Circuit identities

Let U be a 2×2 unitary matrix. The controlled-U is a two-qubit gate, written $C(U)$, which when applied to qubit registers q_1, q_2, is defined by:

U is applied if $k_{q_1} = 1$, otherwise it does not.

$$C(U)[q_1, q_2]\ |k_1\rangle \dots |k_{q_1}\rangle \dots |k_{q_2}\rangle \dots |k_n\rangle \quad = \quad |k_1\rangle \dots |k_{q_1}\rangle \dots (\underline{U^{k_{q_1}} |k_{q_2}\rangle}) \dots |k_n\rangle$$

where q_1 is the control qubit and q_2 is the target qubit, and where every $k_i \in \{0, 1\}$. The matrix representation of $C(U)$ for application to two qubits is:

$$C(U) \quad = \quad \begin{pmatrix} I & \mathbf{0} \\ \mathbf{0} & U \end{pmatrix}$$

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

where I is the 2×2 identity matrix and $\mathbf{0}$ is the 2×2 matrix in which every entry is 0. Notice that CNOT $= C(X)$, where X is one of the Pauli matrices.

Define SWAP to be the two-qubit gate that swaps the states of two qubit registers:

$$\text{SWAP}[q_1, q_2]\ |k_1 \dots k_{q_1} \dots k_{q_2} \dots k_n\rangle \quad = \quad |k_1 \dots k_{q_2} \dots k_{q_1} \dots k_n\rangle$$

where every $k_i \in \{0, 1\}$.

The assignment: Prove the following properties of controlled gates:

1. $\text{SWAP}[q_1, q_2] = C(X)[q_1, q_2]\ C(X)[q_2, q_1]\ C(X)[q_1, q_2]$.
2. $C(X)[p, q] = H[q]\ C(Z)[p, q]\ H[q]$.
3. $C(Z)[p, q] = C(Z)[q, p]$.
4. $H[p]\ H[q]\ C(X)[p, q]\ H[p]\ H[q] = C(X)[q, p]$.
5. $C(X)[p, q]\ X[p]\ C(X)[p, q] = X[p]\ X[q]$.
6. $C(X)[p, q]\ Z[p]\ C(X)[p, q] = Z[p]$.
7. $C(X)[p, q]\ X[q]\ C(X)[p, q] = X[q]$.
8. $C(X)[p, q]\ Z[q]\ C(X)[p, q] = Z[p]\ Z[q]$.

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

SWAP $[q_1, q_2]$: swap the state of q_1 and q_2

$C(X)[q_1, q_2]$: flip the state of q_2 if q_1 is in state $|1\rangle$

1. $\text{SWAP}[q_1, q_2] = C(X)[q_1, q_2]\ C(X)[q_2, q_1]\ C(X)[q_1, q_2]$.

Assume that $|q_1, q_2\rangle = |a, b\rangle$ as the initial state

Apply $C(x)[q_1, q_2]$: $C(x)[q_1, q_2]\,|a, b\rangle = |a, a \oplus b\rangle$

Apply $C(x)[q_2, q_1]$: $C(x)[q_2, q_1]\,|a, a\oplus b\rangle = |a \oplus (a\oplus b), a\oplus b\rangle$

$= |(a\oplus a)\oplus b, a\oplus b\rangle = |0\oplus b, a\oplus b\rangle = |b, a\oplus b\rangle$

Apply $C(x)[q_1, q_2]$: $C(x)[q_1, q_2]\,|b, a\oplus b\rangle = |b, (a\oplus b)\oplus b\rangle$

$= |b, a\oplus (b\oplus b)\rangle = |b, a\oplus 0\rangle = |b, a\rangle$

$\therefore\ C(x)[q_1, q_2]\ C(x)[q_2, q_1]\ C(x)[q_1, q_2]\,|a, b\rangle = |b, a\rangle$

$\because\ \text{SWAP}[q_1, q_2]\,|a, b\rangle = |b, a\rangle$

$\therefore\ \text{SWAP}[q_1, q_2] = C(x)[q_1, q_2]\ C(x)[q_2, q_1]\ C(x)[q_1, q_2]$

2. $C(X)[p,q] = H[q]\ C(Z)[p,q]\ H[q]$.

Initial State: $|p,q\rangle = |a,b\rangle$

Apply $H[q]$: $H[q]\,|a,b\rangle = |a, H\cdot b\rangle$

Apply $C(Z)[p,q]$: $C(Z)[p,q]\,|a, H\cdot b\rangle = |a, Z^a(H\cdot b)\rangle$

Apply $H[q]$: $H[q]\,|a, Z^a(H\cdot b)\rangle = |a, H(Z^a(H\cdot b))\rangle$

$C(Z)[p,q]$: if p is in state $|1\rangle$, then q is in state $-|b\rangle$

if p is in state $|0\rangle$, then q is unchanged.

When $|a\rangle = |0\rangle$

When $|b\rangle = |0\rangle$, $H\ Z^a\ H\,|b\rangle = H\,Z^a\,H\,|0\rangle = H Z^a\,|+\rangle$

$= H\cdot I\cdot|+\rangle = H\,|+\rangle = |0\rangle$

When $|b\rangle = |1\rangle$, $H\ Z^a\ H\,|b\rangle = H\ Z^a\ H\,|1\rangle = H\ Z^a\ |-\rangle$

$= H\cdot I\cdot |-\rangle = H\,|-\rangle = |1\rangle$

When $|a\rangle = |1\rangle$

When $|b\rangle = |0\rangle$, $H\ Z^a\ H\,|b\rangle = H\ Z^a\ H\,|0\rangle = H\ Z^a\ |+\rangle$

$= H\cdot Z\cdot |+\rangle = H\cdot|-\rangle = |1\rangle$

When $|b\rangle = |1\rangle$, $H\ Z^a\ H\,|b\rangle = H\ Z^a\ H\,|1\rangle = H\ Z^a\ |-\rangle$

$= H\cdot Z\cdot |-\rangle = H\cdot|+\rangle = |0\rangle$

$\therefore$ $H\,C(Z)\,H$ flips the state of q if p is in state $|1\rangle$

and q is unchanged if p is in state $|0\rangle$

$\therefore$ It is a CNOT gate

$\therefore$ $C(X)[p,q] = H[q]\ C(Z)[p,q]\ H[q]$.

3. $C(Z)[p,q] = C(Z)[q,p]$.

When $|p\rangle = |1\rangle$

$|q\rangle = |0\rangle$: $C(Z)[p,q]\,|a,b\rangle = |1,\ Z^1\cdot 0\rangle = |1,0\rangle$

$C(Z)[q,p]\,|b,a\rangle = |0,\ I\cdot 1\rangle = |0,1\rangle$

$|q\rangle = |1\rangle$: $C(Z)[p,q]\,|a,b\rangle = |1,\ Z^1\cdot 1\rangle = -|1,1\rangle$

$C(Z)[q,p]\,|b,a\rangle = |1,\ Z^1\cdot 1\rangle = -|1,1\rangle$

When $|p\rangle = |0\rangle$

$|q\rangle = |1\rangle$: $C(Z)[p,q]\,|a,b\rangle = |0,\ I\cdot 1\rangle = |0,1\rangle$

$C(Z)[q,p]\,|b,a\rangle = |1,\ Z^1\cdot 0\rangle = |1,0\rangle$

$|q\rangle = |0\rangle$: $C(Z)[p,q]\,|a,b\rangle = |0,\ I\cdot 0\rangle = |0,0\rangle$

$C(Z)[q,p]\,|b,a\rangle = |0,\ I\cdot 0\rangle = |0,0\rangle$

$\therefore$ We can see that

$C(Z)[p,q]\,|0,0\rangle = C(Z)[q,p]\,|0,0\rangle$

$C(Z)[p,q]\,|0,1\rangle = C(Z)[q,p]\,|0,1\rangle$

$C(Z)[p,q]\,|1,0\rangle = C(Z)[q,p]\,|1,0\rangle$

$C(Z)[p,q]\,|1,1\rangle = C(Z)[q,p]\,|1,1\rangle$

$\therefore\ C(Z)[p,q] = C(Z)[q,p]$

4. $H[p]\ H[q]\ C(X)[p,q]\ H[p]\ H[q] = C(X)[q,p]$.

Initial state: $|p,q\rangle = |00\rangle$

Apply H[p] and H[q] to the initial state

$H[p]\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\quad$ $H[p]\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$H[q]\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\quad$ $H[q]\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

We are transforming both qubits p and q into superposition states:

$$H[p]H[q]\,|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$= \frac{1}{2}\Big(|0\rangle * (|0\rangle + |1\rangle) + (|1\rangle * (|0\rangle + |1\rangle)\Big)$$
$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Apply CNOT:

$$C(X)[p,q]\ H[p]\,H[q]\,|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |11\rangle + |10\rangle)$$

Apply H[q]:

$$(I \otimes H)\ \frac{1}{2}(|00\rangle + |01\rangle + |11\rangle + |10\rangle)$$
$$= \frac{1}{2}\Big[|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) + |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) + |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$= \frac{1}{2\sqrt{2}}(|00\rangle + |01\rangle + |00\rangle - |01\rangle + |10\rangle - |11\rangle + |10\rangle + |11\rangle)$$
$$= \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

Apply H[p]:

$$(H \otimes I)\ \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}\Big[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle\Big)$$
$$= \frac{1}{2}(|00\rangle + |10\rangle + |00\rangle - |10\rangle) = |00\rangle$$

$\because\ C(X)[q,p]\,|00\rangle = |00\rangle$

$\therefore\ H[p]\,H[q]\ C(X)[p,q]\ H[p]\,H[q] = C(X)[q,p]$

5. $C(X)[p, q]\ X[p]\ C(X)[p, q] = X[p]\ X[q]$.

$X[p]$: flip the qubit p.

When p is in the $|0\rangle$ state:

Apply $C(X)[p,q]$, the qubit q won't be flipped.

$$C(X)[p,q]\,|p,q\rangle = |p,q\rangle$$

Apply $X[p]$, it flips the qubit p to $|1\rangle$ state.

Apply $C(X)[p,q]$, the qubit q will be flipped since $p=|1\rangle$

$\therefore$ At the end, both qubits are flipped once.

$\therefore$ $C(X)[p,q]\ X[p]\ C(X)[p,q] = X[p]\ X[q]$ when $p=|0\rangle$.

When p is in the $|1\rangle$ state:

Apply $C(X)[p,q]$, the qubit q will be flipped.

Apply $X[p]$, it flips the qubit p to $|0\rangle$ state.

Apply $C(X)[p,q]$, the qubit q won't be flipped since $p=|0\rangle$

$\therefore$ At the end, both qubits are flipped once.

$\therefore$ $C(X)[p,q]\ X[p]\ C(X)[p,q] = X[p]\ X[q]$ when $p=|1\rangle$.

$\therefore$ $C(X)[p,q]\ X[p]\ C(X)[p,q] = X[p]\ X[q]$

6. $C(X)[p,q]\ Z[p]\ C(X)[p,q] = Z[p]$.

Z[p] : flip the phase of the qubit |1> and leaves |0> unchanged

When p is in the |0> state,

Z[p] won't change p.

∴ both C(X)[p, q] will leave q unchanged since p is |0>.

∴ C(X)[p, q] Z[p] C(X)[p, q] doesn't change anything.

∴ C(X)[p, q] Z[p] C(X)[p, q] = Z[p].

When p is in the |1> state,

Z[p] flips the phase of the qubit p.

Both C(X)[p, q] will flip q since p is in the |1> state,

but the change happened twice cancels out, so q doesn't change.

∴ C(X)[p, q] Z[p] C(X)[p, q] only flips the phase of p.

∴ C(X)[p, q] Z[p] C(X)[p, q] = Z[p].

7. $C(X)[p, q]\ X[q]\ C(X)[p, q] = X[q]$.

X[q]: flip the qubit q.

When p is in the |0> state:

∴ both C(x)[p, q] won't change q since p is |0>.

∴ C(x)[p,q] X[q] C(x)[p,q] only applies X gate to qubit q and qubit q is flipped once.

∴ C(x)[p,q] X[q] C(x)[p,q] = X[q]

When p is in the |1> state:

Apply C(x)[p, q], the qubit q will be flipped.

Apply X[q], the qubit q will be flipped back to the initial state

Apply C(x)[p, q], the qubit q will be flipped again

∴ At the end, the qubit q is changed

∴ C(x)[p, q] X[q] C(x)[p, q] = X[q] when p = |1>.

∴ C(x)[p, q] X[q] C(x)[p, q] = X[q]

8. $C(X)[p,q]\ Z[q]\ C(X)[p,q] = Z[p]\ Z[q]$.

Z[q]: flip the phase of the qubit |1> and leaves |0> unchanged

When p is in the |0> state,

Both C(X)[p,q] will leave q unchanged since p is in |0>

∴ C(X)[p,q] Z[q] C(X)[p,q] only applies Z gate to qubit q

Z[p] won't change p since Z leaves |0> unchanged.

∴ C(X)[p,q] Z[q] C(X)[p,q] = Z[p] Z[q] when p is in |0>

When p is in the |1> state,

Apply C(X)[p,q], the qubit q is flipped and the state becomes X[q].

Apply Z[q], the state becomes $-X[q]$ when q is in |0>

X[q] when q is in |1>

$-X[q]$: apply C(X)[p,q]. the qubit q is flipped again.

the state becomes $X[-X[q]] = -I$

X[q]: apply C(X)[p,q], the qubit q is flipped again.

the state becomes $X[X[q]] = I$

For Z[p] Z[q], |p> = |1>, |q> = |0> Z[p] Z[q] = $-I$

|p> = |1>, |q> = |1> Z[p] Z[q] = I

∴ It matches the result of C(X)[p,q] Z[q] C(X)[p,q]

∴ C(X)[p,q] Z[q] C(X)[p,q] = Z[p] Z[q] when p is in |1>

∴ C(X)[p,q] Z[q] C(X)[p,q] = Z[p] Z[q]