Universal Fault-Tolerant Quantum Computation with Only Transversal Gates and Error Correction

Adam Paetznick[1] and Ben W. Reichardt[2]

[1]David R. Cheriton School of Computer Science and Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

[2]Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, California 90089, USA

(Received 13 April 2013; published 29 August 2013)

Transversal implementations of encoded unitary gates are highly desirable for fault-tolerant quantum computation. Though transversal gates alone cannot be computationally universal, they can be combined with specially distilled resource states in order to achieve universality. We show that "triorthogonal" stabilizer codes, introduced for state distillation by Bravyi and Haah [Phys. Rev. A **86**, 052329 (2012)], admit transversal implementation of the controlled-controlled-Z gate. We then construct a universal set of fault-tolerant gates without state distillation by using only transversal controlled-controlled-Z, transversal Hadamard, and fault-tolerant error correction. We also adapt the distillation procedure of Bravyi and Haah to Toffoli gates, improving on existing Toffoli distillation schemes.

DOI: 10.1103/PhysRevLett.111.090505 PACS numbers: 03.67.Pp, 03.67.Lx

Quantum computers are highly susceptible to noise. For protection, the data can be stored in a code [1,2], and encoded operations can be applied "fault tolerantly," in order to prevent a single error from spreading to multiple qubits in a codeword [3]. Between operations, fault-tolerant error correction keeps errors from accumulating. The simplest fault-tolerant operation is the application of physical gates transversally across the codewords, meaning that the jth gate is applied to the jth qubits of the codewords, for every j. Depending on the gate, this may or may not preserve the codespace and implement a valid encoded operation. Unfortunately, no quantum code admits transversal implementation of a universal set of encoded gates [4]. Instead, universality is usually achieved by combining some transversal gates with specially prepared resource states in a process known as state injection and distillation [5]. State distillation can be orders of magnitude more costly than direct transversal gates, and dominates the resource overhead for implementing a quantum computer [6,7].

Here we propose a way of implementing a universal set of quantum gates transversally, up to a correction that can be made by the standard error-correction procedure. In effect, our protocol shows that the impossibility theorem of Ref. [4] can be circumvented without adding any new machinery. Separate injection and distillation procedures are not required. The construction works only for the class of "triorthogonal" quantum stabilizer codes, introduced recently by Bravyi and Haah [8]. Therefore, implementing our construction directly may not reduce the overhead compared to using state distillation with more efficient codes that can tolerate higher noise rates. However, based on our construction, we derive a state-distillation procedure that, with realistic error parameters, reduces the overhead compared to previous state-of-the-art state distillation methods [9,10].

Our construction is based on two main insights. First, we observe that the controlled-controlled-Z operation [defined by $\mathrm{CCZ}|a, b, c\rangle = (-1)^{abc}|a, b, c\rangle$ for bits a, b, c] can be implemented transversally for any triorthogonal quantum code. Second, we show that the Hadamard $H = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)/\sqrt{2}$ can be implemented by transversal H gates followed by stabilizer measurements and Pauli X corrections. Together, H and CCZ are universal for quantum computation [11,12].

As an example, consider the [[15, 7, 3]] quantum Hamming code, which uses 15 qubits to protect seven encoded qubits to distance 3. The codespace is the simultaneous $+1$ eigenspace of the eight operators

$$IIIIIIIXXXXXXX, \quad IIIIIIIZZZZZZZ,$$
$$IIIXXXXIIIIXXXX, \quad IIIZZZZIIIIZZZZ,$$
$$IXXIIXXIIXXIIXX, \quad IZZIIZZIIZZIIZZ,$$
$$XIXIXIXIXIXIXI, \quad ZIZIZIZIZIZIZI,$$

each the tensor product of Pauli operators I, X, and Z. Choose a basis for this codespace so the logical X and Z operators on the first encoded qubit are transversal X and Z, respectively. Provided that the other six "gauge" qubits are prepared as encoded $|0^6\rangle$, the CCZ operation is transversal. Moreover, transversal H gates preserve the codespace and apply a logical H to the first encoded qubit. Transversal H corrupts the gauge qubits, but they can be restored to $|0^6\rangle$ by measuring the six corresponding logical Z operators and applying X corrections as necessary. Measurement of the gauge qubits' logical Z operators can be performed fault tolerantly using standard error-correction techniques [3,13].

In addition to allowing for universal quantum computation directly, our result also permits more efficient state

injection and distillation when nontriorthogonal codes are used for computation. Traditional injection and distillation procedures are used for fault tolerantly implementing the $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{smallmatrix}\right)$ gate. Recently, Eastin [9] and Jones [10,14] have shown that the cost of implementing a Toffoli gate can be reduced by distilling so-called Toffoli states rather than using fault-tolerant T gates. We observe that the distillation procedure of Ref. [8] for T gates can be adapted to Toffoli states in order to improve on the procedures of Eastin and Jones.

Let us begin by specifying the construction of stabilizer codes based on triorthogonal matrices. For two binary vectors $f, g \in \{0,1\}^n$, let $f \cdot g \in \{0,1\}^n$ be their entrywise product, and let $|f|$ denote the Hamming weight of f. Call an $m \times n$ binary matrix G, with rows $f_1, \ldots, f_m \in \{0,1\}^n$, triorthogonal if

$$|f_i \cdot f_j| = 0 \pmod 2 \quad \text{and} \quad |f_i \cdot f_j \cdot f_k| = 0 \pmod 2$$

for all pairs (i, j) and triples (i, j, k) of distinct indices.

An $m \times n$ triorthogonal matrix G can be used to construct an n-qubit, triorthogonal, stabilizer code as follows [8]. For each even-weight row of G, add a stabilizer by mapping nonzero entries to X operators, e.g., $(1,0,1) \mapsto X \otimes I \otimes X$. Add a stabilizer for each row of the orthogonal complement $G^\perp$ by similarly mapping nonzero entries to Z operators. The logical X and Z operators are then given by mapping nonzero entries of the odd-weight rows of G to X and Z, respectively.

For example, fixing the six gauge qubits of the 15-qubit Hamming code to $|0^6\rangle$ gives a [[15, 1, 3]] triorthogonal code [15]. Bravyi and Haah have constructed a [[49, 1, 5]] and a family of $[[3k+8, k, 2]]$ triorthogonal codes [8].

We next construct a fault-tolerant Toffoli gate for a triorthogonal code. Shown in Fig. 1, the Toffoli gate is equivalent to a CCZ gate in which the target qubit is conjugated by Hadamard gates.

The main component of the construction is an implementation of an encoded CCZ gate. We claim that for any triorthogonal code, transversal application of CCZ gates realizes CCZ gates on the encoded qubits. For simplicity consider the case of a triorthogonal code with a single encoded qubit, i.e., based on a triorthogonal matrix G with a single odd-weight row $f_\star$. (The argument with multiple encoded qubits is fully analogous.) Let $\mathcal{G}_0 \subseteq \{0,1\}^n$ be the linear span of all the even-weight rows of G and let $\mathcal{G}_1$ be the coset $\{f_\star + g : g \in \mathcal{G}_0\}$. Then the

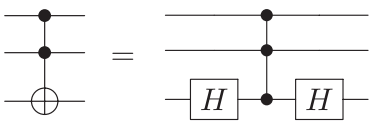

FIG. 1. The Toffoli gate is equivalent to a CCZ gate in which the target qubit is conjugated by Hadamard gates.

encoding of $|a\rangle$, for $a \in \{0,1\}$, is given by the uniform superposition over $\mathcal{G}_a$: $|\bar{a}\rangle = \sum_{g \in \mathcal{G}_a} |g\rangle / \sqrt{|\mathcal{G}_a|}$.

The action of transversal CCZ gates on an encoded basis state $|\overline{a,b,c}\rangle$, for $a, b, c \in \{0,1\}$ is therefore given by

$$\begin{aligned} \mathrm{CCZ}^{\otimes n} |\overline{a,b,c}\rangle &= \sum_{g \in \mathcal{G}_a, h \in \mathcal{G}_b, i \in \mathcal{G}_c} \mathrm{CCZ}^{\otimes n} |g,h,i\rangle \\ &= \sum_{g \in \mathcal{G}_a, h \in \mathcal{G}_b, i \in \mathcal{G}_c} (-1)^{|g \cdot h \cdot i|} |g,h,i\rangle. \end{aligned} \quad (1)$$

Here $g \cdot h \cdot i$ can be expanded as $(af_\star + g') \cdot (bf_\star + h') \cdot (cf_\star + i')$, where $g', h', i' \in \mathcal{G}_0$. Expanding further gives one term $abc(f_\star \cdot f_\star \cdot f_\star) = abcf_\star$, plus other triple product terms in which $f_\star$ appears at most twice. Since G is triorthogonal, these other terms necessarily have even weight. The term $abcf_\star$ has odd weight if and only if $a = b = c = 1$. Substituting back into Eq. (1), as desired,

$$\mathrm{CCZ}^{\otimes n} |\overline{a,b,c}\rangle = (-1)^{abc} |\overline{a,b,c}\rangle. \quad (2)$$

To complete the Toffoli construction, we also require a fault-tolerant implementation of the Hadamard H. For H to be transversal, the code must be self-dual, i.e., $\mathcal{G}_0 = G^\perp$. Unfortunately, no triorthogonal code is self-dual. Indeed, otherwise, since CCZ is transversal it would be possible obtain a transversal implementation of Toffoli and H for the same code. However, Toffoli and H together are universal [11,12], and it is known that universality cannot be achieved by transversal gates alone [4] (see also Refs. [16,17]).

Nonetheless, compact and fault-tolerant implementations of logical H are still possible. When transversal H is performed on a triorthogonal code, the logical operators are transformed properly: logical X maps to logical Z and vice versa. A subset of the stabilizers is preserved: observe that $\mathcal{G}_0 \subset G^\perp$, and thus each element of $\mathcal{G}_0$ corresponds to both X and Z stabilizers, which transversal H swaps. Transversal H does not preserve the Z stabilizers corresponding to $G^\perp \setminus \mathcal{G}_0$, so these must be restored by measuring and correcting them. In the [[15, 7, 3]] example above, this involved measuring the six gauge qubits' logical Z operators.

The Z stabilizers of $G^\perp \setminus \mathcal{G}_0$ can be restored during an X error-correction procedure. Steane's procedure, for example, involves a transversal CNOT from the data to an encoded $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ "ancilla" state [13,18]. The transversal CNOT implements encoded CNOT and has the effect of copying the unwanted X stabilizers onto the ancilla, and copying the desired Z stabilizers from the ancilla to the data. Transversal Z-basis measurements of the ancilla then permit correcting X errors on the data, while simultaneously restoring the stabilizer group. (Once again, in the [[15, 7, 3]] example, the ancilla's gauge qubits are prepared in $|0^6\rangle$. Each is measured as 0 or 1, with a correction required in the latter case.) See Fig. 2. Alternatively, Shor's error-correction procedure uses a

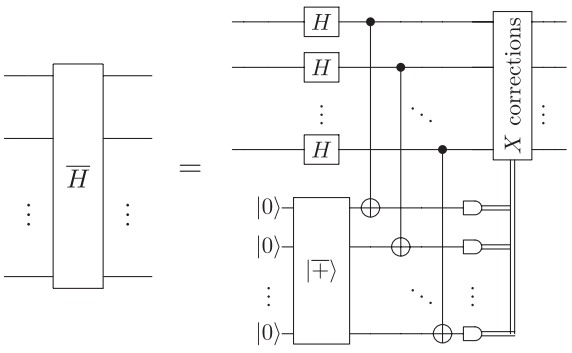

FIG. 2. An implementation of the logical Hadamard operation in a triorthogonal code. Transversal Hadamard gates are applied to the data block. In order to restore the data to the codespace, and also correct any X errors, an encoded $|+\rangle$ state is prepared, coupled to the data with transversal CNOT gates and measured. X corrections are applied as necessary.

separate GHZ state $(|00\ldots0\rangle + |11\ldots1\rangle)/\sqrt{2}$ for each stabilizer to be measured [3]. In either case, the required stabilizers can be measured and corrected using H, X, CNOT, $|0\rangle$ preparation and Z-basis measurements. By using CCZ gates to simulate CNOT and X, the entire Toffoli requires only H and CCZ gates.

Importantly, even with additional X corrections to fix the Z stabilizers of $G^{\perp} \setminus \mathcal{G}_0$, the X error-correction procedure is fault tolerant. That is, k gate failures can lead to a data error of weight at most k, for k less than half the code's distance d. Indeed, d is the minimum of the code's distance d_Z against Z errors (determined by the X stabilizers of $\mathcal{G}_0$) and its distance d_X against X errors (determined by the Z stabilizers of $G^{\perp}$), and since $\mathcal{G}_0 \subset G^{\perp}$, $d_Z \leq d_X$. Thus any X error of weight less than $d/2$ can be corrected using only the Z stabilizers of $\mathcal{G}_0$, and the Z stabilizers of $G^{\perp} \setminus \mathcal{G}_0$ can be corrected separately. Indeed, the Hadamard construction of Fig. 2 works for any CSS code in which the X and Z logical operators have identical supports and transversal Hadamard conjugates the X stabilizers to a subset of the Z stabilizers.

The simplest way to use the Toffoli construction above is with a concatenated triorthogonal code. A universal set of fault-tolerant operations can be constructed from only CCZ and H gates. Thus using triorthogonal codes for computation could be useful for circuits that contain large numbers of Toffoli gates. One could also imagine using multiple codes for computation by, for example, teleporting into the code best suited for each logical operation. In this setting, a triorthogonal code could be used to implement efficiently the CCZ operation.

Our construction allows for quantum computation to arbitrary accuracy, so long as the error rate per physical gate is below a constant "threshold" value [19,20]. Threshold error rates for triorthogonal codes are largely unknown, though estimates for the [[15, 1, 3]] code are roughly 0.01 percent per gate [21]. If the CCZ operation is constructed from a sequence of one- and two-qubit gates, then the threshold is likely lower. Since resource overhead increases rapidly as the physical noise rate approaches threshold, our construction is likely to be outperformed by schemes based on other codes, for which the threshold can be nearly one percent or higher (see, e.g., Refs. [6,22,23]). The existence of high-performing triorthogonal codes is not out of the question, however.

A more conventional way to achieve universality is through state injection and distillation. Bravyi and Haah have proposed distillation procedures using triorthogonal codes that permit fault-tolerant implementation of the T gate [8]. Our result implies that a similar procedure could be used to implement Toffoli gates.

The Toffoli state is defined by the output of the Toffoli gate on input $|+, +, 0\rangle$, where the third qubit is the target. A Toffoli state can be used to implement the CCZ gate as shown in Fig. 3. Distillation with a $[[3k + 8, k, 2]]$ triorthogonal code uses $3k + 8$ transversal CCZ gates with error rate p to produce k Toffoli states with error rate $(3k + 1)p^2$, to leading order in p. See Fig. 4. The CCZ gates in the distillation circuit can be implemented recursively, or by using an existing Toffoli distillation procedure [9,10,14]. Note that the Hadamard gates are performed after decoding and thus the circuit in Fig. 2 is not required. For simplicity, Clifford operations including encoding and decoding operations are assumed to be perfect.

The distillation procedure given by Fig. 4 can reduce the cost of implementing a Toffoli gate. Suppose we wish to implement a Toffoli gate with error below 10^{-13}. The procedure of Ref. [10] consumes eight T gates with error p to produce a Toffoli state with error $28p^2$. The T gates can be implemented using a combination of protocols; Table I of Ref. [24] lists optimal protocol combinations for a large range of target error rates. If physical T gates can be performed with error at most 10^{-2}, then using the Toffoli construction of Ref. [10], as given, requires on average 540.16 T gates.

Alternatively, we could use a $[[3k + 8, k, 2]]$ triorthogonal code for distillation at the top level, and use Toffoli states from Ref. [10] as input to implement the CCZ gates

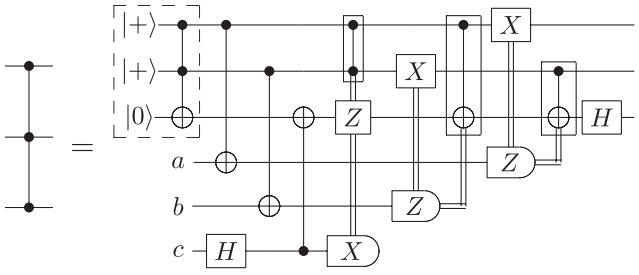

FIG. 3. A CCZ gate can be implemented by consuming a single Toffoli state [26]. The input qubits are teleported into the Toffoli state (enclosed by the dashed line) with Clifford corrections conditioned on the measurement outcomes.

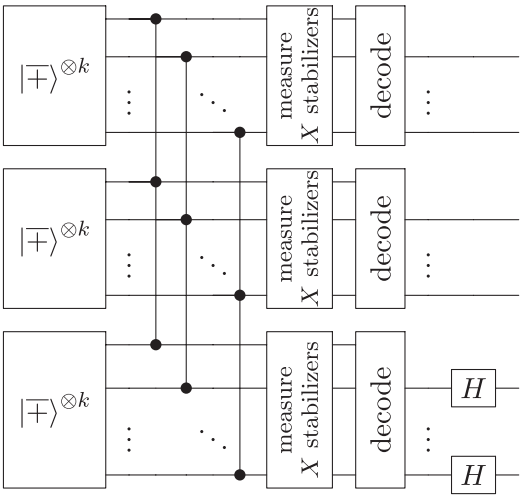

FIG. 4. A Toffoli state distillation circuit using a triorthogonal code encoding k qubits. Three separate blocks are encoded into the state $|+\rangle^{\otimes k}$ and then transversal CCZ gates are applied. Conditioned on detecting no errors, each block is decoded and Hadamard gates are applied to each of the target qubits, yielding k Toffoli states.

in Fig. 4. The distillation circuit fails to detect a faulty Toffoli state input only if the number of errors on each triorthogonal code block is even. To leading order, this occurs only if a pair of input Toffoli states contain identical errors. Each of the seven possible errors on the output of states from Ref. [10] is equally likely. Thus, if the input Toffoli states have error p_1, then to leading order the failure probability of the triorthogonal protocol is given by

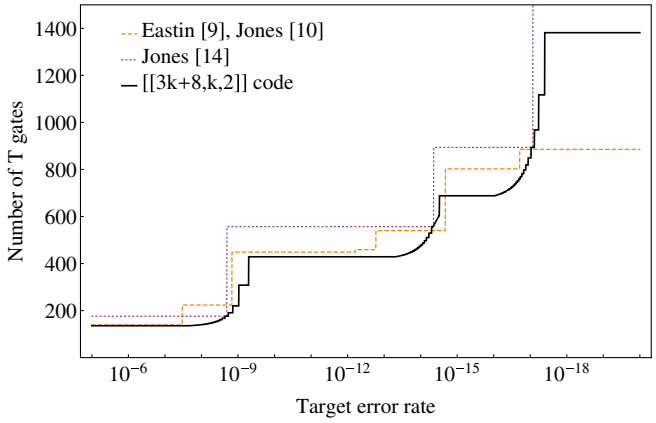

FIG. 5 (color online). The average number of physical T gates required for three different Toffoli state distillation protocols. For the previous protocols of Refs. [9,10,14], input T gates are first distilled to the appropriate fidelity according to Table I of Ref. [24]. The solid black line shows the cost of our protocol for $[[3k+8, k, 2]]$ triorthogonal codes where an even integer $2 \leq k \leq 100$ has been optimally selected at each target error rate. Input CCZ gates to the triorthogonal protocol are produced using Ref. [10]. Physical T gates are assumed to have error at most 10^{-2}. Detailed calculations are provided as Supplementary Material [27].

$7(3k+1)(p_1/7)^2$. For $k = 100$, this yields an average T-gate cost of 428.7, a savings of 25% over Ref. [10] alone. Calculations for a range of target error rates are shown in Fig. 5.

The T gate cost alone is an incomplete measure of the overhead. Indeed, Fig. 5 shows that the double error-detecting protocol of Ref. [14] usually has a higher T gate cost than the single error-detecting protocol. However, the double error-detecting protocol can still yield significant savings since smaller code distances may be used for Clifford gates in intermediate distillation levels [7,10,14]. Our protocol similarly allows for reduced Clifford gate costs and offers the flexibility to be used recursively or on top of any other Toffoli state distillation protocol, including those of Refs. [9,10,14]. Complete overhead calculations depend on architectural considerations.

Finally, we note that if the orthogonality conditions on the matrix G are increased, then additional types of diagonal operations are transversal. If G satisfies the condition that all j-tuple products have weight (0 mod 2) for all $2 \leq j \leq h$, then the h-fold controlled-Z gate is transversal in the corresponding stabilizer code. This observation is similar to a result of Landahl and Cesare, who demonstrated that codes satisfying increasingly stringent conditions on weights of the codewords admit transversal Z-axis rotations of increasing powers of $1/2^k$ [25].

The authors would like to thank Cody Jones for helpful feedback. This work was supported by ARO Grant No. W911NF-12-1-0541, NSF Grant No. CCF-1254119, and by the Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center Contract No. D11PC20166. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of IARPA, DoI/NBC, or the U.S. Government.

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[2] D. Gottesman, Ph.D. thesis, California Institute of Technology [arXiv:quant-ph/9705052].
[3] P. W. Shor, *FOCS'96 Proceedings of 37th IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, DC, 1996), pp. 56–65.
[4] B. Eastin and E. Knill, Phys. Rev. Lett. **102**, 110502 (2009).
[5] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[6] R. Raussendorf and J. Harrington, Phys. Rev. Lett. **98**, 190504 (2007).
[7] A. G. Fowler, S. J. Devitt, and C. Jones, Sci. Rep. **3**, 1939 (2013).
[8] S. Bravyi and J. Haah, Phys. Rev. A **86**, 052329 (2012).
[9] B. Eastin, Phys. Rev. A **87**, 032321 (2013).

[10] C. Jones, Phys. Rev. A **87**, 022328 (2013).
[11] Y. Shi, Quantum Inf. Comput. **3**, 84 (2003).
[12] D. Aharonov, arXiv:quant-ph/0301040.
[13] A. M. Steane, Phys. Rev. Lett. **78**, 2252 (1997).
[14] C. Jones, Phys. Rev. A **87**, 052334 (2013).
[15] E. Knill, R. Laflamme, and W. H. Zurek, arXiv:quant-ph/9610011.
[16] B. Zeng, A. W. Cross, and I. L. Chuang, IEEE Trans. Inf. Theory **57**, 6272 (2011).
[17] X. Chen, H. Chung, A. W. Cross, B. Zeng, and I. L. Chuang, Phys. Rev. A **78**, 012353 (2008).
[18] A. M. Steane, arXiv:quant-ph/0202036.
[19] D. Aharonov and M. Ben-Or, *STOC'97 29th Annual Symposium on Theory of Computing, El Paso, TX, 1997* (ACM New York, NY, 1997), p. 176.
[20] P. Aliferis, D. Gottesman, and J. Preskill, Quantum Inf. Comput. **6**, 97 (2006).
[21] A. W. Cross, D. P. DiVincenzo, and B. Terhal, Quantum Inf. Comput. **9**, 541 (2009).
[22] E. Knill, Nature (London) **434**, 39 (2005).
[23] D. S. Wang, A. G. Fowler, and L. C. L. Hollenberg, Phys. Rev. A **83**, 020302 (2011).
[24] C. Jones, Phys. Rev. A **87**, 042305 (2013).
[25] A. J. Landahl and C. Cesare, arXiv:1302.3240.
[26] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[27] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.111.090505 for detailed overhead calculations.