

Generating k EPR-pairs from an n -party resource state

Sergey Bravyi* Yash Sharma† Mario Szegedy‡ Ronald de Wolf§

Abstract

Motivated by quantum network applications over classical channels, we initiate the study of n -party resource states from which LOCC protocols can create EPR-pairs between any k disjoint pairs of parties. We give constructions of such states where k is not too far from the optimal $n/2$ while the individual parties need to hold only a constant number of qubits. In the special case when each party holds only one qubit, we describe a family of n -qubit states with k proportional to $\log n$ based on Reed-Muller codes, as well as small numerically found examples for $k = 2$ and $k = 3$. We also prove some lower bounds, for example showing that if $k = n/2$ then the parties must have at least $\Omega(\log \log n)$ qubits each.

1 Introduction

1.1 Generating EPR-pairs from a resource state

Quantum communication networks combine several quantum computers to enable them to solve interesting tasks from cryptography, communication complexity, distributed computing etc. Building a large-scale quantum communication network is a daunting task that will take many years, but networks with a few small quantum computers are under construction and may start to appear in the next few years [WEH18].

These networks are either based on channels that physically communicate quantum states, or rely on classical communication in tandem with shared entanglement, or a combination of both. Communication over classical channels cannot increase entanglement, so in the absence of quantum channels we have to rely on prior entangled states. For example, if two parties share an EPR-pair, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, then one party can transmit (“teleport”) a qubit to the other via two classical bits of communication, consuming the EPR-pair in the process [BBC⁺93]. If we want to enable many qubits to be sent in this way, then we could start with an entangled state where each pair among the n parties shares its own EPR-pair. This would allow any pair to exchange a qubit, but would require us to start with a rather large initial entangled state of $\binom{n}{2}$ EPR-pairs, and each of the n parties would need to hold $n - 1$ qubits (see Figure 1 for $n = 4$).

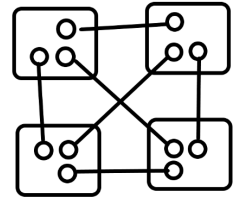


Figure 1: State of $n = 4$ parties with 6 EPR-pairs

*IBM Quantum, IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA. sbravyi@us.ibm.com

†Rutgers University, yash.sharma@rutgers.edu

‡Rutgers University, szegedy@cs.rutgers.edu

§QuSoft, CWI and University of Amsterdam, the Netherlands. Partially supported by the Dutch Research Council (NWO) through Gravitation-grant Quantum Software Consortium, 024.003.037. rdewolf@cwi.nl

Now suppose that we know in advance that only some k pairs out of the n parties will be required to exchange a qubit, but we do not know in advance what those k pairs are. In this paper we study what initial n -party resource states are sufficient or necessary to achieve this task. Note that an EPR-pair between two parties allows them to exchange a qubit in either direction via local operations and classical communication (LOCC), and conversely the ability to exchange a qubit between two parties allows them to share an EPR-pair (one party locally creates the EPR-pair and sends one of its qubits to the other party). This shows that the ability to exchange qubits between any k disjoint pairs of parties is essentially equivalent to the ability to establish EPR-pairs between any k disjoint pairs. We focus on the latter task in this paper.

We call an n -party state $|\psi\rangle$ *k-pairable* if for every k disjoint pairs $\{a_1, b_1\}, \dots, \{a_k, b_k\}$ of parties, there exists an LOCC protocol that starts with $|\psi\rangle$ and ends up with a state where each of those k pairs of parties shares an EPR-pair. The local quantum operations and the classical communication are free, but we do care about the number of qubits per party in $|\psi\rangle$: the fewer the better. The same resource state $|\psi\rangle$ has to work for every possible k -pairing, so it is fixed before the pairing task is given. For example, the n -qubit GHZ-state

$$\frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$$

is 1-pairable: in order to obtain an EPR-pair between two parties Alice and Bob, the other $n - 2$ parties can measure their qubit in the Hadamard basis and communicate the classical measurement outcomes to Alice and Bob, who convert their remaining 2-qubit state into an EPR-pair if one of them (say Alice) does a Z -gate conditioned on the parity of the $n - 2$ bits they received.

The GHZ-example has the minimal possible 1 qubit per party, but unfortunately k is only 1 there. We are interested in resource states that are k -pairable for larger $k \leq n/2$. We give both upper and lower bounds for k -pairability, considering both the situation where we allow $m > 1$ qubits per party (but not too many), and the situation where we insist that each of the n parties has only the minimal $m = 1$ qubits.

1.2 Our results 1: constructions of k -pairable resource states

In Section 2 we first study k -pairable resource states where each of the n parties is allowed to have $O(1)$ qubits (hence $|\psi\rangle$ will have $O(n)$ qubits in total). We show that we can make k as large as $n/\text{polylog}(n)$ while each party holds only 10 qubits. Roughly, the idea is to take a special kind of n -vertex expander graphs that guarantee existence of k edge-disjoint paths for any k disjoint pairs, let each edge in the graph correspond to an EPR-pair, and create the k desired EPR-pairs via entanglement-swapping along the edge-disjoint paths. If we allow $m = O(\log n)$ qubits per party instead of $m = O(1)$, then we can construct k -pairable resource states with $k = n/2$, meaning that from our fixed resource state we can create EPR-pairs across any perfect matching of the n parties into disjoint pairs.¹ This result essentially requires only classical off-the-shelf routing arguments.

Since qubits are expensive, especially when lots of error-correction is needed to protect them, we also look at what is possible when each party holds only 1 qubit, which is of course the bare

¹Note that if we allow one party to hold many more qubits than the others, then we could use a star graph, where the central party shares an EPR-pair with each of the $n - 1$ other parties, and uses entanglement-swapping (see the proof of Lemma 1) to link up the k pairs as desired. This $(2n - 2)$ -qubit state is k -pairable for the maximal $k = n/2$, and $n - 1$ parties hold the minimal 1 qubit. However, the central party holds $n - 1$ qubits and has to do all the work in obtaining the k -pairing. In the spirit of the small quantum networks of small quantum computers that we'll have in the near and medium-term future, we prefer constructions where none of the parties needs to hold many qubits.

minimum. In this case, we construct n -party (which in this case is the same as n -qubit) resource states for the case $k = 1$ for arbitrary n (this corresponds to the GHZ-state). For $k \geq 2$ it is not clear that k pairability is a property monotone in n . What we have is that k -pairable states exist for $k = 2$ for $n = 16$ and higher powers of 2 (we also give numerical evidence for the existence of a 2-pairable state on $n = 10$ qubits); for $k = 3$ for $n = 32$ and higher powers of 2; and for arbitrary k for $n = 2^{3k}$ and higher powers of 2. These resource states will be superpositions over the codewords in a Reed-Muller code, and we use the stabilizer formalism to design LOCC protocols for obtaining the desired k EPR-pairs from the resource state. Our construction is efficient in the sense that all steps in the LOCC protocol can be computed in time $\text{poly}(n)$. To prove correctness of the protocol we reduce the problem of EPR-pair generation to a version of the polynomial regression problem: constructing a multi-variate \mathbb{F}_2 -valued polynomial of fixed degree that takes prescribed values at a given set of points. One of our main technical contributions is developing tools for solving a particular family of such polynomial regression problems.

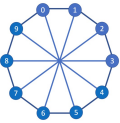

	GHZ state $\frac{ 0^n\rangle + 1^n\rangle}{\sqrt{2}}$	Graph state 	Reed-Muller CSS states $ \psi\rangle \sim \sum_{x \in C} x\rangle$			EPR networks on expander graphs 	
Number of parties n	any	10	16	32	any	any	any
Qubits per party	1	1	1	1	1	10	$\log(n)$
How many EPR-pairs can be generated?	1	2	2	3	$\log(n)$	$\frac{n}{\text{poly}(\log n)}$	$\frac{n}{2}$
	worst					best	

Figure 2: Informal summary of our constructions. We consider resource states of different type shared among n parties such that each party holds a fixed number of qubits ranging between 1 and $\log(n)$. The last row shows the pairability parameter k —the number of EPR-pairs that can be generated by LOCC starting from the respective resource state. For simplicity, we ignore constant factors in the $\log(n)$ scaling and ignore minor restrictions on the number of parties n in certain cases, see Sections 2,3 for details. Our proof of k -pairability is analytic in all cases except for $n = 10$ and 32 where we provide only a computer-aided proof.

1.3 Our results 2: obstructions

Next we look at *obstructions*, namely lower bounds on the achievable tradeoff between n , k , and m . First consider the case where we can pair up any $k = n/2$ disjoint pairs. An ideal resource state would allow us to do this (i.e., be $n/2$ -pairable) with only $m = 1$ qubits per party. As mentioned above, we have shown that k -pairability with only 1 qubit per party is indeed achievable if $k \ll n/2$, but in Section 4 we show it is not achievable if $k = n/2$: in that case $m = \Omega(\log \log n)$ qubits per party are needed. The proof is by an intricate dimension-counting argument, which gives upper and lower bounds on the dimension of the space of states that can be reached (with non-zero

probability) by LOCC protocols on a fixed nm -qubit resource state $|\psi\rangle$. In Section 5 we extend this approach to the case of partial pairings, so where $k < n/2$, showing $m = \Omega\left(\log\left(\frac{k \log n}{n \log \log n}\right)\right)$ in this more general case. In particular, if $m = O(1)$ then k can be at most $O\left(n \frac{\log \log n}{\log n}\right) = o(n)$, so achieving something close to complete pairability (i.e., $k = \Omega(n)$) requires a super-constant number of qubits per party. Up to the power of the polylog, this matches our construction of k -pairable states with $k = n/\text{polylog}(n)$ and $m = 10$ qubits per party (Section 1.2).

1.4 Related work

To the best of our knowledge, the problem of what resource states allow LOCC protocols to construct EPR-pairs between any k pairs of parties has not been studied before. However, we are aware of a number of related works, which we will briefly discuss here.² These works can be organized into two categories.

Entanglement routing assisted by quantum communication.

Here some parties are allowed to exchange qubits in addition to performing LOCC on the initial resource state.

Schoute et al. [SMI⁺16] consider quantum networks where parties can create EPR-pairs with their immediate neighbors and then use entanglement-swapping combined with efficient routing algorithms to create desired long-distance entanglement. This differs from our approach in allowing the ability to create new EPR-pairs when needed (which requires quantum communication), while we allow only LOCC starting from one fixed entangled resource state.

Hahn, Pappa, and Eisert [HPE19] also study a quite similar problem to ours, but starting from a network where some parties are linked via a quantum channel, while some other parties are not (directly) linked at all. In addition to efficiently generating EPR-pairs they also study generating GHZ-states between specified parties.

Pant et al. [PKT⁺19] study how a network whose nodes are connected via lossy optical links and have limited quantum processing capabilities, can obtain EPR-pairs simultaneously between many pairs of nodes; their limitations per node are analogous to our goal of having only few qubits per party, but they allow quantum communication while we allow only classical communication.

Restricted variants of k -pairability.

Here the parties are only allowed to perform LOCC on the initial resource state. The parties may be able to generate k EPR pairs for some but not all choices of such pairs.

Miguel-Ramiro, Pirker, and Dür [MPD23] consider resource states interpolating between the two extreme cases discussed in our introduction: the GHZ state shared among n parties and $\binom{n}{2}$ EPR states shared between each pair of parties. This work proposed clustering and merging algorithms that produce resource states with the desired functionality. However, these methods do not appear to provide k -pairable resource states with few qubits per party.

²We won't go over the literature on quantum network coding (which assumes the ability to send qubits over specific edges) nor the massive experimental physics literature on preparation of entangled states on actual noisy hardware such as optical links and repeaters.

Du, Shang, and Liu [DSL17] study a problem similar to ours but starting from resource states that consist only of pre-shared EPR-pairs between adjacent parties in a given network. Like us, they use entanglement-swapping to create EPR-pairs between distant parties.

Contreras-Tejada, Palazuelos, and de Vicente [CPdV22] gave similar constructions as we gave in Section 2 (with EPR-pairs on the edges of an n -vertex graph), but focus primarily on the question for what type of graphs the long-range entanglement survives constant amounts of noise on the edges.

Illiano et al. [IVK⁺22] study 1-pairable states with the additional property that the identity of the one pair that ends up sharing an EPR-pair remains unknown to the other $n - 2$ parties (in fact one can get this easily from the n -party GHZ-state if the other parties broadcast their measurement outcomes to everyone rather than sending it only to the two parties that want an EPR-pair).

Meignant, Markham, and Grosshans [MMG19] and Fischer and Townsley [FT21] studied what is roughly a partial “dual” of our problem: how many EPR-pairs between which parties of a given n -party network are necessary and sufficient to generate a classically given n -party graph state?

Dahlberg, Helsen, and Wehner [DHW20] show that it is NP-complete to decide whether a classically given n -party stabilizer state can be transformed into a set of EPR-pairs on specific qubits using only single-qubit Clifford operations, single-qubit Pauli measurements and classical communication (such protocols are more restricted than the LOCC we allow in our paper). They also give some algorithms to do the transformation in some special cases [DHW18].

2 Constructions with multiple qubits per party

In this section we combine classical network routing strategies and the standard entanglement swapping protocol to construct n -party k -pairable resource states with k nearly linear in n , such that each party holds at most $m = O(1)$ qubits. Increasing the number of qubits per party from a constant to $m = O(\log n)$ yields maximally pairable resource states with $k = n/2$.

Suppose $G = (V, E)$ is a graph with n vertices $V = \{1, 2, \dots, n\}$. Vertex $i \in V$ represents the i -th party. We place two qubits at every edge $(i, j) \in E$ such that in total there are $n = 2|E|$ qubits. Define an n -party resource state

$$|\psi_G\rangle = \bigotimes_{(i,j) \in E} |\Phi_{i,j}\rangle,$$

where $|\Phi_{i,j}\rangle$ is an EPR-pair located on an edge (i, j) . The state $|\psi_G\rangle$ is shared among n parties such that the two qubits located on an edge $(i, j) \in E$ are assigned to the parties i and j who share the EPR-pair $|\Phi_{i,j}\rangle$. Thus each party shares one EPR-pair with each of its neighbors. Accordingly, each party holds at most d qubits, where d is the maximum vertex degree of G .

Lemma 1. *The resource state $|\psi_G\rangle$ is k -pairable if for any choice of k disjoint pairs of vertices $\{a_1, b_1\}, \dots, \{a_k, b_k\}$ in the graph G , there exist k edge-disjoint paths $P_1, \dots, P_k \subseteq E$ such that the path P_i connects vertices $\{a_i, b_i\}$.*

Proof. Suppose Charlie shares an EPR-pair with Alice and another EPR-pair with Bob. The following well-known entanglement-swapping protocol uses LOCC to create an EPR-pair between Alice and Bob. First, Charlie measures the parity of his two qubits in the standard basis $\{|0\rangle, |1\rangle\}$, sends the 1-bit measurement outcome to Bob, and conditioned on it he applies a σ^x (bitflip) on his second qubit and Bob applies a σ^x to his qubit. This results in a 4-qubit GHZ-state

$\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$). Now Charlie measures each of his two qubits in the Hadamard basis $\{|+\rangle, |-\rangle\}$, sends the parity of the two outcomes to Bob, who conditioned on that bit applies a σ^z (phaseflip) to his qubit. It may be verified that now Alice and Bob share an EPR-pair.

The creation of the k EPR-pairs using the k edge-disjoint paths is now fairly straightforward: the parties on the path from a_i to b_i use the EPR-pairs with their neighbors on the path to create an EPR-pair between a_i and b_i via entanglement-swapping. Because the k paths are edge-disjoint, no edge (=EPR-pair) is used more than once. \square

Below it will be convenient to relax the edge-disjointness condition in Lemma 1 and consider pairability by nearly edge-disjoint paths. More precisely, suppose $p \geq 1$ is an integer. Consider a resource state $|\psi_G\rangle^{\otimes p}$ such that each copy of $|\psi_G\rangle$ is shared among n parties as specified above. Then each party holds at most pd qubits, where d is the maximum vertex degree of G . Each party shares p EPR-pairs with each of its neighbors. An immediate corollary of Lemma 1 is the following.

Corollary 2. *The resource state $|\psi_G\rangle^{\otimes p}$ is k -pairable if for any choice of k disjoint pairs of vertices $\{a_1, b_1\}, \dots, \{a_k, b_k\}$ in the graph G , there exist k paths $P_1, \dots, P_k \subseteq E$ such that the path P_i connects vertices $\{a_i, b_i\}$ and each edge of G belongs to at most p paths.*

To keep the number of qubits per party small, we would like the graph G to have a small vertex degree and, at the same time, allow vertex pairability by (nearly) edge-disjoint paths for any choice of k disjoint vertex pairs. We would like to maximize the pairability parameter k while keeping the vertex degree d as small as possible. Luckily, the problem of constructing such graphs has been already studied due to its importance for classical communication networks. A graph $G = (V, E)$ is said to have *edge expansion* h if for any subset of vertices $S \subseteq V$ with $|S| \leq |V|/2$, the number of edges that have exactly one endpoint in S is at least $h|S|$. We shall use the following fact.

Fact 1 (Broder, Frieze, Upfal [BFU94]). *For any constants $d \geq 3$ and $h > 1$ there exists a constant $c > 0$ such that the following is true. Suppose G is an n -vertex d -regular graph with edge expansion at least h . Then for any choice of $k \leq n/\log^c(n)$ disjoint vertex pairs in G there exists a family of paths P_1, \dots, P_k connecting the chosen pairs of vertices such that every edge of G belongs to at most two paths. These paths can be found in time $\text{poly}(n)$.*

It is known [Bol88] that d -regular graphs with edge expansion $h > 1$ exist for any constant $d \geq 5$ and all large enough n . Thus Corollary 2 and Fact 1 imply that for all large enough n there exist k -pairable resource states with $k = n/\text{poly}\log n$ and at most 10 qubits per party.

Let us say that a graph G is path-pairable if the number of vertices n is even and the condition of Lemma 1 holds for $k = n/2$. We shall need the following fact stated as Corollary 2 in [GMM17].

Fact 2 (Györi, Mezei, Mészáros [GMM17]). *For any integer $q \geq 1$ there exists a d -regular n -vertex path-pairable graph with $d = 18q$ and $n = 18^q$.*

Combining Lemma 1 and Fact 2 we infer that $m = O(\log n)$ qubits per party suffices for complete pairings, in contrast with the naive resource state where every one of the $\binom{n}{2}$ pairs shares an EPR-pair and hence each party holds $m = n - 1$ qubits.

Corollary 3. *There exists a family of n -party $(n/2)$ -pairable resource states with $m = 18 \log_{18}(n) \approx 4.3 \log_2(n)$ qubits per party.*

3 Constructions that use only one qubit per party

In this section we study k -pairability of n -party quantum states under the most stringent restriction: each party holds only one qubit (obviously, k -pairability with $k \geq 1$ is impossible if some party has no qubits). This problem is well-motivated since qubits, especially error-corrected logical qubits, built on top of multiple physical qubits, are expensive and we would prefer to have n -party k -pairable resource states with as few qubits per party as possible.

We have already seen that the n -qubit GHZ-state shared by n parties is 1-pairable. Naively, one might think that the GHZ-example is already best-possible and $k = 1$ is as far as one can get with one qubit per party. Surprisingly, this naive intuition turns out to be wrong. Here we give examples of k -pairable states with one qubit per party for an arbitrary k . We choose the resource state $|\psi\rangle$ as the uniform superposition of codewords of a suitable linear code \mathcal{C} of codelength n . The GHZ-example $|\psi\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$ with $k = 1$ is the special case with the repetition code $\mathcal{C} = \{0^n, 1^n\}$.

To achieve k -pairability for $k \geq 2$ we choose \mathcal{C} as the Reed-Muller code $\text{RM}(k-1, m)$ with a suitable parameter m , see below for details.³ The LOCC protocol converting $|\psi\rangle$ to the desired EPR-pairs can be described by a pair of disjoint subsets $X, Z \subseteq [n]$ such that all qubits contained in Z and X are measured in the standard basis $\{|0\rangle, |1\rangle\}$ and the Hadamard basis $\{|+\rangle, |-\rangle\}$ respectively. The protocol creates EPR-pairs on $2k$ qubits contained in the complement $[n] \setminus (X \cup Z)$. Here $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Finally, a Pauli correction σ^x or σ^z is applied to each EPR qubit a_1, \dots, a_k . The correction depends on the measurement outcomes and requires classical communication from parties in $X \cup Z$ to parties a_1, \dots, a_k .

Our construction is efficient in the sense that the subsets of qubits X and Z can be computed in time $O(n)$ for any given choice of EPR qubits. Furthermore, the initial resource state $|\psi\rangle$ can be prepared by a quantum circuit of size $O(n^2)$. While describing the subsets X and Z is relatively simple, proving that the resulting LOCC protocol indeed generates the desired EPR-pairs is considerably more complicated in the case $k \geq 2$, as compared with the GHZ-example for $k = 1$. For resource states based on Reed-Muller codes $\text{RM}(k-1, m)$, we will see below that the proof can be reduced to solving a polynomial regression problem: constructing a polynomial $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ of degree $k-1$ whose values $f(x)$ are fixed at a certain subset of points x . The number of qubits $n = n(k)$ used by our construction is given by $n(2) = 16$, $n(3) = 32$, and $n(k) = 2^{3k}$ for $k \geq 4$ (note that the number of qubits is the same as the number of parties throughout this section). While this scaling $n(k)$ may be far from optimal, the main value of our result is demonstrating that k -pairability with an arbitrary k is possible in principle even in the most restrictive setting with one qubit per party. To the best of our knowledge, this was not known prior to our work. We leave as an open question whether k -pairable states based on Reed-Muller codes can achieve a more favorable scaling $n(k) = \text{poly}(k)$ or even the scaling $n(k) = O(k \text{ polylog}(k))$ that can be achieved if we allow 10 qubits per party instead of 1 (end of Section 2). Such an improvement may require consideration of more general LOCC protocols that use all three types of Pauli measurements, in the $\sigma^x, \sigma^y, \sigma^z$ bases.

Finally, we describe a numerically-found example of a 10-qubit 2-pairable state with one qubit per party; this is more efficient than the 16-qubit 2-pairable state from the above results. This example is based on a stabilizer-type resource state and an LOCC protocol with Pauli measure-

³We follow the standard notation for the parameter m of Reed-Muller codes. It should not be confused with the number of qubits per party, which equals 1 throughout this section.

ments. We also show that no stabilizer state with $n \leq 9$ qubits is 2-pairable using only Pauli measurements. In that sense our 10-qubit example is optimal.

The rest of this section is organized as follows. We introduce CSS-type resource states and give sufficient conditions for k -pairability of such states in Section 3.1. Reed-Muller codes and their basic properties are described in Section 3.2. We define resource states based on Reed-Muller codes and describe our LOCC protocol for generating EPR-pairs in Section 3.3. A proof of k -pairability for $k = 2, 3$, and for an arbitrary k is given in Sections 3.4, 3.5, and 3.6 respectively. Finally, we describe the 10-qubit 2-pairable example in Section 3.7.

3.1 Pairability of CSS stabilizer states

To describe our construction we need more notation. Let $\mathbb{F}_2^n = \{0, 1\}^n$ be the n -dimensional vector space over \mathbb{F}_2 . Given a vector $f \in \mathbb{F}_2^n$ and a bit index j , let $f(j) \in \{0, 1\}$ be the j -th bit of f . We write $f \cdot g = \sum_{j=1}^n f(j)g(j)$ for the dot product of vectors $f, g \in \mathbb{F}_2^n$. Unless stated otherwise, addition of binary vectors and the dot product are computed modulo two. The weight of a vector $f \in \mathbb{F}_2^n$ is the number of bits j such that $f(j) = 1$. A linear code of length n is simply a linear subspace $\mathcal{C} \subseteq \mathbb{F}_2^n$. Vectors $f \in \mathcal{C}$ are called codewords. The code is said to have distance d if any nonzero codeword has weight at least d . The dual code of \mathcal{C} , denoted \mathcal{C}^\perp , is the subspace of vectors $f \in \mathbb{F}_2^n$ such that $f \cdot g = 0$ for all $g \in \mathcal{C}$. An affine subspace of dimension d is a set of vectors $\{f + h \mid f \in \mathcal{C}\}$, where $\mathcal{C} \subseteq \mathbb{F}_2^n$ is a linear subspace of dimension d and $h \in \mathbb{F}_2^n$ is some fixed vector.

Suppose our n -qubit resource state $|\psi\rangle$ has the form

$$|\psi\rangle = |\mathcal{C}\rangle := \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{f \in \mathcal{C}} |f\rangle, \quad (1)$$

where $\mathcal{C} \subseteq \mathbb{F}_2^n$ is a linear code. Such states are known as Calderbank-Shor-Steane (CSS) stabilizer states [CS96, Ste96, CRSS98]. It is well-known that the state $|\mathcal{C}\rangle$ can be prepared by a quantum circuit of size $O(n^2)$ for any linear code \mathcal{C} , see for instance [AG04]. We begin by deriving a sufficient condition under which a CSS stabilizer state is k -pairable. Below we assume that each of the n parties holds only one qubit.

Lemma 4 (Pairability of CSS stabilizer states). *Suppose $\mathcal{C} \subseteq \mathbb{F}_2^n$ is a linear code. Suppose for any set of k disjoint pairs of qubits $\{a_1, b_1\}, \dots, \{a_k, b_k\}$ there exists a partition of the n qubits into three disjoint subsets*

$$\{1, 2, \dots, n\} = EXZ \quad (2)$$

such that $E = \{a_1, b_1, \dots, a_k, b_k\}$ and the following conditions hold for all $i = 1, 2, \dots, k$:

CSS1: $\exists f \in \mathcal{C}$ such that $f(a_i) = f(b_i) = 1$ and for all $p \in EZ \setminus \{a_i, b_i\}$: $f(p) = 0$

CSS2: $\exists \bar{f} \in \mathcal{C}^\perp$ such that $\bar{f}(a_i) = \bar{f}(b_i) = 1$ and for all $p \in EX \setminus \{a_i, b_i\}$: $\bar{f}(p) = 0$

Then the n -qubit state $|\mathcal{C}\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{f \in \mathcal{C}} |f\rangle$ is k -pairable.

Here and below we use shorthand set union notation $XY \equiv X \cup Y$ whenever X and Y are disjoint sets. The desired EPR-pairs can be generated in three steps. First, each qubit $p \in Z$ is measured in the standard basis $\{|0\rangle, |1\rangle\}$ and each qubit $p \in X$ is measured in the Hadamard basis $\{|+\rangle, |-\rangle\}$. Next, each party $p \in XZ$ broadcasts their binary measurement outcome to a_1, \dots, a_k . Finally, a Pauli correction is applied to each qubit a_i ; this may depend on the measurement outcomes.

Proof of Lemma 4. We assume some familiarity with the stabilizer formalism [CS96, Got98, NC02]. Let σ_j^x and σ_j^z be single-qubit Pauli operators acting on the j -th qubit tensored with the identity on all other qubits. The resource state $|\mathcal{C}\rangle$ has Pauli stabilizers⁴

$$\sigma^x(f) \equiv \prod_{p: f(p)=1} \sigma_p^x \quad \text{for } f \in \mathcal{C}$$

and

$$\sigma^z(\bar{f}) \equiv \prod_{p: \bar{f}(p)=1} \sigma_p^z \quad \text{for } \bar{f} \in \mathcal{C}^\perp.$$

Thus we have $\sigma^x(f)|\mathcal{C}\rangle = \sigma^z(\bar{f})|\mathcal{C}\rangle = |\mathcal{C}\rangle$. Suppose f and \bar{f} obey conditions CSS1, CSS2 for some pair $\{a_i, b_i\}$. Let $m_p = \pm 1$ be the measurement outcome on a qubit $p \in XZ$. Condition CSS1 implies that the stabilizer $\sigma^x(f)$ commutes with Pauli operators σ_p^z on qubits $p \in Z$, which are measured in the standard basis. Thus $\sigma^x(f)$ and $\{m_p \sigma_p^x \mid p \in X\}$ are stabilizers of the final state after the measurement. We infer that the final state is stabilized by

$$S_i^x = \sigma^x(f) \prod_{p \in X: f(p)=1} m_p \sigma_p^x = \sigma_{a_i}^x \sigma_{b_i}^x \prod_{p \in X: f(p)=1} m_p.$$

Here the second equality follows from CSS1. Likewise, CSS2 implies that the stabilizer $\sigma^z(\bar{f})$ commutes with Pauli operators σ_p^x on qubits $p \in X$, which are measured in the Hadamard basis. Thus $\sigma^z(\bar{f})$ and $\{m_p \sigma_p^z \mid p \in Z\}$ are stabilizers of the final state. We infer that the final state is stabilized by

$$S_i^z = \sigma^z(\bar{f}) \prod_{p \in Z: \bar{f}(p)=1} m_p \sigma_p^z = \sigma_{a_i}^z \sigma_{b_i}^z \prod_{p \in Z: \bar{f}(p)=1} m_p.$$

Here the second equality follows from CSS2. This is only possible if the final state contains an EPR-pair on the qubits $\{a_i, b_i\}$, up to a Pauli correction $\sigma_{a_i}^x$ and/or $\sigma_{a_i}^z$. The correction can be applied via LOCC if each party $p \in XZ$ broadcasts their measurement outcome m_p to all parties a_1, \dots, a_k . \square

Thus it suffices to show that for any $k \geq 1$ one can choose a sufficiently large n and a linear code $\mathcal{C} \subseteq \mathbb{F}_2^n$ that satisfies k -pairability conditions CSS1 and CSS2 of Lemma 4. Below we will choose \mathcal{C} from the family of Reed-Muller codes [MS77] to achieve this.

3.2 Reed-Muller codes

First, let us record the definition and some basic properties of Reed-Muller codes. Let $m \geq 1$ be an integer. A Boolean function $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ can be considered as a binary vector of length $n = 2^m$ which lists the function values $f(x)$ for all inputs $x \in \mathbb{F}_2^m$ in some fixed (say, the lexicographic) order. For example, if $m = 2$ and $f(x) = 1 + x_1 x_2$ then we can consider f as a length-4 binary vector

$$[f(00), f(10), f(01), f(11)] = [1, 1, 1, 0].$$

⁴Note that $\sigma^x(f)|\mathcal{C}\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{g \in \mathcal{C}} \sigma^x(f)|g\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{g \in \mathcal{C}} |f+g\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{g' \in \mathcal{C}} |g'\rangle = |\mathcal{C}\rangle$ for any $f \in \mathcal{C}$. Here the third equality uses the fact that \mathcal{C} is a linear code, i.e., a subspace. Furthermore, $\sigma^z(\bar{f})|\mathcal{C}\rangle = |\mathcal{C}\rangle$ since $\sigma^z(\bar{f})|g\rangle = (-1)^{\bar{f} \cdot g} |g\rangle$ for any $\bar{f} \in \mathcal{C}^\perp$ and $g \in \mathcal{C}$.

Reed-Muller code $\text{RM}(r, m)$ has length $n = 2^m$ and its codewords are the n -bit vectors associated with m -variate degree- r polynomials $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$. One can choose generators of $\text{RM}(r, m)$ as a set of monomials $\prod_{j \in S} x_j$ where S runs over all subsets of $[m]$ of size at most r . The monomial associated with the empty set $S = \emptyset$ is the constant-1 function. For example, $\text{RM}(0, m)$ is the repetition code of length $n = 2^m$ since there are only two degree-0 polynomials: $f(x) \equiv 1$ and $f(x) \equiv 0$. We shall use the following facts.

Fact 3 (Code parameters). *The Reed-Muller code $\text{RM}(r, m)$ has dimension*

$$D(r, m) = \sum_{p=0}^r \binom{m}{p}$$

and distance 2^{m-r} .

Fact 4 (Dual code). *Suppose $0 \leq r < m$. Then $\text{RM}(r, m)^\perp = \text{RM}(m - r - 1, m)$.*

Fact 5 (Affine invariance). *Suppose $A \in \mathbb{F}_2^{m \times m}$ is an invertible matrix, and $b \in \mathbb{F}_2^m$ is a vector. If $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ is a degree- r polynomial, then the function $f'(x) = f(Ax + b)$ is also a degree- r polynomial. The map $f \rightarrow f'$ is a bijection of the set of all m -variate degree- r polynomials.*

For the proof of Facts 3, 4, 5, see e.g. Chapter 13 of [MS77]. As a consequence of Fact 5, the resource state $|\mathcal{C}\rangle$ with $\mathcal{C} = \text{RM}(r, m)$ is invariant under a permutation of the $n = 2^m$ qubits defined as $W_\varphi|f\rangle = |f'\rangle$, where $f'(x) = f(\varphi(x))$ for all $x \in \mathbb{F}_2^m$. Here $\varphi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ is any invertible affine map. In other words, $W_\varphi|\mathcal{C}\rangle = |\mathcal{C}\rangle$. This generalizes the symmetry of the n -qubit GHZ-state which is invariant under any permutation of the n qubits.

Recall that minimum-weight codewords of a linear code are non-zero codewords whose weight equals the code distance.

Fact 6 (Codewords from affine subspaces). *A vector $f \in \mathbb{F}_2^n$ is a minimum-weight codeword of $\text{RM}(r, m)$ if and only if the support of f is an $(m - r)$ -dimensional affine subspace of \mathbb{F}_2^m .*

For the proof see, e.g., Proposition 2 and Corollary 4 in [AJ92]. We shall see that verification of conditions CSS1 and CSS2 of Lemma 4 with $\mathcal{C} = \text{RM}(r, m)$ can be reduced to (multiple instances of) the following problem.

Problem 1 (Polynomial regression). *Find a degree- r polynomial $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ that satisfies a system of equations*

$$f(x^i) = g_i \quad \text{for } i = 1, \dots, s \tag{3}$$

where $x^1, \dots, x^s \in \mathbb{F}_2^m$ are distinct points and $g_1, \dots, g_s \in \{0, 1\}$.

Lemma 5. *The polynomial regression problem has a solution f if at least one of the following conditions is satisfied: (1) $s < 2^{r+1}$, or (2) $s = 2^{r+1}$ and $\sum_{i=1}^s g_i = 0$.*

Here the sum $\sum_{i=1}^s g_i$ is evaluated modulo two.

Proof. $\text{RM}(r, m)^\perp = \text{RM}(m - r - 1, m)$ by Fact 4. The code $\text{RM}(m - r - 1, m)$ has distance 2^{r+1} , see Fact 3, and thus every $2^{r+1} - 1$ columns of its parity check matrix are linearly independent. The parity check matrix M of $\text{RM}(m - r - 1, m)$ is the generator matrix of its dual, $\text{RM}(r, m)$, so

the above implies that if $s < 2^{r+1}$, then the rank of the matrix M_X formed by the columns of M with indices from $X = \{x^1, \dots, x^s\}$ is s , so \mathbb{F}_2^X is in the span of the rows of M_X .

If $s = 2^{r+1}$, then the rank of M_X is either 2^{r+1} or $2^{r+1} - 1$. If 2^{r+1} , we proceed as above. If $2^{r+1} - 1$, the only linear combination of the columns of M_X that gives the zero-vector, is the sum of all columns of M_X , and a vector $(g_1, \dots, g_s) \in \mathbb{F}_2^X$ can be generated from the rows of M_X if and only if $\sum_{i=1}^s g_i = 0 \pmod{2}$. \square

3.3 Resource state and LOCC protocol

Our candidate k -pairable state is a CSS stabilizer state $|\mathcal{C}\rangle$ with

$$\mathcal{C} = \text{RM}(k-1, m) \quad (4)$$

and a suitable parameter $m = m(k)$. To describe the subsets of qubits $X, Z \subseteq \mathbb{F}_2^m$ satisfying conditions CSS1 and CSS2 of Lemma 4, we need one extra piece of notation.

Definition 1. Suppose $S \subseteq \mathbb{F}_2^m$ is a non-empty subset. An affine subspace spanned by S , denoted $\text{Aff}(S)$, is defined as

$$\text{Aff}(S) = \left\{ \sum_{v \in T} v \mid T \subseteq S \text{ and } |T| = 1 \pmod{2} \right\}. \quad (5)$$

Thus $\text{Aff}(S)$ contains all vectors that can be written as a sum of an odd number of vectors from S . For example, $\text{Aff}(\{a\}) = \{a\}$, $\text{Aff}(\{a, b\}) = \{a, b\}$, and $\text{Aff}(\{a, b, c\}) = \{a, b, c, a+b+c\}$. Note that $|\text{Aff}(S)| = 2^d$, where $d \leq |S| - 1$ is the dimension of $\text{Aff}(S)$.

Let $n = 2^m$ be the number of qubits. Suppose our goal is to generate k EPR-pairs on pairs of qubits $\{a_1, b_1\}, \dots, \{a_k, b_k\}$. Define a subset of ‘‘EPR qubits’’

$$E = \{a_1, b_1, \dots, a_k, b_k\}$$

and a family of k affine subspaces $\mathcal{S}_1, \dots, \mathcal{S}_k \subseteq \mathbb{F}_2^m$ such that

$$\mathcal{S}_i = \text{Aff}(\{a_i, b_i, c_1, c_2, \dots, c_k\} \setminus \{c_i\}) \subseteq \mathbb{F}_2^m \quad (6)$$

where $c_1, \dots, c_k \in \mathbb{F}_2^m$ are vectors that will be appropriately defined in Sections 3.4, 3.5, 3.6. The c -vectors may depend on the a 's and b 's. The set of EPR qubits E is obviously contained in the union of $\mathcal{S}_1, \dots, \mathcal{S}_k$. We choose the subsets of qubits X and Z in Lemma 4 as

$$X = \mathbb{F}_2^m \setminus (\mathcal{S}_1 \cup \dots \cup \mathcal{S}_k) \quad \text{and} \quad Z = (\mathcal{S}_1 \cup \dots \cup \mathcal{S}_k) \setminus E \quad (7)$$

The subsets E, X, Z are pairwise disjoint and $\mathbb{F}_2^m = EXZ$. We illustrate the relationships between these sets in Figure 3. In the GHZ-example one has $k = 1$ and $\mathcal{S}_1 = \{a_1, b_1\}$. In this case $Z = \emptyset$ and $X = \mathbb{F}_2^m \setminus \{a_1, b_1\}$, that is, the LOCC protocol requires only measurements in the Hadamard basis. In the rest of this section we prove that the vectors c_1, \dots, c_k in Eq. (6) can always be chosen such that the subsets X and Z satisfy conditions CSS1 and CSS2 of Lemma 4.

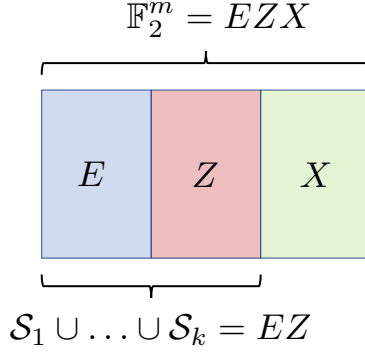


Figure 3: Measurement pattern for the resource state $|\mathcal{C}\rangle$, where $\mathcal{C} = \text{RM}(k-1, m)$ and $\mathcal{C}^\perp = \text{RM}(m-k, m)$. We consider $n = 2^m$ qubits. Each qubit is labeled by an m -bit string. Qubits are partitioned into three disjoint subsets, EZX , where $E = \{a_1, b_1, \dots, a_k, b_k\}$ is the set of EPR qubits, Z is the set of qubits measured in the standard basis $\{|0\rangle, |1\rangle\}$ and X is the set of qubits measured in the Hadamard basis $\{|+\rangle, |-\rangle\}$. We choose $Z = (\mathcal{S}_1 \cup \dots \cup \mathcal{S}_k) \setminus E$, where the \mathcal{S}_i are k -dimensional affine subspaces of \mathbb{F}_2^m , see Eq. (6). These subspaces are chosen such that $\mathcal{S}_i \cap E = \{a_i, b_i\}$ for all i . We choose X as the complement of EZ . A codeword $\bar{f} \in \mathcal{C}^\perp$ satisfying condition CSS2 for some pair of EPR qubits $\{a_i, b_i\}$ is chosen as the characteristic function of the subspace \mathcal{S}_i , that is, $\bar{f}(x) = 1$ if $x \in \mathcal{S}_i$ and $\bar{f}(x) = 0$ if $x \in \mathbb{F}_2^m \setminus \mathcal{S}_i$. A codeword $f \in \mathcal{C}$ satisfying condition CSS1 is constructed using the polynomial regression, see Lemma 5.

3.4 2-pairability

We now need to show how to choose c_1, \dots, c_k . We begin with the simple case $k = 2$.

Lemma 6. *Suppose $k = 2$ and $m \geq 4$. Choose any vector $c \in \mathbb{F}_2^m \setminus \text{Aff}(E)$ and let $c_1 = c_2 = c$. Then the subsets X, Z defined in Eqs. (6,7) satisfy conditions CSS1 and CSS2 with $\mathcal{C} = \text{RM}(1, m)$.*

Proof. Note that a vector c as above exists since $|\text{Aff}(E)| \leq 2^{|E|-1} = 8$ and $|\mathbb{F}_2^m| \geq 16$ for $m \geq 4$. Specializing Eq. (6) to the case $k = 2$ and $c_1 = c_2 = c$ one gets

$$\mathcal{S}_1 = \{a_1, b_1, c, a_1 + b_1 + c\} \quad \text{and} \quad \mathcal{S}_2 = \{a_2, b_2, c, a_2 + b_2 + c\}. \quad (8)$$

The assumption that $c \notin E$ implies that the \mathcal{S}_i are 2-dimensional affine subspaces, and in particular, $|\mathcal{S}_i| = 4$ ($i = 1, 2$). We claim that

$$\mathcal{S}_i \cap E = \{a_i, b_i\}. \quad (9)$$

Indeed, by definition, $a_i, b_i \in \mathcal{S}_i$. Suppose $a_1 \in \mathcal{S}_2$. Since all EPR qubits are distinct, the inclusion $a_1 \in \mathcal{S}_2$ is only possible if $a_1 = c$ or $a_1 = a_2 + b_2 + c$. In both cases $c \in \text{Aff}(E)$, which contradicts the choice of c . Thus $a_1 \notin \mathcal{S}_2$. Applying the same arguments to a_2, b_1, b_2 proves Eq. (9).

Let us first check condition CSS2 with $i = 1$ (the same argument applies to $i = 2$). Choose

$$\bar{f}(x) = \begin{cases} 1 & \text{if } x \in \mathcal{S}_1 \\ 0 & \text{otherwise} \end{cases}$$

Since \mathcal{S}_1 is a 2-dimensional affine subspace, Fact 6 implies that $\bar{f} \in \mathcal{C}^\perp$. We have $\bar{f}(a_1) = \bar{f}(b_1) = 1$ since $a_1, b_1 \in \mathcal{S}_1$. From Eq. (9) one gets $EX \cap \mathcal{S}_1 = E \cap \mathcal{S}_1 = \{a_1, b_1\}$. Thus $\bar{f}(v) = 0$ for all $v \in EX \setminus \{a_1, b_1\}$, as claimed. This proves condition CSS2.

Let us check condition CSS1 with $i = 1$ (the same argument applies to $i = 2$). We can invoke Lemma 5 (polynomial regression) with $r = 1$ and $s = 4$ to show that there exists a degree-1 polynomial $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ such that

$$f(a_1) = f(b_1) = 1 \quad \text{and} \quad f(a_2) = f(b_2) = 0. \quad (10)$$

We can use condition (2) of Lemma 5 since $s = 2^{r+1} = 4$. By definition, f is a codeword of $\mathcal{C} = \text{RM}(1, m)$ and $f(a_1) = f(b_1) = 1$. We need to check that $f(v) = 0$ for all $v \in EZ \setminus \{a_1, b_1\}$. By definition,

$$EZ \setminus \{a_1, b_1\} = (\mathcal{S}_1 \cup \mathcal{S}_2) \setminus \{a_1, b_1\} = \{a_2, \quad b_2, \quad c, \quad a_1 + b_1 + c, \quad a_2 + b_2 + c\}.$$

We already know that $f(a_2) = f(b_2) = 0$ by Eq. (10). Since f is a degree-1 polynomial, one has

$$f(a_1 + b_1 + c) = f(a_1) + f(b_1) + f(c) = 1 + 1 + f(c) = f(c).$$

Likewise, $f(a_2 + b_2 + c) = 1 + 1 + f(c) = f(c)$. If $f(c) = 0$, then we are done. Suppose $f(c) = 1$. Since $c \notin \text{Aff}(E)$ there is an affine subspace S with co-dimension one, which contains $\text{Aff}(E)$, but $c \notin S$. Let g be the linear function that is 0 on S and 1 on \bar{S} . Let $h = f + g$. Then h on a_1, b_1, a_2, b_2 takes the same values as f , but $h(c) = 0$, and we apply the above argument for h instead of f . This proves CSS1. \square

3.5 3-pairability

In the case $k = 3$ we choose $m = 5$ and $\mathcal{C} = \text{RM}(2, 5)$. The resource state $|\mathcal{C}\rangle$ requires $n = 32$ qubits. We checked conditions CSS1 and CSS2 of Lemma 4 numerically using exhaustive search over all tuples of EPR qubits and all choices of vectors c_1, c_2, c_3 in the definition of subsets X and Z . It was observed that for any tuple $\{a_1, b_1, a_2, b_2, a_3, b_3\}$ of EPR qubits, there exists at least one choice of the c -vectors such that X and Z obey conditions CSS1 and CSS2. The search space was pruned by exploiting the affine invariance of Reed-Muller codes, see Fact 5. Namely, choose any invertible affine map $\varphi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ such that $\varphi(a_1) = 0^m$ and $\varphi(b_1) = 10^{m-1}$. Fact 5 implies that a permutation of the $n = 2^m$ qubits described by φ is an automorphism of \mathcal{C} . Thus this permutation of qubits leaves the resource state $|\mathcal{C}\rangle$ invariant and we can assume w.l.o.g. that $a_1 = 0^m$ and $b_1 = 10^{m-1}$. We also pruned the search over the c -vectors by imposing a constraint $c_1 + c_2 + c_3 = 0$ which is analogous to the constraint $c_1 = c_2$ used for $k = 2$. The remaining search over a_2, b_2, a_3, b_3 took less than one hour on a laptop computer. Note that the affine invariance of Reed-Muller codes also implies that $|\text{RM}(2, m)\rangle$ is 3-pairable for all $m \geq 5$ since we can always apply an affine map φ as above such that $\varphi(a_i)$ and $\varphi(b_i)$ has nonzeros only on the first 5 bits. We note that the choice of parameters $r = 2, m = 5$ is minimal for 3-pairability of resource states $|\text{RM}(r, m)\rangle$, as follows from a simple code distance argument.⁵

⁵ k -pairability of the CSS resource state $|\mathcal{C}\rangle$ requires both codes \mathcal{C} and \mathcal{C}^\perp to have minimum distance at least $2k$ since otherwise a stabilizer of $|\mathcal{C}\rangle$ may have support on a subset of the EPR qubits $a_1, b_1, \dots, a_k, b_k$ and anti-commute with some stabilizer of the target EPR-pairs. In particular, 3-pairability requires \mathcal{C} and \mathcal{C}^\perp to have distance at least 6. Reed-Muller codes $\mathcal{C} = \text{RM}(r, m)$ do not have this property for $r = 1$ and $m \leq 4$, see Facts 3, 5. Meanwhile, the code $\text{RM}(2, 5)$ is self-dual and has distance 8.

3.6 k -pairability for an arbitrary k (and sufficiently large n)

In this section we prove that the resource state $|\text{RM}(k-1, m)\rangle$ is k -pairable for any $k \geq 2$ and $m \geq 3k$ (note that the number of parties can be any $n = 2^m \geq 2^{3k}$). First let us exploit the affine invariance of Reed-Muller codes (Fact 5) to convert the set of EPR qubits $a_1, b_1, \dots, a_k, b_k$ into a certain standard form. Choose a linear invertible map $\varphi : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ such that $\varphi(a_i)$ and $\varphi(b_i)$ have zeros on the first k bits for all i (recall that we label the $n = 2^m$ qubits by m -bit strings). This is always possible for $m \geq 3k$. Since the state $|\text{RM}(k-1, m)\rangle$ is invariant under the permutation of the $n = 2^m$ qubit-labels associated with φ , we can replace a_i, b_i by $\varphi(a_i)$ and $\varphi(b_i)$. Accordingly, from now on we assume that a_i and b_i have zeros on the first k bits. The linear map φ can be computed in time $O(m^3)$ using Gaussian elimination. In addition, we can assume that

$$\{a_1, b_1, \dots, a_k, b_k\} \cap \{0^m, a_1 + b_1, \dots, a_k + b_k\} = \emptyset. \quad (11)$$

Indeed, to see this, suppose $h \in \mathbb{F}_2^m$ is a vector whose first k bits are zero, and none of the vectors $a_i + h$ or $b_i + h$ belongs to the set $\{0^m, a_1 + b_1, \dots, a_k + b_k\}$. Using the affine invariance of Reed-Muller codes one can replace a_i and b_i by $a_i + h$ and $b_i + h$. The new vectors a_i, b_i obey the extra condition Eq. (11). The number of bad h s (h s we should not pick) is at most

$$|\{a_1, b_1, \dots, a_k, b_k\}| \cdot |\{0^m, a_1 + b_1, \dots, a_k + b_k\}| = 2k(k+1)$$

(upper bounding the number of all possible differences between the two sets). The number of h s we can pick from (all those vectors starting with k 0s) is at least 2^{2k} . Now $2k(k+1) < 2^{2k}$ (which holds for all $k \geq 2$) gives the claimed property. Hence, from now on we assume Eq. (11).

We choose vectors c_1, \dots, c_k in Eq. (6) as the basis vectors of \mathbb{F}_2^m such that the j -th bit of c_j is 1 and all other bits of c_j are 0,

$$c_j = \underbrace{[0, \dots, 0]_{j-1}}_{j-1}, \underbrace{[1, 0, \dots, 0]_{m-j}}_{m-j}, \quad j = 1, \dots, k. \quad (12)$$

Thus the c -vectors are supported on the first k bits while all a - and b -vectors are supported only on the last $m - k$ bits. Next we use Eqs. (6,7) to define the subsets of qubits $X, Z \subseteq \mathbb{F}_2^m$ to be measured in the Hadamard (X) and in the standard (Z) basis, respectively. For convenience, we restate the definitions of X, Z , and \mathcal{S}_i below.

$$X = \mathbb{F}_2^m \setminus (\mathcal{S}_1 \cup \dots \cup \mathcal{S}_k) \quad \text{and} \quad Z = (\mathcal{S}_1 \cup \dots \cup \mathcal{S}_k) \setminus E,$$

$$\mathcal{S}_i = \text{Aff}(\{a_i, b_i, c_1, c_2, \dots, c_k\} \setminus \{c_i\}).$$

It remains to prove that X and Z satisfy conditions CSS1, CSS2 of Lemma 4 with

$$\mathcal{C} = \text{RM}(k-1, m) \quad \text{and} \quad \mathcal{C}^\perp = \text{RM}(m-k, m).$$

Below we shall use the following property.

Proposition 7. *The affine subspace \mathcal{S}_i is k -dimensional and obeys*

$$\mathcal{S}_i \cap E = \{a_i, b_i\}. \quad (13)$$

Proof. We have $|\mathcal{S}_i| = 2^k$ since all c -vectors are linearly independent and have zeros on the last $m - k$ bits, while a_i, b_i have zeros on the first k bits and $a_i \neq b_i$. Thus \mathcal{S}_i is k -dimensional.

Let us check Eq. (13). By definition, \mathcal{S}_i contains both a_i and b_i . Suppose $i \neq j$ and $a_j \in \mathcal{S}_i$. Then a_j is an odd linear combination of vectors $\{a_i, b_i, c_1, c_2, \dots, c_k\} \setminus \{c_i\}$. Recall that the last $m - k$ bits of all c -vectors are zero and the first k bits of all a - and b -vectors are zero. Thus a_j must be an odd linear combination of vectors a_i and b_i only. This is only possible if $a_j = a_i$ or $a_j = b_i$. However, we assumed that all EPR qubits $a_1, b_1, \dots, a_k, b_k$ are distinct. Thus $a_j \notin \mathcal{S}_i$. The same argument shows that $b_j \notin \mathcal{S}_i$. \square

First let us check condition CSS2 with $i = 1$ (the same argument works for any i). Choose a function $\bar{f} : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ as

$$\bar{f}(x) = \begin{cases} 1 & \text{if } x \in \mathcal{S}_1 \\ 0 & \text{otherwise} \end{cases}$$

Since \mathcal{S}_1 is a k -dimensional affine subspace, Fact 6 implies that $\bar{f} \in \mathcal{C}^\perp$. We have $\bar{f}(a_1) = \bar{f}(b_1) = 1$ since $a_1, b_1 \in \mathcal{S}_1$. From Eq. (13) one gets $EX \cap \mathcal{S}_1 = E \cap \mathcal{S}_1 = \{a_1, b_1\}$. Thus $\bar{f}(v) = 0$ for all $v \in EX \setminus \{a_1, b_1\}$, as claimed. This proves condition CSS2.

Checking condition CSS1 requires more technical work, and we strongly encourage the reader to first study the proof of a quite general special case in Appendix A, which is much simpler.

As before, we can focus on the case $i = 1$ (the same argument works for any i). Then condition CSS1 is equivalent to the existence of a degree- $(k - 1)$ polynomial $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ such that

$$f(a_1) = f(b_1) = 1 \quad \text{and} \quad f(x) = 0 \quad \text{for all } x \in (\mathcal{S}_1 \cup \dots \cup \mathcal{S}_k) \setminus \{a_1, b_1\}. \quad (14)$$

Any degree- $(k - 1)$ polynomial $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ can be written as

$$f(x) = \sum_{T \subsetneq [k]} f_T(x) \prod_{j \in T} x_j \quad (15)$$

where $f_T : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ is some polynomial of degree $k - 1 - |T|$ that depends only on the variables x_{k+1}, \dots, x_m . It remains to choose the polynomials f_T with $0 \leq |T| \leq k - 1$. We shall use induction on $|T|$ starting with $T = \emptyset$. At each induction step we shall use polynomial regression (Lemma 5) to argue that the desired polynomial f_T exists (there is no need to construct f_T explicitly). Given $\emptyset \neq T \subsetneq [k]$, define the following set of m -bit strings

$$e(T) = \begin{cases} \{a_i, b_i \mid i \in [k] \setminus T\} & \text{if } |T| \text{ is even,} \\ \{0^m\} \cup \{a_i + b_i \mid i \in [k] \setminus T\} & \text{if } |T| \text{ is odd.} \end{cases} \quad (16)$$

Proposition 8. *Consider a function $f(x)$ of the form Eq. (15), where the $f_T(x)$ are some functions that depend only on the variables x_{k+1}, \dots, x_m . Then $f(x)$ satisfies condition Eq. (14) iff:*

$$f_\emptyset(a_1) = f_\emptyset(b_1) = 1, \quad f_\emptyset(a_i) = f_\emptyset(b_i) = 0 \quad \text{for } 2 \leq i \leq k, \quad (17)$$

and for every $\emptyset \neq T \subsetneq [k]$ and every $x \in e(T)$:

$$\sum_{U \subseteq T} f_U(x) = 0 \quad \left(\text{equivalently, } f_T(x) = \sum_{U \subsetneq T} f_U(x) \right) \quad (18)$$

Proof. CSS1 requires that f takes given values on $S = \mathcal{S}_1 \cup \dots \cup \mathcal{S}_k$, namely $f(a_1) = f(b_1) = 1$, and f must be zero on the rest of S . When we plug these input values into Eq. (15), it is a straightforward calculation to see that Eq. (17) exactly says that $f(a_i) = f(b_i) = 1$ if and only if $i = 1$, and Eq. (18) exactly says that $f(x) = 0$ for all $x \in S \setminus E$. More precisely, Eq. (18) for some $\emptyset \neq T \subsetneq [k]$ and $x \in e(T)$ expresses exactly $f(y) = 0$ for $y = \chi_T + x \in S$, where χ_T is the characteristic vector of T . Eq. (16) was engineered so that the above y ranges over all of $S \setminus E$. \square

In the rest of the section we concentrate our efforts on finding a family $\{f_T\}_{T \subsetneq [k]}$ of polynomials that satisfy Proposition 8. Below we focus on the case when k is even. The analysis for odd k requires only a few minor modifications, as detailed in Appendix B.

For fixed k, a_i s and b_i s we recursively (in the increasing size of $|T|$) construct f_T , and inductively show that f_T has the desired properties. To enable induction, we supplement Eqs. (17,18) with a few extra conditions on the polynomials f_T . Let $\ell \geq 0$ be an integer. We will say that a family of polynomials $f_T : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ labeled by subsets $T \subsetneq [k]$ with $|T| \leq \ell$ is *valid* if all conditions stated below are satisfied for $|T| \leq \ell$:

- I1:** f_T depends only on the variables x_{k+1}, \dots, x_m
- I2:** f_T has degree $k - 1 - |T|$
- I3:** $f_\emptyset(a_1) = f_\emptyset(b_1) = 1$ and $f_\emptyset(a_i) = f_\emptyset(b_i) = 0$ for $2 \leq i \leq k$
- I4:** $f_T(x) = \sum_{U \subsetneq T} f_U(x)$ for every non-empty set $T \subsetneq [k]$ and every $x \in e(T)$
- I5:** $f_T \equiv 0$ if $|T|$ is odd and $|T| \leq k - 3$
- I6:** $f_T(0^m) = f_T(a_i + b_i) = 0$ if $i \notin T$ and $|T| \leq k - 4$
- I7:** $f_T(a_i) = f_T(b_i)$ if $i \notin T$ and $|T| \leq k - 2$

Here (I1,I3,I4) are the conditions stated in Proposition 8 and (I2) ensures that a polynomial $f(x)$ constructed from the family $\{f_T\}_{T \subsetneq [k]}$ according to Eq. (15) has degree $k - 1$. Thus (I1,I2,I3,I4) alone imply CSS1. We shall use induction on ℓ to prove that a valid family of polynomials exists for all $\ell \leq k - 1$. The extra conditions (I5,I6,I7) facilitate analysis of the induction step.

The base case of the induction is $\ell = 0$. Then a valid family is a single polynomial f_\emptyset . Condition (I2) demands that f_\emptyset has degree $d_T = k - 1$. Conditions (I4) and (I5) can be skipped for $T = \emptyset$. Condition (I7) follows trivially from (I3). It remains to check (I3,I6) Note that conditions (I3) and (I6) with $T = \emptyset$ are imposed at disjoint set of points, see Eq. (11). Thus (I3) and (I6) are consistent. We fix the value of f_\emptyset at $s = 2k$ points in (I3) if $k \leq 3$, and at $s = 3k + 1$ points in (I3,I6) if $k \geq 4$. We can show that the desired polynomial f_\emptyset exists using Lemma 5. Below we always apply the lemma to polynomials satisfying condition (I1). This is justified since the first k bits of all vectors a_i and b_i are zero. If $k \leq 3$ then we have $s = 2k \leq 2^{d_T+1} = 2^k$. Thus we can use part (2) of Lemma 5. The extra condition $\sum_{i=1}^s g_i = 0$ of the lemma is satisfied since (I3) fixes the value of f_\emptyset to 1 at an even number of points. If $k \geq 4$ then we have $s = 3k + 1 < 2^{d_T+1} = 2^k$ and thus we can use part (1) of Lemma 5.

We shall now prove the induction step. Suppose we have already constructed a valid family of polynomials f_T with $|T| \leq \ell - 1$. Consider a subset $T \subsetneq [k]$ with $|T| = \ell$ such that $1 \leq \ell \leq k - 2$. The case $\ell = k - 1$ will be considered afterwards.

Suppose $|T|$ is odd. Since k is even and $\ell \leq k - 2$, this is only possible if $|T| \leq k - 3$. We set $f_T \equiv 0$ to satisfy (I5). Then conditions (I2), (I6), (I7) are satisfied automatically. Condition (I3) can be skipped since $T \neq \emptyset$. Condition (I4) with $f_T \equiv 0$ demands that $\sum_{U \subsetneq T} f_U(x) = 0$ for any $x \in e(T)$. Since $|T|$ is odd, $e(T)$ is the set of points 0^m and $a_i + b_i$ with $i \notin T$. Each term $f_U(x)$ with odd $|U|$ vanishes due to (I5). Each term $f_U(x)$ with even $|U|$ vanishes for $x \in e(T)$ due to (I6) since $|U| \leq |T| - 1 \leq k - 4$. Thus choosing $f_T \equiv 0$ satisfies (I4).

Suppose $|T|$ is even. Condition (I2) demands that f_T has degree $d_T = k - 1 - |T|$. Conditions (I3), (I5) can be skipped since $|T|$ is even and $T \neq \emptyset$. We claim that (I7) follows from (I4). Indeed, we have $x \in e(T)$ iff $x = a_i$ or $x = b_i$ with $i \notin T$. We have $f_T(x) = \sum_{U \subsetneq T} f_U(x)$ due to (I4). If $|U|$ is odd then $f_U \equiv 0$ due to (I5) since $|U| \leq |T| - 1 = \ell - 1 \leq k - 3$. If $|U|$ is even then $|U| \leq |T| - 2 \leq k - 4$. Thus $f_U(a_i) = f_U(b_i)$ since (I7) holds for f_U . This implies $f_T(a_i) = f_T(b_i)$ for any $i \notin T$, as claimed in (I7). It remains to check (I4, I6). We fix the value of f_T at $s = |e(T)| = 2(k - |T|)$ points in (I4) if $|T| \geq k - 3$. We fix the value of f_T at $s = |e(T)| + k - |T| + 1 = 3(k - |T|) + 1$ points in (I4, I6) if $|T| \leq k - 4$. Consider first the case $|T| \geq k - 3$. Then $|T| = k - 2$ since k and $|T|$ are even. Thus $s = 2(k - |T|) = 4$ and $2^{d_T+1} = 2^{k-|T|} = 4$. We can use part (2) of Lemma 5 to construct f_T . The extra condition $\sum_{i=1}^s g_i = 0$ of the lemma is equivalent to

$$\sum_{x \in e(T)} \sum_{U \subsetneq T} f_U(x) = 0. \quad (19)$$

Each term $f_U(x)$ with odd $|U|$ vanishes due to (I5) since $|U| \leq |T| - 1 = k - 3$. Each term $f_U(x)$ with even $|U|$ obeys $f_U(a_i) = f_U(b_i)$ for $i \notin T$ since f_U obeys (I7). Thus we have $\sum_{x \in e(T)} f_U(x) = 0$ for any $U \subsetneq T$ which implies Eq. (19). Thus the desired polynomial f_T exists by part (2) of Lemma 5, that is, we have checked (I4) in the case $|T| \geq k - 3$. Condition (I6) can be skipped in this case. In the remaining case, $|T| \leq k - 4$, we can use part (1) of Lemma 5 since $s = 3(k - |T|) + 1 < 2^{d_T+1} = 2^{k-|T|}$ for $|T| \leq k - 4$. Thus conditions (I4, I6) are satisfied.

It remains to prove the induction step for $\ell = k - 1$. Suppose we have already constructed a valid family of polynomials f_T with $|T| \leq k - 2$. Consider a subset $T \subsetneq [k]$ with $|T| = k - 1$. Since we assumed that k is even, $|T|$ is odd. Condition (I2) demands that f_T has degree $k - 1 - |T| = 0$, that is, f_T is a constant function. We can skip conditions (I3, I5, I6, I7) since none of them applies if $|T| = k - 1$. It remains to check (I4). Note that $e(T) = \{0^m, a_i + b_i\}$ for some $i \in [k]$ such that $T = [k] \setminus \{i\}$. Condition (I4) fixes the value of $f_T(x)$ at $x = 0^m$ and at $x = a_i + b_i$. Since we want f_T to be a constant function, it suffices to check that the desired values $f_T(0^m)$ and $f_T(a_i + b_i)$ are the same. Substituting the desired values from (I4), we have to check that

$$\sum_{U \subsetneq T} f_U(0^m) + f_U(a_i + b_i) = 0. \quad (20)$$

The sum contains terms with $|U| \leq |T| - 1 = k - 2$. All terms f_U with odd $|U|$ must have $|U| \leq k - 3$ since k is even. Such terms vanish due to (I5). All terms f_U with even $|U| \leq k - 4$ vanish due to (I6). Thus we can restrict the sum Eq. (20) to terms with $|U| = k - 2$. However, f_U is a degree-1 polynomial if $|U| = k - 2$ due to (I2). Thus $f_U(0^m) + f_U(a_i + b_i) = f_U(a_i) + f_U(b_i)$ and Eq. (20) is equivalent to

$$\sum_{\substack{U \subsetneq T \\ |U|=k-2}} f_U(a_i) + f_U(b_i) = 0. \quad (21)$$

Since f_U obeys (I7), we have $f_U(a_i) = f_U(b_i)$, which implies Eq. (21). We have now verified (I4). This completes the proof of the induction step.

Accordingly, having shown that both conditions CSS1 and CSS1 of Lemma 4 are satisfied, we can now conclude that the resource state $|\text{RM}(k-1, m)\rangle$ is k -pairable.

3.7 10-qubit 2-pairable example

The 2-pairable state of Section 3.4 used $n = 16$ qubits. Extending 2-pairability to states with fewer qubits would be good. Here we give a 10-qubit example and describe Pauli measurements generating $k = 2$ EPR-pairs for all choices of such pairs (modulo certain symmetries).

We choose the resource state $|\psi\rangle$ as the graph state associated with the 10-vertex “wheel graph” shown in Figure 4:

$$|\psi\rangle = \prod_{(i,j) \in E} \text{CZ}_{i,j}|+\rangle^{\otimes 10}. \quad (22)$$

Here E is the set of graph edges and CZ is the controlled- Z gate.

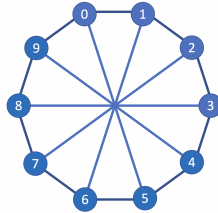


Figure 4: 10-vertex “wheel graph”. The corresponding 10-qubit graph state is 2-pairable with one qubit per party (to avoid confusion: the center of the picture is not an 11th vertex).

The number of ways to choose two EPR-pairs $\{a_1, b_1\}$ and $\{a_2, b_2\}$ is $3\binom{n}{4} = 630$ for $n = 10$ qubits. However, the number of cases we need to consider can be reduced by noting that the graph state $|\psi\rangle$ is invariant under certain permutations of qubits and local Clifford operations. Indeed, if W_φ is a permutation of n qubits (considered as a unitary operator) and C is a product of single-qubit Clifford gates such that $W_\varphi|\psi\rangle = C|\psi\rangle$, then an LOCC protocol generating EPR-pairs $\{a_1, b_1\}$ and $\{a_2, b_2\}$ can be easily converted into one generating EPR-pairs $\{\varphi(a_1), \varphi(b_1)\}$ and $\{\varphi(a_2), \varphi(b_2)\}$. This conversion requires only relabeling of qubits and local basis changes.

Suppose qubits are labeled by elements of the cyclic group $\mathbb{Z}_{10} = \{0, 1, \dots, 9\}$. Clearly, $|\psi\rangle$ is invariant under the cyclic shift of qubits, $j \rightarrow j + 1$ and inversion $j \rightarrow -j$. Here and below qubit indexes are computed modulo 10. Consider a permutation $\varphi : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}$ such that $\varphi(j) = 3j$. Let W_φ be the 10-qubit unitary that implements the permutation φ . We claim that

$$W_\varphi|\psi\rangle = H^{\otimes 10}|\psi\rangle, \quad (23)$$

where H is the Hadamard gate. Indeed, it is known [RBB03] that the graph state $|\psi\rangle$ has stabilizers

$$S_j = \sigma_j^x \prod_{i: (i,j) \in E} \sigma_i^z = \sigma_j^x \sigma_{j-1}^z \sigma_{j+1}^z \sigma_{j+5}^z, \quad j \in \mathbb{Z}_{10}.$$

Thus $|\psi\rangle$ is also stabilized by

$$S'_j := S_{j-3} S_{j+3} S_{j+5} = \sigma_j^z \sigma_{j-3}^x \sigma_{j+3}^x \sigma_{j+5}^x.$$

It follows that $H^{\otimes 10}|\psi\rangle$ is stabilized by

$$S''_j := H^{\otimes 10} S'_j H^{\otimes 10} = \sigma_j^x \sigma_{j-3}^z \sigma_{j+3}^z \sigma_{j+5}^z = W_\varphi S_i W_\varphi^\dagger,$$

where $i = \varphi^{-1}(j)$. Thus $W_\varphi^\dagger H^{\otimes 10} |\psi\rangle$ is stabilized by S_i for all $i \in \mathbb{Z}_{10}$, which implies Eq. (23).

Since $|\psi\rangle$ is also invariant under the cyclic shift of qubits, we can assume w.l.o.g. that $a_1 = 0$. The permutation φ maps 0 to 0 while any qubit $b_1 \in \mathbb{Z}_{10} \setminus \{0\}$ can be mapped to either 1, or 2, or 5 by repeated applications of φ . Thus we can assume w.l.o.g. that $a_1 = 0$ and $b_1 \in \{1, 2, 5\}$.

For each of the remaining choices of EPR-pairs we numerically examined all 3^6 Pauli measurement bases on qubits $\mathbb{Z}_{10} \setminus \{a_1, b_1, a_2, b_2\}$ and computed the final post-measurement state of qubits a_1, b_1, a_2, b_2 using the standard stabilizer formalism. To test whether the final state is locally equivalent to the desired EPR-pairs, we checked whether the entanglement entropies of the final state obey $S(a_i) = S(b_i) = 1$ and $S(a_i b_i) = 0$ for $i = 1, 2$. The entanglement entropy of a stabilizer state can be extracted from its tableaux as described in [FCY⁺04]. Any two-qubit stabilizer state of qubits a_i, b_i satisfying $S(a_i) = S(b_i) = 1$ and $S(a_i b_i) = 0$ has to be maximally entangled and thus equivalent to the EPR-pair modulo single-qubit Clifford gates. We found a Pauli basis generating maximally-entangled states on qubits $\{a_1, b_1\}$ and $\{a_2, b_2\}$ in all considered cases, see Figure 5. We also observed that the graph state $|\psi\rangle$ is not 2-pairable if the Pauli bases are restricted to σ^x and σ^z only.

1122ZZXXZZ	11XX2Z2XZZ	1212ZZYYXY	1Z1X2Z2XXX	122ZY1YZZY	1ZZ2Y12YYZ
112X2ZXXZZ	11ZX2ZZ2XZ	121X2ZXXXX	1Z1X2ZZ2XX	122Z2Y1XYYY	1ZZ2Z1Z2XZ
112ZX2XXZX	11ZX2ZZZ2Z	121ZY2YXY	1Z1Y2XXY2Y	12XX21XXXX	1ZZ2Z1ZZ2Z
112ZZZ2XZZ	11ZY2YZZY2	121ZY2YYY	1Z1Y2XYYY2	12XXX12XXX	1XX2Z1ZZX2
112XYZY2YZ	11XZX22XZX	121XZX2XX	1Z1XX2ZZZX	12ZYX1Y2YY	1ZZX212XXZ
112ZXXY2Y	11ZZX2Z2XX	121ZZYYY2Y	1Z1Y2Z2X2YY	12ZYX1XY2Y	1ZZY21Y2YZ
112ZXXXXZ2	11ZZX2ZZ2X	121ZZYYXY2	1Z1XX2ZZ2X	12ZYY1YYY2	1ZZX21XXZ2
11Z22ZZZZZ	11ZZX2ZZZ2	1X122ZZXXZ	1X1Z2ZZZ2	1Z2Z21ZZZZ	1XXX21XXX2
11Z2Y2ZZY	11XXZY2ZYY	1Z12Z2YYY	1Z1XZ2Z2XX	1Z2X21XXZ2	1XXYY122XY
11X2ZZ2XZZ	11XYX2Y2X	1Z12ZY2XY	1Z1XXX2Z2X	1Z2XX12XZ2	1ZZXX12XZ2
11Z2ZZ2Z2X	11XZX2XZ2	1X12ZZZ2XZ	1Z1YYX2Y22	1Z2ZZ1Z2ZZ	1XXXX12XX2
11Z2ZZZZ2Z	11ZZZZ2Z2Z	1Z12YYYX2Y	1Z1XYYY22X	1Z2ZZ1Z2Z2	1ZZZZ1Z2Z2
11X2YYYXZ2	11ZZXXZ2X2	1Z12YYYYY2	1Z1YYYY2Z2	1X2YX1XY2	1XXZZ1Z2X2
11XY2ZYXZY	11ZZXXZZ2Z	1Z1X22YYYX	1X1ZXXZ2Z2	1XX221YXY	1XYZY1YZ22

Figure 5: Measurement patterns for the 10-qubit 2-pairable resource state associated with the “wheel graph”. Here ‘1’ and ‘2’ stand for the EPR qubits $\{a_1, b_1\}$ and $\{a_2, b_2\}$ respectively. A qubit labeled by ‘X’, ‘Y’, or ‘Z’ is measured in the Pauli basis σ^x , σ^y , and σ^z respectively. Here we only consider the case $a_1 = 0$ and $b_1 \in \{1, 2, 5\}$. All other cases can be obtained by a permutation of qubits that leaves the resource state invariant (modulo a bitwise Hadamard).

We verified numerically that no stabilizer state with $n < 10$ qubits is 2-pairable using LOCC protocols based on Pauli measurements, by checking all possible 9-qubit graph states as listed in [AMSDS20]. The code is available at <https://github.com/yashsharma25/generating-k-epr-pairs>

4 Obstructions for complete pairings ($k = n/2$)

Now we turn from constructions to proving limitations on all possible k -pairable resource states. Let n be the number of parties as in the previous sections. Since we are talking about complete pairings in this section, we assume here that n is divisible by 2. For a pairing

$$\pi = \{\{a_1, b_1\}, \dots, \{a_{n/2}, b_{n/2}\}\} \quad \text{with} \quad \cup \pi = [n]$$

the tensor product $|\pi\rangle$ of the $n/2$ EPR-pairs,

$$|\pi\rangle = \bigotimes_{i=1}^{n/2} |+\rangle_{a_i, b_i}$$

is a state on n qubits, where by definition $|+\rangle_{a,b} = \frac{1}{\sqrt{2}}(|0_a 0_b\rangle + |1_a 1_b\rangle)$.

For our first type of lower bounds we assume that the n parties want to achieve all possible *complete* pairings on $[n]$. Then we find a super-constant lower bound on the required number m of qubits per party:

Theorem 9. *Suppose $|\psi\rangle$ is a fixed state of nm qubits shared by n parties such that each party holds m qubits of $|\psi\rangle$. Suppose that for any pairing π of n qubits a transformation $|\psi\rangle \rightarrow |\pi\rangle \otimes |w_\pi\rangle$ is realizable by an LOCC protocol such that at the end of the protocol the i -th qubit of $|\pi\rangle$ belongs to the i -th party for all i , and $|w_\pi\rangle$ is an arbitrary state on the qubits not belonging to $|\pi\rangle$.⁶ Then*

$$m = \Omega(\log \log n).$$

The proof of this theorem is going to be a dimension calculation, but with a twist. Given a starting state $|\psi\rangle$ we estimate the dimension of the space that contains all those states that can be obtained (with positive probability) from $|\psi\rangle$ by an LOCC protocol. We want to compare this with the dimension of the space induced by all possible states that should arise as output, where we let the input range over all possible pairings. This by itself, however, will not yield the desired lower bound. The mathematical idea is that rather than representing each state by itself, we represent it by its r^{th} tensor power, where r will be carefully set in the magnitude of $\Theta(\log n)$. Let

$$\mathcal{L}_r = \text{span}(|\pi\rangle^{\otimes r} \mid \pi \text{ is an } n\text{-qubit pairing})$$

be the linear space induced by the r^{th} tensor powers of all possible output states. Before stating a lower bound on $\dim(\mathcal{L}_r)$ we prove a lemma:

Lemma 10. *Let π and ρ be two pairings. Then $\langle \pi | \rho \rangle = 2^{\mu - n/2}$, where μ is the number of cycles in $\pi \cup \rho$, as a graph on vertex set $[n]$.*

Proof. Note that the graph $\pi \cup \rho$ (the union of the two perfect matchings π and ρ on the same vertex set $[n]$) is a collection of cycles. We have

$$\langle \pi | \rho \rangle = \sum_{x \in \Lambda} \frac{1}{2^{n/2}}$$

where $\Lambda \subseteq \{0, 1\}^n$ is the set of binary strings, corresponding to the vertex labeling λ of the graph $\pi \cup \rho$ such that for every $\{a_i, b_i\} \in \pi$ we have $\lambda(a_i) = \lambda(b_i)$, and for every $\{a'_i, b'_i\} \in \rho$ we have $\lambda(a'_i) = \lambda(b'_i)$. In other words, the labeling λ must be constant on each connected component of $\pi \cup \rho$. Therefore,

$$|\Lambda| = 2^{\# \text{ of connected components of } \pi \cup \rho} = 2^{\# \text{ of cycles in } \pi \cup \rho}.$$

□

⁶Without loss of generality we may assume $|w_\pi\rangle = |0^{n(m-1)}\rangle$.

Lemma 11. *There exist constants $C, C' > 0$ such that $\dim(\mathcal{L}_{C'+\log_2 n}) \geq n^{n/4} \cdot 2^{-Cn}$*

Proof. Let $A = [n/2]$, $B = [n/2 + 1, n]$. Let

$$V = \{ \pi \mid \pi \text{ is an } n\text{-qubit pairing with } a_i \in A, b_i \in B \text{ for } 1 \leq i \leq n/2 \}$$

We define an undirected graph G on V by

$$\begin{aligned} V(G) &= V \\ E(G) &= \{ (\pi, \rho) \in V^2 \mid \pi \neq \rho \text{ and } \pi \cup \rho \text{ consists of at least } n/4 \text{ cycles} \} \end{aligned}$$

Let us view each $\pi \in V$ as a 1-1 map from A to B . Then $(\pi, \rho) \in E(G)$ if and only if $\pi\rho^{-1}$ is a permutation on A with at least $n/4$ cycles. If we fix π , then as ρ varies, $\pi\rho^{-1}$ runs through all permutations of $A = [n/2]$. Thus, every vertex of G has degree D , where D is the number of permutations of $[n/2]$ having at least $n/4$ cycles. Let $c(n, \ell)$ be the unsigned Stirling numbers of the first kind. It is known that $c(n, \ell)$ is exactly the number of permutations of n elements with ℓ disjoint cycles. Thus

$$D = \sum_{\ell=0}^{n/4} c(n/2, n/4 + \ell)$$

It is also known that

$$c(n, n - \ell) = \sum_{0 \leq i_1 < i_2 < \dots < i_\ell < n} i_1 i_2 \dots i_\ell$$

The right-hand side above is at most

$$\binom{n}{\ell} \cdot (n - \ell) \dots (n - 1) \leq \frac{2^n}{(n - \ell - 1)!} (n - 1)!$$

Therefore:

$$D = \sum_{\ell=0}^{n/4} c(n/2, n/4 + \ell) \leq (n/2)! \cdot \frac{2}{n} \sum_{\ell=0}^{n/4} \frac{2^{n/2}}{(n/4 + \ell - 1)!} \leq (n/2)! \frac{2^{n/2}}{(n/4 - 1)!} - 1.$$

Then,

$$\frac{|V|}{D + 1} = \frac{(n/2)!}{D + 1} \geq \frac{(n/4 - 1)!}{2^{n/2}},$$

implying the existence of an independent set in G of size at least $(n/4 - 1)!/2^{n/2}$ by a well-known greedy argument: pick a vertex to add to the independent set, remove it and its $\leq D$ neighbors, and continue with the remaining graph. Using Stirling's formula to estimate the factorials, there is a C ($\approx 1 + \frac{1}{4} \log_2 e$, when $n \rightarrow \infty$) such that $(n/4 - 1)!/2^{n/2} \geq n^{n/4} \cdot 2^{-Cn}$. Let I be an independent set in G of size $n^{n/4} \cdot 2^{-Cn}$ (we ignore rounding to an integer for simplicity). Define the linear space

$$\mathcal{L}_{I,r} = \text{span}(|\pi\rangle^{\otimes r} \mid \pi \in I).$$

From now on we set $r = C' + \log_2 n$, where $C' = 1 + 4C$ ($\approx 5 + \log_2 e$, when $n \rightarrow \infty$). It is enough to show that we have $\dim(\mathcal{L}_{I,r}) = |I|$ ($= n^{n/4} \cdot 2^{-C}$), since $\mathcal{L}_{I,r} \leq \mathcal{L}_r$. Let us define the $|I| \times |I|$ Gram matrix \mathbb{G} of the $\{|\pi\rangle^{\otimes r}\}_{\pi \in I}$ system:

$$\mathbb{G}_{\pi,\rho} = \langle \pi | \rho \rangle^r \quad \pi, \rho \in I$$

For $\dim(\mathcal{L}_{I,r}) = |I|$ it is sufficient to show that \mathbb{G} has full rank.

Gershgorin's circle theorem implies, for any (complex) square matrix A : if $R_i = \sum_{j: j \neq i} |A_{i,j}| < |A_{i,i}|$ for all indices i , then A has full rank.

In order to apply this theorem, we compute for the π -row of our matrix \mathbb{G} :

$$\sum_{\rho \in I: \rho \neq \pi} |\mathbb{G}_{\pi, \rho}| \leq \sum_{\rho \in I: \rho \neq \pi} 2^{-nr/4} \leq 2^{-nr/4} |I| = 2^{-n(1+4C+\log_2 n)/4} \cdot \underbrace{n^{n/4} \cdot 2^{-Cn}}_{\text{size of } I} < 1$$

where we used Lemma 10. Since in addition, $\mathbb{G}_{\pi, \pi} = 1$ for all $\pi \in I$, Gershgorin's circle theorem implies that our matrix \mathbb{G} has full rank. Hence $\dim(\mathcal{L}_{I,r}) = |I| = n^{n/4} \cdot 2^{-Cn}$. \square

Lemma 11 says that for any fixed state $|\psi\rangle$, the possible outputs (over all input pairings π), when taking their r^{th} tensor power with $r = \Theta(1) + \log n$, should span a space of dimension $\geq n^{\Theta(\log n)}$.

This number we have to compare with the dimension of the span of r^{th} tensor powers of possible states that can be produced *by an LOCC protocol* from $|\psi\rangle$. Although LOCC protocols may use unlimited classical communication, they cannot create new entanglement, so all entanglement in their final state is a *local linear transformation* of the entanglement that already existed in the starting state $|\psi\rangle$.

When each party only possesses m qubits, where m is very small, the variety of states that an LOCC protocol can produce from $|\psi\rangle$ is limited in the way we describe below.

To capture this limitation, notice that any LOCC protocol can be described by a completely positive trace-preserving (CPTP) map, with *separable* Kraus operators. It follows that for any pairing π there exists a product Kraus operator

$$K^\pi = K_1^\pi \otimes K_2^\pi \otimes \cdots \otimes K_n^\pi \quad (24)$$

such that K_i^π maps m qubits to one qubit for all $1 \leq i \leq n$ and for all pairings π :

$$K^\pi |\psi\rangle = c_\pi |\pi\rangle \quad \text{for some } c_\pi \neq 0 \quad (25)$$

Define:

$$\mathcal{M}_r = \text{span}((K|\psi\rangle)^{\otimes r} \mid K = K_1 \otimes K_2 \otimes \cdots \otimes K_n)$$

where the K_i are arbitrary operators mapping m qubits to one qubit (K_i may depend on i), and $|\psi\rangle$ is our fixed starting state. From Equations (25) and (24) we get the subspace inclusion

$$\mathcal{L}_r \leq \mathcal{M}_r$$

and hence, using Lemma 11, for some $C, C' > 0$ we have $\dim(\mathcal{M}_{C'+\log_2 n}) \geq n^{n/4} \cdot 2^{-C}$. However, when $m = o(\log \log n)$ this cannot be the case because of the following upper bound:

Lemma 12. $\dim(\mathcal{M}_r) \leq \binom{2^{m+1} + r - 1}{2^{m+1} - 1}^n$.

Proof. Linear operators K_i that map m qubits to one qubit can be considered as vectors in a complex space of dimension $D = 2^{m+1}$ (use the vectorized form of operators). Crucially, the r -fold tensor products $K_i^{\otimes r}$ live in the *symmetric subspace* of $(\mathbb{C}^D)^{\otimes r}$, which has dimension

$$\binom{D + r - 1}{D - 1} \quad (26)$$

(this is where the big saving occurs: without the information that the vector is in the symmetric subspace, we would have to calculate with D^r instead of the above expression, and would get only a trivial bound). It follows that operators of the form $K^{\otimes r} = K_1^{\otimes r} \otimes \cdots \otimes K_n^{\otimes r}$ span a linear space of operators with dimension at most

$$\binom{D+r-1}{D-1}^n \quad (27)$$

Thus states of the form $(K|\psi\rangle)^{\otimes r} = K^{\otimes r}|\psi\rangle^{\otimes r}$ with a fixed $|\psi\rangle$ span a linear space with dimension upper bounded by Equation (27). Substituting $D = 2^{m+1}$, one gets the statement of the lemma. \square

It is now an easy calculation to show that with $r = \Theta(\log n)$, the above lemma together with Lemma 11 gives

$$2^m = \Omega\left(\frac{\log n}{\log r}\right).$$

This implies $m = \Omega(\log \log n)$ and concludes the proof of Theorem 9.

5 Obstructions for partial pairings

In this section we generalize the result of the previous section to partial pairings and show:

Theorem 13. *Let n be an integer, $k \leq n/2$, and $|\psi\rangle$ be a k -pairable state for n parties where each party has m qubits. Then*

$$k = O\left(n2^m \frac{\log \log n}{\log n}\right)$$

Proof. For technical reasons we assume that n is divisible by 4. In the proof we also assume that $k \geq n/\log n$, since otherwise there is nothing to prove: the expression in parentheses on the right-hand side is always larger than $n/\log n$. A k -pairing of $[n]$ is

$$\pi = \{\{a_1, b_1\}, \dots, \{a_k, b_k\}\} \quad \text{with} \quad \cup \pi \subseteq [n], \quad |\cup \pi| = 2k$$

We denote the set of k -partial pairings on $[n]$ with $\Pi_{n,k}$. As in the previous section, we assume that each party has m qubits, and one of these m is designated as the output qubit, which will hold a qubit of an EPR-pair at the end of the protocol whenever π involves the party in question. The goal is to be able to produce

$$|\pi\rangle = |0^{n-2k}\rangle \otimes \bigotimes_{i=1}^k |+\rangle_{a_i, b_i}$$

from some fixed initial nm -qubit resource state $|\psi\rangle$, for all $\pi \in \Pi_{n,k}$. We note that in the above tensor product the listing order of the qubits depends on π , and we list only the n qubits designated to be output bits. (We list even those designated output qubits of parties that are not covered by the current partial matching π , since they will participate in the output for other π s.) For the remaining $n(m-1)$ qubits, we assume w.l.o.g. that they end up in the $|0\rangle$ -state, and hence are not entangled with the rest. To achieve this the parties can set these qubits to $|0\rangle$ by a local operation.

The proof is a slight variation of our proof for the complete-pairing case. There $\dim(\mathcal{M}_r)$ was calculated, and similarly to the previous section this dimension upper bounds the dimension of

$$\mathcal{L}_{k,r} = \text{span}(|\pi\rangle^{\otimes r} \mid \pi \in \Pi_{n,k}).$$

The calculation is very similar to the case of complete pairings:

1. We will find $n^{\Theta(k)}$ different π s such that their r^{th} tensor powers, where $r = \Theta(\log n)$, are linearly independent. (In the complete pairing case it was $n^{\Theta(n)}$ different π s.)
2. Setting $r = \Theta(\log n)$ is still the only reasonable choice. Further, the approach breaks down at $m > \log \log n$, so we will be satisfied with investigating $m \leq \log \log n$. With the above parameters for r and m we have $2^{m+1} + r - 1 = \Theta(r)$, hence via Lemma 12 we have:

$$\dim(\mathcal{M}_r) \leq \binom{\Theta(r)}{2^m}^n \leq r^{\Theta(2^m n)}.$$

3. Similarly to our argument in the previous section, the dimension of $\mathcal{L}_{k,r}$ must lower bound the dimension of $\mathcal{M}_{C \log n}$, which is $r^{\Theta(2^m n)} = 2^{\Theta(n 2^m \log \log n)}$.
4. Combining 1 and 3, we get $\Theta(k \log n) \leq \Theta(n \cdot 2^m \log \log n)$, which implies Theorem 13.

Points 2-4 require no explanation as they just reiterate ideas of the previous section. However, we need to prove Point 1.

First we prove the analogue of Lemma 10 for partial pairings.

Lemma 14. *Let π and ρ be two partial pairings with k pairs. Then*

$$\langle \pi | \rho \rangle = 2^{\mu - k}$$

where μ is the number of cycles in $\pi \cup \rho$, as a graph on vertex set $[n]$.

Proof. We have:

$$\langle \pi | \rho \rangle = \sum_{x \in \Lambda} \frac{1}{2^k}$$

where $\Lambda \subseteq \{0, 1\}^n$ is the set of binary strings, corresponding to the vertex labeling, λ , of the graph $\pi \cup \rho$ such that for every $\{a_i, b_i\} \in \pi$ we have $\lambda(a_i) = \lambda(b_i)$, and for every $\{a'_i, b'_i\} \in \rho$ we have $\lambda(a'_i) = \lambda(b'_i)$ and furthermore every element of vertex set $[n]$ that is not covered by both a π -edge and a ρ -edge (that is, elements not in $(\cup \pi) \cap (\cup \rho)$) must get label 0.⁷ Thus, only the cycles in $\pi \cup \rho$ can be labeled two ways, and no more than two ways, since the edges of π and ρ force the condition that all labels over the cycle must be either 0 or 1. (Paths cannot be labeled two ways as the label at their endpoint is fixed to 0.) This calculation of $|\Lambda|$ gives the formula. \square

We let $A = [n/2]$, $B = [n/2 + 1, n]$ and define

$$V = \{ \pi \in \Pi_{n,k} \mid \pi \text{ is an } n\text{-qubit partial pairing with } a_i \in A, b_i \in B \text{ for } 1 \leq i \leq k \}$$

Then $|V| = \binom{n/2}{k} (n/2)! / (n/2 - k)!$. We need a lower bound on $|V|$. Using the well-known bounds

$$\binom{n/2}{k} \geq \left(\frac{n}{2k}\right)^k \quad \text{and} \quad k! \geq e^{-k} k^k$$

⁷The formula for $\langle \pi | \rho \rangle$ comes from computing the inner product in the most straightforward way: we notice that both $|\pi\rangle$ and $|\rho\rangle$ have only two kinds of entries: 0 and $1/\sqrt{2^k}$. Then we just identify those entries where both $|\pi\rangle$ and $|\rho\rangle$ are non-zero and compute the number of such entries.

one gets

$$|V| = \binom{n/2}{k}^2 k! \geq \left(\frac{n}{2k}\right)^{2k} e^{-k} k^k = \frac{n^{2k}}{k^k (4e)^k} \geq \frac{n^{2k}}{(n/2)^k (4e)^k} = n^k (2e)^{-k},$$

where the second inequality follows from $k \leq n/2$. We again create a graph with:

$$\begin{aligned} V(G) &= V \\ E(G) &= \{(\pi, \rho) \in V^2 \mid \pi \neq \rho \text{ and } \pi \cup \rho \text{ has at least } k/2 \text{ cycles}\} \end{aligned}$$

Note that G is again regular as in the previous section, since it is vertex-symmetric. Like before, we want to lower bound $|V|/(D+1)$ where D is the degree of a $\pi \in V$, which is then a lower bound on the size of a maximal independent set in G . In fact, for an arbitrary fixed $\pi \in V$ we have:

$$D + 1 = |\{\rho \in V \mid \pi \cup \rho \text{ has at least } k/2 \text{ cycles}\}|$$

To upper bound the size of D , w.l.o.g. let $\pi = \{\{1, 1 + n/2\}, \dots, \{k, k + n/2\}\}$: we match the first k vertices in the first half with the first k vertices in the second half. We can upper bound the number of neighbors of π by enumerating them, each possibly multiple times. To define a somewhat elaborate enumeration, first notice that the nodes of any cycle in $\pi \cup \rho$ must be fully contained in the vertex set $\cup \pi = [1, k] \cup [1 + n/2, k + n/2]$. Assume ρ is a neighbor of π such that $\pi \cup \rho$ has μ cycles. Pick an (arbitrary) point in every cycle, such that the selected points belong to A . Let these points be $1 \leq p_1 < \dots < p_\mu \leq k$, and let

$$P = \{p_i\}_{1 \leq i \leq \mu}$$

Let $2L_i$ be the length of the cycle that goes through p_i (all cycles have even length, because the edges alternate between π and ρ), and denote:

$$\begin{aligned} K_\nu &= \sum_{i=1}^{\nu} L_i \quad 1 \leq \nu \leq \mu \\ K &= \{K_\nu\}_{1 \leq \nu \leq \mu} \end{aligned}$$

Since $K_\mu \leq k$, we have $K \subseteq [k]$. Finally, let us define

$$R = \{a \in A \mid a \text{ is an } A\text{-endpoint of some edge in } \rho\}$$

The triplet (P, K, R) with one piece of additional information, which will be defined next, will determine ρ . The number of (P, K, R) triplets is $2^{O(n)}$, since all three of P, K, R can be given as subsets of sets of size at most n (e.g., K is a subset of $[n]$ due to $K_\mu \leq n$).

Let us now understand the magnitude of the additional information⁸ that together with (P, K, R) determines ρ . It will turn out that this information is $ck \log n$ bits, where very crucially, c is less

⁸We could have chosen information-theoretic terminology for our explanation, where we relate the $|V|/(D+1)$ ratio to the mutual information between ρ and π . We have opted for an equivalent counting explanation, but the reader has to bear in mind, that our underlying intuition is that every cycle that ρ and π jointly create, increases their mutual information by $\Omega(\log n)$ bits (essentially, the edge of ρ that ‘‘closes the cycle’’ is cheap to communicate, given π). The ratio $|V|/(D+1)$ is simply the exponential of this mutual information.

than 1 (in fact, c will be essentially $1/2$). This implies an upper bound on $D + 1$, which in turn implies the following lower bound on the size of the largest independent set in G :

$$\frac{|V|}{D+1} \geq \underbrace{n^k(2e)^{-k}}_{\text{lower bound on } |V|} \cdot \underbrace{2^{-O(n)}}_{\text{due to } (P,K,R)} \cdot \underbrace{2^{-ck \log n}}_{\text{due to additional information}} = n^{(1-c)k}(2e)^{-k}2^{-O(n)}. \quad (28)$$

Additional data that with (P, K, R) uniquely determines ρ , given that ρ is π 's neighbor in G :

We shall define an order e_1, \dots, e_k of edges of ρ . We will denote the B -endpoint of e_i by q_i .

Before telling the order, note that the cycles in $\pi \cup \rho$ already have a natural order, modulo the (P, K, R) information, namely the i^{th} cycle is the cycle that contains p_i . To “extend” this order to the edges we introduce:

1. Among all edges of ρ those edges come earlier that are edges of some $\pi \cup \rho$ cycle.
2. If two edges both participate in a $\pi \cup \rho$ cycle, but these two cycles are different, then the edge comes first that belongs to an earlier cycle.

We need to tell how to order edges within the same cycle. Also, we need to tell how to order edges that do not belong to any cycle.

Ordering of edges of ρ that belong to a given cycle.

If the cycle is the i^{th} cycle, we simply walk through the the cycle and order the ρ -edges as we encounter them. The walk-through starts from p_i with a ρ -edge (which determines that in which orientation we follow the cycle). For instance, consider the first cycle. For this example notice that if e_ℓ is a cycle-edge in $\pi \cup \rho$, then $\{q_\ell - n/2, q_\ell\} \in \pi$ belongs to the same cycle as e_ℓ . We get:

$$\begin{aligned} e_1 & \text{ is the edge of } \rho \text{ with } A\text{-endpoint } p_1 \\ e_2 & \text{ is the edge of } \rho \text{ with } A\text{-endpoint } q_1 - n/2 \\ e_3 & \text{ is the edge of } \rho \text{ with } A\text{-endpoint } q_2 - n/2 \\ & \dots \\ e_{L_1} & \text{ is the edge of } \rho \text{ with } A\text{-endpoint } q_{L_1-1} - n/2 \end{aligned}$$

Ordering of edges of ρ that do not belong to any cycle:

These edges are simply ordered by the numerical value of their A -endpoints: edges with a smaller A -endpoint come earlier.

Let us now assume that Alice has to specify ρ to Bob. First Alice gives Bob the (P, K, R) triplet. Then she starts to tell Bob q_1, q_2, \dots (Recall, q_i is the B -endpoint of e_i .) Two remarkable observations lead to our conclusions.

1. Even though Alice only tells the B -endpoints to Bob, Bob will (recursively) figure out the A -endpoints as well. This is in fact trivial. For instance, the A -endpoint of e_1 is p_1 , which is known to Bob, since (P, K, R) is given to him, etc. When the last cycle is exhausted, Bob knows this (this is after K_μ edges had been encountered—the total number of cycle-edges; K_μ in turn is given as the last element of the K -sequence), and from then on Bob relies on R to get the A -endpoints.

2. When Alice arrives at an edge that closes a $\pi \cup \rho$ cycle, she does not need to send the B -endpoint of this edge! It is simply $p_i + n/2$, if the cycle was the i^{th} cycle. In other words, it is the other endpoint of the edge of π incident to p_i . Therefore, we just assume that Alice skips telling the B -endpoint of the last edge of every cycle. But how does Bob know that he has arrived at the last edge of the current cycle? He knows this, because the cycle lengths are encoded in K : the length of the i^{th} cycle is $K_i - K_{i-1}$ if $i \geq 2$ and K_1 for $i = 1$.

In summary, the information Alice gives to Bob besides (P, K, R) to identify ρ , is the q_1, q_2, \dots sequence, but crucially, completely leaving out from this sequence the B -endpoints of all the cycle-closing edges. We have μ cycle-closing edges. Describing any q_ℓ takes $\log n$ bits, since $q_\ell \in [n]$. Therefore:

The number of bits Alice needs to send Bob to fully describe a ρ that creates μ cycles with π is:

$$O(n) + (k - \mu) \log n$$

In conclusion, the number of different ρ s that form μ cycles with π can be upper bounded by $2^{O(n)} n^{k-\mu}$. To upper bound D , recall that μ is allowed to vary from $k/2$ to k , so $D + 1$ is upper bounded by $(\frac{k}{2} + 1) 2^{O(n)} n^{k/2} + 1$. Thus, looking back at Eq. (28) and using that $k \leq n$, there exists an independent set of size $n^{k/2} 2^{-O(n)}$ in G . Consequently, we can find a set of that many partial permutations such that if $\pi \neq \rho$ belongs to this set, then the inner product of $|\pi\rangle^{\otimes r}$ and $|\rho\rangle^{\otimes r}$ is at most $2^{-kr/2}$. Setting r to be $2 \log n$ (generously, in fact: we care only about the $k \geq n \frac{\log \log n}{\log n}$ case, hence the $2^{O(n)}$ factor becomes $n^{o(k)}$) and applying Gershgorin's circle theorem in the same fashion as in the proof of Lemma 11 in the previous section, we prove Point 1 and conclude the proof of Theorem 13. \square

Theorem 13 has the following consequence for the case where each party is restricted to a constant number of qubits:

Corollary 15. *Let $|\psi\rangle$ be a k -pairable state for n parties where each party has $m = O(1)$ qubits. Then $k = O\left(n \frac{\log \log n}{\log n}\right)$.*

As mentioned in the introduction, up to the power of the polylog this matches our expander-based construction of k -pairable states where $m = 10$ and $k \geq n/\text{polylog}(n)$ (Corollary 3).

6 Conclusion and future work

In this paper we initiated the study of n -party resource states from which LOCC protocols can create EPR-pairs between any k disjoint pairs of parties. These EPR-pairs then enable quantum communication over a classical channel via teleportation. Our focus was on the tradeoff between the number k of to-be-created EPR-pairs (which we want to be large) and the number m of qubits per party (which we want to be small).

This work leaves open several questions for future work:

- Our constructions of k -pairable states may be far from optimal, and it would be interesting to improve them. For example, it might be possible to significantly reduce the number of qubits

$n(k)$ of our Reed-Muller-based construction of k -pairable states with one qubit per party. Also, the case $m = 2$ remains largely open since two qubits per party is not enough to realize entanglement swapping protocols on expander graphs, see Section 2. All our constructions are based on stabilizer-type resource states. Can one improve the tradeoff between k and m using more general resource states? Can one express the pairability parameter k in terms of some previously studied entanglement measures?

- Regarding lower bounds (obstructions), we showed in Section 4 that a resource state for complete pairings ($n = k/2$) requires $m = \Omega(\log \log n)$ qubits per party. Can we improve this lower bound to $m = \Omega(\log n)$ qubits, matching the upper bound we obtained from expander graphs at the end of Section 2? Our lower bounds are actually for a stronger model, applying to LOCC protocols that produce the desired state with positive probability; there may be better upper bounds in this setting, and/or stronger lower bounds for LOCC protocols that are required to succeed with probability 1.
- How well do our resource states behave under noise? Contreras-Tejada, Palazuelos, and de Vicente [CPdV22] already proved some negative results here for the type of constructions we gave in Section 2 (with EPR-pairs on the edges of an n -vertex graph), showing that genuine multipartite entanglement only survives constant amounts of noise per edge if the graph has a lot of connectivity.
- We can ask a very similar *classical* question, where the classical analogue of an EPR-pair is a uniform bit shared between two parties and unknown to all others. Such shared secret bits can then be used for secure communication over public classical channels (via the one-time pad), similarly to how shared EPR-pairs can be used for secure quantum communication over public classical channels (via teleportation). We believe our techniques can be modified to obtain non-trivial results about the question: what classically correlated n -party resource states are necessary and sufficient for LOCC protocols (with public classical communication) to generate such secret shared bits between any k disjoint pairs of parties? One difference is that the straightforward classical analogue of the GHZ-state (a uniformly random bit known to all n parties) is not 1-pairable in this classical sense.

Acknowledgements. We thank Carlos Palazuelos for a pointer to [CPdV22] and Jorge Miguel-Ramiro for a pointer to [MPD23].

References

- [AG04] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5):052328, 2004.
- [AJ92] E. F. Assmus Jr. On the Reed-Muller codes. *Discrete mathematics*, 106:25–33, 1992.
- [AMSDS20] Jeremy C. Adcock, Sam Morley-Short, Axel Dahlberg, and Joshua W. Silverstone. Mapping graph state orbits under local complementation. *Quantum*, 4:305, 2020.
- [BBC⁺93] Charles Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

- [BFU94] Andrei Z. Broder, Alan M. Frieze, and Eli Upfal. Existence and construction of edge-disjoint paths on expander graphs. *SIAM Journal on Computing*, 23(5):976–989, 1994.
- [Bol88] Béla Bollobás. The isoperimetric number of random regular graphs. *European Journal of combinatorics*, 9(3):241–244, 1988.
- [CPdV22] Patricia Contreras-Tejada, Carlos Palazuelos, and Julio I. de Vicente. Asymptotic survival of genuine multipartite entanglement in noisy quantum networks depends on the topology. *Physical Review Letters*, 128:220501, 2022. arXiv:2106.04634.
- [CRSS98] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory*, 44(4):1369–1387, 1998.
- [CS96] A. Robert Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.
- [DHW18] Axel Dahlberg, Jonas Helsen, and Stephanie Wehner. How to transform graph states using single-qubit operations: computational complexity and algorithms, 2018. arXiv:1805.05306.
- [DHW20] Axel Dahlberg, Jonas Helsen, and Stephanie Wehner. Transforming graph states to Bell-pairs is NP-complete. *Quantum*, 4:348, 2020.
- [DSL17] Gang Du, Tao Shang, and Jian-Wei Liu. Quantum coordinated multi-point communication based on entanglement swapping. *Quantum Information Processing*, 2017.
- [FCY⁺04] David Fattal, Toby S. Cubitt, Yoshihisa Yamamoto, Sergey Bravyi, and Isaac L. Chuang. Entanglement in the stabilizer formalism, 2004. quant-ph/0406168.
- [FT21] Alex Fischer and Don Townsley. Distributing graph states across quantum networks. In *Proceedings of IEEE International Conference on Quantum Computing and Engineering (QCE)*, 2021. arXiv:2009.10888.
- [GMM17] Ervin Györi, Tamás Róbert Mezei, and Gábor Mészáros. Note on terminal-pairability in complete grid graphs. *Discrete Mathematics*, 340(5):988–990, 2017.
- [Got98] Daniel Gottesman. The Heisenberg representation of quantum computers. *arXiv preprint quant-ph/9807006*, 1998.
- [HPE19] Frederik Hahn, Anna Pappa, and Jens Eisert. Quantum network routing and local complementation. *npj Quantum Information*, 5(1):1–7, 2019.
- [IVK⁺22] Jessica Illiano, Michele Viscardi, Seid Koudia, Marcello Caleffi, and Angela Sara Cacciapuoti. Quantum internet: from medium access control to entanglement access control. arXiv:2205.11923, 2022.
- [MMG19] Clément Meignant, Damian Markham, and Frédéric Grosshans. Distributing graph states over arbitrary quantum networks. *Physical Review A*, 100(052333), 2019. arXiv:1811.05445.

- [MPD23] Jorge Miguel-Ramiro, Alexander Pirker, and Wolfgang Dür. Optimized quantum networks. *Quantum*, 7:919, 2023. arXiv:2107.10275.
- [MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977.
- [NC02] Michael A. Nielsen and Isaac Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2002.
- [PKT⁺19] Mihir Pant, Hari Krovi, Don Towsley, Leandros Tassioulas, Liang Jiang, Prithwish Basu, Dirk Englund, and Saikat Guha. Routing entanglement in the quantum internet. *npj Quantum Information*, 5(1):1–9, 2019.
- [RBB03] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Physical review A*, 68(2):022312, 2003.
- [SMI⁺16] Eddie Schoute, Laura Mančinska, Tanvirul Islam, Iordanis Kerenidis, and Stephanie Wehner. Shortcuts to quantum network routing. arXiv:1610.05238, 2016.
- [Ste96] Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.
- [WEH18] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412), 2018.

A Constructing an f that satisfies condition CSS1, when all a_i, b_i are independent

In this appendix we give a proof for a simpler but instructive special case of how we satisfy CSS1 in Section 3.6. The additional assumption of our special case is to suppose that $a_1, b_1, \dots, a_k, b_k \in \mathbb{F}_2^m$ are linearly independent.

Let \mathcal{L} be the linear subspace of \mathbb{F}_2^m spanned by c_1, \dots, c_k and $a_1, b_1, \dots, a_k, b_k$ (so in particular, $m = 3k$). Let x_1, \dots, x_m be (mod 2) variables. Then the above $3k$ vectors define $3k$ linear functions over \mathcal{L} : every vector $x \in \mathcal{L}$ can be uniquely written as

$$x = \sum_{i=1}^k \alpha_i a_i + \beta_i b_i + \gamma_i c_i$$

for some binary coefficients $\alpha_i, \beta_i, \gamma_i$ that are functions of $x = (x_1, \dots, x_m)$. As such, all these functions are linear, since when writing down $x + x'$ as above, we add the corresponding coefficients. In the sequel we shall create higher-degree polynomials over x_1, \dots, x_m from these linear functions (e.g., $\alpha_1(x)\beta_1(x)$ is a quadratic function).

Let $S \equiv \mathcal{S}_1 \cup \mathcal{S}_2 \cup \dots \cup \mathcal{S}_k$. Note that $S \subseteq \mathcal{L}$. Condition CSS1 (with $i = 1$) asks for a degree- $(k-1)$ polynomial f such that

$$f(a_1) = f(b_1) = 1 \quad \text{and} \quad f(x) = 0 \quad \text{for all } x \in S \setminus \{a_1, b_1\}. \quad (29)$$

Let us show that Eq. (29) is satisfied if we choose f as

$$f(x) = (\alpha_1(x) + \beta_1(x))g(x) \pmod{2}, \quad (30)$$

where

$$g(x) = \sum_{M \subseteq [k]} \prod_{j \in M} \gamma_j(x) \pmod{2}. \quad (31)$$

The polynomial f defined in Eq. (30) has degree k , because $\alpha_1(x) + \beta_1(x)$ has degree 1 and $g(x)$ has degree $k - 1$. However, we will see that the restriction of f onto S coincides with a degree- $(k - 1)$ polynomial.

First, we show that

$$g(x) = \begin{cases} 1 & \text{if } \gamma_1(x) = \gamma_2(x) = \cdots = \gamma_k(x), \\ 0 & \text{otherwise} \end{cases}$$

Indeed, extending the sum over M in Eq. (31) to all subsets $M \subseteq [k]$ would give a function $\prod_{j=1}^k (1 + \gamma_j(x))$ which is zero mod 2 unless $\gamma_j(x) = 0$ for all j . The missing monomial $\prod_{j=1}^k \gamma_j(x)$ associated with the subset $M = [k]$ is zero unless $\gamma_j(x) = 1$ for all j .

By definition of \mathcal{S}_j , any vector $x \in \mathcal{S}_j$ can be written as a sum of an odd number of vectors from the set $\{a_j, b_j, c_1, \dots, c_k\} \setminus \{c_j\}$. In particular, $\gamma_j(x) = 0$ for any $x \in \mathcal{S}_j$. Thus the restriction of $g(x)$ onto S is zero unless $\gamma_j(x) = 0$ for all j . In the latter case one has $x = a_j$ or $x = b_j$ for some $j \in [k]$. If $j = 1$ then $f(x) = 1$ since $\alpha_1(x) + \beta_1(x) = 1$. If $j \geq 2$ then $f(x) = 0$ since $\alpha_1(x) + \beta_1(x) = 0$. This proves Eq. (29).

Next we claim that degree- k monomials in $f(x)$ can be replaced by monomials of degree at most $k - 1$ without changing the restriction of f onto S . Indeed, the sum of all degree- k monomials in $f(x)$ can be written as

$$f'(x) = (\alpha_1(x) + \beta_1(x)) \sum_{i=1}^k \prod_{j \in [k] \setminus \{i\}} \gamma_j(x) \pmod{2}. \quad (32)$$

Suppose $x \in S$. We claim that $f'(x) = 1$ iff $x = a_1 + c_2 + \cdots + c_k$ or $x = b_1 + c_2 + \cdots + c_k$. Indeed, if $x \in \mathcal{S}_j$ for $j \geq 2$ then $f'(x) = 0$ since $\alpha_1(x) + \beta_1(x) = 0$. Suppose $x \in \mathcal{S}_1$. Then $\gamma_1(x) = 0$ and thus $f'(x) = (\alpha_1(x) + \beta_1(x))\gamma_2(x) \cdots \gamma_k(x) \pmod{2}$. By definition of \mathcal{S}_1 , one can write x as a sum of an odd number of vectors from the set $\{a_1, b_1, c_2, \dots, c_k\}$. Hence $f'(x) = 1$ iff $x = a_1 + c_2 + \cdots + c_k$ or $x = b_1 + c_2 + \cdots + c_k$.

If k is even then none of the vectors $a_1 + c_2 + \cdots + c_k$ and $b_1 + c_2 + \cdots + c_k$ belongs to \mathcal{S}_1 . Thus $f'(x) = 0$ for all $x \in S$. If k is odd, the same arguments as above show that

$$f'(x) = \prod_{j=2}^k \gamma_j(x) \quad \text{for any } x \in S. \quad (33)$$

Thus we can replace $f'(x)$ by a monomial of degree either zero (if k is even) or degree $k - 1$ (if k is odd) without changing the restriction of f onto S . This proves condition CSS1.

A numerical example: Let $k = 4$, $m = 12$, and let

$$\begin{aligned}
a_1 &= 000010000000 \\
b_1 &= 000001000000 \\
a_2 &= 000000100000 \\
b_2 &= 000000010000 \\
a_3 &= 000000001000 \\
b_3 &= 000000000100 \\
a_4 &= 000000000010 \\
b_4 &= 000000000001
\end{aligned}$$

We also set $c_i = x_i$ for $1 \leq i \leq 4$, so $c_1 = 100000000000$, etc. To address condition CSS1 for $i = 1$ we want to write down a degree-3 polynomial $f(x_1, \dots, x_{12})$ over \mathbb{F}_2 that on the set $EZ = \mathcal{S}_1 \cup \dots \cup \mathcal{S}_k$ takes value 1 on a_1 and b_1 , and 0 on the rest of EZ . (By symmetry then we can write down similar functions for $i = 2, 3, 4$.) Let $w_4(x)$ be the Hamming weight of the first 4 bits of x and let $w_{-8}(x)$ be the Hamming weight of the last 8 bits of x . Notice that for all $x \in EZ$ we have $w_4(x) \leq 3$ and $w_{-8}(x) \leq 2$, and even within this restriction some weight combinations $(w_4, w_{-8}(x))$ may never arise for any element of EZ . Such weight combinations we will call ‘‘impossible pairs.’’ For each weight combination we have calculated the number of elements of EZ that have that weight combination, see the table below. We put an asterisk (rather than 0) in the entries that represent impossible weight combinations.

$w_{-8} \backslash w_4$	0	1	2	3
0	*	4	*	4
1	8	*	24	*
2	*	12	*	4

The entries are not hard to calculate, and to give a typical example we calculate the (1, 2)-entry: There are 8 weight-1 strings of the last 8 bits, and 6 weight-2 strings of the first 4 bits. However, not all elements of the set $\{a_1, b_1, a_2, \dots, b_4\}$ can be added to some element of the set $\{c_1 + c_2, \dots, c_3 + c_4\}$. For instance $c_1 + c_2 + a_1$ does not occur in EZ , as \mathcal{S}_1 does not contain c_1 . It is easy to see that these bad combinations are half of all possible $8 \cdot 6 = 48$ combinations, hence we obtain 24 as the (1, 2)-entry of the table.

Observe now that $|EZ| = 56 > 16$, so Lemma 5 cannot be applied directly to get a degree-3 polynomial. Let us now construct a degree-3 polynomial $f : \mathbb{F}_2^{12} \rightarrow \mathbb{F}_2$ that *restricted to* EZ satisfies condition CSS1 for $i = 1$. First note that f satisfies CSS1 for $i = 1$ if

$$\forall x \in EZ : f(x) = 1 \iff w_4(x) = 0 \wedge x_5 + x_6 = 1.$$

Consider now the polynomial

$$g(x) = 1 + \sum_{i=1}^4 x_i + \sum_{1 \leq i < j \leq 4} x_i x_j$$

One can easily check that

$$\begin{aligned}
\text{When } w_4(x) &= 0 & 1 & 2 & 3 \\
\text{then } g(x) \bmod 2 &= 1 & 0 & 0 & 1
\end{aligned}$$

and that the polynomial $f(x) = (x_5 + x_6)g(x)$ then takes values on EZ exactly as needed. (For instance, when $w_4 = 3$ and $x \in EZ$ then $x_5 + x_6$ will always give zero, etc.)

B Induction step of Section 3.6: modifications for odd k

Here we extend the proof of k -pairability given in Section 3.6 to odd values of k . Suppose $\ell \geq 0$ is an integer. We say that a family of polynomials $f_T : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ labeled by subsets $T \subsetneq [k]$ with $|T| \leq \ell$ is *valid* if it satisfies the following conditions.

- I1:** f_T depends only on the variables x_{k+1}, \dots, x_m
- I2:** f_T has degree $k - 1 - |T|$
- I3:** $f_\emptyset(a_1) = f_\emptyset(b_1) = 1$ and $f_\emptyset(a_i) = f_\emptyset(b_i) = 0$ for $2 \leq i \leq k$
- I4:** $f_T(x) = \sum_{U \subsetneq T} f_U(x)$ for any non-empty set $T \subsetneq [k]$ and any $x \in e(T)$
- I5:** $f_T \equiv 0$ if $|T|$ is odd and $|T| \leq k - 3$
- I6:** $f_T(0^m) = f_T(a_i + b_i) = 0$ if $i \notin T$ and $|T| \leq k - 4$
- I7:** $f_T(a_i) = f_T(b_i)$ if $i \notin T$ and $|T| \leq k - 3$

These conditions are identical to the ones given in Section 3.6, except for condition (I7) which is now imposed only for $|T| \leq k - 3$. Below we assume that k is odd. As before, we shall use induction on ℓ to prove that a valid family of polynomials exists for all $\ell \leq k - 1$.

The base of induction is $\ell = 0$. Then a valid family is a single polynomial f_\emptyset . The construction of f_\emptyset is identical to the one given in Section 3.6.

We shall now prove the induction step. Suppose we have already constructed a valid family of polynomials f_T with $|T| \leq \ell - 1$. Consider a subset $T \subsetneq [k]$ with $|T| = \ell$ such that $1 \leq \ell \leq k - 2$. The case $\ell = k - 1$ will be considered afterwards.

Suppose $|T|$ is odd. Condition (I2) demands that f_T has degree $d_T = k - 1 - |T|$. Condition (I3) can be skipped since $T \neq \emptyset$. Consider two cases.

Case 1: $|T| \leq k - 3$. Then (I5) demands $f_T \equiv 0$. This automatically satisfies (I6,I7). It remains to check (I4) which is equivalent to

$$\sum_{U \subsetneq T} f_U(x) = 0 \tag{34}$$

for $x \in e(T)$. Note that $e(T)$ consists of points 0^m and $a_i + b_i$ with $i \notin T$. All terms $f_U(x)$ with odd $|U|$ vanish due to (I5). All terms $f_U(x)$ with even $|U|$ obey (I6). Since $|U| \leq |T| - 1 \leq k - 4$, we have $f_U(0^m) = 0$ and $f_U(a_i + b_i) = 0$ due to (I6). Thus all terms $f_U(x) = 0$ vanish, that is, Eq. (34) is satisfied.

Case 2: $|T| \geq k - 2$. Then $|T| = k - 2$ since both k and $|T|$ are odd. We can skip (I5,I6,I7). Thus we just need to satisfy (I4). It fixes the values of f_T at $s = |e(T)| = k - |T| + 1 = 3$ points, namely, 0^m and $a_i + b_i$ with $i \notin T$. Since $s = 3 < 2^{d_T+1} = 2^{k-|T|} = 4$, the desired polynomial f_T exists by part (1) of Lemma 5.

Suppose $|T|$ is even. Condition (I2) demands that f_T has degree $d_T = k - 1 - |T|$. Conditions (I3),(I5) can be skipped since $|T|$ is even and $T \neq \emptyset$. We claim that (I7) follows from (I4). Indeed, we have $x \in e(T)$ iff $x = a_i$ or $x = b_i$ with $i \notin T$. We have $f_T(x) = \sum_{U \subsetneq T} f_U(x)$ due to (I4). If $|U|$ is odd then $f_U \equiv 0$ due to (I5) since $|U| \leq |T| - 1 = \ell - 1 \leq k - 3$. If $|U|$ is even then $|U| \leq |T| - 2 \leq k - 4$. Thus $f_U(a_i) = f_U(b_i)$ since (I7) holds for f_U . This implies $f_T(a_i) = f_T(b_i)$ for any $i \notin T$, as claimed in (I7). It remains to check (I4,I6). We fix the value of f_T at $s = |e(T)| = 2(k - |T|)$ points in

(I4) if $|T| \geq k - 3$. We fix the value of f_T at $s = |e(T)| + k - |T| + 1 = 3(k - |T|) + 1$ points in (I4,I6) if $|T| \leq k - 4$. Consider first the case $|T| \geq k - 3$. Then $|T| = k - 3$ since k is odd, $|T|$ is even, and $|T| = \ell \leq k - 2$. Thus $s = 2(k - |T|) = 6 < 2^{d_T+1} = 2^{k-|T|} = 8$. Part (1) of Lemma 5 implies that the desired polynomial f_T exists. Next consider the case $|T| \leq k - 4$. Then $s = 3(k - |T|) + 1 < 2^{d_T+1} = 2^{k-|T|}$. Part (1) of Lemma 5 implies the desired polynomial f_T exists.

It remains to prove the induction step for $\ell = k - 1$. Suppose we have already constructed a valid family of polynomials f_T with $|T| \leq k - 2$. Consider a subset $T \subsetneq [k]$ with $|T| = k - 1$. Since we assumed that k is odd, $|T|$ is even. Condition (I2) demands that f_T has degree $k - 1 - |T| = 0$, that is, f_T is a constant function. We can skip conditions (I3,I5,I6,I7) since none of them applies if $|T| = k - 1$. It remains to check (I4). Note that $e(T) = \{a_i, b_i\}$ for some $i \in [k]$ such that $T = [k] \setminus \{i\}$. Condition (I4) fixes the value of f_T at a_i and b_i . Since we want f_T to be a constant function, it suffices to check that the desired values $f_T(a_i)$ and $f_T(b_i)$ are the same. Substituting the desired values from (I4), we have to check that

$$\sum_{U \subsetneq T} f_U(a_i) + f_U(b_i) = 0. \quad (35)$$

All terms $f_U(a_i) + f_U(b_i)$ with $|U| \leq k - 3$ vanish since f_U obeys (I7). Thus we can restrict the sum Eq. (35) to terms with $|U| = k - 2$. However f_U is a degree-1 polynomial if $|U| = k - 2$ due to (I2). Thus $f_U(a_i) + f_U(b_i) = f_U(0^m) + f_U(a_i + b_i)$ and Eq. (35) is equivalent to

$$\sum_{\substack{U \subsetneq T \\ |U|=k-2}} f_U(0^m) + f_U(a_i + b_i) = 0. \quad (36)$$

Since f_U obeys (I4) and $|U|$ is odd, we have $f_U(X) = \sum_{V \subsetneq U} f_V(x)$ for $x = 0^m$ or $x = a_i + b_i$. Thus Eq. (36) is equivalent to

$$\sum_{\substack{U \subsetneq T \\ |U|=k-2}} \sum_{V \subsetneq U} f_V(0^m) + f_V(a_i + b_i) = 0. \quad (37)$$

All terms f_V with odd $|V|$ vanish due to (I5) since $|V| \leq |U| - 1 = k - 3$. All terms f_V with even $|V|$ and $|V| \leq k - 4$ vanish due to (I6). Thus we can restrict the sum Eq. (37) to terms with $|V| = k - 3$ and it suffices to check that

$$\sum_{\substack{U \subsetneq T \\ |U|=k-2}} \sum_{\substack{V \subsetneq U \\ |V|=k-3}} f_V(0^m) + f_V(a_i + b_i) = 0. \quad (38)$$

However, each term $f_V(0^m)$ and $f_V(a_i + b_i)$ is counted exactly two times: if $V = T \setminus \{p, q\}$ then one can choose $U = T \setminus \{p\}$ or $U = T \setminus \{q\}$. Since we do all arithmetic modulo two, this implies Eq. (38). Thus (I4) is satisfied. This completes the induction step for odd k .