quantum computer initially in the pseudopure state of Eq. (1), the typical protocol [6,15] for determining the input class is based on the expectation value for the target qubit

$$\langle \sigma_z \rangle_{\text{t}} = \begin{cases} \varepsilon & \text{for class 0} \\ -\varepsilon & \text{for class 1}. \end{cases} \tag{5}$$

This evidently allows one to distinguish the input class by "measuring an expectation value" (provided that the polarization is suitably large for detection in a particular experimental setup) and checking whether it is $+\varepsilon$ or $-\varepsilon$. However, for an ensemble with a finite number of members M and whose final state is mixed as in Eq. (4), the random nature of the target qubit measurement outcomes on individual ensemble members generates statistical fluctuations which will yield outcomes that are almost never precisely $\langle \sigma_z \rangle_{\text{t}} = \pm\varepsilon$. It is then essential to elaborate the protocol for deciding the input class, determine the probability with which this gives a correct result and compare this to a classical probabilistic algorithm which uses the same resources.

The protocol which we advocate replaces $\langle \sigma_z \rangle_{\text{t}}$ by a suitable sample average of computational basis measurement outcomes over all the ensemble members. We assume that a computational basis measurement is performed on each ensemble member and that each measurement outcome is scaled to be compatible with the eigenvalues of σ_z, i.e., let $z_j = +1$, $z_j = -1$ correspond to the outcome of the measurements associated with projectors $\hat{P}_0 = |0\rangle\langle 0|$ and $\hat{P}_1 = |1\rangle\langle 1|$, respectively. These yield a sample average

$$\bar{z} := \frac{1}{M} \sum_{i=1}^{M} z_i, \tag{6}$$

which typically approximates $\langle \sigma_z \rangle_{\text{t}}$ well as $M \to \infty$. This leads to the decision protocol

$$\bar{z} > 0 \Rightarrow \text{input is class 0},$$

$$\bar{z} = 0 \Rightarrow$$

guess the input class with probability 1/2

for either type, and

$$\bar{z} < 0 \Rightarrow \text{input is class 1}. \tag{7}$$

This amounts a majority vote on the number of individual ensemble member outcomes which are $z_j = +1$ or $z_j = -1$ or a completely unbiased guess whenever the numbers of the two outcomes are identical. Let M_+ be the number of times that that $z_i = +1$ and M_- the number of times that $z_i = -1$. It is straightforward to verify that

$$\bar{z} := \frac{\Delta M}{M},$$

where $\Delta M := M_+ - M_-$ represents the excess of positive measurement outcomes. The protocol of Eq. (7) assumes the best possible resolution in the measuring apparatus. That is, one can distinguish between $\Delta M = \pm 1$ (for M odd) or $\Delta M = -2$, 0, or 2 (for M even). We refer to this as the *best resolution case*. We shall later generalize this to arbitrary measurement resolution and demonstrate that the best resolution case is optimal.

The probability with which the quantum algorithm misidentifies the input type can be determined by considering the various routes to failure. The probability that that a class 0 input will be misidentified as class 1 will be denoted as $p_{\text{fail best 0}}$ and the probability that a class 1 input will be misidentified as class 0 as $p_{\text{fail best 1}}$. Assuming that an input is chosen from class 0 with the same probability as from class 1, the quantum failure probability is $p_{\text{fail best}}{}^{q} = (p_{\text{fail best 0}} + p_{\text{fail best 1}})/2$. Now suppose that the algorithm is run with a class 0 input. The input will be misidentified if $M_+ < M_-$ or if an incorrect class is guessed when $M_+ = M_-$. The probabilities with which these occur can be derived from those for measurement outcomes on individual ensemble members. In this case it follows from Eqs. (2) and (4) that

$$\Pr(z_i = +1) = \text{Tr}(\hat{P}_0 \hat{\rho}_{\text{final}}) = \left(\frac{1+\varepsilon}{2} \right),$$

$$\Pr(z_i=-1)=\mathrm{Tr}(\hat{P}_1\hat{\rho}_{\mathrm{final}})=\left(\frac{1-\varepsilon}{2}\right). \tag{8}$$

Similarly if the algorithm is run with a class 1 input the failure probability can be determined by switching M_+ with M_- in the conditions for misidentification and $z_i=+1$ with $z_i=-1$ in Eq. (8). The symmetry in these situations implies that $p_{\mathrm{fail\ best\ 1}}=p_{\mathrm{fail\ best\ 0}}$ and thus $p_{\mathrm{fail\ best}}{}^{q}=p_{\mathrm{fail\ best\ 0}}$. Since measurements on each ensemble member amount to a Bernoulli trial the class 0 failure probability is a cumulative binomial distribution. The precise form of this depends on whether M is even or odd. For odd M, the case $M_+=M_-$ cannot occur and

$$p_{\mathrm{fail\ best}}{}^{q}(\varepsilon,M)=\Pr(M_->M_+)=\Pr\left(M_-\geqslant\frac{M+1}{2}\right)$$
$$=\sum_{k=\frac{M+1}{2}}^{M}\binom{M}{k}\left(\frac{1-\varepsilon}{2}\right)^k\left(\frac{1+\varepsilon}{2}\right)^{M-k}, \tag{9}$$

indicating the dependence of the failure probability on polarization and ensemble size. For even M, the case $M_+=M_-$ can occur and

$$p_{\mathrm{fail\ best}}{}^{q}(\varepsilon,M)=\Pr(M_->M_+)+\frac{1}{2}\Pr(M_-=M_+)$$
$$=\Pr\left(M_-\geqslant\frac{M}{2}+1\right)+\frac{1}{2}\Pr\left(M_-=\frac{M}{2}\right)$$
$$=\sum_{k=\frac{M}{2}+1}^{M}\binom{M}{k}\left(\frac{1-\varepsilon}{2}\right)^k\left(\frac{1+\varepsilon}{2}\right)^{M-k}+\frac{1}{2}\binom{M}{M/2}\left(\frac{1-\varepsilon}{2}\right)^{M/2}\left(\frac{1+\varepsilon}{2}\right)^{M/2}. \tag{10}$$

The best resolution case assumes that the measurement apparatus allows one to distinguish between two circumstances where the values of ΔM differ by as little as 2 and thus values of $\bar{z}$ which differ by as little as $2/M$. In a *general resolution case* we assume that one can only distinguish between two situations where the values of ΔM differ by a *resolution* of at least R, which could depend on M. In the context of the protocol of Eq. (7) this means that outcomes for which $-R/2<\Delta M<R/2$ can be regarded as pure noise. The maximum magnitude of the sample average associated with this noise is $|\bar{z}|=R/2M$ and noting that the maximum sample average associated with any outcome has magnitude $|\bar{z}|=1$, the signal to noise ratio is represented by $R/2M$. This can be used as a guide to precise behavior of the resolution as a function of ensemble size, which may depend on the details of the apparatus. Regardless of these details, the decision protocol for the general resolution case is

$$\bar{z}\geqslant\frac{R}{2M}\Rightarrow\text{input is class 0},$$

$$\frac{R}{2M}>\bar{z}>-\frac{R}{2M}\Rightarrow$$

guess the input class with probability

1/2 for either type, and

$$\bar{z}\leqslant-\frac{R}{2M}\Rightarrow\text{input is class 1}. \tag{11}$$

Note that the best resolution case is represented by $R=2$. The symmetry in this protocol again results in $p_{\mathrm{fail}}{}^{q}=p_{\mathrm{fail0}}$. The class 0 input failure probabilities are more conveniently expressed in terms of M_-. To do so, note that unequivocal failure, i.e., $\bar{z}\leqslant-(R/2M)$, corresponds to $\Delta M\leqslant-\lceil R/2\rceil$ and, since $2M_-=M-\Delta M$ this is equivalent to $M_-\geqslant\lceil(M+\lceil R/2\rceil)/2\rceil$. For convenience define the minimum number of occurrences of $z_i=-1$ needed for unequivocal failure as

$$M_{\min}:=\lceil(M+\lceil R/2\rceil)/2\rceil. \tag{12}$$

Clearly $M_{\min}>M/2$. Also, it is easily shown that the ambiguous outcome $(R/2M)>\bar{z}>-(R/2M)$ is equivalent to $M_{\min}-1\geqslant M_-\geqslant M-M_{\min}+1$. Thus the quantum algorithm fails with probability

$$p_{\mathrm{fail}}{}^{q}(\varepsilon,M,M_{\min})=\Pr(M_-\geqslant M_{\min})+\frac{1}{2}\Pr(M_{\min}-1\geqslant M_-\geqslant M-M_{\min}+1)$$
$$=\frac{1}{2}[\Pr(M_-\geqslant M_{\min})+\Pr(M_-\geqslant M-M_{\min}+1)]$$
$$=\frac{1}{2}\sum_{k=M_{\min}}^{M}\binom{M}{k}\left(\frac{1-\varepsilon}{2}\right)^k\left(\frac{1+\varepsilon}{2}\right)^{M-k}+\frac{1}{2}\sum_{k=M-M_{\min}+1}^{M}\binom{M}{k}\left(\frac{1-\varepsilon}{2}\right)^k\left(\frac{1+\varepsilon}{2}\right)^{M-k}. \tag{13}$$

Several important properties of this general quantum failure probability are proved in Appendix A. First, for fixed M and $M_{\min}$, $p_{\mathrm{fail}}{}^{q}(\varepsilon,M,M_{\min})$ is a monotonically decreasing function of ε and

$$p_{\mathrm{fail}}{}^{q}(0,M,M_{\min})=\frac{1}{2}, \tag{14}$$

$$p_{\mathrm{fail}}{}^{q}(1,M,M_{\min})=0. \tag{15}$$

The former corresponds to a maximally mixed initial state, for which the algorithm produces a maximally mixed final state and any decisions about input classes amount to unbiased guesses. The latter case corresponds to a pure initial state, for which the algorithm never fails. Second, for fixed ε and M, as the resolution decreases, i.e., $M_{\min}$ increases, $p_{\mathrm{fail}}{}^{q}(\varepsilon,M,M_{\min})$ increases. Thus the best resolution case provides a lower bound on the failure probability for the quantum algorithm, as is to be expected. This bounding

property is important since it appears to be easier to arrive at certain results for the best resolution case than the general resolution case. Two important results regarding the best resolution case are also proved in Appendix A. First, if M is odd then the best resolution case failure probabilities for M and $M+1$ are equal. Second, if M is odd then the best resolution failure probability for $M+2$ is strictly less than that for M unless $\varepsilon=0$ or $\varepsilon=1$ (both statements require fixed ε). Thus, in the best resolution case at least, it is advantageous to using ensembles of increasing size.

In general there are no closed form expressions for cumulative binomial distributions of the sort encountered in Eqs. (9), (10), and (13). However, the following result due to Bahadur [16] can give good approximations, particularly for $M\to\infty$. If $0<p<1$, m and n are positive integers, and

$$B_n(m) := \sum_{k=m}^{n} \binom{n}{k} p^k (1-p)^{m-k} \tag{16}$$

then, provided that $np \leqslant m \leqslant n$,

$$A_n(m)\left[1+\frac{np(1-p)}{(m-np)^2}\right] \leqslant B_n(m) \leqslant A_n(m), \tag{17}$$

where

$$A_n(m) = \binom{n}{m} p^m (1-p)^{n-m} \frac{(m+1)(1-p)}{(m+1)-(n+1)p}. \tag{18}$$

Consider first the best resolution case, in which case it is only necessary to consider situations where M is odd. It is straightforward to verify that the conditions for Bahadur's approximation are satisfied for the cumulative binomial distribution of Eq. (9). The factor on the left side of Eq. (17) becomes

$$1+\frac{np(1-p)}{(m-np)^2} = 1+\frac{(1-\varepsilon^2)}{(1/\sqrt{M}+\sqrt{M}\varepsilon)^2} \tag{19}$$

and thus tends to 1 as $M\to\infty$ provided that $\sqrt{M}\varepsilon\to\infty$ as $M\to\infty$ (this will be shown to applicable to the Deutsch-Jozsa algorithm). In such cases the quantum error probability is well approximated by Eq. (18) after the correct substitutions for m, n, and p. Now consider the general resolution case. Bahadur's approximation applies to the first term on the right of Eq. (13) since $M_{\min} > M/2$ but in general the conditions are not satisfied for the second term on the right of Eq. (13). In other cases it is shown in Appendix A that it applies to the second term on the right of Eq. (13) when $\varepsilon \geqslant \lceil R/2 \rceil / M$. Thus provided that R scales as $R_0 M^\alpha$ where R_0 is constant and $0 \leqslant \alpha < 1$, the approximation applies for almost all ε as $M\to\infty$. The result analogous to that of Eq. (19) must be determined for each term on the right of Eq. (13). For $M \gg 1$ the first term gives

$$1+\frac{np(1-p)}{(m-np)^2} = 1+\frac{(1-\varepsilon^2)}{(\lceil R \rceil/2\sqrt{M}+\sqrt{M}\varepsilon)^2} \tag{20}$$

while for the second term it gives

$$1+\frac{np(1-p)}{(m-np)^2} = 1+\frac{(1-\varepsilon^2)}{(1/\sqrt{M}-\lceil R \rceil/2\sqrt{M}+\sqrt{M}\varepsilon)^2} \tag{21}$$

Again, these tend to 1 as as $M\to\infty$ provided that $\sqrt{M}\varepsilon\to\infty$ as $M\to\infty$ and the quantum failure probability is well approximated using Eq. (18) twice with appropriate m, n, and p.

It remains to compare the failure probability for a quantum algorithm to that for competing classical probabilistic algorithms. This is easiest for algorithms, such as the Deutsch-Jozsa algorithm or search algorithms, which solve problems with the aid of an oracle. In these the input is a function f drawn from one of two classes. The only aid allowed is an oracle which can evaluate f at any possible argument. The task is to determine the input type with the fewest oracle queries. We henceforth restrict the discussion to such oracle query algorithms. We are concerned with cases where M is very large since these are typical in NMR realizations and also the quantum failure probability in the best resolution case decreases as M increases. However, the ensemble size must be included in the count of resources and we do so by incorporating this into the total number of oracle queries (this has been used in the context of ensemble realizations of the Deutsch-Jozsa algorithm on thermal equilibrium-type states [17]). Suppose that $\hat{U}_{\text{alg}}$ invokes the oracle q times. Since $\hat{U}_{\text{alg}}$ is applied to each ensemble member, the aggregate number of oracle queries is $Q := Mq$. Thus a quantum algorithm using q queries per quantum computer operating on an ensemble with M members must be compared to a classical probabilistic algorithm which uses Q oracle queries. Denote the classical failure probability with Q oracle queries by $p_{\text{fail}}{}^{\text{q}}(Q)$. It is assumed that $p_{\text{fail}}{}^{\text{c}}(Q) \leqslant 1/2$ and that $p_{\text{fail}}{}^{\text{c}}(Q)$ decreases as Q increases. Then the critical polarization is the minimum ε required for the quantum failure probability to drop beneath the classical failure probability, is obtained by solving $p_{\text{fail}}{}^{\text{c}}(Q) = p_{\text{fail}}{}^{\text{c}}(Mq) = p_{\text{fail}}{}^{\text{q}}(\varepsilon, M, M_{\min})$ for ε. Since $p_{\text{fail}}{}^{\text{q}}(\varepsilon, M, M_{\min})$ decreases monotonically from $1/2$ to 0 with increasing ε, there will be a unique critical polarization, $\varepsilon(M)$, for each M.

The precise behavior of $\varepsilon(M)$ depends on the behavior of the ratio the quantum failure probability to the classical failure probability as a function of M as well as the behavior of the resolution as a function of M. This is somewhat simplified by considering the best resolution case since it bounds the quantum failure probability for the general resolution case from below and will provide a lower bound on $\varepsilon(M)$. Thus consider the best resolution case. If the critical polarization is bounded from below in the sense that there exists M_0 and $\varepsilon_0 > 0$ such that for $M > M_0, \varepsilon(M) \geqslant \varepsilon_0$ then the conditions for Bahadur's approximation apply and it gives (see Appendix B)

$$\varepsilon(M) = \sqrt{1-\{M[p_{\text{fail}}{}^{\text{c}}(Mq)]^2\}^{1/M}} \tag{22}$$

for large M.

For example, consider a classical probabilistic algorithm for which $p_{\text{fail}}{}^{\text{c}}(Q) = 1/c^Q$ where $c>1$. It is shown in Appendix B that if $M \geqslant 2/\log c$ then $\varepsilon \geqslant \sqrt{1-1/c^2}$. This satisfies the

conditions leading to Eq. (22) and gives a critical polarization in the best resolution case of

$$\varepsilon(M) = \sqrt{1 - \frac{1}{c^{2q}} M^{1/M}}. \tag{23}$$

In the asymptotic limit, $M^{1/M} \to 1$ as $M \to \infty$ and

$$\varepsilon(M) \to \sqrt{1 - \frac{1}{c^{2q}}}. \tag{24}$$

The general resolution case depends on the behavior of the resolution R as a function of M. However, if R scales as $R_0 M^{\alpha}$ where R_0 is constant and $0 \leqslant \alpha < 1$, then Bahadur's approximation again applies and it is straightforward to show that as $M \to \infty, M_{\min} \to M/2$ which approaches the best resolution case. It follows that Eqs. (22)–(24) apply to this situation as well.

As an aside, this method provides estimates for minimum number of oracle queries, and hence, ensemble size, required to ensure that the algorithm is successful. For fixed polarization, we require M such that

$$p_{\text{fail}}{}^{\text{c}}(Mq), p_{\text{fail}}{}^{\text{q}}(\varepsilon, M, M_{\min}) < \delta,$$

where $0 < \delta < 1$. We aim to find M as $\delta \to 0$. The quantum algorithm is most easily assessed by considering the best resolution case with M odd. If $0 < \varepsilon < 1$ the quantum failure probability decreases as M increases through successive odd values. Thus, as $\delta \to 0$, $p_{\text{fail}}{}^{\text{q}}(\varepsilon, M, M_{\min}) < \delta$ can only be satisfied by increasing M. Then, for sufficiently small δ, the arguments that lead to Eq. (B2) apply, giving

$$\sqrt{\frac{2}{\pi M}} \frac{(1+\varepsilon)}{2\varepsilon} (1 - \varepsilon^2)^{M/2} < \delta.$$

Thus the *quantum algorithm* failure probability is bounded by δ provided that

$$M > \frac{\log(1/\delta)}{|\log(1 - \varepsilon^2)|}, \tag{25}$$

where only the remaining dominant terms as $\delta \to 0$ and $M \to \infty$ have been retained and the base of the logarithms is arbitrary. When the classical algorithm satisfies $p_{\text{fail}}{}^{\text{c}}(Q) = 1/c^Q$ is is straightforward to show that the classical failure probability is bounded by δ if

$$M > \frac{\log(1/\delta)}{\log(c^q)}. \tag{26}$$

In Sec. III we shall apply our general scheme to the Deutsch-Jozsa algorithm, which can easily be modified so that the output is a single bit. Furthermore we shall show that it satisfies the requirements which lead to Eqs. (22) and (23). To date, we are unaware of any other oracle quantum algorithms, in whose typical formulations the output is a single bit. However, the problems which the other known oracle quantum algorithms solve could be modified so that the goal is to determine *just one bit of the typical output*. For the most important of these, the Grover search algorithm [18], this amounts to determining a single bit of the marked item's location. Here the classical failure probability does not obey

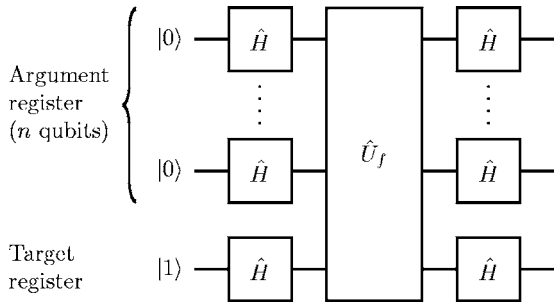

FIG. 1. Quantum circuit for the standard version of the Deutsch-Jozsa algorithm. The actions of the gates are defined in the text and the algorithm terminates with a computational basis measurement on all n control register qubits.

$p_{\text{fail}}{}^{\text{c}}(Q) = 1/c^Q$ and thus Eq. (23) will not apply. However, it is unclear whether the critical polarization is bounded from below by $\varepsilon_0 > 0$ and hence Eq. (22) applies. Nor is it obvious whether $\sqrt{M}\varepsilon \to \infty$ as $M \to \infty$ and the terms in Eqs. (19)–(21) tend to 1 as $M \to \infty$ leaving the closed form approximation for quantum failure probability of Eq. (B2). We leave the extent to which our general scheme and its sequence of approximations is applicable to Grover's and other quantum algorithms an open issue. We present it in the event that other single output quantum algorithms for which the critical polarization is bounded from below emerge.

III. EXAMPLE: THE DEUTSCH-JOZSA ALGORITHM

The Deutsch-Jozsa problem [19] considers functions $f: \{0,1\}^n \to \{0,1\}$ which are guaranteed to be either constant or balanced. A balanced function yields 0 for precisely half of the $N = 2^n$ possible arguments and 1 for the remaining half. The task is to identify the function type using the minimum number of invocations of an oracle which can evaluate $f(x)$ at any $x = 0, \ldots N-1$. The approaches for determining the function type with *certainty* are well-known [19,20]; classically, in the worst case, the function must be evaluated for $2^{n-1}+1$ different arguments; if two different inputs yield different outputs it is balanced but if all inputs return the same output it is constant.

The circuit for the standard Deutsch-Jozsa quantum algorithm is illustrated in Fig. 1 where the gate operations are defined on computational basis states as

$$\hat{H}|x\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{x \cdot y} |y\rangle \tag{27}$$

for the Hadamard gate and

$$\hat{U}_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle \tag{28}$$

for the oracle. These are extended linearly to arbitrary superpositions of quantum states.

It is straightforward to demonstrate that if f is constant then final state of the two registers is $|\psi_{\text{final}}\rangle = |0 \ldots 0\rangle |1\rangle$. while, if f is balanced, $|\psi_{\text{final}}\rangle = \Sigma_{x=1}^{N-1} \alpha_x |x\rangle |1\rangle$. Notably, for a balanced function, the state $|0 \ldots 0\rangle$ does not appear in the argument register superposition. Thus an n-qubit computa-

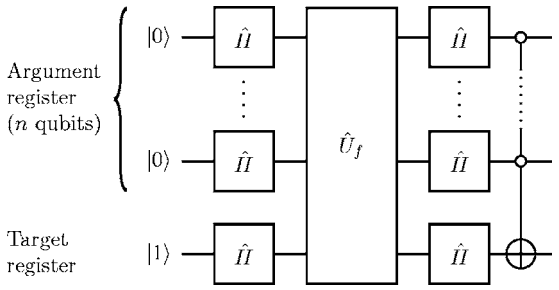

FIG. 2. Modified quantum circuit which produces a single bit output for the Deutsch-Jozsa problem. The final gate is a multiply controlled NOT which applies a NOT to the target register when every argument register qubit is in state $|0\rangle$.

tional basis measurement on the argument register reveals the function type. This quantum algorithm requires just one oracle invocation to accomplish this (giving $q=1$).

In the language developed earlier, the constant functions correspond to class 0 and balanced functions to class 1 and the algorithm should be modified so as to yield a single bit output. This is accomplished by an additional multiply controlled NOT as illustrated in Fig. 2.

If f is constant, the final state of both registers is $|\psi_{\text{final}}\rangle = |\phi_0\rangle|0\rangle$, while if f is balanced, the final state will be $|\psi_{\text{final}}\rangle = |\phi_1\rangle|1\rangle$ for some (irrelevant) $|\phi_j\rangle$. Thus a *computational basis measurement on the target qubit* reveals the function type. Note that the extra multiply controlled NOT gate can be decomposed into a sequence of $O(n^2)$ basic one and two qubit gates [21].

The framework developed earlier can be used to compare the performance of ensemble realizations of this algorithm to its classical probabilistic counterparts. The classical probabilistic algorithm proceeds by evaluating f on $M < N/2+1$ distinct arguments. If all outputs are the same f is identified as constant, whereas if two outputs differ f will be identified as balanced. This can only fail when a balanced function happens to return the same output for all M arguments. Assuming that a balanced or constant function is chosen with equal probability, it is shown in Appendix C that the probability with this occurs is well approximated by

$$p_{\text{fail}}{}^{\text{c}}(M) = \frac{1}{2^M} \tag{29}$$

provided that $M \ll N/2$.

The critical polarization is determined by solving

$$p_{\text{fail}}{}^{\text{q}}(\varepsilon, M) = \frac{1}{2^M}. \tag{30}$$

For the best resolution case, the approximation of Eq. (22) with $c=2$ gives

$$\varepsilon(M) = \sqrt{1 - \tfrac{1}{4}(M)^{1/M}}. \tag{31}$$

We note that a better approximation for intermediate ensemble sizes is

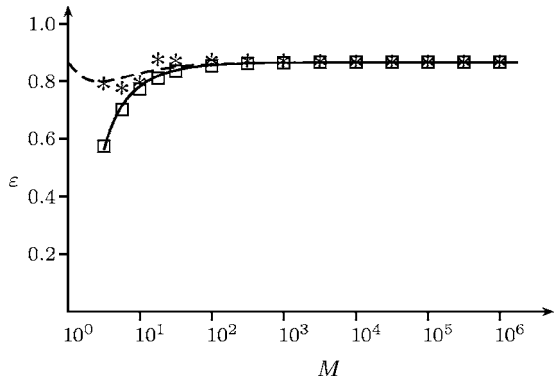

FIG. 3. Critical polarization vs ensemble size for the Deutsch-Jozsa algorithm. The solid line is generated via Eq. (32) while the dashed line is generated via Eq. (31). The squares display data obtained by solving Eq. (30) numerically for the best resolution case, while the asterisks are for a resolution $R=\sqrt{M}$.

$$\varepsilon(M) = \sqrt{1 - \tfrac{1}{4}(2.44\pi M)^{1/M}}. \tag{32}$$

These are illustrated, along with data obtained by numerically solving Eq. (30), in Fig. 3.

In the limit $M \to \infty$, Eq. (24) implies $\varepsilon \to \sqrt{3/4} = 0.866\,025$. By comparison a standard room-temperature, solution state NMR realization on 500 MHz spectrometer, using pulsed pseudopure preparation schemes [6,22,23] typically has $\varepsilon \lesssim 10^{-5}$. A more promising but more complicated method [14] using parahydrogen induced polarization to produce a two qubit ensemble quantum computer has attained $\varepsilon = 0.9$. It should be noted that, to date, all NMR realizations of the Deutsch-Jozsa algorithm [4,24–30] have had $n \leqslant 5$ and $M \sim 10^{20} \gg N/2$ and, by our criteria, a classical algorithm with comparable resources would determine the function type with certainty and thus outperform these realizations.

IV. CONCLUSION

In conclusion, we have provided a method for comparing the performance of ensemble versions of quantum algorithms whose output is extracted from a measurement on a single qubit to their classical probabilistic counterparts. We have applied this to realizations of the Deutsch-Jozsa algorithm and calculated the minimum polarization required for the quantum algorithm to outperform the classical probabilistic algorithm. Our calculations indicate that the standard room temperature solution state NMR approach attains polarizations several orders of magnitude too small but that newer approaches using parahydrogen induced polarization attain suitable polarizations for the ensemble quantum computer to outperform the classical probabilistic algorithm.

ACKNOWLEDGMENT

This work was supported by NSF REU Grant No. PHY-0097424.

APPENDIX A: QUANTUM FAILURE PROBABILITY

The following useful representation of cumulative binomial distributions [31] can be verified by repeated integration by parts:

$$B_n(m) := \sum_{k=m}^{n} \binom{n}{k} p^k (1-p)^{n-k} = I_p(m, n-m+1), \quad \text{(A1)}$$

where $I_p(x,y)$ is the incomplete beta function defined by

$$I_p(x,y) := \frac{\Gamma(x+y)}{\Gamma(x)\Gamma(y)} \int_0^p t^{x-1}(1-t)^{y-1}\, dx. \quad \text{(A2)}$$

1. Behavior with respect to ε

It is trivial to show by direct substitution that $p_{\text{fail}}^{\text{q}}(1,M,M_{\min})=0$. Now consider

$$\begin{aligned} p_{\text{fail}}^{\text{q}}(0,M,M_{\min}) &= \frac{1}{2}\sum_{k=M_{\min}}^{M} \binom{M}{k}\left(\frac{1}{2}\right)^k\left(\frac{1}{2}\right)^{M-k} \\ &\quad + \frac{1}{2}\sum_{k=M-M_{\min}+1}^{M} \binom{M}{k}\left(\frac{1}{2}\right)^k\left(\frac{1}{2}\right)^{M-k} \\ &= \frac{1}{2^{M+1}}\sum_{k=M_{\min}}^{M} \binom{M}{k} + \frac{1}{2^{M+1}}\sum_{k=M-M_{\min}+1}^{M} \binom{M}{k} \end{aligned}$$

and, since $M_{\min} > M/2$,

$$p_{\text{fail}}^{\text{q}}(0,M,M_{\min}) = \frac{1}{2^M}\sum_{k=M_{\min}}^{M} \binom{M}{k} + \frac{1}{2^{M+1}}\sum_{k=M-M_{\min}+1}^{M_{\min}-1} \binom{M}{k}.$$

It is straightforward to show that

$$\sum_{k=M-M_{\min}+1}^{M_{\min}-1} \binom{M}{k} = 2\sum_{k=\lfloor (M+1)/2 \rfloor}^{M_{\min}-1} \binom{M}{k}$$

and thus

$$p_{\text{fail}}^{\text{q}}(0,M,M_{\min}) = \frac{1}{2^M}\sum_{k=\lfloor (M+1)/2 \rfloor}^{M} \binom{M}{k} = \frac{1}{2}. \quad \text{(A3)}$$

Now consider the behavior as ε increases. We show that

$$\frac{\partial p_{\text{fail}}^{\text{q}}(\varepsilon,M,M_{\min})}{\partial \varepsilon} < 0 \quad \text{(A4)}$$

for $0<\varepsilon<1$. To prove this, note that derivatives of cumulative binomial distributions are easily computed using Eqs. (A1) and (A2),

$$\begin{aligned} \frac{\partial B_n(m)}{\partial p} &= \frac{\partial}{\partial p} I_p(m, n-m+1) \\ &= \frac{\Gamma(n+1)}{\Gamma(m)\Gamma(n-m+1)} p^{m-1}(1-p)^{n-m} > 0 \end{aligned}$$

provided that $0<p<1$. Equation (13) shows that the quantum failure probability is just the sum of two positively weighted cumulative binomial distributions with $p=(1-\varepsilon)/2$, and applying the chain rule proves the result.

2. Behavior with respect to $M_{\min}$

We show that, for any fixed ε and M,

$$p_{\text{fail}}^{\text{q}}(\varepsilon,M,M_{\min}+1) \geqslant p_{\text{fail}}^{\text{q}}(\varepsilon,M,M_{\min}) \quad \text{(A5)}$$

provided that $M/2 < M_{\min} \leqslant M-1$. Let

$$\Delta p_M := p_{\text{fail}}^{\text{q}}(\varepsilon,M,M_{\min}+1) - p_{\text{fail}}^{\text{q}}(\varepsilon,M,M_{\min}).$$

Then

$$\begin{aligned} \Delta p_M &= \frac{1}{2}\left\{ \sum_{k=M_{\min}+1}^{M} \binom{M}{k}\left(\frac{1-\varepsilon}{2}\right)^k\left(\frac{1+\varepsilon}{2}\right)^{M-k} \right. \\ &\quad \left. - \sum_{k=M_{\min}}^{M} \binom{M}{k}\left(\frac{1-\varepsilon}{2}\right)^k\left(\frac{1+\varepsilon}{2}\right)^{M-k} \right\} \\ &\quad + \frac{1}{2}\left\{ \sum_{k=M-M_{\min}}^{M} \binom{M}{k}\left(\frac{1-\varepsilon}{2}\right)^k\left(\frac{1+\varepsilon}{2}\right)^{M-k} \right. \\ &\quad \left. - \sum_{k=M-M_{\min}+1}^{M} \binom{M}{k}\left(\frac{1-\varepsilon}{2}\right)^k\left(\frac{1+\varepsilon}{2}\right)^{M-k} \right\} \end{aligned}$$

and only one term within each bracket remains, giving

$$\begin{aligned} \Delta p_M &= -\frac{1}{2}\binom{M}{M_{\min}}\left(\frac{1-\varepsilon}{2}\right)^M\left(\frac{1+\varepsilon}{2}\right)^{M-M_{\min}} + \frac{1}{2}\binom{M}{M-M_{\min}} \\ &\quad \times \left(\frac{1-\varepsilon}{2}\right)^{M-M_{\min}}\left(\frac{1+\varepsilon}{2}\right)^M \\ &= \frac{1}{2}\binom{M}{M_{\min}}\left(\frac{1-\varepsilon}{2}\right)^{M-M_{\min}}\left(\frac{1+\varepsilon}{2}\right)^{M-M_{\min}} \\ &\quad \times \left\{ \left(\frac{1+\varepsilon}{2}\right)^{M_{\min}} - \left(\frac{1-\varepsilon}{2}\right)^{M_{\min}} \right\}. \end{aligned}$$

Since $0 \leqslant \varepsilon \leqslant 1$, the term between brackets is positive. This proves the result.

3. Best resolution case behavior with respect to M

Consider the quantum failure probability for the best resolution case when M is odd. We show that the quantum failure probability remains constant if one additional ensemble member is added

$$p_{\text{fail best}}^{\text{q}}(\varepsilon,M+1) = p_{\text{fail best}}^{\text{q}}(\varepsilon,M). \quad \text{(A6)}$$

Let

$$\Delta p_M := p_{\text{fail best}}^{\text{q}}(\varepsilon,M+1) - p_{\text{fail best}}^{\text{q}}(\varepsilon,M).$$

Then Eqs. (9), (10), and (A1) imply, with $p := (1-\varepsilon)/2$,

$$\begin{aligned} \Delta p_M &= \frac{1}{2} I_p\left(\frac{M+1}{2}, \frac{M+1}{2}+1\right) + \frac{1}{2} I_p\left(\frac{M+1}{2}+1, \frac{M+1}{2}\right) \\ &\quad - I_p\left(\frac{M+1}{2}, \frac{M+1}{2}\right) \\ &= 0 \end{aligned} \quad \text{(A7)}$$

since $I_p(x+1,x)+I_p(x,x+1)=2I_p(x,x)$. This proves the result.

Now consider passing from M to $M+2$. We show that, for the best resolution case and M odd

$$p_{\text{fail best}}{}^{\text{q}}(\varepsilon,M+2) \leqslant p_{\text{fail best}}{}^{\text{q}}(\varepsilon,M), \tag{A8}$$

with equality only when $\varepsilon=0$ or $\varepsilon=1$. Let

$$\Delta p_M := p_{\text{fail best}}{}^{\text{q}}(\varepsilon,M+2) - p_{\text{fail best}}{}^{\text{q}}(\varepsilon,M).$$

Then Eqs. (9) and (A1) imply, with $p := (1-\varepsilon)/2$,

$$\begin{aligned}\Delta p_M(p) &= I_p\left(\frac{M+1}{2}+1,\frac{M+1}{2}+1\right)+I_p\left(\frac{M+1}{2}+1,\frac{M+1}{2}\right)\\ &= \binom{M}{\frac{M+1}{2}}\int_0^p t^{(M-1)/2}(1-t)^{(M-1)/2}\\ &\quad\times\left[2t(1-t)(M+2)-\frac{M+1}{2}\right]\mathrm{d}t.\end{aligned}$$

Now consider

$$g(p) := -\binom{M}{\frac{M+1}{2}}(1-2p)p^{(M+1)/2}(1-p)^{(M+1)/2}.$$

It is straightforward to show that

$$\frac{dg}{dp}=\frac{d\Delta p_M}{dp}$$

and that $g(0)=\Delta p_M(0)$. Since both functions are continuous it follows that they are identical,

$$\Delta p_M = -\binom{M}{\frac{M+1}{2}}(1-2p)p^{(M+1)/2}(1-p)^{(M+1)/2}.$$

However, $0<p<1/2$ for $0<\varepsilon<1$, and thus $\Delta p_M<0$. For $\varepsilon=0$ and $\varepsilon=1$, corresponding to $p=1/2$ and $p=0$ respectively, $\Delta p_M=0$. This proves the result.

APPENDIX B: QUANTUM FAILURE PROBABILITY VERSUS CLASSICAL FAILURE PROBABILITY

1. Applying Bahadur's approximation

Consider a circumstance where it is known that there exist a positive integer M_0 and $\varepsilon_0>0$ such that for $M>M_0, \varepsilon(M)\geqslant\varepsilon_0$ and where the resolution scales as R_0M^α where $R_0>0$ is constant and $0\leqslant\alpha<1$. Then $\sqrt{M}\varepsilon\to\infty$ as $M\to\infty$. Thus the term

$$1+\frac{np(1-p)}{(m-np)^2}$$

in Eqs. (19)–(21) tends to 1 as $M\to\infty$. It remains to approximate $A_n(m)$ in Eq. (18). Clearly for the resolution which scales as described above, $M_{\min}\approx M/2$ if $M\gg 1$ and Eq. (13) implies

$$\begin{aligned}p_{\text{fail}}{}^{\text{q}}(\varepsilon,M,M_{\min}) &\simeq \tfrac{1}{2}A_M(M/2)+\tfrac{1}{2}A_M((M+1)/2)\\ &\simeq A_M(M/2).\end{aligned}$$

For $M\gg 1$ this gives

$$\begin{aligned}p_{\text{fail}}{}^{\text{q}}(\varepsilon,M,M_{\min}) &\simeq \binom{M}{M/2}\left(\frac{1-\varepsilon}{2}\right)^{M/2}\left(\frac{1+\varepsilon}{2}\right)^{M/2}\\ &\quad\times\frac{(M/2+1)(1+\varepsilon)/2}{(M/2+1)-(M+1)(1-\varepsilon)/2}\\ &\simeq \binom{M}{M/2}\frac{(1-\varepsilon^2)^{M/2}}{2^M}\frac{(1+\varepsilon)}{2\varepsilon}.\end{aligned} \tag{B1}$$

The binomial coefficient can be approximated using Stirling's formula

$$n!\simeq\sqrt{2\pi n}n^ne^{-n}$$

for $n\gg 1$. Thus

$$\binom{M}{M/2}=\frac{M!}{(M/2)!(M/2)!}\simeq\frac{\sqrt{2\pi M}}{\pi M}\frac{M^M}{(M/2)^M}=\sqrt{\frac{2}{\pi M}}2^M,$$

giving

$$p_{\text{fail}}{}^{\text{q}}(\varepsilon,M,M_{\min})\simeq\sqrt{\frac{2}{\pi M}}\frac{(1+\varepsilon)}{2\varepsilon}(1-\varepsilon^2)^{M/2}. \tag{B2}$$

The critical polarization is determined by $p_{\text{fail}}{}^{\text{q}}(\varepsilon,M,M_{\min})=p_{\text{fail}}{}^{\text{c}}(Mq)$ and this yields

$$1-\varepsilon^2=\left[p_{\text{fail}}{}^{\text{c}}(Mq)\sqrt{2\pi M}\frac{\varepsilon}{1+\varepsilon}\right]^{2/M}. \tag{B3}$$

Now consider $M\gg 1$. Since we have assumed that $\varepsilon(M)\geqslant\varepsilon_0\neq 0$, the factors on the right which are constants or contain ε are approximately 1. Thus

$$\varepsilon^2=1-[p_{\text{fail}}{}^{\text{c}}(Mq)\sqrt{M}]^{2/M},$$

giving Eq. (22).

Note that this can be improved for intermediate sized M by retaining the factor of $\sqrt{2\pi}$ in Eq. (B3). However, we found an even better approximation for the case of the Deutsch-Jozsa algorithm by solving numerically for $\varepsilon(M)$ for small M and substituting in to the last fraction on the first line of Eq. (B1). This explains Eq. (32).

2. Exponential classical failure probability

Consider the case $p_{\text{fail}}{}^{\text{c}}(Q)=1/c^Q$ where $c>1$ and $Q=Mq$ is the total number of oracle queries over the entire ensemble. We shall prove that there exist a positive integer M_0 and $\varepsilon_0>0$ such that for $M>M_0$, $\varepsilon(M)\geqslant\varepsilon_0$. The strategy is to consider the ratio of the best resolution case quantum failure probability to the classical failure probability

$$p_{\text{fail ratio}}(\varepsilon,M) := \frac{p_{\text{fail best}}{}^{\text{q}}(\varepsilon,M)}{p_{\text{fail}}{}^{\text{c}}(Mq)},$$

and to show that for some M_0 and $\varepsilon_0>0, p_{\text{fail ratio}}(\varepsilon,M)>1$ when $M>M_0$ and $\varepsilon_0>\varepsilon$. This establishes that the critical

polarization, for which $p_{\text{fail ratio}}(\varepsilon,M)=1$, is bounded from below by ε_0 and this applies regardless of the resolution, since the best resolution case provides a lower bound for polarization.

The crux is to establish that for sufficiently small ε, $p_{\text{fail ratio}}(\varepsilon,M)$ increases as M increases. Note that for odd M, $p_{\text{fail ratio}}(\varepsilon,M+1)>p_{\text{fail ratio}}(\varepsilon,M)$ for any ε since the best resolution case quantum failure probability remains constant while the classical failure probability decreases. Thus consider

$$\Delta p(\varepsilon,M) \coloneqq p_{\text{fail ratio}}(\varepsilon,M+2)-p_{\text{fail ratio}}(\varepsilon,M)$$

for odd M. Then using Eq. (A1) with $p\coloneqq(1-\varepsilon)/2$,

$$\begin{aligned}\Delta p(\varepsilon,M) &= c^{qM}\left[c^{2q}I_p\left(\frac{M+1}{2}+1,\frac{M+1}{2}+1\right)\right.\\ &\quad\left.-I_p\left(\frac{M+1}{2},\frac{M+1}{2}\right)\right]\\ &= c^{qM}\binom{M}{\frac{M+1}{2}}\int_0^p [t(1-t)]^{(M-1)/2}\\ &\quad\times\left[2t(t-1)(M+2)c^{2q}-\frac{M+1}{2}\right]\mathrm{d}t.\end{aligned}$$

Then

$$\begin{aligned}\frac{\partial\Delta p}{\partial\varepsilon} &= -\binom{M}{\frac{M+1}{2}}\frac{c^{qM}}{2^M}(1-\varepsilon^2)^{(M-1)/2}\\ &\quad\times[(1-\varepsilon^2)(M+2)c^{2q}-(M+1)]\end{aligned}$$

which is negative if

$$\varepsilon<\sqrt{1-\frac{M+1}{M+2}c^{-2q}}. \tag{B4}$$

Since the right hand side of Eq. (B4) increases as M increases, $(\partial\Delta p/\partial\varepsilon)<0$ when $\varepsilon<\sqrt{1-2c^{-2q}/3}$.

Now consider $p_{\text{fail ratio}}(0,M)=c^{qM}/2$. Then $p_{\text{fail ratio}}(0,M)>1$ when $M>M_0\coloneqq\lceil\log 2/q\log c\rceil\geqslant 1$. But there is some polarization $\varepsilon'>0$ such that $p_{\text{fail ratio}}(\varepsilon',M_0)=1$. Then choosing $\varepsilon_0=\min\{\varepsilon',\sqrt{1-2c^{-2q}/3}\}\neq 0$ (note that this is independent of M) implies that $p_{\text{fail ratio}}(\varepsilon,M)>1$ for $M>M_0$ and $\varepsilon<\varepsilon_0$. Finally this implies that $\varepsilon(M)\geqslant\varepsilon_0\neq 0$ for $M>M_0$.

APPENDIX C: CLASSICAL FAILURE PROBABILITY FOR THE DEUTSCH-JOZSA PROBLEM

In the classical probabilistic algorithm, f is evaluated on $M\leqslant N/2$ arguments. The algorithm fails when a balanced function yields M identical outputs. If the choice of balanced functions is unbiased, then the probability with which this occurs is the number of balanced functions for which the first M arguments all return the same result divided by the total number of balanced functions. The number of balanced functions which return 0 (or equivalently 1) for the first M arguments is $\binom{N-M}{N/2-M}$ and the total number of balanced functions is $\binom{M}{M/2}$. Thus the probability of misidentifying a balanced function is $2\binom{N-M}{N/2-M}\Big/\binom{N}{N/2}$ where the factor of 2 counts both the cases which output 0 and those that output 1. For $N\gg 2M$, this can be approximated using Stirling's formula. Thus the classical failure probability is

$$\begin{aligned}\binom{N-M}{N/2-M}\Big/\binom{N}{N/2} &= \frac{(N-M)!(N/2)!}{N!(N/2-M)!}\\ &\simeq \sqrt{\frac{(N-M)N/2}{N(N/2-M)}}\left(\frac{N/2-M}{N-M}\right)^M\\ &\quad\times\left[\frac{(N-M)(N/2)}{(N/2-M)N}\right]^{NM\ll N/2}\to\frac{1}{2^M}.\end{aligned} \tag{C1}$$

Thus the classical failure probability tends to $p_{\text{bal}}2/2^M$ where p_{bal} is the probability with which a balanced function (versus a constant function) is chosen. In the unbiased case considered in this paper, $p_{\text{bal}}=1/2$. Thus the classical failure probability is well approximated by $1/2^M$ provided that $M\ll N/2$.

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

[2] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, R. Cleve, and I. L. Chuang, Nature **414**, 883 (2001).

[3] L. M. K. Vandersypen, M. Steffen, M. H. Sherwood, C. S. Yannoni, G. Breyta, and I. L. Chuang, Appl. Phys. Lett. **76**, 646 (2000).

[4] R. Marx, A. F. Fahmy, J. M. Myers, W. Bermel, and S. J. Glaser, Phys. Rev. A **62**, 012310 (2000).

[5] D. G. Cory, M. D. Price, and T. F. Havel, Physica D **120**, 82 (1998).

[6] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung, Proc. R. Soc. London, Ser. A **454**, 447 (1998).

[7] D. G. Cory, A. F. Fahmy, and T. F. Havel, Proc. Natl. Acad. Sci. U.S.A. **94**, 1634 (1997).

[8] N. A. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).

[9] L. J. Schulman and U. Vazirani, *Proc. 31st ACM Symposium on Theory of Computing 1999*, p. 322

[10] I. L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998).

[11] E. Knill, I. Chuang, and R. Laflamme, Phys. Rev. A **57**, 3348 (1997).

[12] W. S. Warren, Science **277**, 1688 (1997).

[13] R. Schack and C. M. Caves, Phys. Rev. A **60**, 4354 (1999).

[14] M. S. Anwar, D. Blazina, H. A. Carteret, S. B. Duckett, T. K. Halstead, J. A. Jones, C. M. Kozak, and R. J. K. Taylor, Phys. Rev. Lett. **93**, 040501 (2004).

[15] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[16] R. R. Bahadur, Ann. Math. Stat. **31**, 43 (1960).
[17] Arvind and D. Collins, Phys. Rev. A **68**, 052301 (2003).
[18] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[19] D. Deutsch and R. Jozsa, Proc. R. Soc. London, Ser. A **439**, 553 (1992).
[20] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. London, Ser. A **454**, 339 (1998).
[21] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1975).
[22] J. A. Jones, Fortschr. Phys. **48**, 909 (2000).
[23] R. Laflamme, D. G. Cory, C. Negrevergne, and L. Viola, Quantum Inf. Comput. **2**, 166 (2001).
[24] V. L. Ermakov and B. M. Fung, J. Chem. Phys. **118**, 10376 (2003).
[25] D. Collins, K. W. Kim, W. C. Holton, H. Sierzputowska-Gracz, and E. O. Stejskal, Phys. Rev. A **62**, 022304 (2000).
[26] K. Dorai, Arvind, and A. Kumar, Phys. Rev. A **61**, 042306 (2000).
[27] J. Kim, J.-S. Lee, S. Lee, and C. Cheong, Phys. Rev. A **62**, 022312 (2000).
[28] N. Linden, H. Barjat, and R. Freeman, Chem. Phys. Lett. **296**, 61 (1998).
[29] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung, and S. Lloyd, Nature **393**, 143 (1998).
[30] J. A. Jones, M. Mosca, and R. H. Hansen, Nature **399**, 344 (1998).
[31] N. L. Johnson, S. Kotz, and A. W. Kemp, *Univariate Discrete Distributions* (Wiley, New York, 1992).