Quantum Computing CO484

Tutorial*

Sheet 1 - Answers

Exercise 1 *Consider a single qubit system, i.e. a system with* $\mathcal{H} = \mathbb{C}^2$.

(i) Does the following matrix represent an observable *on* $\mathbb{C}^2$

$$\mathbf{A}_1 = \begin{pmatrix} 3 & 0 \\ 0 & 7 \end{pmatrix}?$$

What are its eigenbase vectors and eigenvalues?

(ii) Construct an observable $\mathbf{A}_2$ *(i.e. it's matrix representation) on* $\mathbb{C}^2$ *which has eigenvalues* $\{+1, -1\}$ *and eigenvectors*

$$\{\frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(-1,1)\}.$$

(iii) What happens if you measure either of the two observables $\mathbf{A}_1$ *and* $\mathbf{A}_2$ *in the state* $|x\rangle = \frac{1}{\sqrt{2}}(1,-1)$*? Sketch the situation geometrically.*

Note: The em outer product $|x\rangle\langle y|$ *for vectors* $|x\rangle = (x_1, \ldots, x_n)^T$ *and* $\langle y| = (y_1, \ldots, y_n)$ *is an operator/matrix:* $(|x\rangle\langle y|)_{ij} = x_i y_j$*. It could be treated just as a formal combination of a ket and a bra vector.*

Solution

(i) Yes, this is an observable (it is self-adjoint). Eigenvectors are the standard base vectors $|0\rangle = (1,0)$ and $|1\rangle = (0,1)$ and the corresponding eigenvalues are 3 and 7.

*Based partly on the tutorials by Abbas Edalat.

(ii) In the base $\{\frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(-1,1)\}$ the matrix $\mathbf{A}_2$ is represented by

$$\mathbf{A}_2 = \begin{pmatrix} +1 & 0 \\ 0 & -1 \end{pmatrix}$$

In the standard base it with $|+\rangle = \frac{1}{\sqrt{2}}(1,1)$ and $|-\rangle = \frac{1}{\sqrt{2}}(-1,1)$ it could be constructed with

$$|+\rangle\langle+| = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix}(1 \;\; 1) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$|-\rangle\langle-| = \frac{1}{2}\begin{pmatrix} -1 \\ 1 \end{pmatrix}(-1 \;\; 1) = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

so we get

$$(+1\cdot\frac{1}{2})\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + (-1\cdot\frac{1}{2})\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

(iii) If we measure $\mathbf{A}_1$ in state $|x\rangle = \frac{1}{\sqrt{2}}(1,-1)$ we will measure either 3 or 7, the probability of either is 0.5 (as this is the inner product $\langle 0|x\rangle = \langle 1|x\rangle$.

Measuring $\mathbf{A}_2$ in $|x\rangle = \frac{1}{\sqrt{2}}(1,-1)$ results in the potential measurement results $+1$ and -1. However as $|+\rangle$ is *orthogonal* to $|x\rangle$ we have probability $0 = \langle+|x\rangle$ to see $+1$ but we will get -1 with probability $1 = \langle-|x\rangle$.

Exercise 2 *Consider the complex numbers* $\mathbb{C}$.

(i) Show that for complex numbers x and y we have: $|x+y|^2 = |x|^2 + |y|^2 + 2Re(x^*y)$.

(ii) Compare x^*x with x^2 for a complex number x and explain why the inner product of two complex vectors $v, w \in \mathbb{C}^d$ is defined as $v^\dagger w$ rather than $v^T w$.

Solution Based on the arithmetic rules in $\mathbb{C}$ we have:

(i) Let $x = x_1 + ix_2$ and $y = y_1 + iy_2$. Then $x + y = x_1 + y_1 + i(x_2 + y_2)$. Hence,

$$\begin{aligned} |x+y|^2 &= (x_1+y_1)^2 + (x_2+y_2)^2 = \\ &= (x_1^2 + x_2^2) + (y_1^2 + y_2^2) + 2(x_1y_1 + x_2y_2) = \\ &= |x|^2 + |y|^2 + 2\mathrm{Re}(x^*y), \end{aligned}$$

since $\mathrm{Re}(x^*y) = \mathrm{Re}[(x_1 - iy_1)(x_2 + iy_2)] = x_1x_2 + y_1y_2$.

(ii) x^*x is always a non-negative real number, the length of the complex number x, whereas x^2 is in general a complex number. Since we would like $\langle v, v\rangle$ to give us the length of the complex vector v, we need to use $v^\dagger$ in the definition of the inner product $\langle v, w\rangle = v^\dagger w$ to get we a non-negative real number.

Exercise 3 *Complex numbers (again)*

(i) Give the cartesian representation of (in polar coordinates) the following complex numbers $(1, \frac{\pi}{4})$, $(1, \frac{\pi}{2})$ *and* $(1, \pi)$.

(ii) What is $1^{\frac{1}{4}}$*?*

(iii) Proof **De Moivre's formula***:* $(e^{i\theta})^n = \cos(n\theta) + i\sin(n\theta)$

Solution

(i) $\sin(\frac{\pi}{4}) + i\cos(\frac{\pi}{4})$, i, and -1.

(ii) $1^{\frac{1}{4}} = \sqrt[4]{1} = \{1, -1, -i, i\}$ or $\{e^{ik\frac{\pi}{2}}\}_{k=0,1,2,3}$.

(iii) We know that $e^{i\theta} = \cos(\theta) + i\sin(\theta)$, geometrically or in polar coordinates, the multiplication of two complex numbers corresponds to an addition of the angels and multiplication of radiuses (here $r = 1$).

Therefore: $e^{i\theta}e^{i\theta} = e^{2i\theta} = \cos(2\theta) + i\sin(2\theta)$ etc.

Exercise 4 *Generalise the following notions and properties given for the vector space* $\mathbb{R}^2$ *to* $\mathbb{R}^d$.

(i) Define linear independence and linear dependence of vectors in $\mathbb{R}^d$.

(ii) What is the least integer n *such that any set of* n *vectors in* $\mathbb{R}^d$ *will be linearly dependent?*

(iii) What is a basis of $\mathbb{R}^d$*? How many linearly independent vectors it takes to get a basis for* $\mathbb{R}^d$*?*

(iv) Define the notion of an orthonormal *basis for* $\mathbb{R}^d$*. What would be the* standard *basis of* $\mathbb{R}^d$*?*

Solution

(i) Same definition as in $\mathbb{R}^2$: the vectors

$$\{v_i \in \mathbb{R}^d \mid i = 1, 2, \ldots, k\}$$

are *linearly independent* if whenever

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0$$

for $a_i \in \mathbb{R}$ $(i = 1, \ldots, k)$ then $a_i = 0$ for all $i = 1, \ldots, k$. Otherwise they are called linearly dependent.

(ii) $d + 1$.

(iii) A basis of $\mathbb{R}^d$ is any set of linearly independent vectors in $\mathbb{R}^d$ such that any vector in $\mathbb{R}^d$ can be expressed as a linear combination of vectors in the set. Any d linearly independent vectors in $\mathbb{R}^d$ form a basis.

(iv) A basis $\{v_i \mid 1 \leq i \leq d\}$ is an orthonormal basis if $v_i \cdot v_i = 1$, for $1 \leq i \leq d$ and $v_i \cdot v_j = 0$ for $i \neq j$. The standard basis of $\mathbb{R}^d$ consists of the d vectors v_i, $1 \leq i \leq d$, such that all entries of the column vector v_i are 0 except the ith entry which is 1.

Exercise 5 *Generalise the following notions and properties given for the vector space $\mathbb{C}^2$ to $\mathbb{C}^d$.*

(i) Define the norm $\|w\|$ of a vector and the inner product of two vectors w_1 and w_2 in $\mathbb{C}^d$. What is the dual of a vector w in $\mathbb{C}^d$ and what can it be identified with?

(ii) Define linear independence and linear dependence of vectors in $\mathbb{C}^d$.

(iii) What is the least integer n such that any set of n vectors in $\mathbb{C}^d$ will be linearly dependent?

(iv) What is a basis of $\mathbb{C}^d$? How many linearly independent vectors it takes to get a basis for $\mathbb{C}^d$?

(v) Define the notion of an orthonormal *basis for $\mathbb{C}^d$. What would be the* standard *basis of $\mathbb{C}^d$?*

Solution The notions can be generalised simply as follows:

(i) The norm of a vector w with $w^T = (w_1, w_2, \ldots, w_d)$ is $\|w\| = \sqrt{\sum_{j=1}^{d} |w_j|^2}$.

The inner product of the two vectors w_1 and w_2 with $w_1^T = (w_{11}, w_{12}, \ldots, w_{1d})$ and $w_2^T = (w_{21}, w_{22}, \ldots, w_{2d})$ is $\langle w_1, w_2 \rangle = \sum_{j=1}^{d} w_{1j}^* w_{2j}$.

The dual of w is the linear map $L_w : \mathbb{C}^d \to \mathbb{C}$ defined by $L_w(v) = (w, v) = w^\dagger v$ and can be identified with $w^\dagger$.

(ii) Exactly as in $\mathbb{C}^2$.

(iii) $d + 1$.

(iv) A basis of $\mathbb{C}^d$ is any set of linearly independent vectors in $\mathbb{C}^d$ such that any vector in $\mathbb{C}^d$ can be expressed as a linear combination of vectors in the set. Any d linearly independent vectors in $\mathbb{C}^d$ form a basis.

(v) A basis $\{w_i \mid 1 \leq i \leq d\}$ is is an orthonormal basis if $(w_i, w_i) = 1$, for $1 \leq i \leq d$ and $(w_i, w_j) = 0$ for $i \neq j$.

Exercise 6 *Show that the two vectors w_1 and w_2 in $\mathbb{C}^4$ with $w_1^T = \frac{1}{2}(1, 1, 1, 1)$ and $w_2^T = \frac{1}{2}(1, -1, 1, -1)$ are orthogonal unit vectors. Find vectors w_3 and w_4 such that the collection $\{w_1, w_2, w_3, w_4\}$ forms an orthonormal basis for $\mathbb{C}^4$.*

Solution $\|w_1\| = \sqrt{\frac{1^2+1^2+1^2+1^2}{4}} = 1$ and $\|w_2\| = \sqrt{\frac{1^2+(-1)^2+1^2+(-1)^2}{4}} = 1$.

Also $(w_1, w_2) = \frac{1-1+1-1}{4} = 0$. To find $w_3 = (a, b, c, d)$ and $w_4 = (e, f, g, h)$ we need to solve:

(i) $(w_1, w_3) = a + b + c + d = 0$,

(ii) $(w_1, w_4) = e + f + g + h = 0$,

(iii) $(w_2, w_3) = a - b + c - d = 0$,

(iv) $(w_2, w_4) = e - f + g - h = 0$,

(v) $(w_3, w_4) = ae + bf + cg + dh = 0$,

(vi) $\|w_3\|^2 = a^2 + b^2 + c^2 + d^2 = 1$ and

(vii) $\|w_4\|^2 = e^2 + f^2 + g^2 + h^2 = 1$.

These are seven equations with eight unknowns. Therefore, there are an infinite number of solutions. By inspection, we see that $w_3 = \frac{1}{\sqrt{2}}(1, 0, -1, 0)$ and $w_4 = \frac{1}{\sqrt{2}}(0, 1, 0, -1)$ is one particularly simple solution.

Exercise 7 *Linear Maps*

(i) Show that composition of two linear maps (on $\mathbb{C}^2$) is again linear.

(ii) Show that if $\mathbf{L}_1, \mathbf{L}_2 : \mathbb{C}^2 \to \mathbb{C}^2$ are linear, so is $\alpha_1\mathbf{L}_1 + \alpha_2\mathbf{L}_2 : \mathbb{C}^2 \to \mathbb{C}^2$ defined by

$$(\alpha_1\mathbf{L}_1 + \alpha_2\mathbf{L}_2)(v) = \alpha_1\mathbf{L}_1(v) + \alpha_2\mathbf{L}_2(v).$$

(iii) Show that for $|\psi\rangle, |\phi\rangle \in \mathbb{C}^2$, the map $|\psi\rangle\langle\phi| : \mathbb{C}^2 \to \mathbb{C}^2$ defined, using the bracket notation, by $|\psi\rangle\langle\phi|(|x\rangle) = \langle\phi|x\rangle\,|\psi\rangle$ is linear.

Solution

(i) Let $\mathbf{L} : \mathbb{C}^2 \to \mathbb{C}^2$ and $\mathbf{L}' : \mathbb{C}^2 \to \mathbb{C}^2$ be linear maps. Then $\mathbf{L} \circ \mathbf{L}' : \mathbb{C}^2 \to \mathbb{C}^2$ and $\mathbf{L} \circ \mathbf{L}'(a_1v_1 + a_2v_2) = \mathbf{L}(\mathbf{L}'(a_1v_1 + a_2v_2)) = \mathbf{L}(a_1\mathbf{L}'(v_1) + a_2\mathbf{L}'(v_2)) = a_1\mathbf{L}(\mathbf{L}'(v_1)) + a_2\mathbf{L}(\mathbf{L}'(v_2)) = a_1\mathbf{L} \circ \mathbf{L}'(v_1) + a_2\mathbf{L} \circ \mathbf{L}'(v_2)$.

(ii) This follows step by step from the definitions: $(\alpha_1\mathbf{L}_1 + \alpha_2\mathbf{L}_2)(a_1v_1 + a_2v_2) = \alpha_1\mathbf{L}_1(a_1v_1 + a_2v_2) + \alpha_2\mathbf{L}_2(a_1v_1 + a_2v_2) = (\alpha_1a_1\mathbf{L}_1(v_1) + \alpha_1a_2\mathbf{L}_1(v_2)) + (\alpha_2a_1\mathbf{L}_2(v_1) + \alpha_2a_2\mathbf{L}_2(v_2)) = a_1(\alpha_1\mathbf{L}_1 + \alpha_2\mathbf{L}_2)(v_1) + a_2(\alpha_1\mathbf{L}_1 + \alpha_2\mathbf{L}_2)(v_2)$.

(iii) This is a consequence of the linearity of the dual $\langle\phi|$ of the vector $|\phi\rangle$:
$|\psi\rangle\langle\phi|(\alpha\,|x\rangle + \beta\,|y\rangle) = (\alpha\,\langle\phi|x\rangle + \beta\,\langle\phi|y\rangle)\,|\psi\rangle = \alpha\,|\psi\rangle\langle\phi|(|x\rangle) + \beta\,|\psi\rangle|\phi\rangle(|y\rangle)$.

Exercise 8 *Show that the matrix representation of the* NOT *gate – i.e. a linear map on $\mathbb{C}^2$ which maps $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$ – in the basis $|0\rangle$, $|1\rangle$ is given by*

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

What is its matrix representation in the basis $|+\rangle$, $|-\rangle$?

Solution We have $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$. Hence,

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

is the matrix representation.

We have $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Hence, $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ and $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$. Therefore, the matrix for the change of basis is

$$\mathbf{B} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ and } \mathbf{B}^{-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Hence the matrix representation of NOT in the new basis is:

$$\mathbf{B}\mathbf{X}\mathbf{B}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Exercise 9 *Unitary Maps and Matrices*

(i) Check that a matrix (in computational basis) is unitary iff its columns (or its rows) form an orthonormal *basis.*

(ii) Check: the matrix for a change in the computational basis is unitary.

(iii) Show that $(\mathbf{AB})^\dagger = \mathbf{B}^\dagger\mathbf{A}^\dagger$ *and deduce that if a linear map has a unitary matrix representation, then its matrix representation in any computational basis is unitary.*

Solution

(i) If $\mathbf{U}$ is unitary then $\mathbf{U}^\dagger\mathbf{U} = \mathbf{I}$ and $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I}$ where $\mathbf{I}$ is the identity matrix. The first equality tells us that the columns of $\mathbf{U}$ form an orthonormal basis and the second equality says that the rows of $\mathbf{U}$ form an orthonormal basis. Conversely, suppose that the columns of $\mathbf{U}$ form an orthonormal basis. Then $\mathbf{U}^\dagger\mathbf{U} = \mathbf{I}$ and hence $\mathbf{U}^\dagger = \mathbf{U}^{-1}$. Similarly if the rows of $\mathbf{U}$ form an orthonormal basis. Then $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I}$ and hence $\mathbf{U}^\dagger = \mathbf{U}^{-1}$.

(ii) Let $\delta_{mi} = 1$ if $m = i$ and 0 otherwise. Suppose $|w_j\rangle \in \mathbb{C}^d$ (for $j = 1, \ldots, d$) and $|v_j\rangle \in \mathbb{C}^d$ (for $j = 1, \ldots, d$) are computational basis with $\mathbf{B} = (b_{ij})$ as the matrix for the change of basis:

$$|w_i\rangle = \sum_k b_{ki} |v_k\rangle \quad \text{and thus} \quad \langle w_m| = \sum_t b^*_{tm} \langle v_t| .$$

Thus we have: $\delta_{mi} = \langle w_m|w_i\rangle = \sum_{k,t} b^*_{tm} b_{ki} \langle v_t|v_k\rangle = \sum_{k,t} b^*_{tm} b_{ki} \delta_{tk} = \sum_k b^*_{km} b_{ki}$. This shows that the columns of $\mathbf{B}$ form an orthonormal basis. Hence, $\mathbf{B}$ is unitary.

(iii) Note that $(\mathbf{AB})^T = \mathbf{B}^T\mathbf{A}^T$ since $((\mathbf{AB})^T)_{ij} = (\mathbf{AB})_{ji} = \sum_m \mathbf{A}_{jm}\mathbf{B}_{mi} = \sum_m \mathbf{B}_{mi}\mathbf{A}_{jm} = \sum_m (\mathbf{B}^T)_{im}(\mathbf{A}^T)_{mj} = (\mathbf{B}^T\mathbf{A}^T)_{ij}$. Furthermore, since for complex numbers x and y we have $(xy)^* = x^*y^*$, it follows that $(\mathbf{AB})^\dagger = ((\mathbf{AB})^T)^* = (\mathbf{B}^T\mathbf{A}^T)^* = (\mathbf{B}^T)^*(\mathbf{A}^T)^* = \mathbf{B}^\dagger\mathbf{A}^\dagger$.

Now assume a linear map has a unitary matrix representation $\mathbf{U}$, i.e. $\mathbf{U}^\dagger = \mathbf{U}^{-1}$. Suppose we have a different basis with $\mathbf{B}$ the matrix of the change of basis. Then the matrix representation in the new basis is $\mathbf{BUB}^{-1} = \mathbf{BUB}^\dagger$ since the matrix for a change in basis is unitary by part (ii). We have: $(\mathbf{BUB}^\dagger)^\dagger = (\mathbf{B}^\dagger)^\dagger\mathbf{U}^\dagger\mathbf{B}^\dagger = \mathbf{BU}^{-1}\mathbf{B}^\dagger$. The result follows as the latter is the inverse of $\mathbf{BUB}^{-1}$.

Exercise 10 *Show that* $\langle u|\mathbf{A}v\rangle = \langle \mathbf{A}^\dagger u|v\rangle$*.Deduce that a matrix* $\mathbf{M}$ *is* unitary *iff it preserves all inner products, i.e. iff* $\langle \mathbf{M}u|\mathbf{M}v\rangle = \langle u|v\rangle$ *for all* $u, v \in \mathbb{C}^2$*.*

Solution $\langle u|\mathbf{A}v\rangle = \sum_i u_i^*(\mathbf{A}v)_i = \sum_i u_i^* \sum_j \mathbf{A}_{ij}v_j = \sum_i \sum_j (\mathbf{A}^T)_{ji}u_i^*v_j = \sum_i \sum_j ((\mathbf{A}^T)^*)_{ji}^* u_i^* v_j = \sum_i \sum_j (\mathbf{A}^\dagger)_{ji}^* u_i^* v_j = \sum_j ((\mathbf{A}^\dagger u)_j)^* v_j = \langle \mathbf{A}^\dagger u|v\rangle$.

Now, if $\mathbf{M}$ is unitary then $\langle \mathbf{M}u|\mathbf{M}v\rangle = \langle \mathbf{M}^\dagger\mathbf{M}u|v\rangle = \langle u|v\rangle$. On the other hand, suppose $\langle \mathbf{M}u|\mathbf{M}v\rangle = \langle u|v\rangle$ for all $u, v \in \mathbb{C}^2$, then $\langle u|\mathbf{M}^\dagger\mathbf{M}v\rangle = \langle u|v\rangle$ for all $u, v \in \mathbb{C}^2$.

Suppose $(\mathbf{M}^\dagger\mathbf{M})_{ii} \neq 1$ for some i, then $\langle i|\,\mathbf{M}^\dagger\mathbf{M}\,|i\rangle = \langle i|\,(\mathbf{M}^\dagger\mathbf{M})_{ii}\,|i\rangle = (\mathbf{M}^\dagger\mathbf{M})_{ii} \neq 1 = \langle i|i\rangle$. Hence, $(\mathbf{M}^\dagger\mathbf{M})_{ii} = 1$ for all i. Similarly, suppose $(\mathbf{M}^\dagger\mathbf{M})_{ij} \neq 0$ for some $i \neq j$, then $\langle i|\,\mathbf{M}^\dagger\mathbf{M}\,|j\rangle = \langle i|\,(\mathbf{M}^\dagger\mathbf{M})_{ij}\,|j\rangle = (\mathbf{M}^\dagger\mathbf{M})_{ij} \neq 0 = \langle i|j\rangle$. Hence, $(\mathbf{M}^\dagger\mathbf{M})_{ij} = 0$ for all $i \neq j$.

Exercise 11 *Show that any unitary matrix* $\mathbf{U}$ *can be expressed as*

$$\mathbf{U} = \begin{pmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\gamma/2 & -e^{i(\alpha-\beta/2+\delta/2)}\sin\gamma/2 \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\gamma/2 & e^{i(\alpha+\beta/2+\delta/2)}\cos\gamma/2 \end{pmatrix}$$

where α*,* β*,* δ *and* γ *are real numbers.*

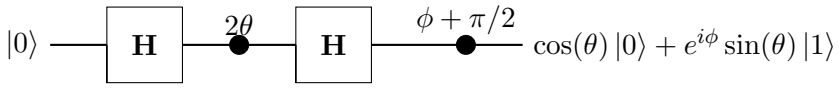
Solution Let $\mathbf{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Since the rows (respectively, the columns) must form unit vectors, we can put:

$$a = e^{iA}\cos\frac{\gamma}{2},\ b = e^{iB}\sin\frac{\gamma}{2},\ c = -e^{iC}\sin\frac{\gamma}{2},\ d = e^{iD}\cos\frac{\gamma}{2}.$$

Now, the two columns must be orthogonal, hence: $-A+C = -B+D$. Now let $\alpha = (A+D)/2$, $\beta = D - C$ and $\delta = -A + C = -B + D$. Then, we get:

$$\begin{aligned} 2A &= 2\alpha - \delta - \beta \quad & 2C &= 2\alpha - \beta + \delta \\ 2D &= 2\alpha + \beta + \delta \quad & 2B &= 2D - 2\delta = 2\alpha + \beta - \delta. \end{aligned}$$

Exercise 12 *Verify the output, up to a global phase, of the following:*



Solution Evaluate the quantum circuit step by step:

$$\begin{aligned}
\mathbf{H}: \quad & |0\rangle && \mapsto && \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}. \\
2\theta: \quad & \begin{pmatrix} 1 \\ 1 \end{pmatrix} && \mapsto && \begin{pmatrix} 1 & 0 \\ 0 & e^{2i\theta} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ e^{2i\theta} \end{pmatrix} = e^{i\theta} \begin{pmatrix} e^{-i\theta} \\ e^{i\theta} \end{pmatrix}. \\
\mathbf{H}: \quad & \begin{pmatrix} e^{-i\theta} \\ e^{i\theta} \end{pmatrix} && \mapsto && \tfrac{1}{\sqrt{2}} \begin{pmatrix} e^{-i\theta} + e^{i\theta} \\ e^{-i\theta} - e^{i\theta} \end{pmatrix} = \sqrt{2} \begin{pmatrix} \cos\theta \\ -i\sin\theta \end{pmatrix}. \\
\phi + \pi/2: \quad & \begin{pmatrix} \cos\theta \\ -i\sin\theta \end{pmatrix} && \mapsto && \begin{pmatrix} \cos\theta \\ -ie^{i(\phi+\pi/2)}\sin\theta \end{pmatrix} = \begin{pmatrix} \cos\theta \\ e^{i\phi}\sin\theta \end{pmatrix}.
\end{aligned}$$