Quantum Information and Computation
Homework 2

(Report Due: 23:00, April 6, 2022)

Here and subsequently, we denote by $\mathbb{Z}_2^n := \{0,1\}^n$ the set of all n-bit strings (i.e. n-tuples of 0's and 1's) for any integer n. The set $\mathbb{Z}_2^n$ forms a vector space over $\mathbb{Z}_2$. For example, for vectors $101, 001 \in \mathbb{Z}_2^3$ and scalars $0, 1 \in \mathbb{Z}_2$, we have

$$\begin{aligned} 101 + 001 \ (\mathrm{mod}\ 2) &:= (1 \oplus 0)(0 \oplus 0)(1 \oplus 1) = 100 \in \mathbb{Z}_2^3; \\ 101 \cdot 1 &= (1 \cdot 1)(0 \cdot 1)(1 \cdot 1) = 101 \in \mathbb{Z}_2^3; \\ 101 \cdot 0 &= (1 \cdot 0)(0 \cdot 0)(1 \cdot 0) = 000 \in \mathbb{Z}_2^3. \end{aligned}$$

Note that this vector space has dimension n since it can be generated by the n linearly independent vectors consisting of n-bit strings with exactly one 1 in the k-th position, for $k = 1, 2, \ldots, n$.

1. **(25 points) Intercept-resend attack in BB84 QKD.**
   A general orthonormal qubit basis can be expressed as

   $$\mathcal{B}(a,b) = \{\, |\beta_0\rangle = a\,|0\rangle + b\,|1\rangle\,, \quad |\beta_1\rangle = -b^*\,|0\rangle + a^*\,|1\rangle \,\},$$

   where $a, b \in \mathbb{C}$, $|a|^2 + |b|^2 = 1$ and * denotes complex conjugation.

   Alice and Bob are distantly separated in space. They can communicate classically and are also connected by a noiseless quantum channel. They perform BB84 quantum key distribution.

   Suppose Eve, hiding in between, attempts to eavesdrop by following the intercept-resend strategy, measuring each passing qubit in the basis $\mathcal{B}(a,b)$ and sending on the post-measurement state to Bob. Eve interprets her measurement outcome $|\beta_i\rangle$ as bit value i.

   (a) **(10 points)** Calculate the average bit error rate, as a function of a and b, that Eve's action will cause in Alice and Bob's strings.

   (b) **(5 points)** Calculate also the probability that Eve learns Alice's encoded bit correctly.

   (c) **(5 points)** Show that the minimum bit error rate can be achieved by using *real* values of a and b, i.e. if Eve is trying not to be detected then use of complex a and b does not help.

   (d) **(5 points)** Let $a = \cos\theta$ and $b = \sin\theta$ with $0 \le \theta \le \pi/2$. For what value of θ does Eve cause the least disturbance i.e. minimum bit error rate? For what value of θ does Eve gain the most information i.e. maximum probability of learning Alice's bit?

2. **(20 points) Bernstein–Vazirani problem/algorithm.**
   For n-bit strings $x = x_1 \ldots x_n$ and $a = a_1 \ldots a_n$ in $\mathbb{Z}_2^n$, we have the sum $x \oplus a$ which is an n-bit string, and now introduce the 1-bit "dot product" $x \cdot a = x_1 a_1 \oplus x_2 a_2 \oplus \cdots \oplus x_n a_n \in \mathbb{Z}_2$.
   For any fixed n-bit string $a = a_1 \ldots a_n$, consider the function $f_a : \mathbb{Z}_2^n \to \mathbb{Z}_2$ given by

   $$f_a(x_1, \ldots, x_n) = x \cdot a. \tag{1}$$

Input: An oracle for a function $f_a : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is given for some $a \in \mathbb{Z}_2^n$.
Promise: The oracle computes (1).
Problem: Determine the n-bit string a.

(a) **(4 points)** Show that for any $a \neq 00\ldots0$, f_a is a balanced function i.e. f_a has output-value 0 (respectively 1) on exactly half of its inputs x.

(b) **(4 points)** Given a classical black box that computes f_a, describe a classical algorithm that will identify the string $a = a_1 \ldots a_n$ on which f_a is based. Show that any such black box classical algorithm must have query complexity at least n.

(c) **(4 points)** For any integer n, let $H_n = H^{\otimes n}$ be the application of H to each qubit of a row of n qubits. Show that (for $x \in \mathbb{Z}_2$ and $a \in \mathbb{Z}_2^n$)

$$H\left|x\right\rangle = \frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}\left|y\right\rangle; \quad H_n\left|a\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{Z}_2^n}(-1)^{a\cdot y}\left|y\right\rangle. \tag{2}$$

(d) **(8 points)** For each a consider the function f_a which is a balanced function if $a \neq 00\ldots0$ (as shown above). Show that the Deutsch–Jozsa algorithm will perfectly distinguish and identify the $2^n - 1$ balanced functions f_a (for $a \neq 00\ldots0$) with only *one* query to the function (quantum oracle for f). Indeed, show that the n bit output of the final measurements of the algorithm gives the string a with certainty for these special balanced functions. On the other hand, for $a = 00\ldots0$, the algorithm again identifies it with certainty.

Hint. Recall which quantum gates were used in the Deutsch–Jozsa algorithm. You may need to use them too. In this problem, the quantum oracle is constructed according to (1). Also, identities (2) may be helpful in solving Problem 2d.

Remark. From Problems 2b and 2d, we can see that the Bernstein–Vazirani algorithm provides an *polynomial speedup* instead of the exponential speedup as in the Deutsch–Jozsa algorithm. However, remember that the Deutsch–Jozsa algorithm only guarantees exponential speedup against classical *deterministic* algorithms; classical randomized algorithms only require $O(1)$ queries as mentioned in class.

3. **(15 points) Grover's algorithm.**
Let $x_0 \in \mathbb{Z}_2^n$ be an unknown target string and $\left|x_0\right\rangle$ be the associated basis vector state, and let $\mathcal{P}(x_0)$ be a real plane spanned by $\left|x_0\right\rangle$ and $\left|\psi_0\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\mathbb{Z}_2^n}\left|x\right\rangle$ as in Grover's algorithm taught in class.

(a) **(3 points)** Find an orthonormal basis, say $\mathcal{B} = \{\left|e_0\right\rangle, \left|e_1\right\rangle, \ldots\}$, for this plane $\mathcal{P}(x_0)$.

(b) **(12 points)** Using the basis $\mathcal{B}$, show algebraically (rather than geometrically via the reflection operators as in lectures) that the Grover iteration operator $\mathcal{G}$ is a rotation in the plane $\mathcal{P}(x_0)$ and derive the angle of rotation.

Hint. Recall that a rotation matrix in an Euclidean space can be written as

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

for certain angle θ. You may use the basis $\mathcal{B}$ and write down the matrix representation of operation $\mathcal{G}$ with respect to $\mathcal{B}$.

4. **(20 points) B92 quantum key distribution.**

We will describe a quantum key distribution scheme (devised by C. Bennett in 1992) that uses only *two* non-orthogonal qubit states, $|0\rangle$ and $|+\rangle$, instead of the four states used in BB84.

Alice first generates a uniformly random n bit string $x = x_1x_2\ldots x_n$ (a subset of which will provide the shared secret key). She encodes these bits into qubit states using $|0\rangle$ for bit value 0 and $|+\rangle$ for bit value 1. Then she sends them over to Bob (in order). For each received qubit, Bob randomly (with probability half) chooses to measure it in the Z eigenbasis or the X eigenbasis.

(a) **(6 points)** Show that for some of Bob's possible measurement outcomes, he can correctly learn Alice's corresponding bit and know for sure that he has learnt it. For what fraction μ on average, of Alice's bits, will this happen (assuming a perfectly noiseless quantum channel and no eavesdropping)?

Hint. You may assume Bob uses the Z eigenbasis as measurement. For certain measurement outcomes, he could not conclude for sure what Alice has sent, while for some outcomes he can. Similar reasoning applies for using the Z eigenbasis. Hence, you can obtain the fraction μ.

Next in the B92 protocol, Bob (publicly) announces to Alice the positions (i.e. subscripts $1 \le i \le n$) for which he has learn her bit (but does not disclose the bit values themselves), and they both retain only these bits, discarding all the others. In the ideal situation of a noiseless channel and no eavesdropping, the resulting string (of average length μn) gives the desired shared secret key.

(b) **(12 points)** We will consider the simple example of an intercept-resend attack by Eve, while assuming the qubit channel is noiseless. Suppose that Eve measures each passing qubit in the Breidbart basis and sends the post-measurement state on to Bob.
Consider only those qubits for which Alice sent $|0\rangle$. (A similar analysis will apply for $|+\rangle$). Show that the fraction of these for which Bob will think that he has learnt Alice's bit, is the same as the value of μ in 4a.

(c) **(2 points)** Show that for these bits, the bit error rate will be $1/2$, i.e. Bob will conclude the wrong value of Alice's bit for half of these on average.

Hint. You may use the probabilistic branching tree again as taught in class to list out all the possible outcomes Bob obtained. Using the Bob's strategy in 4a, you can answer 4b. As for Problem 4c, calculate $\Pr(B \text{ concludes wrong answers} \mid B \text{ thinks he learnt } A\text{'s bit})$.

5. **(20 points) Simon's algorithm.**
Simon's decision problem is the following:

> *Input*: An oracle for a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ is given.
> *Promise*: f is either (i) a one-to-one function or (ii) a two-to-one function of the following special form — there is an $\xi \in \mathbb{Z}_2^n$ such that $f(x) = f(y)$ if and only if $y = x \oplus \xi$ (i.e. ξ is the hidden period of f when its domain is viewed as being the group $\mathbb{Z}_2^n$).
> *Problem*: determine which of (i) or (ii) is true (with any prescribed success probability $1 - \varepsilon$ for any $\varepsilon > 0$).

It can be argued that for classical computation, this requires at least $O\left(2^{\frac{n}{4}}\right)$ queries to the oracle. In this question we will develop a quantum algorithm that that solves the problem with quantum query complexity only $O(n)$. Even more, the algorithm will determine the period ξ if (ii) holds. Thus (unlike the balanced vs. constant problem) we will have a provable exponential separation between classical and quantum query complexities, even in the presence of bounded error.

To begin, consider $2n$ qubits with the first (resp. last) n comprising the input (resp. output) register for a quantum oracle U_f computing f, i.e. $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$ for any $x, y \in \mathbb{Z}_2^n$.

(a) **(6 points)** With all qubits starting in state $|0\rangle$ apply H to each qubit of the input register, query U_f and then measure the output register (with respect to the computational basis). Write down the generic form of the n-qubit state $|\alpha\rangle$ of the resulting input register, obtained after the measurement. Suppose we then measure $|\alpha\rangle$. Would the result provide any information about the period ξ?

Hint. This bears a resemblance to the *periodic state* as taught in the lecture of quantum Fourier transform. It's recommended that you play with examples with small n, say $n = 3$, e.g.

$$\begin{cases} f(000) = f(001) = 000, \\ f(010) = f(011) = 001, \\ f(100) = f(101) = 010, \\ f(110) = f(111) = 011. \end{cases}$$

Here, the period $\xi = 001$ (you may find the output values do not really matter). Use such a function f as an oracle. Measure the second register of $U_f|x\rangle|y\rangle$ will probably yield different measurement outcomes. Let us assume you get certain outcome $010 \in \mathbb{Z}_2^3$. What is the post-measurement state on the first 3-qubit? You may obtain other outcome, say 111, etc.

(b) **(6 points)** Having obtained $|\alpha\rangle$ as in 5a, apply H to each qubit to obtain a state denoted $|\beta\rangle$. Show that if we measure $|\beta\rangle$ then the n-bit outcome is a uniformly random n-bit string y satisfying $\xi \cdot y = 0$ (so any such y is obtained with probability $1/2^{n-1}$).

Now we can run this algorithm repeatedly, each time independently obtaining another string y satisfying $\xi \cdot y = 0$. Recall that $\mathbb{Z}_2^n$ is a vector space over the field $\mathbb{Z}_2$. If $y_1, \ldots, y_s$ are s linearly independent vectors (bit strings) then their linear span contains 2^s of the 2^n vectors in $\mathbb{Z}_2^n$. Furthermore to solve systems of linear equations over $\mathbb{Z}_2^n$ we can use the standard Gaussian elimination method (calculating with the algebra of the field $\mathbb{Z}_2$), which runs in poly(n) time.

(c) **(Bonus 5 points)** Show that if $(n-1)$ bit strings y are chosen uniformly randomly and independently satisfying $y \cdot \xi = 0$ then they will be linearly independent (and not include the all-zero string $00\ldots0$) with probability

$$\prod_{k=1}^{n-1}\left(1 - \frac{2^{k-1}}{2^{n-1}}\right) = \frac{1}{2}\prod_{k=1}^{n-2}\left(1 - \frac{2^{k-1}}{2^{n-1}}\right).$$

Show that this is at least $\frac{1}{4}$. (It may be helpful here to recall that for a and b in $[0,1]$ we have $(1-a)(1-b) \geq 1-(a+b)$).

(d) **(8 points)** Show how the above algorithm may be used to solve Simon's problem with $O(n)$ quantum query complexity (for any desired success probability $0 < 1-\varepsilon < 1$).

Remark. Here, we briefly illustrate why the problem is classically hard; suppose that (ii) actually holds. Then we will argue that we need to query f an exponential number of times to have a reasonable probability of noticing that f is not one-to-one. Indeed, we obtain no information until we are lucky enough to choose two queries x and y with $f(x) = f(y)$ i.e. $x \oplus y = \xi$. Suppose for example that we choose $M = 2^{n/4}$ queries (independently and uniformly at random). Then the number of pairs of queries is $\binom{M}{2} \leq (2^{n/4})^2$ and for each pair the probability that $x \oplus y = \xi$ is 2^{-n}. Thus the probability of successfully seeing the existence of ξ is less than $2^{-n}(2^{n/4})^2 = 2^{-n/2}$ i.e. even as many as $2^{n/4}$ queries cannot notice the difference between between (i) and (ii) with better than an exponentially small probability and hence cannot form the basis of any *bounded* error algorithm. This argument can be made rigorous e.g. allowing arbitrary strategies for choices for queries, but we omit the technicalities here. For more details see D. Simon "On the power of quantum computation," *S.I.A.M. Journal on Computing*, 28, p1474–1483, 1997.