MATH 1800: Quantum Information Theory with Applications to Cryptography

Midterm Exam 2
Review

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]

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

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.

[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 $\cos(\varphi) = 1 - 2\sin^2\left(\frac{\varphi}{2}\right)$.

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

(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]

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

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

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

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

[3]**Hint:** notice that $\xi = -\overline{\omega}$.

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 $\mathbb{Z}_{115}^{\times}$?

(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).

(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).

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

[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).

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

(f) Assume that measuring of the first register produced $j = 3$ 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]

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

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

Discrete logarithm problem (DLP)

Problem 6.

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

(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 $sg \equiv h \pmod{131}$.