QUANTUM ALGORITHMS
HOMEWORK 6 SELECTED SOLUTIONS

PROF. MATTHEW MOORE

6.5. a) Let $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Write the matrix of the operator $H[2]$ acting on the space $\mathfrak{B}^{\otimes 3}$.

b) Let U be an arbitrary two-qubit operator with matrix elements $u_{jk} = \langle j|\, U\, |k\rangle$, where $j, k \in \{00, 01, 10, 11\}$. Write the matrix for $U[3, 1]$.

Solution:

a): H is a one-qubit operator, so

$$H[2] \coloneqq I_{\mathfrak{B}^{\otimes 1}} \otimes H \otimes I_{\mathfrak{B}^{\otimes 1}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & 1 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & -1 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \cdot \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} & 0 \cdot \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} & 1 \cdot \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{pmatrix}.$$

Date: March 23, 2021.

b): We partition the matrix described in the problem into 2×2 matrices:

$$U = \begin{pmatrix} u_{00|00} & u_{00|01} & u_{00|10} & u_{00|11} \\ u_{01|00} & u_{01|01} & u_{01|10} & u_{01|11} \\ u_{10|00} & u_{10|01} & u_{10|10} & u_{10|11} \\ u_{11|00} & u_{11|01} & u_{11|10} & u_{11|11} \end{pmatrix} = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix}.$$

It follows that we have a representation of U as the sum of tensor produces of 2×2 matrices,

$$U = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes U_{00} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes U_{01} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes U_{10} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes U_{11},$$

so we have

$$\begin{aligned} U[3,1] = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} [3]\; U_{00}[1] + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} [3]\; U_{01}[1] & \\ + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} [3]\; U_{10}[1] + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} [3]\; U_{11}[1]. \end{aligned}$$

As in the previous part, we have

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} [3]\; U_{00}[1] &= \left(I_{\mathfrak{B}^{\otimes 2}} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right) \left(U_{00} \otimes I_{\mathfrak{B}^{\otimes 2}} \right) \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ &\quad \cdot \begin{pmatrix} u_{00|00} & 0 & 0 & 0 & u_{00|01} & 0 & 0 & 0 \\ 0 & u_{00|00} & 0 & 0 & 0 & u_{00|01} & 0 & 0 \\ 0 & 0 & u_{00|00} & 0 & 0 & 0 & u_{00|01} & 0 \\ 0 & 0 & 0 & u_{00|00} & 0 & 0 & 0 & u_{00|01} \\ u_{01|00} & 0 & 0 & 0 & u_{01|01} & 0 & 0 & 0 \\ 0 & u_{01|00} & 0 & 0 & 0 & u_{01|01} & 0 & 0 \\ 0 & 0 & u_{01|00} & 0 & 0 & 0 & u_{01|01} & 0 \\ 0 & 0 & 0 & u_{01|00} & 0 & 0 & 0 & u_{01|01} \end{pmatrix} \\ &= \begin{pmatrix} u_{00|00} & 0 & 0 & 0 & u_{00|01} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & u_{00|00} & 0 & 0 & 0 & u_{00|01} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ u_{01|00} & 0 & 0 & 0 & u_{01|01} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & u_{01|00} & 0 & 0 & 0 & u_{01|01} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \end{aligned}$$

Similarly,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} [3]\, U_{01}[1] = \begin{pmatrix} 0 & u_{00|10} & 0 & 0 & 0 & u_{00|11} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & u_{00|10} & 0 & 0 & 0 & u_{00|11} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & u_{01|10} & 0 & 0 & 0 & u_{01|11} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & u_{01|10} & 0 & 0 & 0 & u_{01|11} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} [3]\, U_{10}[1] = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ u_{10|00} & 0 & 0 & 0 & u_{10|01} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & u_{10|00} & 0 & 0 & 0 & u_{10|01} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ u_{11|00} & 0 & 0 & 0 & u_{11|01} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & u_{11|00} & 0 & 0 & 0 & u_{11|01} & 0 \end{pmatrix}, \qquad \text{and}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} [3]\, U_{11}[1] = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & u_{10|10} & 0 & 0 & 0 & u_{10|11} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & u_{10|10} & 0 & 0 & 0 & u_{10|11} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & u_{11|10} & 0 & 0 & 0 & u_{11|11} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & u_{11|10} & 0 & 0 & 0 & u_{11|11} \end{pmatrix}.$$

Adding these four matrices together gives us

$$U[3,1] = \begin{pmatrix} u_{00|00} & u_{00|10} & 0 & 0 & u_{00|01} & u_{00|11} & 0 & 0 \\ u_{10|00} & u_{10|10} & 0 & 0 & u_{10|01} & u_{10|11} & 0 & 0 \\ 0 & 0 & u_{00|00} & u_{00|10} & 0 & 0 & u_{00|01} & u_{00|11} \\ 0 & 0 & u_{10|00} & u_{10|10} & 0 & 0 & u_{10|01} & u_{10|11} \\ u_{01|00} & u_{01|10} & 0 & 0 & u_{01|01} & u_{01|11} & 0 & 0 \\ u_{11|00} & u_{11|10} & 0 & 0 & u_{11|01} & u_{11|11} & 0 & 0 \\ 0 & 0 & u_{01|00} & u_{01|10} & 0 & 0 & u_{01|01} & u_{01|11} \\ 0 & 0 & u_{11|00} & u_{11|10} & 0 & 0 & u_{11|01} & u_{11|11} \end{pmatrix}$$

AP 1. Prove that the inner product and the tensor product commute:

$$\langle \alpha \otimes \beta \mid \gamma \otimes \delta \rangle = \langle \alpha \mid \gamma \rangle \langle \beta \mid \delta \rangle .$$

This is asserted on page 57 of the textbook.

Solution:

Proof. In order for the inner product to be defined, α and γ must be elements of the same vector space, say $\mathbb{A}$. Likewise β and δ must be elements of the same vector space, say $\mathbb{B}$. Let

$\mathbb{A}$ and $\mathbb{B}$ have ordered basis

$$\{\tau_1, \ldots, \tau_n\} \qquad\qquad \{\sigma_1, \ldots, \sigma_m\}$$

respectively. We may furthermore assume that these bases are *orthonormal* (we either assume this, or define the inner product in terms of them so that they are). It follows that each of the vectors α, β, γ, δ have decompositions in terms of their respective bases, say

$$\alpha = \sum_{i=1}^{n} a_i\tau_i, \qquad \gamma = \sum_{i=1}^{n} c_i\tau_i, \qquad \beta = \sum_{i=1}^{m} b_i\sigma_i, \qquad \delta = \sum_{i=1}^{m} d_i\sigma_i.$$

for $a_i, c_i, b_i, d_i \in \mathbb{C}$. It follows that

$$\langle \alpha \mid \gamma \rangle = \sum_{i=1}^{n} a_i^* c_i \qquad\qquad \langle \beta \mid \delta \rangle = \sum_{i=1}^{m} b_i^* d_i$$

and hence

$$\langle \alpha \mid \gamma \rangle \langle \beta \mid \delta \rangle = \left(\sum_{i=1}^{n} a_i^* c_i\right)\left(\sum_{i=1}^{m} b_i^* d_i\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i^* c_i b_j^* d_j.$$

We now examine the tensors. From above and from bilinearity, we have

$$\alpha \otimes \beta = \left(\sum_{i=1}^{n} a_i\tau_i\right) \otimes \left(\sum_{i=1}^{m} b_i\sigma_i\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_i \tau_i \otimes \sigma_j \qquad \text{and}$$

$$\gamma \otimes \delta = \left(\sum_{i=1}^{n} c_i\tau_i\right) \otimes \left(\sum_{i=1}^{m} d_i\sigma_i\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} c_i d_i \tau_i \otimes \sigma_j.$$

Using the bilinearity of the inner product, this yields

$$\begin{aligned}\langle \alpha \otimes \beta \mid \gamma \otimes \delta \rangle &= \left\langle \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_i \tau_i \otimes \sigma_j \mid \sum_{i=1}^{n}\sum_{j=1}^{m} c_i d_i \tau_i \otimes \sigma_j \right\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{n}\sum_{\ell=1}^{m} (a_i b_i)^* c_i d_i \langle \tau_i \otimes \sigma_j \mid \tau_k \otimes \sigma_\ell \rangle.\end{aligned}$$

Using the orthonormality of the bases, we have

$$\langle \tau_i \otimes \sigma_j \mid \tau_k \otimes \sigma_\ell \rangle = \begin{cases} 1 & \text{if } i = k \text{ and } j = \ell, \\ 0 & \text{otherwise.}\end{cases}$$

Therefore the four-sum above reduces

$$\begin{aligned}\langle \alpha \otimes \beta \mid \gamma \otimes \delta \rangle &= \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{n}\sum_{\ell=1}^{m} (a_i b_j)^* c_k d_\ell \langle \tau_i \otimes \sigma_j \mid \tau_k \otimes \sigma_\ell \rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} a_i^* b_j^* c_i d_j.\end{aligned}$$

This is equal to $\langle \alpha \mid \gamma \rangle \langle \beta \mid \delta \rangle$ as calculated in the previous paragraph, as claimed. $\square$

AP 2. An n-ary function $f : \mathbb{B}^n \to \mathbb{B}$ is *idempotent* if

$$f(0, \ldots, 0) = 0 \qquad \text{and} \qquad f(1, \ldots, 1) = 1.$$

Find a basis $\mathcal{A}$ so that every idempotent Boolean function is representable as a circuit over $\mathcal{A}$. Prove your answer is correct. [*Hint 1: Post's Lattice.*] [*Hint 2:* ? :.]

Solution: The idempotent functions are those functions which "preserve" the all 0 tuple and the all 1 tuple, in the language of Post's lattice. They correspond to the set P in the

Wikipedia article on it. In that same article, a basis for the set is given — ? :, the "inline if" statement. It is defined as follows

$$x \;?\; y : z = \begin{Bmatrix} y & \text{if } x = 1, \\ z & \text{otherwise} \end{Bmatrix} = \text{"if } x \text{ then } y\text{, else } z\text{"}.$$

Let $\mathcal{I} = \{?\,:\}$. We will prove that every idempotent function can be generated by a circuit over $\mathcal{I}$.

Claim. *$\mathcal{I}$ is a complete basis for the set of idempotent functions.*

Proof of claim. Similar to the proof that $\{\neg, \wedge, \vee\}$ is a complete basis for all functions, the proof shall be by induction the function we wish to express as a circuit over $\mathcal{I}$. Let $f : \mathbb{B}^n \to \mathbb{B}$ be idempotent. We proceed by induction on n.

For the base case of $n = 1$, there is only one idempotent function, namely $f(x) = x$. We have that

$$f(x) = x = x \;?\; x : x,$$

so $f(x)$ is a circuit in $\mathcal{I}$, establishing the base case. In the argument below, we implicitly assume that $n \geq 3$ (additionally, we make use of $\wedge$), so we will also need to prove the claim for 2-ary functions. There are just four 2-ary idempotent functions:

(x, y)	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$g_1(x,y)$	0	0	0	1
$g_2(x,y)$	0	0	1	1
$g_3(x,y)$	0	1	0	1
$g_4(x,y)$	0	1	1	1

Observe that $g_2(x,y) = x$ and $g_3(x,y) = y$, functions already covered by the base case. A closer look at g_1 and g_4 reveals that $g_1(x,y) = x \wedge y$ and $g_4(x,y) = x \vee y$. We have that

$$x \;?\; y : x = x \wedge y = g_1(x,y) \qquad \text{and} \qquad x \;?\; x : y = x \vee y = g_4(x,y).$$

This establishes the claim for 2-ary functions.

Suppose now that we have proven that every n-ary idempotent function is expressible as a circuit over $\mathcal{I}$, and that f is $(n+1)$-ary and idempotent. Let us imagine evaluating f on some arguments, say $f(a_1, \dots, a_{n+1})$. Looking at the first 3 arguments of f, there must be two of these values which are equal. Therefore, $f(a_1, a_2, a_3, \dots, a_{n+1})$ is equal to one of

$$f(a_1, a_1, a_3, \dots, a_{n+1}), \quad f(a_1, a_2, a_1, \dots, a_{n+1}), \quad \text{or} \quad f(a_1, a_2, a_2, \dots, a_{n+1})$$

for this particular input. Define n-ary functions f_{12}, f_{13}, f_{23} by

$$\begin{aligned} f_{12}(x_1, x_2, x_3, \dots, x_n) &= f(x_1, x_1, x_2, x_3, \dots, x_n), \\ f_{13}(x_1, x_2, x_3, \dots, x_n) &= f(x_1, x_2, x_1, x_3, \dots, x_n), \\ f_{23}(x_1, x_2, x_3, \dots, x_n) &= f(x_1, x_2, x_2, x_3, \dots, x_n). \end{aligned}$$

We now design a circuit to test which two of x_1, x_2, x_3 are equal and select the appropriate f_{ij}. Define

$$A(z) = (x_1 \wedge x_2) \;?\; f_{12}(x_1, x_3, x_4, \dots, x_{n+1}) : \big((x_1 \wedge x_2 \;?\; z : f_{12}(x_1, x_3, x_4, \dots, x_{n+1})\big).$$

Note that if $x_1 = x_2$, then

$$\begin{aligned} A(z) = f_{12}(x_1, x_3, x_4, \dots, x_n) &= f(x_1, x_1, x_3, x_4, \dots, x_{n+1}) \\ &= f(x_1, x_2, x_3, x_4, \dots, x_{n+1}), \end{aligned}$$

and if $x_1 \neq x_2$ then $A(z) = z$. Continuing in this vein, define

$$B(z) = (x_1 \wedge x_3) \;?\; f_{13}(x_1, x_2, x_4, \dots, x_{n+1}) : \big((x_1 \wedge x_3 \;?\; z : f_{13}(x_1, x_2, x_4, \dots, x_{n+1})\big)$$

and

$$C(z) = (x_2 \wedge x_3) \;?\; f_{23}(x_1, x_2, x_4, \dots, x_{n+1}) : \big((x_2 \wedge x_3 \;?\; z : f_{23}(x_1, x_2, x_4, \dots, x_{n+1})\big).$$

It's not difficult to show that

$$f(x_1, x_2, x_3, x_4, \ldots, x_{n+1}) = A \circ B \circ C(x_1)$$

(the x_1 argument is immaterial — the circuit will never go down that branch). Since each of A, B, and C involves functions of arity at most n, the inductive hypothesis applies and we can construct circuits over $\mathcal{I}$ for each of them. It follows that f is representable as a circuit over $\mathcal{I}$. $\circ$