International Journal of Quantum Information
Vol. 5, No. 4 (2007) 627–640

GENERAL CIRCUITS FOR INDIRECTING AND DISTRIBUTING MEASUREMENT IN QUANTUM COMPUTATION

M. GUPTA*, A. PATHAK*,¶, R. SRIKANTH†,‡ and P. K. PANIGRAHI§

*Jaypee Institute of Information Technology, Noida 201 307, India

†Poornaprajna Institute of Scientific Research, Devanahalli, Bangalore 562 110, India

‡Raman Research Institute, Sadashiva Nagar, Bangalore 560 012, India

§Physical Research Laboratory, Navrangpura, Ahmedabad 380 009, India

¶anirban.pathak@jiit.ac.in

†srik@rri.res.in

§prasanta@prl.ernet.in

Received 9 July 2007

A question of theoretical and practical interest is how a quantum system may be measured indirectly by means of an ancilla that interacts with it, and furthermore, how a system of ancillas may be used to implement a coherent measurement of spatially separated qudits. We provide general circuits that can be used to implement such measurements. These circuits are relevant to quantum error correction, measurement-based quantum computation and Bell state discrimination across a quantum network involving multiple parties. The last mentioned problem is treated in detail. Our circuitry can also help to optimize the quantum communication complexity for performing measurements in distributed quantum computing.

Keywords: Entanglement; quantum computation; quantum communication.

PACS Number(s): 03.67.Hk, 03.67.Mn

1. Introduction

Entangled states play a key role in the transmission and processing of quantum information.[1,2] Using an entanglement channel,[3] an unknown state can be teleported[4] with local unitary operations, appropriate measurement and classical communication; one can achieve entanglement swapping through joint measurement on two entangled pairs.[5] Entanglement leads to an increase in the capacity of the quantum information channel, by means of quantum dense coding.[6] The bipartite, maximally entangled Bell states provide the most transparent illustration of these aspects, although three-particle entangled states like GHZ and W states are beginning to be employed for various purposes.[7,8] Nonorthogonal states cannot be discriminated with certainty,[9] while the discrimination of orthogonal states are possible in principle. A large number of results regarding locally [i.e. via local operations and classical communication (LOCC)] distinguishing various orthogonal states shared between two distant parties, have recently been established.[10–15]

In contrast to the above works, which are concerned with *local* distinguishability of one or more copies of orthogonal states, in the present work, we study the related but quite different and less restricted problem of implementing measurements on multi-qudit states across a quantum network in which quantum communication of ancillary qubits is allowed. Our goal is to obtain (efficient) circuits for such a *distribution of measurement*. Except for some basic similarity, our proposed task is quite different from that of local distinguishability in several ways: (1) in our task, quantum communication is permitted; (2) as a direct consequence, our results always require only a single copy of the measured state. In contrast, local distinguishability results depend on the number of states to be distinguished and copies thereof. For example, if only one copy of one of two Bell states is given, it can be identified,[10] but not if any of the four Bell states are admissible; (3) as another direct consquence of (1), our method of measurement is always non-destructive, i.e. if the measured state is one of the orthogonal states to be discriminated, then it is not destroyed. In contrast, local distinguishability necessarily consumes an identified Bell state. Of course, the outcome of this task can be used to locally recreate the identified Bell state, provided pre-shared entanglement is available. However, this is essentially a destroy-recreate method, which is not non-destructive; (4) the multi-qudit measurement we implement is always incomplete, i.e. it distinguishes between classes of orthogonal basis states in a given basis, rather than all the basis states. (However, these measurements are non-destructive, so that repeated measurements may be made to effectively implement a complete measurement, such as distinguishing the full set of n-qudit Bell states.)

It may be noted that our use of quantum communication can be replaced by that of priorly shared entanglement. Each instance of transmission of a qudit is then substituted by teleportation by consuming the entanglement.

If quantum communication is allowed, obviously the direct method for implementing a multi-qubit measurement is to bring the qudits together for joint measurement, and then redistribute them.[16–20] Alternatively, they may be separately brought into interaction with a common ancilla, which is then measured to obtain the relevant information. We will be concerned with the latter sort of indirect, ancilla-mediated measurement circuits.

This work presents a general strategy for obtaining circuits which indirectly distribute measurement. The basic theory underlying our circuits is presented in Sec. 2. In particular, our method is used in Sec. 4 to implement *incomplete* measurements, which are useful in quantum error correction,[23,24] measurement-based quantum computation[28–35] and Bell-state discrimination.[21] In generalizing the latter work, we introduce a new kind of generalized Bell states, and provide circuits that distribute their discrimination. In Sec. 5, we point out that our circuits can also lead to lower quantum communication complexity in distributed computing. Finally, we conclude with Sec. 6.

2. Indirecting Quantum Measurement

Suppose we wish to measure observable W on system A, which is difficult to measure, but couples well with another system B that is amenable to easier measurement. System B is measured in a suitable basis W_B, the output of which should indicate the result of indirectly measuring W on A. In our case, we choose W_B to be the computational basis always. An experimental situation of this kind is presented in Ref. 39. We desire a method whereby B can be used as an ancilla through which W is measured indirectly on A. To this end, we require that the two systems be evolved together according to a suitable two-particle unitary operation V, followed by a measurement on ancilla B in the computational basis. If the system A is in an eigenstate of W, then the indirect measurement should of course not destroy the state. In our terminology, we say that the measurement of W on A is *indirected* or delegated to ancilla B.

We now present a method of constructing V given W. For the special case where W is a qubit observable with eigenvalues ± 1, cf. Fig. 10.13, Ref. 1, where V is given by a controlled-W operation, with B serving as control qubit and A as the target qubit. Our first result, Theorem 1, is that given observable W, its measurement can be indirected by means of a controlled-U interaction, where U is an operator compatible with W, i.e. $[W, U] = 0$. If, further, U and W also share the degenerate eigenspaces, if any, then we can write $W = g(U)$, where g is in general a complex valued function. The operators U and W satisfying this stronger condition are said to be functionally compatible. Throughout the present work, the symbols I, X, Y and Z denote the Pauli operators.

Theorem 1. *Given observable W for a system and a unitary operator U functionally compatible with it, measurement of W can be indirected to an ancilla using the control-operation given by $\mathcal{C}_U \equiv \sum_j |j\rangle\langle j| \otimes U^j$, where the ancilla serves as the control-particle.*

Proof. The unitary operator can in general be written in its diagonal basis by $U = \sum_{j,k} e^{2\pi\iota j/d}|j;k\rangle\langle j;k|$ $(0 \leq j \leq d-1)$, where index k accounts for degeneracy, and is dropped in the absence of degeneracy. The observable compatible with it is designated to be $W = \sum_{j,k} f(j)|j;k\rangle\langle j;k|$, where $f(\cdot)$ is any real-valued function. We observe that U and W are not only compatible, but must share their degenerate subspaces. The state to be measured is some $|\Psi\rangle = \sum_{k,l} \alpha_{k,l}|k;l\rangle$ entering the upper wire in Fig. 1(a). At stage 1, the state of the ancilla-system complex is $d^{-1/2}\sum_{j,k,l} \alpha_{k,l}|j\rangle_a|k;l\rangle_s$, where the first ket denotes the ancilla, the second denotes the principal system (the subscripts are dropped whenever there is no danger of confusion). Via action of the controlled-U gate, in stage 2, the state of the complex is $d^{-1/2}\sum_{j,k,l} \alpha_k e^{2\pi\iota jk/d}|j\rangle_a|k;l\rangle_s$. At stage 3, by the action of $H_d^\dagger$, the above state is transformed to $d^{-1/2}\sum_{j,k,l,m} \alpha_k e^{(2\pi\iota j/d)(k-m)}|m\rangle_a|k;l\rangle_s = \sum_{k,l} \alpha_{k;l}|k\rangle_a|k;l\rangle_s$ since the summation over j is non-vanishing only when $k = m$. Therefore, a measurement

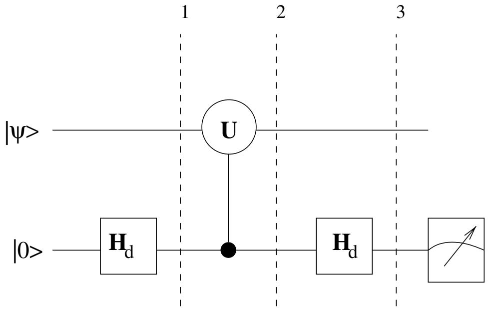

Fig. 1. Circuit for indirecting measurement from a principal system to an ancilla. The upper wire denotes an arbitrary system, on which measurement of W is indirectly performed by means of an ancilla (lower wire). The circle-link represents the generalized controlled-U operation $\mathcal{C}_U$.

on the ancilla in the computational basis $\{|j\rangle\}$ is equivalent to a measurement of observable W on the system. □

Some points worth noting are: if the system was initially in an eigenstate of W, the indirect measurement is nondestructive, and the state remains available for future use. If W (and hence U) is degenerate, then the measurement is incomplete, i.e. the measurement projectors, given by $\Pi_j \equiv \sum_k |j,k\rangle\langle j,k|$, are of dimension greater than one.

3. Distributing Quantum Measurement

A direct measurement (i.e. one not mediated by an ancilla) of a multipartite observable, whose eigenstates are in general entangled, cannot be performed except by bringing together all the qudits and measuring them jointly (otherwise, the no-signalling condition would be violated). In this sense, a direct measurement on a multipartite system cannot in general be *distributed*. In contrast, the indirect measurement described in the preceding section may be distributed as follows. The ancilla interacts separately first with one qudit. It is then quantum communicated to another system qudit, with which it interacts, and so forth, for any other possible system qudits. Finally, the ancillary qudit is measured in a suitable basis W_B, the output of which should indicate the result of measuring the corresponding multiparticle observable on the qudits. In our case, we choose W_B to be the computational basis always.

A sufficient condition for the distributability of (indirect) measurement is that the operator U is a tensor product of unitary qudit operators, e.g. $X \otimes X \otimes Z$ or $X \otimes Y$, etc. In this case, the control-operation is obtained by replacing each of the operators in the product by the corresponding control-operation. In other words, the control-U of Theorem 1 can be broken up into a set of control-gates acting pairwise on each system qudit from a common ancillary qudit, before the ancilla is finally measured. This is the feature that enables distribution of the measurement.

The indirect measurement so effected is necessarily *incomplete*, and the corresponding observable W is necessarily incomplete/degenerate, because the measured n-qudit system is of dimension d^n $(n \geq 2)$, whereas the ancilla is only d-dimensional. Therefore, if the required measurement is *complete*, we must be able to express it as a set of incomplete measurements that are distributable in the above sense. The next section gives an example where in a complete Bell state, discrimination is obtained by a set of incomplete, distributed measurements which yield parity and phase information.

Our method of distribution is stated more clearly in Theorem 2.

Theorem 2. *Let U be a unitary operator compatible with degenerate observable W, such that $U = \bigotimes_m U_m$, where m $(= 1, 2, \ldots, n)$ labels subsystems. The indirect measurement of W can be distributed by means of separate controlled operations on the individual subsystems j from the same ancilla. The control-operations may be performed in any order* [*e.g. Fig.* 2(*a*)] *or grouped together* [*e.g.* 2(*b*)].

Proof. From Theorem 1, the required controlled operation is $\mathcal{C}_U = \sum_j |j\rangle\langle j| \otimes U^j = \sum_j |j\rangle\langle j| \bigotimes_m (U_m)^j$. Thus, the controlled operation can be broken up into single-qudit controlled operations with n target qudits interacting with a single control qudit action. We will call this type 1 decomposition (cf. Fig. 2(a) for the case $n = 4$). Further, the last expression above can be written as $(\sum_j |j\rangle\langle j| \otimes (U_1)^j \otimes \mathbb{I}^{\otimes(n-1)})(\sum_{j'} |j'\rangle\langle j'| \otimes \mathbb{I} \otimes (U_2)^{j'} \otimes \mathbb{I}^{\otimes(n-2)}) \cdots (\sum_{j''} |j''\rangle\langle j'| \otimes \mathbb{I}^{\otimes(n-1)} (U_n)^{j''})$. Therefore $\mathcal{C}_U = \mathcal{C}_{U_1} \times \mathcal{C}_{U_2} \times \cdots \mathcal{C}_{U_m}$, where $\mathcal{C}_{U_k} \equiv \sum |j\rangle\langle j| \otimes (U_k)^j$. Since the $\mathcal{C}_{U_j}$'s commute with each other, they may be performed in any order. This is type 2 decomposition [cf. Fig. 2(b)], in which the ancilla interacts with each qudit separately. The ancilla is quantum communicated from one to another system qudit in order to make it available for the control-gate action with that system qudit. □

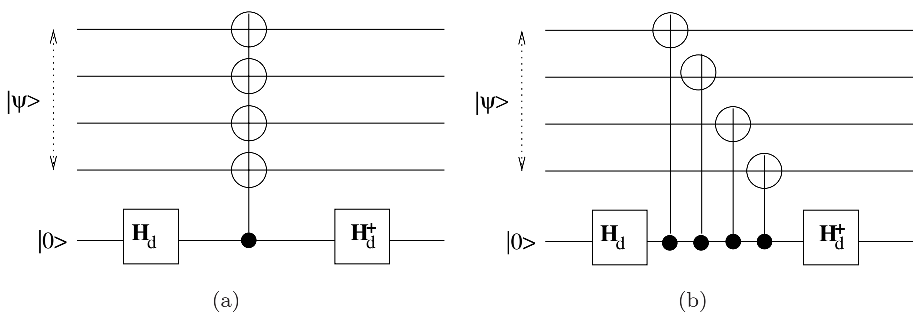

Fig. 2. Two equivalent ways of distributing an (indirect) measurement of $X^{\otimes n}$. The four upper wires denote four qubits of the measured system. The crossed circle-links represent CNOT operations. The control-operations may be (a) clustered into a single collective control-operation, or (b) performed in sequence (in any order).

Note that W itself need not have the product form of U. Given some function g, $W = g(U)$ will not have the product form unless g preserves product structure, i.e. $g(abc\cdots) = g(a)g(b)g(c)\cdots$. In particular, we may select $g(\cdot) = \exp[-i\log(\cdot)]$, which has this property. If $U = \sum_{j,k,\dots}\left(e^{2\pi ij/d}|j\rangle\langle j| \otimes e^{2\pi ik/d}|k\rangle\langle k| \otimes \cdots\right)$, then $W' = \sum_{j,k,\dots}\left(e^{2\pi j/d}|j\rangle\langle j| \otimes e^{2\pi k/d}|k\rangle\langle k| \otimes \cdots\right)$. In the case of Pauli operators, the situation is simpler because any tensor products of Pauli operators is both Hermitian and unitary, and we can simply set $W = U$, i.e. given observable W, a unitary operator compatible with it is itself. A case where this simplicity is not available is considered in the next section.

A natural application of the above results is in situations requiring incomplete measurements. For example, $X \otimes X$ is incomplete (if measured without projecting the two qubits individually). It represents the "phase observable" for a two-qubit system, whose two eigenspaces are spanned by $\{|00\rangle + |11\rangle, |01\rangle + |10\rangle\}$ and $\{|00\rangle - |11\rangle, |01\rangle - |10\rangle\}$. From Theorems 1 and 2, we know that incomplete $X \otimes X$ can be implemented using two CNOTs and an ancilla. Figure 2 gives alternative ways to indirect measurement of $X^{\otimes 4}$: Fig. 2(a) shows how it can be indirected using a single multiqudit control-operation; Fig. 2(b) shows how it can be broken down into a set of two-qubit interactions, and in principle, distributed.

A family of quantum error correcting codes that can be systematically built from classical linear codes are the Calderbank–Shor–Steane (CSS) codes[23,24] which can be described using the more general stabilizer formalism.[40,41] Here, the code C is chosen to lie in the $+1$ eigenspace of commuting operators M_j, which must be tensor products of Pauli matrices. By choosing a sufficient number of M_j's, one can ensure that for any pair of distinct correctible errors E_1, E_2, there is an M_j that anticommutes with E_1E_2, which allows the errors to be distinguished via the error correction condition. The M_j's form the set T, the *stabilizer* of the code C. To detect and determine an error, it suffices to measure the $n - k$ generators g_j of T. As a simple application of the above two theorems, we can construct circuits to measure the generators. We note the following two facts: (1) The g_j's are Hermitian operators drawn from the Pauli group, so that they are also unitary. To indirect their measurement, we set $W = U$ in Theorem 1; (2) they are tensor products of local operators (Pauli operators, here), which means that we can apply Theorem 2.

For example, consider a generator to the stabilizer of the 7-qubit Steane code, $XIIIXXX$, where the tensor product between successive operators is implicit. Theorem 1 implies that this syndrome can be measured indirectly by applying the controlled operation $|0\rangle\langle 0| \otimes IIIIIII + |1\rangle\langle 1| \otimes XIIIXXX$, where the first qubit is an ancilla. Next, Theorem 2 shows that the X's can be replaced with CNOTs from an ancilla onto the 1st, 5th, 6th and 7th system qubits. This gives the first syndrome measurement in Fig. 10.16 of Ref. 1, which is similar to measurement of the Steane code stabilizer generator $ZIZZIIZ$, where the Z's are replaced with controlled-phase gates (cf. Fig. 10.16 of Ref. 1). In this way, our method of constructing circuits can be applied to any syndrome computation. It can similarly be extended to codes living in the Hilbert space of higher-dimensional qudits.

Incomplete measurements corresponding to the product of operators are also essential in measurement-based quantum computation. The latter is a novel paradigm of universal quantum comptutation, recently studied by several authors,[25–35] who show, surprisingly, that universal quantum computation is possible using only measurements as computational steps. Two distinct models of measurement-based quantum computation are teleportation-based quantum computation (TQC)[28–30] and one-way quantum computation,[31–33] also called cluster-state quantum computing. TQC, which employs teleportation as a quantum computation primitive, was evolved from the idea of indirectly effecting certain gates and measurements, using ancillas. The method was generalized[25–27] by understanding the connection to teleportation.[36]

For example, a TQC strategy to teleport two qubits through a CNOT gate makes use of 2-qubit incomplete measurements $Z \otimes Z$ and $X \otimes Z$ on an input state $|\psi\rangle$ and an ancilla (see Eq. (34) of Ref. 35). Being the tensor products of Pauli operators, they are straightforwardly indirected and distributed. In particular, the operator $Z \otimes Z$ is simply the parity operator for Bell states, and its indirect measurement can be distributed using, as we shall see later, the circuit such as that in the second or third box in Fig. 4. Such simple recipes allow us to indirect a universal set of operations for quantum computation. In principle, this can be used to distribute TQC over a quantum network.

4. An Example: Distribution of Discrimination of Bell-States

The requirement that the distributed measurement must be an incomplete measurement of a certain type need not be restrictive. In this section, we give an example of a complete measurement $\mathcal{W}$ that can be implemented by means of several incomplete measurements W_j such that the W_j's can be distributed. This allows us to effectively distribute the measurement of $\mathcal{W}$.

We consider the problem of distributing Bell-state discrimination among n qudits. The full observable $\mathcal{W}$ in this case has generalized Bell states as its eigenstates, and lives in the Hilbert space $\mathcal{H}$ of dimension d^n, where each qudit is d-dimensional. We will show how $\mathcal{W}$ can be analyzed into a set of incomplete measurements corresponding to relative parity and phase, which are distributed.

The two-qubit case was considered in Ref. 21, where two separated users wish to perform a distributed Bell state measurement via quantum communication, and the states to be discriminated are the usual Bell states $|\Phi^{\pm}\rangle = (1/\sqrt{2})(|00\rangle \pm |11\rangle)$ and $|\Psi^{\pm}\rangle = (1/\sqrt{2})(|01\rangle \pm |10\rangle)$. These are the eigenstates of $X \otimes X$ and $Z \otimes Z$, which are also unitary. These operators commute with each other and have a manifestly product form. We can regard $X \otimes X$ as the phase observable (in that it informs us whether the Bell state contains a $+$ or $-$) and $Z \otimes Z$ as the parity observable (in that it informs us whether the superposition terms have odd or even parity). Thus we can apply Theorems 1 and 2 to measure $X \otimes X$ and $Z \otimes Z$ incompletely, to get complete information of the Bell state.

More generally, we can readily extend these results to the two-qudit space.[22] We replace the Pauli matrices with their d-dimensional analogs.[42] Accordingly, instead of X and Z, we have X_d and Z_d, respectively, given by the action:

$$Z_d|j\rangle \mapsto e^{2\pi\iota j/d}|j\rangle; \quad X_d|j\rangle \mapsto |j+1\rangle, \tag{1}$$

where the increment in the ket is in mod d arithmetic. The operators X_d and Z_d are related by a Fourier transform $X_d = H_d Z_d H_d^\dagger$, where H_d is the generalized Hadamard transformation given by:

$$(H_d)_{jk} = \frac{1}{\sqrt{d}} e^{-2\pi\iota j\cdot k/d}. \tag{2}$$

Unlike the qubit case, Z_d, X_d and H_d are not Hermitian. The d^2 2-qudit Bell states are[36]: $|\Psi_{pq}\rangle = 1/\sqrt{d}\sum_j e^{2\pi\iota jp/d}|j\rangle|j+q\rangle$ $(0 \leq p, q \leq d-1)$, the simultaneous eigenstates of $X_d \otimes X_d$ and $Z_d \otimes Z_d^\dagger$, with eigenvalues $e^{-2\pi ip/d}$ and $e^{-2\pi iq/d}$. Parameter p denotes the generalized phase, and q denotes the generalized parity. Thus, $X_d \otimes X_d$ and $Z_d \otimes Z_d^\dagger$, can be considered as unitary operators compatible with the generalized "phase observable" M_p, with eigenvalues p, and the generalized parity observable M_q, with eigenvalues q. In fact, $X_d \otimes X_d = e^{-2\pi i M_p/d}$ and $Z_d \otimes Z_d^\dagger = e^{-2\pi i M_q/d}$.

The generalization of the CNOT that one obtains according to the definition given in Theorem 2 is:

$$\mathcal{C}_{X_d} : |j\rangle|k\rangle \mapsto |j\rangle|j+k\rangle, \tag{3}$$

where the first (second) qudit is the control (target). Consider indirecting the measurement of Z_d on a qudit. Following Theorem 1, this measurement can be indirected using $\mathcal{C}_{Z_d}$, which is a controlled-phase operation. That is, in Fig. 1, we set $U \equiv Z_d$. However, by means of Hadamards, it is possible to turn $\mathcal{C}_{Z_d}$ into a $\mathcal{C}_{X_d}$ operation. To see this, we note that for any integer j,

$$(Z_d)^j = (H_d X_d H_d^\dagger)^j = H_d (X_d)^j H_d^\dagger. \tag{4}$$

We can therefore replace the unitary $U \equiv Z_d$ in the upper wire of Fig. 1 by an X_d, sandwiched between Hadamards outside the control operation. Thus, the indirection of the measurement of Z_d is equivalent to the circuit in Fig. 3(a). Furthermore, a circuit identity means that, by dropping the Hadamards in Fig. 3(a), reversing the control direction and taking the transpose-conjugate, we perform an equivalent operation, depicted in Fig. 3(b). This identity is proved in Theorem 3, which provides a qudit equivalent of the qubit control reversal depicted in Fig. 10 of Ref. 38.

Theorem 3. *The measurement circuits depicted in Fig.* 3 *are equivalent.*

Proof. Let the incoming state of the two qudits be $|\Psi\rangle = \sum_{jk} \alpha_{jk}|j\rangle|k\rangle$ (we ignore the fact that the summation can run on a single index on account of Schmidt decomposability). It may be seen that at stages 1–3, this state is successively

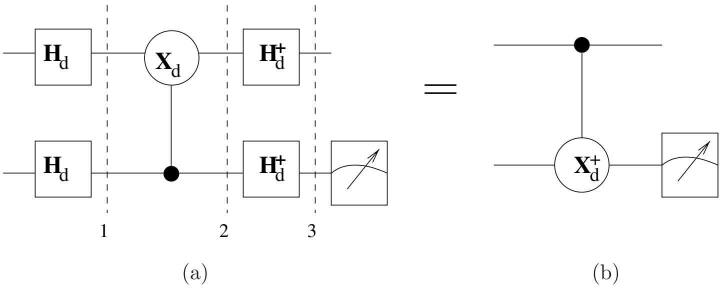

Fig. 3. The above circuits are equivalent to indirecting measurement of Z_d. The measured principal system enters in the upper wire, the ancilla is the lower wire. Dropping the Hadamards reverses the direction of control.

transformed first into $|\Psi_1\rangle \equiv (1/d)(\sum_{j,j',k,k'}(\alpha_{jk}\exp[(2\pi\iota/d)(-jj'-kk')]|j'\rangle|k'\rangle))$, then $|\Psi_2\rangle \equiv (1/d)(\sum_{j,j',k,k'}(\alpha_{jk}\exp[(2\pi\iota/d)(-jj'-kk')]|j'+k'\rangle|k'\rangle))$, and finally $|\Psi'\rangle \equiv (1/d^2)(\sum_{j,k,j',k',j'',k''}\alpha_{jk}\exp[(2\pi\iota/d)(-jj'-kk'+j''[j'+k']+k''k)]|j''\rangle|k''\rangle)$. Using the fact that $(1/\sqrt{d})\sum_{x=0}^{d-1}\exp[(2\pi\iota/d)(x\cdot y)] = \delta(y)$, $|\Psi'\rangle$ may be simplified to $\sum_{j,k}\alpha_j\beta_k|j\rangle|k-j\rangle$, which is also the state obtained by applying on $|\Psi\rangle$ the circuit in Fig. 3(b). □

With these results, we can extend the n-qubit result of Refs. 21 and 22 to the 2-qudit case, using Theorems 1–3. We now consider the more general system of "Bell states" on n qudits, which we introduce below. A complete, maximally entangled Bell basis for the Hilbert space $\mathbb{C}^{d^n}$ is given by

$$|\Psi_{pq_1q_2\cdots q_{n-1}}\rangle = \sum_{j=0}^{d-1} e^{2\pi\iota j\cdot p/d}|j, q_1+j, q_2+j, \ldots, q_{n-1}+j\rangle. \tag{5}$$

We call them Bell states in the sense that any state $|\Psi_{pq_1q_2\cdots q_{n-1}}\rangle$ is a simultaneous eigenstate of mutually commuting operators $X_d^{\otimes n}$ and $Z_d(j)\otimes Z_d^\dagger(k)$ $(1 \le j,k \le (n-1)$ and $j \ne k)$, having, respectively, eigenvalues $e^{-2\pi ip/d}$ and $e^{-2\pi i[q_k-q_j]/d}$. They are functions of, respectively, the generalized phase observable M_p, with eigenvalues p, and the generalized relative parity observable $M_{q_{j,k}}$ with eigenvalues $q_k - q_j$. In fact, $X_d^{\otimes n} = e^{-2\pi iM_p/d}$ and $Z_d(j)\otimes Z_d^\dagger(k) = e^{2\pi iM_{q_{j,k}}/d}$.

The circuit that accomplishes indirection of the measurement of M_p and $M_{q_{j,k}}$ is given in Fig. 4. According to Theorem 1, their measurements can be indirected using controlled-$(X_d^{\otimes n})$ and controlled-$(Z_d\otimes Z_d^\dagger)$ operations. According to Theorem 2, these joint controlled operations can be split into controlled operations on separate target qudits. The phase variable measurement (first box) employs type 2 decomposition, with n applications of $\mathcal{C}_{X_d}$, which is suitable for a distributed computing context in which the ancilla is sequentially passed from one node to another. The type 1 variant of this subcircuit would be to combine all the $\mathcal{C}_{X_d}$'s into a single controlled action, a controlled-$(X_d)^{\otimes n}$ gate, having the effect: $\mathcal{C}_U : |j\rangle|j_1\rangle\cdots|j_n\rangle \mapsto |j\rangle|j_1+j\rangle\cdots|j_n+j\rangle$, analogous to Fig. 2(b). Note that

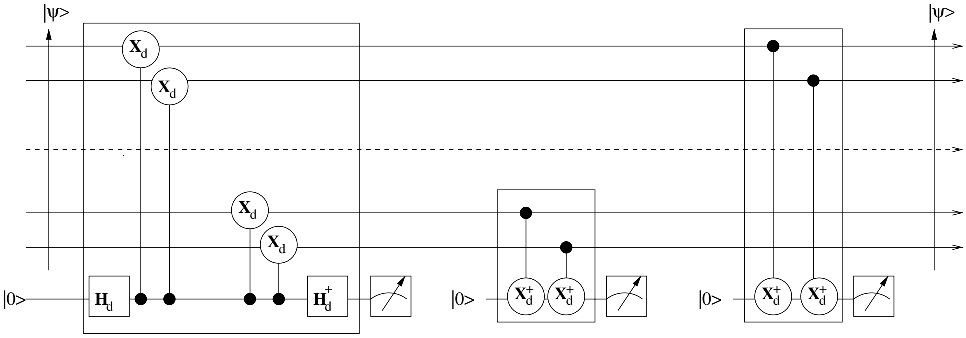

Fig. 4. Diagram depicting the circuit for the indirection of generalized orthonormal qudit Bell state discriminator. The first box depicts the indirected measurement of the generalized phase observable, M_p, compatible with $X_d^{\otimes n}$ in type 2 configuration. The other two boxes depict the indirected measurement of an observable compatible with $Z_d^\dagger \otimes Z_d$, which yields the relative parity between the two qudits. To obtain the full information on the Bell state, n ancilla measurements are needed in all: one to obtain phase information p, and $n-1$ needed to obtain relative parity information q_j.

controlled-$(Z_d \otimes Z_d^\dagger)$ is equivalent to $(H_d \otimes H_d)$(controlled-$(X_d \otimes X_d^\dagger))(H_d^\dagger \otimes H_d^\dagger)$, which is seen by an argument analogous to Eq. (4). In type 2 configuration, the controlled-$(X_d \otimes X_d^\dagger)$ can be written as a sequence of two $\mathcal{C}_{X_d}$'s acting from the same ancilla onto two different system qudits. Using Theorem 3, the direction of control can be inverted, and we get the subcircuits in the second and later boxes in Fig. 4. A total of n ancillary qudits are required, one for each incomplete, d-dimensional observable. In practical situations, the choice of the $n-1$ pairs (j,k) of the relative parity observable will depend on the topology of the quantum communication network available (cf. Sec. 5).

5. Quantum Communication

A novel practical use of the above circuits can be in overcoming restrictions coming from the topology of a quantum communication network. The classical and especially the quantum resources required to implement the network are expected to be expensive. Thus, it is worthwhile to use protocols that minimize both of them. As a particular application, suppose that we are faced with the task of nondestructively measuring quantum states in a network involving several users, who represent the network nodes. Quantum communication between the nodes is allowed but must preferably be minimized.

The direct way to perform multi-qudit measurement across a quantum network is for all other members to communicate their qudits to a single node, whose member (called, say Alice) performs a joint measurement on all n qubits or qudits to determine the state, and transmits back the measured state. For example, consider implementing Bell state discrimination across a quantum network. Alice can apply a string of $n-1$ $\mathcal{C}_X^\dagger$ operations on each consecutive pair of qudits in the Bell state

$|\Psi_{pq_1q_2\cdots q_{n-1}}\rangle$ in Eq. (5), with the control (target) qudit being the preceding (following) qudit, and then finally apply H_d on the first qudit. It is easily seen that each application of $\mathcal{C}_X^\dagger$ will disentangle the controlled qudit from the rest. For the Bell states, this procedure effects the transformation:

$$|\Psi_{pq_1q_2\cdots q_{n-1}}\rangle \ \mapsto \ |p\rangle|q_2 - q_1\rangle\cdots|q_{n-1} - q_{n-2}\rangle. \tag{6}$$

Subsequent measurement of each qudit in the computational basis completely characterizes the Bell state. The state thus being discriminated, the above procedure can be reversed to re-create the state $|\Psi_{pq_1q_2\cdots q_{n-1}}\rangle$ and transmit it back to the remaining players.

In contrast, protocols based on our circuits quite generally involve only transmission of the ancilla rather than the system qudits along the network edges. At each node, the ancilla interacts with the local qudit as necessary. For example, in the case of a n-qudit Bell state discrimination, the ancilla measuring the phase observable M_p visits each node.

Irrespective of network topology, the direct strategy for Bell-state discrimination requires the implementation of $2(n-1)$ two-qudit gates in all. In our method, the number of two-qudit gates is the sum of n two-qudit gates for determining the phase parameter p and $2(n-1)$ for determining the (relative) parities, giving a total of $3n-2$ two-qudit gates. From this viewpoint of consumption of nonlinear resources, our method does not offer any advantage. However, this turns out not to be the case from the viewpoint of quantum communication complexity, that is, the quantity of quantum information (measured in qudits) that must be communicated between different network nodes in order to perform a computation. Still, one point worth noting here is that whereas the full state is available in the measure-recreate technique just after Alice's measurement, in our protocol, the full sequence of communication must be completed in order to recover the initial state. Otherwise, the ancilla remains entangled with the system qudits. In this work, we ignore both noise and physical distance issues.

Suppose that a quantum communication network with a star topology and n members is given, as for example, in Fig. 5(a), where $n = 6$. For all members to transmit their qudits to Alice (at A), and for her to transmit them back would require $2(n-1)$ qudits to be communicated. Each edge through which a qudit is communicated is counted as a unit of quantum communication complexity. In our method, for measuring the "phase observable" M_p among $n(> 2)$ parties, the ancillary qudit is communicated $2(n-2)$ times [for example, using the path $BACADAEAF$, starting at B and being measured at F, giving a complexity of 8 for Fig. 5(a)]; the communication complexity for relative parity measurement is the number of edges, $n-1$. In all, this requires $3n-5$ instances of qudit communication, which is larger than that required for the direct method.

However, consider a linear configuration of the communication network, as in Fig. 5(b), where members are linked up in a single series. In the direct method, if Alice is located at one end, the communication complexity is seen to be $n(n-1)$

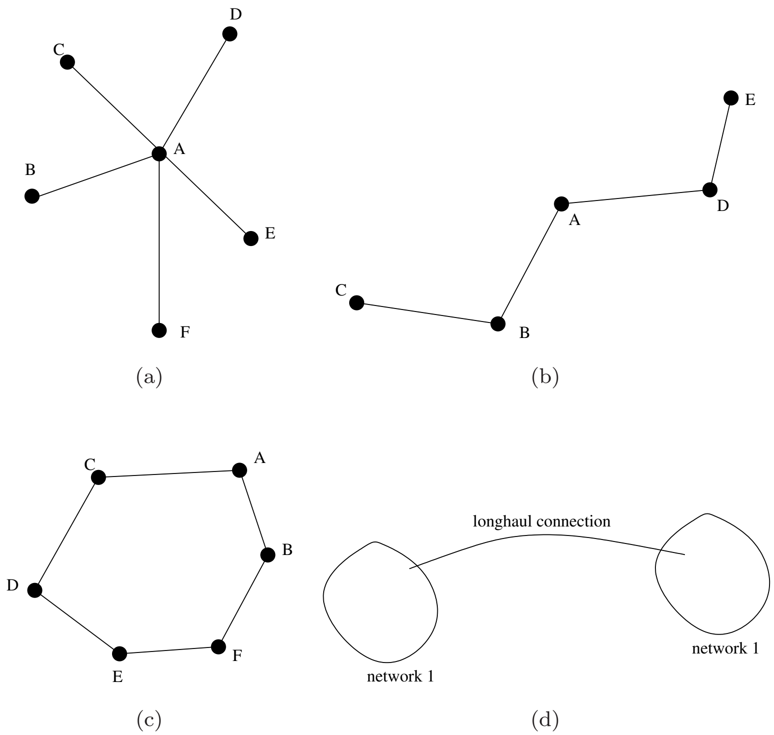

Fig. 5. Four possible configurations of the quantum communication network: (a) In a star topology, a set of "relative parity" measurements could be along each edge; (b) in the linear configuration, the strategy of observing consecutive qubits or qudits, in the manner of Fig. 4, can be used with advantage. Similar is the case with ring topology in (c) and the situation in Fig. (d), which depicts two subgraphs connected by an expensive edge, for example, a long-haul connection.

qudits (again, counting each traversed edge as one unit of quantum communication); it is $(n^2-1)/2$ if she is in the middle. In either case, it is (of order) $O(n^2)$. In contrast, our method can be implemented using $n-1$ qudit communications for the phase and one qudit communication for each relative parity measurement. For example, to measure the phase observable, the ancillary qudit traverses the path $CBADE$, starting at C and being measured at E, giving a complexity of 4. This requires only $2(n-1)$ qudits to be communicated in all, so that the required communication is only $O(n)$. Thus, a distributed rather than direct method gives a quadratic saving in quantum communication complexity.

A similar quadratic saving is seen to hold for the ring topology shown in Fig. 5(c). The situation described in Fig. 5(d) is of even greater practical relevance. In real life, we find the global Internet formed by long-haul connections between various local area networks (LANs). A corresponding quantum situation is encountered when the distributed computing occurs over a large area, where two relatively inexpensive quantum LANs of arbitrary topology [networks 1 and 2 in Fig. 5(d)] are linked by a much more costly connection, typically an expensive long-haul quantum channel. To perform a Bell state discrimination over the global net, the direct strategy would necessitate all qubits on one of the LANs to be transmitted across the long-haul channel. On the other hand, our distributed strategy allows for no more than two ancillary qudits to be transmitted across this channel, one for the phase observable measurement, and the other for one relative parity measurement between any member of network 1 and any member of network 2.

6. Conclusions

We have developed a general method for constructing circuits to indirect and distribute measurements on multiple qudits. This generalizes and unifies a number of known circuit results. A side-benefit for quantum communication in distributed computing was also noted. We conclude by noting possible directions for generalizing our work. One way is to study the general conditions under which any (possibly complete) multi-qudit observable can be effectively distributed. Another is to allow for more general initial state preparation of ancillas. This could be used to extend optimal partial deterministic quantum teleportation of qubits[43] to qudits. Another idea is to allow the ancillas to be measured by positive-operator values measures rather than by only projective measurements.

Acknowledgments

We are thankful to Prof. J. Pasupathy, V. Aravindan and H. Harshavardhan, Dr. Ashok Vudayagiri, Dr. Ashoka Biswas and Dr. Shubhrangshu Dasgupta for useful discussions.

References

1. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
2. J. Stolze and D. Suter, *Quantum Computing* (Wiley-Vich, 2004).
3. A. Einstein, B. Rosen and B. Podolsky, *Phys. Rev.* **47** (1935) 777.
4. D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, *Nature* **390** (1997) 575–579.
5. J. W. Pan, D. Bouwmeester, H. Weinfurter and A. Zeilinger, *Phys. Rev. Lett.* **80** (1998) 3891.
6. K. Mattle, H. Weinfurter, P. G. Kwait and A. Zeilinger, *Phys. Rev. Lett.* **76** (1996) 4656.
7. A. R. R. Carvalho, F. Mintert and A. Buchleitner, *Phys. Rev. Lett.* **93** (2004) 230501.
8. M. Hein, W. Dr and H.-J. Briegel, *Phys. Rev. A* **71** (2004) 032350.
9. W. K. Wootters and W. H. Zurek, *Nature* **299** (1982) 802.
10. J. Walgate, A. J. Short, L. Hardy and V. Vedral, *Phys. Rev. Lett.* **85** (2000) 4972.
11. S. Ghosh, G. Kar, A. Roy, A. S. Sen (De) and U. Sen, *Phys. Rev. A* **87** (2001) 277902.
12. S. Virmani, M. F. Sacchi, M. B. Plenio and D. Markham, *Phys. Lett. A* **288** (2001) 62.
13. Y. X. Chen and D. Yang, *Phys. Rev. A* **64** (2001) 064303.
14. S. Ghosh, G. Kar, A. Roy and D. Sarkar, *Phys. Rev. A* **70** (2004) 022304.

15. M. Horodecki, A. Sen(De), U. Sen and K. Horodecki, *Phys. Rev. Lett.* **90** (2003) 047902.
16. M. M. Cola and M. G. A. Paris, *Phys. Lett. A* **337** (2005) 10.
17. J. W. Pan and A. Zeilinger, *Phys. Rev. A* **57** (1998) 2208.
18. Y. H. Kim, S. P. Kulik and Y. Shih, *Phys. Rev. Lett.* **86** (2001) 1370.
19. J. Preskill, *Lecture Notes on Quantum Computation*, http://www.theory.caltech.edu/people/preskill/p299/#lecture.
20. D. Boschi, S. Branca, F. D. Martini, L. Hardy and S. Popescu, *Phys. Rev. Lett.* **80** (1998) 1121.
21. M. Gupta and P. Panigrahi, Deterministic Bell State Discrimination, eprint quant-ph/0504183.
22. P. Panigrahi, M. Gupta, A. Pathak and R. Srikanth, in *Proc. AIP Conf. on Quantum Computing Back Action*, IIT Kanpur, India **864** (2006) 197.
23. A. M. Steane, *Proc. Roy. Soc. London A* **452** (1996) 2551.
24. A. R. Calderbank and P. Shor, *Phys. Rev. A* **54** (1996) 1098.
25. D. Gottesman and I. L. Chuang, *Nature* (*London*) **402** (1999) 390.
26. X. Zhou, D. Leung and I. Chuang, *Phys. Rev. A* **62** (2000) 052316.
27. X. Zhou, D. Leung and I. Chuang, Methodology for quantum logic gate construction, arXiv e-print quant-ph/0002039.
28. M. A. Nielsen, *Phys. Lett. A* **308** (2003) 96.
29. D. Leung, Two-qubit projective measurements are universal for quantum computation, eprint quant-ph/0111122.
30. D. Leung, *Int. J. Quant. Inf.* **2** (2004) 33.
31. R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86** (2001) 5188.
32. R. Raussendorf, D. E. Browne and H. J. Briegel, *Phys. Rev. A* **68** (2003) 022312.
33. M. Fujii, Continuous-variable quantum teleportation with a conventional loser, eprint quant-ph/0301045.
34. S. Perdrix and P. Jorrand, Measurement-based quantum turing machines and their universality, eprint quant-ph/0404146.
35. A. M. Childs, D. W. Leung and M. A. Nielsen, *Phys. Rev. A* **71** (2005) 032318.
36. C. H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres and W. K. Wootters, *Phys. Rev. Lett.* **70** (1993) 1895.
37. E. Knill, R. Laflamme and G. J. Milburn, *Nature* (*London*) **409** (2001) 46.
38. J. Preskill, *Proc. Roy. Soc. Lond. A* **454** (1998) 385.
39. P. O. Schmidt *et al.*, *Science* **309** (2005) 749.
40. D. Gottesman, PhD thesis, Caltech (1997).
41. D. Gottesman, Stabilizer codes and quantum error correction, eprint quant-ph/9705052.
42. E. Knill, Non-binary unitary error bases and quantum codes, eprint quant-ph/9608048.
43. L. Mišta and R. Filip, *Phys. Rev. A* **71** (2005) 022319.