Fault Tolerant Quantum Computation (Notes)

Physics of Classical and Quantum Information

1st Semester 2015/16

JAGANATH PRASAD MOHANTY, Reg. Number: 82909, ist424046

Quantum state transformation of the three qubit Toffoli Gate using fault tolerant circuit

We construct one of the transformation of gates for error recovery in a fault tolerant quantum computation procedure, following the work by Peter Shor [1] considering set of three gates- rotations around the x-axis and the z-axis by $\pi/2$, and Toffoli gates – as a universal set of gates sufficient for quantum computation.

In this note, we have shown a construction of a single stage of our Toffoli gate fault tolerantly using a set of ancillary quantum bits (in a encoded state), which uses only linear operations and $\pi/2$ rotations on encoded qubits.

The Toffoli gate is a three-qubit gate, as follows:

$$
\begin{aligned}
|000\rangle &\rightarrow |000\rangle \\
|001\rangle &\rightarrow |001\rangle \\
|010\rangle &\rightarrow |010\rangle \\
|011\rangle &\rightarrow |011\rangle \\
|100\rangle &\rightarrow |100\rangle \\
|101\rangle &\rightarrow |101\rangle \\
|110\rangle &\rightarrow |111\rangle \\
|111\rangle &\rightarrow |110\rangle
\end{aligned} \qquad (1)
$$

This gate is a reversible classical gate which is universal for classical computation.

Using the ancillary state

Suppose we had an ancillary set of qubits known to be in the encoded state $|A\rangle$ as shown:

$$|A\rangle = \tfrac{1}{2}(|s_0\, s_0\, s_0\rangle + |s_0\, s_1\, s_0\rangle + |s_1\, s_0\, s_0\rangle + |s_1 s_1 s_1\rangle)$$

Then we build a gate that transforms two encoded qubits to three encoded qubits, with the third bit is a 1, if and only if the first two are both 1's, and 0 otherwise.

$$
\begin{aligned}
|s_0\, s_0\rangle &\rightarrow |s_0\, s_0\, s_0\rangle \\
|s_0\, s_1\rangle &\rightarrow |s_0\, s_1\, s_0\rangle \\
|s_1 s_0\rangle &\rightarrow |s_1\, s_0\, s_0\rangle \\
|s_1\, s_1\rangle &\rightarrow |s_1\, s_1\, s_1\rangle
\end{aligned} \qquad (2)
$$

Further we append the ancilla $|A\rangle$ to the first two qubits, and then XOR the third qubit into the first, and the fourth qubit into the second, which produces the following transformation

$$
\begin{aligned}
|s_0\, s_0\rangle\ |A\rangle &\rightarrow \tfrac{1}{2}(|s_0\, s_0\, s_0 s_0 s_0\rangle + |s_0 s_1 s_0 s_1 s_0\rangle + |s_1 s_0 s_1 s_0\, s_0\rangle + |s_1 s_1 s_1 s_1 s_1\rangle) \\
|s_0\, s_1\rangle\ |A\rangle &\rightarrow \tfrac{1}{2}(|s_0 s_1 s_0 s_0 s_0\rangle + |s_0 s_0 s_0 s_1 s_0\rangle + |s_1 s_1 s_1\, s_0\, s_0\rangle + |s_1 s_0 s_1 s_1 s_1\rangle) \\
|s_1 s_0\rangle\ |A\rangle &\rightarrow \tfrac{1}{2}(|s_1 s_0\, s_0 s_0\, s_0\rangle + |s_1 s_1 s_0 s_1 s_0\rangle + |s_0 s_0 s_1 s_0 s_0\rangle + |s_0 s_1 s_1 s_1 s_1\rangle) \\
|s_1 s_1\rangle\ |A\rangle &\rightarrow \tfrac{1}{2}(|s_1 s_1 s_0 s_0 s_0\rangle + |s_1 s_0 s_0 s_1 s_0\rangle + |s_0 s_1 s_1 s_0 s_0\rangle + |s_0 s_0 s_1 s_1 s_1\rangle)
\end{aligned} \qquad (3)
$$

This is where we do the measurement on the first two encoded qubits. If we trace the elements of the superposition where the first and second encoded qubits are both 0, we get the transformation shown by (1). If we trace $|s_0 s_1\rangle$ as the first and second encoded qubits, and pull out the relevant elements in the superposition we have the following

$$
\begin{aligned}
|s_0 s_0\rangle &\rightarrow |s_0 s_1 s_0\rangle \\
|s_0 s_1\rangle &\rightarrow |s_0 s_0 s_0\rangle \\
|s_1 s_0\rangle &\rightarrow |s_1 s_1 s_1\rangle \\
|s_1 s_1\rangle &\rightarrow |s_1 s_0 s_0\rangle
\end{aligned} \qquad (4)
$$

This transformation can be converted to the one we wnat by first appllying a controlled NOT from the first qubit to the third qubit, and then applying a NOT to the second qubit. On doing this we get the following

$$
\begin{aligned}
|s_0\, s_0\rangle &\rightarrow |s_0\, s_1 s_0\rangle \rightarrow |s_0 s_1 s_0\rangle \rightarrow |s_0 s_0 s_0\rangle \\
|s_0\, s_1\rangle &\rightarrow |s_0\, s_0 s_0\rangle \rightarrow |s_0 s_0 s_0\rangle \rightarrow |s_0 s_1 s_0\rangle \\
|s_1 s_0\rangle &\rightarrow |s_1\, s_1 s_1\rangle \rightarrow |s_1 s_1 s_0\rangle \rightarrow |s_1 s_0 s_0\rangle \\
|s_1 s_1\rangle &\rightarrow |s_1\, s_0 s_0\rangle \rightarrow |s_1 s_0 s_1\rangle \rightarrow |s_1 s_1 s_1\rangle
\end{aligned} \qquad (5)
$$

Similarly, tracing other two cases (observing $|s_1 s_0\rangle$ or $|s_1 s_1\rangle$) can be corrected by linear operations to the required gate.

Moreover to get the complete Toffoli gate on three qubits, as in equation (1), we can do the following transformation. We start by applying transformation explained in equation (1) to the first two qubit. Next we apply a controlled NOT from our original third qubit (fourth one shown below) to the newly introduced qubit (third one). Finally $|s_0\rangle \rightarrow (1/\sqrt{2})\,(|s_0\rangle + |s_1\rangle)$, and $|s_1\rangle \rightarrow (1/\sqrt{2})\,(|s_0\rangle - |s_1\rangle)$ is applied to the original third qubit (represented in fourth place below), which gives the depicted transformation

$$
\begin{aligned}
|s_0 s_0 s_0\rangle &\rightarrow (1/\sqrt{2})\,|s_0 s_0 s_0\rangle\,(|s_0\rangle + |s_1\rangle) \\
|s_0 s_1 s_0\rangle &\rightarrow (1/\sqrt{2})\,|s_0 s_1 s_0\rangle\,(|s_0\rangle + |s_1\rangle) \\
|s_1 s_0 s_0\rangle &\rightarrow (1/\sqrt{2})\,|s_1 s_0 s_0\rangle\,(|s_0\rangle + |s_1\rangle) \\
|s_1 s_1 s_0\rangle &\rightarrow (1/\sqrt{2})\,|s_1 s_1 s_1\rangle\,(|s_0\rangle + |s_1\rangle) \\
|s_0 s_0 s_1\rangle &\rightarrow (1/\sqrt{2})\,|s_0 s_0 s_1\rangle\,(|s_0\rangle - |s_1\rangle) \\
|s_0 s_1 s_1\rangle &\rightarrow (1/\sqrt{2})\,|s_0 s_1 s_1\rangle\,(|s_0\rangle - |s_1\rangle) \\
|s_1 s_0\, s_1\rangle &\rightarrow (1/\sqrt{2})\,|s_1 s_0 s_1\rangle\,(|s_0\rangle - |s_1\rangle) \\
|s_1 s_1 s_1\rangle &\rightarrow (1/\sqrt{2})\,|s_1 s_1 s_0\rangle\,(|s_0\rangle - |s_1\rangle)
\end{aligned} \qquad (6)
$$

On observing the fourth qubit in the above expression, we can see the Toffoli gate being approximated. If we observe $|s_0\rangle$ we can easily check the Toffoli gate, and seeing $|s_1\rangle$ we need to fix the resulting state up, which can be transformed by applying

$$
|s_a s_b s_c\rangle \rightarrow (-1)^{a.b}\,(-1)^{c}\,|s_a s_b s_c\rangle \qquad (7)
$$

to the three remaining encoded qubits. This fault tolerant operation is the composition of two linear operations $|s_a s_b\rangle \rightarrow (-1)^{a.b}$ and $|s_c\rangle \rightarrow (-1)^{c}$, that can be done using error correcting methods.

[1] Peter W. Shor, Fault Tolerant Quantum Computation. arXiv:quant-ph/9605011v2 5 Mar 1997