Graph State Quantum Repeater Networks

Michael Epping,* Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, D-40225 Düsseldorf, Germany

We show how general graph states, an important resource state for multipartite quantum protocols, can be distributed over large distances using intermediate repeater stations. To this aim we describe a one way quantum repeater scheme using encoding in the language of graph states. For a general Calderbank-Shor-Steane (CSS) code we do a refined error analysis that allows to correct qubit errors and erasures caused by imperfect preparation, gates, transmission, detection, etc.. We analyze the cost and the repeater rate for this general scheme. The concept is exemplified by the 7-qubit Steane code and the quantum Golay code.

PACS numbers: 03.67.Dd,03.67.Bg,03.67.Pp

I. INTRODUCTION TO QUANTUM REPEATERS

Signals in long distance telecommunications are subject to corruptions. Typically the amplitude decreases exponentially with the covered distance. Thus intermediate repeaters which amplify and purify the signal are necessary building blocks for reliable transmission. In quantum cryptography and quantum communication the signals carry coherent quantum information.

One possibility to overcome the exponential scaling of losses with distance is the entanglement swapping and -distillation based repeater scheme, which was developed by H.-J. Briegel et al. in [1]. Here entangled pairs are distributed amongst neighboring repeater stations and Bell measurements on each station result in entangled states covering a larger distance (so-called entanglement swapping). These operations introduce errors which can be tackled by entanglement distillation, i.e. protocols that concentrate several imperfect copies of entangled states into a single copy with higher fidelity with respect to a maximally entangled state. Two-way classical communication is used to acknowledge reception of photons.

A different approach, introduced by L. Jiang et al. in [2], replaces the entanglement distillation step by the use of quantum error correction codes that allow for forward error correction, i.e. communication is only required in one direction. In comparison to the previous schemes these improve the repeater rate at the cost of being more demanding in terms of resources and the quality of operations. Subsequent work considered different codes and improved the error analysis [3–7].

II. A REPEATER NETWORK BASED ON GRAPHS

In the talk we present the scheme that we described in [8]. Our scheme generalizes error correction based repeater schemes to networks, over which a multipartite entangled state is distributed amongst several parties. This generalization naturally arises from our use of the graph state formalism [9]. We briefly introduce graph states, which are states associated with mathematical graphs, such that each vertex corresponds to a qubit and each edge to an entangling gate acting on these two linked vertices. Given a mathematical graph $G = (V, E)$, where V is a set of vertices and $E \subset V \times V$ a set of edges, the corresponding graph state $|G\rangle$ is

$$|G\rangle = \prod_{(i,j)\in E} C_Z^{(i,j)} |+\rangle^{\otimes N}, \tag{1}$$

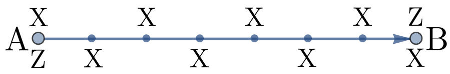
where C_Z is the controlled-phase gate and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The state $|G\rangle$ is the (unique) common eigenstate to the eigenvalue $+1$ of the operators

$$g_i = X_i \prod_{\substack{j\in V\\(i,j)\in E}} Z_j, \qquad i = 1, ..., N, \tag{2}$$

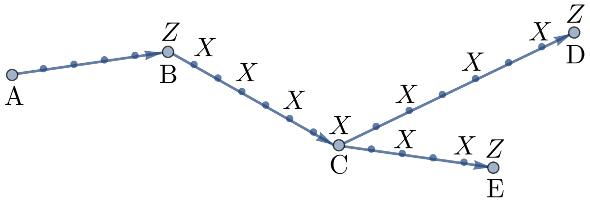
the generators of the stabilizer of $|G\rangle$ (X_i and Z_i are Pauli operators for vertex i).

In our scheme a repeater network corresponds to a (logical) graph state and each party or repeater station is associated with a vertex (see Figure 1). Measuring the qubit on each repeater station in the X-basis effectively erases the vertices from the graph projecting the shared state of the parties to the desired graph state (up to byproduct operators that depend on the measurement outcomes). This can be seen from the N "main stabilizers" of the network. The main stabilizer S_i centered on party i consists of an X-operator on its qubit and chains of X-operators on every second qubit leading to a Z operator on the neighboring parties (this is possible for an even number of repeater stations on each line, odd numbers lead to the same result up to a local basis

* epping@hhu.de



(a) The basic building block of repeaters linking two parties. The upper and lower operators form the main stabilizer centered on A and B, respectively.



(b) Example of a multipartite repeater network. The shown operators belong to the main stabilizer centered on C.

FIG. 1: The state corresponding to the graph of the large vertices is obtained up to byproduct operators, when all the repeater stations (small vertices) are measured in the X-basis. Arrowheads indicate transmission directions.

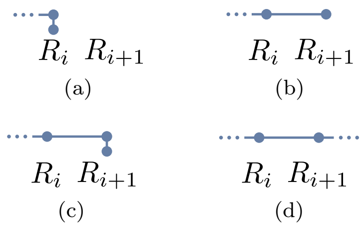


FIG. 2: The operations on repeater stations R_i and R_{i+1}. The preparation and the gate of station R_i (a) and the transmission of the qubit produced at R_i to R_{i+1} (b) creates the edge $(i, i+1)$, where the same procedure is repeated to create the next edge (c,d).

change), see Figure 1. Thus measuring the repeater qubits in the X-basis projects onto a state stabilized by the generators of the graph state associated with the graph where the repeater vertices have been erased.

Let us consider the basic building block of such networks, a line of repeater stations corresponding to a line graph with N vertices numbered from 1 to N. The first and the last qubit is in possession of Alice and Bob, respectively. The edges of the graph state are created by the following steps (see Figure 2). The edge $(i, i+1)$ is created locally at the repeater station i: the qubit $i+1$ is prepared in the (logical) $|+\rangle$-state and processed by a C_Z gate entangling it with qubit i (which was received from station $i-1$). Afterwards it is send to the station $i+1$. Here the same procedure repeats to create the edge $(i+1, i+2)$.

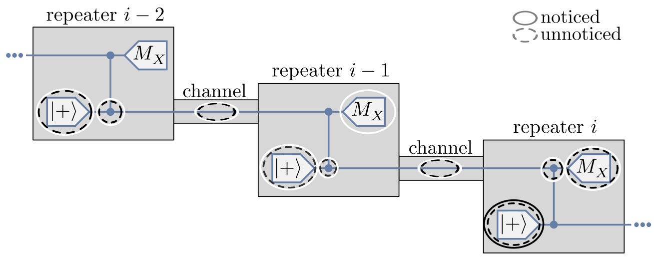


FIG. 3: The circuit for creating the graph state. Encircled processes can lead to an error on the qubit measured at repeater i. Solid and dashed lines denote unnoticed and noticed errors, respectively. Black circle errors lead to a flip of the measurement outcome. The outcome will be marked as ? if any white circle error occurred.

III. SHIFT TO LOGICAL GRAPH STATES USING CSS CODES

We employ an error model, in which corrupted qubits, including lost ones, are set to the completely mixed state. There is a convenient equivalent viewpoint that corruptions in the circuit are randomly occurring discrete X or Z errors, i.e. these operators are inserted into an otherwise perfectly working circuit [10, 11].
The corresponding circuit diagram helps to identify all possible errors that flip the measurement outcome at station i, when one pays attention to the propagation of errors by C_Z gates (see Figure 3). An X error on the control qubit before the gate is transformed into an X error on the control qubit plus a Z-error on the target, which flips its X-measurement outcome. Z-errors in turn do not spread. Even numbers of flips cancel each other and thus the physical error rate f_q is the probability to have an odd number of errors in the encircled processes.
Because the information is encoded into a bigger quantum system with redundancy using a Calderbank-Shor-Steane (CSS) code, a certain amount of errors is correctable. CSS codes are an important subclass of stabilizer codes, for which it is possible to write the generators of the stabilizer of the code space each solely with X *or* Z operators. They have the favorable property that controlled-Phase gates can be implemented transversally (qubitwise) up to a logical basis change on one of the two qubits. This implies that the previous analysis of error propagation directly transfers to the logical C_Z gate.
In absence of errors the measurement outcomes are codewords of the employed code, so a classical decoder is used for error correction. The additional information of noticed errors (like heralded losses) can be used to improve the error correction, i.e. it can allow to correct more errors. The logical error rate $\bar{f}_q$ of a repeater station, i.e. the probability that the decoder cannot correct the errors in the (classical) data, can be

estimated from the effective bit-flip and erasure rates f_q and f_l.
The logical errors propagate to the parties via the application of the byproduct operators. Odd numbers of errors on one main stabilizer lead to the production of a state that is orthogonal to the intended one, decreasing the corresponding fidelity. The formulas for the calculation that we just sketched can be found in [8].

IV. DISCUSSION OF THE RESULTS

The derivation of the final state is done analytically and independently of the employed CSS code. To our knowledge this is the first full error analysis of repeaters with general CSS codes in the sense that losses and operational errors are taken into account.
We calculated the probabilities of errors on the final graph state for several CSS codes, separations of the parties and gate qualities. From these rates we can directly calculate the secret key rate of a quantum key distribution protocol (e.g. BB84 [12]). We judge different codes by a cost function introduced by S. Muralidharan et al. in [7]. It is the total number of qubits per secret key rate and total distance. Here we want to mention the following results. Already the popular 7-qubit-Steane code allows to beat a transmission line without any repeaters for low gate error rates of approximately $f_G = 10^{-4}$. While this gate quality is clearly demanding, the number of seven (flying) qubits per repeater station is very low compared to other schemes in the literature (e.g. [4, 7]), so this code might be interesting for proof-of-principle experiments.
For gate errors $\lesssim 0.1\%$ (and distances that are meaningful on earth) the 23-qubit-Golay code performs remarkably well, such that it might even be unnecessary to go to larger codes for the time being. In this regime it is the most cost-efficient code as far as we can assess. Unfortunately, the repeater spacing is limited to very small distances, which is an obstacle until the required components can be made cost- and space-saving. This seems to be a general challenge for quantum repeaters with encoding. In our case the repeater spacings are in the order of a kilometer. However, one should keep in mind, that despite the large number of repeater stations, the cost is relatively low, because different repeater schemes with larger repeater separations need a large number of parallel transmission lines to achieve the same rates.

V. OUTLOOK

Given the formula for the secret key rate it will be interesting to model errors of different experimental setups and to optimize over the code as well as the parameters of the repeater scheme such as the number of repeater stations. Further research might focus on proof-of-principle experiments, e.g. of multipartite quantum communication protocols or conference key agreement in small networks without trusted nodes. Furthermore improvements from the theoretical side can be expected when optimizing the protocol over the possible abortion strategies (on specific loss patterns).

[1] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[2] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Phys. Rev. A **79**, 032325 (2009).
[3] W. Munro, K. Harrison, A. Stephens, S. Devitt, and K. Nemoto, Nat. Phot. **4**, 792 (2010).
[4] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg, Phys. Rev. Lett. **104**, 180503 (2010).
[5] N. K. Bernardes and P. van Loock, Phys. Rev. A **86**, 052301 (2012).
[6] W. Munro, A. Stephens, S. Devitt, K. Harrison, and K. Nemoto, Nat. Phot. **6**, 777 (2012).
[7] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014).
[8] M. Epping, H. Kampermann, and D. Bruß, ArXiv e-prints (2015), arXiv:1504.06599 [quant-ph].
[9] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
[10] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Series on Information and the Natural Sciences (Cambridge University Press, 2000).
[11] D. Lidar and T. Brun, *Quantum Error Correction* (Cambridge University Press, 2013).
[12] C. Bennett and G. BRassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing , 175 (1984).