Homework 6

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

1. We have qubit space of 3 and Hardman operator on subset of 2 qubits, given by below formula,

$$X[p] = I_{B^{\otimes(p-1)}} \otimes I_{B^{\otimes(n-p)}}$$

2. In our case $n = 3, p = 2$, we get, $H[2] = I_{B^{\otimes(1)}} \otimes H \otimes I_{B^{\otimes(1)}}$

$$H[2] = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

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

6.5.b.

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

$$\text{Matrix} = \text{elements of } \langle j|U|k\rangle = \sum_{jk} U_{jk} |j\rangle\langle k|$$

U = 2-qubit operator = $2^r \times 2^r$ matrix

$$U = \left[\begin{array}{cc|cc} U_{0000} & U_{0001} & U_{0010} & U_{0011} \\ U_{0100} & U_{0101} & U_{0110} & U_{0111} \\ \hline U_{1000} & U_{1001} & U_{1010} & U_{1011} \\ U_{1100} & U_{1101} & U_{1110} & U_{1111} \end{array}\right] = \begin{bmatrix} V_{00} & V_{01} \\ V_{10} & V_{11} \end{bmatrix}$$

Decompose matrix U into 1-qubit matrices

$$U = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \overbrace{\begin{bmatrix} U_{0000} & U_{0001} \\ U_{0100} & U_{0101} \end{bmatrix}}^{V_{00}} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \otimes \overbrace{\begin{bmatrix} U_{0010} & U_{0011} \\ U_{0110} & U_{0111} \end{bmatrix}}^{V_{01}}$$

$$+ \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \otimes \underbrace{\begin{bmatrix} U_{1000} & U_{1001} \\ U_{1100} & U_{1101} \end{bmatrix}}_{V_{10}} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \underbrace{\begin{bmatrix} U_{1010} & U_{1011} \\ U_{1110} & U_{1111} \end{bmatrix}}_{V_{11}}$$

Apply U on the subset of qubits $[3,1]$

$$U[3,1] = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}[3] \cdot V_{00}[1] + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}[3] \cdot V_{01}[1]$$
$$+ \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}[3] \cdot V_{10}[1] + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}[3] \cdot V_{11}[1]$$

we know that $X[P] = I_B^{\otimes(P-1)} \otimes X \otimes I_B^{\otimes(n-P)}$

n = n-qubit space

P = qubit

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}[3] = I_{B^{\otimes}(2)} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes I_0 = I_{4\times 4} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$n=3,\ P=3$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$V_{00}[1] = I_{B^{\otimes}(0)} \otimes V_{00} \otimes I_{B^{\otimes}2} = \begin{bmatrix} U_{0000} & U_{0001} \\ U_{0100} & U_{0101} \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$n=3;\ P=1$

$$= \begin{bmatrix} U_{0000} & 0 & 0 & 0 & U_{0001} & 0 & 0 & 0 \\ 0 & U_{0000} & 0 & 0 & 0 & U_{0001} & 0 & 0 \\ 0 & 0 & U_{0000} & 0 & 0 & 0 & U_{0001} & 0 \\ 0 & 0 & 0 & U_{0000} & 0 & 0 & 0 & U_{0001} \\ U_{0100} & 0 & 0 & 0 & U_{0101} & 0 & 0 & 0 \\ 0 & U_{0100} & 0 & 0 & 0 & U_{0101} & 0 & 0 \\ 0 & 0 & U_{0100} & 0 & 0 & 0 & U_{0101} & 0 \\ 0 & 0 & 0 & U_{0100} & 0 & 0 & 0 & U_{0101} \end{bmatrix}$$

$\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} [3] \right) \left(V_{00} [1] \right)$ – matrix multiplication

$$= \begin{bmatrix} U_{0000} & 0 & 0 & 0 & U_{0001} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & U_{0000} & 0 & 0 & 0 & U_{0001} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ U_{0100} & 0 & 0 & 0 & U_{0101} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & U_{0100} & 0 & 0 & 0 & U_{0101} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\left(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} [3] \right) \left(V_{01} [1] \right) = \begin{bmatrix} 0 & U_{0010} & 0 & 0 & 0 & U_{0011} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & U_{0010} & 0 & 0 & 0 & U_{0011} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_{0110} & 0 & 0 & 0 & U_{0111} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & U_{0110} & 0 & 0 & 0 & U_{0111} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$V_{01} = \begin{bmatrix} U_{0010} & U_{0011} \\ U_{0110} & U_{0111} \end{bmatrix}$$

$$\left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} [3] \right) \left(V_{10} [1] \right) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ U_{1000} & 0 & 0 & 0 & U_{1001} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & U_{1000} & 0 & 0 & 0 & U_{1001} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ U_{1100} & 0 & 0 & 0 & U_{1101} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & U_{1100} & 0 & 0 & 0 & U_{1101} & 0 \end{bmatrix}$$

$$V_{10} = \begin{bmatrix} U_{1000} & U_{1001} \\ U_{1100} & U_{1101} \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}([3])(V_{11}[1]) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_{1010} & 0 & 0 & 0 & U_{1011} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & U_{1010} & 0 & 0 & 0 & U_{1011} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & U_{1110} & 0 & 0 & 0 & U_{1111} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & U_{1110} & 0 & 0 & 0 & U_{1111} \end{bmatrix}$$

$$V_{11} = \begin{bmatrix} U_{1010} & U_{1011} \\ U_{1110} & U_{1111} \end{bmatrix}$$

$$U[3,1] = \begin{bmatrix} U_{0000} & U_{0010} & 0 & 0 & U_{0001} & U_{0011} & 0 & 0 \\ U_{1000} & U_{1010} & 0 & 0 & U_{1001} & U_{1011} & 0 & 0 \\ 0 & 0 & U_{0000} & U_{0010} & 0 & 0 & U_{0001} & U_{0011} \\ 0 & 0 & U_{1000} & U_{1010} & 0 & 0 & U_{1001} & U_{1011} \\ U_{0100} & U_{0110} & 0 & 0 & U_{0101} & U_{0111} & 0 & 0 \\ U_{1100} & U_{1110} & 0 & 0 & U_{1101} & U_{1111} & 0 & 0 \\ 0 & 0 & U_{0100} & U_{0110} & 0 & 0 & U_{0101} & U_{0111} \\ 0 & 0 & U_{1100} & U_{1110} & 0 & 0 & U_{1101} & U_{1111} \end{bmatrix}$$

7.1. Prove that negation and Toffoli gate form a complete basis for reversible circuits.

1. Any function $f : 0, 1^n \to 0, 1^m$ is computable by a boolean circuit. We know that negation $\neg$ and conjunction $\wedge$ are complete basis for boolean circuits, that is, any such function can be built using negation and conjunction.

2. By lemma 7.1 and 7.2, we can say that any function $f : 0, 1^n \to 0, 1^m$ may be efficiently transformed in to a reversible circuit over the basis $A_{\oplus}$ having the function $(x, y) \to (x, y, x \oplus y)$

3. Toffoli gate $(x, y, c) \to (x, y, c \oplus (x \wedge y)$ is universal if ancillas, $allsetto|1\rangle$ and garbage outputs are allowed. If we include $\neg$ in our basis, such basis can realize any such function with ancillas set to $|0\rangle$

4. By above points, we can say that Toffoligate and negation form the complete basis for reversible circuits.

1. Prove that the inner product and the tensor product commute: $\langle \alpha \otimes \beta \mid \gamma \otimes \delta \rangle = \langle \alpha \mid \gamma \rangle \langle \beta \mid \delta \rangle$

1. We know that $|\varepsilon\rangle = \langle \varepsilon^\dagger|$, where $\dagger = Conjugate\ transpose$. Let,

$$|\alpha\rangle = \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix},\ |\beta\rangle = \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix},\ |\gamma\rangle = \begin{bmatrix} \gamma_1 \\ \gamma_2 \end{bmatrix},\ |\delta\rangle = \begin{bmatrix} \delta_1 \\ \delta_2 \end{bmatrix}$$

$$\langle \alpha^\dagger| = \begin{bmatrix} \alpha_1^\dagger & \alpha_2^\dagger \end{bmatrix},\ \langle \beta^\dagger| = \begin{bmatrix} \beta_1^\dagger & \beta_2^\dagger \end{bmatrix},\ \langle \gamma^\dagger| = \begin{bmatrix} \gamma_1^\dagger & \gamma_2^\dagger \end{bmatrix},\ \langle \delta^\dagger| = \begin{bmatrix} \delta_1^\dagger & \delta_2^\dagger \end{bmatrix}$$

2. Using above vectors, we can define tensors as below,

$$|\alpha \otimes \beta\rangle = \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix} \otimes \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} \text{ and } \langle \alpha \otimes \beta| = \begin{bmatrix} \alpha_1^\dagger & \alpha_2^\dagger \end{bmatrix} \otimes \begin{bmatrix} \beta_1^\dagger & \beta_2^\dagger \end{bmatrix} = \begin{bmatrix} \alpha_1^\dagger\beta_1^\dagger & \alpha_1^\dagger\beta_2^\dagger & \alpha_2^\dagger\beta_1^\dagger & \alpha_2^\dagger\beta_2^\dagger \end{bmatrix}$$

$$|\gamma \otimes \delta\rangle = \begin{bmatrix} \gamma_1 \\ \gamma_2 \end{bmatrix} \otimes \begin{bmatrix} \delta_1 \\ \delta_2 \end{bmatrix} = \begin{bmatrix} \gamma_1\delta_1 \\ \gamma_1\delta_2 \\ \gamma_2\delta_1 \\ \gamma_2\delta_2 \end{bmatrix}$$

$$\langle \alpha \otimes \beta \mid \gamma \otimes \delta \rangle = \alpha_1^\dagger\beta_1^\dagger\gamma_1\delta_1 + \alpha_1^\dagger\beta_2^\dagger\gamma_1\delta_2 + \alpha_2^\dagger\beta_1^\dagger\gamma_2\delta_1 + \alpha_2^\dagger\beta_2^\dagger\gamma_2\delta_2$$

3. We will derive inner product as below,

$$\langle \alpha \mid \gamma \rangle = \begin{bmatrix} \alpha_1^\dagger & \alpha_2^\dagger \end{bmatrix} \begin{bmatrix} \gamma_1 \\ \gamma_2 \end{bmatrix} = \alpha_1^\dagger\gamma_1 + \alpha_2^\dagger\gamma_2 \text{ and } \langle \beta \mid \delta \rangle = \begin{bmatrix} \beta_1^\dagger & \beta_2^\dagger \end{bmatrix} \begin{bmatrix} \delta_1 \\ \delta_2 \end{bmatrix} = \beta_1^\dagger\delta_1 + \beta_2^\dagger\delta_2$$

$$\langle \alpha \mid \gamma \rangle \langle \beta \mid \delta \rangle = [\alpha_1^\dagger\gamma_1 + \alpha_2^\dagger\gamma_2][\beta_1^\dagger\delta_1 + \beta_2^\dagger\delta_2] = \alpha_1^\dagger\beta_1^\dagger\gamma_1\delta_1 + \alpha_1^\dagger\beta_2^\dagger\gamma_1\delta_2 + \alpha_2^\dagger\beta_1^\dagger\gamma_2\delta_1 + \alpha_2^\dagger\beta_2^\dagger\gamma_2\delta_2$$

4. From the results of point 2 and 3, we can say that,

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

2. Find the basis A so that every idempotent Boolean function is representable as a circuit over A.

1. An idempotent function is a self inverse function. It should preserve the state of the input 0,1.

2. According to Post's Lattice, Clone $P = P_0P_1$ is the clone of constant-preserving functions. It is the set of idempotent boolean functions.

3. One of the bases for above clone is $x?y : z$
$x\ ?\ y : z = y, if\ x \neq 0\ else = z.$ Equivalent to the terenary operator in programming.

- For any $k \geq 1$, $T_0^{\,k}$ is the set of functions *f* such that

$$\mathbf{a}^1 \wedge \cdots \wedge \mathbf{a}^k = \mathbf{0} \Rightarrow f(\mathbf{a}^1) \wedge \cdots \wedge f(\mathbf{a}^k) = 0.$$

  Moreover, $\mathrm{T}_0^\infty = \bigcap_{k=1}^{\infty} \mathrm{T}_0^k$ is the set of functions bounded above by a variable: there exists $i = 1, ..., n$ such that $f(\mathbf{a}) \leq a_i$ for all $\mathbf{a}$.

  As a special case, $P_0 = T_0^{\,1}$ is the set of *0-preserving* functions: $f(\mathbf{0}) = 0$. Furthermore, $\top$ can be considered $T_0^{\,0}$ when one takes the empty meet into account.

- For any $k \geq 1$, $\mathrm{T}_1^{\,k}$ is the set of functions *f* such that

$$\mathbf{a}^1 \vee \cdots \vee \mathbf{a}^k = \mathbf{1} \Rightarrow f(\mathbf{a}^1) \vee \cdots \vee f(\mathbf{a}^k) = 1,$$

  and $\mathrm{T}_1^\infty = \bigcap_{k=1}^{\infty} \mathrm{T}_1^k$ is the set of functions bounded below by a variable: there exists $i = 1, ..., n$ such that $f(\mathbf{a}) \geq a_i$ for all $\mathbf{a}$.

  The special case $P_1 = T_1^{\,1}$ consists of the *1-preserving* functions: $f(\mathbf{1}) = 1$. Furthermore, $\top$ can be considered $T_1^{\,0}$ when one takes the empty join into account.

- The largest clone of all functions is denoted $\top$, the smallest clone (which contains only projections) is denoted $\perp$, and $P = P_0P_1$ is the clone of ***constant-preserving*** functions.

4. Reference - https://en.wikipedia.org/wiki/