Fault-Tolerant Conversion between the Steane and Reed-Muller Quantum Codes

Jonas T. Anderson, Guillaume Duclos-Cianci, and David Poulin
Département de Physique, Université de Sherbrooke, Sherbrooke, Québec J1K 2R1, Canada

(Received 1 April 2014; published 20 August 2014)

Steane's 7-qubit quantum error-correcting code admits a set of fault-tolerant gates that generate the Clifford group, which in itself is not universal for quantum computation. The 15-qubit Reed-Muller code also does not admit a universal fault-tolerant gate set but possesses fault-tolerant T and control-control-Z gates. Combined with the Clifford group, either of these two gates generates a universal set. Here, we combine these two features by demonstrating how to fault-tolerantly convert between these two codes, providing a new method to realize universal fault-tolerant quantum computation. One interpretation of our result is that both codes correspond to the same subsystem code in different gauges. Our scheme extends to the entire family of quantum Reed-Muller codes.

DOI: 10.1103/PhysRevLett.113.080501 PACS numbers: 03.67.Pp, 03.67.Lx

A prominent technique of fault-tolerant quantum computation is the use of transversal gates [1]. In an architecture where each logical qubit is encoded in a code block which can protect against up to t errors, a gate is said to be transversal if it does not couple qubits inside a given block. As a consequence of transversality, the number of errors or faults in a block cannot increase under the application of a gate: the number of errors after the gate is at most the number of initial errors in the data plus the number of faults in the execution of the gate. Single-qubit errors can propagate to single-qubit errors in other blocks, but these will be corrected independently on each block. In this way, an error-rate ϵ becomes $c\epsilon^{t+1}$ after error correction, where c is at most the number of different ways of getting $t+1$ faults in a single block. Recursing this procedure leads to the celebrated accuracy threshold theorem [1–5].

Unfortunately, it is not possible to construct a quantum code which admits a universal set of transversal gates [6], so additional techniques are required. In many circumstances it is possible to fault-tolerantly implement the Clifford group, a finite subgroup of the unitary group which is not universal. In particular, all codes of the Calderbank-Shor-Steane (CSS) family have transversal controlled-not operations [7], and code deformation can be used to implement the entire Clifford group in topological codes [8]. Magic-state distillation and injection [9] is the most common technique to complete the universal gate set.

Recently, other techniques have been proposed to circumvent this no-go on transversal gates. Jochym-O'Connor and Laflamme [10] used a "relaxed" notion of transversality which only demands that gates do not transform a single error or fault into an uncorrectable error, without prohibiting that it couples qubits from the same block. The same idea is responsible for the success of code deformation [8,11], which changes the error-correcting code in such a way that a full cycle returning to the original code implements a gate. Because each step in the deformation acts on a number of qubits which is less than the minimum distance of the codes, the transformation is fault tolerant despite being nontransversal [12]. Therefore, schemes for topological quantum computation [13] are a form of code deformation. Paetznick and Reichardt [14] (see also a related idea of Knill, Laflamme, and Zurek [15]) proposed a scheme where transversal gates take the system outside the code space, but a subsequent round of error correction restores it. As we discuss below, this is conceptually equivalent to Bombín's scheme [16] where transversal gates are applied to a subsystem code [17,18], altering the gauge degrees of freedom while applying a logical gate to the encoded data. The gauge can be returned to a standard state before a new gate is applied.

Here, we propose a scheme that converts between two codes which, jointly, possess a universal set of transversal gates. Clifford group transformations are realized in Steane's 7-qubit code [19], while the $T = Z^{1/4}$ gate and/or the control-control-Z gate are realized using the 15-qubit Reed-Muller code [15]; either of these last two gates is sufficient to complete the universal gate set, but an over-complete set can reduce the compilation overhead [20]. While it is always possible to convert between codes by preparing a special ancillary entangled state to teleport the data, our main contribution is a fault-tolerant scheme which directly converts the information in place. Much like in the approaches outlined above, the code is modified during the computation. One important difference here is that the codes involved have different numbers of qubits, an aspect that should be taken into account when optimizing resources to realize a given quantum circuit. Similarly to the proposals of Refs. [14] and [16], our scheme can be seen as a subsystem encoding [17,18] with different gauge fixing. In fact, our approach should be seen as complementary to Refs. [14,16], which enables a much richer set of transversal gates and extends to the entire quantum Reed-Muller code family.

The rest of this Letter is organized as follows: After a brief review of classical and quantum codes, we present the family of quantum Reed-Muller codes and highlight some of their key properties. Then, we review transversal gate constructions for these codes. We then explain the conversion scheme, which essentially relies on a recursive definition of the Reed-Muller codes. Lastly, we present an alternative derivation in terms of subsystem codes, and conclude by discussing possible applications of our scheme.

Codes.—An n-bit classical linear code encoding k bits is defined as the null space of a $(n-k)\times n$ parity-check matrix H (in $\mathbb{Z}_2$ arithmetic), i.e., $\mathcal{C}=\{x\in\mathbb{Z}_2^n\colon Hx=0\}$. Its minimum distance d is the minimum number of bit flips required to map one code word to another. Given an erroneous string $x'=x+e$ obtained from a code word x and error e, the error syndrome is given by $s=Hx'=He$ and can unambiguously identify any error acting on less than or equal to $(d-1)/2$ bits. The code can also be defined as the row space of a $k\times n$ generator matrix G, i.e., $\mathcal{C}=\mathrm{row}(G)$, which is the dual of H, i.e., $HG^T=0$.

A stabilizer code encoding k qubits into n qubits is specified by a set $\mathcal{A}$ of n-k independent stabilizer generators, which are commuting and Hermitian elements of the n-qubit Pauli group (obtained from the n-fold tensor product of the 2×2 identity I and the Pauli matrices X, Y, and Z). The code space $\mathcal{C}$ is a subspace of the n-qubit Hilbert space stabilized by $\mathcal{A}$,

$$\mathcal{C}=\{|\psi\rangle\in(\mathbb{C}^2)^{\otimes n}\colon\ A|\psi\rangle=|\psi\rangle\quad\forall\ A\in\mathcal{A}\}.\tag{1}$$

Equivalently, it can be defined as the image of the code projector $P_{\mathcal{A}}=\prod_{A\in\mathcal{A}}(I+A)/2=(1/2^{|\mathcal{A}|})\sum_{S\in\mathcal{S}}S$, where $\mathcal{S}$ is the stabilizer group generated by $\mathcal{A}$. When a code state $|\psi\rangle\in\mathcal{C}$ undergoes a Pauli error E, error correction is realized by measuring the stabilizer generators. The ± 1 measurement outcome of measuring $A_j\in\mathcal{A}$ indicates whether A_j commutes or anticommutes with E: $A_j(E|\psi\rangle)=\pm EA_j|\psi\rangle=\pm(E|\psi\rangle)$. Logical operators transform the state but preserve the code space; i.e., they are elements of $N(\mathcal{S})-\mathcal{S}$, where N denotes the normalizer of a group. A code has distance d if it takes an error of weight d or more to map a code word to a distinct code word. These parameters of a code are collectively denoted (n, k, d) in the classical setting and [[n, k, d]] in the quantum setting.

The Reed-Muller code.—The Reed-Muller codes of order 1 can be defined recursively [21]: the code $\mathsf{RM}(1,1)$ has generator matrix

$$G_1=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\tag{2}$$

and the code $\mathsf{RM}(1,m+1)$ has generator matrix

$$G_{m+1}=\begin{pmatrix}G_m & G_m\\ \mathbf{0} & \mathbf{1}\end{pmatrix}.\tag{3}$$

(and bold symbols $\mathbf{0}$ and $\mathbf{1}$ designate strings of 0 s and 1 s of lengths fixed by the context). The dual of $\mathsf{RM}(1,m)$ is $\mathsf{RM}(m-2,m)$ and has generator matrix H_m. Quantum codes are derived from shortened Reed-Muller codes $\overline{\mathsf{RM}}(1,m)$, where the first row and column are deleted from G_m. We can similarly define shortened dual codes $\overline{\mathsf{RM}}(m-2,m)$ with generator matrix $\bar{H}_m$. Hence, the generator matrices of $\overline{\mathsf{RM}}(1,m)$ obey the recursive definition

$$\bar{G}_{m+1}=\begin{pmatrix}\bar{G}_m & \bar{G}_m & \mathbf{0}^T\\ \mathbf{0} & \mathbf{1} & 1\end{pmatrix}\tag{4}$$

(we have permuted the columns for later convenience). Note that $\overline{\mathsf{RM}}(m-2,m)$ is not the dual of $\overline{\mathsf{RM}}(1,m)$. Using this definition, the following facts can easily be verified (see Appendix A in the Supplemental Material [22]) by induction for $m\geq 2$.

1. For $x\in\mathsf{RM}(1,m)$ or $\overline{\mathsf{RM}}(1,m)$, $|x|=0\bmod 2^{m-1}$.
2. For $m\geq 3$, $\overline{\mathsf{RM}}(1,m)$ is contained in its dual, i.e., $\bar{G}_m\bar{G}_m^T=0$.
3. The minimum distance of the dual code to $\overline{\mathsf{RM}}(1,m)$ is 3.
4. $\overline{\mathsf{RM}}(1,m)$ is contained in the dual of $\overline{\mathsf{RM}}(m-2,m)$, i.e., $\bar{H}_m\bar{G}_m^T=0$.
5. $\overline{\mathsf{RM}}(1,m)$ is contained in $\overline{\mathsf{RM}}(m-2,m)$, i.e., $\mathrm{row}(\bar{G}_m)\subset\mathrm{row}(\bar{H}_m)$.
6. For $x_1,\ x_2,\ldots,x_p\in\overline{\mathsf{RM}}(1,m)$, $x_1\cdot x_2\cdot\ldots x_p=0\bmod 2^{m-p}$.

The quantum Reed-Muller codes [23] $\mathsf{QRM}(m)$ derived from $\overline{\mathsf{RM}}(1,m)$ codes are CSS codes, meaning that their stabilizer generators break into two sets $\mathcal{A}_m^x$ and $\mathcal{A}_m^z$ [24,25]. Elements of $\mathcal{A}_m^x$ are obtained from rows of $\bar{G}_m$, by substituting 1 s by X's and 0 s for I's. Elements of $\mathcal{A}_m^z$ are obtained in a similar way, but from the generator matrix of the shortened dual code $\overline{\mathsf{RM}}(m-2,m)$.

In a CSS code, $\mathcal{A}^x$ detects z-type errors and $\mathcal{A}^z$ detects x-type errors. It follows from fact 3 that $\mathsf{QRM}(m)$ have minimum distance $d=3$, so the parameters of the code are [[$n=2^m-1$, $k=1$, $d=3$]]. The logical operators are given by the rows that were removed in the shortening procedure, they are $\bar{X}_m=X^{\otimes n}$ and $\bar{Z}_m=Z^{\otimes n}$. Finally, note that the commutation of the stabilizer generators follows from the orthogonality of $\overline{\mathsf{RM}}(1,m)$ and $\overline{\mathsf{RM}}(m-2,m)$ (fact 4).

Transversal gates.—The logical 0 state of a code should be a simultaneous $+1$ eigenstate of $\bar{Z}$ and all elements of $\mathcal{A}$. The state $|\mathbf{0}\rangle$ is already a $+1$ eigenstate of $\bar{Z}$ and of all $\mathcal{A}_m^z$, so we obtain the logical 0 by projecting it onto the $+1$ eigenspace of elements of $\mathcal{A}_m^x$,

$$|\bar{0}\rangle_S = \prod_{A\in\mathcal{A}_m^x} \frac{I+A}{2}|\mathbf{0}\rangle \tag{5}$$

$$= \frac{1}{|\mathcal{S}_x|}\sum_{S\in\mathcal{S}_m^x} S|\mathbf{0}\rangle \tag{6}$$

$$= \frac{1}{|\mathcal{S}_x|}\sum_{x\in\mathrm{row}(\bar{G}_m)} |x\rangle. \tag{7}$$

The logical 1 is obtained by applying $\bar{X}_m$ to this state, so it is $|\bar{1}\rangle = 1/|\mathcal{S}_x|\sum_{x\in\mathrm{row}(\bar{G}_m)}|x\oplus\mathbf{1}\rangle$. It follows from fact 1 that $|\bar{0}\rangle$ is the superposition of strings of weight $0 \bmod 2^{m-1}$ and $|\bar{1}\rangle$ is the superposition of strings of weight $-1 \bmod 2^{m-1}$.

Consider now the single-qubit gate $Z(\omega_\ell) = \mathrm{diag}(1,\omega_\ell)$ where ω_ℓ is the ℓth root of unity. Observe that for any n-bit string x, $Z(\omega_\ell)^{\otimes n}|x\rangle = \omega_\ell^{|x|}|x\rangle = \omega_\ell^{(|x| \bmod \ell)}|x\rangle$. From the above consideration on the weights of the basis states appearing in the logical states $|\bar{0}\rangle$ and $|\bar{1}\rangle$, it follows that for $\ell = 2^{m-1}$, the transversal gate $Z(\omega_\ell)^{\otimes n}$ acts as the logical $Z(\omega_\ell)^\dagger$ on $\mathsf{QRM}(m)$ [26–28].

The codes $\mathsf{QRM}(m)$ also have a transversal k-fold controlled-Z gate for $k \le m-2$. Note that the transversal k-fold controlled gate acts on a basis state $|x_1\rangle|x_2\rangle\ldots|x_{k+1}\rangle$ by introduction of a phase factor $(-1)^{x_1\cdot x_2\cdot\ldots x_{k+1}}$. A logical state $|\bar{y}\rangle$ is the superposition of states of the form $|x+y\mathbf{1}\rangle$ where $x\in\overline{\mathsf{RM}}(1,m)$. When acted on by a transversal k-fold controlled-Z gate, a logical state $|\bar{y}_1\rangle|\bar{y}_2\rangle\ldots|\bar{y}_{k+1}\rangle$ will pick up a phase factor $(x_1+y_1\mathbf{1})\cdot(x_2+y_2\mathbf{1})\cdot\ldots(x_{k+1}+y_{k+1}\mathbf{1})$ where $x_j\in\overline{\mathsf{RM}}(1,m)$ for all j. Expanding this product, all terms containing x's produce a trivial phase due to fact 6, so only the term $y_1y_2\ldots y_{k+1}$ contributes to the phase, which produces the desired transformation.

The 7-qubit Steane code is derived from the classical code $\overline{\mathsf{RM}}(1,3)$, also known as the classical (7,4,3) Hamming code. This is a special case as it is self-dual, which implies that $\mathcal{A}_3^x$ and $\mathcal{A}_3^z$ are equal up to exchanging X's for Z's. As a consequence it has transversal Clifford gates. The Hadamard gate H exchanges X and Z. It is thus clear that the transversal gate $H^{\otimes 7}$ preserves the code space (as it only swaps $\mathcal{A}_3^x$ with $\mathcal{A}_3^z$) and acts as the logical Hadamard by exchanging $\bar{X}$ with $\bar{Z}$. The CNOT operation acting on two qubits maps the operators (IX, XI, IZ, ZI) to (IX, XX, ZZ, ZI). The transversal gate $\mathrm{CNOT}^{\otimes 7}$ therefore acts on the logical operators as a logical CNOT operation, and maps the set of generators $\{I\mathcal{A}_3^x, \mathcal{A}_3^x I, I\mathcal{A}_3^z, \mathcal{A}_3^z I\}$ of $\mathcal{S}_3\otimes\mathcal{S}_3$ to $\{I\mathcal{A}_3^x, \mathcal{A}_3^x\mathcal{A}_3^x, \mathcal{A}_3^z\mathcal{A}_3^z, \mathcal{A}_3^z I\}$, which is simply a different set of generators for $\mathcal{S}_3\otimes\mathcal{S}_3$, so the code is preserved. Finally, the phase gate P corresponds to $Z(\omega_4)$ defined above and is transversal as we have seen.

Conversion.—The key feature of quantum Reed-Muller codes which enables our construction, and which follows from fact 5 $\overline{\mathsf{RM}}(1,m)\subset\overline{\mathsf{RM}}(m-2,m)$, is that $\mathcal{A}_m^z$ contains the same operators as $\mathcal{A}_m^x$ with X's replaced by Z's, plus some additional operators. In other words, if we consider the checks $\mathcal{A}_m'^z$ obtained by replacing X by Z in $\mathcal{A}_m^x$, then $\mathcal{A}_m^z = \mathcal{A}_m'^z \cup \tilde{\mathcal{A}}_m^z$ for some set of z-stabilizer generators $\tilde{\mathcal{A}}_m^z$. Since elements of $\mathcal{A}_m^x$ can unambiguously discriminate all single-qubit z errors, it follows that $\mathcal{A}_m'^z$ can unambiguously discriminate all single-qubit x errors; i.e., operators from $\tilde{\mathcal{A}}_m^z$ are superfluous. Starting from the "relevant" stabilizers $\mathcal{A}_m^x$ and $\mathcal{A}_m'^z$, there are many ways to complete the list of stabilizers in order to obtain a valid error-correcting code. Our scheme will make use of this freedom to convert between different codes.

It follows from Eq. (4) that the relevant stabilizers $\mathcal{A}_m^x$ and $\mathcal{A}_m'^z$ can be defined recursively. Given two ordered sets $\mathcal{A} = \{A_1, A_2, \ldots\}$ and $\mathcal{B} = \{B_1, B_2, \ldots\}$, we introduce the notation $\mathcal{A}\times\mathcal{B} = \{A_1\otimes B_1, A_2\otimes B_2, \ldots\}$, and write

$$\mathcal{A}_{m+1}^x = \left\{\begin{matrix} \mathcal{A}_m^x & \times & \mathcal{A}_m^x & \otimes & I, \\ I^{\otimes n} & \otimes & \bar{X}_m & \otimes & X \end{matrix}\right\} \quad \text{and} \tag{8}$$

$$\mathcal{A}_{m+1}'^z = \left\{\begin{matrix} \mathcal{A}_m'^z & \times & \mathcal{A}_m'^z & \otimes & I, \\ I^{\otimes n} & \otimes & \bar{Z}_m & \otimes & Z \end{matrix}\right\}. \tag{9}$$

Let us first explain how to convert from $\mathsf{QRM}(m)$ to $\mathsf{QRM}(m+1)$. We begin with some information encoded in a (2^m-1)-qubit state of $\mathsf{QRM}(m)$, $|\bar{\psi}\rangle_m$. We prepare a 2^m-qubit quantum state $|\Phi\rangle = 1/\sqrt{2}(|\bar{0}\rangle_m|0\rangle + |\bar{1}\rangle_m|1\rangle)$ consisting of a maximally entangled state between a bare qubit and a qubit encoded in $\mathsf{RM}(m)$. Viewing the joint state $|\bar{\psi}\rangle_m\otimes|\Phi\rangle$ as an encoded state of a $(2^{m+1}-1)$-qubit code, we can write the generators for this "extended quantum Reed-Muller code" as

$$\begin{gathered} \mathcal{A}_m^z\otimes I^{\otimes n}\otimes I, \\ \mathcal{A}_m^x\otimes I^{\otimes n}\otimes I, \\ I^{\otimes n}\otimes\mathcal{A}_m^z\otimes I, \\ I^{\otimes n}\otimes\mathcal{A}_m^x\otimes I, \\ I^{\otimes n}\otimes\bar{Z}_m\otimes Z, \\ I^{\otimes n}\otimes\bar{X}_m\otimes X. \end{gathered} \tag{10}$$

We can change the generating set without changing the code and instead use

$$\begin{gathered} \mathcal{A}_m'^z\times\mathcal{A}_m'^z\otimes I, \\ \mathcal{A}_m^x\times\mathcal{A}_m^x\otimes I, \\ I^{\otimes n}\otimes\bar{Z}_m\otimes Z, \\ I^{\otimes n}\otimes\bar{X}_m\otimes X, \\ \tilde{\mathcal{A}}_m^z\times\tilde{\mathcal{A}}_m^z\otimes I, \\ \mathcal{A}_m^z\otimes I^{\otimes n}\otimes I, \\ \mathcal{A}_m^x\otimes I^{\otimes n}\otimes I. \end{gathered} \tag{11}$$

We immediately recognize the first $2m+2$ generators of this list [first four rows of Eq. (11)] as generating the relevant stabilizers of $\mathsf{QRM}(m+1)$, i.e., $\mathcal{A}^x_{m+1}$ and $\mathcal{A}'^z_{m+1}$. Indeed, compare to Eqs. (8), (9). Thus, only operators from the last three lines of Eq. (11) differ, and must be substituted by $\tilde{\mathcal{A}}^z_{m+1}$ to convert into $\mathsf{QRM}(m+1)$. In fact, only the m stabilizers of the last line are a problem, since $\tilde{\mathcal{A}}^z_m \times \tilde{\mathcal{A}}^z_m \otimes I$ and $\mathcal{A}^z_m \otimes I^{\otimes n} \otimes I \subset \tilde{\mathcal{A}}^z_{m+1}$.

But as explained in the previous paragraphs, these m stabilizers are superfluous in the sense that they are not required to diagnose single-qubit errors. Thus, if we fault-tolerantly measure all stabilizers of $\mathsf{QRM}(m+1)$ on the state $|\bar{\psi}\rangle_m \otimes |\Phi\rangle$, we can use the syndrome from the first six rows of Eq. (11) to diagnose errors, and remove any syndrome associated to the last m stabilizers by a fault-tolerant error-correction procedure (or by adapting the Pauli frame). Specifically, given a set of stabilizer generators $\mathcal{A} = \{A_1, \ldots, A_{n-k}\}$ and logical operators $\mathcal{L} = \{\bar{X}_a, \ldots, \bar{}X_k, \bar{Z}_1, \ldots, \bar{X}_k\}$, there exists a set of "pure errors" $\mathcal{T} = \{T_1, \ldots, T_{n-k}\}$ such that T_j commutes with all elements of $\mathcal{L}$, $\mathcal{T}$, and $\mathcal{A}$ except A_j with which it anticommutes. A syndrome $A_j = -1$ revealed by one of the last m stabilizers $j = n-k-m, \ldots, n-k$ is corrected by applying T_j.

To summarize, to convert from $\mathsf{QRM}(m)$ to $\mathsf{QRM}(m+1)$, we first fault-tolerantly prepare the 2^m-qubit stabilizer state $|\Phi\rangle$, append it to the system, fault-tolerantly measure the stabilizer generators of $\mathsf{QRM}(m+1)$, error-correct given the first $2^{m+1}-m-2$ syndrome bits [first six rows of Eq. (11)], and restore the last m syndrome bits using their associated pure errors.

To convert from $\mathsf{QRM}(m+1)$ to $\mathsf{QRM}(m)$, we simply fault-tolerantly measure the stabilizers of Eq. (11), use the first $2^{m+1}-m-2$ syndrome bits [first six rows of Eq. (11)] to diagnose errors, and restore the last m syndrome bits using the associated pure errors. We can then remove the additional 2^m qubits and be left with the (2^m-1)-qubit state $|\bar{\psi}\rangle_m$ encoded in $\mathsf{QRM}(m)$.

Subsystem code interpretation.—It is possible to recast the above conversion scheme using the subsystem code formalism [17,18], which highlights its similarity with the Paetznick and Reichardt [14] and the Bombín [16] schemes. We can define a stabilizer code from the stabilizers that are common to $\mathsf{QRM}(m+1)$ and the extended $\mathsf{QRM}(m)$. There are $2^{m+1}-m-2$ of these and they are given by the first six lines of Eq. (11). Thus, this code encodes $k = m+1$ logical qubits and has minimum distance $d = 3$, so it can error correct any single-qubit error.

One of these logical qubits, which we label 0, is the one encoded in the original code and has logical operators $\bar{X}^0 = \bar{X}_m$ and $\bar{Z}^0 = \bar{Z}_m$. The other logical operators associated with "gauge qubits" $\bar{X}^j$ with $j = 1, \ldots, m$ correspond to elements of the last line of Eq. (11). Their conjugate partners $\bar{Z}^j$ are generated by elements of $\tilde{\mathcal{A}}^z_{m+1}$.

We obtain a subsystem code by choosing to encode information only in the first logical qubit of the code. The other logical qubits $j = 1, 2, \ldots, m$ carry no information, and can be fixed to an arbitrary state. The conversion scheme described above then simply consists in fixing these m gauge qubits all in state $|\bar{0}\rangle$ or all in state $1/\sqrt{2}(|\bar{0}\rangle + |\bar{1}\rangle)$. The first scenario can be realized by measuring the operators $\bar{Z}^j$, and flipping the qubit using $\bar{X}^j$ if the outcome is -1. This procedure brings the state to the extended quantum Reed-Muller code, and the last 2^m qubits can be discarded to obtain a state encoded in $\mathsf{QRM}(m)$. The second scenario can be realized by measuring the operators $\bar{X}^j$, and flipping the qubit using $\bar{Z}^j$ if the outcome is -1. This procedure brings the state to $\mathsf{QRM}(m+1)$.

Thus, we see that the different quantum Reed-Muller codes all correspond to the same subsystem code with different gauge fixing. Depending on the chosen gauge, some qubits become unentangled with the part of the code supporting the data, and can be discarded. At the bottom of this hierarchy is Steane's 7-qubit code, which realizes the entire Clifford group transversally. Above is an infinite family of quantum Reed-Muller codes which admit increasingly complex transversal gates [29].

Conclusion and outlook.—We have presented a scheme to directly and fault-tolerantly convert between a family of quantum error-correcting codes. By combining the transversal gate sets of these codes, we obtain a (overcomplete) universal gate set. Our result offers a deeper understanding of a recent proposal [14] and complements it in many ways.

An important advantage of our conversion scheme is its potential reduction of overhead. We can envision an architecture where special areas in the computer are dedicated to the execution of non-Clifford gates. In those areas, the encoding uses concatenated Reed-Muller codes, while the rest of the computer is encoded with concatenated Steane codes, an important overhead reduction over Ref. [14] when few non-Cliford gates are executed in parallel. Qubits are brought into these special areas to realize non-Clifford gates.

Finally, we note that the higher-order Reed-Muller codes $\mathsf{RM}(r,m)$ obey a similar recursive definition

$$G_{r,m+1} = \begin{pmatrix} G_{r,m} & G_{r,m} \\ 0 & G_{r-1,m} \end{pmatrix} \tag{12}$$

and are dual-containing when their rates are more than $1/2$ [21], so our conversion procedure can be extended to this broader class of codes (see Appendix B in the Supplemental Material [22]). The two main motivations to study these codes is that they can have a larger minimal distance and admit a richer set of transversal gates [28]. Moreover, the Reed-Muller code family can be used to distill magic states [14,26–28]. Distillation is a procedure which uses Clifford operations to increase the fidelity of nonstabilizer states, which can be injected into the computation to realize non-Clifford transformations [9]. Higher-order Reed-Muller codes of minimal distance greater than 3 could be used to improve magic state distillation protocols.

This work was partially funded by Canada's NSERC, Québec's FRQNT through the network INTRIQ, and the Lockheed Martin Corporation. D. P. acknowledges the hospitality of The University of Sydney where this project was completed. We thank Michael Beverland for comments on this manuscript.

[1] P. W. Shor, in *Proceedings of the 37th Symposium on the Foundations of Computer Science (FOCS), Los Alamitos, California, 1996* (IEEE, New York, 1996), pp. 56–65.

[2] D. Aharonov and M. Ben-Or, in Proceedings of the 29th Annual ACM Symposium on Theory of Computing (STOC), El Paso, Texas, 1997 (ACM, New York, 1997), pp. 176–188.

[3] A. Y. Kitaev, Russ. Math. Surv. **52**, 1191 (1997).

[4] E. Knill, R. Laflamme, and W. H. Zurek, Proc. R. Soc. A **454**, 365 (1998).

[5] J. Preskill, Proc. R. Soc. A **454**, 385 (1998).

[6] B. Eastin and E. Knill, Phys. Rev. Lett. **102**, 110502 (2009).

[7] A. M. Steane, Nature (London) **399**, 124 (1999).

[8] H. Bombin and M. Martin-Delgado, J. Phys. A **42**, 095302 (2009).

[9] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).

[10] T. Jochym-O'Connor and R. Laflamme, Phys. Rev. Lett. **112**, 010505 (2014).

[11] H. Bombin, New J. Phys. **13**, 043005 (2011).

[12] H. Bombin, G. Duclos-Cianci, and D. Poulin, New J. Phys. **14**, 073048 (2012).

[13] R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).

[14] A. Paetznick and B. W. Reichardt, Phys. Rev. Lett. **111**, 090505 (2013).

[15] E. Knill, R. Laflamme, and W. Zurek, arXiv:quant-ph/9610011.

[16] H. Bombín, arXiv:1311.0879.

[17] D. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).

[18] D. Poulin, Phys. Rev. Lett. **95**, 230504 (2005).

[19] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[20] G. Duclos-Cianci and D. Poulin, arXiv:1403.5280.

[21] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977).

[22] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.113.080501 for proofs of the six facts and generalization to higher rank Reed-Muller codes.

[23] A. M. Steane, IEEE Trans. Inf. Theory **45**, 1701 (1999).

[24] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[25] A. M. Steane, Proc. R. Soc. A **452**, 2551 (1996).

[26] E. T. Campbell, H. Anwar, and D. E. Browne, Phys. Rev. X **2**, 041021 (2012).

[27] S. Bravyi and J. Haah, Phys. Rev. A **86**, 052329 (2012).

[28] A. Landahl and C. Cesare, arXiv:1302.3240.

[29] D. Gottesman and I. Chuang, Nature (London) **402**, 390 (1999).

Supplementary Information:
Fault-tolerant conversion between the Steane and Reed-Muller quantum codes

Jonas T. Anderson, Guillaume Duclos-Cianci, and David Poulin*
Département de Physique, Université de Sherbrooke, Sherbrooke, Québec, Canada

(Dated: June 18, 2014)

Appendix A— In this appendix we prove the 6 properties of the shortened Reed-Muller codes listed in the main text as Facts. It will be useful to make use of an alternative recursive definition of these codes [1]:

$$\mathsf{RM}(1,m+1)=\{(x,x),(x,x+\mathbf{1}):x\in\mathsf{RM}(1,m)\}\,. \quad (1)$$

Fact 1. For $\mathsf{RM}(1,m)$, the base case $m=2$ can be verified directly. Suppose that the fact holds for m, which means that the allowed weights of elements of $\mathsf{RM}(1,m)$ are $w_m=0$, 2^{m-1}, or 2^m. Using Eq. (1), we see that the weight of elements of $\mathsf{RM}(1,m+1)$ will be either $2w_m$ or $w_m+(2^m-w_m)$, so the condition is satisfied. When we shorten the code to get $\overline{\mathsf{RM}}(1,m)$, we remove a row from G_m which contains all 1s and then remove a column containing all 0s. Thus, we have

$$\mathsf{RM}(1,m)=\left\{(0,x),(1,x+\mathbf{1}):x\in\overline{\mathsf{RM}}(1,m)\right\}. \quad (2)$$

Thus, the set $\{(0,x):x\in\overline{\mathsf{RM}}(1,m)\}$ is a subset of $\mathsf{RM}(1,m)$, so the property holds for $\overline{\mathsf{RM}}(1,m)$ as well.

Fact 2. The base case $m=3$ is well known, it corresponds to the Hamming code (Steane's code). The induction yields

$$\overline{G}_{m+1}\overline{G}_{m+1}^T=\begin{pmatrix}0 & \overline{G}_m\cdot\mathbf{1}^T\\ \mathbf{1}\cdot\overline{G}_m^T & 0\end{pmatrix}. \quad (3)$$

Noting that $\overline{G}_m\cdot\mathbf{1}^T$ is simply the vector of weights mod 2 of the rows of $\overline{G}_m$ and that these are even by Fact 1 proves Fact 2.

Fact 3. Since we are interested in the dual code, we should think of G_m as the parity check matrix of a code. The base case $m=2$ corresponds to the parity-check matrix

$$\overline{G}_2=\begin{pmatrix}1&0&1\\0&1&1\end{pmatrix}. \quad (4)$$

The minimum distance is obviously bounded by the length of the code $d\leq 3$. This parity-check matrix can uniquely identify any single bit error since all its columns are distinct, so it has minimum-distance 3. In its recursive definition Eq. (4, main text), $\overline{G}_{m+1}$ contains three blocks of bits: the first two of size 2^m-1 and the last of size 1. It is clear that the minimum distance for $m+1$ is no greater than the minimum distance for m, since an error occurring in the first block is only seen by $\overline{G}_m$. On the other hand, a single-bit error occurring in different blocks will trigger different syndrome patterns. If it is in block 1 its first m syndrome bits will be non-trivial and its last syndrome bit will be trivial. If it is in block 2 its first m syndrome bits will be non-trivial and its last syndrome bit will be non-trivial. If it is in block 3 its first m syndrome bits will be trivial and its last syndrome bit will be non-trivial. Moreover, in each case the syndrome can uniquely identify the error by induction, proving the fact.

Fact 4. To prove this fact it is important to know that for shortening, the row which is deleted from H_m is all 1s and that the subsequently deleted column is all 0s. The fact that H_m contains an all 1s row simply reflects the fact that elements of $\mathsf{RM}(1,m)$ have even weight for $m\geq 2$. The fact that the rest of the first column is all 0s can always be obtained by Gaussian elimination. By definition, $G_mH_m^T=0$, or in other words

$$\begin{pmatrix}1 & 1\ldots 1\\ 0 & \\ 0 & \overline{G}_m\\ 0 & \end{pmatrix}\begin{pmatrix}1 & 0\ldots 0\\ 1 & \\ 1 & \overline{H}_m^T\\ 1 & \end{pmatrix} \quad (5)$$

$$=\begin{pmatrix}0 & \overline{H}_m\cdot\mathbf{1}^T\\ \mathbf{1}\cdot\overline{H}_m^T & \overline{G}_m\overline{H}_m^T\end{pmatrix}=0. \quad (6)$$

Fact 5. First, we prove that $\mathrm{row}(G_m)\subset\mathrm{row}(H_m)$. This follows from the fact that $G_mG_m^T=0$, which we prove by induction:

$$G_{m+1}G_{m+1}^T=\begin{pmatrix}0 & G_m\cdot\mathbf{1}^T\\ \mathbf{1}\cdot G_m^T & 0\end{pmatrix}. \quad (7)$$

The r.h.s is 0 since rows of G_m have even weight from Fact 1. The fact follows from the observation that $\overline{G}_m$ and $\overline{H}_m$ are obtained from G_m and H_m by the same shortening procedure: first remove an all 1s row and then remove an all 0s column.

Fact 6: For this Fact it is convenient to define $\mathsf{RM}(1,m)$ as boolean polynomials with all terms of degree 1 [1]. Then, $x_1\cdot x_2\cdot\ldots x_p$ is a boolean polynomial with all terms of degree p, and these have weights $0 \mod 2^{m-p}$ [1].

Appendix B— In this appendix we discuss the generalization to higher rank Reed-Muller codes, defined recursively by [1]

$$\mathsf{RM}(r,m+1)= \quad (8)$$
$$\{(x,x+y):x\in\mathsf{RM}(r,m),y\in\mathsf{RM}(r-1,m)\}\,,$$

* David.Poulin@USherbrooke.ca

or equivalently by Eq. (12, main text).

Denote $G_{r,m}$ the generator matrix of $\mathsf{RM}(r,m)$. We choose a pair of codes $\mathsf{RM}(m-r-1,m)$ and $\mathsf{RM}(m-r,m+1)$ both of rates greater than $1/2$. Such codes contain their dual [1], so in particular the first code contains $\mathsf{RM}(r,m)$, which implies that $\mathsf{RM}(r,m)$ is self-orthogonal, and the same reasoning applies to $\mathsf{RM}(r,m+1)$. Since $\mathsf{RM}(m-r,m)$ has a rate greater than $\mathsf{RM}(m-r-1,m)$, it follows that $\mathsf{RM}(r-1,m)$ is also self-orthogonal. In short, we have just shown $G_{r,m}G_{r,m}^T = 0$, $G_{r-1,m}G_{r-1,m}^T = 0$, and $G_{r,m+1}G_{r,m+1}^T = 0$. This last equality combined to Eq. (12, main text) implies that $G_{r,m}G_{r-1,m}^T = 0$.

As a consequence of these orthogonality conditions, we can use the rows of $G_{r,m}$ to build a self-dual CSS code $\mathsf{QRM}(r,m)$. Similarly, we can build a self-dual CSS code $\mathcal{G}$ from the union of the rows of $\mathsf{RM}(r,m)$ and $\mathsf{RM}(r-1,m)$. The code $\mathcal{G}$ has minimum distance $\geq d_{r-1,m}$. There are many inequivalent ways of building subsystem codes from these, by converting some logical qubits into gauge qubits, by shortening the codes, and by adding additional stabilizers $\tilde{\mathcal{A}}_{r,m}$ or equivalently fixing the gauge in various ways. Below we briefly discuss one possible construction, which converts between two subsystem codes with stabilizers given by $\mathsf{QRM}(r,m)$ and $\mathsf{QRM}(r,m+1)$, and has minimum distance $d_{r,m} = 2^{m-r}$.

$m+1 \rightarrow m$ conversion: We begin in a subsystem code with stabilizers $\mathsf{QRM}(r,m+1)$. As of Eq. (12, main text), we can naturally partition the 2^{m+1} qubits into two blocks of 2^m qubits. We can measure the stabilizers of $\mathcal{G}$ on the second block, and correct any errors it reveals. This leaves the first block in the code $\mathsf{QRM}(r,m)$. The logical operators of $\mathsf{QRM}(r,m)$ acting on the first block are preserved by this procedure.

$m \rightarrow m+1$ conversion: We begin in the stabilizer code $\mathsf{QRM}(r,m)$. We append to the system a state ρ prepared in the code $\mathcal{G}$. The resulting state is stabilized by $\mathsf{QRM}(r,m+1)$. We can measure any additional stabilizers and use their associated pure errors to restore their $+1$ value in order to restore a given gauge. The logical operators of $\mathsf{QRM}(r,m)$ acting on the first block are preserved by this procedure provided that they do not conflict with the gauge choice.

Note that, while the conversion scheme presented here and in the main text are conceptually identical, the codes presented in the main text are not a special case of the quantum codes $\mathsf{QRM}(r,m)$ since these have not been punctured or shortened. It is an interesting open problem to study the various ways in which Reed-Muller codes can be punctured and shortened to produce quantum codes with interesting transversal gates and code parameters. We note for instance that applying the standard puncture and shortening procedure (remove the all-1 column and row) to $\mathsf{RM}(2,7)$ yields a $[[127,1,7]]$ quantum code with transversal T gate [2], which could be important for magic state distillation.

[1] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Publishing Company, 1977)

[2] The online encyclopedia of interer sequences http://oeis.org/a006006