MATH 1800: Quantum Information Theory with Applications to Cryptography

Midterm Exam 1
Review

Problem 1 Write each of the states below in the standard basis (**do not use the sum notation**).

(a) $H\left(\frac{3|0\rangle - 4|1\rangle}{5}\right)$

(b) $H^{\otimes 5}(|+-++-\rangle)$

(c) $|0\rangle \otimes H^{\otimes 3}(|011\rangle) \otimes |1\rangle$

(d) $H(|0\rangle) \otimes T(|+\rangle)$[1]

Problem 2 Check if the operator is unitary and find the matrix of the inverse operator if it is.

(a) $A = \begin{pmatrix} i & 0 & 0 \\ 0 & e^{2\pi i/7} & 0 \\ 0 & 0 & e^{2\pi i/2022} \end{pmatrix}$

[1]Recall that $T = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

(b) $B = \begin{pmatrix} i & 1 & 1+i \\ i-1 & e^{2\pi i/7} & 1-i \\ 0 & 3-i & e^{2\pi i/2022} \end{pmatrix}$

Problem 3 Find all possible pairs of values of a and b for which the operator $C = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & a \\ 2i & b \end{pmatrix}$ is unitary.

Problem 4

(a) Write the matrix of the operator CH_1 in the standard basis of $(\mathbb{C}^2)^{\otimes 2}$, the controlled Hadamard operator with the first qubit being the controlling one. Draw the corresponding circuit.

(b) Write the matrix of the operator CH_2 in the standard basis of $(\mathbb{C}^2)^{\otimes 2}$, the controlled Hadamard operator with the second qubit being the controlling one. Draw the corresponding circuit.

(c) Find a matrix σ with $CH_2 = \sigma CH_1 \sigma$.[2]

Problem 5 Write the CNOT operator as a composition of negation $\neg$ and CCNOT gates using ancilla consisting of one auxiliary bit in state 0 (the bit must be returned to that state at the end of the circuit).

Problem 6 Let $U_1, U_2 \in U_n(\mathbb{C})$ be unitary operators and $\widetilde{U}_1, \widetilde{U}_2 \in U_n(\mathbb{C})$ approximations with precision ε_1 and ε_2, respectively. Show that $\widetilde{U}_1\widetilde{U}_2$ approximates $U_1 U_2$ with precision $\varepsilon_1 + \varepsilon_2$. [3]

[2]**Hint:** what is the matrix of the operator swapping the first and second qubit?

[3]**Hint:** you need to show that $\|U_1U_2 - \widetilde{U}_1\widetilde{U}_2\| \leq \varepsilon_1 + \varepsilon_2$. Here is a helpful 'arithmetic trick': add $0 = \widetilde{U}_1 U_2 - \widetilde{U}_1 U_2$ to the expression and use various properties of the norm to deduce the result.

Bernstein-Vazirani algorithm

Problem 7 Let $f_s : \mathbb{B}^4 \to \mathbb{B}$ be a function given by $f_s(x) := x \cdot s = x_1 s_1 + x_2 s_2 + x_3 s_3 + x_4 s_4 \pmod 2$ for any $x \in \mathbb{B}^4$ and a fixed string $s \in \mathbb{B}^4$.

(a) Find s given that

$$f_s(1111) = 1$$
$$f_s(1110) = 0$$
$$f_s(1100) = 0$$
$$f_s(1000) = 1.$$

(b) Using your answer in (a) show the steps of execution of Bernstein-Vazirani algorithm in this example.

Simon's algorithm

Problem 8 Let $f : \mathbb{B}^3 \to \mathbb{B}^3$ be a map, promised to satisfy the condition

$$f(x) = f(y) \Leftrightarrow x = y \text{ or } x = y \oplus s$$

for some fixed string $s \in \mathbb{B}^3$. The function is given by

$$f(000) = f(101) = 111$$
$$f(001) = f(100) = 010$$
$$f(010) = f(111) = 100$$
$$f(110) = f(011) = 001.$$

(a) Find s in a straightforward way.

(b) Now let's run Simon's algorithm. Write $\mathcal{O}_f(H^{\otimes 3}(|000\rangle) \otimes |000\rangle)$ in the standard basis.

(c) Give the state after measuring the second register (suppose the measurement gave $|100\rangle$).

(d) Apply $H^{\otimes 3}$ to the first three qubits of the state vector you obtained in (c) and measure the first register.

(e) Write the linear equation on s that you obtained from (d) given that the measurement produced any vector except $|000\rangle$.

(f) Repeat (c) – (e) with the assumption that this time the result of the first measurement was $|001\rangle$. Get one more linear equation on s. Use this equation together with the one you got in (e) and find s.