CO 639 — Quantum Error Correcting Codes
Fault tolerant, universal quantum operations

Scribe: Niel de Beaudrap
Edited by Daniel Gottesman

February 19, 2004

1 Basic Definitions & Results

Recall the definition of a universal set of gates:

Definition 1. A *universal set* of quantum gates is a set which generates a group of operations which is dense in the group of unitary operations on any Hilbert space.

The denseness criterion is sufficient for practical purposes: we don't care about exact unitary operations (an unrealistic goal at any rate) so long as we can at least approximate any unitary operation to arbitrary finite precision.

Theorem 1 (Rains, Solovay). *The Clifford group, together with any gate not from the Clifford group, is universal for quantum computation.*

Although contained in the above theorem, the following sets of gates in particular are more easily proven to be universal for quantum computation:

- Clifford group, along with the Toffoli gate
- Clifford group, along with the $\frac{\pi}{8}$ gate
- Clifford group, along with the controlled-$\frac{\pi}{4}$ gate

Being able to approximate operations with arbitrary precision is important, but also important is the amount of effort to achieve the desired precision. The following Theorem provides us with a reason to consider this model of computing realistic.

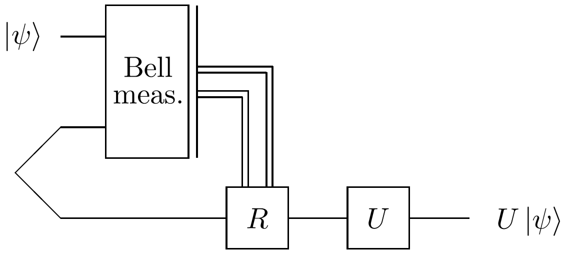
Theorem 2 (Solovay, Kitaev). *For any universal set of gates S, we can approximate an arbitrary unitary operation U over a Hilbert space $\mathcal{H}$ of fixed dimension (≥ 2) to precision $\varepsilon > 0$, using* $\operatorname{poly}(\log \varepsilon)$ *gates from S.*

2 Using teleportation for universal computation

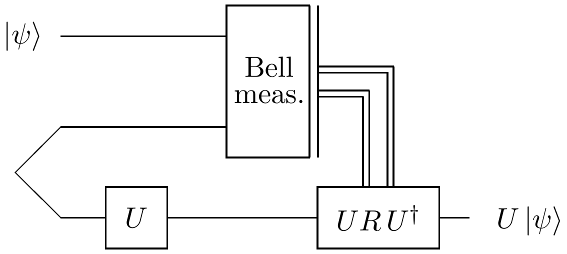
Although it is often considered a sort of communication protocol rather than a quantum operation, teleportation can be used as a tool for computation in conjunction with specially prepared states. In the context of fault-tolerant computation, this idea comes in useful.

2.1 Clifford group operations

Suppose that we want to perform a Clifford group operation U to some qubit state. Teleporting the state between the input and the point where we perform the gate U doesn't affect the overall operation, so we might perform this operation with the following circuit:



(Here, the R operation is some Pauli operation controlled classically by the result of the Bell measurement.) We don't have to perform the U operation after the teleportation: we could pull the U operation past the Pauli operation R, and arrive at the following modified circuit:



Now, as U is a Clifford gate, then $URU^\dagger$ is in the Pauli group. Then, if we can create the input state $(I \otimes U)|\Phi^+\rangle$, we could perform U on arbitrary quantum states via teleportation. The advantage of this approach is that the preparation of such states $(I \otimes U)|\Phi^+\rangle$ could be done "offline" by building a reserve supply for future use.

Note that the stabilizer of the state $(I \otimes U)|\Phi^+\rangle$ is generated by the two operators

$$X \otimes UXU^\dagger$$
$$Z \otimes UZU^\dagger\,,$$

and because U is a Clifford group operation, these are Pauli operations as well. Then, using Pauli measurements, we can easily create the state $(I \otimes U)|\Phi^+\rangle$.

What we see here is that Clifford group operations can be simulated using Pauli operations and Pauli measurements. (The Bell basis measurement in the teleportation, of course, can also be performed using Pauli measurements.) Then, if we perform the Pauli operations and measurements fault-tolerantly, we can perform all Clifford group operations fault-tolerantly as well. Since we can perform logical Pauli operations and measurements for any stabilizer code, this shows that we have a fault-tolerant construction of the Clifford group for any stabilizer code.

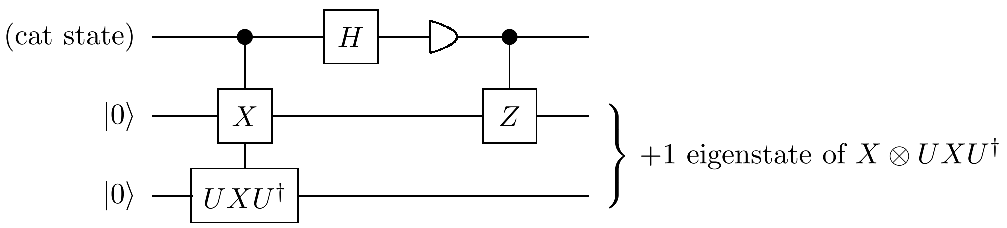
2.2 Moving beyond the Clifford Group

Next, let's consider what happens when we use a gate such as the $\frac{\pi}{8}$ gate instead of a Clifford operation for U. The $\frac{\pi}{8}$ gate transforms the Pauli operations as follows:

$$\begin{aligned} UZU^\dagger &= Z \\ UXU^\dagger &= \mathrm{e}^{i\pi/4} X P^\dagger_{\pi/2} \\ UYU^\dagger &= \mathrm{e}^{i\pi/4} Y P^\dagger_{\pi/2} \end{aligned}$$

What we see here is that U now conjugates the Pauli group into the Clifford group. Then, the modified teleportation circuit involves Clifford group operations — which we already know we can perform fault-tolerantly. Then, the problem of performing the $\frac{\pi}{8}$ gate U fault-tolerantly has been reduced to creating the state $(I \otimes U)\,|\Phi^+\rangle$.

Once more, we can consider this state as the $+1$ eigenvalue of a stabilizer generated by $X \otimes UXU^\dagger$ and $Z \otimes UZU^\dagger$. One circuit to do this would just be as follows:



The operation performed by all but the last operation is effectively an $X \otimes UXU^\dagger$ measurement. In order to be able to perform this fault-tolerantly, we need to be able to perform fault-tolerant controlled operations for Clifford group gates. So far, we only know how to perform Clifford group operations fault-tolerantly, not controlled operations. We can, however, do the controlled operation when the control register is a cat state: If the transversal implementation of the Clifford group gate is $C^{\otimes n}$, for instance, the controlled Clifford group gate is just controlled-C from each qubit of the cat state to the corresponding qubit of the code register. Then either C is performed on none of the qubits in the code block (when the cat state is all $|0\rangle$) or on all of them (when the cat state is all $|1\rangle$). The controlled-Z operation at the end is to "steer" the measured state into the $+1$ eigenstate of the measurement.

We can perform a similar operation in order to project this into the $+1$ eigenspace of $Z \otimes UZU^\dagger$ (using a controlled-not gate to steer the state into the appropriate eigenspace). Using this circuit, then, we can prepare $(I \otimes U)\,|\Phi^+\rangle$ fault-tolerantly, and thereby perform the $\frac{\pi}{8}$ gate fault-tolerantly.

2.3 Boot-strapping

We can use the technique we've been describing above to boot-strap our way to universal fault-tolerant computation, using teleportation. On a Hilbert space $\mathcal{H}$, we can define an infinite sequence of gate-families in terms of commutation relations, with the Pauli group at the base:

$$\begin{aligned} \mathcal{C}_1(\mathcal{H}) &= \text{Pauli group on } \mathcal{H} \\ \mathcal{C}_{k+1}(\mathcal{H}) &= \left\{ U \in \mathcal{U}(\mathcal{H}) \;\middle|\; U\mathcal{C}_1 U^\dagger \subseteq \mathcal{C}_k \right\} \end{aligned}$$

From this definition, the Clifford group would be equal to $\mathcal{C}_2(\mathcal{H})$, and the Toffoli and $\frac{\pi}{8}$ gates are in $\mathcal{C}_3(\mathcal{H})$.

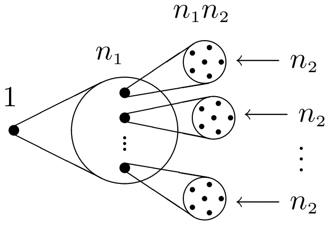
Note that these sets $\mathcal{C}_k$ need not be groups. In particular, the $\frac{\pi}{8}$ gate cannot be generated exactly by the Clifford group and the Toffoli operation, although these are all operations in $\mathcal{C}_3$. Also, note that $\mathcal{C}_3$ is universal for quantum computation, and therefore generates an infinite group, while $\mathcal{C}_3$ itself is finite.

If we let $\mathcal{H}$ be the Hilbert space of n qubits, we can prove by the teleportation construction that you can perform operations in $\mathcal{C}_{k+1}(\mathcal{H})$, provided that you can perform operations and measurements of operations in $\mathcal{C}_k(\mathcal{H})$. We have also seen that by performing operations in $\mathcal{C}_k(\mathcal{H})$, Pauli measurements, and performing operations such as the controlled-Z and controlled-not gates, we can perform measurements in $\mathcal{C}_k(\mathcal{H})$ as well. Then, by induction, we can prove that Pauli operations, measurements, and the controlled-not and controlled-Z operations are sufficient to perform universal fault-tolerant quantum computation.

3 Composing error correction codes

Is this a winning game? Can we perform fault-tolerant computation, reducing errors so that they have an arbitrarily small effect on our computations? The answer is yes — provided that the error rate on the physical qubits is low enough, we can make it arbitrarily low on the encoded qubits.

Take two codes, $[\![n_1\,, 1\,, k_1]\!]$ and $[\![n_2\,, 1, k_2]\!]$, and concatenate them.



If d_2 erasure errors occur in each of d_1 different blocks, we can cause errors in each of the sub-blocks that the second code can't correct. Then, these will act as d_1 errors in the second level code. Depending on the particular encoded error that occurs, the first code may actually be able to detect and correct this error: although the first code cannot correct *all* errors of weight d_1 , it may be able to correct *some* . What is clear, though, is that if fewer than d_1d_2 erasure errors occur, then fewer than d_1 blocks have at least d_2 erasure errors in them; then, performing the lower-level error correction, fewer than d_1 blocks will have encoded errors in them, so the higher-level error correction will fix all of the errors that occurred. Then, the composite code will have distance at least d_1d_2 .

Some examples:

- Composing the 5-qubit code with itself will yield a $[\![25, 1, 9]\!]$ qubit code. If we use the usual description for the 5-qubit code,

$$\begin{aligned} S_1 &= X \otimes Z \otimes Z \otimes X \otimes I \\ S_2 &= I \otimes X \otimes Z \otimes Z \otimes X \\ S_3 &= X \otimes I \otimes X \otimes Z \otimes Z \\ S_4 &= Z \otimes X \otimes I \otimes X \otimes Z \\ \overline{X} = \tilde{X} &= X \otimes X \otimes X \otimes X \otimes X \\ \overline{Z} = \tilde{Z} &= Z \otimes Z \otimes Z \otimes Z \otimes Z \end{aligned}$$

Then the stabilizer for the composite code is given by

$$\begin{array}{ccccccccc} \tilde{X} & \otimes & \tilde{Z} & \otimes & \tilde{Z} & \otimes & \tilde{X} & \otimes & I^{\otimes 5} \\ I^{\otimes 5} & \otimes & \tilde{X} & \otimes & \tilde{Z} & \otimes & \tilde{Z} & \otimes & \tilde{X} \\ \tilde{X} & \otimes & I^{\otimes 5} & \otimes & \tilde{X} & \otimes & \tilde{Z} & \otimes & \tilde{Z} \\ \tilde{Z} & \otimes & \tilde{X} & \otimes & I^{\otimes 5} & \otimes & \tilde{X} & \otimes & \tilde{Z} \end{array}$$

which corrects all of the encoded errors, as well as

$$\begin{array}{ccccccccc} S_1 & \otimes & I^{\otimes 5} & \otimes & I^{\otimes 5} & \otimes & I^{\otimes 5} & \otimes & I^{\otimes 5} \\ I^{\otimes 5} & \otimes & S_1 & \otimes & I^{\otimes 5} & \otimes & I^{\otimes 5} & \otimes & I^{\otimes 5} \\ & & & & \vdots & & & & \\ S_2 & \otimes & I^{\otimes 5} & \otimes & I^{\otimes 5} & \otimes & I^{\otimes 5} & \otimes & I^{\otimes 5} \\ I^{\otimes 5} & \otimes & S_2 & \otimes & I^{\otimes 5} & \otimes & I^{\otimes 5} & \otimes & I^{\otimes 5} \\ & & & & \vdots & & & & \\ & & & & \&c & & & & \end{array}$$

which corrects errors in individual blocks of the code. The encoded operations for this code will clearly be $\overline{X} = \tilde{X}^{\otimes 5}$ and $\overline{Z} = \tilde{X}^{\otimes 5}$.

- Composing the 7-qubit code with itself k times will yield a $[\![7^k, 1, 3^k]\!]$ code.