Tianran Cui
Kurt Hahn
Claire Kreisel

I. Matrix Proof for Decomposed CZ

The control-z gate (with q_0 as the control), $C_{Z(0,1)}$, can be decomposed into a Hadamard gate on q_1, followed by a CNOT gate with q_0 as the control, then another Hadamard gate on q_1

$$H_1 C_{X(0,1)} H_1 = C_{Z(0,1)}$$

$$(H \otimes I) C_{X(0,1)} (H \otimes I)$$

This equivalence can be shown using the matrix representations of these gates.

$$\left[\tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right] \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\end{pmatrix} \left[\tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right]$$

$$= \tfrac{1}{2}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix} \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\end{pmatrix} \begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix}$$

$$= \tfrac{1}{2}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix} \begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & 1\end{pmatrix}$$

$$= \tfrac{1}{2}\begin{pmatrix}2 & 0 & 0 & 0\\ 0 & 2 & 0 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & -2\end{pmatrix}$$

$$= \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{pmatrix} = C_{Z(0,1)}$$

II. Finding the Oracles with X gate

Grover's algorithm consists of three steps: 1) Use a $H^{\otimes n}$ gate to create a uniform superposed state, where n is the number of bits, 2) An oracle U_f to "mark" the desired state by inverting it, 3) Grover's diffusion operator U_g to amplify this state, then repeating $\sqrt{2^n}$ times.

The circuit is arranged as so:

$H^{\otimes n}\ U_g\ H^{\otimes n}\ U_f\ H^{\otimes n}\ |00...0\rangle$

The oracle for the 11 state, $U_{|11\rangle} = C_{Z(0,1)}$ acting on a uniform superposition of all four states:

$$
\begin{aligned}
& C_{Z(0,1)} H^{\otimes 2} |00\rangle \\
&= C_{Z(0,1)} \tfrac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2} \\
&= C_{Z(0,1)} \tfrac{1}{\sqrt{2}} (\tfrac{|0\rangle+|1\rangle}{\sqrt{2}} |0\rangle + \tfrac{|0\rangle+|1\rangle}{\sqrt{2}} |1\rangle) \\
&= \tfrac{1}{\sqrt{2}} (\tfrac{|0\rangle+|1\rangle}{\sqrt{2}} |0\rangle + Z \tfrac{|0\rangle+|1\rangle}{\sqrt{2}} |1\rangle) \\
&= \tfrac{1}{\sqrt{2}} (\tfrac{|0\rangle+|1\rangle}{\sqrt{2}} |0\rangle + \tfrac{|0\rangle-|1\rangle}{\sqrt{2}} |1\rangle) \\
&= \tfrac{|00\rangle+|01\rangle+|10\rangle-|11\rangle}{2}
\end{aligned}
$$

The oracle inverted the phase on the $|11\rangle$ state so that Grover's diffusion operator increases its amplitude.

We can use this example to "reverse-engineer" an oracle for the other states with the end goal of a uniform distribution of all four states. For the $|10\rangle$ state:

$$\frac{|00\rangle+|01\rangle-|10\rangle+|11\rangle}{2}$$

$$= \frac{1}{\sqrt{2}}(\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$$

This state looks similar to the one for the inverted $|11\rangle$ state, except for the bit value for q_0. This is important because q_1 can only pass through a Z gate if $q_0 = |1\rangle$. We can make this state identical this by having a X gate operate on q_0. Then we apply the control-z gate (with q_0 as the control and q_1 as the target).

$$= X_0 C_{Z(0,1)} C_{Z(0,1)} X_0 \frac{1}{\sqrt{2}}(\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$$

$$= X_0 C_{Z(0,1)} C_{Z(0,1)} \frac{1}{\sqrt{2}}(\frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle)$$

$$= X_0 C_{Z(0,1)} \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle)$$

$$\Rightarrow U_{|10\rangle} = X_0 C_{Z(0,1)}$$

$$\Rightarrow \boxed{U_{|10\rangle} = (I \otimes X) C_{Z(0,1)}}$$

Thus an oracle for the $|10\rangle$ state is a control-z gate followed by a Z gate on q_1.

We can continue this method to find oracles for the $|01\rangle$ and $|00\rangle$ states.

$\frac{|00\rangle-|01\rangle+|10\rangle+|11\rangle}{2}$

$= \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle - \frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle)$

$= X_1 C_{Z(0,1)} C_{Z(0,1)} X_1 \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle - \frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle)$

$= X_1 C_{Z(0,1)} C_{Z(0,1)} \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle)$

$= X_1 C_{Z(0,1)} \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$= X_1 C_{Z(0,1)} \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$

$\Rightarrow U_{|01\rangle} = X_1 C_{Z(0,1)}$

$\Rightarrow \boxed{U_{|01\rangle} = (X \otimes I) C_{Z(0,1)}}$

$\frac{-|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$

$= \frac{1}{\sqrt{2}}(-\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$= X^{\otimes 2} C_{Z(0,1)} C_{Z(0,1)} X^{\otimes 2} \frac{1}{\sqrt{2}}(-\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$= X^{\otimes 2} C_{Z(0,1)} C_{Z(0,1)} \frac{1}{\sqrt{2}}(\frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle)$

$= X^{\otimes 2} C_{Z(0,1)} \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle)$

$= X^{\otimes 2} C_{Z(0,1)} \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$

$\Rightarrow \boxed{U_{|00\rangle} = X^{\otimes 2} C_{Z(0,1)}}$

III. Matrix Proof for Oracles with X gate

$|00\rangle$

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \otimes \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{bmatrix} \begin{bmatrix}0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\end{bmatrix} = \begin{bmatrix}0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\end{bmatrix}$$

$|01\rangle$

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \otimes \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{bmatrix} \begin{bmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix} = \begin{bmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\end{bmatrix}$$

$|10\rangle$

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \otimes \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{bmatrix} \begin{bmatrix}0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} = \begin{bmatrix}0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & -1 & 0\end{bmatrix}$$

IV. Finding the Oracles with Z gate

We have also found that the oracles can be build using a Z gate, as seen below:

$\frac{|00\rangle+|01\rangle-|10\rangle+|11\rangle}{2}$

$= \frac{1}{\sqrt{2}}(\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

This state looks similar to the one for the inverted $|11\rangle$ state, except for the bit value for q_0. We can make this state identical to this by having a Z gate operate on q_1. Then we apply the control-z gate (with q_0 as the control and q_1 as the target).

$= Z_1 C_{Z(0,1)} C_{Z(0,1)} Z_1 \frac{1}{\sqrt{2}}(\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$= Z_1 C_{Z(0,1)} C_{Z(0,1)} \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle)$

$= Z_1 C_{Z(0,1)} \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$= Z_1 C_{Z(0,1)} \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$

$\Rightarrow U_{|10\rangle} = Z_1 C_{Z(0,1)}$

$\Rightarrow \boxed{U_{|10\rangle} = (Z \otimes I) C_{Z(0,1)}}$

Thus another oracle for the $|10\rangle$ state is a control-z gate followed by a Z gate on q_1. Interestingly, the math also works for the Z gate followed by the control-z gate. This commutativity turns out to be true for the other oracles with the Z gate.

$= C_{Z(0,1)} Z_1 \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$

$\Rightarrow U_{|10\rangle} = C_{Z(0,1)} Z_1$

$\Rightarrow U_{|10\rangle} = C_{Z(0,1)} (Z \otimes I)$

We can continue this method to find oracles for the $|01\rangle$ and $|00\rangle$ states.

$\frac{|00\rangle-|01\rangle+|10\rangle+|11\rangle}{2}$

$= \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle - \frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle)$

$= Z_0 C_{Z(0,1)} C_{Z(0,1)} Z_0 \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle - \frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle)$

$= Z_0 C_{Z(0,1)} C_{Z(0,1)} \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle)$

$= Z_0 C_{Z(0,1)} \frac{1}{\sqrt{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$= Z_0 C_{Z(0,1)} \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$

$\Rightarrow U_{|01\rangle} = Z_0 C_{Z(0,1)}$

$\Rightarrow \boxed{U_{|01\rangle} = (I \otimes Z) C_{Z(0,1)}}$

$\frac{-|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$

$= \frac{1}{\sqrt{2}}(-\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$= Z^{\otimes 2} C_{Z(0,1)} C_{Z(0,1)} Z^{\otimes 2}(-\frac{|0\rangle-|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$= Z^{\otimes 2} C_{Z(0,1)} C_{Z(0,1)}(-\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle - \frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle)$

$= Z^{\otimes 2} C_{Z(0,1)}(-\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle - \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$= (-1) Z^{\otimes 2} C_{Z(0,1)}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$\equiv Z^{\otimes 2} C_{Z(0,1)}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle+|1\rangle}{\sqrt{2}}|1\rangle)$

$\Rightarrow \boxed{U_{|00\rangle} = Z^{\otimes 2} C_{Z(0,1)}}$

The (-1) generated at the end can be ignored since it is the global phase.

V. Matrix Proof for Oracles with Z gate

$$(Z \otimes I)C_{Z(0,1)}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = U_{|10\rangle}$$

$$(I \otimes Z)C_{Z(0,1)}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = U_{|01\rangle}$$

$$(-1)Z^{\otimes 2}C_{Z(0,1)}$$

$$= (-1) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$= (-1) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = U_{|00\rangle}$$