Solving for the Unknown (?) Marked Gates for a Decomposed Toffoli Quantum Circuit

Niloy Kumar Mondal

github.com/QuitttCat
nkm2105044@gmail.com
+8801792023909

October 8, 2025

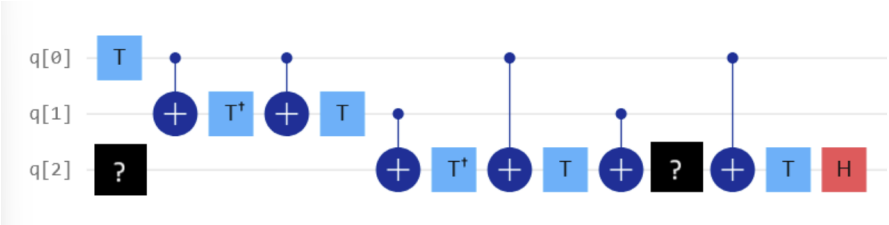
Contents

1 Problem Statement

Gate Tomography

When designing a set of universal gates, one must prove that any unitary operation can be performed by combining gates of that set, which is known as circuit equivalence. In this case, you have to find the parameters of the U3 gates such that the following circuit is equivalent to a Toffoli gate, in which the U3 gates are marked with '?':

$$U3(\theta,\phi,\lambda) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda}\sin\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) & e^{i(\phi+\lambda)}\cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$



NOTE: The parameters of the U3 gates might not be the same for both!

2 Toffoli Gate

The Toffoli gate, or Controlled-Controlled-NOT (CCNOT) gate, is a three-qubit gate that is universal for classical computation. It flips the target qubit if and only if both control qubits are in the state $|1\rangle$. In quantum computation, its matrix representation in the computational basis $\{|000\rangle, ..., |111\rangle\}$ is:

$$\text{Toffoli} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The problem at hand is to find the parameters for two U3 gates, denoted as (?), in the provided circuit diagram such that the entire circuit is equivalent to a Toffoli gate.

3 Solution

3.1 Analysis of the output of the first two qubits

Let $\omega := e^{i\pi/4}$. Recall

$$T|x\rangle = \omega^x|x\rangle, \qquad T^\dagger|x\rangle = \omega^{-x}|x\rangle, \qquad \mathrm{CNOT}_{0\to1}: \ |a,b\rangle \mapsto |a,\, b\oplus a\rangle.$$

The only gates that can change the *bit values* of the first two qubits are the two $\mathrm{CNOT}_{0\to1}$ gates; since the same CNOT appears twice with the same control and target, their net action on the second qubit is the identity:

$$b \xrightarrow{\oplus a} b\oplus a \xrightarrow{\oplus a} (b\oplus a)\oplus a = b.$$

Thus, the first two qubits emerge with the *same* computational values (a, b) for all four inputs. However, the single–qubit $T/T^\dagger$ gates may add phases. Evaluating the prefix on the top two lines,

$$P := T_0\ \mathrm{CNOT}_{0\to1}\ T_1^\dagger\ \mathrm{CNOT}_{0\to1}\ T_1,$$

we obtain the following case-by-case behavior on basis states $|ab\rangle$:

Input $ab = 00$**.** No CNOT fires and $T/T^\dagger$ on $|0\rangle$ contribute no phase:

$$P\,|00\rangle = |00\rangle.$$

Input $ab = 01$**.** No CNOT fires; $T^\dagger$ then T on the second qubit cancel:

$$P\,|01\rangle = (\omega^{-1}\omega)\,|01\rangle = |01\rangle.$$

Input $ab = 10$**.** The first CNOT flips $b : 0 \to 1$, so $T^\dagger$ contributes ω^{-1}; the second CNOT flips back to 0, and T on $|0\rangle$ does nothing. Multiplying by the T on the first qubit (phase ω) gives

$$P\,|10\rangle = (\omega\cdot\omega^{-1})\,|10\rangle = |10\rangle.$$

Input $ab = 11$**.** The first CNOT flips $b : 1 \to 0$ so $T^\dagger$ does nothing; the second CNOT flips back to 1, and T on the second qubit contributes ω. Together with the T on the first qubit we get

$$P\,|11\rangle = (\omega\cdot\omega)\,|11\rangle = \omega^2\,|11\rangle = e^{i\pi/2}\,|11\rangle.$$

Therefore, *as classical bits* the first two qubits are unchanged for all four inputs:

$$|ab\rangle \longmapsto |ab\rangle \qquad (ab \in \{00, 01, 10, 11\}),$$

while a transient relative phase ω^2 appears only on the branch $ab = 11$. In the full circuit, the middle block that couples to the target qubit implements the compensating phase (a CCZ gadget), so this ω^2 phase is canceled; hence the overall unitary leaves the first two qubits *exactly* unchanged for all inputs, as required for a Toffoli/CCX decomposition.

3.2 Core logic of the main solution (formal proof)

We analyse the unitary acting on the target qubit $q[2]$ conditional on the computational values of the two controls $q[0], q[1]$. Throughout we use the identities (global phases ignored):

$$XTX = e^{i\pi/4}T^\dagger \sim T^\dagger, \qquad XT^\dagger X = e^{-i\pi/4}T \sim T, \tag{1}$$

$$TT^\dagger = T^\dagger T = I, \qquad HZH = X. \tag{2}$$

Every CNOT with control value 1 conjugates the immediately adjacent single–qubit gates on the target by X (hence (1) applies).

Let M_{ab} denote the effective operator on $q[2]$ when the controls are ab with $a, b \in \{0, 1\}$. Reading the target wire from left to right in the circuit of Fig. **??** (and suppressing the CNOTs that are *inactive* for the chosen a, b), the single–qubit gates on $q[2]$ appear in the order

$$U_1 \ \cdots \ T^\dagger \ \cdots \ T \ \cdots \ U_2 \ \cdots \ T \ H,$$

where each "$\cdots$" may insert a conjugation by X if the corresponding CNOT fires.

Branch $ab = 00$. No CNOT fires; hence

$$M_{00} = U_1\, T^\dagger T\, U_2\, T\, H = U_1 U_2\, T\, H. \tag{3}$$

Imposing the Toffoli requirement "do nothing on the target" gives $M_{00} = I$, i.e.

$$U_1 U_2 = (TH)^{-1} = HT^\dagger. \tag{4}$$

A convenient solution of (4) is

$$U_1 = H, \qquad U_2 = T^\dagger.$$

Branch $ab = 01$. Exactly those CNOTs controlled by $q[1]$ fire. They conjugate the two highlighted $T/T^\dagger$ gates on the target by X, which by (1) swaps $T \leftrightarrow T^\dagger$ (up to a global phase). Thus the same two gates still cancel:

$$M_{01} \sim U_1\, T\, T^\dagger\, U_2\, T\, H = U_1 U_2\, T\, H \overset{(4)}{=} I.$$

Branch $ab = 10$. Now only the CNOTs controlled by $q[0]$ fire. The same conjugation logic applies and the cancelling pair remains:

$$M_{10} \sim U_1\, T\, T^\dagger\, U_2\, T\, H = U_1 U_2\, T\, H \overset{(4)}{=} I.$$

Branch $ab = 11$**.** All the relevant CNOTs fire. Conjugating by X where appropriate flips some $T \leftrightarrow T^\dagger$ so that *one* Z survives between U_1 and U_2 (this is the well–known phase–polynomial realization of a CCZ):

$$M_{11} \sim U_1\, Z\, U_2\, T\, H.$$

Substituting $U_1 = H$ and $U_2 = T^\dagger$ and using $T^\dagger T = I$ and (2) we obtain

$$M_{11} \sim HZT^\dagger TH = HZH = X.$$

Hence the target flips exactly in the $ab = 11$ branch.

Combining the four branches we have

$$M_{ab} = \begin{cases} I, & (a,b) \in \{00, 01, 10\}, \\ X, & (a,b) = 11, \end{cases}$$

which is precisely the action of a Toffoli gate with controls $q[0], q[1]$ and target $q[2]$. Therefore the choice $U_1 = H$ and $U_2 = T^\dagger$ makes the given circuit implement CCX (up to an irrelevant global phase).

3.3 Finding parameters for $U_1 = H$ and $U_2 = T^\dagger$

We use the standard matrix parametrization

$$U3(\theta, \phi, \lambda) = \begin{pmatrix} \cos(\frac{\theta}{2}) & -e^{i\lambda} \sin(\frac{\theta}{2}) \\ e^{i\phi} \sin(\frac{\theta}{2}) & e^{i(\phi+\lambda)} \cos(\frac{\theta}{2}) \end{pmatrix}.$$

Parameters for $U_1 = H$**.** The Hadamard matrix is

$$H = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Equating entries with $U3(\theta, \phi, \lambda)$ (up to a global phase) gives

$$\cos\Big(\tfrac{\theta}{2}\Big) = \sin\Big(\tfrac{\theta}{2}\Big) = \tfrac{1}{\sqrt{2}} \;\Rightarrow\; \theta = \tfrac{\pi}{2},$$

$$-e^{i\lambda} = 1 \;\Rightarrow\; \lambda \equiv \pi \pmod{2\pi}, \qquad e^{i\phi} = 1 \;\Rightarrow\; \phi \equiv 0 \pmod{2\pi}.$$

A principal choice is therefore

$$\boxed{U_1 = U3\big(\tfrac{\pi}{2},\, 0,\, \pi\big) = H}$$

(and any $(\frac{\pi}{2},\, 2\pi k,\, \pi + 2\pi m)$ yields the same matrix).

Parameters for $U_2 = T^\dagger$. The $T^\dagger$ gate is diagonal:

$$T^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix}.$$

With $\theta = 0$ we obtain

$$U3(0, \phi, \lambda) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i(\phi+\lambda)} \end{pmatrix},$$

so we need $e^{i(\phi+\lambda)} = e^{-i\pi/4}$, i.e.

$$\phi + \lambda \equiv -\tfrac{\pi}{4} \pmod{2\pi}.$$

A convenient principal choice is

$$\boxed{U_2 = U3\big(0,\, 0,\, -\tfrac{\pi}{4}\big) = T^\dagger}$$

(and more generally $U3(0,\, \phi,\, -\frac{\pi}{4} - \phi)$ for any ϕ).

4 Verification

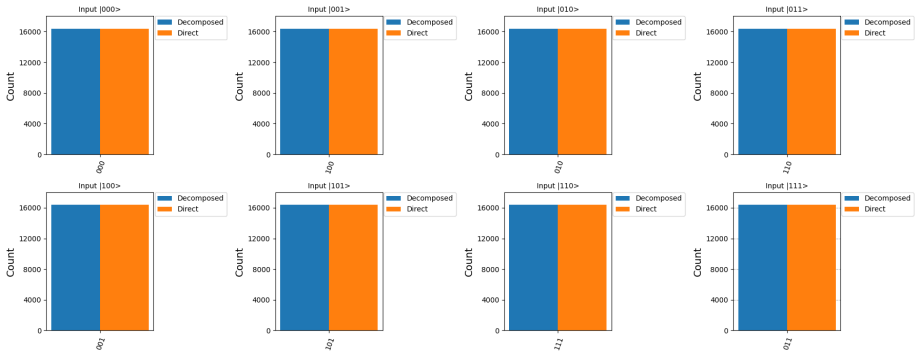


Figure 1: Decomposed vs Direct Toffoli Gate Output Compare

Output is identical. So our identification is correct.

5 Remarks on Methodology

A formal, brute-force approach to finding the unknown gates U_1 and U_2 would involve representing them as general 2x2 unitary matrices with variable entries. The next step would be to construct the full 8x8 unitary matrix for the entire circuit by performing tensor products and matrix multiplication for every gate

in sequence. Finally, this resulting complex 8x8 matrix would be equated to the known 8x8 matrix of the Toffoli gate.

This method would produce a large system of coupled, non-linear algebraic equations. Solving such a system for the matrix variables is mathematically intensive and computationally prohibitive in terms of time complexity.

Therefore, a more practical approach was adopted: a property-based analysis. Instead of solving the entire system at once, we use the defining properties of the Toffoli gate to derive constraints on the circuit's behavior.