1 Homework 4

1. Let $U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$. Write a matrix representation of $U[1]$ and $U[2]$ for $n = 2$. For $n = 3$, write a matrix representation of CNOT[3, 1].

2. Let $A = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & 1 \\ 1 & i \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Which 2-qubits gate can you apply on the first qubits at the end of the circuit to get a Toffoli gate?

2 Gate Sets for Quantum Circuits

The aim of this exercise is to prove the following theorem:

**Theorem 2.1.** The set of all two-qubits unitary operators allows the realization of an arbitrary unitary operator.

**Remark.** One-qubit unitaries operators are particular cases of two-qubits unitary operators.

Thanks to the homework, we already know that we can realize a Toffoli gate with only two-qubits unitaries. This will be a useful tool in the next parts of the proof.

2.1 Controled Unitaries

Recall that $\Lambda^k(U)$ denotes the $k$-controlled unitary $U$, which is defined by:

$$\Lambda^k(U) (|x_1x_2\ldots x_k\rangle \otimes |\psi\rangle) := \begin{cases} |x_1x_2\ldots x_k\rangle \otimes U|\psi\rangle & \text{if } x_1 \land x_2 \land \ldots \land x_k = 1 \\ |x_1x_2\ldots x_k\rangle \otimes |\psi\rangle & \text{otherwise} . \end{cases}$$

The aim of this part is to prove that we can realize $\Lambda^k(U)$, with $U$ acting on one qubit, using only two-qubits unitaries.

1. Design a classical circuit that computes $x_1 \land x_2 \land \ldots \land x_k$. What is its size? Its depth?

2. Design a quantum circuit $A$ that computes $x_1 \land x_2 \land \ldots \land x_k$, i.e. that $A|x_1x_2\ldots x_k\rangle \otimes |0\rangle^{(N-k)} = |G(x_1x_2\ldots x_k)\rangle \otimes |x_1 \land x_2 \land \ldots \land x_k\rangle$, with $|G(x_1x_2\ldots x_k)\rangle$ acting on $N - 1$ qubits is some garbage state, using only Toffoli and NOT gates. What is its size? Its depth?

3. Design an efficient quantum circuit that computes $A^{-1}$ efficiently. What is its size? Its depth?

4. Design a quantum circuit that computes $\Lambda^k(U)$ using only two-qubits unitaries, with the help of ancillas, i.e. some circuit $L$ such that:

$$L \left( |x_1x_2\ldots x_k\rangle \otimes |\psi\rangle \otimes |0\rangle^{(N-1-k)} \right) = \left( \Lambda^k(U) \left( |x_1x_2\ldots x_k\rangle \otimes |\psi\rangle \right) \right) \otimes |0\rangle^{(N-1-k)} .$$
2.2 Almost Diagonal Unitaries

The aim of this part is to show that unitaries $U$ on $\mathbb{C}^{2^n}$ of the form $\text{Diag} \left(1, \ldots, 1, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, 1, \ldots, 1 \right)$ can be realized using only two-qubits unitaries.

1. What can you say about $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$?

2. Write $\Lambda^{n-1} \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)$ in matrix form. Show that there exists a permutation matrix $P$ such that:

$$U = P^{-1} \Lambda^{n-1} \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) P.$$ 

3. Design a quantum circuit that computes $P$ and another that computes $P^{-1}$ using only two-qubits unitaries. What are their sizes? Their depths?

4. Design a quantum circuit that computes $\text{Diag} \left(1, \ldots, 1, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, 1, \ldots, 1 \right)$. What is its size? Its depth?

2.3 General form of an Arbitrary Unitary

Recall the following lemma seen during last lecture:

**Lemma 2.2.** Any unitary operator $U$ on $\mathbb{C}^M$ can be written as a product of $O(M^2)$ unitary matrices of the form $\text{Diag} \left(1, \ldots, 1, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, 1, \ldots, 1 \right)$.

1. Prove theorem 2.1 using ancillas. What is the size of the circuit? Its depth?

3 Quantum 1-Machine

You have a device that outputs only $|0\rangle$. You can use this device several times, and measure in any basis. How many calls to the device do you need to get a $|1\rangle$?

4 Simon’s Problem Generalized

Consider a function $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ with the promise that there exists a vector subspace $V$ of $\{0, 1\}^n$ (seen as a vector space over $\mathbb{F}_2$) such that:

$$\forall x, y \in \{0, 1\}^n, f(y) = f(x) \iff \exists v \in V, x = y + v.$$ 

Show that one run of Simon’s algorithm output $x \in \{0, 1\}^n$ such that $x$ is orthogonal to $V$ ($\forall y \in V, x \cdot y = 0 \mod 2$).

**Remark:** the usual version of Simon’s Problem is when $V = \{0, a\}$ for some $a \in \{0, 1\}^n$. 