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 $|0\rangle \mapsto |1\rangle$, $|1\rangle \mapsto |0\rangle$.

Solution

This is just the Pauli X gate, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

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 $|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |11\rangle$, $|11\rangle \mapsto |10\rangle$.

Solution

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

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 $|0\rangle \mapsto |+\rangle$, $|1\rangle \mapsto |-\rangle$.

Solution

This is the Hadamard gate, $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

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.

Solution

$$\mathrm{C}\,U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{pmatrix}.$$

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 $|1\rangle \mapsto e^{i\varphi}|1\rangle$.

Solution

$$S_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}.$$

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.

Solution

We first apply the Hadamard gate H to the first qubit. This maps $|00\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$. Then we apply a CNOT gate, with the first qubit as control and the second qubit as target. This further maps $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Thus, our simple 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?

Solution

The input space is $\{0,1\}^n$, it consists of 2^n elements. The output space consists of 2 elements. Thus, there are 2^{2^n} Boolean functions mapping n bits to 1 bit. This can be seen by thinking of the description of the function as an array specifying the output (0 or 1) for each of the (ordered) possible inputs. So each possible function is defined by a binary array with as many elements as there are possible inputs (2^n). Consequently, the number of possible functions is the number of possible binary arrays with 2^n elements, that is 2^{2^n}.

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.

Solution

The number of circuits with at most G gates is at most $16^G(G+2n+1)^G$. Here, the first factor 16^G comes from each two-bit gate being one of the $2^{2^2} = 2^4 = 16$ possible two-bit gates, and the factor $(G+2n+1)^{2G} = (2+n+n+(G-1))^{2G}$ comes from each gate input being either a constant (0 or 1), an entry of an input string, a negated entry of an input string, or the output of some other gate, and from each gate having two inputs.

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.

Solution

Combining the results of (a) and (b), the fraction of Boolean functions mapping n bits to 1 bit with circuit complexity at most G is $\frac{16^G(G+2n+1)^{2G}}{2^{2^n}}$. For $G = \frac{2^n}{3n}$, WolframAlpha tells us:

$$\lim_{n\to\infty} \frac{16^{2^n/3n}\left(\frac{2^n}{3n}+2n+1\right)^{2^n/3n}}{2^{2^n}} = 0\,.$$

In words: As n grows, the overwhelming majority of all functions mapping n bits to 1 bit requires effectively exponential circuit complexity.

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.

Solution

The space $\mathbb{C}^{2\times 2}$ is 4-dimensional, so we need 4 basis elements to span the space. (Remember that one possible choice of basis would have been the computational basis $\{|0\rangle\langle 0|, |0\rangle\langle 1|, |1\rangle\langle 0|, |1\rangle\langle 1|\}$.) We now need to verify that the given elements are normalized and they are orthogonal.
First, normalization results from the fact that the single-qubit Pauli matrices are unitary, so for any of $P \in \{\mathbb{1}_2, X, Y, Z\}$ we have that $P^\dagger P = \mathbb{1}$. With this,

$$\mathrm{Tr}\left[\left(\frac{1}{\sqrt{2}}P\right)^\dagger \left(\frac{1}{\sqrt{2}}P\right)\right] = \frac{1}{2}\,\mathrm{Tr}[\mathbb{1}] = 1\,.$$

Now orthogonality. For any $P \in \{X, Y, Z\}$, we have

$$\mathrm{Tr}[\mathbb{1}P] = \mathrm{Tr}[P] = 0\,,$$

so X, Y and Z are orthogonal to $\mathbb{1}$. Now, for two matrices $P, P' \in \{X, Y, Z\}$ and $P \neq P'$, we can use that $P^\dagger \cdot P' = P \cdot P' \propto P''$ where P'' is the third matrix from $\{X, Y, Z\}$. Here we also used the Hermicity of the Pauli matrices, that is $P^\dagger = P$. With that at hand, we can conclude that

$$\mathrm{Tr}[P^\dagger \cdot P'] \propto \mathrm{Tr}[P''] = 0\,.$$

With this have that the set of normalized single-qubit Pauli matrices are mutually orthogonal, and thus form an orthonormal basis.

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* $\mathrm{Tr}[BD]$*?*

Solution

We use the fact that the inner product of tensor products factorizes, that is

$$\mathrm{Tr}\left[(A\otimes B)(C\otimes D)\right] = \mathrm{Tr}[AC]\,\mathrm{Tr}[BD]\,.$$

With that, normalization and orthogonality follow from (a) as follows: Let us consider a Pauli string $P = P_1 \otimes P_2 \otimes \ldots P_n$ with $P_i \in \left\{\frac{1}{\sqrt{2}}\mathbb{1}_2, \frac{1}{\sqrt{2}}X, \frac{1}{\sqrt{2}}Y, \frac{1}{\sqrt{2}}Z\right\}$. Then

$$\mathrm{Tr}[P^\dagger P] = \prod_{i=1}^{n} \frac{1}{2}\,\mathrm{Tr}[P_i^\dagger P_i] = \frac{1}{2^n}\,\mathrm{Tr}[\mathbb{1}]^n = 1\,.$$

Now let us consider two such Pauli strings P and P'.

$$\mathrm{Tr}[P^\dagger P'] = \prod_{i=1}^{n} \frac{1}{2}\,\mathrm{Tr}[P_i^\dagger P_i']$$

From (a) we see that this is only 1 if $P_i = P_i'$ for all i. However, if for any i we have that $P_i \neq P_i'$ then there is a 0 in the product, resulting in $\mathrm{Tr}[P^\dagger P'] = 0$. With this we can conclude that the set of normalized Pauli strings form an ONB for $\mathbb{C}^{2^n\times 2^n}$.

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.

Solution

$$\begin{aligned} U_{k\ell}U_{k'\ell'} &= \left(\sum_{j=0}^{d-1} \zeta^{j\ell} |k+j\rangle\langle j|\right)\left(\sum_{j'=0}^{d-1} \zeta^{j'\ell'} |k'+j'\rangle\langle j'|\right) \\ &= \sum_{j,j'=0}^{d-1} \zeta^{j\ell}\zeta^{j'\ell'}\delta_{j,k'+j'} |k+j\rangle\langle j'| \\ &= \sum_{j'=0}^{d-1} \zeta^{(j'+k')\ell+j'\ell'} |k+k'+j'\rangle\langle j'| \\ &= \zeta^{\ell k'} \sum_{j=0}^{d-1} \zeta^{j(\ell+\ell')} |k+k'+j\rangle\langle j| \,, \end{aligned}$$

were in the last step we renamed the index j' to j to match the original definition. By inspection one can recognize that the final sum is indeed $U_{k+k',\ell+\ell'}$.

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)

Solution

First, observe that $U_{00} = \sum_{j=0}^{d-1} |j\rangle\langle j| = \mathbb{1}_d$. By definition of the inverse, this means that $U_{k\ell}^{-1}$ is the unique matrix satisfying

$$U_{k\ell}U_{k\ell}^{-1} = \mathbb{1} = U_{00}$$

From (i) we have that $U_{k\ell}U_{k'\ell'} = \zeta^{\ell k'} U_{k+k',\ell+\ell'}$. For this to be proportional to the identity, we need to have $k' = -k$ and $\ell' = -\ell$. Then,

$$U_{k\ell}U_{k'\ell'} = U_{k\ell}U_{-k,-\ell} = \zeta^{-\ell k} U_{00} \quad \Leftrightarrow \quad U_{k\ell}\zeta^{\ell k} U_{-k,-\ell} = \mathbb{1}_d \,.$$

So, $U_{k\ell}^{-1} = \zeta^{\ell k} U_{-k,-\ell}$.

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

Solution

Variant 1: By (b), $U_{k\ell}^{-1} = \zeta^{k\ell} U_{-k,-\ell}$. Now note that

$$\begin{aligned} U_{k\ell}^{\dagger} &= \sum_{j=0}^{d-1} \bar{\zeta}^{j\ell} |j\rangle\langle k+j| \\ &= \sum_{j=0}^{d-1} \bar{\zeta}^{(j-k)\ell} |j-k\rangle\langle j| \\ &= \bar{\zeta}^{-k\ell} \sum_{j=0}^{d-1} \bar{\zeta}^{j\ell} |j-k\rangle\langle j| \\ &= \zeta^{k\ell} \sum_{j=0}^{d-1} \zeta^{-j\ell} |j-k\rangle\langle j| \\ &= \zeta^{k\ell} U_{-k,-\ell} \\ &= U_{k\ell}^{-1} \,. \end{aligned}$$

This shows unitarity.
If the second equation (the change from j to $j-k$) is not obvious, consider that

$$\sum_{j=0}^{d-1} \bar{\zeta}^{j\ell} |j\rangle\langle k+j| = \left(\sum_{j=0}^{d-1} \bar{\zeta}^{j\ell} |j\rangle\langle j| \right) \left(\sum_{j'=0}^{d-1} |j'\rangle\langle k+j'| \right) .$$

Then, looking at the second term, and remembering that the sum is performed modulo d, we have that we can shift the index j' inside the sum, so $\sum_{j'=0}^{d-1} |j'\rangle\langle k+j'| = \sum_{j'=0}^{d-1} |j'-k\rangle\langle j'|$. It is essentially changing which is the first or last element, from

$$|0\rangle\langle k| + |1\rangle\langle k+1| + \cdots + |d-1-k\rangle\langle d-1| + |d-k\rangle\langle 0| + \cdots + |d-1\rangle\langle k-1|$$

to

$$|-k+(d-1)\rangle\langle d-1| + |-k+1+(d-1)\rangle\langle 0| + \cdots + |d-1\rangle\langle k-1| + |0\rangle\langle k| + |1\rangle\langle k+1| + \ldots$$

which is irrelevant. Now putting things back together,

$$\left(\sum_{j=0}^{d-1} \bar{\zeta}^{j\ell} |j\rangle\langle j| \right) \left(\sum_{j'=0}^{d-1} |j'-k\rangle\langle j'| \right) = \sum_{j'=0}^{d-1} \bar{\zeta}^{(j'-k)\ell} |j'-k\rangle\langle j'| \,.$$

Solution

Variant 2: An operator U is unitary if $U^\dagger U = \mathbb{1}$. For the Heisenberg-Weyl operators we have

$$\begin{aligned} U_{k\ell}^\dagger U_{k\ell} &= \left(\sum_{j=0}^{d-1} \zeta^{j\ell} |k+j\rangle\langle j|\right)^\dagger \left(\sum_{j'=0}^{d-1} \zeta^{j'\ell} |k+j'\rangle\langle j'|\right) \\ &= \sum_{j,j'=0}^{d-1} \overline{\zeta^{j\ell}} \zeta^{j'\ell} |j\rangle\langle k+j|k+j'\rangle\langle j'| \\ &= \sum_{j=0}^{d-1} \bar{\zeta}^{j\ell} \zeta^{j\ell} |j\rangle\langle j| \\ &= \sum_{j=0}^{d-1} |j\rangle\langle j| \\ &= \mathbb{1}. \end{aligned}$$

In the third equation we used that $\langle k+j|k+j'\rangle = \delta_{j,j'}$ and in the fourth we applied the definition of ζ such that $\bar{\zeta} = \zeta^{-1}$.

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).*

Solution

We first show that $\mathrm{Tr}[U_{k,l}] = d\delta_{k,0}\delta_{l,0}$. Again, remember that $U_{00} = \mathbb{1}$, so $\mathrm{Tr}[U_{00}] = d$. In contrast, if $k \neq 0$, then $\mathrm{Tr}[U_{kl}] = 0$ since it has only off-diagonal elements. Also, $\mathrm{Tr}[U_{0\ell}] = \sum_{j=0}^{d-1} e^{2\pi i j\ell/d} = d\delta_{\ell,0}$. So we have that $\mathrm{Tr}[U_{k,l}] = d\delta_{k,0}\delta_{l,0}$.
Now, we can use that $U_{k\ell}^{-1} = \zeta^{k\ell} U_{-k,-\ell}$ (by (b)). On the other hand, unitarity (from (c)) gives us that $U_{k\ell}^\dagger = U_{k\ell}^{-1}$. Putting things together, $U_{k\ell}^\dagger = \zeta^{k\ell} U_{-k,-\ell}$. Now we use that $U_{k\ell}U_{k'\ell'} = \zeta^{\ell k'} U_{k+k',\ell+\ell'}$ (by (a)) to obtain

$$U_{k\ell}^\dagger U_{k'\ell'} = \zeta^{k\ell} U_{-k,-\ell} U_{k'\ell'} = \zeta^{k\ell}\zeta^{-\ell k'} U_{k'-k,\ell'-\ell}\,.$$

Finally,

$$\mathrm{Tr}[U_{k\ell}^\dagger U_{k'\ell'}] = \zeta^{\ell(k-k')}\,\mathrm{Tr}[U_{k'-k,\ell'-\ell}] = \zeta^{\ell(k-k')} d\delta_{k,k'}\delta_{\ell,\ell'} = d\delta_{k,k'}\delta_{\ell,\ell'}\,.$$

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.

Solution

From the previous question, we see that the set $\{U_{k\ell}\}_{k,\ell=0}^{d-1}$ is orthogonal. Furthermore, the squared norm of $U_{k\ell}$ with respect to the Hilbert-Schmidt inner product is d. Consequently, the set $\{\frac{1}{\sqrt{d}} U_{k\ell}\}_{k,\ell=0}^{d-1}$ forms an orthonormal basis.

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)?

Solution

For $n = 1$ we have

$$\begin{aligned} U_{00} &= |0\rangle\langle 0| + |1\rangle\langle 1| &&= \mathbb{1}_2 \\ U_{01} &= |0\rangle\langle 0| + e^{2\pi i/2}|1\rangle\langle 1| &&= Z \\ U_{10} &= |1\rangle\langle 0| + |0\rangle\langle 1| &&= X \\ U_{11} &= |1\rangle\langle 0| + e^{i\pi}|0\rangle\langle 1| &&= -iY\,, \end{aligned}$$

so for $n = 1$ the bases coincide up to global phases. For $n > 1$ however, one has

$$U_{01} = \sum_{j=0}^{d-1} \zeta^j |j\rangle\langle j| = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \zeta & 0 & \dots & 0 \\ 0 & 0 & \zeta^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \zeta^{d-1} \end{pmatrix}$$

and

$$U_{10} = \sum_{j=0}^{d-1} |j+1\rangle\langle j| = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}\,.$$

These are known as the clock and shift operators respectively, and are not part of the n-qubit Pauli string basis, not even up to global phases. For U_{01}, this can be seen as follows: The entries of the single-qubit Paulis are $0, \pm 1, \pm i$. Hence, the entries of a Pauli string are products thereof, so again $0, \pm 1, \pm i$. Therefore, for $n > 2$, a Pauli string cannot have all the powers of $\zeta = e^{2i\pi/2^n}$ among its entries, not even up to a global phase. For U_{10}, just observe that it is not Hermitian. As tensor products of Hermitian matrices (like Pauli matrices) are Hermitian, U_{10} can not be a Pauli string. It can also not be a Pauli string up to a global phase, since if we had that $U_{10} = e^{i\varphi}P$ then we would have

$$U_{10}^\dagger = e^{-i\varphi}P^\dagger = e^{-i\varphi}P = e^{-2i\varphi}U_{10}\,.$$

So the diagonal shifted upwards by 1 should also have non-zero elements, which is not the case.

Total Points: 21 (+5)