

Quantum communication cost of preparing multipartite entanglement

Caroline Kruszynska,^{1,2,*} Simon Anders,¹ Wolfgang Dür,^{1,2} and Hans J. Briegel^{1,2}

¹*Institut für Theoretische Physik, Universität Innsbruck, Technikerstr. 25, 6020 Innsbruck, Austria*

²*Institut für Quantenoptik und Quanteninformation der ÖAW, Technikerstr. 21a, 6020 Innsbruck, Austria*

(Dated: 25 April 2006)

We study the preparation and distribution of high-fidelity multi-party entangled states via noisy channels and operations. In the particular case of GHZ and cluster states, we study different strategies using bipartite or multipartite purification protocols. The most efficient strategy depends on the target fidelity one wishes to achieve and on the quality of transmission channel and local operations. We show the existence of a crossing point beyond which the strategy making use of the purification of the state as a whole is more efficient than a strategy in which pairs are purified before they are connected to the final state. We also study the efficiency of intermediate strategies, including sequences of purification and connection. We show that a multipartite strategy is to be used if one wishes to achieve high fidelity, whereas a bipartite strategy gives a better yield for low target fidelity.

PACS numbers: 03.67.Mn, 03.67.Hk, 03.67.Pp

I. INTRODUCTION

In the past, (multipartite) entanglement has been mainly considered as a puzzling artifact of quantum mechanics. More recently, however, the focus on entanglement has shifted, as it was realized that entanglement also constitutes a valuable resource for quantum information processing. Possible applications of multipartite entanglement include certain security tasks in distributed communication scenarios [1, 2], the improvement of frequency standards [3], as well as measurement based quantum computation schemes [4].

In this context, the problem of generating multipartite entanglement of high fidelity arises. If entangled states are to be distributed among spatially separated parties, as it is e. g. required in distributed communication scenarios, the main obstacle comes from channel noise. Possible ways to overcome channel noise and hence to successfully generate high-fidelity multipartite entangled states have been developed. These methods are based on (i) quantum error correction and make use of (concatenated) quantum error correction codes [5], or (ii) entanglement purification [6, 7, 8, 9]. While (i) is applicable to directly distribute arbitrary states, (ii) concentrates on the generation of specific, maximally entangled pure states. The generation of maximally entangled pairs of particles allows in turn to distribute arbitrary states by means of teleportation. In both cases, a substantial overhead is required to guarantee successful, high fidelity generation of the desired states. In (i) this overhead arises from redundant encoding, enabling one to perform error correction, while for (ii) several identical copies need to be prepared and locally processed to generate high fidelity entangled states. The quantification of this overhead, or the quantum communication cost,

which we shall define more precisely, is the main concern of this article.

To be specific, we will concentrate on schemes based on entanglement purification. These schemes are specially suited to generate entangled states of a specific form, and are hence expected to perform better than general purpose schemes such as (i). In fact, a remarkable robustness of entanglement purification protocols against noise in local operations –which we consider in addition to channel noise– has been found [8, 9]. That is, errors of the order of several percent in local control operations can be tolerated, still allowing for the generation of high fidelity entangled states, even in the presence of very noisy quantum channels and with only a moderate overhead. For perfect local operations, the required overhead in resources is solely determined by the noisy quantum channels. In this case, the channel capacity [10, 11] provides a suitable measure for this overhead. In a bipartite communication scenario, the channel capacity gives the optimal rate of quantum communication, i. e. the amount of quantum information transmitted per actual channel usage. While one might think that the abstract notion of channel capacity may also be employed to our problem –the generation of certain high fidelity entangled pure states–, one actually faces a number of difficulties. First, channel capacities are asymptotic quantities which are very complicated to calculate; second, the definition of channel capacity is not suitable to account for imperfect local operations (e. g. noise in local coding and decoding procedures); and third, we are actually considering a restricted problem, namely the generation of specific multipartite entangled states, rather than the successful transmission of arbitrary quantum information.

We thus introduce a quantity closely related to quantum channel capacity, namely the *quantum communication cost* $C_{F,G}$. $C_{F,G}$ denotes a family of quantities which specify the number of uses of the noisy quantum channel required to prepare a specific (multipartite) entangled state $|G\rangle$ with fidelity $\tilde{F} \geq F$. In this paper, we

*Electronic address: caroline.kruszynski@uibk.ac.at

will focus on target states $|G\rangle$ which are so-called two-colorable graph states. These states include, for instance, GHZ states and cluster states – a universal resource for measurement based quantum computation [4]– and they are locally equivalent to codewords of Calderbank-Shor-Steane error correcting codes [12, 13]. We establish upper bounds on $C_{F,G}$ by optimizing over a large class of different strategies that generate these multipartite entangled states. These strategies include, as extremal cases, (i) the generation and purification of pairwise entanglement, from which, by suitable connection processes (or, alternatively, teleportation) the desired multipartite states are generated; (ii) the generation and direct multipartite purification of the desired target states. Intermediate strategies, e. g. the purification of smaller states to high fidelity and their subsequent connection to the desired larger state, will also be investigated. Depending on the actual noise parameters for channels and local control operations, and on the desired target fidelity F , the optimal strategy varies. For high target fidelities, multipartite strategies turn out to be favorable.

This article is organized as follows: In Sec. II, we present the concepts we will use: We start with a review of the graph state formalism in order to introduce notation and the two types of states we wish to distribute, namely GHZ states and 1D cluster states. We shall also introduce a technique to connect two smaller graph states to obtain a larger one. Then, we give details for our noise models and review the employed purification protocols. Readers familiar with these concepts may skip this section. Sec. III explains the different strategies for employing the protocols that we wish to compare. The actual comparison is done using extensive numerical Monte Carlo simulations and results are presented in Sec. IV. In order to corroborate these results we have done analytical studies for certain restricted noise models (Sec. V). We conclude with a summary (Sec. VI).

II. BASIC CONCEPTS

A. The graph-states formalism

A graph $G = (V, E)$ is a collection $V = \{a, b, c, \dots\}$ of $N = |V|$ vertices connected by edges $E \subset [V]^2$. The description of the edges is given by the adjacency matrix Γ_G associated with the graph

$$(\Gamma_G)_{ab} = \begin{cases} 1, & \text{if } a \text{ and } b \text{ are connected by an edge,} \\ & \text{i.e. } \{a, b\} \in E \\ 0, & \text{otherwise} \end{cases}$$

The neighborhood $N_a \subset V$ of vertex a is defined as the set of vertices connected with it by an edge, $N_a = \{b : \{a, b\} \in E\}$.

With each graph G we associate a pure quantum state. If the graph's vertex set can be separated into two sets A and B such that no edges exist between vertices of

the same set, we call it a two-colorable graph (Footnote [14]). The vertices are qubits and the edges represent interactions.

There are three equivalent descriptions of graph states which are reviewed in the following sections (For a detailed treatment see [15]):

1. Graph states in the stabilizer formalism

Associated with a graph G is a set of N operators

$$K_G^{(a)} = \sigma_x^{(a)} \prod_{b \in N_a} \sigma_z^{(b)}. \quad (1)$$

They form a complete set of commuting observables for the system of qubits associated with the graph and therefore possess a set of common eigenstates which form a basis of the Hilbert space. These eigenstates are called graph states and are here written as $|G, \boldsymbol{\mu}\rangle$ where the a^{th} component of vector $\boldsymbol{\mu} \in \{0, 1\}^N$ is equal to 0 if $K_G^{(a)}|G, \boldsymbol{\mu}\rangle = |G, \boldsymbol{\mu}\rangle$ and 1 if $K_G^{(a)}|G, \boldsymbol{\mu}\rangle = -|G, \boldsymbol{\mu}\rangle$. We abbreviate $|G\rangle := |G, \mathbf{0}\rangle$. We also sometimes suppress the letter “ G ” and write just $|\boldsymbol{\mu}\rangle$, if the context makes clear which graph G is meant.

2. Graph states in the interaction picture

A graph state with $\boldsymbol{\mu} = \mathbf{0}$ can be written in the computational basis in the following manner:

$$|G\rangle = \left(\prod_{\{a,b\} \in E} \Lambda Z^{(ab)} \right) |+\rangle^{\otimes |V|} \quad (2)$$

where ΛZ is the controlled phase gate,

$$\Lambda Z^{(a,b)} = |00\rangle_{ab}\langle 00| + |01\rangle_{ab}\langle 01| + |10\rangle_{ab}\langle 10| - |11\rangle_{ab}\langle 11|, \quad (3)$$

which corresponds to an Ising-type interaction, $\Lambda Z^{(ab)} = e^{-i\pi H^{(ab)}}$, with interaction Hamiltonian $H^{(ab)}$ given by

$$H^{(ab)} = \frac{1}{2} \left(\mathbb{1} - \sigma_z^{(a)} \right) \otimes \frac{1}{2} \left(\mathbb{1} - \sigma_z^{(b)} \right) = |11\rangle_{ab}\langle 11|.$$

That is, $|G\rangle$ is generated from a pure product state by applying interactions between all pairs of particles connected by edges.

We list some useful relations for later reference: The 2^N common eigenstates of the operators $K^{(a)}$ can be generated from $|G\rangle$ by applying all possible products of

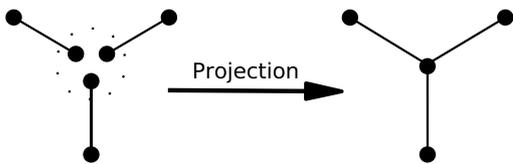


FIG. 1: Producing a graph state in the VBS picture.

$\sigma_z^{(a)}$, $a \in 1, 2, \dots, N$. This can be seen from

$$\begin{aligned}
 K^{(b)} \sigma_z^{(a)} |G\rangle &= \sigma_x^{(b)} \prod_{c \in N_b} \sigma_z^{(c)} \sigma_z^{(a)} |G\rangle \\
 &= \sigma_x^{(b)} \sigma_z^{(a)} \prod_{c \in N_b} \sigma_z^{(c)} |G\rangle \\
 &= (-1)^{\delta_{ab}} \sigma_z^{(a)} \sigma_x^{(b)} \prod_{c \in N_b} \sigma_z^{(c)} |G\rangle \\
 &= (-1)^{\delta_{ab}} \sigma_z^{(a)} |G\rangle,
 \end{aligned} \tag{4}$$

which means that $\sigma_z^{(a)} |G, \mathbf{0}\rangle = |G, 0 \dots 0 \overset{a}{\downarrow} 1 0 \dots 0\rangle$. From this relation, together with the fact that $\sigma_y^{(a)} = i\sigma_x^{(a)}\sigma_z^{(a)}$, one can deduce the effect of $\sigma_x^{(a)}$ and $\sigma_y^{(a)}$ (see Ref. [15] and [9] for proofs): Splitting the index vector $\boldsymbol{\mu}$ into μ_a , $\boldsymbol{\mu}_{N_a}$ (neighborhood of vertex a), and $\boldsymbol{\mu}_{R_a}$ (remaining vertices), we write

$$\sigma_z^{(a)} |G, \mu_a \boldsymbol{\mu}_{N_a} \boldsymbol{\mu}_{R_a}\rangle = |G, \overline{\mu_a} \boldsymbol{\mu}_{N_a} \boldsymbol{\mu}_{R_a}\rangle \tag{5}$$

$$\sigma_x^{(a)} |G, \mu_a \boldsymbol{\mu}_{N_a} \boldsymbol{\mu}_{R_a}\rangle = (-1)^{\mu_a} |G, \mu_a \overline{\boldsymbol{\mu}_{N_a}} \boldsymbol{\mu}_{R_a}\rangle \tag{6}$$

$$\sigma_y^{(a)} |G, \mu_a \boldsymbol{\mu}_{N_a} \boldsymbol{\mu}_{R_a}\rangle = i(-1)^{\overline{\mu_a}} |G, \overline{\mu_a} \overline{\boldsymbol{\mu}_{N_a}} \boldsymbol{\mu}_{R_a}\rangle \tag{7}$$

where the over-bar means bit complementation.

3. Graph states in the valence bond solid (VBS) picture

Another description of graph states was introduced in Ref. [16]. In this picture, every edge is replaced by a pair in a maximally entangled state, usually $(|00\rangle + |01\rangle + |10\rangle - |11\rangle)/2$. Each qubit a gets replaced by d_a virtual qubits, where $d_a = |N_a|$ is the degree of vertex a . The physical qubit is recovered by projecting the virtual qubits onto the two-dimensional subspace of the physical one (see Fig. 1) using as projector

$$P_d = |\tilde{0}\rangle\langle 0 \dots 0| + |\tilde{1}\rangle\langle 1 \dots 1|. \tag{8}$$

4. Cluster states and GHZ states

In this article, we study the purification of graph states using two important representatives from this class as



FIG. 2: Graphs for (a) cluster and (b) GHZ states.

examples. By “cluster states”, we mean graph states associated with a regular lattice as graph, in this article always a line as in Fig. 2 (a), and with $\boldsymbol{\mu} = \mathbf{0}$. The term GHZ state will *in this article* be used for a graph state (again with $\boldsymbol{\mu} = \mathbf{0}$) associated with a star-shaped graph G_* as in Fig. 2 (b). Such a state can be written as

$$|G_*\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |+\rangle^{\otimes(N-1)} + |1\rangle \otimes |-\rangle^{\otimes(N-1)} \right)$$

and is hence in its entanglement properties equivalent to an “ordinary” GHZ state $\frac{1}{\sqrt{2}} (|0\rangle^{\otimes N} + |1\rangle^{\otimes N}) = (\mathbb{1} \otimes \text{Had}^{\otimes(N-1)}) |G_*\rangle$ (where $|\pm\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle)$ and Had is the Hadamard operation $\text{Had} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$).

5. Bell pairs and graph-state formalism

In order to keep a certain homogeneity, we will employ a new notation for the states of the Bell basis, usually written as:

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle)$$

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle),$$

Applying a Hadamard operation on the second qubit, one obtains a new basis formed by the graph states $|G_2, 00\rangle, |G_2, 01\rangle, |G_2, 10\rangle$ and $|G_2, 11\rangle$, where G_2 denotes the graph composed of two vertices and one edge. Our new notation shows directly the relation between this two bases:

$$\begin{aligned}
 |\Phi^+\rangle &=: |B; 00\rangle = \text{Had}^{(2)} |G_2, 00\rangle \\
 |\Psi^+\rangle &=: |B; 01\rangle = \text{Had}^{(2)} |G_2, 01\rangle \\
 |\Phi^-\rangle &=: |B; 10\rangle = \text{Had}^{(2)} |G_2, 10\rangle \\
 |\Psi^-\rangle &=: |B; 11\rangle = \text{Had}^{(2)} |G_2, 11\rangle.
 \end{aligned} \tag{9}$$

6. Connection of graph-states

In this section, we define a procedure to connect two graph states, $|G_1\rangle$ with N_1 qubits, and $|G_2\rangle$ with N_2 qubits, “fusing” together their respective vertices a_1 and a_2 , yielding a state $|G\rangle$ with $N_1 + N_2 - 1$ qubits. This process is depicted in Fig. 3. To realize this action, one applies a projective measurement on a_1 and a_2 , given by

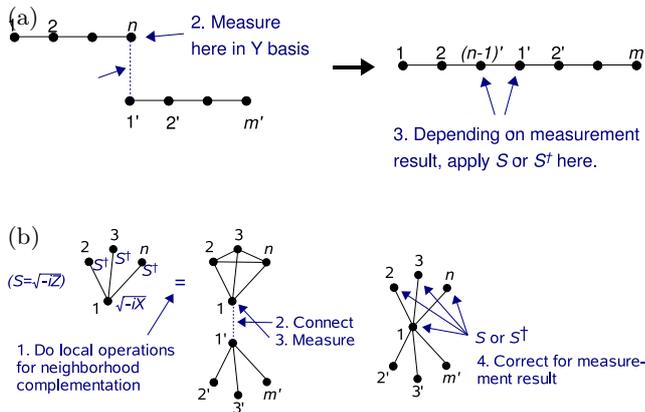


FIG. 3: (Color online.) How to use the connection procedure of Sec. II A 6 to assemble large (a) cluster and (b) GHZ states from smaller cluster or GHZ states.

$P_2 = |0\rangle\langle 00| + |1\rangle\langle 11|$ and $P_2^\perp = |0\rangle\langle 01| + |1\rangle\langle 10|$ (with outcomes 0 and 1). P_2 is defined like in the VBS picture. By similarity with this picture, if the result of the measurement is 0, the final state is the graph state resulting from the connection of G_1 and G_2 . If one obtains 1, a correction has to be done. As shown below, it is sufficient to apply $\prod_{b \in N_{a_2}} \sigma_z^{(b)}$ to the resulting state. Recalling that $K_G^{(a)}|G\rangle = |G\rangle$ with $K_G^{(a)} = \sigma_x^{(a)} \prod_{b \in N_a} \sigma_z^{(b)}$, one sees that any graph state can be decomposed as $|G\rangle = |0\rangle_a \otimes |\chi\rangle + |1\rangle_a \otimes \prod_{b \in N_a} \sigma_z^{(b)} |\chi\rangle$. Applying $\prod_{b \in N_{a_2}} \sigma_z^{(b)}$ to the state resulting from P_2^\perp one obtains

$$\prod_{b \in N_{a_2}} \sigma_z^{(b)} P_2^\perp |G_1\rangle |G_2\rangle = \prod_{b \in N_{a_2}} \sigma_z^{(b)} \left(\sigma_z^{(d)} |0\rangle \otimes |\chi_1\rangle \otimes \prod_{d \in N_{a_2}} |\chi_2\rangle + |1\rangle \otimes \prod_{c \in N_{a_1}} \sigma_z^{(c)} |\chi_1\rangle |\chi_2\rangle \right) = |0\rangle \otimes |\chi_1\rangle \otimes |\chi_2\rangle + \prod_{b \in (N_{a_1} + N_{a_2})} \sigma_z^{(b)} |1\rangle \otimes |\chi_1\rangle \otimes |\chi_2\rangle = |G_1 + G_2\rangle \quad (10)$$

Fig. 3 shows how to use this technique to assemble cluster and GHZ states from $|G_2\rangle$ states.

B. Noise model

1. Channel noise

In any realistic setting, channels will be noisy. We study the influence of channel noise by considering restricted noise models, where the Kraus representation of the superoperators is diagonal in the Pauli basis. This is a common and usually sufficiently general model [17] (In particular, any noisy channel can be brought to such a form by means of (probabilistic) local operations). This allows for an efficient and convenient simulation by Monte Carlo techniques (see Sec. IV A). We consider the following channels:

phase-flip channel:

$$\rho \mapsto \mathcal{E}_z^{(a)}(\rho) = q\rho + (1-q)\sigma_z^{(a)}\rho\sigma_z^{(a)} \quad (11)$$

bit-flip channel:

$$\rho \mapsto \mathcal{E}_x^{(a)}(\rho) = q\rho + (1-q)\sigma_x^{(a)}\rho\sigma_x^{(a)} \quad (12)$$

depolarizing channel:

$$\rho \mapsto \mathcal{E}^{(a)}(\rho) = q\rho + \frac{1-q}{3} \left(\sigma_x^{(a)}\rho\sigma_x^{(a)} + \sigma_y^{(a)}\rho\sigma_y^{(a)} + \sigma_z^{(a)}\rho\sigma_z^{(a)} \right) \quad (13)$$

In case of depolarizing channel, we define

$$p = (4q - 1)/3$$

which allow us to rewrite Eq. (13) as

$$\rho \mapsto \mathcal{E}^{(a)}(\rho) = p\rho + \frac{1-p}{4} \left(\rho + \sigma_x^{(a)}\rho\sigma_x^{(a)} + \sigma_y^{(a)}\rho\sigma_y^{(a)} + \sigma_z^{(a)}\rho\sigma_z^{(a)} \right) \quad (14)$$

$(1-q)$ will be called the *alteration probability* and p the *reliability*.

2. Local noise

As part of the purification protocols, local one- and two-qubit unitary operations are employed which may be noisy. An imperfect operation is modeled by preceding the perfect operation $U^{(ab)}$ with the application of one of the noise superoperators \mathcal{E} from Eqs. (11–13), i. e. the state is transformed as

$$\rho \mapsto U^{(ab)} (\mathcal{E}^a(\mathcal{E}^b(\rho))) U^{\dagger(ab)}.$$

We assume that the protocols are executed with the least possible number of operations to keep accumulated noise low. Hence, if a two-qubit gate $U_{12}^{(ab)}$ is preceded by one-qubit gates $U_1^{(a)}$ and $U_2^{(b)}$ we apply one combined unitary $U^{(ab)} = U_1^{(a)}U_2^{(b)}U_{12}^{(ab)}$ which is subjected to noise only once.

3. Commutation between connection and noise

We now state an observation that will later (in Sec. VB) be of use.

For any graph states $|G_1\rangle$ and $|G_2\rangle$ which are connected by the procedure described in Sec. II A 6, one can show that the noise processes commute with the connection procedure, if they are expressed by a superoperator by only σ_z Pauli operators. This comes from the fact that the neighborhood of the connected vertices a_1 and a_2 changes with the connection and hence, σ_x and σ_y Pauli operators will affect different vertices (see Eqs. (5), (6) and (7)).

The commutation rules between projector P_2 (see Eq. (8)) and σ_z can be deduced from the following expression of the connected graph state:

$$\begin{aligned} P_2|G_1\rangle|G_2\rangle &= P_2\left(|0\rangle_{a_1}|0\rangle_{a_2}|\chi\rangle_1|\chi\rangle_2 + \right. \\ &+ \prod_{c \in N_{a_2}} \sigma_z^{(c)}|0\rangle_{a_1}|1\rangle_{a_2}|\chi\rangle_1|\chi\rangle_2 + \\ &+ \prod_{b \in N_{a_1}} \sigma_z^{(b)}|1\rangle_{a_1}|0\rangle_{a_2}|\chi\rangle_1|\chi\rangle_2 + \\ &\left. + \prod_{b \in N_{a_1}} \sigma_z^{(b)} \prod_{c \in N_{a_2}} \sigma_z^{(c)}|1\rangle_{a_1}|1\rangle_{a_2}|\chi\rangle_1|\chi\rangle_2\right) \end{aligned}$$

Recalling that $\sigma_z|0\rangle = |0\rangle$, $\sigma_z|1\rangle = -|1\rangle$ one can show that:

$$P_2\sigma_z^{(a_1)}|G_1\rangle|G_2\rangle = \sigma_z^{(a_1)}P_2|G_1\rangle|G_2\rangle \quad (15)$$

$$P_2\sigma_z^{(a_2)}|G_1\rangle|G_2\rangle = \sigma_z^{(a_2)}P_2|G_1\rangle|G_2\rangle \quad (16)$$

C. Local noise equivalent

To judge how close state ρ is to the desired state $|\psi\rangle$, one often usually employs the fidelity $F := \langle\psi|\rho|\psi\rangle$. However, it may be advantageous to regauge the fidelity by introducing the following derived measure: We define the local noise equivalent (LNE) as the level of local depolarizing noise (in terms of the alteration probability $(1-q)$ of Eq. (13)) that one has to apply to each qubit of the perfect state $|\psi\rangle$ to deteriorate it to the same fidelity F as ρ has. The advantage of this measure is twofold: (i) It is more natural for uses of states in quantum error correction schemes, as it can be compared directly to the fault-tolerance threshold in case of uncorrelated-noise models. (ii) It does not fall off exponentially with

the size of a state for constant noise levels, as the fidelity does. On the other hand, it often cannot be calculated analytically in a straight-forward way. We hence used a numerical Monte Carlo simulation of the state deterioration (which is why the LNE scale in the figures has error bars).

D. Purification protocols

The purpose of entanglement purification is the following: One is given an ensemble of multi-party states, which all are distributed over two (or more) sites and exhibit entanglement between the sites. These states are only an approximation to the desired state $|\Psi\rangle\langle\Psi|$ with an insufficient fidelity, which one wishes to improve. As the sites are spatially separated, one cannot apply joint operation on the distributed parts of a state. Instead, one compares (in case of the so-called recurrence protocols, which are considered here solely) pairs of entangled states, makes joint operations on them, and then measures one of the state in order to gain information about the other. Only for specific measurement outcomes, the other state is kept. After iterating this procedure, one is left with an ensemble of smaller number of particles but higher fidelity.

1. Bipartite purification

Several protocols have been proposed to purify bipartite entangled states [6, 7, 18]. To test the different strategies, we used the most efficient which can be used to purify an ensemble of $|\Phi^+\rangle$ states, namely the one described in Ref. [7]. We present here a modified version of this bipartite entanglement purification protocol (BEPP) which allows for the purification of the connected graph-state pair. As we are concerned only with this graph in this section, we simply write $|\mu\nu\rangle$ for the different basis states $|G_2, \mu\nu\rangle$. Recall that $|00\rangle = 1/\sqrt{2}(|0\rangle|+\rangle + |1\rangle|-\rangle)$ (see Eq. (9)).

Alice and Bob want to share entangled pairs with high fidelity. At the beginning they are given an ensemble of noisy $|0,0\rangle$ states, each of them owning one part of the pairs. We consider a state diagonal in the graph-state basis,

$$\rho = x_{00}|00\rangle\langle 00| + x_{01}|01\rangle\langle 01| + x_{10}|10\rangle\langle 10| + x_{11}|11\rangle\langle 11|. \quad (17)$$

We remark that such a standard form can always be achieved by means of depolarization, i.e. applying certain (random) local unitary operations. Each step of the protocol consists of the following operations: (i) Alice and Bob perform unitary operations on their particles, with Alice's and Bob's unitaries given by

$$S_A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}, S_B = \frac{1}{\sqrt{2}} \text{Had} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \text{Had}^\dagger.$$

(ii) Alice performs a CNOT operation from the first state to the second and Bob from the second state to the first; (iii) Alice and Bob measure the second state in different bases. To see the effect of this procedure, we calculate the fidelity and yield obtained after one step with two initial states given by (17).

In (i), Alice and Bob apply S_A and S_B , respectively, in order to swap $|11\rangle$ and $|10\rangle$. Then, in step (ii), they apply the bilateral CNOT. One can check that the effect of this operation on the graph state basis is given by the following map:

$$|\mu_A \mu_B\rangle |\nu_A \nu_B\rangle \mapsto |\mu_A \oplus \nu_A, \mu_B\rangle |\nu_A, \nu_B \oplus \mu_B\rangle, \quad (18)$$

(Here, \oplus indicates bitwise AND, i. e. addition modulo 2.) Last (iii), Alice and Bob measure the qubits of the target state. This is done in the eigenbasis $\{|0\rangle_x, |1\rangle_x\}$ of σ_x for Alice and in the computational basis $\{|0\rangle_z, |1\rangle_z\}$, for Bob. By this they obtain the eigenvalue of the correlation operator K_2 defined in Eq. (1) and determine the value of the second bit describing the state. If it is 0, they keep the first state. They discard it otherwise.

After the measurement, they keep the control state with success probability $k = (x_{00} + x_{11})^2 + (x_{01} + x_{10})^2$ and the new coefficients are given by:

$$\begin{aligned} x'_{00} &= (x_{00}^2 + x_{11}^2)/k \\ x'_{01} &= (x_{01}^2 + x_{10}^2)/k \\ x'_{10} &= (2x_{00}x_{11})/k \\ x'_{11} &= (2x_{01}x_{10})/k. \end{aligned} \quad (19)$$

Hence, the fidelity is $F = x'_{00} = (x_{00}^2 + x_{11}^2)/k$. The yield of the step, defined as the number of remaining states divided by the number of states before the step, is given by $k/2$ as half of the states (the targets) are measured and discarded.

The unitary operations performed at the beginning of the protocol (step (i)) are required for its convergence. It guarantees that fidelity 1 is a fix point of the protocol which is approached when iterating the procedure. The CNOT operation is a means of transferring information from the first qubit to the second. The measurement allows to distinguish between $\{|0, 0\rangle, |1, 0\rangle\}$ and $\{|0, 1\rangle, |1, 1\rangle\}$ and hence, determines the second bit of the index vector.

2. Multipartite purification

Multipartite purification protocols (MEPP) have been introduced in Ref. [19] for GHZ states, were further developed in Ref. [20] and extended to all two-colorable graph states in Refs. [8, 9]. Recall that a two-colorable graph-state is a graph state in which the vertices can be separated into two sets V_A and V_B such that no edges exist between vertices of the same set. Using the procedure described in Ref. [9], one can depolarize any mixed

state ρ to the form

$$\rho = \sum_{\mu_A, \mu_B} \lambda_{\mu_A, \mu_B} |G, \mu_A, \mu_B\rangle \langle G, \mu_A, \mu_B| \quad (20)$$

without changing the diagonal coefficients (where μ_A, μ_B are binary vectors corresponding to sets V_A, V_B respectively). Hence we will restrict our attention to input states of this form. The protocol is composed of two subprotocols P1 and P2 which we will describe here:

a. Subprotocol P1: The states composing the ensemble of two-colorable graph-states are processed pairwise. All parties belonging to set V_A perform a CNOT operation from the second state of a pair of states to the first one while the parties belonging to set V_B perform a CNOT from the first one to the second one. This leads to the transformation

$$\begin{aligned} |G, \mu_A, \mu_B\rangle |G, \nu_A, \nu_B\rangle \\ \mapsto |G, \mu_A, \mu_B \oplus \nu_B\rangle |G, \nu_A \oplus \mu_A, \nu_B\rangle, \end{aligned} \quad (21)$$

As in the bipartite protocol, the last step consists of measuring the second state of the pair. The parties belonging to set V_A measure their qubit a in the eigenbasis $\{|0\rangle_x, |1\rangle_x\}$ of σ_x , obtaining results $\xi_a \in \{0, 1\}$, while the ones belonging to set V_B make their measurement in the computational basis, obtaining results $\zeta_b \in \{0, 1\}$. From this, we can calculate the part of the index vector of the measured state (second state of the r. h. s. of Eq. (21)) corresponding to set V_A :

$$\nu'_A = \nu_A \oplus \mu_A = \left(\xi_a \oplus \bigoplus_{b \in N_a} \zeta_b \right)_{a \in V_A}.$$

If this is $\mathbf{0}$, it is most likely that $\mu_A = \mathbf{0}$, and hence, the first state is kept (and otherwise discarded). As consequence, in the expansion (20) of the ensemble density matrix, elements of the form $\lambda_{\mathbf{0}, \mu_B}$ are increased. One finds that the new matrix elements are given by

$$\lambda'_{\gamma_A, \gamma_B} = \frac{1}{\kappa} \sum_{\{\nu_B, \mu_B\} | \nu_B \oplus \mu_B = \gamma_B} \lambda_{\gamma_A, \nu_B} \lambda_{\gamma_A, \mu_B} \quad (22)$$

where κ is a normalization constant such that $\text{tr}(\tilde{\rho}) = 1$.

b. Subprotocol P2: As explained above, subprotocol P1 is employed to purify with respect to the eigenvalues μ_A associated with set V_A . The second subprotocol leads to the purification with respect to the eigenvalues of set V_B . It is obtained from P1 by exchanging the roles of set V_A and V_B . The protocol's action is described by the following map:

$$\begin{aligned} |G, \mu_A, \mu_B\rangle |G, \nu_A, \nu_B\rangle \\ \mapsto |G, \mu_A \oplus \nu_A, \mu_B\rangle |G, \nu_A, \nu_B \oplus \nu_B\rangle. \end{aligned} \quad (23)$$

One measures the second state. The measurements on set V_B are done in the eigenbasis $\{|0\rangle_x, |1\rangle_x\}$ of σ_x while they are done in the computational basis in set V_A . This

leads to the determination of part μ_B of the index vector. As in subprotocol P1, one keeps the state if $\mu_B = \mathbf{0}$. The new coefficients are given by

$$\lambda'_{\gamma_A, \gamma_B} = \frac{1}{\kappa} \sum_{\{(\nu_A, \mu_A) | \nu_A \oplus \mu_A = \gamma_A\}} \lambda_{\nu_A, \gamma_B} \lambda_{\mu_A, \gamma_B} \quad (24)$$

where κ is a normalization constant such that $\text{tr}(\tilde{\rho}) = 1$, as before.

III. STRATEGIES

A. Quantum communication cost $C_{F,G}$

We now define our figure of merit, the quantum communication cost. We consider N spatially separated parties A_k , $k = 1, 2, \dots, N$ which are pairwise connected by noisy quantum channels \mathcal{E}_{kl} , described by completely positive maps acting on density operators for qubits. We will quantify the quantum communication through these quantum channels using the quantum communication cost C_{kl} , i.e. the number of usages of the quantum channel \mathcal{E}_{kl} , while classical communication between pairs of parties will be considered to be for free. Sending a single qubit through the quantum channel \mathcal{E}_{kl} costs 1 unit, i.e. $C_{kl} = 1$, while the transmission of an arbitrary state of M qubits costs $C_{kl} = M$. We will be interested in the total quantum communication cost C , where

$$C = \sum_{k < l} C_{kl}. \quad (25)$$

We consider the generation of multipartite entangled states (graph states, to be specific) $|G\rangle$ distributed among the parties A_k . The goal is to generate states $\Lambda = \bigotimes_{i=1}^L \rho_i$, where the fidelity of each ρ_i , $F_i = \langle G | \rho_i | G \rangle$, fulfills $F_i \geq F$. That is, each of the states has a fidelity larger than a threshold value F , which we call the “desired target fidelity”. We remark that we demand that the ensemble of output states are in a tensor product form. In principle, weaker requirements such as that only the reduced density operators of Λ have fidelity larger than F are conceivable, however one faces certain difficulties in this case. For instance, it is not clear whether each of the copies of the state can be independently used for further quantum information processing tasks due to possible classical correlations among the copies. Hence, we deliberately demand the tensor product structure. We will be interested in the total quantum communication cost C required to generate $\Lambda = \bigotimes_{i=1}^L \rho_i$ with $F_i \geq F$. In particular, we consider the quantum communication cost per copy,

$$C_{F,G} = \frac{C}{L}, \quad (26)$$

where one optimizes over all possible strategies to generate Λ . Due to this optimization, the quantity $C_{F,G}$ is

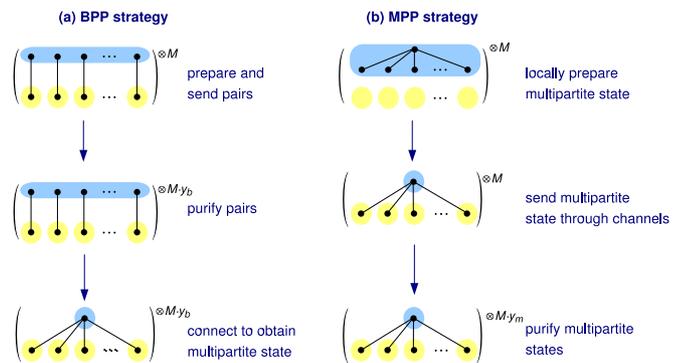


FIG. 4: (Color online.) Distribution of N -qubit GHZ states over noisy channels. (a) Bipartite entanglement purification strategy: Bell pairs are sent over the channels and purified using a BEPP. The purified pairs are then connected (using the procedure of Fig. 3) to the desired GHZ state. (b) Multipartite entanglement purification strategy: Alice prepares the GHZ state locally and sends all but one of the particles through the channels. Then, the MEPP protocol is used.

very difficult to calculate. Hence we restrict ourselves to establish upper bounds on $C_{F,G}$ by considering explicit strategies to generate high fidelity multipartite entangled states.

Multiple variations of this problem are conceivable. For simplicity we will assume that all parties are pairwise connected by identical quantum channels, $\mathcal{E} = \mathcal{E}_{kl}$. Inhomogeneous situations where only some pairs of parties are connected by quantum channels (a restricted communication web), or where the classical communication is limited, or cases where quantum channels between different pairs of parties are different (i.e. different noise parameter) will not be considered here.

We will look mainly at two scenarios depicted in Fig. 4, which we describe now.

B. Bipartite purification strategy

In the BEPP strategy, the parties A_k , $k = 1, 2, \dots, N$ wish to create a shared ensemble of N -qubit graph states of high fidelity using a BEPP, where party A_k holds the qubit corresponding to vertex a_k . For each edge of the graph, one of the two parties connected by this edge prepares a connected graph-state pair, $|G_2, 00\rangle$ (equivalent to a Bell pair up to a local unitary) and sends one qubit of the pair to the other party through a noisy channel. (Alternatively, one could use a teleportation-based strategy: Alice distributes Bell pairs to the $N - 1$ other parties. The pairs are purified and then used to distribute the multipartite state that Alice has prepared locally.) The effect of the channels is given by Eq. (13) leading to states of fidelity $F = q + \frac{1-q}{4}$ and diagonal in the graph-state basis. The parties repeat the operation M times so that at the end $M |E|$ entangled pairs are distributed

between the different partners, where $|E|$ is the number of edges in the graph. The BEPP (reviewed in Section IID 1) is then applied. This leads to a smaller ensemble of states given by a density matrix of the same form but with higher fidelity. Finally, the connection procedure described in Sec. IIA 6 is applied: Each party A_k merges together the $|N_{a_k}|$ qubits which will connect vertex a_k with its neighbors leading to the desired graph state. We call

$$Y(F) = \frac{\# \text{ final states}}{\# \text{ initial states}} = \frac{\# \text{ final states}}{M}$$

the yield of the production of final states with fidelity F . To build up the desired multipartite state $|G\rangle$, we need one $|G_2\rangle$ pair for each edge of G . The number of edges for 1D cluster and GHZ states is (as for any tree graph) $|E| = N - 1$. Hence, the quantum communication cost is related to the yield by

$$C_{F,G} = \frac{N - 1}{Y(F)}. \quad (27)$$

The numerator is the number of channel uses (i. e. number of transmitted qubits) required to distribute one state. This dependence on the size of the state properly reflects that for larger states, already the preparation of the raw states is more costly. To allow for easier comparison with the yield, a figure that may feel more familiar to the reader, we have plotted in all graphs the *inverse* communication cost $C_{F,G}^{-1} = Y(F)/(N - 1)$ which is proportional to the yield.

C. Multipartite purification strategy

Alternatively, in the MEPP strategy, a central party, called Alice, creates M N -qubit graph states locally. For each graph state, she keeps one qubit and sends the other $N - 1$ qubits through the channels to the $N - 1$ other parties. The resulting states are then purified using direct multipartite entanglement purification, i. e. the MEPP reviewed in Sec. IID 2. Hence, to distribute one state, we need $N - 1$ channel uses, the same as in the BEPP case. Thus, Eq. (27) holds for MEPP, as well.

D. Mixing of strategies

Assume that the application of, say, m steps of one of the protocols mentioned above reaches a final fidelity F_1 with a communication cost of C_1 , and application of $m+1$ steps achieves fidelity $F_2 > F_1$ with communication cost $C_2 > C_1$ (i. e. $Y_2 < Y_1$). For a certain application, a fidelity of F with $F_1 < F < F_2$ is required, i. e. m steps are insufficient, but $m+1$ steps achieve a higher fidelity than desired at the cost of lower yield. In this case, one can find a compromise between the two strategies by mixing ensembles:

Choosing an $\alpha \in [0, 1]$, one prepares M raw states and then uses the first strategy on αM of them in order to gain $\alpha M Y_1$ states of fidelity F_1 , and the second strategy on the remaining $(1 - \alpha)M$ states to obtain $(1 - \alpha)M Y_2$ states of fidelity F_2 . Mixing these states gives an ensemble of fidelity

$$F = \frac{\alpha Y_1 F_1 + (1 - \alpha) Y_2 F_2}{\alpha Y_1 + (1 - \alpha) Y_2} \quad (28)$$

with a yield $Y = \alpha Y_1 + (1 - \alpha) Y_2$. This method allows one to obtain intermediate fidelities with a better yield. The communication cost mixes according to

$$\frac{1}{C} = \frac{\alpha}{C_1} + \frac{1 - \alpha}{C_2}. \quad (29)$$

E. Intermediate strategies

As a ‘‘compromise’’ between BEPP and MEPP, we shall also consider the following set of strategies: Assemble small states of N_1 qubits, send them through the channels, purify them, and then use the connection scheme described in Sec. IIA 6 to connect L of the N_1 -qubit states to one state with $N = L N_1 - L + 1$ qubits.

IV. NUMERICAL SIMULATIONS

A. Technique

In generic cases, an explicit numerical simulation of a quantum systems is intractable due to the exponential growth of the Hilbert space with the number of involved particles or qubits. In our case, however, an efficient simulation is possible for two reasons: (i) All gates that are employed by the protocols are elements of the so-called Clifford group and hence, the Gottesman-Knill theorem applies, which allows for efficient simulations of pure state evolutions. (ii) The considered noise channels have Kraus representations that are diagonal in the Pauli basis.

To explain (i), we start by reviewing the Gottesman-Knill theorem [21, 22]. It says that it is possible to simulate so-called stabilizer circuits efficiently on a classical computer. These are quantum circuits containing only preparation of computational basis states, operations from the Clifford group, and measurements in the computational basis. The N -qubit Clifford group \mathcal{C}_N is the group of those unitary operations that map Pauli operators onto Pauli operators under conjugation, i. e.

$$\mathcal{C}_N := \{U \in SU(2^N) \mid U P U^\dagger \in \mathcal{P}_N \quad \forall P \in \mathcal{P}_N\}, \\ \mathcal{P}_N := \{\pm 1, \pm i\} \cdot \{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}^{\otimes N}. \quad (30)$$

It happens to contain all the operations that we need for purifying, and hence, we can simulate the execution of the purification protocols described in Section IID.

Aaronson and Gottesman have given a fast algorithm which can perform such a simulation, and also supplied an implementation in the C programming language [23]. We have used this software at the beginning of our studies, but after realizing that its performance is not sufficient for our purposes, developed a new, faster algorithm, which is described elsewhere [24].

The state represented in our simulator is always a pure state (Footnote [25]). However, in entanglement purification, one usually deals with mixed states, represented as density matrices. Nevertheless, due to the fulfillment of condition (ii), we can get around this problem using a Monte Carlo technique, which we describe now.

To represent the ensembles of states we start with a high number N_i of qubits, typically several thousand times the number of qubits in the states to be purified. The qubits are initialized to a tensor product of $|G, \mathbf{0}\rangle$ states. Note that all these qubits can potentially get entangled, and hence have to be part of the same simulated quantum register. This would be prohibitive without a very efficient algorithms for the stabilizer simulation.

We then simulate all steps that are required to prepare Bell pairs or graph states, to purify them and to measure them. Depending on the measurement results, states are kept or discarded. Several iterations of the protocols are simulated.

The transmission through the perfect channels amount to a simple relabeling: The program remembers the new site, where the qubit resides, as this indicates which qubits can be subject of joint operations.

Simulating the channel noise is done by randomizing over many simulation runs as follows. The three noisy channels that we have considered, Eqs. (11-13), are simulated using a pseudo-random number generator (RNG). Whenever noise is to be applied onto a qubit, a random number between 0 and 1 is generated, and if it is smaller than $(1 - q)$ (the noise level), σ_x (σ_z) is applied for bit-flip (phase-flip) noise. For depolarizing noise, the RNG is used again to obtain an integer between 1 and 4 which determines which of the operators $\mathbb{1}, \sigma_x, \sigma_y, \sigma_z$ to apply.

After the preparation of M initial states, m iterations of the protocol and for the BEPP case, connection of the purified pairs, N_f final states remain. The yield is then given by $\tilde{Y} = \frac{N_f}{M}$. This is, however, not a good estimate for the asymptotic yield in the limit of infinite ensembles for the following reason: If the number N_{i-1} of states at the beginning of purification step i is odd, we have to discard one state, because we can only deal with pairs of states. Hence, we better estimate the yield by

$$Y = \frac{N_1}{\lfloor\lfloor M \rfloor\rfloor} \cdot \frac{N_2}{\lfloor\lfloor N_1 \rfloor\rfloor} \cdot \dots \cdot \frac{N_f}{\lfloor\lfloor N_{m-1} \rfloor\rfloor} \quad (31)$$

(with $M \equiv N_0$, $N_f \equiv N_m$, and $\lfloor\lfloor N \rfloor\rfloor = N$ for even N , and $\lfloor\lfloor N \rfloor\rfloor = N - 1$ for odd N .)

The fidelity can be determined by measuring the final states in the graph basis. This is because all the intended operations and the random noise operations map graph states onto graph states, so that all N_f final states are of

the form $|G, \boldsymbol{\mu}\rangle$. The index $\boldsymbol{\mu}$ can be determined as follows: For each state, the graph state creation operation of Eq. (2), $\prod_{\{a,b\} \in E} \Lambda Z^{(ab)}$ (which is Hermitian) is applied again onto the state. If one then applies Hadamard gates on all qubits and measures in the σ_z basis, the measurement results spell out the index vector $\boldsymbol{\mu}$. As we intended to create $|G, \mathbf{0}\rangle$ states, we call the number of states for which we measured $\mathbf{0}$ the number N_g of ‘‘good’’ states and hence estimate the fidelity as

$$F = \frac{N_g^{\text{tot}}}{N_f^{\text{tot}}} \pm \sqrt{\frac{N_g^{\text{tot}}(N_f^{\text{tot}} - N_g^{\text{tot}})}{(N_f^{\text{tot}})^3}}.$$

The superscript ‘‘tot’’ indicates that many runs of the simulations are made and that the numbers are the sums of the numbers in the individual runs. The uncertainty term follows from the expectation that, given a true fidelity F_T , the number of good states N_g^{tot} output by the Monte Carlo simulations after many runs is distributed according to a binomial distribution with length N_f^{tot} , hit probability F_T and hence standard deviation $N_f^{\text{tot}} \sqrt{F_T(1 - F_T)}$. Thus, $\frac{N_g}{N_f}$ is the estimate for F_T with the given statistical uncertainty at 1σ level.

In the same way, the yield can be assigned an uncertainty, (Footnote [26])

$$Y = \frac{N_f^{\text{tot}}}{M^{\text{tot}}} \pm \sqrt{\frac{N_f^{\text{tot}}(M^{\text{tot}} - N_f^{\text{tot}})}{(M^{\text{tot}})^3}}.$$

The 1σ uncertainties are indicated by error bars in the plots.

B. Extremal strategies

We now present the results obtained for the two extremal strategies described in Secs. IIIB and IIIC with the following parameters: The distribution of the qubits is done through noisy channels and each step of protocol requires imperfect two-qubit operations. The noise considered is depolarizing noise as defined in Eq. (13) with reliability $p = 0.9$ (10% noise) for the channels and $p_l = 0.99$ (1% noise) for the local operations. We used the Monte-Carlo simulation method described in Sec. IVA to reach a precision on the fidelity varying from 1‰ to 1% depending on the size of the states and the number of iterations.

For the MEPP case, one has to decide, which sequence of the sub-protocols P1 and P2 to use. The alternating sequence, P1-P2-P1-..., turns out to be not optimal in terms of yield and fidelity, neither for GHZ nor for cluster states. To find the optimum, one might hence consider to simulate, after each step, both sub-protocols, and then continue with the better one. Somewhat surprisingly, this leads to worse results (see Fig. 5). Thus, to find the optimal sequence of m protocol-steps, one would need to try all 2^m possibilities. As this is not practical,

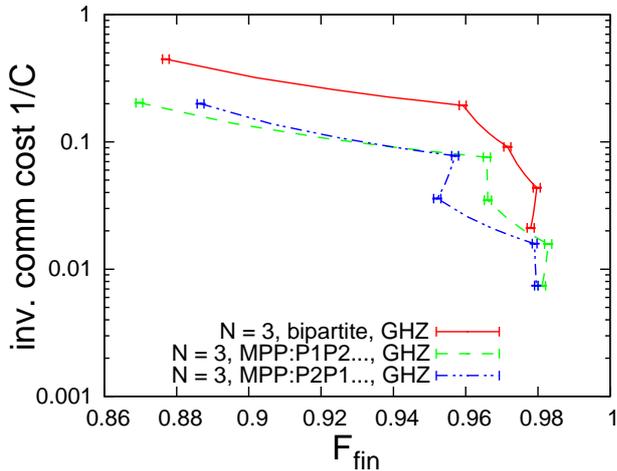


FIG. 5: (Color online.) Comparison of the values of inverse of communication cost and fidelity obtained after a number of steps varying from 1 to 5 for 3-qubit GHZ states. The red solid line stands for the BEPP strategy, the green dashed line for the alternating sequence of MEPP subprotocols beginning with P1 and the blue small dashed line for the alternating sequence beginning with P2.

we decided to stick with the alternating sequence, which turned out, though it is not optimal, to give very descent performance. For GHZ states, there is also a difference between the alternating sequences P1-P2-P1-... and P2-P1-P2-..., due to the asymmetry of the sets V_A (containing only Alice's qubit) and V_B (containing the rest). Starting with P1 works better, and this is what we use in all plots discussed in this section.

1. GHZ states

We start with the results obtained for GHZ states. We made our simulations for states of three to 10 qubits and a maximum number of steps varying from 5 to 7. As an example, Fig. 6 shows the quantum communication cost as a function of desired fidelity for 5-qubit GHZ states. The data points are the outputs for 1 to 6 steps of the protocol. This plots allow us to determine, for a given fidelity, the strategy which will give the best yield (lowest communication cost).

After 6 iterations, the increase in fidelity obtained by an additional step is smaller than the chosen precision of 1%. We therefore take this value as estimate of the maximum reachable fidelity. A comparison of the maximal reachable fidelity for both strategies as a function of the number of parties (Fig. 7a) shows that the maximal reachable fidelity is higher in the MEPP case for a number of parties strictly smaller than 10. In this case, there is a transition value of target fidelity from which on the MEPP strategy gives a better yield. We will refer to the value pair of fidelity and communication cost, where this transition happens, as the cross-over point. Fig. 8

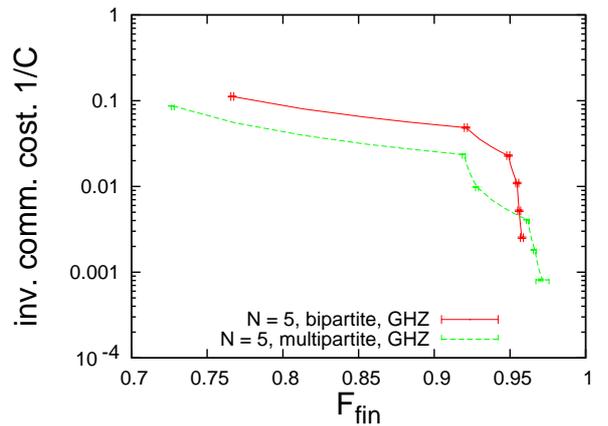


FIG. 6: (Color online.) Inverse of communication cost for different target fidelities for 5-qubit GHZ states and with $p = .9$ and $p_i = .99$ (where p is the reliability defined in Eq. (14)). The data points are the outputs for 1, 2, ..., 6 iterations of the protocol. The connecting lines are obtained by mixing ensembles of different fidelities according to Eq. (29). The red solid line gives the obtained value in the MEPP and the green dashed line for the BEPP. The gain on fidelity from one step to the other becomes smaller at each step. From 6 to 7 steps, the gain in fidelity is smaller than the uncertainty both in the BEPP and in the MEPP strategy. We consider this value as the maximal reachable fidelity.

presents the yield as function of fidelity for $N = 3$ and $N = 10$ as well as the cross-over points for intermediate number of parties. $N = 9$ is the highest number of qubits for which there is a cross-over point. For higher number of parties, the BEPP strategy is always better. This is because of the fragility against noise of GHZ states for large particle numbers [27, 28]. The communication cost and fidelity of the cross-over points as function of the number of parties are presented in Fig. 9a.

2. Cluster states

Next, we did simulations cluster states using the same parameter as for the GHZ states. The results are quite different.

We made our simulations for states of three to fifteen qubits. In this range, as one can see in Fig. 10, there is always a cross-over point. This is in stark contrast with the GHZ case. This main difference in behavior between this two kind of states is due to the much higher robustness of cluster states against noise [27, 28]. Moreover, the range of target fidelity for which the multipartite strategy is the only one available increases with the number of parties as shown in Fig. 7b. In Fig. 9b, we present the fidelity and communication cost of the cross-over point. Both values decrease with the number of parties. This is due to the increasing cost of producing bigger and bigger states and also to the fact that we consider here the global fidelity and not the LNE presented in Sec. II C.

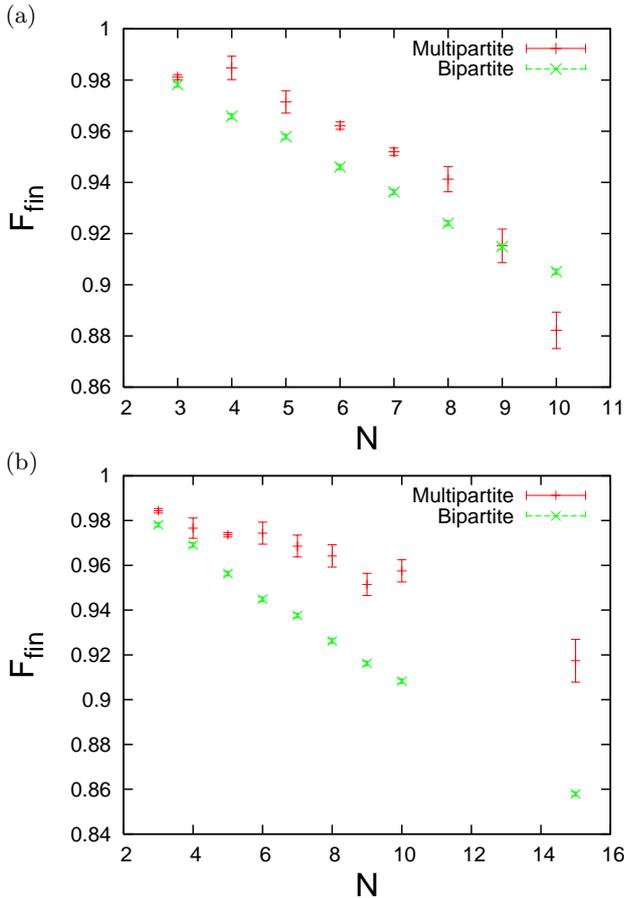


FIG. 7: (Color online.) Maximal reachable fidelity as function of N for (a) GHZ and (b) cluster states for the bipartite (green \times) and multipartite (red bars) strategies with reliabilities (cf. Eq. (14)) $p = 0.9$ for channel transmission and $p_l = 0.99$ for local operations. The final fidelity is estimated as follows: For a given number of parties, we iterated the protocol as long as we obtained an increase of fidelity larger than the uncertainty (typically 1%). We took the last value as maximal fidelity and assigned its uncertainty to the maximal reachable fidelity. The green crosses give the values in the bipartite case while the red bars give it for the multipartite case. One sees here the main difference in behavior between GHZ and cluster states. In the first case, there is a range where the multipartite strategy is better than the bipartite one for a number of parties strictly smaller than 10. For more parties, the multipartite protocol fails because of the fragility of GHZ states against noise. On the other hand, the robustness of cluster states allow us to purify them even for a large number of parties. The range of fidelity where MEPP is superior increases with the number of parties.

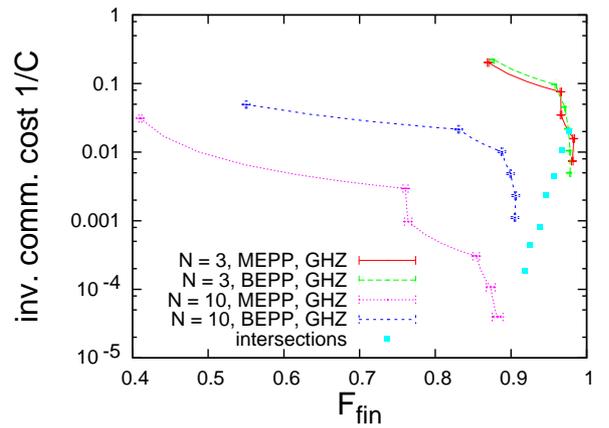


FIG. 8: (Color online.) Inverse of communication cost for different target fidelities of GHZ states of 3 to 10 qubits with alteration probabilities (as in Fig. 7) $1 - p = 0.1$ and $1 - p_l = 0.01$. The dashed green line stands for 3-qubit GHZ states and BEPP strategy, the red solid line for 3-qubit GHZ states and MEPP strategy, the blue small-dashed line for 10-qubit GHZ states and BEPP strategy, the pink dotted line for 10-qubit GHZ states and MEPP strategy. The blue squares give the cross-over points, i.e. the fidelity where MEPP becomes more efficient than BEPP, for $N = 3, 5, 6, 7, 8$ and 9. For $N = 3$ and $N = 10$, the purification curves are plotted as well. For $N = 3$, they cross at the corresponding blue square.

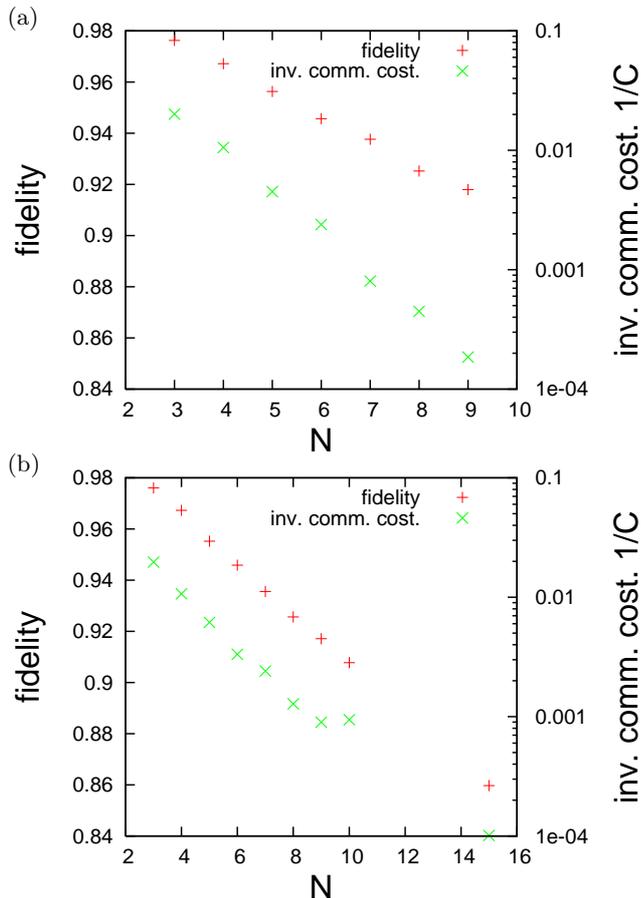


FIG. 9: (Color online.) Inverse of communication cost (green \times) and fidelity (red +) of the cross-over depending on the number of parties for (a) GHZ and (b) cluster states. This values are obtained by using the Monte Carlo method and are therefore submitted to errors. The cross-over indicates the range of target fidelity from which up the MEPP strategy is more efficient than the BEPP strategy. Note the log scale for the inverse of communication cost. In the GHZ case, there is no cross-over for more than 9 parties.

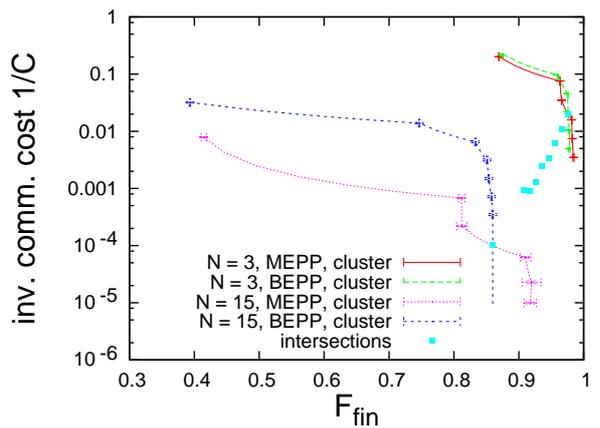


FIG. 10: (Color online.) Inverse of communication cost for different target fidelities for 3 (red solid line for MEPP and green dashed line for BEPP) and 15 (pink dotted line for MEPP and blue small dashed line for BEPP) qubit cluster states. The data points are the outputs for 1, 2, 3, ... iterations of the protocol. The intermediate points are obtained by mixing ensembles of different fidelities. For more than 6 steps, the difference between the reached fidelity and the maximum reachable fidelity is smaller than the uncertainty. For any number of parties, the curves representing the two strategies cross over. The disks give this cross-over for $N = 3, 4, 5, 6, 7, 8, 9, 10, 15$. (That one curve seems to “go back” is just an artifact of the statistical inaccuracies of the Monte Carlo method.)

Mn	prepare an n -qubit cluster or GHZ state
B2	prepare a Bell pair
S	send the states through the channels
P1	apply multipartite purification protocol P1
P2	apply multipartite purification protocol P2
Pb	apply bipartite protocol
$C\ell$	connect ℓ states to a larger one

TABLE I: Legend for the instruction strings in Figs. 11 and 12.

C. Intermediate strategies

Since switching from BEPP to MEPP can result in such striking differences in yield, one might expect that, especially near the break-even point, certain intermediate strategies, mixing characteristics of BEPP and MEPP, might perform even better. After all, in the BEPP case, one purifies small states (with only 2 qubits) and then connects them, while in the MEPP scenario, the states are first connected to large units, which are then purified. One can also connect pairs to states of intermediate size, purify these, connect them to the desired full size, and perhaps purify again. This can be seen e. g. in Fig. 11. In this figure, we have simulated many different strategies which are described in short by instruction strings which are processed from left to right and tell the software in which order which preparations, transmissions, connections or purifications should be simulated (cf. Table I).

It can be seen that for low fidelities and high yields (left side of the plots), the BEPP case is best, as already seen above, and for high fidelities and low yields (right margin of the plots), MEPP catches up. In the middle region, one may indeed increase the performance by first preparing small states of, say, 4, 5 or 7 qubits, purifying them, and then connecting them to the desired 13-qubit state. (Do not get confused by the appearance of “M13-S” at the left margin. This looks like MEPP, but is not, as it contains no purification at all. Also note that there is a subtle difference between using the BEPP protocol (denoted “B2-S-Pb-...”) and using the MEPP protocol on the $|G_2\rangle$ state (denoted “M2-S-P1-...” or “M2-S-P2-...”), with the former performing better.)

Of course, only discrete ways of assembling the desired states from equal smaller states are available. Recall that connecting L states of n qubits will give a state of

$$N = Ln - (L - 1) \quad (32)$$

qubits because $(L - 1)$ qubits have to be measured in the connection process. In the plots, we have taken all possible values of L for the given state size n and calculated data points for the corresponding strategies with up to four purification steps. The blue curve in the plot marks the optimum that can be achieved using these strategies, and mixing them as described in Section III D.

To demonstrate the efficiency of our procedure, we also considered purification of cluster states of 31 qubits (Fig. 12). In order to allow for easier comparison, Fig.

12, as well as Fig. 11, show a regauging of the fidelity axis to the so-called local noise equivalent (LNE) described in Sec. II C.

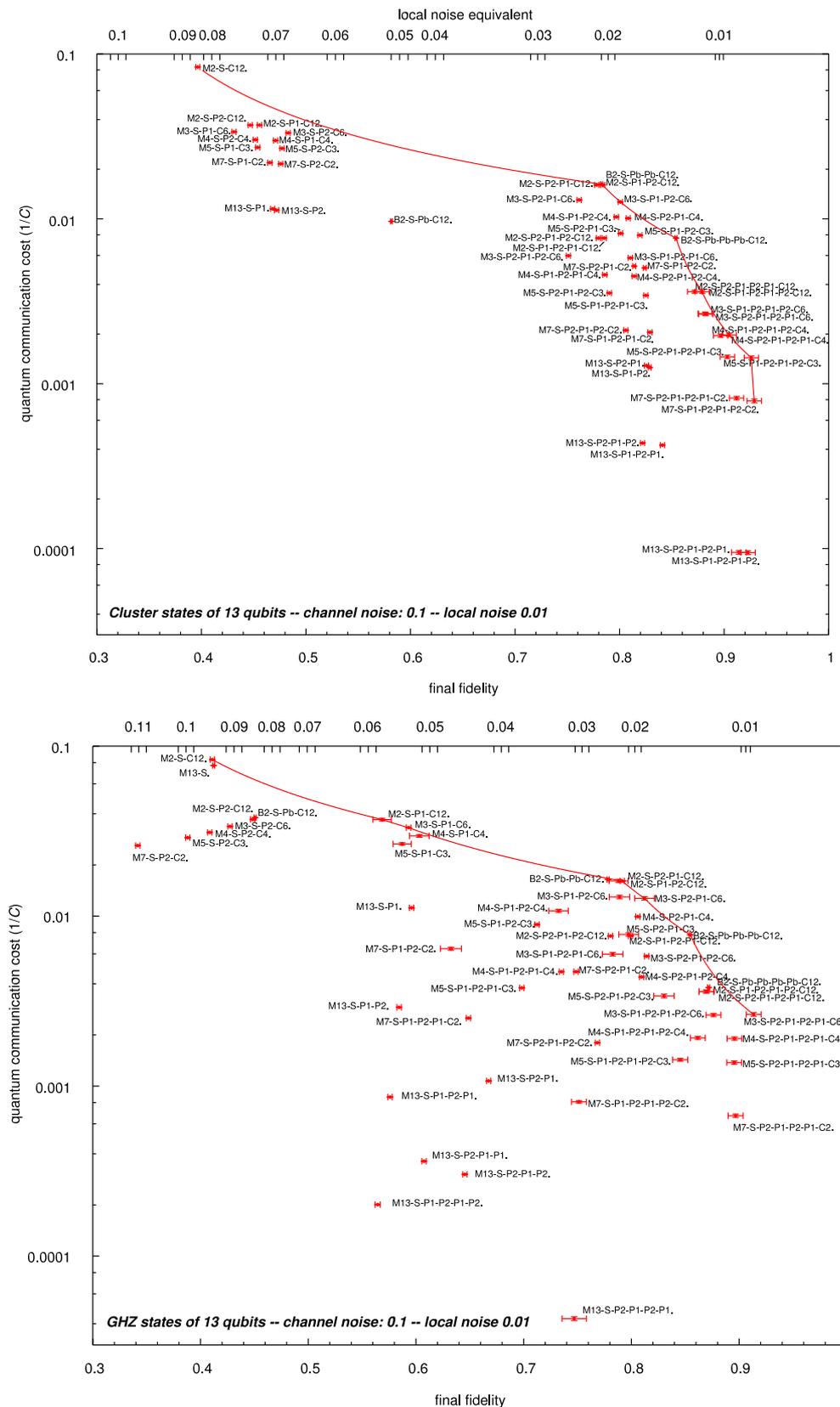


FIG. 11: (Color online). Examples for the use of intermediate purification strategies, here for 13-qubit (a) cluster and (b) GHZ states. Plotted is the inverse of communication cost as function of final fidelity. See Table I for the meaning of the instruction strings. The blue curve marks the maximal achievable yield for a given desired fidelity and is obtained by connecting the optimal strategies with curves according to Eq. (28). Noise levels are $(1 - q) = 0.1$ for the channels and $(1 - q_l) = 0.01$ for local operations. In (a), one can –following the dark blue line– see well, how for small target fidelity BEPP (“M2-S-...”) gives the best yield, while for high fidelities ($F \gtrsim 0.9$), distributing larger and larger states becomes advantageous. (For even higher fidelities, one expects the full MEPP strategy, i. e. “M13-S-...”, to appear on the blue curve. However, this will happen at communication costs larger than the scales shown on the plot, which ends with “M13-S-P1-P2-P1”, i. e. MEPP with only three purification steps.) In (b), the picture is not as clear, at the GHZ states already start to deteriorate under the given level of local noise.

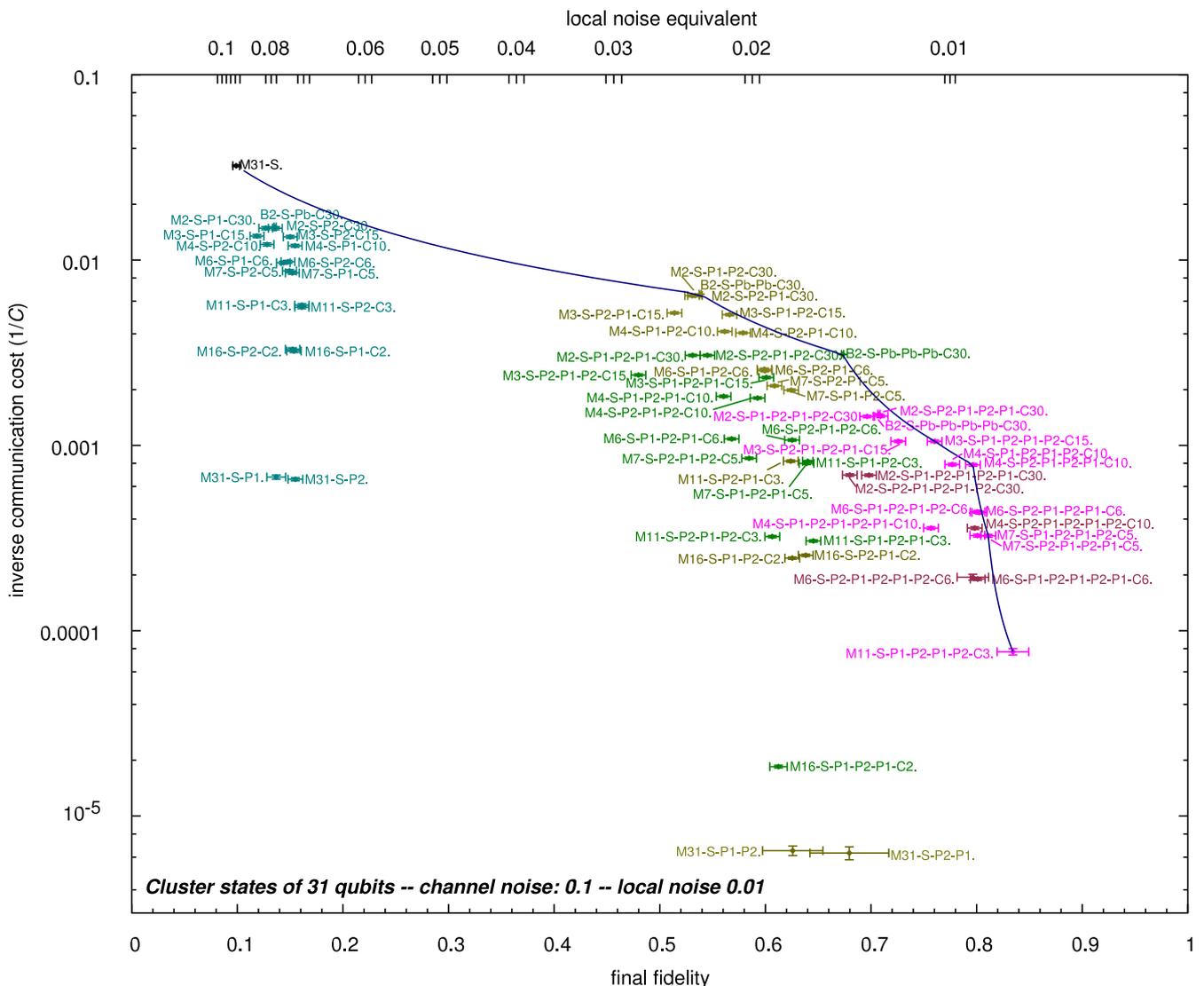


FIG. 12: (Color online). Production of 31-qubit cluster states, using intermediate strategies. The “instruction strings” are explained in Table I. Data points with the same number of purification steps are plotted in the same color. Note how the distribution of initially larger states becomes advantageous for higher target fidelities. Noise levels are $(1 - q) = 0.1$ for the channels and $(1 - q_l) = 0.01$ for local operations. (Note also that the data points at the low end of the plot have few purification steps: Those steps beginning with “M16” or “M31” that should appear on the curve of optimal strategies are again, as in Fig. 11, beyond the range of the plot.)

V. ANALYTICAL TREATMENT FOR A SIMPLIFIED MODEL

For a better understanding of the numerical results, we now develop an analytical treatment for both BEPP and MEPP. To make this task feasible we have to restrict ourselves to a simplified noise model. We only consider GHZ states.

As before, we define two sets V_A and V_B corresponding to the bi-coloration of the graph. V_A is the set containing only one qubit, namely the central vertex which is connected to all the others, and V_B contains the rest.

In the toy models presented below, the central party,

called Alice wants to share an N -qubit GHZ state with $(N - 1)$ partners. Depending on the strategy, the initial states are either Bell pairs or GHZ states, which are noisy due to the transmission through the channels. First, in Subsection V A, we consider local operations to be perfect. We will see that this fails to reproduce features seen in the numerical results. Hence, we extend our model, in Section V B, such that it incorporates local noise.

A. Perfect local operations

To start, we assume to local operations to be perfect. Of the channels we considered in Eqs. (11-13), only bit-flip channels and phase-flip channels allow for a simple analytical treatment. We present the calculation for phase-flip channels. The calculation and the results for bit-flip channels are very similar. We have hence not included them in the paper.

1. BEPP strategy

Following the BEPP scenario described in Sec. III B, Alice sends one qubit of each entangled pair $\rho = |G_2; 0, 0\rangle\langle G_2; 0, 0|$ of her initial ensemble through the channel to party B_k , obtaining

$$\rho = q|G_2; 0, 0\rangle\langle G_2; 0, 0| + (1 - q)|G_2; 0, 1\rangle\langle G_2; 0, 1|.$$

She then applies the BEPP. The state of the pairs that are kept after one step is given by (see Eq. 19)

$$\rho = \frac{q^2}{q^2 + (1 - q)^2} |G_2; 0, 0\rangle\langle G_2; 0, 0| + \frac{(1 - q)^2}{q^2 + (1 - q)^2} |G_2; 0, 1\rangle\langle G_2; 0, 1|. \quad (33)$$

In this step, the probability of keeping the source state after the measurement of the other state is given by $k^{\text{BEPP}}(q, 1) = q^2 + (1 - q)^2$ (probability of having same measurement outcomes). We denote by $f^{\text{BEPP}}(q, m)$ the fidelity after m steps. The quantity $k(q, m)$ is called success probability in step m . Note that the ratios of the ensemble sizes after and before the step is given by $k(q, m)/2$ as one half of the states are measured and discarded. One obtains the total yield Y^{BEPP} after m steps by multiplying these ratios for the individual steps. By iterating the protocol over m steps one finds:

$$f^{\text{BEPP}}(q, m) = \frac{q^{2^m}}{q^{2^m} + (1 - q)^{2^m}}, \quad (34)$$

$$k^{\text{BEPP}}(q, m) = \frac{q^{2^m} + (1 - q)^{2^m}}{[q^{2^{m-1}} + (1 - q)^{2^{m-1}}]^2}, \quad (35)$$

$$Y^{\text{BEPP}}(q, m) = \prod_{i=1}^m \frac{k(q, i)}{2} = \frac{q^{2^m} + (1 - q)^{2^m}}{2^m \prod_{i=1}^{m-1} (q^{2^i} + (1 - q)^{2^i})}. \quad (36)$$

After the bipartite purification, Alice connects $(N - 1)$ pairs to produce an N -qubit GHZ state. To connect two pairs, she applies a controlled phase gate (Eq. (3)) followed by a σ_y measurement on one of the two qubits just connected (cf. Fig. 3). This procedure is repeated $(N - 1)$ times between different pairs of parties (A, B_k) ,

$k = 1, \dots, N - 1$, in order to obtain the N -qubit GHZ state.

Note that the qubits that Alice connects have not been sent through channels and are hence unaffected by channel noise. Thus, it does not matter whether we first apply the superoperator for the channel noise and then the one for the local noise due to the connection process, or *vice versa*. This means that the final state is obtained by applying noise on all qubits of the GHZ state that do not belong to Alice. This leads to a fidelity

$$F^{\text{BEPP}}(N, q, m) = f^{\text{BEPP}}(q, m)^{N-1}$$

and (as the channels are used $N - 1$ times to create one N -qubit GHZ state) a quantum communication cost

$$C^{\text{BEPP}} = \frac{N - 1}{Y^{\text{BEPP}}(q, m)}.$$

2. MEPP strategy

In the MEPP setting, Alice prepares an N -qubit GHZ state locally and distributes it through depolarizing channels to her $(N - 1)$ partners. We then have the state

$$\rho^{(0)} = \left(\prod_{a=2}^N \mathcal{E}_z^{(a)} \right) |G_*; 0, \mathbf{0}\rangle\langle G_*; 0, \mathbf{0}|, \quad (37)$$

where $\mathcal{E}_z^{(a)}$ is the phase-flip channel defined in Eq. (11). We shall from now on suppress the symbol G_* which indicates the N -vertices star graph of Fig. 2.

We shall see that all states that we encounter have the form

$$\begin{aligned} \rho^{(m)} = & r_0^{(m)} |\mathbf{0}\rangle\langle \mathbf{0}| + \\ & + r_1^{(m)} \sum_{i_1=2}^N |0, \dots, 0 \overset{i_1}{\downarrow} 1 \dots 0\rangle\langle 0, \dots, 0 \overset{i_1}{\downarrow} 1 \dots 0| + \\ & + r_2^{(m)} \sum_{\substack{i_1, i_2=2 \\ i_1 < i_2}}^N |0, \dots, 0 \overset{i_1}{\downarrow} 1 \dots 0 \overset{i_2}{\downarrow} 1 \dots\rangle\langle 0, \dots, 0 \overset{i_1}{\downarrow} 1 \dots 0 \overset{i_2}{\downarrow} 1 \dots| + \\ & + \dots + r_{N-1}^{(m)} |0, 11 \dots 1\rangle\langle 0, 11 \dots 1|, \quad (38) \end{aligned}$$

where $r_j^{(m)}$ denotes the coefficient in front of the terms with j entries “1” after the m th step of the purification protocol. These states are diagonal in the graph state basis and symmetric w. r. t. permutations of the qubits in set V_B . They are hence characterized by only N coefficients $r_0^{(m)}, \dots, r_{N-1}^{(m)}$.

We start by carrying out the application of the superoperator in Eq. (37). Indeed, one obtains a mixture of the form (38) with coefficients

$$r_j^{(0)} = q^{N-1-j} (1 - q)^j. \quad (39)$$

As only set V_B is affected by the noise, subprotocol P2 is sufficient to purify the state. Following [9], one

sees that after each step of the subprotocol, the state is changed such that each coefficient becomes proportional to the square of its former value, i. e.

$$r_j^{(m)} = \frac{[r_j^{(m-1)}]^2}{\sum_{i=0}^{N-1} \binom{N-1}{i} [r_i^{(m-1)}]^2}. \quad (40)$$

Inserting Eq. (39), one gets for the first step (using the binomial theorem)

$$r_j^{(1)} = \frac{q^{2(N-1-j)}(1-q)^{2j}}{[q^2 + (1-q)^2]^{N-1}},$$

and iterating the formula, one finds

$$r_j^{(m)} = \frac{q^{2^m(N-1-j)}(1-q)^{2^m j}}{[q^{2^m} + (1-q)^{2^m}]^{N-1}}.$$

The fidelity of the state at step m can now be read off:

$$F^{\text{MEPP}}(N, q, m) = r_0^{(m)} = \left[\frac{q^{2^m}}{q^{2^m} + (1-q)^{2^m}} \right]^{N-1}.$$

Note that this is the same expression as we got before for the BEPP: $F^{\text{MEPP}}(N, q, m) = F^{\text{BEPP}}(N, q, m)$.

To calculate the yield, we need the success probability $k^{\text{MEPP}}(N, q, m)$ that a state is kept. Using a similar argument as we did for Eq. (40) we find

$$\begin{aligned} k^{\text{MEPP}}(N, q, m) &= \sum_{i=0}^{N-1} \binom{N-1}{i} [r_i^{(m-1)}]^2 \\ &= \left(\frac{q^{2^m} + (1-q)^{2^m}}{[q^{2^{m-1}} + (1-q)^{2^{m-1}}]^2} \right)^{N-1}. \end{aligned}$$

From this, we can find the yield as before

$$\begin{aligned} Y^{\text{MEPP}}(N, q, m) &= \prod_{i=1}^m \frac{k^{\text{MEPP}}(N, q, i)}{2} \\ &= 2^{-m} \left(\frac{q^{2^m} + (1-q)^{2^m}}{\prod_{i=1}^{m-1} [q^{2^i} + (1-q)^{2^i}]^2} \right)^{N-1} \end{aligned} \quad (41)$$

Comparing to the BEPP case, one sees that

$$Y^{\text{MEPP}}(N, q, m) = 2^{m(N-2)} [Y^{\text{BEPP}}(N, q, m)]^{N-1}. \quad (42)$$

3. Conclusion

In the particular case of dephasing channels and perfect local operations, both strategies lead to the same fidelity after iterating the protocol the same number of steps. However, they differ in the communication cost.

As one sees from Eq. (42), the yield of the MEPP strategy is always lower (and the communication cost hence larger). This fact can be explained from the higher probability of throwing away states at each step, which even increases further with the number of parties.

We have also done analytical calculations for bit-flip channels (Eq. (11)) and numerical simulations for depolarizing channels (Eq. (13)) (always in case of perfect local operations) and found a similar behavior.

In order to see regions where MEPP is superior as we did with the Monte Carlo simulations, it is hence necessary to give up the simplification of assuming noiseless local operations.

B. Imperfect local operations

If local operations are not assumed to be perfect, results are quite different. We again consider GHZ states of arbitrary size, to be purified with the BEPP or MEPP strategy.

For the noise, we define a model which is simple enough to allow for analytical calculations but still shows the general features obtained numerically (especially it shows cross-over points): The channel through which Alice sends qubit to the other parties is the phase-flip channel of Eq. (11) with alteration probability $(1-q)$. The imperfection of the local gates are modeled by bit-flip noise (Eq. (12)), for Alice's operations, and phase-flip noise for all other parties, always with alteration probability $(1-ql)$.

1. MEPP strategy

As before, Alice prepares perfect N -qubit GHZ state and distributes them using the channels. We get the same initial state $\rho^{(0)}$ as before, again of the form (38) with coefficients as in Eq. (39). We shall see that, again, the form (38) is preserved by the purification steps even though they are now assumed to be noisy.

The values of the r_i are changed according to a linear map:

$$r_j^{(m)} = \sum_{k=0}^{N-1} \Lambda_{jk} r_k^{(m-1)}.$$

We shall construct this map in two steps. First, we see, how the phase-flip noise of the local gates acting on the qubits in V_B ,

$$\prod_{i=2}^N \mathcal{E}_z^{(i)}(ql), \quad (43)$$

changes the coefficients and denote the map corresponding to this action by λ :

$$r'_j = \sum_{k=0}^{N-1} \lambda_{jk} r_k^{(m-1)}.$$

Then, we consider the action of the bit-flip noise on Alice's qubit get the full map Λ .

For the first step, we call a state $|G_*, \boldsymbol{\mu}\rangle$ a k -state, if $\boldsymbol{\mu}$ starts with a 0 (for the central qubit in V_A) and contains, within the indices corresponding to V_B , k entries "1" and $(N-1-k)$ entries "0". We can now calculate the probability $p_{j \leftarrow k}$ that the superoperator (43) changes a pure k -state to any j -state: Say, s of the k entries "1" are flipped to "0". Then $\bar{s} = j - k + s$ of the $(N-1-k)$ entries "0" have to be flipped to "1". Hence,

$$p_{j \leftarrow k} = \sum_{s=0}^k \binom{k}{s} (1-q_l)^s q_l^{k-s} \times \binom{N-1-k}{\bar{s}} (1-q_l)^{\bar{s}} q_l^{N-1-k-\bar{s}}. \quad (44)$$

There are $\binom{N-1}{j}$ j -states and $\binom{N-1}{k}$ k -states, and so

$$\lambda_{jk} = \frac{\binom{N-1}{k}}{\binom{N-1}{j}} p_{j \leftarrow k},$$

which can also be written in terms of Gauß's hypergeometric function F as

$$\lambda_{jk} = \frac{j!}{k!(j+k)!} \times F\left(\frac{(1-q_l)^2}{q_l^2}; -k, j-N+1, j+k+1\right) \times (1-q_l)^{j-k} q_l^{N-1-j+k} \quad (45)$$

Now, we can do the second step and apply the noise for the imperfection of Alice's local gates, modeled by $\mathcal{E}_x^{(1)}(q_l)$. We get, due to Eq. (6),

$$r_j^{(m)} = q_l r'_j + (1-q_l) r'_{N-j} = \sum_{k=0}^{N-1} \Lambda_{jk} r_k,$$

where

$$\Lambda_{jk} = \frac{\binom{N-1}{k}}{\binom{N-1}{j}} \sum_{s=0}^k \binom{k}{s} \times \left[\binom{N-1-k}{j-k+s} q_l^{N-1-j+k-2s+1} (1-q_l)^{j-k+2s} + \binom{N-1-k}{j-s} q_l^{N-1-j-k+2s} (1-q_l)^{j+k-2s+1} \right]. \quad (46)$$

The fidelity and the yield corresponding to one step of protocol can then be calculated:

$$f(N, q, q_l, m) = \frac{\left[r_0^{(m)} \right]^2}{\sum_{k=0}^{N-1} \binom{N-1}{k} \left[r_k^{(m)} \right]^2} = \frac{\left(\sum_{j=0}^{N-1} \Lambda_{0j} r_j^{(m-1)} \right)^2}{\sum_{k=0}^{N-1} \binom{N-1}{k} \left(\sum_{j=0}^{N-1} \Lambda_{kj} r_j^{(m-1)} \right)^2}$$

As before, the denominator of the previous expression is the success probability $k(N, q, q_l, m)$ of the step m (Footnote [29]), and we get the total yield $Y^{\text{MEPP}}(N, q, q_l, m)$ by multiplying up the factors $k/2$ of all m steps:

$$Y^{\text{MEPP}}(N, q, q_l, m) = \prod_{i=1}^m \frac{k(N, q, q_l, i)}{2}$$

(For the corresponding quantum communication cost, Eq. (27) has to be used.)

2. BEPP strategy

Next, we find an analytical treatment for the BEPP strategy. In order to facilitate the calculation, we will consider the BEPP as a special case of the MEPP. We first show why this is possible without changing the results:

Considering the restricted noise model presented in this Section, the state can always be written as a contribution of $|G_2; 0, 0\rangle\langle G_2; 0, 0|$ and $|G_2; 0, 1\rangle\langle G_2; 0, 1|$ only. It can hence be purified using only subprotocol P2. In addition, the only difference between the BEPP protocol as described in Sec. IID 1 and subprotocol P2 is the exchange of the states $|G_2; 1, 0\rangle$ and $|G_2; 1, 1\rangle$ in the former, and not in the latter. As these states have no contribution in the present model, the two protocols give identical results.

The results obtained in the last section can be used to calculate the fidelity $f(q, q_l, m)$ and the yield $Y^{\text{BEPP}}(q, q_l, m)$ before connection. After purification, Alice connects qubits a_1, \dots, a_{N-1} of $(N-1)$ pairs described by the states $\rho_k = q|G_2\rangle_k\langle G_2| + (1-q)\sigma_z^{(b_k)}|G_2\rangle_k\langle G_2|\sigma_z^{(b_k)}$ respectively. The joint state of the pairs is given by

$$\rho = q^{N-1} \left(\bigotimes_{k=1}^{N-1} |G_2\rangle_k\langle G_2| \right) + (1-q) q^{N-2} \sum_{i=1}^{N-1} \sigma_z^{(b_i)} \left(\bigotimes_{k=1}^{N-1} |G_2\rangle_k\langle G_2| \right) \sigma_z^{(b_i)} + \dots + (1-q)^{N-1} \left(\prod_{i=1}^{N-1} \sigma_z^{(b_i)} \right) \left(\bigotimes_{k=1}^{N-1} |G_2\rangle_k\langle G_2| \right) \left(\prod_{i=1}^{N-1} \sigma_z^{(b_i)} \right).$$

The connection is performed using the procedure described in Sec. IIA 6. As the noise contains only σ_z operators, it commutes with the projectors and correction operators that are used in this procedure. The state after

projection is given by

$$\begin{aligned}
P_2 \rho &= q^{N-1} |G_*\rangle \langle G_*| \\
&+ (1-q) q^{N-2} \sum_{b=2}^N \sigma_z^{(b)} |G_*\rangle \langle G_*| \sigma_z^{(b)} + \dots + \\
&+ (1-q)^{N-1} \left(\prod_{b=2}^N \sigma_z^{(b)} \right) |G_*\rangle \langle G_*| \left(\prod_{b=2}^N \sigma_z^{(b)} \right).
\end{aligned}$$

It follows that after the connection, the fidelity is given by

$$F^{\text{BEPP}} = f(q, q_l, m)^{N-1}$$

and the quantum communication cost by

$$C^{\text{BEPP}} = \frac{N-1}{Y^{\text{MEPP}}(2, q, q_l, m)}.$$

3. Discussion

The results obtained the way just explained are presented in Figs. 13, 14, and 15, always for MEPP and BEPP.

The cross-over points, i. e. the fidelity values (and corresponding costs) above which MEPP performs better than BEPP, are plotted as blue squares in Fig. 13 for up to 70 parties. We have also plotted the fidelity-cost function for selected numbers N of parties, which cross in their respective blue squares. The other cross points were determined in the same way by observing where the MEPP and the BEPP curve intersect. Compare this figure with Fig. 8: Our analytical toy model could reproduce the appearance of cross points which we had already discussed in Section IV B 1, an essential feature observed for the more general noise model. It does not, however, reproduce the fact that a cross-over ceases to appear above a certain number (here: 9) of parties. This fact is due to the particular kind of noise of our toy model under which GHZ states appear less fragile than under depolarizing noise so that the break-down of MEPP for large states does not happen.

We can use our analytic model to explore the parameter space more thoroughly. For instance, one might be interested how the positions of the cross points change if the local noise is increased. This is shown in Fig. 14 where the right-most curve is the same as the disks in Fig. 13 and the others are for higher local noise levels. Observe how the effect of local noise depends more and more on the state size as its level approaches the order of magnitude of the channel noise.

The vertical tails of the curves in Fig. 13 already allow to easily read off the maximum reachable fidelity, which is plotted in Fig. 15. There, the advantage of MEPP over BEPP increases with the number of parties. This effect can also be seen in the numerical calculations for depolarizing noise (Fig. 7a). In the latter case, it is, however, soon overcome by the competing effect of the break-down of MEPP under realistic (depolarizing) noise.

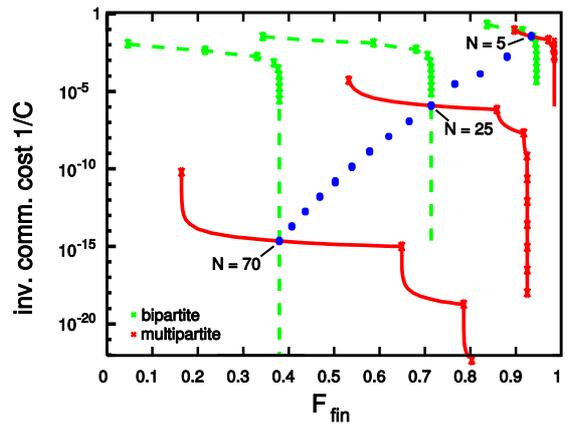


FIG. 13: (Color online.) Inverse of communication cost as function of final fidelity for the simplified noise model used in section VB. Analytical calculation for GHZ states of different number of qubits N varying from 5 to 70, with alteration probability for the channel and local noise of $(1-q) = 0.1$ and $(1-q_l) = 0.05$ respectively. The green dashed lines stand for MEPP strategy while the red solid lines stand for BEPP strategy. The blue circles give the crossing points for all number of parties between 5 and 70.

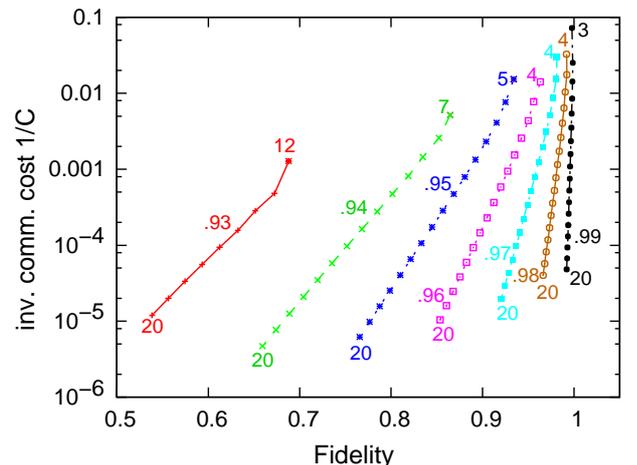


FIG. 14: (Color online.) Analytical results for different number of parties and different amount of local noise. Each curve gives the yield as function of fidelity for the cross-over for a given alteration probability $(1-q_l)$ (See Eq. (11) and (12)). This parameter varies from $q_l = 0.93$ (left curve) to $q_l = 0.99$ (right curve).

C. Testing the numerics

The analytical formulas are also very useful for verifying the code of our numerical calculations. Switching the programs from depolarizing noise to the simplified noise considered here is a trivial alteration. We find that the numerical results agree well with the analytics, see Fig. 16 to 17. This fact makes us confident in the correctness of our codes.

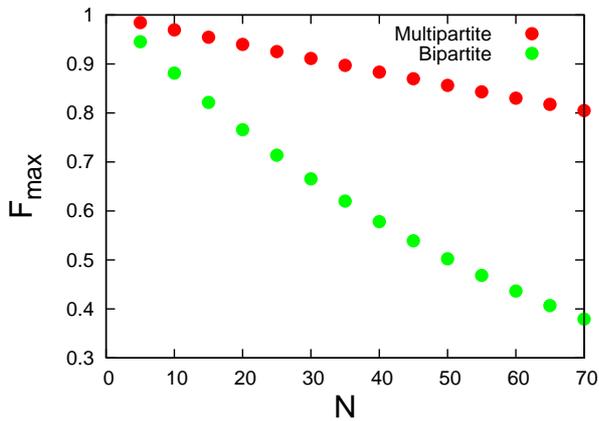


FIG. 15: (Color online.) Maximal reachable fidelity F_{max} plotted against the number of parties for the simplified model described in Sec. VB applied to GHZ states. The alteration probability for the channels and the local noise are given by $(1 - q) = 0.1$ and $(1 - q_l) = 0.01$ respectively. The results were obtained analytically.

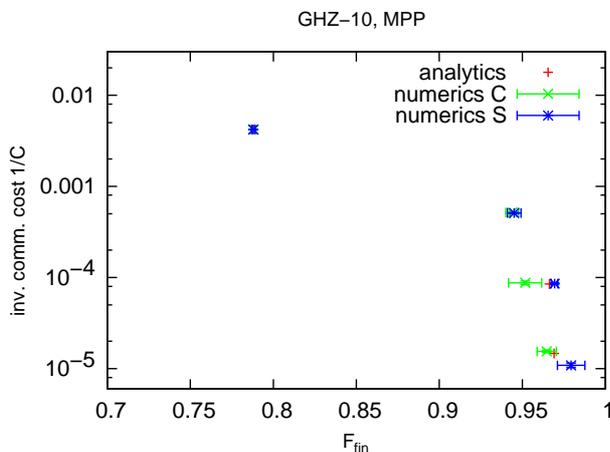


FIG. 16: (Color online.) Testing the numerics: We switched the programs that were used to calculate the results of section IV B (program C) and section IV C (program S) to the simplified noise model of section VB. The plot shows the inverse of communication cost as function of the final fidelity. The red symbols (+) stand for the analytical results while the green (x) and the blue (*) symbols stand for the output of program C and program S respectively. The error bars stand for 1σ errors. A comparison with the derived analytical formulas shows satisfactory agreement. The calculation was done for MEPP of GHZ-states with 10 qubits (b) at noise levels $q = 0.9$ and $q_l = 0.95$.

VI. SUMMARY AND CONCLUSIONS

In this article, we have investigated the quantum communication cost of preparing a class of multipartite entangled states with high fidelity. The presence of noisy quantum channels and imperfect local control operations requires the usage of error correction or—in our case—entanglement purification schemes to achieve this aim.

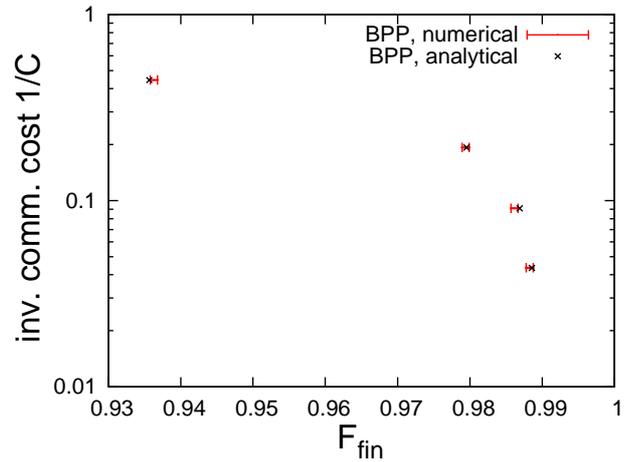


FIG. 17: (Color online.) Testing the numerics obtained for the BEPP strategy. Noisy entangled pairs, arising from sending one of the qubits through a depolarizing channel, are purified using the BEPP. The plot shows the inverse of communication cost as function of final fidelity. The black crosses give the exact values while the red bars give the numerical results of the Monte-Carlo simulation.

We have considered various strategies to generate these high-fidelity states and have established in this way upper bounds on the quantum communication cost. The optimal strategy strongly depends on the error parameters for channels and local control operations, and on the desired target fidelity. For a simple error model and the generation of GHZ states based on various strategies, we have obtained analytic results that allow us to compare these strategies. Numerical simulations for generic error models, based on Monte Carlo simulation, show essentially the same features as observed in the simplified model. The simulation makes use of a recently developed method that allows one to efficiently simulate the evolution of stabilizer states (or graph states) under Clifford operations on a classical computer [23, 24]. We have also applied this method to investigate not only the generation of GHZ states but also of other types of multipartite entangled states, e.g. cluster states.

We find that for high target fidelities, strategies based on multipartite entanglement purification generally perform better than strategies based on bipartite purification. For low target fidelities, strategies based on bipartite purification have a higher efficiency, leading to smaller communication cost.

We believe that the generation of high-fidelity multipartite entangled states is of significant importance in the context of (distributed) quantum information processing. Such multipartite entangled states represent resources, e. g. for measurement-based quantum computation, conference key agreement and secret sharing schemes, and may be used for other security tasks. Our investigation takes both channel noise and noisy apparatus into account. We could show that the choice of a proper strategy not only allows one to significantly reduce the quantum

communication cost, but to reach fidelity of target state that are not accessible otherwise.

Acknowledgments

This work was supported in part by the Austrian Science Foundation (FWF), the Deutsche Forschungs-

gemeinschaft (DFG), the European Union (IST-2001-38877, -39227, OLAQUI, SCALA). W. D. is supported by project APART of the ÖAW. The numerical calculations have been carried out on the Linux compute cluster of the University of Innsbruck's Konsortium Hochleistungsrechnen.

-
- [1] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999); Kai Chen, and Hoi-Kwong Lo, quant-ph/0404133.
- [2] C. Crépeau, D. Gottesman, and A. Smith: *Secure multi-party quantum computation*, Proceedings of 34th Annual ACM Symposium on Theory of Computing, Montreal, Canada. ACM, 2002, pp. 643 – 652. (see also E-print quant-ph/0206138).
- [3] D. J. Wineland, J. J. Bollinger, W. M. Itano, F. L. Moore, and D. J. Heinzen, Phys. Rev. A **46**, R6797 (1992); D. J. Wineland, J. J. Bollinger, W. M. Itano, and D. J. Heinzen, Phys. Rev. A **50**, 67 (1994); S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac, Phys. Rev. Lett. **79**, 3865 (1997).
- [4] R. Raussendorf, D. E. Browne, and H.-J. Briegel, Phys. Rev. A **68**, 022312 (2003).
- [5] E. Knill and R. Laflamme, quant-ph/9608012 (1996).
- [6] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
- [7] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
- [8] W. Dür, H. Aschauer, and H. J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).
- [9] H. Aschauer, W. Dür, and H. J. Briegel, Phys. Rev. A **71**, 012319 (2005).
- [10] H. Barnum, E. Knill, and M. A. Nielsen, IEEE Trans. Info. Theory **46**, 1317 (2000).
- [11] W. Dür, J. I. Cirac, and P. Horodecki, Phys. Rev. Lett. **93**, 020503 (2004).
- [12] A. R. Calderbank, and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
- [13] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
- [14] Mathematical literature prefers to call such graphs *bi-partite* but we reserve this term to denote operations or settings comprised of two different sites (locations).
- [15] M. Hein, J. Eisert and H. J. Briegel, Phys. Rev. A **69** 062311 (2004).
- [16] F. Verstraete, and J. I. Cirac, Phys. Rev. A **70** 060302(R) (2004).
- [17] W. Dür, M. Hein, J. I. Cirac, and H. J. Briegel, Phys. Rev. A **72**, 052326 (2005)
- [18] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [19] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, R4075 (1998).
- [20] E. N. Maneva and J. A. Smolin, in *Quantum Computation and Quantum Information*, edited by J. Samuel and J. Lomonaco, Vol. **305** of AMS Contemporary Mathematics (American Mathematical Society, Providence, RI, 2002); e-print quant-ph/0003099.
- [21] D. Gottesman, quant-ph/9807006.
- [22] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
- [23] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
- [24] S. Anders and H. J. Briegel, quant-ph/0504117, accepted for publication in Phys. Rev. A.
- [25] There is an algorithm for simulation the evolution of a rather restricted class of mixed states [23], which is however not general enough for our purposes.
- [26] To be precise, we should calculate the uncertainty not from $Y = \frac{N_f}{M}$, but following Eq. (31). This simplification is however justified, as it only increases the uncertainty estimate, and this only slightly.
- [27] W. Dür and H. J. Briegel, Phys. Rev. Lett. **92**, 180403 (2004).
- [28] M. Hein, W. Dür, and H. J. Briegel, Phys. Rev. A **71**, 032350 (2005).
- [29] Note that Λ is dependent on m although we have suppressed this to keep notation simple.

