Intro to Quantum Computing
CSCI/PHYS 3090
CU Boulder Spring 2020
Practice Midterm II Solutions

1 EPR Paradox, Bell Experiment

1.1 Classical

Alice and Bob got together a long time ago, and wrote down a long list of common strategies they could possibly use. Soon after, they moved far apart from each other and never talked to each other again, unable to modify their stategy. Now, Alice is given as input a random bit x_A and Bob a random bit x_B. Without communicating with each other, Alice and Bob wish to output bits a and b respectively such that $x_A \wedge x_B = a \oplus b$. Prove that any protocol that Alice and Bob follow has success probability at most 3/4. [Hint: Consider their strategies as fixed functions $f_A, f_B : \{0,1\} \to \{0,1\}$ where $a = f_A(x_A)$ and $b = f_B(x_B)$. What can these functions be? What happens in each case?]

Solution: There are 4 unique choices for f_A: $f_A(x) = \{0, 1, x, 1-x\}$. We will analyze the two cases when f_A is the identity and f_A is identically 1, the others follow the same argument.

Assume that $f_A(x_A) = x_A$. Then Alice outputs $a = x_A$. They win if and only if Bob outputs $b = (x_A \wedge x_B) \oplus x_A$. There are 2 choices for Bob's input:

- $x_B = 1$: Then $b = (x_A \wedge x_B) \oplus x_A = x_A \oplus x_A = 0$ so if Bob outputs $b = 0$ then they win with probability 1.
- $x_B = 0$: Then b must equal x_A. Bob does not know x_A and so they can only win with probability 1/2.

Therefore, we have

$$\begin{aligned} Pr(\text{win}) &= Pr(\text{win}|x_B = 1)Pr(x_b = 1) + Pr(\text{win}|x_B = 0)Pr(x_b = 0) \\ &= (1/2)(1) + (1/2)(1/2) \\ &= 3/4 \end{aligned}$$

Now assume that $f_A(x_A) = 1$. Then Alice outputs $a = 1$.

- $x_B = 1$: Then b must equal $1 + x_A$ to win. Bob does not know x_A and so they can only win with probability 1/2.
- $x_B = 0$: Then $b = 1$ wins with probability 1.

Therefore, we have

$$
\begin{aligned}
Pr(\text{win}) &= Pr(\text{win}|x_B = 1)Pr(x_b = 1) + Pr(\text{win}|x_B = 0)Pr(x_b = 0) \\
&= (1/2)(1/2) + (1/2)(1) \\
&= 3/4
\end{aligned}
$$

1.2 Quantum

Now we assume that Alice and Bob each share a qubit of the entangled system $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Once again, Alice is given as input a random bit x_A and Bob a random bit x_B. Without communicating with each other (but with possible operations on their qubit), Alice and Bob wish to output bits a and b respectively such that $x_A \wedge x_B = a \oplus b$. Prove that Alice and Bob can win with probability at least 0.8. [Hint: Consider applying rotations θ_A and θ_B where $|\theta_A| = |\theta_B| = \frac{\pi}{8}$.]

Solution: The main trick we use is the following: if a measurement in the standard basis results in $|0\rangle$ with probability 1, then if a state is rotated by an angle θ, measurement results in $|0\rangle$ with probability $\cos^2(\theta)$.

Here is the strategy:

- If Alice receives a 1, then she applies a rotation of $\frac{\pi}{8}$ to her qubit before measuring and outputting her result.
- If Bob receives a 1, then he applies a rotation of $-\frac{\pi}{8}$ to his qubit before measuring and outputting his result.

There are 4 cases to analyze, all occurring with probability 1/4.

- $x_A = x_B = 0$: They each simply measure and so $Pr(a = b|x_A = x_B = 0) = 1$.
- $x_A = 0, x_B = 1$: Bob applies his transformation before measuring and so $Pr(a = b|x_A = 0, x_B = 1) = \cos^2 \frac{-\pi}{8} \geq .85$
- $x_A = 1, x_B = 0$: By same logic, $Pr(a = b|x_A = 1, x_B = 0) = \cos^2 \frac{\pi}{8} \geq .85$
- $x_A = x_B = 1$: Here they win if $a \neq b$. This case is a bit sloppier. Both apply their transformation resulting in the following (unnormalized) state:

$$
\begin{aligned}
&(\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle)(\cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle) \\
&+(-\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle)(\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle) \\
&= \left(\cos^2(\pi/8) - \sin^2(\pi/8)\right)|00\rangle - 2\sin(\pi/8)\cos(\pi/8)|01\rangle \\
&+2\sin(\pi/8)\cos(\pi/8)|10\rangle + \left(\cos^2(\pi/8) - \sin^2(\pi/8)\right)|11\rangle \\
&= 2\sin(\pi/8)\cos(\pi/8)\left(|00\rangle - |01\rangle + |10\rangle + |11\rangle\right)
\end{aligned}
$$

  where the last line follows from trigonometric identities. Since they all have the same coefficients, the normalized state is $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$. Thus, $Pr(a \neq b|x_A = x_B = 1) = 1/2$.

Putting this all together, we have $Pr(\text{win}) \geq (1/4)(1) + (1/2)(.85) + (1/4)(1/2) = 0.8$.

2 Number Theory

Let p be an odd prime and let x be a uniformly random number modulo p. Show that the period of x modulo p is even with probability at least 1/2. [Hint: . Look up the following group theory terms if you do not know them: *order/period* of an element and *generator*. Use Fermat's Little Theorem]

Solution: By FLT, we have that $x^{p-1} = 1 \mod p$ which implies that $ord(x)|p-1$. This alone is not enough to determine the parity of $ord(x)$. Let g be the generator for $\{0, \ldots, p-1\} = \mathbb{Z}_p$. In particular, there exists a $k \in \mathbb{Z}_p$ such that $x = g^k \mod p$. Equality is preserved under raising both sides to the same power in this group so we have $x^{ord(x)} = (g^k)^{ord(x)} \mod p$. This gives $(g^k)^{ord(x)} = 1 \mod p$ and now we have $p-1|k * ord(x)$. Since p is odd, $p-1$ is even and so $k * ord(x)$ is even.

x was chosen uniformly random so we also have that k is uniformly random, thus $Pr(k \text{ odd}) = 1/2$. Say k is odd. Then $ord(x)$ is even since $k * ord(x)$ is even. If we say k is even, then we cannot conclude anything about $ord(x)$. Thus $Pr(ord(x) \text{ even}) \geq Pr(k \text{ odd}) = 1/2$.

3 QFT

Let $|a\rangle = \Sigma_{j=0}^{N-1} a_j |j\rangle$ and let $|b\rangle = \Sigma_{j=0}^{N-1} |j\rangle$ be its Quantum Fourier Transform. Consider the shift of the superposition $|a\rangle$, $|a'\rangle = \Sigma_{j=0}^{N-1} a_j |j + 1(\text{mod}N)\rangle$, and let $|b'\rangle = \Sigma_{j=0}^{N-1} b'_j |j\rangle$ be its QFT. Derive an expression for $|b'\rangle$ as a function of $|b\rangle$.

Solution:

We know from HW 7 that we have that $b'_j = b_j w^j$. Then, using $\langle j|b\rangle = b_j$, we can write

$$|b'\rangle = \sum_{j=0}^{N-1} w^j |j\rangle \langle j|b\rangle$$

4 RSA

Suppose you are developing an RSA public key encryption scheme. You decide to use the primes $p = 11$ and $q = 19$, and the semiprime $n = pq = 209$ as the modulus for the encryption/decryption.

Part A

We would like to show that $e = 7$ is a valid public encryption key for our choice of p, q, and n. A valid encryption key e must be coprime with $(p-1)(q-1) = 180$. Since $e = 7$ is prime and $7 \nmid 180$, then the encryption key is coprime to $(p-1)(q-1)$ and is therefore valid.

Part B

The decryption key d is the multiplicative inverse of e modulo $(p-1)(q-1)$.

$$d \cdot e = 1 \mod 180$$

We can begin with Euclid's algorithm:

$$\begin{aligned} 180 &= 7 \cdot 25 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 2 + 0 \end{aligned}$$

This confirms that the $gcd(180, 7) = 1$. The point of doing that however was so that we can now "climb back up" the Euclidean algorithm to find the inverse of e.

$$1 = 5 - 2 \cdot 2$$
$$1 = 5 - 2(7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7$$
$$1 = 3(180 - 7 \cdot 25) - 2 \cdot 7$$
$$1 = 3 \cdot 180 - 77 \cdot 7$$
$$\implies d = -77 \mod 180$$
$$d = 103 \mod 180$$

This is the smallest positive value which can be used for our decryption key.

Part C

Now, consider using $p = 11$ and $q = 5$, so $n = 55$, with $e = 7$ and $d = 23$. Encrypt the message "SEND" (using single-letter blocks) where "SEND" is (18 04 13 03). We encode each letter through the following scheme: $c = m^e \mod n$ where c is the encrypted message and m is the plaintext.

$$18^7 = 18^{2^2+2^1+2^0}$$
$$18^7 = 18^{2^2}18^{2^1}18^{2^0}$$
$$18^1 = 18 \mod 55$$
$$18^2 = 324 = 49 \mod 55$$
$$18^4 = (18^2)^2 = (49)^2 = 2401 = 36 \mod 55$$
$$\implies 18^7 = (18)(49)(36) = 31752 = 17 \mod 55$$

We can perform the same operation for each of the following letter blocks and we get the following:

$$c(\text{E}) = 49 \mod 55,\ c(\text{N}) = 7 \mod 55,\ c(\text{D}) = 42 \mod 55$$

Therefore the encrypted message is $c(\text{SEND}) = 17\ 49\ 07\ 42$.

Part D

Decrypt the message "Y J A R Y" (24 09 00 17 24) The message can be recovered by the following procedure: $m = c^d \mod n$. We know that the binary representation of $23 = 10111$ and so we can use fast modular exponentiation.

$$24^23 = 24^{2^4}24^{2^2}24^{2^1}24^{2^0}$$
$$24 \mod 55 = 24$$
$$24^2 = 576 = 26 \mod 55$$
$$24^4 = (24^2)^2 = (26)^2 = 676 = 16 \mod 55$$
$$24^8 = (24^4)^2 = (16)^2 = 256 = 36 \mod 55$$
$$24^{16} = (24^8)^2 = (36)^2 = 31 \mod 55$$
$$24^{23} = (24)(26)(16)(31) = 309504 = 19 \mod 55$$

Following the same method, we get the following:

$$m(\text{J}) = 14 \mod 55,\ m(\text{A}) = 0 \mod 55,\ m(\text{R}) = 18 \mod 55,\ m(\text{Y}) = 19 \mod 55$$

The message is therefore $m = 19\ 14\ 0\ 18\ 19$, which in letters is TOAST.