Stabilizer Codes as Resource for non-universal Quantum Information Processing on the Example of the Quantum Anonymous Broadcast

Markus S. Kesselring
University of Basel - Department of Physics

(Dated: 9.7.2016)

The quantum anonymous broadcast (QAB) is an example of an information protocol not relying on the full universal gate set. It can be carried out with gates in the Clifford group alone. This makes it an interesting candidate for the study of fault tolerant means to achieve it. Systems with a high resilience against errors, such as surface codes or Majorana zeromodes, have the flaw of not trivially having access to the whole universal gate set. We study how to implement the QAB in a variety of fault tolerant systems. In a last section, non-destructive ways to measure the charge of multiple Majorana zeromodes is discussed.

1. INTRODUCTION

The prospect of using the laws that govern the quantum realm to our advantage by means of quantum information processing was proposed by Richard Feynman in 1982. Classical computers do not meet the challenge to simulate quantum systems, whose Hilbert spaces grow exponentially with the number of degrees of freedom. But highly controlled quantum resources can be used to simulate arbitrary quantum systems of interest. After this initial interest, first algorithms for every day applications have been found, which outperform their classical counterparts. Since the eighties a great deal of advances have been made. But there seems to be a fundamental challenge to control quantum systems sufficiently for information processing. Specifically, the problem of tolerance against background noise and faulty gates is a big challenge.

The prospect of relying on topologically protected systems to store and manipulate quantum information in a fault tolerant fashion has become a popular and important field within quantum computing research. There seems to be a unfavourable relation: systems that are believed to be buildable in the near future seem to be lacking the capacity for universal quantum computation. Generalizations and extensions solving these problems are either relying on high dimensional structures or fight with a huge overhead for simple operations.

In this work, we want to focus on the accessible operations in systems such as surface codes and Majorana zeromodes. As an example for a protocol that can be carried out with less than the universal gate set, the Quantum Anonymous Broadcast (QAB) is chosen.

It's classical counterpart is discussed in a first section. Then, a well known version of the protocol relying on GHZ-states is studied with respect to quantum noise. Next, fault tolerant means to tackle the protocol are presented, using surface codes and Majorana zeromodes. The final part of the work addresses the question, how non-destructible collective charge measurements on multiple Majorana zeromodes can be carried out.

2. CLASSICAL ANONYMOUS BROADCAST

The goal of the protocol is to send a classical message publicly, but keeping the senders identity anonymous within a group of N participants. Perfect anonymity means, the chance to identify the sender is as good as guessing even if players try to cheat.

2.1. Classical Protocols

To understand the quantum version of this protocol, it is useful to keep the classical counterparts in mind. Many equivalences can be found and observations of the classical protocol can be translated into the quantum case. Let us briefly look at two ways to implement an anonymous broadcasting protocol using classical means.

2.1.1. Random Strings

A trusted referee prepares a binary strings of lenghts N, where N is the number of players taking part in the protocol. This string is created randomly with the only condition of containing an even number of 1's. The referee distributes the string, such that each player obtains one bit. Every player announces publicly the value of their bit. The sender applies a NOT-gate to their bit before announcing it in order to send a 1. A 0 is sent if he announces his bit truthfully. All players can by counting the number of 1's announced reconstruct the sent bit by observing the parity. An odd parity means a 1 has been broadcast. This protocol does not reveal the senders identity. Since the original bit string was randomly created, the observed parity changing bit-flip is equally likely to have occurred on any bit. Messages of length m can be sent repeating this protocol m times.

Anonymity is endangered, if the referee is not fully trustworthy. He knows the whole original string and can deduce the senders identity from the announced bits of the players.

2.1.2. Shared Secret Bits

A way around the trusted referee problem is the following, as proposed in [1]. The N players sit in a circle. Player n shares a random bit r_n with their neighbour $n+1$. To create their personal bit b_n, each player applies an OR-gate on the two bits they saw: $b_n = r_{n-1} \oplus r_n$. Since every random bit r_n has been seen twice, the sum of all b_n's is even.

The rest of the sending and readout part of the protocol are carried out as in section 2.1.1. This version eliminates the need for a trusted referee and associated problems. It is however not completely secure against mischievous players.

Conspiring players: Two players, E_1 and E_2, assuming they are not direct neighbours, can collaborate to obtain information about the senders identity. Since the players are arranged in a circle, E_1 and E_2 split the remaining players into two groups, $\mathcal{A}$ and $\mathcal{B}$. I a round where 1 was sent, E_1 and E_2 can deduce if the sender is in $\mathcal{A}$. This is done by applying on OR-gate on the two bits r_n that E_1 and E_2 shared with player in $\mathcal{A}$. If all announced bits from $\mathcal{A}$ together with the newly created bit have odd parity, the sender is in $\mathbb{A}$.

Such collaborations can be made more difficult, if the graph of shared bits between players is more connected. This increases the number of players needed to conspire. Full security is reached, if the graph is fully connected. I.e. if all possible pairs of players share a secret bit. Such a cheat would now require $N-1$ conspirators and is thus trivial. However, this solution requires $N(N-1)/2$ randomly created bits, scaling with $\mathcal{O}(N^2)$, which makes it impractical for large N.

2.2. Problems with classical protocols

The referee in 2.1.1 can be bribed and mischievous players can break anonymity in 2.1.2. But all classical protocols have even more fundamental security issues. As classical information can be copied infinitely, and classical transmission can be eavesdropped unbeknownst to the sender and receiver, all classical protocols are fundamentally flawed. Let us thus turn our focus to quantum versions of the anonymous broadcast, where these flaws can be overcome.

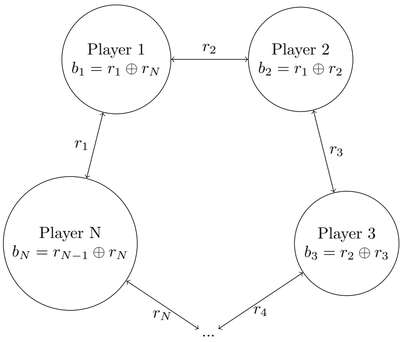

FIG. 1: Random bits r_n are shared between neighbouring players. To obtain their personal secret bit b_n, players apply an OR-gate on the two r_n's they see.

3. QUANTUM VERSIONS OF THE ANONYMOUS BROADCAST

In this section, different quantum versions of the protocol are studied. We start with a close look at a version of the protocol using GHZ-states, as proposed in [2]. To this end, relevant properties and descriptions of the GHZ-state are reviewed. The protocol is then studied with respect to conspiring players and its resilience against errors. Solutions for the arising problems are found in a range of topological versions of the protocol, using the Toric Code or Majorana fermionic excitations in surface codes. Generalizations to higher dimensions are discussed as well.

3.1. Qubit GHZ-States

The GHZ-QAB can be thought of as a quantum version of the protocol presented in 2.1.1. But instead of a trusted referee, a GHZ-state is used to produce random bit-strings of even parity. Thus the protocol is carried out in a very similar fashion as seen above:

3.1.1. The Protocol

The protocol for a single round consists of three parts:

a. Preparation: A N-qubit GHZ-state $|GHZ^+\rangle = |+\rangle^{\otimes N} + |-\rangle^{\otimes N}$ is set up and shared between the N players, such that each player obtains exactly one qubit.

b. Sending: If player s wishes to send a bit 1, he applies $U_{send} = \sigma_s^x$, the Pauli-x matrix acting on his qubit. If he wants to send 0, he does nothing.

c. Readout: For the readout, every player measures his qubit in the z-basis. Each measurement will yield a random outcome $+1$ or -1 for the states $|0\rangle$ or $|1\rangle$ respectively. Each player then announces his measurement result publicly. An even (odd) parity of all announced -1 measurements corresponds to the sent bit 0 (1).

3.1.2. Properties of the GHZ-state

The following N-particle GHZ-states are regarded:

$$\begin{aligned} \left|GHZ^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}\left[\left|+\right\rangle^{\otimes N} \pm \left|-\right\rangle^{\otimes N}\right] \\ &= \sum_{b \in {even \atop odd}} \frac{1}{\sqrt{2^{N-1}}}\left|b\right\rangle \end{aligned} \tag{1}$$

where b is a bit-string of length N.

While the expansion in the x-basis is rather straight forward, in the z-basis, the state is an equal superposition of all even (odd) bit-strings. This is readily understood by expanding $\left|+\right\rangle^{\otimes N}$ and $\left|-\right\rangle^{\otimes N}$ separately in the z-basis. Terms with an odd number of 1's obtain a minus sign from the $\left|-\right\rangle^{\otimes N}$-part which leads to the cancellation of states with even (odd) parity.

Note, the single qubit operation σ_n^x changes $\left|GHZ^+\right\rangle \leftrightarrow \left|GHZ^-\right\rangle$ for all n.

3.1.3. GHZ-state in terms of stabilizers:

For the following discussion, it is helpful to consider the GHZ-states as described by their stabilizer generators $\mathcal{S}$:

$$\mathcal{S}_n^{\pm} := \sigma_n^x \sigma_{n+1}^x \text{ for } n < N,\ \mathcal{S}_N^{\pm} := \pm \bigotimes_{n=1}^{N} \sigma_n^z \tag{2}$$

Note, only the sign of $\mathcal{S}_N$ differs in the description of $\left|GHZ^+\right\rangle$ compared to $\left|GHZ^-\right\rangle$.

As required to have a simultaneous common eigenstate, all stabilizer generators commute pairwise, $[\mathcal{S}_n^{\pm}, \mathcal{S}_m^{\pm}] = 0\ \forall(n,m)$, since $(\sigma_n^x)^2 = \mathbb{1}$, $\left[\sigma_n^{\alpha}, \sigma_{m \neq n}^{\beta}\right] = 0$ and $\left[\sigma_n^{\alpha}\sigma_m^{\alpha}, \sigma_n^{\beta}\sigma_m^{\beta}\right] = 0$.

While the sending gate σ_n^x commutes with $\mathcal{S}_{n<N}^{\pm}$, it anticommutes with $\mathcal{S}_N^{\pm}$. This results in the change $\left|GHZ^+\right\rangle \leftrightarrow \left|GHZ^-\right\rangle$, as discussed above.

Since this last stabilizer acts the same on all qubits, such an operation can not be traced back to a single player. This assures the senders anonymity.

Note also that the readout is measured in the z-basis. Thus, the readout checks, whether the given state is stabilized by $\mathcal{S}_N^+$ or $\mathcal{S}_N^-$.

The parallels between this and the classical protocols are striking. It is therefore an obvious step to check the equivalence of the trusted referee - the state preparation. Ways to protect against collaborating players are discussed as well.

3.1.4. GHZ-State Preparation for Anonymous Broadcasting

In the classical version of the protocol (section 2.1.1), a referee is needed to prepare bit-strings. Here, random bit-strings are created by measurement of GHZ-states in the z-basis. But the preparation of the state by a referee might still be exploited to breach anonymity.

For a m-bit message, $m + \epsilon$ GHZ-states are prepared, where ϵ depends on the trust between players and referee. Out of all states, ϵ are chosen at random to check if they indeed are $\left|GHZ^+\right\rangle$-states. To this end, two $LOCC$ checks are carried out. The first is done as the normal readout by measuring each qubits separately in the z-basis.

$$H_{check1} = \prod_{n=1}^{N} \sigma_n^z \tag{3}$$

This measurement is expected to give a random string with an even number of 1's, as seen in (1). It makes sure that the given state is stabilized by $\mathcal{S}_N^+$.

The second check is a measurement of all qubits in the x-basis.

$$H_{check2} = \prod_{n=1}^{N} \sigma_n^x \tag{4}$$

According to (1), this reveals one of two measurement outcomes. Either all players measure $+1$ or all measure -1. It probes the stabilizers $\mathcal{S}_{n<N}^+$.

Since both test measure individual qubits in anticommuting bases, rather than measuring parities, only one test can be carried out on a given state. But after successfully testing several states, the confidence is high for all states to be stabilized by all $\mathcal{S}_n^+$. The only ones to pass both tests are $\left|GHZ^+\right\rangle$.

3.1.5. Conspiring Players

Again, we assume two conspiring players E_1 and E_2 splitting the remaining $N-2$ players into two groups, $\mathcal{A}$ and $\mathcal{B}$. $N_{\mathcal{A}(\mathcal{B})}$ is the number of qubits in each group. E_1 and E_2 control additional quantum resources $\mathcal{E}$. Their goal is to deduce to which group the sender belongs. In principle they are allowed to produce any state $\left|\psi\right\rangle$, as long as it passes the checks introduced above.

For simplicity, let us consider the simplest case, where the groups $\mathcal{A}$ and $\mathcal{B}$ consist of one single player each, A and B. This is a valid assumption, if all players in $\mathcal{A}$ and $\mathcal{B}$ are assumed to play nicely. Then, their whole subspace can be collapsed into one single qubit, as it is stabilized by $N_{\mathcal{A}(\mathcal{B})} - 1$ stabilizers. The sending unitary is thus $\sigma_{A(B)}^x$ and the readout $\sigma_{A(B)}^z$.

The second check (4) can be carried out at any time. The conspiring players thus have to make sure that state $|\psi\rangle$ is an eigenstate of $H_{check2} = \sigma^x_A \sigma^x_B \sigma^x_{E_1} \sigma^x_{E_2}$ at all times:

$$\sigma^x_A \sigma^x_B \sigma^x_{E_1} \sigma^x_{E_2} |\psi\rangle = |\psi\rangle \tag{5}$$

To still obtain information about the subgroup to which the sender belongs, the conspiring players want to make sure that the state $|\psi\rangle$ is also an eigenstate of $\sigma^z_A \sigma^z_{E_1} \sigma^z_{E_2}$ and $\sigma^z_B \sigma^z_{E_1} \sigma^z_{E_2}$:

$$\sigma^z_A \sigma^z_{E_1} \sigma^z_{E_2} |\psi\rangle = \sigma^z_B \sigma^z_{E_1} \sigma^z_{E_2} |\psi\rangle = |\psi\rangle \tag{6}$$

This leads to a contradiction between (5) and (6): These operators do not commute and thus can not have a simultaneous eigenstate.

Introducing additional quantum resources $\mathcal{E}$ does not work either: The above operators could be extended such that they would commute. Using the hermitian $H'_{\mathcal{E}}$ and $H''_{\mathcal{E}}$ which fulfil $\{H'_{\mathcal{E}}, H''_{\mathcal{E}}\} = 0$. This would generate measurements like $\sigma^z_A \sigma^z_{E_1} \sigma^z_{E_2} H'_{\mathcal{E}}$, which does not convey the desired information, unless $H'_{\mathcal{E}}$ itself is a stabilizer. In which case, it would anticommute with the stabilizer extended by $H''_{\mathcal{E}}$.

3.2. Qudit GHZ-States

So far, each player controlled a qubit, a quantum system with dimension $d = 2$. In this section, players are given access to higher particles where $d > 2$, so called qudits. First, the protocol is generalized to this new framework. Then, advantages and extensions of the protocol possible with this approach are discussed.

For the following the generalized Pauli matrices are used:

$$\sigma^x = \sum_{j=1}^{d} |j\rangle\langle j \oplus 1| \tag{7}$$

$$\sigma^z = \sum_{j=1}^{d} \omega^j \, |j\rangle\langle j| \tag{8}$$

where $\omega = e^{2\pi i/d}$.

The stabilizers for a generalized GHZ-state are:

$$\mathcal{S}^k_n := \sigma^x_n (\sigma^x_{n+1})^\dagger \text{ for } n < N, \; \mathcal{S}^k_N := \omega^k \bigotimes_{n=1}^{N} \sigma^z_n \tag{9}$$

where k gives the parity of the state when measured in the z-basis on every qudit.

Higher dimensional systems allow to distinguish d messages per round. This implies less rounds for a classical message of a set length. But it also allows for generalizations, such as the anonymous rating. If N players rate on a scale from 0 to q, the required dimension of carrying out this protocol is bound by $d \leqslant qN$.

3.2.1. Environmental Noise

Simple *LOCC* checks can prevent collaborating players from breaking anonymity. This is a clear advantage over comparable classical protocols. But so far, only perfect gates and measurements were considered. This, however, is not a physical assumption. In reality, flawed devices and environmental noise gravely affect the system. In this section we investigate quantum noise and consider, if it endangers the anonymity of the sender. We compare the use of qubits versus qudits with different d. The effects of faulty devices for sending and measuring are studied in the next section 3.2.2.

To be able to fairly compare qubits with qudits, the following error model is chosen: A random hermitian $(d \times d)$ matrix H is created. The diagonal entries β_i are chosen at random in $[0, \delta_{max}]$. Complex off-diagonal entries $\alpha_{i,j}$ are also chosen at random, but from all complex number with $|\alpha_{i,j}| \leqslant \delta_{max}$.

$$H_{rand} = \begin{pmatrix} \beta_1 & \alpha_{1,2} & \alpha_{1,3} & \cdots & \alpha_{1,d} \\ \alpha^*_{1,2} & \beta_2 & \alpha_{2,3} & \cdots & \alpha_{2,d} \\ \alpha^*_{1,3} & \alpha^*_{2,3} & \beta_3 & \ddots & \alpha_{3,d} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \alpha^*_{1,d} & \alpha^*_{2,d} & \alpha^*_{3,d} & \cdots & \beta_d \end{pmatrix} \tag{10}$$

To obtain a unitary matrix, the created hermitian matrix is exponentiated:

$$U_{rot} = exp(i\theta H_{rand}) \tag{11}$$

where θ is a random angle within $[0, \theta_{max}]$.

To probe the effect of this error model on the anonymous broadcast, such a unitary is applied to all qudits right before the readout. The sending and readout are assumed to be perfect gates in this section.

This error model simulates small angle rotations around arbitrary axes. These rotations are uncorrelated between qudits.

First, the effect of this error model on the qubit protocol is studied. Every (2×2)-unitary can be expressed as a sum of Pauli matrices. Thus, it is sufficient to study their effect on the state. The unity $\mathbb{1}$ has but a trivial effect, and σ^y_n can be expressed as $\sigma^y_n = i\sigma^x_n \sigma^z_n$. It is thus sufficient to study the effect of σ^x_n and σ^Z_n on singe qubits.

The error channel σ^x_n has the same effect on the state as the sending unitary. This means, the sent bit gets inverted if this error does occur. The second relevant error channel σ^z_n has a more involved

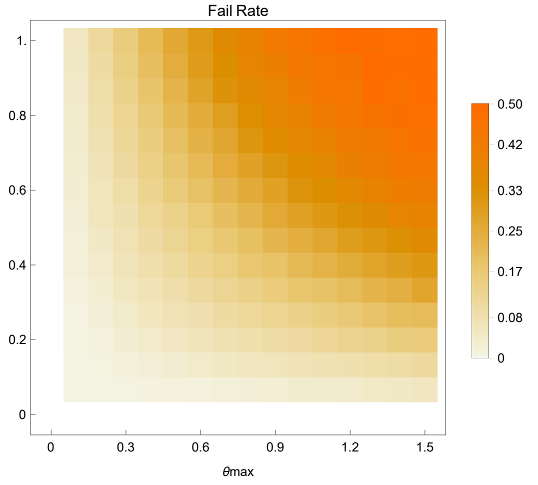

FIG. 2: The probability of a failed transmission with respect to δ_{max} and θ_{max} for environmental noise.

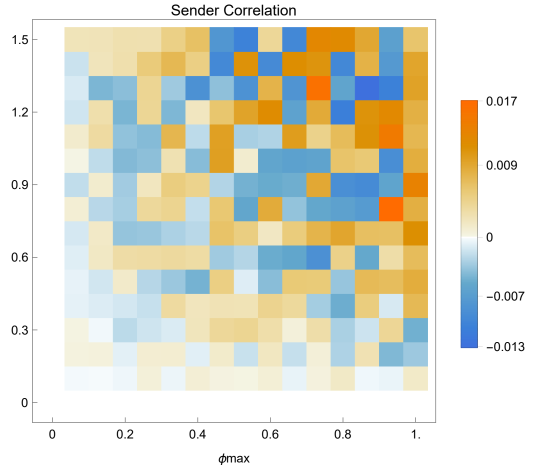

FIG. 3: Normalized correlation between senders measurement result compared of those of the other players for varying δ_{max} and θ_{max}.

effect on the state. But since the readout is performed in the z-basis, such an error does commute with the readout and does not affect the results at all.

Thus, environmental noise might corrupt the sent messages, but is not threat to the anonymity.

FIG. 2 shows the probability of a failed transmission as a function of θ_{max} and δ_{max}. It was created using $N = 3$, the sender was assumed to control the second qubit. Each data point is the average value of 1000 iterations.

As can be seen, either $\delta_{max} = 0$ or $\theta_{max} = 0$ ensure perfect transmission.

The relative probability of having the sender measuring a different outcome than the other players was studied as well. Such a correlation would reveal their identity. Specifically, $P_{brokenanonymity}(\theta_{max}, \delta_{max})$ from (12) was evaluated.

$$P_{brokenanonymity}(\theta_{max}, \delta_{max}) = \frac{p(+1,-1,+1) - (p(+1,+1,-1) + p(-1,+1,+1))/2}{p(+1,-1,+1) + p(+1,+1,-1) + p(-1,+1,+1)} \tag{12}$$

As can be seen in FIG. 3, there is no predictable correlation to be found.

To compare qudits with different d, θ_{max} is fixed to be 1.5 bigger than δ_{max}. This reduces the number of variables, while maintaining a sensible model. FIG. 4 shows the fail rates for $d = 2, 4$ and 8.

For $\delta_{max} \to 1$, the fail rate P_{fail} approaches $\frac{d-1}{d}$. To fairly compare different d's, the fail rate is corrected to be $\widetilde{P}_{fail} = 1 - (1 - P_{fail})^{\frac{1}{\log_2(d)}}$. When comparing qudits with $d = 2^k$ to virtual qudits made up of k qubits, this rate is helpful. It gives an upper bound for an acceptable fail rate for each of the k qubits. Below this bound, qudits composed of k qubits outperform real qudits. As one can see in the lower graph of FIG. 4, the rates are higher for larger values of d. In this error model, it is thus favourable to compose a qudit out of multiple qubits, instead of using a physical qudit.

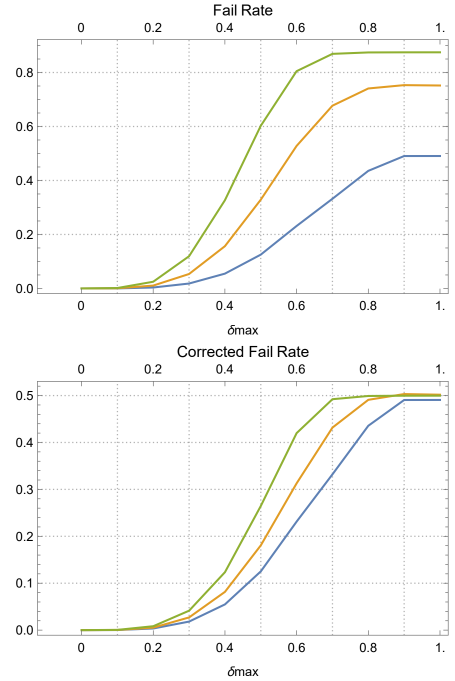

FIG. 4: Probability of a failed transmission with $\theta_{max} = 1.5\delta_{max}$ assuming environmental noise. The lines show how qudits of different dimensions are affected: $d = 2$ in blue, $d = 4$ in orange, and $d = 8$ in green. The lower graph is corrected to make different d's comparable.

3.2.2. *Faulty Devices*

The state preparation is controlled by the checks from (3) and (4). Thus, a fundamental trust in the preparation of the states is established beforehand. But during the sending- and the readout-step, players rely on devices to carry out unitary rotations or measurements.

The error model considered in 3.2.1 introduces small angle rotations. Here, the sending is assumed to happen slightly off-axis. Thus, a unitary as in (11) is used, to rotate the sending gate:

$$\widetilde{U}_{send} = U_{rot}^{\dagger} U_{send} U_{rot} \tag{13}$$

Similarly, the readout is done off-axis as well. The hermitian used to make the single qudit measurements is rotated as well.

$$\widetilde{H}_{readout} = U_{rot}^{\dagger} H_{readout} U_{rot} \tag{14}$$

Note, for each qudit a new random U_{rot} is considered. Also, the way in which the values for β_i and $\alpha_{i,j}$ are chosen is changed. β_i and the imaginary part of $\alpha_{i,j}$ are now assumed to be positive. This corresponds to a minimal correlation between the errors happening on different qudits. But since the devices are the error sources, such an assumption is reasonable.

FIG. 5 shows the probability of a failed transmission as a function of δ_{max} and θ_{max}. This data is obtained by running a simulation 1000 times for each point with uncorrelated random parameters.

As before, θ_{max} is fixed with respect to δ_{max} as $\theta_{max} = 1.5\delta_{max}$. The result for different d is shown in FIG. 6.

The fail rate is higher as in FIG. 4, which is due to the fact that the senders qudit experiences the error twice, once for the act of sending, and once when the readout is carried out.

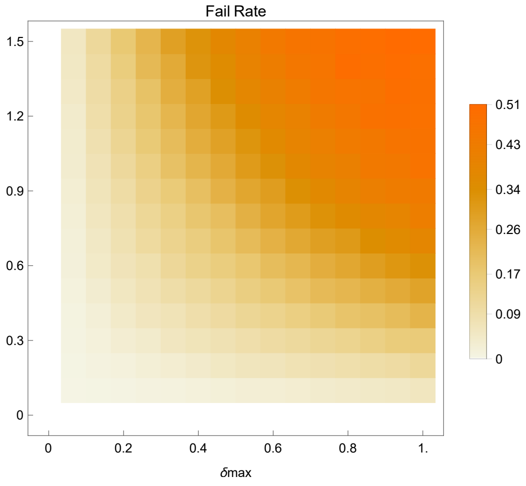

FIG. 5: The probability of a failed transmission with respect to δ_{max} and θ_{max} for faulty devices.

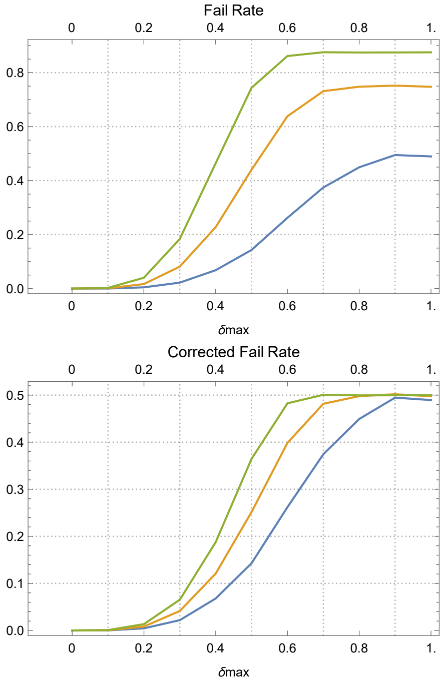

FIG. 6: Probability of a failed transmission with $\theta_{max} = 1.5\delta_{max}$ assuming faulty devices. The lines show how qudits of different dimensions are affected: $d = 2$ in blue, $d = 4$ in orange, and $d = 8$ in green. The lower graph is corrected to make different d's comparable.

To investigate how the senders anonymity is affected by the considered error model, we first have to identify suitable metric. Measurements which yield the same outcome for all players except for one are considered. The rate at which these occur is compared to the rate, at which the same measurement outcomes are obtained in a different permutation. FIG. 7 shows this correlation for the outcomes $(\omega^0, \omega^1, \omega^0)$ compared to $(\omega^1, \omega^0, \omega^0)$ and $(\omega^0, \omega^0, \omega^1)$ using a formula equivalent to (12).

The outcome $(\omega^0, \omega^1, \omega^0)$ has, according to the data presented in FIG. 7 a up to 17% higher relative likelihood of being measured than either $(\omega^1, \omega^0, \omega^0)$ or $(\omega^0, \omega^0, \omega^1)$.

Again, θ_{max} is fixed to $1.5\delta_{max}$, in order to compare different d's. See FIG. 8 for the results.

Surprisingly, the correlations peak at a certain value of δ_{max}, before dropping down again. This peak happens to coincide with the point, where the fail rate starts to plateau in FIG. 6. After this point is reached, the high occurrence of errors destroys any correlation.

For small δ_{max}, the chance to identify the sender is higher for larger d's. On the other hand, the number of different outcomes increases dramatically with for large d's: There are $d^{(N-1)}$ possible measurement outcomes on N qudits, which all

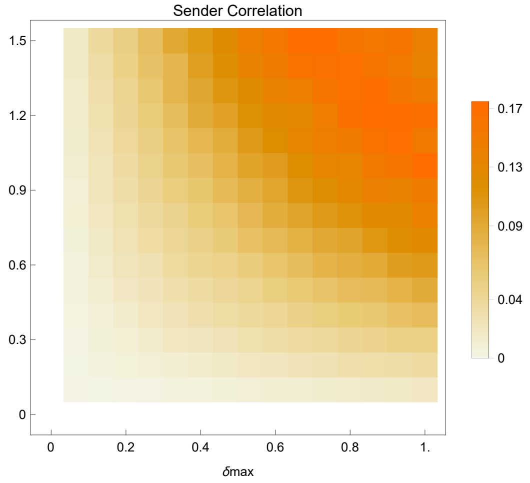

FIG. 7: The probability to identify the sender using qubits and faulty devices, shown for varying values of δ_{max} and θ_{max}.

encode the same message. Ignoring permutations this number reduces to $\binom{N+d-1}{N}$. This reduces the chance to get enough comparable measurement outcomes. $\binom{N+d-1}{N}$ is maximal, if $d = N + 1$. The dimension of the qudits should thus be chosen to be as close as possible to $N + 1$. This does not hold for qudits composed of k qubits. There, the announced measurement results correspond to a unique measurement of the k qubits. Thus, they all can be used to probe for correlations.

In cases where anonymity is valued more than a low error rate, qudits with $d = N + 1$ are the best choice.

3.3. QAB on the Toric Code

The GHZ-protocol has a surprisingly high resilience against errors. The fail rate and the correlations between sender and non-sender readouts are reasonable. Especially considering the fact that no error correction is performed. For high error rates tough, errors render the protocol useless and worse, make the identification of the sender possible.

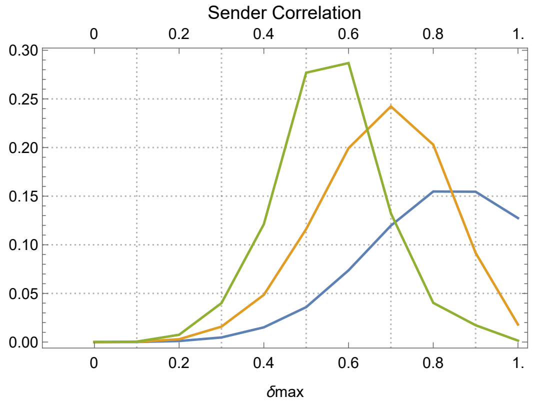

FIG. 8: The probability to identify the sender for $d = 2$ (blue), $d = 4$ (orange), and $d = 8$ (green). θ_{max} is fixed as $1.5\delta_{max}$.

A fault-tolerant way to perform this protocol is thus desired. An obvious candidate is Kitaevs Toric Code [3]. It is known to store information in a fault tolerant fashion. The non-trivial braiding statistics of emerging anyonic excitations can be used to manipulate quantum information. However, the accessible operations do not allow for universal computation[1].

Please see appendix A for more details on the Toric Code.

3.3.1. *Mediate Stabilizer Measurements*

To maintain anonymity of the sender, it is desirable to spatially separate the different players taking part in the protocol.

As seen in FIG. 21, stabilizers on the Toric Code have support on 4 qubits each. To share a single Toric Code between distant players, a way to mediate stabilizer measurements between players has to be found. Here, a scheme relying on Bell-Pairs is used. We assume player a has a rough edge while neighbouring player b has a code with a smooth edge. They share $2L$ Bell-Pairs $(|00\rangle + |11\rangle)/\sqrt{2}$, one for each vertex and plaquette. To measure A_v (B_p), the perform joint σ^x (σ^z)-parity measurements on the qubits belonging to the vertex (plaquette) and on the qubit from the Bell-pair (see FIG. 9). The parity of their respective outcomes determines the occupancy of the vertex (plaquette).

Using only shared Bell-Pairs and *LOCC*, this scheme allows to mediate stabilizer measurements.

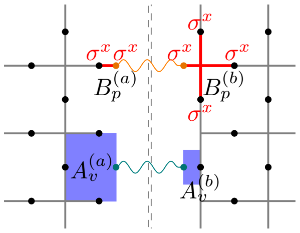

FIG. 9: Wavy lines connect Bell pairs, shared by distant players a on the left and b on the right. They measure their part of the shared vertex (red) and plaquette (blue) together with their half of a Bell-Pair. The occupation of the vertices and plaquettes is obtained by comparing their results using classical communication.

[1] There do exist more involved ideas, using magic state injection [4], or extensions of the original code such as the 3D colour code [5].

But we want a specific state to perform the quantum anonymous broadcast. In the following, ways to prepare such states are investigated.

3.3.2. Ways of Preparation

Splitting a Toric Code: A referee prepares a $(NL) \times L$ Toric Code in the logical state $|\psi_{init}\rangle = |0+\rangle$ by measuring X_1 and Y_2 and correcting. Here, Z_1 and X_2 are defined to be the logical operators with support on L qubits each (see FIG. 10). Next, $\prod_v(\mathbb{1} + A_v)$ and $\prod_p(\mathbb{1} + B_p)$ are applied. This does not change the logical state, but creates the equal superposition of all even number of non-trivial e- and m-loops wrapping around the torus in the short direction, where L qubits lay.

Next, the torus is split into N cylinders of dimension $L \times L$. Each player receives one such cylinder, as shown in FIG. 11. This does not change the logical state of the whole system if the method from section 3.3.1 is used to mediate stabilizer measurements at the edges between players. Interestingly, each player has now access to one of the Pauli measurement on each logical qubit, namely X_1 and Z_2. The other logical operations, Z_1 and X_2, are distributed and can only be measured if all players cooperate via *LOCC*. The part of these measurements controlled by player n shall be called $Z_1^{(n)}$ and $X_2^{(n)}$ respectively.

In the basis of the local logical operators, $X_1, Z_1^{(n)}$ and $X_2^{(n)}, Z_2$, the distributed Toric Code is a GHZ-state: All X_1 and Z_2 measurements will yield the same outcome, whereas $Z_1^{(n)}$ and $X_2^{(n)}$ fulfil the parity constraint. This is in this case set by the fact that an even number of strings go around the non-trivial loops. Thus, we can use one single torus to send two bits of classical information.

A similar set-up is discussed in [6] using a continuous-variable version of the Toric Code.

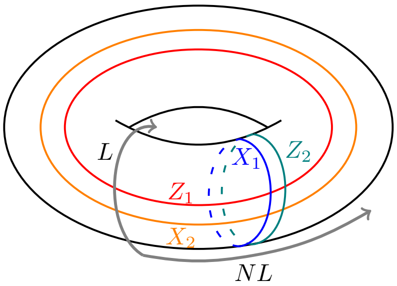

FIG. 10: The set up used to create a state on the Toric Code, usable to broadcast anonymously. The Toric Code has dimensions $(NL) \times L$, the logical X_1 and Z_2 measurements wrap around the short directions and have support on L qubits. Z_1 and X_2 have support on NL qubits.

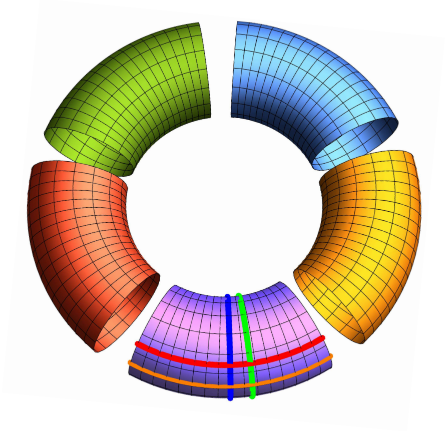

FIG. 11: Torus after splitting for $N = 5$. The coloured lines stand for the logical operators accessible by one single player: blue: X_1, red: $Z_1^{(n)}$, orange: $X_2^{(n)}$ and green: Z_2.

Surgery of Planar Codes: For this method, each player starts with an open boundary code prepared in the $|+\rangle$-state. Next, each player changes his code to a cylinder, by fusing two boundaries together. This can be understood in the framework of lattice surgery, as discussed in section 4.2.1. Ordinarily, such a surgery is carried out between two distinct surface codes. It measures the parity of the two encoded logical qubits while collapsing them into a single one. But since we fuse two boarders of the same planar code in this example, the parity is trivial and the state of the logical qubits is not changed.

This first surgery step is carried out between two smooth edges, which hold e-anyons and determine the logical state of the qubit when measured in the z-basis.

In a second step, all N cylinders are fused using once again lattice surgery. Here, rough edges are fused, resulting in a $X_1^{(n)}X_1^{(n+1)}$-parity measurement between neighbouring codes. These measurements are carried out in sequence going around the circle. If a measurement has outcome -1 the newly added surface code is corrected. Each added code adds a new $X_1^{(n)}X_1^{(n+1)}$-stabilizer. Since each individual code was prepared in a $|0\rangle$-state, they were originally stabilized by $Z_1^{(n)}$ and $Z_1^{(n+1)}$. After the surgery, these stabilizers change to a single $Z_1^{(n)}Z_1^{(n+1)}$-stabilizer. Each subsequent surgery step adds a new X_1X_1-stabilizer while adding a new Z_1 to the end of the singe $Z_1Z_1...Z_1$-stabilizer.

After $N-1$ steps of surgery, the logical qubits are stabilized by the GHZ$^+$-stabilizers as seen in (2). At this stage, we still have two open boundaries. The final surgery appears to be trivial, since it measured the parity $X_1^{(1)}X_1^{(N)}$, which is a product of all other two-qubit stabilizers. But importantly, the topology of the whole code is changed if the last surgery is carried out. From a surface code with semi-open boundary conditions, a Toric Code with periodic boundary conditions is formed. This results in the capacity of a whole new logical qubits to be stored (see appendix A).

This new logical qubit can be measured by two logical operators along non-contractible loops (see FIG. 22). In the here considered situation, one of these logical operators wraps around the long way of the torus with support on NL physical qubits. These measurements can in principle be caried out on codes with open boundary conditions. But their measurement outcomes are meaningless, since it is depending on the exact path of e- and m-strings. When one boundary is closed, like after the first surgery, the e-strings are forced to all be closed. X_2 would thus be measuring an even number and assume the second qubit is in state $|+\rangle$. But since Z_2 is still not a sensible measurement, the second qubit is in fact behaving more like a classical bit. We denote this, by adding a bar over its state. After the first surgery, the system is thus in a state $|0\bar{+}\rangle$.

Only when the final surgery is performed and the Torus is formed is the full access to this second logical qubit gained. But it remains stabilized by X, and is thus in the state $|+\rangle$.

Just as above, a logical qubit $|+\rangle$ stored in a Toric Code distributed amongst N players can be interpreted as a GHZ-state distributed amongst these players.

As a result, this protocol produces the same final state as the protocol described in the above paragraph.

Comparing the two Preparation Methods: Classical communication is cheap, but quantum communication is not. Thus, we should consider which of the above protocols requires a lower number of Bell-Pairs. In the end state, both protocols require $2NL$ bell pairs to mediate certain stabilizer generators. If we assume that the trusted referee preparing the Torus in the first protocol is himself a player, then we still have to distribute $N-1$ $(L \times L)$-codes amongst all players. They could be teleported individually, resulting in a need for $(N-1)L^2$ additional Bell-Pairs. The surgery method starts out with distributed surface code. Therefore no such teleportation step is required. Overall, it uses less quantum resources, which makes it more favourable.

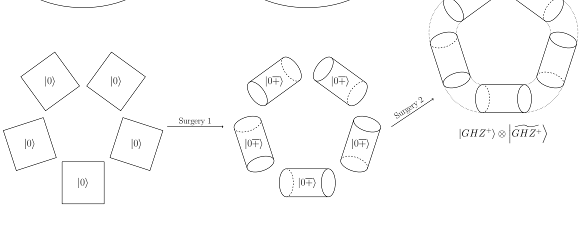

FIG. 12: The top line shows the preparation of a single torus. A state is prepared and the torus is split and distributed. The bottom line shows, how surgery is used to first transform open boundary surface codes into cylinders with semi-open boundary conditions, before fusing them to one single torus.

3.3.3. Protocol

Once a suitable state is prepared, the quantum anonymous bradcast follows a protocol very similar to the one described in section 3.1.1. This does make sense, considering that the prepared state corresponds to GHZ-states. The biggest differences are the unitaries, which now have support on multiple qubits. And the fact that the Toric Code stores two logical qubits and can thus be used to sent two classical bits.

a. Preparation: A distributed Toric Code is prepared in a state equivalent to the GHZ-state. This is done as described in section 3.3.2.

b. Sending: Depending on the sender s wants to send, they apply the logical operations $H_{send} = X_1$ or $H_{send} = Z_2$ on their part of the Toric Code.

c. readout: For the readout, players collaborate to measure Z_1 and X_2 using $LOCC$ only. Each players measurement will yield a random outcome of $+1$ or -1. Each player then announces his measurement result publicly. The parity of all announced measurements corresponds to the sent message.

3.3.4. Attacks and checks

The same argument from section 3.1.5 can be applied here as well. Note, this proof encompasses the most general case of adding extra quantum resources. Consequentially, even cheats that evoke topologies differing from the genus 1 torus are covered by it.

3.4. Majorana fermions

Majorana fermions are non-abelian anyons with the following fusion rules:

$$\begin{aligned} \sigma \times \sigma &= \mathbb{1} + \psi \\ \psi \times \sigma &= \sigma \\ \psi \times \psi &= \mathbb{1} \end{aligned} \tag{15}$$

where × signifies fusion and the + distinguishes possible fusion channels. $\mathbb{1}$ is the vacuum which fuses trivially with all particles, σ represents a Majorana and ψ a Dirac fermion. The fusion outcome

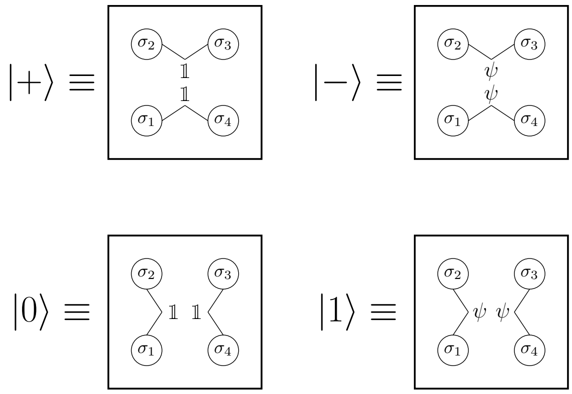

FIG. 13: Four Majoranas encode 1 logical qubit in their fusion space. The horizontal fusion corresponds to a measurement in the x-basis on the encoded qubit. Measuring the fusion outcomes in the vertical direction corresponds to the z-basis.

of Majoranas is governed by the history of the single Majorana fermions and global parity constraints. These rules can be read backwards to obtain decay channels.

The fusion space of two Majorana fermions is 2 dimensional. But it can not be used to store a qubit in it, since only one basis can be measured. To access all three orthogonal bases, four Majoranas governed by an overall parity constraint must be considered. Conventionally, it is assumed that the total parity is vacuum. One popular encoding scheme is presented in FIG. 13. Four Majoranas are prepared in a square. Fusing the two in the top row can result in two outcomes, vacuum or a Dirac fermion, $\mathbb{1}$ or ψ. Due to the fixed parity on all four Majoranas, this outcome fixes the fusion of the bottom pair. The horizontal fusion corresponds to a measurement in the x-basis. The two different fusion outcomes represent the states $|\mathbb{1}\mathbb{1}\rangle_h = |+\rangle$ and $|\psi\psi\rangle_h = |-\rangle$. The vertical fusion conversely corresponds to a z-measurement and thus $|\mathbb{1}\mathbb{1}\rangle_v = |0\rangle$ and $|\psi\psi\rangle_v = |1\rangle$.

Exchanging two neighbouring Majorana fermions has the following effect:

$$R_{j,j+1} = \frac{e^{-i\pi/8}}{\sqrt{2}}(1 + i\ \Pi_{j,j+1}) \tag{16}$$

with $\Pi_{j,j+1} = ic_jc_{j+1}$ as the parity operator, c_j is the operator corresponding to the j-th Majorana mode. Note, these operators fulfil the fermionic anticommutation relations $\{c_i, c_j\} = 0$.

The exchange of pairs of Majoranas has a non-trivial effect on future fusions. Let us for example consider the effect the braiding of σ_2 around σ_3 has on $\Pi_{1,2}$:

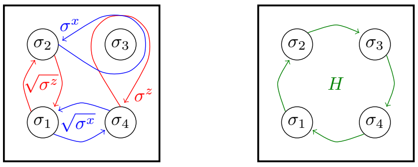

FIG. 14: Exchanging two Majoranas has the effect of a square root of a Pauli. Braiding two Majoranas is like exchanging twice, thus the full Pauli is obtained. The Hadamard gate is a rotation of all Majoranas, as shown on the right.

$$\begin{aligned} &\Pi_{1,2} \mapsto (R^{\dagger}_{2,3})^2\ \Pi_{1,2}\ (R_{2,3})^2 = \\ &(e^{+i\pi/4})\ c_2c_3\ ic_1c_2\ c_3c_2\ (e^{-i\pi/4}) = \\ &c_2c_3\ ic_1c_2\ c_3c_2 = -ic_1c_2 = -\Pi_{1,2} \end{aligned} \tag{17}$$

The parity operator has acquired a minus sign in this process, inverting the fusion outcome. This can be used to manipulate information stored in the fusion space of four Majorana fermions. Using the convention of FIG. 13, braiding and exchanging these four Majorana modes give access to the full single qubit Clifford group. In FIG. 14, all necessary operations are presented.

3.4.1. Majoranas on a Toric code

In this section and the next a more primitive encoding scheme than the one introduced above is used to carry out the QAB. Here, we rely on the Toric Code. Introducing twists or defects in the lattice creates Majorana fermions[7, 8]. Such twists are introduced on a shared Toric Code in such a fashion that each one shares a pair of Majoranas which each of their neighbours. Each such pair of Majoranas fuses to vacuum.

To do the readout, each player fuses his two Majoranas. Individually, each outcome is random and the two outcomes 1 and ψ are equally likely. But since all Majorana fermions where created out of vacuum, the total number of ψ's obtained must be even, in accordance with particle conservation.

To send, a player announces the opposite readout from what he obtained. A second possibility is to share two pairs between neighbouring players. Braiding between these pairs changes the parity of both. To send m bits, $2N(m + 1)$ Majoranas are needed, with one additional line used for braiding.

Braiding Majoranas is said to be a fault tolerant process, since only the topology of the path is relevant. This makes a study of errors obsolete at this point.

A group of conspiring players could try to obtain information about the senders identity by fusing Majoranas from different players. See section 2.1.2 for the classical analogy. This process however can not go unnoticed on a torus. Fusion of Majoranas from different players requires the movement of Majoranas through parts of the torus controlled by players not in on the conspiracy. Changes in the topology can be picked up on by preparing the torus in a GHZ state applying checks, just as in section 3.3.

If a minimal code distance D is required, this method requires mND^2 physical qubits for a message length m and N players. One logical qubit stored in the Toric Code is used to check the topology. The other one is used together with $2N(m-1)$ Majoranas for the QAB. The remaining $2Nm$ Majoranas are used to manipulate the bits sent by the other Majoranas. This requires the same number of physical qubits as for the Toric Code protocol with perfect trust in all other players. When certain players are mistrusted, the Majorana method excels.

3.4.2. N(N-1) protocol

Majoranas can be created on surface codes with arbitrary topology. But to ensure that no unwanted fusion was happening, the topology of the torus was required above. If a surface with different genus is used, this check does not necessarily work. Thus, the protection against collaborating players is potentially removed. As in the classical case, this can be prevented by making the graph of shared Majoranas more connected.

For pure anonymity, i.e. no information gained through a sub-set of collaborating players, the graph has to be fully connected. This requires each player to be in charge of at least $N-1$ Majoranas. For an even number of players, $N-1$ becomes odd, making it impossible to measure the total charge of the Majoranas controlled by an individual player. In this case, some players share 2 pairs of Majoranas, giving each player control over N Majoranas. The smallest amount of total Majoranas required for N players is thus $2N(N-1)$.

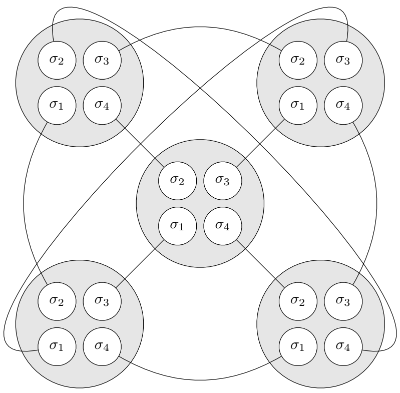

FIG. 15: A fully connected graph for $N = 5$ players. Each player (grey circle), has control over 4 Majoranas (white circles). Such a set-up guarantees full anonymity independent of the topology of the used surface code.

In general, $2NM$ Majoranas are required, where M is the lower bond on the number of players needed to collaborate to obtain information about the senders identity.

This set-up has the advantage that it can be used in any system containing Majorana excitations. The draw back is that the number of Majoranas grows with $\mathcal{O}(N^2)$. This increases the number of physical qubits required dramatically for a set code distance D. Especially, if the number of players N is large.

3.4.3. Majorana GHZ-states

A third approach to using Majorana fermions as a means to transmit classical information anonymously, relies on the power of 4 Majorana fermions to encode one qubit in their fusion space. In addition to the single qubit operations from section 3.4, parity measurements on neighbouring logical qubits are required to create a GHZ-state.

In section 4, the question how these parity measurements can be performed is addressed. For now it is assumed, we are able to perform measurements which tell us about the collective charge of 4 Majoranas in a non-destructive fashion. This can be used to probe the XX-parity of two neighbouring logical qubits, each encoded by four Majorana fermions. The collective charge of two Majoranas from the same column of each qubit gives the XX-parity. This is, if the encoding scheme from FIG. 13 is used.

To create a GHZ-state encoded in $4N$ Majoranas, we arrange them as can be seen in FIG. 14. If we assume to prepare all logical qubits in the $|0\rangle_L$ eigenstate, then the $ZZ...Z$-parity measurement is not required to be carried out. Next, we start on the left and measure the XX-parity between logical qubit 1 and 2. This is done by measuring the total charge within the blue coloured region. If the outcome is -1, a σ_2^z is applied, by braiding horizontally on the second logical qubit, as seen in FIG. 14. Now, we continue to the second and third

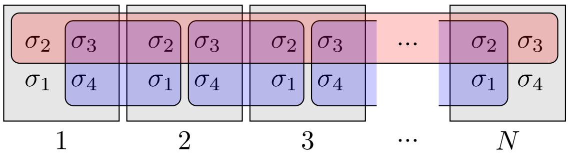

FIG. 16: A N qubit GHZ state, where each qubit is encoded using four Majoranas. The grey boxes define a single qubit. The coloured boxes represent collective charge measurements as stabilizers. The red one does not need to be measured if the qubits are all initialized as $|0\rangle$.

qubit and repeat these steps.

Since only XX-parities have been measured and only single qubit σ_n^z gates have been performed, the $ZZ...Z$-parity is still intact. The resulting state is a GHZ-state. Note the resemblance to the second preparation scheme from section 3.3.2.

After this preparation, the protocol is carried out as above. The sender s performs a σ_s^x if they wish to send a 1. Then, all players measure their qubit in the z-basis by fusing the two Majoranas in the top column for example. As before, the parity of the obtained results contains the sent bit.

3.5. Parafermions

Parafermions are a higher dimensional generalizations of Majorana fermions. In [9], the prospect of using parafermions for means of quantum computing was explored. Their fusion rules are:

$$\begin{aligned} \sigma \times \sigma &= \sum_{k=0}^{d-1} \psi_k \\ \psi_g \times \sigma &= \sigma \\ \psi_g \times \psi_h &= \psi_{g \oplus h} \end{aligned} \tag{18}$$

where σ are parafermions with dimension d and ψ_k are flavours of fermion, with ψ_0 being the vacuum. $\oplus$ denotes addition modulo d.

Again, four parafermions can be used to store a qudit with dimension d in their fusion space. Braiding has the desired effect of applying a higher dimensional Pauli operator, as in (7, and (8)) on the encoded qubit. Certain surface codes are known to exhibit parafermions as excitations [10], the protocol for Majoranas on a torus and the one using $N(N-1)$ pairs of Majoranas can thus easily be extended to parafermions.

Interestingly, unlike Majoranas, parafermions allow for the implementation of an entangling gate by braiding alone. Specifically, the CNOT-gate is obtainable, which allows for the implementation of the qudit GHZ-stabilizers as in (9) by braiding and preparation of logical qudits in a certain state alone. This is possibly an easier path to walk than relying on non-destructive parity measurements of multiple Majoranas. On the flip side, the codes that exhibit parafermionic excitations seem to be more difficult to realize than codes with Majorana fermionic excitations.

3.6. Related protocols

Shared tori, each encoding one bit of classical information which can only be read out if all players cooperate, can be used for more than anonymous broadcasting. A secret sharing protocol can easily be thought of, where all players have to collaborate to obtain a piece of classical information. More involved ways to split the tori can be used to account for differences in the importance between players. For example, a cylindrical piece of the torus can be shared between a subgroup $\mathcal{A}$ of all N players. This is done such that each player in $\mathcal{A}$ still has access to the relevant logical operation on this part of the torus. Now, to obtain the secret bit, it is sufficient if one of the players in $\mathcal{A}$ collaborates with the remaining players outside of $\mathcal{A}$.

4. NON-DESTRUCTIVE COLLECTIVE CHARGE MEASUREMENTS

Through braiding alone, the full single qubit Clifford group is fault tolerantly accessible for a logical qubit stored in the fusion space of four Majorana fermions. Unfortunately, this is not sufficient to get an entangling gate between two qubits encoded in such a fashion. Here, a different prospect of achieving this goal is studied: the non-destructive measurement of the collective charge of multiple Majorana fermions. First, a way is proposed to do such a measurement in the Matching Code [11]. An introduction two the Matching Code in the depth needed to understand the following is given in appendix B. A second approach is given, building on the corner Majorana interpretation put forward in [8].

4.1. In the Matching Code

$2n$ free Majorana modes are created on a Matching Code by flagging n path stabilizers. An area $\mathcal{P}$ is defined, enclosing all $2n$ Majoranas. A matching of the unpaired Majoranas is made and paths are chosen to connect these pairs. The according path stabilizers stay flagged, but factor in the process of colouring the plaquettes black and white.

The effective numbers of ϵ's and e's within $\mathcal{P}$ are defined as

$$\begin{aligned} n_{eff}(\epsilon) &= n(\epsilon) \oplus n(m) \\ n_{eff}(e) &= n(e) \oplus n(m) \end{aligned} \tag{19}$$

where $n(x)$ is the real number of type x-anyons within $\mathcal{P}$, and $\oplus$ is addition modulo 2. In this picture, all m-anyons are part of a composite $\epsilon = e \times m$, the effective number of e anyons corrects any offset this caused.

Measuring the effective number of ϵ's within $\mathcal{P}$ is thus achieved by measuring all stabilizers accounting for m- and ϵ-anyons, i.e. all $W_{p\in b}$ and S_l inside $\mathcal{P}$, also the flagged ones. Since $\prod_l S_l \prod_{p\in b} W_p = \mathbb{1}$ on closed surfaces, this measurement only affects spins on the boundary $d\mathcal{P}$.

If the code is within the stabilizer space, then all excitations in $\mathcal{P}$ have to live on flagged paths.

The above described measurement thus gives the parity of the fusion. If other anyonic excitations are present, then all black plaquettes and all non-flagged paths within $\mathcal{P}$ are to be measured as well. The difference in these two results modulo 2 reveals $n_{eff}(\epsilon)$ and thus the total parity of all $2n$ Majoranas within $\mathcal{P}$.

An alternative explanation is that the measurement of the spins on $d\mathcal{P}$ counts the ϵ-strings entering $\mathcal{P}$. After accounting for non-relevant ϵ's, this gives the occupation of the flagged string operators. Which is exactly the wanted result, the number of fermions obtained when fusing all enclosed Majoranas.

In [12], an equivalent idea is presented considering Majorana modes at the endpoints of dislocation in Kitaev's surface code.

4.2. Corner Majoranas and Surgery

The following section studies a novel interpretation, of how information is stored in open boundary surface codes. The common image relies on the occupation of the edge. An alternative interpretation put forward in the following identifies the corners to host Majorana modes. Quantum information is stored in the fusion space of these four Majoranas.

It is well known that static twists in surface codes host Majorana modes at their endpoints[7, 13]. The same effect can be obtained by removing certain single stabilizer generators. The following discussion builds on a modification of Kitaev's planar code proposed by Wen in [14]. It is obtained by considering the planar code as described in appendix A and replacing vertices (plaquettes) with white (grey) plaquettes and applying a Hadamard gate on half of the physical qubits. After rotation by 45° and cropping, a code as shown in FIG. 17. The regular stabilizers are shown on the right.

For certain double plaquettes, the stabilizer generators are replaced by $\widetilde{W_d} = W_g W_w$, the dyon stabilizer. The white plaquette stabilizer remains unchanged for the double plaquette. These alternative stabilizer generators are shown on the right of the vertical line in FIG. 17. Note that the dyon is now detecting m anyons, while the associated white plaquette stabilizer sees the composite particle $\epsilon = e \times m$.

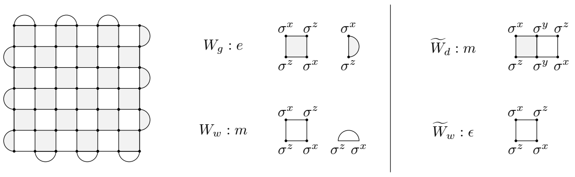

FIG. 17: An open boundary Wen plaquette model. The standard stabilizer generators are shown on the left of the line. Here, m anyons live on grey plaquettes, e's on white plaquettes. On the right, an alternative set of stabilizer generators is shown. The six-term dyon stabilizer detects m's, the white plaquette stabilizer ϵ's.

Next, two double plaquettes are selected and stabilized by the alternative stabilizer generator $\widetilde{W_d}$. The two white plaquette stabilizers $\widetilde{W_w}$ acting within the selected double plaquettes are removed. An example can be seen in FIG. 18, where the two selected double plaquettes are coloured red.

We identify the logical Z_L to be the occupation of one of the white plaquettes. X_L conversely has to change the occupation of the defect. Any operator moving an ϵ from one selected white plaquette to the works. A specific choice for Z_L and X_L is shown in FIG. 18.

To increase the tolerance against X-errors, the separation between the selected plaquettes is increased. For more resilience against Z-errors, the single defects are expanded. This is achieved by selecting a neighbouring double plaquette, stabilizing it using the alternative operators and removing $\widetilde{W_w}$. An additional stabilizer is introduced with the effect of moving an ϵ between the two double plaquettes. This can be repeated to enlarge, shrink and move the defects.

It can be verified that the end points of a single such defect behave like Majorana fermions. The fusion channels are obtained by measuring the occupation of the defect. The presence of an ϵ-anyon corresponds to the fusion to a Dirac fermion ψ. The effect of deforming a defect until it is turned by 180° gives the exchange statistic of paired Majoranas. Exchanging the end points of two separate defects reveals the braid statistics. All findings are indeed consistent with the claim of finding Majoranas at the end points. Please refer to [8] for these proofs.

This leads to a realization of non-abelian excitations on a surface code without the need for physical deformations of the lattice. As only the redefinition of local stabilizers is needed to move the Majoranas around, such an approach seems favourable. This prospect is also discussed in [15].

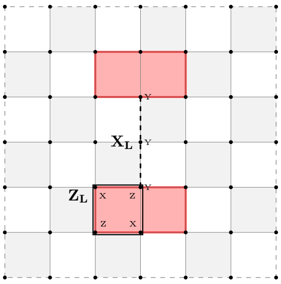

FIG. 18: Two ϵ-defects are used to store one logical qubit by only measuring the dyon stabilizer and removing the white plaquette stabilizer generators on the red coloured double plaquettes. A set of possible operators acting on this logical qubit are indicated.

On an open boundary planar code, ϵ-defects can be joint with the corners. This process creates one fewer new stabilizer generator as it removes $\widetilde{W}_w$'s. The total number of logical qubits is thus decreased by one. Still, the endpoint of this defect should host a Majorana mode. This can be explained by assuming the presence of a Majorana fermion in the corner of the code. In the following, such Majoranas are referred to as corner Majoranas. What follows is a discussion on lattice surgery in the presence of corner Majoranas.

In FIG. 13, an encoding scheme using four Majorana fermions to store one logical qubit has been presented. It turns out, an equivalent scheme can be used for the corner Majoranas, to encode the information stored in the code's stabilizer space. A path fusing the two Majorana modes with support on the top-edge is equivalent to the logical measurement Z_L, up to multiplication by plaquette stabilizers. If the code is in the stabilizer space and all plaquettes are empty, this multiplication has but a trivial effect.

An exchange of corner Majoranas leads to the implementation of the $\sqrt{Z_L}$ and $\sqrt{X_L}$ gates. A clockwise or counter-clockwise rotation of all Majoranas to the neighbouring corner realises the Hadamard gate. Thus, the full single-qubit Clifford group is accessible in this picture.

4.2.1. Lattice Surgery

Lattice surgery enables entangling gates to be carried out. It was first proposed in [16]. Here, we focus on the variation used in [17]. The fusion of two lattices using surgery is shown in FIG. 19. Through creating of new plaquettes, the parity of the two encoded logical qubits is measured. After surgery, one larger surface code is obtained, storing one single qubit.

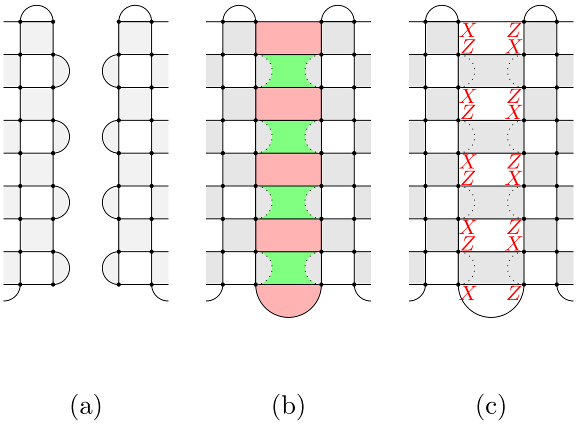

FIG. 19: (a) The boundaries of two Wen plaquette models to be fused. (b) Extended grey-plaquette stabilizers are shown in green. The red plaquettes are newly formed white-plaquette stabilizers. (c) In red, the measurements of the white-plaquette stabilizers is equivalent to the parity of logical Z's on both codes.

A very similar operation was used in section 3.4.3, where multi Majorana parity measurements were used to achieve the same effect. In the following, we want to show that lattice surgery has this exact effect on corner Majorana modes. I.e. it is a destructive way of measuring the parity of four Majorana modes.

One can convince oneself of this fact by considering the following protocol, see FIG. 20. In a first step, corner Majoranas get pulled in the code. Next, new stabilizers are defined, where the two original edges meet. Importantly, these stabilizers are not measured. Now, the corner Majoranas are moved to two double plaquettes in the centre of the code. Lastly, their parity is measured by probing the occupation of said double plaquettes.

This whole process is equivalent to measuring the plaquette stabilizers within an area encompassing all newly created plaquettes. Since the original codes where prepared in the stabilizer space, all plaquettes present before the surgery and the ones that were extended are unoccupied by anyonic excitations. The only ones factoring into the measurement outcome are the newly created plaquettes. Measuring them is, as seen in FIG. 19, equivalent to measuring the parity of the two logical qubits.

We can conclude by stating that lattice surgery can be interpreted as fusion of corner Majoranas from different codes. This delivers the parity of the encoded qubits.

Note, both plaquettes in FIG. 19 have to me measured to obtain the parity. Measurement of one single plaquette does not contain any information about the parity. Instead, it corresponds

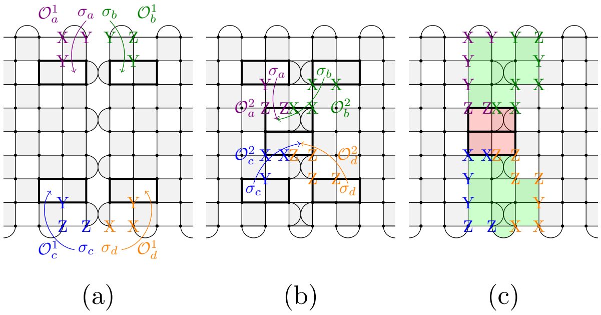

FIG. 20: Part (a) shows an example for operators that move the Majorana modes from the corners into the codes. The framed double plaquette depicts the end point of this movement. In (b) the second part of the movement is shown. Note that this happens after the codes are merged. Also note that the central physical qubit is acted on by two different $\mathcal{O}$'s. Finally, in (c) the product of all previous operators is shown. This is equivalent to the product of all green plaquette stabilizers. The red plaquettes are measured in the final step where the Majoranas are fused and the collective fermionic charge is determined. The whole procedure is equivalent to standard lattice surgery.

to the measurement of a newly created degree of freedom, stemming from the fact that the number of constraints is reduced by one, while keeping the number of Majorana modes constant.

What if the protocol is only carried out partially? Not measuring the $\widetilde{W}_w$ on the red plaquettes leaves the Majorana modes on the defects in middle of the code. The collective charge of these Majoranas is well defined by the parity of the two originally encoded qubits. Thus, a measurement of the parity $X_L^{(1)} X_L^{(2)}$ on both codes reveals the total Majorana parity. This is yet another way to carry out non-destructive multi Majorana parity measurements.

This idea is closely related to measuring loops around multiple defects hosting unpaired Majorana modes as presented in [12]. The parity measurement $X_L^{(1)} X_L^{(2)}$ forms a closed loop around the defect, by connecting to the open boundaries.

Acknowledgement

Many thanks to my supervisors Jiannis K. Pachos, James W. Wootton and Daniel Loss for supervising and making this international project possible.

I would also like to thank my fellow students for many interesting physics and non-physics related discussions, in particular: János, Kamil, Kon, Kris, Chris, Chris, Nick and Alex.

[1] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of cryptology*, vol. 1, no. 1, pp. 65–75, 1988.

[2] M. Christandl and S. Wehner, "Quantum anonymous transmissions," in *ASIACRYPT*, pp. 217–235, Springer, 2005.

[3] A. Y. Kitaev, "Fault-tolerant quantum computation by anyons," *Annals of Physics*, vol. 303, no. 1, pp. 2–30, 2003.

[4] E. T. Campbell and J. O'Gorman, "An efficient magic state approach to small angle rotations," *arXiv preprint arXiv:1603.04230*, 2016.

[5] H. Bombin, R. Chhajlany, M. Horodecki, and M. Martin-Delgado, "Self-correcting quantum computers," *New Journal of Physics*, vol. 15, no. 5, p. 055023, 2013.

[6] N. C. Menicucci, T. F. Demarie, and G. K. Brennen, "Anonymous broadcasting with a continuous-variable topological quantum code," *arXiv preprint arXiv:1503.00717*, 2015.

[7] H. Bombin, "Topological order with a twist: Ising anyons from an abelian model," *Physical review letters*, vol. 105, no. 3, p. 030403, 2010.

[8] K. Laubscher, M. S. Kesselring, B. J. Brown, and J. R. Wootton, "Surface code implementation of the full clifford group," 2016.

[9] A. Hutter and D. Loss, "Quantum computing with parafermions," *Physical Review B*, vol. 93, no. 12, p. 125105, 2016.

[10] A. Hutter, J. R. Wootton, and D. Loss, "Parafermions in a kagome lattice of qubits for topological quantum computation," *Physical Review X*, vol. 5, no. 4, p. 041040, 2015.

[11] J. R. Wootton, "A family of stabilizer codes for anyons and majorana modes," *Journal of Physics A: Mathematical and Theoretical*, vol. 48, no. 21, p. 215302, 2015.

[12] M. B. Hastings and A. Geller, "Reduced space-time and time costs using dislocation codes and arbitrary ancillas," *arXiv preprint arXiv:1408.3379*, 2014.

[13] O. Petrova, P. Mellado, and O. Tchernyshyov, "Unpaired majorana modes on dislocations and string defects in kitaev's honeycomb model," *Physical Review B*, vol. 90, no. 13, p. 134404, 2014.

[14] X.-G. Wen, "Quantum orders in an exact soluble model," *Physical review letters*, vol. 90, no. 1, p. 016803, 2003.

[15] M. J. B. Ferreira, P. Padmanabhan, and P. Teotonio-Sobrinho, "Realizing the fusion rules of ising anyons without lattice defects," *arXiv preprint arXiv:1508.01399*, 2015.

[16] C. Horsman, A. G. Fowler, S. Devitt, and R. V. Meter, "Surface code quantum computing by lattice surgery." 2012 New J. Phys. 14 123011, 2011. arXiv:1111.4022v3.

[17] A. J. Landahl and C. Ryan-Anderson, "Quantum computing by color-code lattice surgery," 2014. arXiv:1407.5103v1.

[18] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, "Topological quantum memory," *Journal of Mathematical Physics*, vol. 43, no. 9, pp. 4452–4505, 2002.

[19] A. Kitaev, "Anyons in an exactly solved model and beyond," *Annals of Physics*, vol. 321, no. 1, pp. 2–111, 2006.

APPENDIX A: THE PLANAR AND THE TORIC CODE

In this appendix, surface codes as proposed in [18] are reviewed.

The Planar and the Toric Code are very similar and differ only in their boundary conditions. Thus, the two are discussed simultaneously. In a later part of this appendix, the differences and their consequences are highlighted.

Both codes consist of a $L \times L$ square lattice with physical qubits placed on all edges. Each physical qubit is part of two plaquettes and two vertices (see FIG. 21).

Two sets of commutating stabilizer generators are defined. A_v (B_p) is the product of σ^x's (σ^z's) on all physical qubits surrounding a vertex v (plaquette p):

$$\begin{aligned} A_v &= \prod_{i\in v} \sigma_i^x \\ B_p &= \prod_{i\in p} \sigma_i^z \end{aligned} \tag{A1}$$

All stabilizers either act in the same basis, or share an even number of physical qubits. Thus, they all commute and simultaneous eigenstates exist.

The stabilizer space is highly degenerate containing all $|\chi\rangle$ for which $A_v |\chi\rangle = B_p |\chi\rangle = |\chi\rangle \ \forall \ v, p$.
Changing this parity creates anyonic excitations. We distinguish e- and m-anyons, which live on vertices or plaquettes respectively. Single spin (phase) flips create or annihilate m (e) anyons in pairs, or move them to a neighboring plaquette (vertex). Importantly, no stabilizers are violated, if an anyonic excitation is fully wrapped around the torus or moved across an open boundary. These loops/lines, depending on what kind of anyon was moved, are called e- or m-loops respectively.

Open Boundaries: For a $L \times L$ Planar Code with open boundaries, there are $L^2+(L-1)^2$ physical qubits and $2L(L-1)$ stabilizers. This means, one single logical qubit can be stored in an open boundary code.

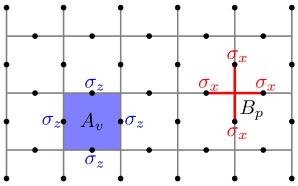

FIG. 21: The Planar/Toric Code lattice. Physical qubits are shown as black dots, they lie on the edges of an underlying lattice, shown in grey. The red cross shows a vertex where the stabilizer A_v acts, the red square a plaquette with its stabilizer B_p.

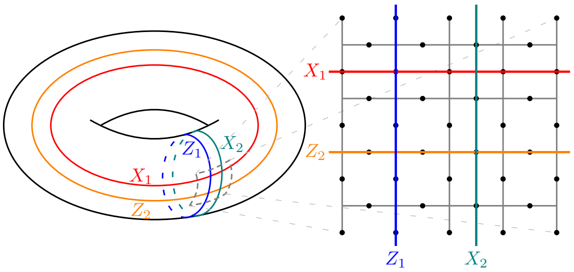

FIG. 22: The left half shows how the logical Pauli-operators wrap around the torus on nontrivial loops. On the right, a detailed picture of the region where they cross. For Z_1, on each qubit lying on the blue line, a σ^z is performed. Analogous for the other logical operators.

The way the edges are constructed allows for only one kind of anyon to be thrown over it. An edge is called rough (smooth), if an e (m)-anyon can be moved over it. Opposite edges have to be of the same type. Information is stored, by the number of anyons an the edges, or equivalently, by the number of e- and m-strings spanning across the code.

Semi-Open Boundaries: If one boundary is periodic, then $L^2 + L(L-1)$ physical qubits are required to make a $L \times L$ Code. The number of plaquette and vertex stabilizers combined is $L^2 + L(L-1)$, but one of them can be expressed as the product of all other stabilizers of the same kind. Consequentially, one logical qubit can be stored.

For the direction with the open boundaries, this is done in the same fashion as described above. In the other direction, non-trivial loops wrapping around the cylinder are used.

Periodic Boundaries: If periodic boundary conditions are assumed, for $2L^2$ physical qubits only $2L^2 - 2$ independent stabilizers are found. This means, 2 logical qubits can be encoded in one Toric Code. Logical qubits are stored by the number of non-contractable e- and m-loops wrapping around the torus.

The logical Pauli-measurements X_k and Z_k, acting on qubit $k \in \{1,2\}$ are depicted in FIG. 22. Each logical operator consists of a sting of single-qubit Paulis wrapping around a non trivial loop. The expected commutation relations are met.

We denote the logical state of the Toric Code as $|\psi_{TC}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle$, with $|\psi_k\rangle$ being the state of the logical qubit k.

APPENDIX B: THE MATCHING CODE

A physical qubit is placed at every vertex of a trivalent lattice. For the following, a honeycomb lattice is considered. The lattice is coloured as shown in FIG. 23.

The three orthogonal bases are associated with one colour each, for example:

$$\alpha_{l\in b} = x$$
$$\alpha_{l\in g} = y$$
$$\alpha_{l\in r} = z$$

For a link l, the link operator $K_l = \sigma_j^{\alpha_l}\sigma_k^{\alpha_l}$ is defined, with $j, k \in l$, α_l is given by the links colour.

Two fundamental types of stabilizer generators are distinguished: Plaquette stabilizers W_p which are the sum of all link operators surrounding a plaquette p (up to a phase of -1):

$$W_p = \sigma_x^1\sigma_y^2\sigma_z^3\sigma_x^4\sigma_y^5\sigma_z^6 \tag{B1}$$

The second type of stabilizer generator is more involved. First, a matching between all vertices is created, such that each vertex is matched with exactly one other vertex. For each matched pair (j, k) we chose one path $P(j, k)$ connecting them and associate a string stabilizer $S_{j,k}$ with it, which is (up to a phase of ± 1 or $\pm i$) the sum of all link operators in said path:

$$S_{j,k} \sim \prod_{l\in P_{j,k}} K_l \tag{B2}$$

Plaquette operators can be thought of as string operators on closed paths around single plaquettes. By construction, all stabilizer generators commute.

Further, a link l is even (odd), if it is part of an even (odd) number of string stabilizers. There ends exactly one string stabilizer at each vertex, due to the way in which the vertices are matched.

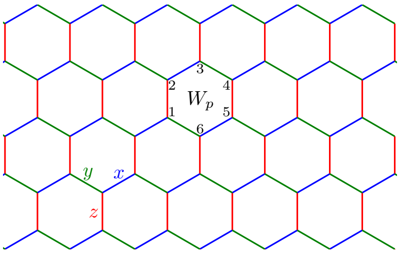

FIG. 23: The honeycomb lattice with a specific choice of coloured links. Each colour is associated with a basis, as shown in the lower left corner. W_p is a plaquette stabilizer acting on the qubits sitting in the numbered vertices.

Thus, there is always an odd number of odd links connected to each vertex. For periodic boundary conditions, this implies that the even links form closed loops, separating the plaquettes naturally into two families. Plaquettes are labelled black b and white w, depending to which family they belong.

Negative eigenvalues of the stabilizers lead to an anyonic excitation. We associate three anyons with the three kinds of stabilizers as follows:

$$W_{p\in b} \leftrightarrow m$$
$$W_{p\in w} \leftrightarrow e$$
$$S_l \leftrightarrow \epsilon$$

The fusion rules are given by the $D(\mathbb{Z}_2)$ anyon model:

$$e\times e = m\times m = \epsilon\times\epsilon = \mathbb{1}, e\times m = \epsilon \tag{B3}$$

Similar as in Kitaevs honeycomb model [19], Paulis acting on single qubits can be mapped to Majorana operators. In this picture, string operators are the parity operator between two Majorana modes at their endpoints.

To obtain Majorana fermionic excitations, single string operators are flagged and removed from the set of stabilizers. This creates one new degree of freedom in our system. Namely the occupation of said string ($\mathbb{1}$ or ϵ) corresponding directly to the parity of the two unpaired Majorana modes at the endpoints.