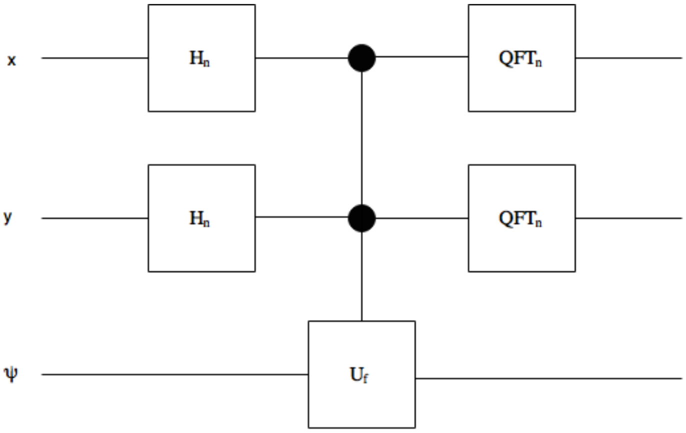
Quantum Information Theory - Homework 05

Roei Rosenzweig 313590937 ♦ 205798440 Roey Maor

July 6, 2017

1 Question 1 - Discrete Logarithm Problem

1. We use the following circuit (where x, y, and ψ are $\left|0\right\rangle_n$):



Its easy to see that this circuit produces the desired state:

$$\begin{aligned}
\left|0\right\rangle_n \left|0\right\rangle_n \left|0\right\rangle_n &\to \left(\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}\left|i\right\rangle\right)\left(\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}\left|i\right\rangle\right)\left|0\right\rangle_n && (H_n\otimes H_n)\\
&= \frac{1}{2^n}\sum_{i=0}^{2^n-1}\sum_{j=0}^{2^n-1}\left|i\right\rangle\left|j\right\rangle\left|0\right\rangle_n\\
&\to \frac{1}{2^n}\sum_{i=0}^{2^n-1}\sum_{j=0}^{2^n-1}\left|i\right\rangle\left|j\right\rangle\left|f\left(i,\,j\right)\right\rangle_n && (U_f)\\
&= \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\left|x\right\rangle\left|y\right\rangle\left|f\left(x,\,y\right)\right\rangle_n && \text{(changing names)}\\
&\to \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\left(\frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1}e^{\frac{2\pi i\cdot lx}{2^n}}\left|l\right\rangle\otimes\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}e^{\frac{2\pi i\cdot ky}{2^n}}\left|k\right\rangle\right)\left|f\left(x,\,y\right)\right\rangle_n && (QFT_n\otimes QFT_n)\\
&= \frac{1}{2^{2n}}\sum_{x,y,l,k=0}^{2^n-1}e^{\frac{2\pi i\cdot lx}{2^n}}e^{\frac{2\pi i\cdot ky}{2^n}}\left|l\right\rangle\left|k\right\rangle\left|f\left(x,\,y\right)\right\rangle_n\\
&= \boxed{\frac{1}{2^{2n}}\sum_{x,y,\ell_1,\ell_2=0}^{2^n-1}e^{\frac{2\pi i\cdot(\ell_1x+\ell_2y)}{2^n}}\left|\ell_1\right\rangle\left|\ell_2\right\rangle\left|f\left(x,\,y\right)\right\rangle_n}
\end{aligned}$$

2.

$$\begin{aligned}
f\left(x,y\right) &= g^x a^y \mod N\\
&= g^x\left(g^s\right)^y \mod N\\
&= g^{x+sy} \mod N
\end{aligned}$$

3.

$$\begin{aligned}
&f\left(x_1, y_1\right) = f\left(x_2, y_2\right) \mod N && \iff \\
&g^{x_1+sy_1} = g^{x_2+sy_2} \mod N && \iff \\
&g^{\left(x_1+sy_1\right)-\left(x_2+sy_2\right)} = 1 \mod N
\end{aligned}$$

The third equation is derived by multiplying with the inverse of $g^{x_2+sy_2}$, which must exist because $\mathbb{Z}_N$ is a group.

4.

$$\begin{aligned}
&f\left(x_1, y_1\right) = f\left(x_2, y_2\right) \mod N && \iff \\
&g^{\left(x_1+sy_1\right)-\left(x_2+sy_2\right)} = 1 \mod N && \iff \\
&\left(x_1+sy_1\right)-\left(x_2+sy_2\right) = (N-1)\cdot k && \text{for k} \in \mathbb{Z} \iff \\
&\left(x_1+sy_1\right)-\left(x_2+sy_2\right) = 0 \mod (N-1) && \iff \\
&x_1+sy_1 = x_2+sy_2 \mod (N-1)
\end{aligned}$$

5. We can use the previous section: $x_1 = x - sk$, $y_1 = y + k$, $x_2 = x$, $y_2 = y$. When we plug everything in we get:

$$x - sk + sk + sy = x + sy \mod N - 1$$

which are indeed equal. So we get $f(x, y) = f(x - sk, y + k)$.

6. The (not normalized) state we are left with after the partial measurement is

$$\left|f\left(x_0, y_0\right)\right\rangle \cdot \left(\frac{1}{2^{2n}} \sum_{x,y,\ell_1,\ell_2=0}^{2^n-1} e^{\frac{2\pi i\cdot\left(\ell_1 x+\ell_2 y\right)}{2^n}} \left|\ell_1\right\rangle \left|\ell_2\right\rangle \left|f\left(x,\, y\right)\right\rangle_n\right)$$

which is essentialy equivilent to eliminating from the sum any pair of x, y which **does not** hold $f\left(x_0, y_0\right) = f(x, y)$. By using subsection (4), we know that the group of (x, y) that does hold this equation are

$$\left\{(x, y) : x + ys = x_0 + y_0 s = c\ (\mod N-1)\right\}$$

so the (not normalized) state after the partial measurement is:

$$\sum_{\ell_1,\ell_2=0}^{2^n-1} \sum_{(x,y)\in\{(x,y):x+ys=c(\mod N-1)\}} e^{\frac{2\pi i\cdot\left(\ell_1 x+\ell_2 y\right)}{2^n}} \left|\ell_1\right\rangle \left|\ell_2\right\rangle$$

7.

2 Question 2 - Quantum Communication

1. If Alice and Bob are using classic and deterministic methods, then each one of them has a table which says what output bit they will send depending on the input bit they will get. We can analyze all the possible scenarios. We denote the 'choosing function' for Alice with f_A, and f_B for Bob.

   - $f_A(x) = 1 - x$, $f_B = x$: Alice and Bob we succeed only if $\left(x_a, x_b\right) \in \{(1,0), (0,1)\}$, which makes it a $\frac{2}{4}$ chance of success method.
   - $f_A(x) = x$, $f_B(x) = x$: Alice and Bob we succeed only if $\left(x_a, x_b\right) \in \{(0,0)\}$, which makes it a $\frac{1}{4}$ chance of success method.
   - $f_A(x) = 0$, $f_B(x) = x$: Alice and Bob we succeed only if $\left(x_a, x_b\right) \in \{(1,1), (1,0), (0,0)\}$, which makes it a $\frac{3}{4}$ chance of success method.

   The other scenarios are similar, and wont produce greater chance of success.

2. Resulting state after Alice's operation:

   - In standard base: $\dfrac{\begin{pmatrix}\cos\alpha\\ \sin\alpha\end{pmatrix}|0\rangle - \begin{pmatrix}-\sin\alpha\\ \cos\alpha\end{pmatrix}|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}\cos\alpha\\ 0\\ \sin\alpha\\ 0\end{pmatrix} - \begin{pmatrix}0\\ -\sin\alpha\\ 0\\ \cos\alpha\end{pmatrix}\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}\cos\alpha\\ \sin\alpha\\ \sin\alpha\\ -\cos\alpha\end{pmatrix}$

- In Bell's base: $\begin{pmatrix} | & | & | & | \\ \phi_+ & \phi_- & \psi_+ & \psi_- \\ | & | & | & | \end{pmatrix}^\dagger \left(\frac{1}{\sqrt{2}} \begin{pmatrix} \cos\alpha \\ \sin\alpha \\ \sin\alpha \\ -\cos\alpha \end{pmatrix} \right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix} \left(\frac{1}{\sqrt{2}} \begin{pmatrix} \cos\alpha \\ \sin\alpha \\ \sin\alpha \\ -\cos\alpha \end{pmatrix} \right) = \frac{1}{2} \begin{pmatrix} 0 \\ 2\cos\alpha \\ 2\sin\alpha \\ 0 \end{pmatrix} = \boxed{\cos\alpha\left|\phi_-\right\rangle + \sin\alpha\left|\psi_+\right\rangle}$

3. Alice will perform R_α operation on her qubit, and Bob will perform $R_\beta^\dagger$ (which is essentialy $R_{-\beta}$) on his qubit. The state in stadard base is:

$$R_\beta^\dagger \cdot \left(\frac{1}{\sqrt{2}} \begin{pmatrix} \cos\alpha \\ \sin\alpha \\ \sin\alpha \\ -\cos\alpha \end{pmatrix} \right) = \frac{1}{\sqrt{2}} \begin{pmatrix} \cos\beta & \sin\beta & 0 & 0 \\ -\sin\beta & \cos\beta & 0 & 0 \\ 0 & 0 & \cos\beta & \sin\beta \\ 0 & 0 & -\sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} \cos\alpha \\ \sin\alpha \\ \sin\alpha \\ -\cos\alpha \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \cos\alpha\cos\beta + \sin\alpha\sin\beta \\ -\cos\alpha\sin\beta + \sin\alpha\cos\beta \\ \sin\alpha\cos\beta - \cos\alpha\sin\beta \\ -\sin\alpha\sin\beta - \cos\alpha\cos\beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \cos(\alpha-\beta) \\ \sin(\alpha-\beta) \\ \sin(\alpha-\beta) \\ -\cos(\alpha-\beta) \end{pmatrix}$$

   Now we can transform it to Bell's base:

$$\begin{pmatrix} | & | & | & | \\ \phi_+ & \phi_- & \psi_+ & \psi_- \\ | & | & | & | \end{pmatrix}^\dagger \left(\frac{1}{\sqrt{2}} \begin{pmatrix} \cos(\alpha-\beta) \\ \sin(\alpha-\beta) \\ \sin(\alpha-\beta) \\ -\cos(\alpha-\beta) \end{pmatrix} \right) = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} \cos(\alpha-\beta) \\ \sin(\alpha-\beta) \\ \sin(\alpha-\beta) \\ -\cos(\alpha-\beta) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 0 \\ 2\cos(\alpha-\beta) \\ 2\sin(\alpha-\beta) \\ 0 \end{pmatrix} = \boxed{\cos(\alpha-\beta)\left|\phi_-\right\rangle + \sin(\alpha-\beta)\left|\psi_+\right\rangle}$$

   Alice and Bob will measure the same bit with a probablity of $\frac{\cos^2(\alpha-\beta)}{\cos^2(\alpha-\beta)+\sin^2(\alpha-\beta)} = \boxed{\cos^2(\alpha-\beta)}$ (The probability of measuring $\left|\phi_-\right\rangle$ in Bell's base).

4. Rational: Alice and Bob know that if they got 0 as their input, they should choose the same bit as output (so that $a \oplus b = 0$). So, we can use what we learned in the previous sections: Alice and Bob will share the state $\left|\phi_-\right\rangle$ before the procedure starts, and will perform R_α and R_β as described before, with α and β that will depend on their input. Then, they will measure the resulting state (which we calculated in section 3), and send the result as output bit. $Pr\{a \oplus b = 0\} = \cos^2(\alpha-\beta)$, so if one participant (either Alice or Bob) get 0 input, he/she should choose his angle so that $\cos^2(\alpha-\beta)$ will be **maximized**. We denote by α_1 the angle Alice chooses if she gets 0, and α_2 the values she chooses for 1. Respectivly, we denote by β_1,β_2 these angles for Bob. The probability for success is given by:

$$p(\alpha_1,\alpha_2,\beta_1,\beta_2) = \frac{1}{4}\left(\cos^2(\alpha_1-\beta_1) + \cos^2(\alpha_2-\beta_1) + \cos^2(\alpha_1-\beta_2) + \sin^2(\alpha_2-\beta_2)\right)$$

   There is probably a vector $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \beta_1 \\ \beta_2 \end{pmatrix}$ for which $p > \frac{3}{4}$, but we weren't successful in finding it...

3 Question 3 - Quantum Encryption Protocol BHM96

1. First, lets compute the projection of $\left|\psi_-\right\rangle$ on the various possible states:

   - $\left|00\right\rangle \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} = 0$
   - $\left|01\right\rangle \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}$
   - $\left|10\right\rangle \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} = \frac{-1}{\sqrt{2}}$
   - $\left|11\right\rangle \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} = 0$
   - $\left|++\right\rangle \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} = \frac{1}{2} - \frac{1}{2} = 0$
   - $\left|+-\right\rangle \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}$
   - $\left|-+\right\rangle \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} = \frac{-1}{\sqrt{2}}$
   - $\left|--\right\rangle \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} = 0$

   From these results, we learn that if Alice and Bob use the same base, and the Center measures $\left|\psi_-\right\rangle$, then Alice and Bob's results must be opposites of each other. Thus, if bob switches his bit, he and Alice will hold the same bit - they will both hold Alice's bit. From the Center point of view, if Alice and Bob choose the standard base then the Center doesn't learn anything about Alice's bit. We show that by partial trace on A:

$$\begin{aligned} tr_A(\psi_-) &= \left|0\right\rangle \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} \frac{\left\langle 01\right| - \left\langle 10\right|}{\sqrt{2}} \left\langle 0\right| + \left|1\right\rangle \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} \frac{\left\langle 01\right| - \left\langle 10\right|}{\sqrt{2}} \left\langle 1\right| \\ &= \frac{\left|0\right\rangle\left\langle 0\right|}{2} + \frac{\left|1\right\rangle\left\langle 1\right|}{2} \end{aligned}$$

   we get the **completely mixed state**, so this measurement doesn't add any information for Center regarding Alice's bit.

2.

3.

4 Question 4 - Implementation of Quantum Error Correction Code

1.

   (a) The overall state before any operators are applied: $\alpha|000\rangle + \beta|100\rangle$. After the first CNOT we get $\alpha|000\rangle + \beta|110\rangle$, and after the second CNOT we get $\alpha|000\rangle + \beta|111\rangle$.

   (b) For brevity, each arrow represent an operator, according to order in which their applied in the circuit.

$$\begin{aligned}
&\alpha|000\rangle + \beta|111\rangle \to \alpha|000\rangle + \beta|101\rangle \to \alpha|000\rangle + \beta|100\rangle \to \alpha|000\rangle + \beta|100\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle \\
&\alpha|100\rangle + \beta|011\rangle \to \alpha|110\rangle + \beta|011\rangle \to \alpha|111\rangle + \beta|011\rangle \to \alpha|011\rangle + \beta|111\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |11\rangle \\
&\alpha|010\rangle + \beta|101\rangle \to \alpha|010\rangle + \beta|111\rangle \to \alpha|010\rangle + \beta|110\rangle \to \alpha|010\rangle + \beta|110\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |10\rangle \\
&\alpha|001\rangle + \beta|110\rangle \to \alpha|001\rangle + \beta|100\rangle \to \alpha|001\rangle + \beta|101\rangle \to \alpha|001\rangle + \beta|101\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |01\rangle
\end{aligned}$$

2. Like before, arrows denote operators in chronical order.

   (a)

$$\alpha|000\rangle + \beta|100\rangle \to \alpha|000\rangle + \beta|110\rangle \to \alpha|000\rangle + \beta|111\rangle \to \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle$$

   (b) It is suffice to show that after the first Hadamard operator, we get the states described in section (1.b):

$$\begin{aligned}
\alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle &\to \alpha|000\rangle + \beta|111\rangle \\
\alpha|{-}{+}{+}\rangle + \beta|{+}{-}{-}\rangle &\to \alpha|100\rangle + \beta|011\rangle \\
\alpha|{+}{-}{+}\rangle + \beta|{-}{+}{-}\rangle &\to \alpha|010\rangle + \beta|101\rangle \\
\alpha|{+}{+}{-}\rangle + \beta|{-}{-}{+}\rangle &\to \alpha|001\rangle + \beta|110\rangle
\end{aligned}$$

3.

$$\begin{aligned}
|\psi\rangle|0\rangle_8 &= \alpha|000\rangle \otimes |000\rangle \otimes |000\rangle + \beta|100\rangle \otimes |000\rangle \otimes |000\rangle \\
&\to \alpha|000\rangle \otimes |000\rangle \otimes |000\rangle + \beta|100\rangle \otimes |100\rangle \otimes |000\rangle \\
&\to \alpha|000\rangle \otimes |000\rangle \otimes |000\rangle + \beta|100\rangle \otimes |100\rangle \otimes |100\rangle \\
&\to \alpha\frac{1}{2\sqrt{2}}(|000\rangle + |100\rangle) \otimes (|000\rangle + |100\rangle) \otimes (|000\rangle + |100\rangle) + \beta\frac{1}{2\sqrt{2}}(|000\rangle - |100\rangle) \otimes (|000\rangle - |100\rangle) \otimes (|000\rangle - |100\rangle) \\
&\to \alpha\frac{1}{2\sqrt{2}}(|000\rangle + |110\rangle) \otimes (|000\rangle + |110\rangle) \otimes (|000\rangle + |110\rangle) + \beta\frac{1}{2\sqrt{2}}(|000\rangle - |110\rangle) \otimes (|000\rangle - |110\rangle) \otimes (|000\rangle - |110\rangle) \\
&\to \alpha\frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) + \beta\frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)
\end{aligned}$$

4.