MATH 1800: Quantum Information Theory with Applications to Cryptography

Midterm Exam 2
Review

Solutions

Problem 1. Let $\omega = e^{2\pi i/n}$ be the primitive n^{th} root of unity. Show that $\sum_{j=0}^{n-1} \omega^j = 0$.[1]

Solution: $\omega \sum_{j=0}^{n-1} \omega^j = \sum_{j=0}^{n-1} \omega^{j+1} = \sum_{j=0}^{n-1} \omega^j \Leftrightarrow (\omega - 1) \sum_{j=0}^{n-1} \omega^j = 0 \Leftrightarrow \sum_{j=0}^{n-1} \omega^j = 0$.

Problem 2. Show that $|1 - e^{i\varphi}| = 2|\sin\left(\frac{\varphi}{2}\right)|$.[2]

Solution: $|1 - e^{i\varphi}|^2 = (1 - e^{i\varphi})(1 - \overline{e^{i\varphi}}) = (1 - e^{i\varphi})(1 - e^{-i\varphi}) = 2 - 2\cos(\varphi) = 2(1 - \cos(\varphi)) = 4\sin^2\left(\frac{\varphi}{2}\right) \Leftrightarrow$ $|1 - e^{i\varphi}| = 2|\sin\left(\frac{\varphi}{2}\right)|$.

Problem 3. Let F_n be the matrix of discrete Fourier transform for the group $G = \mathbb{Z}_n$ in the standard basis (of delta functions).

(a) Write down the matrix of F_6 (let $\omega = e^{2\pi i/6}$ and $\xi = \omega^2 = e^{2\pi i/3}$) and compute the image of δ_4.

Solution. $F_6 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \xi & -1 & \xi^2 & -\xi \\ 1 & \xi & -\omega & 1 & \xi & -\omega \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \xi^2 & \xi & 1 & -\omega & \xi \\ 1 & -\xi & -\omega & -1 & \xi & \omega \end{pmatrix}$ and $F_6(\delta_4) = \delta_0 - \omega\delta_1 + \xi\delta_2 + \delta_3 - \omega\delta_4 + \xi\delta_5$ is given by the fifth column.

(b) Write down the matrices of F_2, F_3 and compute $(F_2 \otimes F_3)(\delta_0 \otimes \delta_1)$.

Solution. $F_2 = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \xi & \xi^2 \\ 1 & \xi^2 & \xi \end{pmatrix}$ with $(F_2 \otimes F_3)(\delta_0 \otimes \delta_1) = \frac{1}{\sqrt{6}}((\delta_0 + \delta_1) \otimes (\delta_0 + \xi\delta_1 + \xi^2\delta_2))$.

(c) Notice that the groups $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ are isomorphic. Consider the isomorphism $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ given by $\varphi(j) = (j \pmod 2, j \pmod 3)$. For instance, $\varphi(4) = (0, 1)$. Write down the 6×6 matrix of $F_2 \otimes F_3$ in the basis $\delta_{j \pmod 2} \otimes \delta_{j \pmod 3}$ with $j \in \mathbb{Z}_6$. What is the relation between matrices of F_6 and $F_2 \otimes F_3$?[3]

Solution. $F_2 \otimes F_3 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -\xi & \xi^2 & -1 & \xi & -\xi^2 \\ 1 & \xi^2 & \xi & 1 & \xi^2 & \xi \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \xi & \xi^2 & 1 & \xi & \xi^2 \\ 1 & -\xi^2 & \xi & -1 & \xi^2 & -\xi \end{pmatrix}$, so substituting $\omega = -\xi^2$ in F_6, we see that F_6 is $F_2 \otimes F_3$ with the columns $1, 5$ and $2, 4$ swapped, respectively.

[1] **Hint:** what happens to the sum when you multiply it by ω?

[2] **Hint:** use that $e^{i\varphi} = \cos(\varphi) + i\sin(\varphi)$, $|z|^2 = z\bar{z}$ and $\cos(\varphi) = 1 - 2\sin^2\left(\frac{\varphi}{2}\right)$.

[3] **Hint:** notice that $\omega = -\xi^2$.

Problem 4. Find the periods of functions on the set of positive integers (in other words, the domain is $\mathbb{Z}_{>0}$).

(a) $f(x) = 7x \pmod{11}$

Solution: $r = 11$

(b) $g(x) = mx \pmod{n}$ with $n, m \in \mathbb{Z}_{>0}$

Solution: $g(x) = g(r + x) \Leftrightarrow mx \equiv m(r + x) \pmod{n} \Leftrightarrow mr \equiv 0 \pmod{n}$ and $r = \dfrac{\operatorname{lcm}(m, n)}{m}$ is the smallest positive integer that satisfies the latter congruence.

(c) $h(x) = 5^x \pmod{13}$

Solution: $5^2 \equiv 12, 5^3 \equiv 8, 5^4 \equiv 1$, so $r = 4$.

On the Shore of factorization

Problem 5. Consider the number $n = 115 = 5 \cdot 23$. The goal of this exercise is to factorize it using Shor's algorithm.

(a) What is the order of the multiplicative group $\mathbb{Z}_{115}^{\times}$?

Solution: $\varphi(5 \cdot 23) = \varphi(5)\varphi(23) = 4 \cdot 22 = 88$.

(b) Notice that the numbers 3 and 115 are coprime, hence, 3 is invertible modulo 115. Find the order r of 3 in $\mathbb{Z}_{115}^{\times}$.[4] Check that the pair (x, r) satisfies the requirements of Shor's algorithm (use the programs at http://tsvboris.pythonanywhere.com/IntrotoCryptography, if necessary).

Solution: $r = 44$ is even and $\gcd(x^{r/2} + 1, n) = \gcd(3^{22} + 1, 115) = \gcd(25, 115) = 5 < 115$.

(c) We will take 7 qubits for the second register as $q = 2^7 = 128$ is the smallest power of 2 larger than 115.[5] Run Shor's algorithm, assuming that the measurement of the second register produced 13 (the smallest number a with $3^a \equiv 13 \pmod{115}$ is $a = 5$). Write the expression that you obtained at that stage (show steps).

Solution: as measuring the second register produced 13, we got the superposition
$\frac{1}{\sqrt{3}}(|5 \otimes 13\rangle + |49 \otimes 13\rangle + |93 \otimes |13\rangle)$. Application of F_{128} gives ($\omega = e^{2\pi i/128}$)

$$F_{128}\left(\frac{1}{\sqrt{3}}(|5\rangle + |49\rangle + |93\rangle)\right) = \frac{1}{\sqrt{3 \cdot 128}} \cdot \sum_{j=0}^{127} (\omega^{5j} + \omega^{49j} + \omega^{93j})|j\rangle.$$

(d) What is an upper bound on the probability of collapsing to a state $|j\rangle$? Is it attained (justify)?[6]

Solution: the upper bound is $\frac{1}{\sqrt{3 \cdot 128}} \cdot |\omega^{5j} + \omega^{49j} + \omega^{93j}|^2 = \frac{1}{\sqrt{3 \cdot 128}} \cdot |\omega^{5j}|^2 |1 + \omega^{44j} + \omega^{89j}|^2 = |1 + \omega^{44j} + \omega^{88j}|^2 \leq (1 + |\omega^{44j}| + |\omega^{88j}|)^2 = \frac{9}{\sqrt{3 \cdot 128}}$. As $\gcd(r, q) = \gcd(44, 128) = 4 > 1$, the upper bound is attained at any j with $44j \equiv 0 \pmod{128} \Leftrightarrow 11j \equiv 0 \pmod{32} \Leftrightarrow j \equiv 0 \pmod{32} \Leftrightarrow j \in \{0, 32, 64, 96\}$.

(e) Compute the probability of measuring $j = 3$ (give the estimate up to 3 decimals using the formula in Problem 2).

Solution: notice that $\omega^{5j} + \omega^{49j} + \omega^{93j} = \dfrac{\omega^{5j}(1 - \omega^{4j})}{1 - \omega^{44j}}$, so $\dfrac{|\omega^{5j}(1 - \omega^{4j})|}{|1 - \omega^{44j}|} = \dfrac{|(1 - \omega^{4j})|}{|1 - \omega^{44j}|} = \dfrac{|(1 - e^{4j \cdot 2\pi i/128})|}{|1 - e^{44j \cdot 2\pi i/128}|}$,

if $j = 3$, then $|\alpha_3|^2 = \dfrac{1}{\sqrt{3 \cdot 128}} \cdot \left(\dfrac{|\sin\left(\frac{3\pi}{32}\right)|}{|\sin\left(\frac{\pi}{32}\right)|} \right)^2 \approx \dfrac{1}{\sqrt{3 \cdot 128}} \cdot \left(\dfrac{0.29028}{-0.098017}\right)^2 \approx \dfrac{8.771}{\sqrt{3 \cdot 128}}$.

---

[4] **Hint:** recall that the order of an element must divide the order of the group

[5] We are 'cheating' here since the actual requirement is $q = 2^\ell > n^2 = 115^2 = 13225$, so $q = 2^{14}$ should be taken instead.

[6] **Hint:** recall that the probability of collapsing to a basic state is equal to the square of the absolute value of the corresponding coefficient in the expression you obtained in (c).

(f) Assume that measuring of the first register produced 3 and find the continued fraction of $\frac{3}{128}$. Let the corresponding sequence be $[a_0 : a_1 : \ldots : a_s]$. Find $\widetilde{r} = q_{s-1}$. Explain why $\widetilde{r} \neq r$.[7]

Solution:

$$\frac{3}{128} = 0 + \frac{1}{\frac{128}{3}} = 0 + \frac{1}{42 + \frac{2}{3}} = 0 + \frac{1}{42 + \frac{1}{1 + \frac{1}{2}}}.$$

The sequence is $[0 : 42 : 1 : 2]$ giving rise to the sequence of denominators

$$\begin{aligned} q_0 &= 1 \\ q_1 &= a_1 = 42 \\ q_2 &= a_2 q_1 + q_0 = 43. \end{aligned}$$

$(g)^{\star}$ (**3 Bonus points on the midterm**). Run Shor's algorithm with $q = 2^{14}$ and your choice of measurements to get $\widetilde{r} = r = 44$.

Discrete logarithm problem (DLP)

Problem 6.

(a) Consider the group $G = (\mathbb{Z}_{131}, +)$ and element $g = 5$. Find the order of g.

Solution. As $\gcd(5, 131) = 1$, the order of g is 131 (it is a generator).

(b) Solve the DLP for $G = (\mathbb{Z}_{131}, +)$, $g = 5$ and $h = 23$. In other words, find a number $1 \leq s \leq \mathrm{ord}(g)$ with $sg \equiv h \pmod{131}$.

Solution. We need to solve the congruence $5s \equiv 23 \pmod{131}$. As $131 = 5 \cdot 26 + 1$ gives $-26 \equiv 5^{-1} \pmod{131}$, one gets $s \equiv -26 \cdot 23 \equiv 57 \pmod{131}$.

[7] **Hint:** take a look at the footnote in (c).