

## Large-scale quantum networks based on graphs

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2016 New J. Phys. 18 053036

(<http://iopscience.iop.org/1367-2630/18/5/053036>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 37.187.129.166

This content was downloaded on 04/06/2016 at 11:15

Please note that [terms and conditions apply](#).



## PAPER

## Large-scale quantum networks based on graphs

## OPEN ACCESS

## RECEIVED

10 February 2016

## REVISED

22 April 2016

## ACCEPTED FOR PUBLICATION

3 May 2016

## PUBLISHED

26 May 2016

Original content from this work may be used under the terms of the [Creative Commons Attribution 3.0 licence](#).

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.



Michael Epping, Hermann Kampermann and Dagmar Bruß

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, D-40225 Düsseldorf, Germany

E-mail: [epping@hhu.de](mailto:epping@hhu.de)**Keywords:** quantum information, quantum repeaters, quantum networks, graph states, quantum error correction, quantum communication**Abstract**

Society relies and depends increasingly on information exchange and communication. In the quantum world, security and privacy is a built-in feature for information processing. The essential ingredient for exploiting these quantum advantages is the resource of entanglement, which can be shared between two or more parties. The distribution of entanglement over large distances constitutes a key challenge for current research and development. Due to losses of the transmitted quantum particles, which typically scale exponentially with the distance, intermediate quantum repeater stations are needed. Here we show how to generalise the quantum repeater concept to the multipartite case, by describing large-scale quantum networks, i.e. network nodes and their long-distance links, consistently in the language of graphs and graph states. This unifying approach comprises both the distribution of multipartite entanglement across the network, and the protection against errors via encoding. The correspondence to graph states also provides a tool for optimising the architecture of quantum networks.

**1. Introduction**

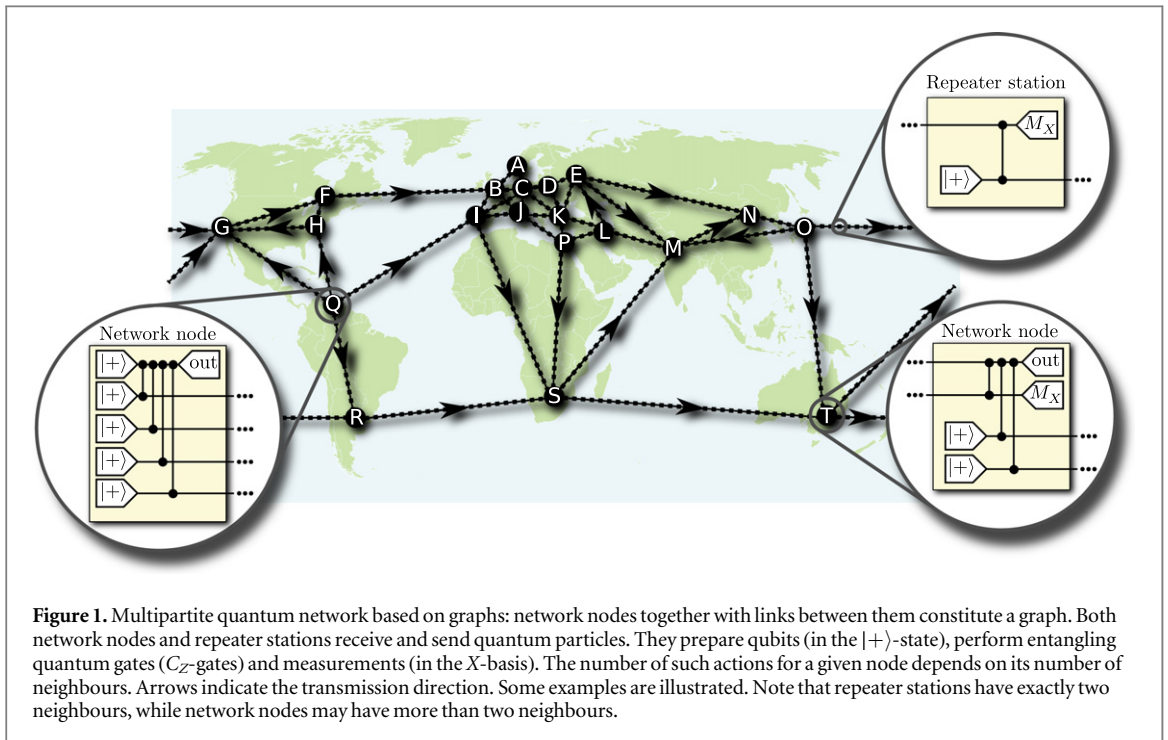
Quantum entanglement is one of the pillars of quantum information processing. Distribution of entanglement among two or more spatially separated parties is a necessary ingredient for many tasks in quantum information theory, including distributed quantum computing [1], blind quantum computing [2], teleportation [3], telecloning [4], secret sharing [5] and quantum cryptography schemes [6–8]. Multipartite entanglement enables a violation of Bell inequalities that grows exponentially with the number of parties [9]. However, the controlled distribution of entanglement, in particular of multipartite entanglement, over long distances is a major challenge, due to unavoidable imperfections such as particle losses and decoherence.

The seminal idea of quantum repeaters [10, 11] is based on the distribution of short-range entanglement between intermediate repeater stations (thus avoiding losses that grow typically exponentially with the distance) and subsequent entanglement swapping, which connects the short links along a line to long-range bipartite entanglement. Several theoretical variations have been proposed: some of them are based on entanglement distillation [12–14] and others are based on forward error correction [15–18]. Much experimental progress towards the realisation of a quantum repeater has been made [19–25].

‘Partially quantum’ networks are considered in the so-called trusted node scenario [26], while fully quantum networks have been investigated in the context of network routing [27–30] and coding [31–33] strategies and heterogeneous network technologies [34].

Here we propose a general multipartite quantum network architecture, where the long-distance links are bridged by quantum repeater stations. This idea is illustrated in figure 1 for the long-term vision of a ‘world-wide quantum web’. This network contains nodes (labelled by letters), which receive, measure and send particles. They could be located at, e.g., key institutions. Network nodes are connected by long-distance transmission channels, which are subdivided into shorter channels by an appropriate number of quantum repeater stations—an example is also shown in figure 1. The geometry of these links is general. In particular it is not restricted to regular lattices.

Any network such as in figure 1 forms a mathematical graph by identifying the network nodes with vertices and the quantum channels with edges. To any graph a corresponding graph state can be associated [35, 36]. These states are highly entangled and constitute a valuable resource, e.g. for one-way quantum computation [35–39]. In our proposal



**Figure 1.** Multipartite quantum network based on graphs: network nodes together with links between them constitute a graph. Both network nodes and repeater stations receive and send quantum particles. They prepare qubits (in the  $|+\rangle$ -state), perform entangling quantum gates ( $C_Z$ -gates) and measurements (in the  $X$ -basis). The number of such actions for a given node depends on its number of neighbours. Arrows indicate the transmission direction. Some examples are illustrated. Note that repeater stations have exactly two neighbours, while network nodes may have more than two neighbours.

the goal is to establish a multipartite entangled graph state between the network nodes, which constitutes a general resource that is required for many quantum information protocols, including the ones mentioned at the beginning.

This goal is reached in two steps. Step 1: a graph state is produced, where *both* the network nodes and the repeater stations constitute vertices. Step 2: the vertices corresponding to the repeater stations are ‘removed’ by appropriate measurements. It is important to note that no memories are needed at the repeater stations, as the measurements can be performed immediately, as will be explained in more detail below. We remark that not all quantum states are graph states. Thus not all multipartite quantum states can be obtained directly via our proposal.

In order to deal with unavoidable errors, for example photon losses in fibres or in the atmosphere, quantum error correction will be used, i.e. the nodes and repeater stations will process higher-dimensional encodings of physical qubits; we will use stabiliser codes throughout this paper.

As the same language of stabilisers is used for both the encoding and the target states, our scheme of a global quantum repeater network is concise and general.

## 2. From graphs to quantum repeater networks

A mathematical graph  $G$  consists of a set  $V$  of  $N$  vertices and a set  $E$  of edges, each of which connects two vertices, i.e.  $E \subset V \times V$ . In figure 1, the network nodes as well as the repeater stations are vertices, and all transmission channels between them are edges of a graph. To each mathematical graph  $G$  corresponds a graph state  $|G\rangle$ , which can be defined in two equivalent ways. First, a graph state can be physically produced by switching on a specific entangling gate for each edge of the graph. Concretely,  $|G\rangle$  is the state that is created from the state  $|+\rangle^{\otimes N}$ , with  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ , by applying a controlled-phase gate  $C_Z$  to each pair  $(i, j)$  of vertices in  $E$ , i.e.

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

where in the computational basis  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$  the entangling gate reads  $C_Z = \text{diag}(1, 1, 1, -1)$ .

Second, a graph state is the unique state which is eigenstate of a set of so-called stabiliser operators, with eigenvalues  $+1$ . Each vertex  $i$  of the graph has an associated stabiliser operator  $g_i$  which is a product of the Pauli- $X$  operator for vertex  $i$  and the Pauli- $Z$  operator for all its neighbours, i.e.  $g_i$  reads

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

Here,  $X_i$  is a short-hand notation for the Pauli operator  $X$  acting on vertex  $i$  and the identity  $\mathbb{1}$  at all other vertices. The graph state  $|G\rangle$  is defined via the eigenequations  $g_i|G\rangle = |G\rangle$ , for all  $i \in V$ . Note that a product of stabiliser operators is also a stabiliser.

In order to present our main idea, let us first describe the two mentioned steps. In step 1, a graph state according to the graph in figure 1 is created: for the simple line graphs, which constitute the long-distance links, each repeater station receives one qubit from the previous station, produces one qubit in state  $|+\rangle$ , entangles it with the qubit from the previous station via a  $C_Z$  gate and then sends the second qubit through the channel to the next repeater station, which acts in the same way. Thus, the edges between repeater stations are created. The network nodes act in a slightly different way: depending on their number of neighbours, they receive a certain number of inputs, create a certain number of qubits in state  $|+\rangle$ , perform entangling  $C_Z$  gates, and send on the appropriate number of qubits to the neighbouring repeater stations. Some examples are given in figure 1. Thus, the whole graph of figure 1 will be produced.

In step 2, the vertices corresponding to all repeater stations are removed by a simple Pauli  $X$ -measurement at each repeater station. The reasoning is as follows: remember that a product of stabilisers is also a stabiliser. Consider the vertex  $S$  (South Africa) in the quantum network shown in figure 1 and assume that the number of repeater stations is even on each edge (odd numbers can be treated in an analogous way). Take the product of the stabiliser generators starting from  $S$  and for every second repeater station, until reaching the neighbours  $T$ ,  $M$ ,  $P$ ,  $I$ , and  $R$ . Due to the definition of  $g_i$  in equation (2) and the fact that  $Z^2 = \mathbb{1}$ , this product of stabilisers contains only  $X$ -operators at  $S$  and the mentioned repeater stations, and  $Z$ -operators on the neighbouring network nodes of  $S$  in the network (see also [40]). We call this stabiliser operator the main stabiliser centred on  $S$ . Measuring all repeater stations in the  $X$ -basis projects the state onto one stabilised by  $\pm X_S Z_T Z_M Z_P Z_I Z_R$  in the Hilbert space of the network nodes only. Here the sign of the stabiliser operator depends on the parity of the measurement outcomes of the repeater stations included in the main stabiliser centred on  $S$ . The minus sign can be removed by applying the so-called by-product operator  $Z_S$  in this case. This reasoning holds for all network nodes. By comparison of the obtained stabilisers with equation (2) it is clear that the graph state corresponding to the global network (large vertices in figure 1) has been produced.

Even though we have explained the procedure in two consecutive steps, it is not necessary to store the full graph state: as the local measurements commute with the operations on other repeater stations, a qubit can be measured immediately after action of the  $C_Z$  gate, which is easier to realise experimentally. Thus, the whole graph state between network nodes is gradually built up in a one-way fashion, as explained in figure 1, without need for memories in the repeater stations.

In an implementation of the above scheme, losses in the transmission channels, noise in the gates as well as errors in preparation and measurement will occur and would lead to a low-quality output state. As a solution to this problem, quantum error correction can be employed: the main idea is to encode the state of a so-called logical qubit redundantly into many physical qubits, such that a local error leads to a unique error syndrome and can be corrected by applying a suitable operation [41]. This is in contrast to previous ideas [42] where graph states were used as resource states for measurement-based implementations of quantum error correction.

In the present article we make use of so-called stabiliser codes [43], which are defined via a set of stabiliser operators, the eigenstates of which (with eigenvalue 1) are the codewords. In particular, we focus here on a subclass of stabiliser codes, the Calderbank-Shor-Steane (CSS) codes [41] which have the useful property of ‘transversal’ logical entangling gates (see appendix B). Thus the only change in our scheme is that instead of initial physical qubit states  $|+\rangle$  multi-qubit encoded logical states, denoted in the following as  $|\bar{+}\rangle$ , need to be generated. The specific structure of  $|\bar{+}\rangle$  depends on the chosen error correction code. Low-error state preparation can be done more efficiently than general quantum operations on an unknown state, see e.g. [44] for a preparation scheme for the quantum Golay code [45–47]. The repeater operation in the encoded case and the short-hand notation  $|\bar{+}\rangle$  and  $M_{\bar{x}}$  for the measurement on the encoded state is illustrated in figure 2.

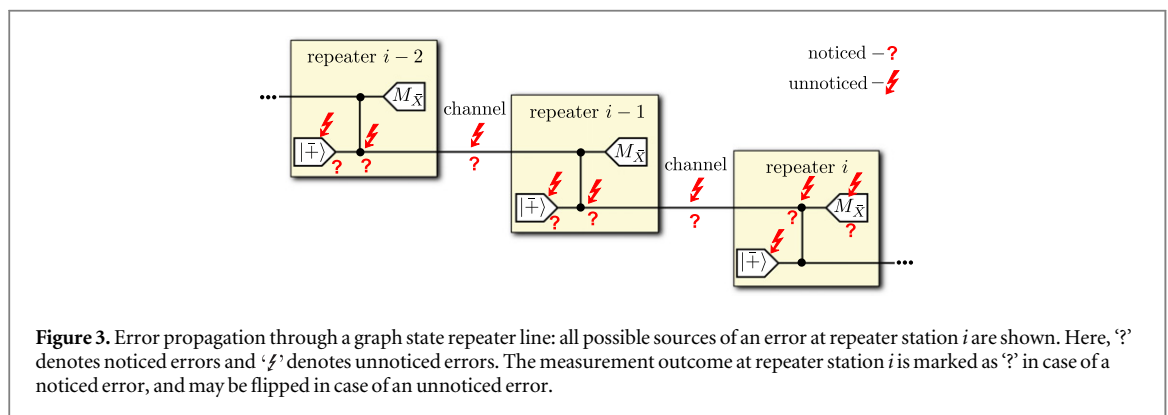
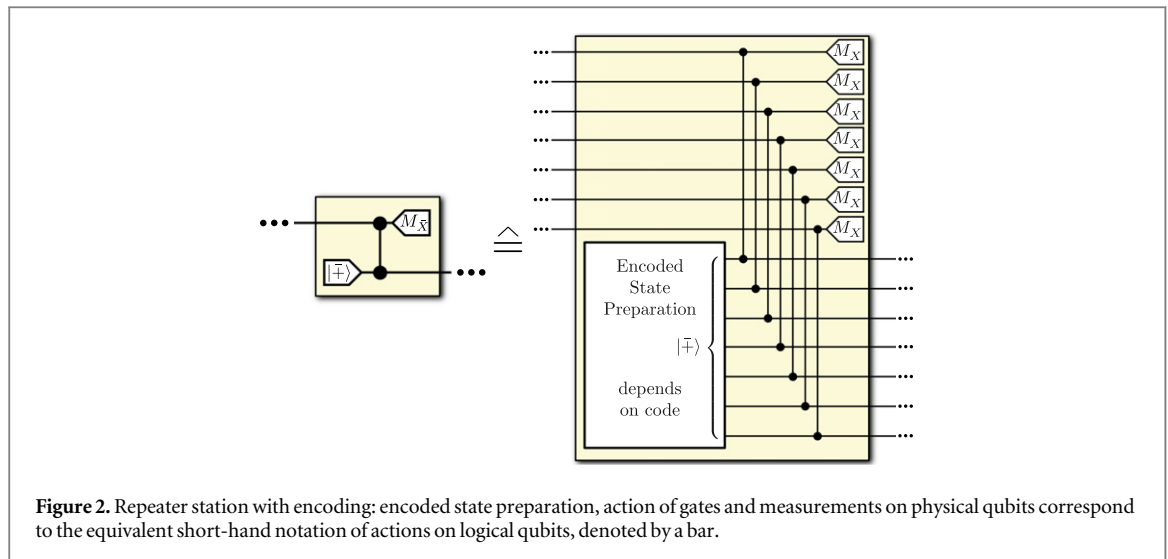
### 3. Error analysis in the graph language

The unified description of the quantum network in terms of stabilisers for both the states and the encoding allows for a comprehensive analysis of errors and performance study. An error can be noticed, in the sense that it is known which qubit is affected (e.g. a no-detection event), or unnoticed (noise). For our performance study we will use the usual exponential loss model in optical fibres, i.e. the failure probability during transmission  $f_T$  is given by

$$f_T = 1 - (1 - f_C)e^{-L_0/L_{\text{att}}}, \quad (3)$$

where  $f_C$  is a coupling failure probability,  $L_0$  is the distance between repeater stations and  $L_{\text{att}}$  is the attenuation length of the fibre, for which we will use the value  $L_{\text{att}} = 20$  km. All qubit errors (for sources, gates, channels, detectors) will be modelled by the depolarising channel, characterised as

$$\rho \rightarrow (1 - f)\rho + f\frac{\mathbb{1}}{2}, \quad (4)$$



i.e. with a failure probability  $f$  the state of the qubit is proportional to the identity, and with probability  $(1 - f)$  it is unaffected. Thus in case of failure the state is depolarised to the completely mixed state. The same effect is achieved by randomly applying bit-flips and phase-flips to the state. This mathematically equivalent viewpoint of a perfect operation followed by discrete  $X$  and  $Z$  errors is very convenient [48].

When a physical  $X$  or  $Z$  error has occurred, it propagates via the gates through the network, i.e. it may influence the consecutive qubits and measurement results. However, fortunately the spreading of errors along a repeater line is restricted to a finite length, concretely to up to two repeater stations. This is due to some simple rules for error propagation via a  $C_Z$  gate: a  $Z$  error that occurs on one of the two input qubits of a  $C_Z$  gate remains a  $Z$  error on the corresponding output qubit and does not affect the other output qubit. An  $X$  error that occurs on one of the two input qubits remains an  $X$  error on the corresponding output qubit, but also causes a  $Z$  error on the other output qubit. (If more than one error has occurred, the output qubits will suffer from corresponding products of errors.) An  $X$  or  $Z$  error may therefore be spread to the next repeater station, where the corresponding qubit will pass through the next  $C_Z$  gate and then will be measured. Regarding the measurement, an  $X$ -( $Z$ -) error before an  $X$ -( $Z$ -) measurement does not affect the measurement outcome, while an  $X$ -( $Z$ -) error before a  $Z$ -( $X$ -) measurement flips the measurement outcome.

The possible sources of errors are shown in figure 3. It is important to note, due to the arguments given above, that repeater station number  $i$  is only influenced by errors propagating from nearest and next-to-nearest neighbours, i.e. from stations  $(i - 1)$  and  $(i - 2)$ .

If an error is noticed, the corresponding measurement outcome is set to '?'. The physical error rate depends on the failure probabilities for transmission, gates and measurements and is explicitly calculated in appendix B.

In figure 3 we focus on the physical error rates along a repeater line. The generalisation of our analysis to more gates and more qubits in the case of the network nodes is straightforward and can be described in terms of the vertex (in- and out-) degree, see appendix D. Note, however, that in a large-scale quantum network there are many more repeater stations than network nodes. Thus the performance of the network mainly depends on the error rate at the repeater stations, which was described above.

Up to now we have described the physical errors. For a given encoding the logical error rate, i.e. the rate of uncorrectable errors, is a function of the physical error rate, see appendix C.

Remember that the (logical) measurement outcomes at the repeater stations of the main stabiliser centred on a node  $v$  determine whether the by-product operator  $Z_v$  needs to be applied. Thus even numbers of logical errors on the corresponding repeater stations cancel each other. The local error rate  $e_v$  at the vertex  $v$  is an important indicator of the quality of the produced state. The formula to calculate  $e_v$  follows the previous reasoning and is given in appendix A. The error rates  $e_v$  effectively combine all errors of the repeater stations and simplify the analysis considerably. The stabiliser error rates allow to bound the fidelity of the established state, see appendix A.

#### 4. Performance and quantum network architectures

The performance of a quantum network may depend on the task it was built for: possible figures of merit are e.g. the rate for the production of a long-distance entangled state, the success probability for a task such as quantum teleportation, or the secret key rate in a cryptographic setting. In the following we will use as figure of merit the cost-performance ratio  $C$  which compares the needed resources [18]: it is defined as the total number of needed qubits divided by the total distance  $L$  and a specific quality factor  $Q$ , i.e.

$$C = \frac{nw}{LQ}, \quad (5)$$

where  $n$  is the number of qubits per station (neglecting preparation overhead) and  $w$  is the number of repeater stations. Our description in the graph state language provides a tool to optimise the architecture of a quantum network: two graphs  $G$  and  $G'$  with the same set of vertices  $V$  but different sets of edges  $E \neq E'$  may correspond to local-unitary equivalent graph states [36], i.e. states that are related by local basis changes. This fact leads to general optimisation arguments for quantum networks; we now consider only network nodes as vertices and their connecting repeater lines as edges, which have a weight according to the number of repeater stations on this line.

- (1) The graph  $G'$  can have fewer edges than  $G$ . This corresponds to a reduced number of repeater lines in a network, see e.g. figure 4(a).
- (2) The graph  $G'$  can have less cycles than  $G$ , see e.g. figures 4(a) and (c). Note that in general cycles increase the required coherence time of the used quantum memories at the network nodes, because the qubits need to be stored until all gates have been applied to them.
- (3) The total length of the edges in  $E$  and  $E'$  may differ, even if the number of edges of  $G'$  and  $G$  are equal, see e.g. figure 4(b). One can thus minimise the total number of repeater stations in the network.
- (4) The maximal vertex degree of  $G$  and  $G'$  may be different. Given that the number of repeater stations is optimised w.r.t.  $C$  for each individual edge, the rate of errors increases with the vertex degree (see appendix A). Thus it can be advantageous to reduce the maximal vertex degree, see e.g. figure 4(c). In order to illustrate the general performance of a graph state quantum repeater and to compare different codes we consider in the following a bipartite setting, i.e. one repeater line. This is a typical quantum cryptographic scenario, and therefore we use as the quality factor  $Q$  in the cost-performance ratio  $C$  the effective secret fraction  $R$ , given by

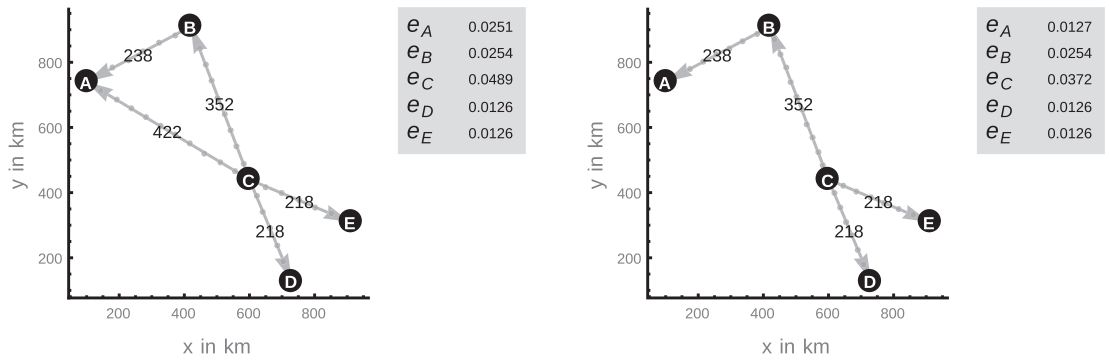
$$R = P_{\text{succ}} r_{\infty}, \quad (6)$$

where  $P_{\text{succ}}$  denotes the probability for not aborting of the protocol (one might choose to abort in case of a 'fatal' pattern of noticed errors in order to increase the quality of the produced state), employing a given code. The factor  $r_{\infty}$  is the secret fraction for the BB84 protocol, given by [49]

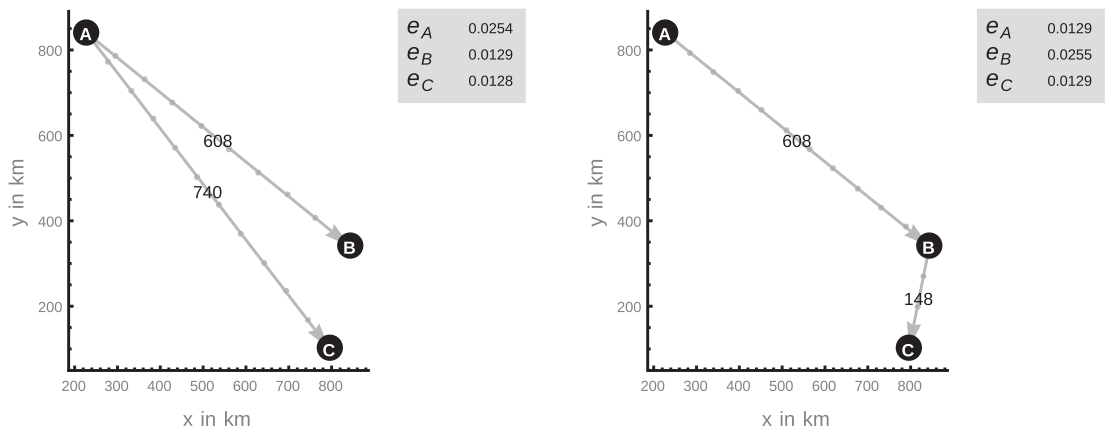
$$r_{\infty} = \max\{1 - h(e_A) - h(e_B), 0\}. \quad (7)$$

Here,  $e_A$  and  $e_B$  are the error rates of the two end nodes, and the binary entropy is defined as  $h(p) = -p \log_2(p) - (1-p) \log_2(1-p)$ . Note that  $e_A$  and  $e_B$  depend on the logical error rate of the error correction code: a logical measurement error remains, if the outcomes are decoded to a codeword with wrong parity.

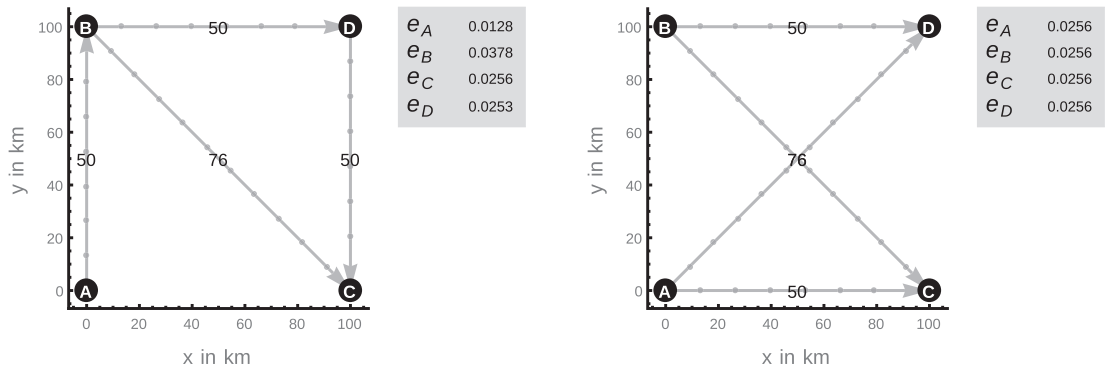
We optimised the cost-performance ratio  $C$  with respect to the number of repeater stations  $w$  for different  $L$  for several codes. The optimal separation distance of the repeater stations decreases with increasing total distance. Note that the number of repeater stations in figure 4, i.e. the optimal weight of the long-distance edges, was also calculated using this bipartite figure of merit for each edge. For a comparison of various encoding schemes with the original repeater see figure 5. For distances on the global scale the cost-performance ratio  $C$  of the Golay code remains in the same order of magnitude, e.g. for  $L = 100\,000$  km it is  $C \approx 63.5$  for optimised repeater spacing (approx. 480 m) and gate error probability  $f_G = 10^{-4}$ . Starting from distances larger than about 800 km, the Golay code outperforms all previous approaches. With our methods, this type of comparison can now be performed for any quantum network architecture and any quantum information processing task, using a corresponding figure of merit for the quality factor  $Q$ .



(a) The network with a cycle on the left produces the same final state as the network without cycle on the right (up to local basis transformations).



(b) While both networks have the same number of links and show comparable performance (in terms of the error rates of the final state), the right requires less repeater stations.

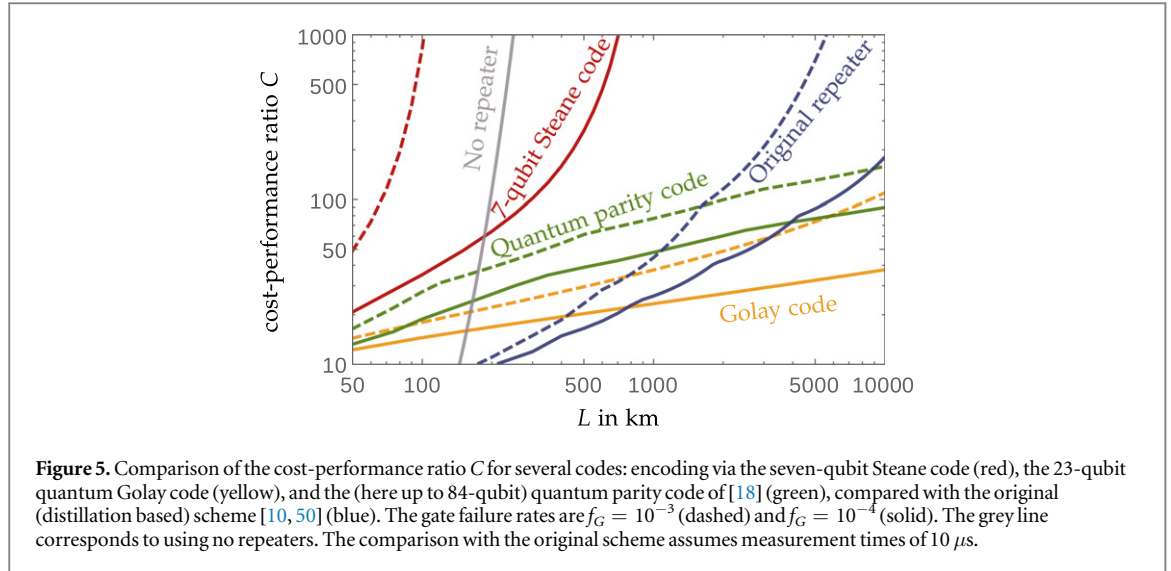


(c) The left network requires less repeaters, because the total length of the repeater lines is shorter. The right network, however, has a better performance in terms of the error rates, because the maximal vertex degree is lower.

**Figure 4.** The left example networks are local-unitary-equivalent to their right-hand side counterparts. Despite producing the same final state up to local basis transformations, these networks can differ in their performance and cost. For all figures a gate error rate of  $f_G = 1 \times 10^{-4}$  has been used. The number of repeater stations on each link minimises its cost-performance ratio  $C$  and is shown as the edge weight. The resulting error rates at the network nodes are shown in the box next to the network. They are approximately proportional to the corresponding vertex degree, because all links introduce roughly the same amount of errors (as a result of the optimisation w.r.t. the cost-performance ratio  $C$ ).

### 5. Discussion

Establishing a large-scale entangled quantum state is a formidable future task. In our proposal of a graph state quantum repeater network this finds a unified description in the elegant language of stabilisers. Though being of abstract mathematical origin, this approach allows to quantitatively evaluate the implementation of a quantum network corresponding to an arbitrary graph and compare it to other networks and different approaches from the literature. For given quantum hardware such as sources, transmission channels, gates and



detectors, a suitable error correction code can be found, and the performance for quantum information processing protocols such as e.g. secret key generation between two or more parties can be determined.

For fixed locations of participating parties, our method helps to design an optimal quantum network in terms of resources and performance with respect to a specific task (e.g. cryptography or synchronisation of distributed clocks [51, 52]). Exploiting local unitary equivalence of different quantum networks has no classical counterpart and deserves further detailed investigations. Future research on quantum networks will benefit from the presented description in the stabiliser formalism. This includes in particular the analysis of the efficient use of the whole network infrastructure to produce entangled states shared by a subset of parties. While we showed that the performance of the 23-qubit quantum Golay code is outstanding for large distances, further research may focus on smaller codes for smaller networks.

## Acknowledgments

M E acknowledges helpful discussions with S Muralidharan and financial support by the German Federal Ministry of Education and Research (BMBF).

## Appendix A. Logical graph states

An  $[[n, k, d]]$  error correction code encodes  $k$  logical qubits into  $n > k$  physical qubits. This redundancy guarantees the correction of up to  $\frac{d-1}{2}$  single qubit errors or  $d - 1$  erasures. Note that erasures, marked in the classical data as '?', are not only caused by losses of qubits at that particular position. In the scheme described in the main text, any noticed error on the qubit  $i$  or  $i - 1$  will lead to an erasure of the measurement outcome at position  $i$ .

Let  $S$  denote the stabiliser group of the codespace of a stabiliser code. Furthermore let  $\bar{X}^{(1)}, \dots, \bar{X}^{(k)}, \bar{Z}^{(1)}, \dots, \bar{Z}^{(k)}$  denote logical  $X$ - and  $Z$ -operators. These operators are elements of the normaliser of  $S$  but not elements of  $S$  and fulfill  $X^{(i)}Z^{(i)} = -Z^{(i)}X^{(i)}$ , while operators on different logical qubits commute. For simplicity we focus on the  $k = 1$  case and drop the label of the logical operator. In analogy to a graph state, we define a logical graph state associated with a graph  $G = (V, E)$  as the unique state  $|\bar{G}\rangle$  that is stabilised by operators

$$\bar{g}_i = \bar{X}_i \prod_{\substack{j \in V \\ (i,j) \in E}} \bar{Z}_j. \quad (\text{A1})$$

This definition can be generalised to  $k > 1$  which leads to  $k$  copies of the graph state.

A logical error  $e$  occurs when the recovery operation leads to a wrong codeword  $e|\bar{G}\rangle \neq \bar{G}$ . This can happen if more errors occurred on one block than the code is able to correct. A logical measurement error occurs if  $e$  anticommutes with the observable. One assumes that the probability of (un-noticed) errors  $f_u$  and erasures  $f_n$  are the same for all physical qubits. Then for any quantum error correction code, the probability of a logical error  $\bar{f}_u$  is a function of  $f_u$  and  $f_n$ . It is possible to retry the production on a particular pattern of noticed errors. Thus the function  $\bar{f}_u(f_u, f_n)$  depends on the error correction code and the strategy of when to abort. Several examples are given in appendix C.

Given the probability of logical measurement errors at each vertex it is straightforward to calculate the logical error rate at the position of the network nodes. For each main stabiliser  $S_i$  centred on party  $i$ , the applied by-product operator  $Z_i^{\sum \bar{x}_j}$  depends on all  $\bar{X}$ -measurement outcomes  $\bar{x}_j$  of the qubits included in the main stabiliser



(i.e. the qubits on which it acts non-trivially). These are half of the qubits on the links from and to party  $i$ , i.e.  $\frac{1}{2} \sum_{j \in V} w_{ij}$ , where  $w_{ij}$  is the number of repeater stations on the link  $(i, j)$ . Even numbers of logical errors cancel each other and the stabiliser error rate is

$$e_i = \text{tr} \left( \rho \frac{\mathbb{I} - \bar{g}_i}{2} \right), \quad (\text{A2})$$

$$= \sum_n \text{tr} \left( \rho \bar{Z}_i \prod_{\substack{k \in V \\ k \neq i}} \bar{Z}_k^{n^{(k)}} |G\rangle \langle G| \bar{Z}_i \prod_{\substack{k' \in V \\ k' \neq i}} \bar{Z}_k'^{n^{(k')}} \right), \quad (\text{A3})$$

$$= P_{\text{odd}} \left( \bar{f}_u(f_u, f_n), \frac{1}{2} \sum_{j \in V} w_{ij} \right), \quad (\text{A4})$$

where  $n^k$  is the  $k$ th binary digit of  $n$  and

$$P_{\text{odd}}(f, N) = \frac{1}{2} (1 - (1 - 2f)^N). \quad (\text{A5})$$

Suppose that the state produced by the quantum network is given by a density matrix  $\rho$ . An error on any stabiliser implies the production of a state orthogonal to the target state  $|G\rangle$ . Note that it suffices to consider only  $\bar{Z}$  errors, as the effect of  $\bar{X}$ -errors can be described with  $\bar{Z}$  errors due the stabilisers of the graph state. One can thus immediately gain bounds on the fidelity of  $\rho$  with respect to the state  $|G\rangle$  from the local error rates  $e_v$ ,

$$1 - \sum_{v \in V} e_v \leq \langle G | \rho | G \rangle \leq 1 - \max \{e_v | v \in V\}. \quad (\text{A6})$$

For the network given in figure 4(b), these bounds evaluate to 94%  $\leq \langle G | \rho | G \rangle \leq$  99%, for example.

## Appendix B. Error propagation through repeater stations

CSS codes allow the transversal implementation of controlled-NOT gates [41]. A transversal application of a quantum gate on two blocks of an  $[[n, k, d]]$  quantum error correction code is the qubit-wise application of the gate, i.e.  $n$  gates act in parallel on the  $i$ th qubit of block one and the  $i$ th qubit of block two,  $i = 1, 2, \dots, n$ , see figure 2. By using two alternating codes in the  $\bar{X}$ - and  $\bar{Z}$ -basis on alternating qubits, the transversal application of the controlled-NOT gates acts like a logical controlled-phase gate and we can stick to the language of graph states. Because only transversal gates are applied in the quantum circuit, it suffices to calculate the physical error rate by considering the first qubit of each block only. We start by calculating the unnoticed error rate  $f_u$  for a repeater station, i.e. the probability to get a flipped measurement outcome. Notice that two errors of this kind cancel each other. We collect all independent sources of errors that lead to the error pattern under consideration (e.g. ‘flipped outcome at position  $i$ ’) into a vector  $\vec{p}$ . Then the probability for this error is

$$f_u = \tilde{P}_{\text{odd}}(\vec{p}) = \sum_{\substack{n=0 \\ |n|_H \text{ odd}}}^{2^N-1} \prod_{k=1}^N p_k^{n^{(k)}} (1 - p_k)^{1-n^{(k)}}, \quad (\text{B1})$$

where  $n^k$  is the  $k$ th binary digit of  $n$ . In case of the repeater stations the error sources correspond to

$$\vec{p} = \left( P_{\text{odd}} \left( \frac{f_{P,u}}{2}, 2 \right), \frac{f_{P,n} + f_{P,u}}{2}, P_{\text{odd}} \left( \frac{f_{G,u}}{2}, 3 \right), P_{\text{odd}} \left( \frac{f_{T,u}}{2}, 2 \right), \frac{f_{M,u}}{2} \right). \quad (\text{B2})$$

Here we included noticed/unnoticed errors for preparation ( $f_{P, n/u}$ ), transmission ( $f_{T, n/u}$ ), gates ( $f_{G, n/u}$ ) and measurement ( $f_{M, n/u}$ ). Remember that  $P_{\text{odd}}(f, N)$  was defined in equation (A5). In order to identify the processes that contribute to  $f_u$  one checks all possible propagations of errors to a  $Z$ -error on the qubit  $i$  under consideration. It is useful to note that only  $X$ -errors spread to  $Z$ -errors on adjacent qubits in a  $C_Z$  gate.

Please note that we have neglected the difference of the physical error rates for qubits at the boundary of a repeater line and ‘typical’ qubits. This is motivated by the fact, that in a large-scale quantum network there are many more repeater stations than parties. Incorporating these boundary effects is however straightforward.

We assume that noticed errors do not cancel each other. Again we collect all independent sources of the error under consideration. In contrast to the case of  $f_u$ ,  $f_n$  denotes the probability that any of these events occurred. Thus the probability for an error of this type is

$$f_n = 1 - (1 - f_{P,n})^2 (1 - f_{G,n})^3 (1 - f_{T,n})^2 (1 - f_{M,n})^2. \quad (\text{B3})$$

## Appendix C. Logical error rate of some CSS codes

In order to calculate the secret key rate for a specific encoding, we need the error rates on odd and even logical qubits. The decoder assigns a codeword to any word given by the measurement, i.e. to the true outcomes altered by the error pattern. This recovered codeword is used to calculate the value of the logical observable. If this recovered value is different from the ‘true outcome’ this word of measurement outcomes contributes to the logical error rate. The decoder may trigger an abort on any error from the set  $\mathcal{F}$ . The naive approach to calculating this rate thus is

$$\bar{f}_{u,c}(f_u, f_n) = \frac{1}{k} \sum_{e \notin \mathcal{F}} f(e) P_e(e), \quad (C1)$$

**Table C1.** Logical error rates of the Steane code.

	7-qubit Steane code ( $n_{\max} = 0$ )
$\bar{f}_u(f_u, f_n)$	$(f_n - 1)^7 f_u^2 (48f_u^5 - 168f_u^4 + 252f_u^3 - 210f_u^2 + 98f_u - 21)$
$P_{\text{succ}}(f_n)$	$(1 - f_n)^7$
	7-qubit Steane code ( $n_{\max} = 1$ )
$\bar{f}_u(f_u, f_n)$	$(f_n - 1)^6 f_u (48(f_n - 1)f_u^6 - 168(f_n - 1)f_u^5 + 252(f_n - 1)f_u^4 - 210(f_n - 1)f_u^3 + 14(9f_n - 7)f_u^2 + 21(1 - 3f_n)f_u + 21f_n)$
$P_{\text{succ}}(f_n)$	$(f_n - 1)^6 (6f_n + 1)$
	7-qubit Steane code ( $n_{\max} = 2$ )
$\bar{f}_u(f_u, f_n)$	$(f_n - 1)^5 f_u (48(f_n - 1)^2 f_u^6 - 168(f_n - 1)^2 f_u^5 + 252(f_n - 1)^2 f_u^4 - 210(f_n - 1)^2 f_u^3 + 14(f_n(3f_n - 16) + 7)f_u^2 + 21(f_n(3f_n + 4) - 1)f_u - 21f_n(2f_n + 1))$
$P_{\text{succ}}(f_n)$	$-(f_n - 1)^5 (15f_n^2 + 5f_n + 1)$
	7-qubit Steane code ( $n_{\max} = 3$ )
$\bar{f}_u(f_u, f_n)$	$\frac{1}{2}(f_n - 1)^4 (f_n^3 (96f_u^7 - 336f_u^6 + 504f_u^5 - 420f_u^4 + 308f_u^3 - 210f_u^2 + 84f_u + 7) - 2f_n^2 f_u (144f_u^6 - 504f_u^5 + 756f_u^4 - 630f_u^3 + 266f_u^2 - 21f_u - 21) + 2f_n f_u (144f_u^6 - 504f_u^5 + 756f_u^4 - 630f_u^3 + 322f_u^2 - 105f_u + 21) + 2f_u^2 (-48f_u^5 + 168f_u^4 - 252f_u^3 + 210f_u^2 - 98f_u + 21))$
$P_{\text{succ}}(f_n)$	$(f_n - 1)^4 (20f_n^3 + 10f_n^2 + 4f_n + 1)$
	7-qubit Steane code ( $n_{\max} = 4$ )
$\bar{f}_u(f_u, f_n)$	$\frac{1}{2}(f_n - 1)^3 (3f_n^4 (32f_u^7 - 112f_u^6 + 168f_u^5 - 140f_u^4 + 84f_u^3 - 42f_u^2 + 14f_u - 7) - f_n^3 (384f_u^7 - 1344f_u^6 + 2016f_u^5 - 1680f_u^4 + 840f_u^3 - 252f_u^2 + 42f_u + 7) + 12f_n^2 f_u^2 (48f_u^5 - 168f_u^4 + 252f_u^3 - 210f_u^2 + 98f_u - 21) - 6f_n f_u (64f_u^6 - 224f_u^5 + 336f_u^4 - 280f_u^3 + 140f_u^2 - 42f_u + 7) + 2f_u^2 (48f_u^5 - 168f_u^4 + 252f_u^3 - 210f_u^2 + 98f_u - 21))$
$P_{\text{succ}}(f_n)$	$-15f_n^7 + 35f_n^6 - 21f_n^5 + 1$
	7-qubit Steane code ( $n_{\max} = 5$ )
$\bar{f}_u(f_u, f_n)$	$\frac{1}{2}(f_n - 1)^2 (6f_n^5 f_u (16f_u^6 - 56f_u^5 + 84f_u^4 - 70f_u^3 + 42f_u^2 - 21f_u + 7) - 2f_n^4 (240f_u^7 - 840f_u^6 + 1260f_u^5 - 1050f_u^4 + 546f_u^3 - 189f_u^2 + 42f_u - 7) + f_n^3 (960f_u^7 - 3360f_u^6 + 5040f_u^5 - 4200f_u^4 + 2016f_u^3 - 504f_u^2 + 42f_u + 7) - 6f_n^2 f_u (160f_u^6 - 560f_u^5 + 840f_u^4 - 700f_u^3 + 336f_u^2 - 84f_u + 7) + 2f_n f_u (240f_u^6 - 840f_u^5 + 1260f_u^4 - 1050f_u^3 + 518f_u^2 - 147f_u + 21) + 2f_u^2 (-48f_u^5 + 168f_u^4 - 252f_u^3 + 210f_u^2 - 98f_u + 21))$
$P_{\text{succ}}(f_n)$	$6f_n^7 - 7f_n^6 + 1$
	7-qubit Steane code ( $n_{\max} = 6$ )
$\bar{f}_u(f_u, f_n)$	$f_n^7 (48f_u^7 - 168f_u^6 + 252f_u^5 - 210f_u^4 + 126f_u^3 - 63f_u^2 + 21f_u - \frac{7}{2}) - \frac{21}{2}f_n^6 (2f_u - 1)^3 (4f_u^4 - 8f_u^3 + 6f_u^2 - 2f_u + 1) + \frac{21}{2}f_n^5 (2f_u - 1)^3 (12f_u^4 - 24f_u^3 + 18f_u^2 - 6f_u + 1) - 105f_n^4 f_u (2f_u - 1)^3 (2f_u^3 - 4f_u^2 + 3f_u - 1) + \frac{7}{2}f_n^3 (2f_u - 1)^3 (60f_u^4 - 120f_u^3 + 90f_u^2 - 30f_u - 1) - 63f_n^2 f_u (2f_u - 1)^3 (2f_u^3 - 4f_u^2 + 3f_u - 1) + 21f_n f_u (2f_u - 1)^3 (2f_u^3 - 4f_u^2 + 3f_u - 1) + f_u^2 (-48f_u^5 + 168f_u^4 - 252f_u^3 + 210f_u^2 - 98f_u + 21)$
$P_{\text{succ}}(f_n)$	$1 - f_n^7$
	7-qubit Steane code ( $n_{\max} = 7$ )
$\bar{f}_u(f_u, f_n)$	$3f_n^7 (2f_u - 1)^3 (2f_u^4 - 4f_u^3 + 3f_u^2 - f_u + 1) - \frac{21}{2}f_n^6 (2f_u - 1)^3 (4f_u^4 - 8f_u^3 + 6f_u^2 - 2f_u + 1) + \frac{21}{2}f_n^5 (2f_u - 1)^3 (12f_u^4 - 24f_u^3 + 18f_u^2 - 6f_u + 1) - 105f_n^4 f_u (2f_u - 1)^3 (2f_u^3 - 4f_u^2 + 3f_u - 1) + \frac{7}{2}f_n^3 (2f_u - 1)^3 (60f_u^4 - 120f_u^3 + 90f_u^2 - 30f_u - 1) - 63f_n^2 f_u (2f_u - 1)^3 (2f_u^3 - 4f_u^2 + 3f_u - 1) + 21f_n f_u (2f_u - 1)^3 (2f_u^3 - 4f_u^2 + 3f_u - 1) + f_u^2 (-48f_u^5 + 168f_u^4 - 252f_u^3 + 210f_u^2 - 98f_u + 21)$
$P_{\text{succ}}(f_n)$	$1$

Table C2. Logical error rate for the Golay-code.

---

Golay code[47] assuming  $\bar{f}_u \approx \frac{f_w}{2}$

$$\bar{f}_u(f_u, f_n) = \frac{1}{2} \left( -\frac{f_n^{23}}{4096} + \frac{23(f_n + f_u - 1)f_n^{22}}{2048} - \frac{253(f_n + f_u - 1)^2 f_n^{21}}{1024} + \frac{1771}{512} (f_n + f_u - 1)^3 f_n^{20} - \frac{8855}{256} (f_n + f_u - 1)^4 f_n^{19} \right. \\ + \frac{33649}{128} (f_n + f_u - 1)^5 f_n^{18} - \frac{100947}{64} (f_n + f_u - 1)^6 f_n^{17} + \frac{245157}{32} (f_n + f_u - 1)^7 f_n^{16} - 30613 (f_n + f_u - 1)^8 f_n^{15} \\ - \frac{253}{16} (f_n - 1)(f_n + f_u - 1)^7 f_n^{15} + 101200 (f_n + f_u - 1)^9 f_n^{14} \\ + \frac{3795}{8} (f_n - 1)(f_n + f_u - 1)^8 f_n^{14} - 272734 (f_n + f_u - 1)^{10} f_n^{13} - \frac{26565}{4} (f_n - 1)(f_n + f_u - 1)^9 f_n^{13} \\ + 560924 (f_n + f_u - 1)^{11} f_n^{12} + \frac{115115}{2} (f_n - 1)(f_n + f_u - 1)^{10} f_n^{12} - 695520 (f_n + f_u - 1)^{12} f_n^{11} \\ - 319424 (f_n - 1)(f_n + f_u - 1)^{11} f_n^{11} + \frac{8855}{2} (f_n + f_u - 1)^{11} (-f_n + 2f_u + 1) f_n^{11} \\ + 949256 (f_n - 1)(f_n + f_u - 1)^{12} f_n^{10} - 97405 (f_n + f_u - 1)^{12} (-f_n + 2f_u + 1) f_n^{10} \\ + 779240 (f_n + f_u - 1)^{13} (-f_n + 2f_u + 1) f_n^9 + 18975 (f_n + f_u - 1)^{13} (-f_n + 6f_u + 1) f_n^9 \\ - 485760 (f_n + f_u - 1)^{14} (-f_n + 6f_u + 1) f_n^8 - 2277 (f_n + f_u - 1)^{14} (-f_n + 14f_u + 1) f_n^8 \\ + 32384 (f_n + f_u - 1)^{15} (-f_n + 14f_u + 1) f_n^7 + \frac{253}{2} (f_n - 1)(f_n + f_u - 1)^{14} (-f_n + 14f_u + 1) f_n^7 \\ + 212520 (f_n + f_u - 1)^{14} (-f_n - 1)^2 + 10f_u (f_n - 1) + 8f_u^2) f_n^7 \\ - 100947 (f_n - 1)(f_n + f_u - 1)^{15} (-f_n + 14f_u + 1) f_n^6 \\ - 28336 (f_n + f_u - 1)^{16} (-f_n + 2f_u + 1)(-f_n + 14f_u + 1) f_n^5 \\ - 5313 (f_n + f_u - 1)^{16} ((f_n - 1)^2 - 15f_u (f_n - 1) + 30f_u^2) f_n^5 \\ + 8855 (f_n + f_u - 1)^{17} ((f_n - 1)^2 - 17f_u (f_n - 1) + 90f_u^2) f_n^4 \\ - 1771 (f_n + f_u - 1)^{17} ((f_n - 1)^3 - 17f_u (f_n - 1)^2 + 138f_u^2 (f_n - 1) + 96f_u^3) f_n^3 \\ - 253 (f_n + f_u - 1)^{18} (-f_n - 1)^3 + 18f_u (f_n - 1)^2 - 171f_u^2 (f_n - 1) + 90f_u^3) f_n^2 \\ + 23 (f_n + f_u - 1)^{19} (-f_n - 1)^3 + 19f_u (f_n - 1)^2 - 190f_u^2 (f_n - 1) + 560f_u^3) f_n + (f_n + f_u - 1)^{23} \\ - 23f_u (f_n + f_u - 1)^{22} + 253f_u^2 (f_n + f_u - 1)^{21} - 1771f_u^3 (f_n + f_u - 1)^{20} + 1) \\ P_{\text{succ}} = 1$$


---

where  $P_e(e)$  is the probability of the error  $e$  and  $f(e)$  is the number of logical errors after decoding. The success probability depends on  $\mathcal{F}$  and reads

$$P_{\text{succ}} = \sum_{e \notin \mathcal{F}} P_e(e) = 1 - \sum_{e \in \mathcal{F}} P_e(e). \quad (\text{C2})$$

Let us consider a decoder that returns the most likely codeword  $c$  in the sense that an error pattern  $e$  that changes  $c$  to the observed data has maximal probability  $P_e(e)$ . If this is not unique the decoder chooses any such  $c$  with equal probability. We use it for the 7-qubit Steane code and use a fatal error set  $\mathcal{F}$  of the form

$$\mathcal{F} = \{e | e \text{ contains more than } n_{\text{max}} \text{ losses}\}, \quad (\text{C3})$$

where  $n_{\text{max}} \in \mathbb{N}$ , i.e. the protocol is aborted if more than  $n_{\text{max}}$  losses occurred. The error rates of the 7-qubit Steane code listed in table C1 were obtained by implementing equation (C1). The logical error rate of the Golay code is given in table C2.

## Appendix D. Generalisation of the error analysis

Given a graph  $G = (V, E)$  with vertices  $V$  and edges  $E$ . The state  $|G\rangle$  is stabilised by the generators of the stabiliser  $g_i$  ( $i = 1, \dots, |V|$ ). The repeater network that creates the graph state  $|G\rangle$  is obtained by replacing each edge  $(i, j)$  in  $E$  by a line graph with  $w_{ij}$  additional vertices (the repeater stations). Let us assume that  $w_{ij}$  is even, for simplicity. All repeater stations are measured in the  $\bar{X}$  basis. This projects onto a state that is stabilised by the  $g_i$  up to byproduct operators that depend on the measurement outcomes. Thus after application of the byproduct operators  $g_i|G\rangle = |G\rangle$  holds. A flip of one measurement outcome on the  $i$ th main stabiliser ( $g_i$  connected by chains of  $X$ -operators) leads to  $g_i|G\rangle = -|G\rangle$ . The same holds for  $\bar{X}$  errors on the neighbours of party  $i$  or a  $Z$  error on the qubit of party  $i$ . The corresponding error probability is  $f_i$ . We denote the probability for the wrong sign in the stabiliser equation of  $g_i$  by  $e_i$ . It is

$$e_i = \tilde{P}_{\text{odd}} \left( \left( P_{\text{odd}} \left( \bar{f}_u, \sum_j w_{ij} \right), f_i, f_j | (i, j) \in E \right) \right). \quad (\text{D1})$$

In analogy to equations (14) and (16) of the article one can estimate the error rate

$$f_{i,u} = \tilde{P}_{\text{odd}} \left( \left( P_{\text{odd}} \left( \frac{f_{P,u}}{2}, 1 + \text{deg}^-(i) \right), P_{\text{odd}} \left( \frac{f_{P,n} + f_{P,u}}{2}, \text{deg}^+(i) \right), P_{\text{odd}} \left( \frac{f_{G,u}}{2}, 1 + \text{deg}(i) \right), P_{\text{odd}} \left( \frac{f_{T,u}}{2}, 1 + \text{deg}^-(i) \right), \frac{f_{M,u}}{2} \right) \right) \quad (\text{D2})$$

and

$$f_{i,n} = 1 - (1 - f_{P,n})^{1+\text{deg}^-(i)} (1 - f_{G,n})^{1+\text{deg}(i)} (1 - f_{T,n})^{1+\text{deg}^-(i)} (1 - f_{M,n})^{1+\text{deg}^-(i)}, \quad (\text{D3})$$

where  $\text{deg}(i)$ ,  $\text{deg}^-(i)$ , and  $\text{deg}^+(i)$  are the degree, in-degree, and out-degree of vertex  $i$ , respectively. From these physical error rates one can calculate the logical error rate in analogy to  $\tilde{f}_u$ , i.e.  $\tilde{f}_i = \tilde{f}_u (f_u = f_{i,u}, f_n = f_{i,n})$ .

## References

- [1] Buhrman H and Röhrig H 2003 *Mathematical Foundations of Computer Science 2003 (Lecture Notes in Computer Science vol 2747)* ed B Rovan and P Vojtas (Berlin: Springer) pp 1–20
- [2] Broadbent A, Fitzsimons J and Kashefi E 2009 *FOCS '09. 50th Annual IEEE Symp. on Foundations of Computer Science, 2009* pp 517–26
- [3] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
- [4] Murao M, Jonathan D, Plenio M B and Vedral V 1999 *Phys. Rev. A* **59** 156
- [5] Markham D and Sanders B C 2008 *Phys. Rev. A* **78** 042309
- [6] Bennett C and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* vol 175
- [7] Chen K and Lo H-K 2007 *Quantum Inf. Comput.* **7** 689–715
- [8] Dür W, Calsamiglia J and Briegel H-J 2005 *Phys. Rev. A* **71** 042336
- [9] Mermin N 1990 *Phys. Rev. Lett.* **65** 1838
- [10] Briegel H-J, Dür W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
- [11] Dür W, Briegel H-J, Cirac J I and Zoller P 1999 *Phys. Rev. A* **59** 169
- [12] Duan L-M, Lukin M D, Cirac J I and Zoller P 2001 *Nature* **414** 413–8
- [13] van Loock P, Ladd T D, Sanaka K, Yamaguchi F, Nemoto K, Munro W J and Yamamoto Y 2006 *Phys. Rev. Lett.* **96** 240501
- [14] Zwerger M, Dür W and Briegel H J 2012 *Phys. Rev. A* **85** 062326
- [15] Knill E and Laflamme R 1996 arXiv:quantph/9608012
- [16] Jiang L, Taylor J M, Nemoto K, Munro W J, Van Meter R and Lukin M D 2009 *Phys. Rev. A* **79** 032325
- [17] Fowler A G, Wang D S, Hill C D, Ladd T D, Van Meter R and Hollenberg L C L 2010 *Phys. Rev. Lett.* **104** 180503
- [18] Muralidharan S, Kim J, Lütkenhaus N, Lukin M D and Jiang L 2014 *Phys. Rev. Lett.* **112** 250501
- [19] Cory D G, Price M D, Maas W, Knill E, Laflamme R, Zurek W H, Havel T F and Somaroo S S 1998 *Phys. Rev. Lett.* **81** 2152
- [20] Yuan Z-S, Chen Y-A, Zhao B, Chen S, Schmiedmayer J and Pan J-W 2008 *Nature* **454** 1098
- [21] Kimble H J 2008 *Nature* **453** 1023
- [22] Sangouard N, Simon C, de Riedmatten H and Gisin N 2011 *Rev. Mod. Phys.* **83** 33
- [23] Schindler P, Barreiro J T, Monz T, Nebendahl V, Nigg D, Chwalla M, Hennrich M and Blatt R 2011 *Science* **332** 1059
- [24] Usmani I, Clausen C, Bussières F, Sangouard N, Afzelius M and Gisin N 2012 *Nat. Photon.* **6** 234
- [25] Hensen B et al 2015 *Nature* **526** 682–6
- [26] Peev M et al 2009 *New J. Phys.* **11** 075001
- [27] Elliott C 2002 *New J. Phys.* **4** 46
- [28] Acin A, Cirac J I and Lewenstein M 2007 *Nat. Phys.* **3** 256
- [29] Van Meter R, Satoh T, Ladd T, Munro W and Nemoto K 2013 *Netw. Sci.* **3** 82
- [30] Perseguers S, Lapeyre Jr G J, Cavalcanti D, Lewenstein M and Acin A 2013 *Rep. Prog. Phys.* **76** 096001
- [31] Leung D, Oppenheim J and Winter A 2006 *IEEE Trans. Inf. Theory* **56** 3478
- [32] Hayashi M 2007 *Phys. Rev. A* **76** 040301
- [33] de Beaudrap N and Rötteler M 2014 arXiv:1403.3533 [quant-ph]
- [34] Nagayama S, Choi B-S, Devitt S, Suzuki S and Van Meter R 2015 *Phys. Rev. A* **93** 042338
- [35] Schlingemann D and Werner R F 2001 *Phys. Rev. A* **65** 012308
- [36] Hein M, Eisert J and Briegel H J 2004 *Phys. Rev. A* **69** 062311
- [37] Raussendorf R, Browne D E and Briegel H J 2003 *Phys. Rev. A* **68** 022312
- [38] Dür W, Aschauer H and Briegel H-J 2003 *Phys. Rev. Lett.* **91** 107903
- [39] Gühne O, Tóth G, Hyllus P and Briegel H J 2005 *Phys. Rev. Lett.* **95** 120405
- [40] Wu J-Y, Kampermann H and Bruß D 2015 *Phys. Rev. A* **92** 012322
- [41] Lidar D and Brun T 2013 *Quantum Error Correction* (Cambridge: Cambridge University Press)
- [42] Zwerger M, Briegel H J and Dür W 2014 *Sci. Rep.* **4** 5364
- [43] Gottesman D 1997 Stabilizer codes and quantum error correction *PhD Thesis* California Institute of Technology, California
- [44] Paetznick A and Reichardt B 2012 *Quantum Inf. Comput.* **12** 1034
- [45] Golay M J E 1949 *Proc. IRE* **37** 657

- [46] Goethals J-M 1971 *J. Comb. Theory A* **11** 178
- [47] Elia M and Taricco G 1995 *Ann. Telecommun.* **50** 721
- [48] Nielsen M and Chuang I 2000 *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences)* (Cambridge: Cambridge University Press)
- [49] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
- [50] Abruzzo S, Bratzik S, Bernardes N K, Kampermann H, van Loock P and Bruß D 2013 *Phys. Rev. A* **87** 052315
- [51] Chuang I L 2000 *Phys. Rev. Lett.* **85** 2006
- [52] Kómár P, Kessler E M, Bishof M, Jiang L, Sørensen A S, Ye J and Lukin M D 2014 *Nat. Phys.* **10** 582