Exercise Sheet 8: Towards quantum computing

Getting to Know Some Quantum Gates

One of the most common ways of thinking about quantum computation is in terms of quantum circuits: A overall quantum computation is decomposed into smaller building blocks, typically referred to as gates. Here, you will familiarize yourself with some important gates and the idea of decomposing an overall unitary into gates.

7 P. Exercise 1.

1 P. (a) Write down the (unitary) matrix for the single-qubit gate that implements an analogue of the classical NOT. That is, the gate should act as $|0\rangle \mapsto |1\rangle$, $|1\rangle \mapsto |0\rangle$.

1 P. (b) Write down the (unitary) matrix for the two-qubit controlled-NOT (CNOT) gate, which implements a computational basis flip on the second qubit controlled on the first qubit being active. That is, the gate should act as $|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |11\rangle$, $|11\rangle \mapsto |10\rangle$.

1 P. (c) Write down the (unitary) matrix for the single-qubit gate that implements the basis change between $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. That is, the gate should act as $|0\rangle \mapsto |+\rangle$, $|1\rangle \mapsto |-\rangle$.

1 P. (d) Let $U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$ be some single-qubit unitary. Write down the (unitary) matrix for the two-qubit controlled-U gate, which implements U controlled on the first qubit being active.

1 P. (e) Let $\varphi \in [0, 2\pi)$. Write down the (unitary) matrix for the single-qubit gate that acts as $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto e^{i\varphi}|1\rangle$.

2 P. (f) Describe a quantum circuit with two gates that, starting from $|00\rangle$, prepares the maximally entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Prove that your circuit acts as desired.

Classical Circuit Complexity

Classical computers perform any operation by combining few elementary building blocks (what we call gates) into more complex operations. As soon as we fix a specific set of available gates (classical computers can do using only the NAND operation between neighboring bits for example), we say we have fixed a *circuit model*. (Sometimes, one additionally assumes restrictions on the circuit layout, but we ignore this here.) Given this model, we can define the *circuit complexity* of a function. This is the minimum number of gates from the given available set that is sufficient to construct the desired function. In other words: A function is said to have circuit complexity at most G (w.r.t. some circuit model) if there is a circuit (in that model) with at most G gates that implements the function.

5 P. Bonus Exercise 1. In this exercise, you will investigate how rare the property of having "small" circuit complexity is.

1 P. (a) How many classical Boolean functions mapping n bits to 1 bit – i.e., functions $f\colon \{0,1\}^n \to \{0,1\}$ – are there?

2 P. (b) Consider a classical circuit model in which circuits are composed of arbitrary two-bit gates whose input bits are either a constant (0 or 1), an entry of an input string or its negation, or an output of some other gate. Let $G \in \mathbb{N}$. Show that there are at most $16^G(G + 2n + 1)^{2G}$ classical Boolean functions mapping n bits to 1 bit that have circuit complexity at most G in this model.

2 P. (c) Conclude that for $G \leq \frac{2^n}{3n}$, the fraction of Boolean functions mapping n bits to 1 bit with circuit complexity at most G vanishes as $n \to \infty$. What does this mean in words?

Hint: Once you have identified the right limit to compute, feel free to let WolframAlpha compute it for you.

Bases for Unitary Quantum Gates

Usually, when talking about quantum computing, people refer to the manipulation of pure quantum states of a certain number of qubits to perform a task of interest. In this setting, the gates (elemental operations that transform the state) are described by unitary matrices. When writing matrices down, the first natural choice is to do it in the computational basis (the input-output relationship between state $|i\rangle$ and $|j\rangle$ under a given operation), but one could choose a different basis. We want to explore this a little in the following two exercises and look at different bases for the space of operators.

3 P. **Exercise 2.** First, we look at the Pauli basis.

2 P. (a) Show that the set $\left\{\frac{1}{\sqrt{2}}\mathbb{1}_2, \frac{1}{\sqrt{2}}X, \frac{1}{\sqrt{2}}Y, \frac{1}{\sqrt{2}}Z\right\}$ of normalized single-qubit Pauli matrices forms an orthonormal basis (ONB) for $\mathbb{C}^{2\times 2}$ w.r.t. the Hilbert-Schmidt inner product.

1 P. (b) Show that the set $\left\{\frac{1}{\sqrt{2}}\mathbb{1}_2, \frac{1}{\sqrt{2}}X, \frac{1}{\sqrt{2}}Y, \frac{1}{\sqrt{2}}Z\right\}^{\otimes n}$ of all tensor products of n normalized Pauli operators – the so-called normalized Pauli strings – forms an ONB for $\mathbb{C}^{2^n\times 2^n}$ w.r.t. the Hilbert-Schmidt inner product.

Hint: How can you express $\mathrm{Tr}\left[(A\otimes B)(C\otimes D)\right]$ *in terms of* $\mathrm{Tr}[AC]$ *and* $\mathrm{Tr}[BD]$*?*

11 P. **Exercise 3.** Next, we look at the Heisenberg-Weyl operators. The Heisenberg-Weyl operators $U_{k\ell}$, $0 \leq k, \ell \leq d-1$, in d dimensions are defined as

$$U_{k\ell} = \sum_{j=0}^{d-1} \zeta^{j\ell} |k+j\rangle\langle j| \,,$$

where $\zeta = \exp(2\pi i/d)$.

2 P. (a) Show that the Heisenberg-Weyl operators satisfy $U_{k\ell}U_{k'\ell'} = \zeta^{\ell k'} U_{k+k',\ell+\ell'}$, where the addition in the index is modulo d.

1 P. (b) Show that $U_{k\ell}^{-1} = \zeta^{k\ell} U_{-k,-\ell}$. (Here, $-k$ is to be understood as the inverse element of k in $\mathbb{Z}_d = \{0,\ldots,d-1\}$, i.e., w.r.t. addition modulo d.)

Hint: Use (a)

2 P. (c) Show that the Heisenberg-Weyl operators are unitaries.

2 P. (d) Show that the Heisenberg-Weyl operators satisfy $\mathrm{Tr}[U_{k\ell}^\dagger U_{k'\ell'}] = d\delta_{k,k'}\delta_{\ell,\ell'}$. In particular, they are orthogonal w.r.t. the Hilbert-Schmidt inner product.

Hint: Start by looking at $\mathrm{Tr}[U_{k\ell}]$*, then use (a), (b) and (c).*

1 P. (e) Conclude that the set $\left\{\frac{1}{\sqrt{d}}U_{k\ell}\right\}_{k,\ell=0}^{d-1}$ forms an ONB for $\mathbb{C}^{d\times d}$ w.r.t. the Hilbert-Schmidt inner product.

3 P. (f) Let $d = 2^n$. We have identified two ONBs for $\mathbb{C}^{2^n\times 2^n}$, namely $\left\{\frac{1}{\sqrt{2}}\mathbb{1}_2, \frac{1}{\sqrt{2}}X, \frac{1}{\sqrt{2}}Y, \frac{1}{\sqrt{2}}Z\right\}^{\otimes n}$ on the one hand and $\left\{\frac{1}{\sqrt{d}}U_{k\ell}\right\}_{k,\ell=0}^{d-1}$ on the other hand . Do these ONBs coincide (up to global phases)?

Total Points: 21 (+5)