Homework set 5 - due 11/11/22

Math 444

This assignment contains a few remarks about matrix decomposition that are pertinent to the subject of quantum circuits. We won't get into details of quantum circuits here (see *Quantum Computations and Quantum Information* by Nielsen and Chuang for a nice exposition, particularly Chapter 4). I believe the material in this assignment would be a helpful preliminary work for placing the more standard expositions of quantum circuits in mathematical perspective.

1. Let the Hilbert space $\mathscr{H} = \mathbb{C}^N$ have the standard orthonormal basis. We write the basis elements in Dirac notation, so that $|j\rangle$ is the column vector consisting of 0 entries, except at position j where it is 1. We define the rank-1 matrix
$$E_{ij} := |i\rangle\langle j|.$$
   (a) If $N = 3$, write E_{23} as an ordinary 3×3-matrix.

   (b) For general N, show that $E_{ij}E_{k\ell} = \delta_{jk}E_{i\ell}$.

   (c) Let $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ be a 2×2-complex matrix and $i, j \in \{1, 2, \dots, N\}$, $i \neq j$. Define the $N\times N$-matrix
$$\varphi_{ij}(A) := I - E_{ii} - E_{jj} + a_{11}E_{ii} + a_{12}E_{ij} + a_{21}E_{ji} + a_{22}E_{jj}.$$
   Describe in words how this matrix is obtained from A.

   (d) Show that if A, B are 2×2-complex matrices then, for $i \neq j$,
      i. $\varphi_{ij}(I_2) = I_N$ $\quad$ (I_d is the identity matrix in dimension d);
      ii. $\varphi_{ij}(AB) = \varphi_{ij}(A)\varphi_{ij}(B)$;
      iii. $\varphi_{ij}(A+B) = \varphi_{ij}(A) + \varphi_{ij}(B) - (I_N - E_{ii} - E_{jj})$;
      iv. $\varphi_{ij}(\alpha A) = \alpha\varphi_{ij}(A) + (1-\alpha)\left(I - E_{ii} - E_{jj}\right)$ $\quad$ ($\alpha \in \mathbb{C}$);
      v. $\varphi_{ij}(A)^{\intercal} = \varphi_{ij}(A^{\intercal})$;
      vi. $\varphi_{ij}(\bar{A}) = \overline{\varphi_{ij}(A)}$.
      vii. $\varphi_{ij}(A^*) = \varphi_{ij}(A)^*$

   (e) Let us define $S_{ij} := \varphi_{ij}(X)$ where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. (Note that $S_{ij} = S_{ji}$.) Let U be any $N\times N$-complex matrix. Explain in words the effect on U of the operations $U \mapsto S_{ij}U$ and $U \mapsto US_{ij}$. (More specifically, what is being done to the rows and columns of U?)

   (f) Let i, j, k, ℓ be distinct integers between 1 and N. Show the following:
$$S_{ij}\varphi_{k\ell}(A)S_{ij} = \varphi_{k\ell}(A), \quad S_{ij}\varphi_{i\ell}(A)S_{ij} = \varphi_{j\ell}(A), \quad S_{ij}\varphi_{kj}(A)S_{ij} = \varphi_{ki}(A), \quad S_{ij}\varphi_{ij}(A)S_{ij} = \varphi_{ji}(A).$$
   (These are somewhat tedious identities to prove. I suggest that you do the last one; with a little thought, one can show it rather easily.)

2. For this exercise, we assume that all the matrices are unitary. The group $U(N)$ of unitary matrices in dimension N consists of all the $N \times N$-matrices whose columns (or rows) constitute an orthonormal basis of $\mathbb{C}^N$.

   (a) Argue that if $A, B \in U(N)$ then the matrices $A^* := \bar{A}^\intercal, \bar{A}, A^\intercal, A^{-1}, AB$ also lie in $U(N)$.

   (b) Argue that if the jth column of a unitary matrix consists of zeros except at position i, then the ith row consists of zeros except at position j.

   (c) Argue that if $A \in U(2)$ then $\varphi_{ij}(A) \in U(N)$.

   (d) Let $U \in U(N)$, $A \in U(2)$ and $i \neq j$. Show that

$$\varphi_{ij}(A)U = \sum_{k,\ell: k \neq i,j} u_{k\ell} E_{k\ell} + \sum_{\ell} (a_{11} u_{i\ell} + a_{12} u_{j\ell}) E_{i\ell} + \sum_{\ell} (a_{21} u_{i\ell} + a_{22} u_{j\ell}) E_{j\ell}.$$

   This operation on U can be described as follows. The kth row of $V := \varphi_{ij}(A)U$ is the same as the kth row of U if $k \neq i, j$; and for each ℓ,

$$\begin{pmatrix} v_{i\ell} \\ v_{j\ell} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} u_{i\ell} \\ u_{j\ell} \end{pmatrix}.$$

   (e) Let $U \in U(N)$. Suppose $u_{i\ell}$ and $u_{j\ell}$ are not both 0. Show that there exists $A \in U(2)$ such that $v_{j\ell} = 0$ where

$$V = \varphi_{ij}(A)U.$$

   By definition, the v_{ji} is the (j,i)-entry of the unitary matrix V.

   (f) Using the idea of row reduction based on the previous item, show that any element of $U(N)$ can be written as a product of unitary matrices of the form $\varphi_{ij}(A)$ for $i, j \in \{1, \ldots, N\}$ and $A \in U(2)$.

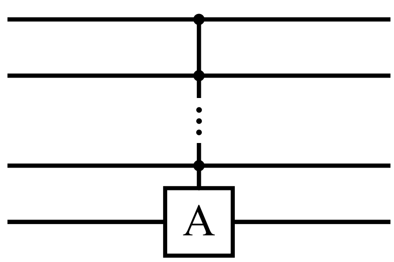

Figure 1: The control gate $C^{n-1}(A)$.

3. Let us now assume that $N = 2^n$. (So $\mathcal{H} = \left(\mathbb{C}^2\right)^{\otimes n}$ is the n-qubit Hilbert space.) We label the standard basis elements in base 2: $|a\rangle = |a_{n-1} \cdots a_0\rangle$ where $a_i \in \{0,1\}$ and $a = a_0 + a_1 2 + a_2 2^2 + \cdots + a_{n-1} 2^{n-1}$.

   (a) Given any two basis elements $|a\rangle, |b\rangle$, show that there is a sequence of basis elements $s_0 = a, s_1, \ldots, s_m = b$ such that any two consecutive elements s_i, s_{i+1} only differ at one binary digit. (Such a sequence is said to define a *Gray code*.) For example, if $a = 101001$ and $b = 110011$, then the sequence

$$|101001\rangle, \ |101011\rangle, \ |100011\rangle, \ |110011\rangle$$

   has this property.

   (b) Argue that any $\varphi_{ij}(A)$ can be written as a product of matrices, one of which being $\varphi_{1\cdots10,1\cdots11}(A)$ and all the others of the form $S_{k\ell}$ (as defined in Exercise 1) such that k and ℓ only differ in one binary digit. Note that $\varphi_{1\cdots10,1\cdots11}(A)$ is what was defined in class as the control gate $C^{n-1}(A)$, whose diagram is shown in Figure 1.

4. Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Let i, j be integers whose binary expansions differ in only one binary digit. Explain how $\varphi_{ij}(A)$ can be given the diagram representation shown in Figure 2. The circuit on the left contain control nodes of two types. The black dots represent 1 and the circles represent 0. When the control bits in the input are different from the values indicated by the two types of dots, the output is the same as the input. When the control bits are equal to the values indicated by the dots and the input is $|x_0 \ldots x_{n-1}\rangle$, the output is given by $|x_0 \cdots x_{i-1}\rangle \otimes A|i\rangle \otimes |x_{i+1} \cdots x_{n-1}\rangle$, where i is the position of the single bit gate A. You don't need to write this down.

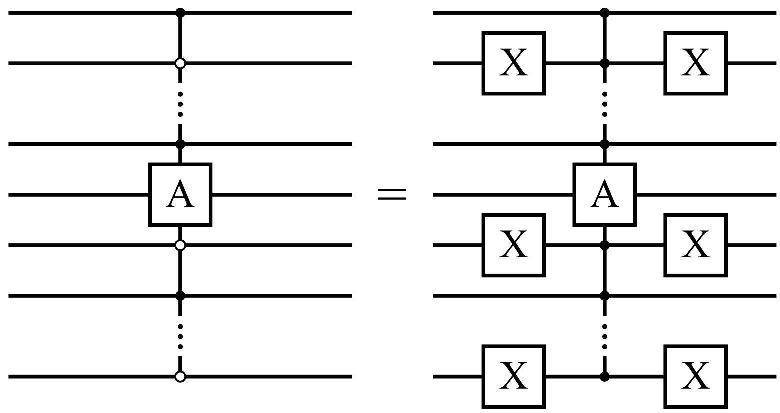

Figure 2: Diagram for Exercise 4.