ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

Introduction to Quantum Computation — Assignment date: June 21, 2023, 15:15

Spring 2023 — Due date: June 21, 2023, 18:15

Final Exam – CS 308 – Room CO1

Write your name and section below and hand back this handout.

There are 3 problems. No electronic devices allowed.

Good luck!

We recall the following matrices used throughout:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Name: _____

Section: _____

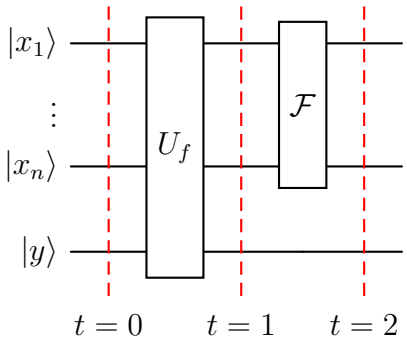
Sciper No.: _____

Problem 1	/ 30
Problem 2	/ 40
Problem 3	/ 30
Total	/100

Problem 1. *A Bernstein-Vazirani algorithm modulo p* (30pts)

Let $x_1, \ldots, x_n$ and $a_1, \ldots, a_n, b$ be integers modulo p. Consider the function $(x_1, \ldots, x_n) \mapsto f(\underline{x}) = a_1 x_1 + \cdots + a_n x_n + b = \underline{a} \cdot \underline{x} + b$ with the sum taken modulo p. We suppose p is a prime number.

The vector $(a_1, \ldots, a_n)$ is "hidden" and the goal is to use a quantum circuit to determine it. We assume that an Oracle computes the function for each entry. Take the following circuit:



The Hilbert space associated with each wire is $\mathbb{C}^p$ and is spanned by states $|0\rangle, |1\rangle, \ldots, |p-1\rangle$. The circuit is initialized in the state

$$|\psi_0\rangle = \left(\frac{1}{p^{\frac{n}{2}}} \sum_{(x_1,\ldots,x_n)\in\{0,\ldots,p-1\}^n} |x_1, \ldots, x_n\rangle \right) \otimes \left(\frac{1}{\sqrt{p}} \sum_{y=0}^{p-1} e^{\frac{2\pi i y}{p}} |y\rangle \right)$$

and the Oracle acts as $U_f(|x_1, \ldots, x_n\rangle \otimes |y\rangle) = |x_1, \ldots, x_n\rangle \otimes |y + f(x_1, \ldots, x_n)\rangle$ where $y + f(x_1, \ldots, x_n)$ is taken modulo p. Moreover, we define the QFT:

$$\mathcal{F}|x_1, \ldots, x_n\rangle = \frac{1}{p^{\frac{n}{2}}} \sum_{(u_1,\ldots,u_n)\in\{0,\ldots,p-1\}^n} e^{\frac{2\pi i}{p}(x_1u_1+\cdots+x_nu_n)} |u_1, \ldots, u_n\rangle$$

1. Compute the state just after the Oracle. Explain in one sentence what is the "kick-back phenomenon".

2. Compute the state at the output of the circuit.

   Hint: For p prime we have that these two sets are equal for any $z \neq 0$:
   $\{0 \bmod p, z \bmod p, 2z \bmod p, 3z \bmod p, ..., (p-1)z \bmod p\} = \{0, 1, 2, 3, ..., p-1\}$.

3. Explain how one can determine $(a_1, \ldots, a_n)$ by measuring the output and, in particular, state what is the measurement basis. Can one determine b?

Solution to problem 1: (total 30 pts)

1. **(10pts)**

$$
\begin{aligned}
|\psi_1\rangle = U_f\,|\psi_0\rangle &= U_f\left(\frac{1}{p^{\frac{n}{2}}}\sum_{x_1,\ldots,x_n}|x_1,\ldots,x_n\rangle\right)\otimes\left(\frac{1}{\sqrt{p}}\sum_y e^{\frac{2\pi i y}{p}}|y\rangle\right)\\
&= \frac{1}{p^{\frac{n}{2}}}\sum_{x_1,\ldots,x_n} U_f\left(|x_1,\ldots,x_n\rangle\otimes\left(\frac{1}{\sqrt{p}}\sum_y e^{\frac{2\pi i y}{p}}|y\rangle\right)\right) =\\
&= \frac{1}{p^{\frac{n}{2}}}\sum_{x_1,\ldots,x_n}|x_1,\ldots,x_n\rangle\otimes\left(\frac{1}{\sqrt{p}}\sum_y e^{\frac{2\pi i y}{p}}|y+f(\underline{x})\rangle\right) =\\
&= \frac{1}{p^{\frac{n}{2}}}\sum_{x_1,\ldots,x_n}|x_1,\ldots,x_n\rangle\otimes e^{-\frac{2\pi i f(\underline{x})}{p}}\left(\frac{1}{\sqrt{p}}\sum_y e^{\frac{2\pi i(y+f(\underline{x}))}{p}}|y+f(\underline{x})\rangle\right) =\\
&\overset{y'\equiv(y+f(\underline{x}))\ \mathrm{mod}\ p=y+f(\underline{x})}{=} \frac{1}{p^{\frac{n}{2}}}\sum_{x_1,\ldots,x_n}|x_1,\ldots,x_n\rangle\otimes e^{-\frac{2\pi i f(\underline{x})}{p}}\left(\frac{1}{\sqrt{p}}\sum_{y'} e^{\frac{2\pi i y'}{p}}|y'\rangle\right) =\\
&= \left(\frac{1}{p^{\frac{n}{2}}}\sum_{x_1,\ldots,x_n} e^{-\frac{2\pi i f(\underline{x})}{p}}|x_1,\ldots,x_n\rangle\right)\otimes\left(\frac{1}{\sqrt{p}}\sum_{y'} e^{\frac{2\pi i y'}{p}}|y'\rangle\right).
\end{aligned}
$$

The kick-back phenomenon is a result of the circuit application where the information in the (ancilla) second register becomes a relative phase in the first register.

2. **(15pts)** As the input state is separable and $\mathcal{F}$ is only applied to the n principal entries, not to the ancilla one, we have:

$$
\begin{aligned}
&\mathcal{F}\left(\frac{1}{p^{\frac{n}{2}}}\sum_{x_1,\ldots,x_n} e^{-\frac{2\pi i f(\underline{x})}{p}}|x_1,\ldots,x_n\rangle\right) =\\
&= \frac{1}{p^{\frac{n}{2}}}\sum_{\underline{x}\in\{0,\ldots,p-1\}^n} e^{-\frac{2\pi i f(\underline{x})}{p}}\left(\frac{1}{p^{\frac{n}{2}}}\sum_{\underline{u}\in\{0,\ldots,p-1\}^n} e^{\frac{2\pi i}{p}(x_1u_1+\cdots+x_nu_n)}|u_1,\ldots,u_n\rangle\right) =\\
&= \frac{1}{p^n}\sum_{\underline{x}\in\{0,\ldots,p-1\}^n}\sum_{\underline{u}\in\{0,\ldots,p-1\}^n} e^{\frac{2\pi i}{p}(x_1u_1+\cdots+x_nu_n-f(\underline{x}))}|u_1,\ldots,u_n\rangle =\\
&= \frac{1}{p^n}\sum_{\underline{x}\in\{0,\ldots,p-1\}^n}\sum_{\underline{u}\in\{0,\ldots,p-1\}^n} e^{\frac{2\pi i}{p}(\underline{u}\cdot\underline{x}-\underline{a}\cdot\underline{x}-b)}|u_1,\ldots,u_n\rangle =\\
&= \frac{1}{p^n}e^{-\frac{2\pi i b}{p}}\sum_{\underline{u}\in\{0,\ldots,p-1\}^n}\left(\sum_{\underline{x}\in\{0,\ldots,p-1\}^n} e^{\frac{2\pi i}{p}[(\underline{u}-\underline{a})\cdot\underline{x}]}\right)|u_1,\ldots,u_n\rangle.
\end{aligned}
$$

Now, simplifying the coefficient:

$$\sum_{\underline{x}\in\{0,\dots,p-1\}^n} e^{\frac{2\pi i}{p}[(\underline{u}-\underline{a})\cdot\underline{x}]} = \sum_{\underline{x}\in\{0,\dots,p-1\}^n} e^{\frac{2\pi i}{p}[(u_1-a_1)x_1]}\cdot\ldots\cdot e^{\frac{2\pi i}{p}[(u_n-a_n)x_n]} =$$

$$= \left(\sum_{x_1\in\{0,\dots,p-1\}} e^{\frac{2\pi i}{p}[(u_1-a_1)x_1]}\right)\cdot\ldots\cdot\left(\sum_{x_n\in\{0,\dots,p-1\}} e^{\frac{2\pi i}{p}[(u_n-a_n)x_n]}\right) =$$

$$= \prod_{i=1\dots n}\left(\sum_{x_i\in\{0,\dots,p-1\}} e^{\frac{2\pi i}{p}[(u_i-a_i)x_i]}\right) = \prod_{i=1\dots n}\left(\sum_{x_i\in\{0,\dots,p-1\}} e^{\frac{2\pi i}{p}[((u_i-a_i)\mod p)x_i]}\right)$$

If $u_i-a_i \not\equiv 0 \mod p$, set of $\{(u_i-a_i)\cdot 0 \bmod p, (u_i-a_i)\cdot 1 \bmod p, \dots, (u_i-a_i)\cdot(p-1) \bmod p\}$ makes a complete set of remainders $\{0,1,\dots,p-1\}$ *because p is prime.* Then:

$$\sum_{x_i\in\{0,\dots,p-1\}} e^{\frac{2\pi i}{p}[((u_i-a_i)\mod p)x_i]} =$$

$$= \begin{cases} \sum_{x_i\in\{0,\dots,p-1\}} e^{\frac{2\pi i}{p}\cdot 0} = \sum_{x_i\in\{0,\dots,p-1\}} 1 = p, u_i = a_i \\ \sum_{x_i'\in\{0,\dots,p-1\}} e^{\frac{2\pi i}{p}x_i'} = \frac{1\cdot\left(1-\left(e^{\frac{2\pi i}{p}}\right)^p\right)}{1-e^{\frac{2\pi i}{p}}} = 0, u_i \neq a_i \end{cases} = p\cdot\mathbb{1}\left[u_i = a_i\right].$$

Therefore:

$$\sum_{\underline{x}\in\{0,\dots,p-1\}^n} e^{\frac{2\pi i}{p}[(\underline{u}-\underline{a})\cdot\underline{x}]} = \prod_{i=1\dots n}\left(p\cdot\mathbb{1}\left[u_i = a_i\right]\right) = p^n\mathbb{1}\left[\underline{u} = \underline{a}\right],$$

and

$$\mathcal{F}\left(\frac{1}{p^{\frac{n}{2}}}\sum_{\underline{x}\in\{0,\dots,p-1\}^n} e^{-\frac{2\pi i f(\underline{x})}{p}}|x_1,\dots,x_n\rangle\right) = \frac{1}{p^n}e^{-\frac{2\pi i b}{p}}\sum_{\underline{u}\in\{0,\dots,p-1\}^n} p^n\mathbb{1}\left[\underline{u} = \underline{a}\right]\cdot|u_1,\dots,u_n\rangle =$$

$$= e^{-\frac{2\pi i b}{p}}|a_1,\dots,a_n\rangle$$

All in all, the output state is:

$$|\psi_2\rangle = \left(e^{-\frac{2\pi i b}{p}}|a_1,\dots,a_n\rangle\right)\otimes\left(\frac{1}{\sqrt{p}}\sum_y e^{\frac{2\pi i y}{p}}|y\rangle\right).$$

3. **(5pts)** States $|0\rangle, |1\rangle, \dots, |p-1\rangle$ can be presented as vectors in $\mathbb{C}^p$:

$$|0\rangle = \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \quad |1\rangle = \begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}, \quad \dots, \quad |p-1\rangle = \begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}.$$

The computational basis is then $|u_1 \dots u_n y\rangle = |x_1\rangle \otimes \dots \otimes |u_n\rangle \otimes |y\rangle$, $u_1, \dots, u_n, y \in \{0, \dots, p-1\}$ and we measure the first n entries in the same basis by using the set of projectors:

$$\{|u_1, \dots, u_n\rangle\langle u_1, \dots, u_n| \text{ such that } \otimes I \mid u_1, \dots, u_n \in \{0, \dots, p-1\}\},$$

where I is identity matrix of size $p \times p$ and acts on the last entry. We obtain $|a_1, \dots, a_n\rangle$ with probability 1, as:

$$\begin{aligned}\mathbb{P}\left(|u_1, \dots, u_n\rangle\right) &= \langle \psi_2 \mid |u_1, \dots, u_n\rangle\langle u_1, \dots, u_n| \otimes I \mid \psi_2\rangle = \\ &= \left|e^{-\frac{2\pi i b}{p}}\right|^2 \langle a_1, \dots, a_n | u_1, \dots, u_n\rangle^2 = \begin{cases} 1, & \underline{u} = \underline{a}, \\ 0, & \underline{u} \neq \underline{a} \end{cases}\end{aligned}$$

In the output, b is only present in the global phase $e^{-\frac{2\pi i b}{p}}$ which cannot be measured, no matter what the basis.

Problem 2. *Quantum random walks on a one-dimensional line* (40pts)

In this problem we look at a quantum random walk and compare it to the simplest classical random walk.

Consider first a classical coin with two possible outcomes $s = -1$ (heads) or $s = +1$ (tail) each with probability $\frac{1}{2}$. The position of a discrete classical random walk on a one dimensional lattice is labelled by a natural integer $x \in \mathbb{Z}$ (thus $x = \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$) and evolves as follows:

- at time $t = 0$ the initial state is $x_0 = 0$.
- for each $t \in \mathbb{N}$ we toss the coin and look at the outcome $s_t = \pm 1$ of the coin and update the position as $x_{t+1} = x_t + s_t$ (coin tosses are independent and identically uniformly distributed as indicated above).

1. Compute the probabilities of the outcomes for $t = 0, 1, 2, 3$ and complete this table:

	$\ldots$	$\mathbb{P}[x_t = -1]$	$\mathbb{P}[x_t = 0]$	$\mathbb{P}[x_t = 1]$	$\ldots$
$t = 0$					
$\vdots$					
$t = 3$					

Now we define the quantum walk on the one dimensional line. Consider a qubit in $\mathbb{C}^2$ with two orthonormal computational basis states $|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. This qubit plays the role of the "coin". The state of the walk belongs to another Hilbert space $\mathcal{H}$ spanned by orthonormal states $\{|x\rangle,\ x \in \mathbb{Z}\}$. The state of the composite system coin+walk is denoted by $|\psi\rangle \in \mathbb{C}^2 \otimes \mathcal{H}$ and evolves as follows:

- at time $t = 0$ the initial state is $|\psi_0\rangle = |\uparrow\rangle \otimes |0\rangle$.
- for $t \in \mathbb{N}$ update the state as $|\psi_{t+1}\rangle = S(H \otimes I)|\psi_t\rangle$ where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{and} \qquad S = |\uparrow\rangle\langle\uparrow| \otimes \sum_{x \in \mathbb{Z}} |x+1\rangle\langle x| + |\downarrow\rangle\langle\downarrow| \otimes \sum_{x \in \mathbb{Z}} |x-1\rangle\langle x|$$

  Here H represents a coin "toss" and S the "shift" of the position of the walk on the lattice.

2. Compute the state vectors $|\psi_t\rangle$ for $t = 0, 1, 2, 3$.

3. Suppose first that we observe the position of the walk at the final time $t = 3$. This corresponds to do a measurement with the set of projectors $\{I \otimes |x\rangle\langle x|,\ x \in \mathbb{Z}\}$. Compute the resulting possible states $|x\rangle$ and corresponding probabilities.

4. Similarly to above, compute also the resulting states and probabilities that would result from measurement at times $t = 0, 1, 2$, and the complete the following table:

	$\ldots$	$\mathbb{P}[x_t = -1]$	$\mathbb{P}[x_t = 0]$	$\mathbb{P}[x_t = 1]$	$\ldots$
$t = 0$					
$\vdots$					
$t = 3$					

5. Draw a circuit corresponding to the quantum walk and measurement at time $t = 3$.

6. Suppose we would do a measurement at each time step and update the state after each measurement. *Guess without calculations* which of the above two tables of probabilities you would obtain ? Give a short two sentence argument (no calculation).

Solution to problem 2: (total 40pts)

1. **(5pts)**

	$\mathbb{P}[x_t=-3]$	$\mathbb{P}[x_t=-2]$	$\mathbb{P}[x_t=-1]$	$\mathbb{P}[x_t=0]$	$\mathbb{P}[x_t=1]$	$\mathbb{P}[x_t=2]$	$\mathbb{P}[x_t=3]$
$t=0$	0	0	0	1	0	0	0
$t=1$	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0
$t=2$	0	$\frac{1}{4}$	0	$\frac{1}{2}$	0	$\frac{1}{4}$	0
$t=3$	$\frac{1}{8}$	0	$\frac{3}{8}$	0	$\frac{3}{8}$	0	$\frac{1}{8}$

(For $n \geq 4$, $\mathbb{P}[x_t = \pm n] = 0$ for $t = 0, 1, 2, 3$.)

2. **(15pts)** Note that $H|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$ and $H|\downarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle)$.

For $t=0$, $|\psi_0\rangle = |\uparrow\rangle \otimes |0\rangle$ by definition.

For $t=1$:

$$\begin{aligned}
|\psi_1\rangle &= S(H\otimes I)|\psi_0\rangle = S\left(H|\uparrow\rangle \otimes I|0\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left[|\uparrow\rangle\langle\uparrow| \otimes \sum_{x\in\mathbb{Z}} |x+1\rangle\langle x| + |\downarrow\rangle\langle\downarrow| \otimes \sum_{x\in\mathbb{Z}} |x-1\rangle\langle x|\right](|\uparrow\rangle\otimes|0\rangle + |\downarrow\rangle\otimes|0\rangle) = \\
&= \frac{1}{\sqrt{2}}\left(|\uparrow\rangle \otimes \left(\left[\sum_{x\in\mathbb{Z}} |x+1\rangle\langle x|\right]|0\rangle\right) + |\downarrow\rangle \otimes \left(\left[\sum_{x\in\mathbb{Z}} |x-1\rangle\langle x|\right]|0\rangle\right)\right) \\
&= \frac{1}{\sqrt{2}}\left(|\uparrow\rangle\otimes|1\rangle + |\downarrow\rangle\otimes|-1\rangle\right).
\end{aligned}$$

For $t=2$:

$$\begin{aligned}
|\psi_2\rangle = S(H\otimes I)|\psi_1\rangle &= \frac{1}{\sqrt{2}} S\left(H|\uparrow\rangle\otimes I|1\rangle + H|\downarrow\rangle\otimes I|-1\rangle\right) \\
&= \frac{1}{2} S\left(|\uparrow\rangle\otimes|1\rangle + |\downarrow\rangle\otimes|1\rangle + |\uparrow\rangle\otimes|-1\rangle - |\downarrow\rangle\otimes|-1\rangle\right) \\
&= \frac{1}{2}\left(|\uparrow\rangle\otimes|2\rangle + |\downarrow\rangle\otimes|0\rangle + |\uparrow\rangle\otimes|0\rangle - |\downarrow\rangle\otimes|-2\rangle\right)
\end{aligned}$$

For $t=3$:

$$\begin{aligned}
|\psi_3\rangle =& S(H\otimes I)|\psi_2\rangle = \\
=& \frac{1}{2\sqrt{2}} S(|\uparrow\rangle\otimes|2\rangle + |\downarrow\rangle\otimes|2\rangle + |\uparrow\rangle\otimes|0\rangle - |\downarrow\rangle\otimes|0\rangle \\
&+ |\uparrow\rangle\otimes|0\rangle + |\downarrow\rangle\otimes|0\rangle - |\uparrow\rangle\otimes|-2\rangle + |\downarrow\rangle\otimes|-2\rangle) = \\
=& \frac{1}{2\sqrt{2}} S(|\uparrow\rangle\otimes|2\rangle + |\downarrow\rangle\otimes|2\rangle + 2|\uparrow\rangle\otimes|0\rangle - |\uparrow\rangle\otimes|-2\rangle + |\downarrow\rangle\otimes|-2\rangle) = \\
=& \frac{1}{2\sqrt{2}}(|\uparrow\rangle\otimes|3\rangle + |\downarrow\rangle\otimes|1\rangle + 2|\uparrow\rangle\otimes|1\rangle - |\uparrow\rangle\otimes|-1\rangle + |\downarrow\rangle\otimes|-3\rangle)
\end{aligned}$$

3. **(10pts)** Let $a_1, a_2 \in \{\uparrow, \downarrow\}, x_1, x_2 \in \mathbb{Z}$. Obviously,

$$(\langle a_2| \otimes \langle x_2|)\,(I \otimes |x\rangle\langle x|)\,(|a_1\rangle \otimes |x_1\rangle) = \langle a_2|a_1\rangle \cdot \langle x_2|x\rangle \cdot \langle x|x_1\rangle = \mathbb{1}\left[a_1 = a_2\right] \cdot \mathbb{1}\left[x_1 = x_2 = x\right],$$

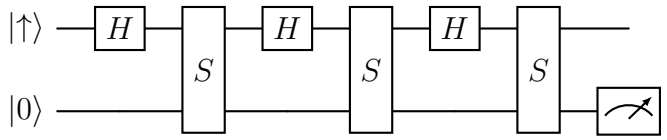
and then, the probability of obtaining the walk $|x\rangle$ is:

$$\mathbb{P}\left[x_t = s\right] = \langle \psi_3 | I \otimes |x\rangle\langle x| | \psi_3\rangle = \begin{cases} \frac{1}{8},\ s = 3; \\ \frac{1}{8}(\underbrace{1^2}_{|\downarrow\rangle} + \underbrace{2^2}_{|\uparrow\rangle}) = \frac{5}{8},\ s = 1; \\ \frac{1}{8},\ s = -1; \\ \frac{1}{8},\ s = -3; \\ 0,\ \text{otherwise.} \end{cases}$$

That means the only possible walks are $\pm 1, \pm 3$. The resulting table is:

	$\mathbb{P}\left[x_t = -3\right]$	$\mathbb{P}\left[x_t = -2\right]$	$\mathbb{P}\left[x_t = -1\right]$	$\mathbb{P}\left[x_t = 0\right]$	$\mathbb{P}\left[x_t = 1\right]$	$\mathbb{P}\left[x_t = 2\right]$	$\mathbb{P}\left[x_t = 3\right]$
$t = 0$	0	0	0	1	0	0	0
$t = 1$	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0
$t = 2$	0	$\frac{1}{4}$	0	$\frac{1}{2}$	0	$\frac{1}{4}$	0
$t = 3$	$\frac{1}{8}$	0	$\frac{1}{8}$	0	$\frac{5}{8}$	0	$\frac{1}{8}$

4. **(8pts)**



5. **(2pts)** If a measurement is done at each time step it is as if the walk is reset at some "classical position" at each time step and thus the moves will be exactly the classical ones. Therefore one will find the first table (same as for the classical walk).

Problem 3. *Steane error correcting code* (30pts)

Recall that the logical code words of the Steane code are

$$|0\rangle_{\text{Steane}} = \frac{1}{\sqrt{8}}\Big\{|0000000\rangle + |1001101\rangle + |0101011\rangle + |0010111\rangle + |0111100\rangle + |1011010\rangle + |1100110\rangle + |1110001\rangle\Big\}$$

and

$$|1\rangle_{\text{Steane}} = \frac{1}{\sqrt{8}}\Big\{|1111111\rangle + |0110010\rangle + |1010100\rangle + |1101000\rangle + |1000011\rangle + |0100101\rangle + |0011001\rangle + |0001110\rangle\Big\}.$$

1. What is the length of this code ?

2. Give the most general form of a quantum codeword belonging to this code and give the dimension of the subspace of quantum codewords.

3. Among the following 8 operators $Z_1Z_2Z_3Z_7$, $Z_2Z_3Z_4Z_5$, $Z_2Z_3Z_5Z_6$, $Z_2Z_4Z_6Z_7$ and $X_1X_2X_3X_7$, $X_2X_3X_4X_5$, $X_2X_3X_5X_6$, $X_2X_4X_6X_7$ there are only 6 of them that form the stabilizer group of the code. Say which of them form this stabilizer group and justify your answer.

4. Suppose now that the original state $\alpha|0\rangle_{\text{Steane}} + \beta|1\rangle_{\text{Steane}}$ undergoes three types of errors:

   (a) a bit flip on the third qubit.

   (b) a phase flip on the third qubit.

   (c) a bit-phase flip on the third qubit.

   Explain how the error and its type are detectable. Then explain how it can be corrected.

5. In the error correction process in the question above (for one qubit errors): explain shortly in a few words what are the crucial properties that the stabilizers must satisfy?

Solution to problem 3: (total 30pts)

1. **(1pts)** Length of the code is 7, as 7 qubits are used.

2. **(2pts)** The general form of a quantum codeword is:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \Longrightarrow |\psi_{\text{Steane}}\rangle = \alpha|0\rangle_{\text{Steane}} + \beta|1\rangle_{\text{Steane}};$$

Dimension of the subspace spanned by codewords is 2, as codewords of type $\alpha|0\rangle_{\text{Steane}} + \beta|1\rangle_{\text{Steane}}$ are lying in the Hilbert subspace of dimension 2^1.

3. **(10pts)** First solution (may be a bit long to check but simplest): Check for which operators the eigenvalues of the Steane codewords are $+1$. One finds that one must exclude $Z_2Z_3Z_5Z_6$ and $X_2X_3X_5X_6$ because for these two the eigenvalues of the Steane codewords are -1. Then one must check that the remaining operators all mutually commute by using $X_iZ_i = -Z_iX_i$ and $X_iZ_j = Z_jX_i$ if $i \neq j$.

   Second solution (connecting to CSS theory): We can notice that $|0\rangle_{\text{Steane}}, |1\rangle_{\text{Steane}}$ can be represented as:

$$|0\rangle_{\text{Steane}} = \frac{1}{\sqrt{|C|}} \sum_{\vec{y}\in C} |\vec{y}\rangle;\ |1\rangle_{\text{Steane}} = \frac{1}{\sqrt{|C|}} \sum_{\vec{y}\in C} |1111111 + \vec{y}\rangle;$$

   where $C = \text{span}\,\langle \vec{u}_1, \vec{u}_2, \vec{u}_3\rangle\,, \vec{u}_1 = 1110001, \vec{u}_2 = 0111100, \vec{u}_3 = 0101011$. Note that:

   - $Z_1Z_2Z_3Z_7$, $Z_2Z_3Z_4Z_5$, $Z_2Z_4Z_6Z_7$ correspond to the application of Z to qubits in positions of ones in those vectors, i.e. $Z_1Z_2Z_3Z_7|\vec{x}\rangle = (-1)^{\vec{x}\cdot\vec{u}_1}|\vec{x}\rangle$, same for others.
   - $X_1X_2X_3X_7$, $X_2X_3X_4X_5$, $X_2X_4X_6X_7$ – of X, i.e.$X_1X_2X_3X_7|\vec{x}\rangle = |\vec{x} + \vec{u}_1\rangle$, same for others.

   This means that $|0\rangle_{\text{Steane}}$ and $|1\rangle_{\text{Steane}}$ are the eigenstates of those operators with eigenvalue 1, which means they are stabilizers. Indeed, for example:

$$X_1X_2X_3X_7|0\rangle_{\text{Steane}} = \frac{1}{2} \sum_{\vec{y}\in\text{span}\langle\vec{u}_2,\vec{u}_3\rangle} X_1X_2X_3X_7 \left(\frac{1}{\sqrt{2}}(|\vec{y}\rangle + |\vec{y} + \vec{u}_1\rangle)\right) =$$
$$= \frac{1}{2} \sum_{\vec{y}\in\text{span}\langle\vec{u}_2,\vec{u}_3\rangle} \frac{1}{\sqrt{2}}(|\vec{y}\rangle + |\vec{y} + \vec{u}_1\rangle) = |0\rangle_{\text{Steane}}$$

   and

$$Z_1Z_2Z_3Z_7|0\rangle_{\text{Steane}} = \frac{1}{2} \sum_{\vec{y}\in\text{span}\langle\vec{u}_2,\vec{u}_3\rangle} Z_1Z_2Z_3Z_7 \left(\frac{1}{\sqrt{2}}(|\vec{y}\rangle + |\vec{y} + \vec{u}_1\rangle)\right) =$$
$$= \frac{1}{2} \sum_{\vec{y}\in\text{span}\langle\vec{u}_2,\vec{u}_3\rangle} (-1)^{\vec{y}\cdot\vec{u}_1} \frac{1}{\sqrt{2}}(|\vec{y}\rangle + |\vec{y} + \vec{u}_1\rangle) \overset{\vec{u}_2\cdot\vec{u}_1=0,\,\vec{u}_3\cdot\vec{u}_1=0}{=} |0\rangle_{\text{Steane}}$$

   For $Z_2Z_3Z_5Z_6$, $X_2X_3X_5X_6$, this is not true.

4. **(10pts)** The errors can be represented as $X_3|\psi_{\text{Steane}}\rangle$ (bit flip), $Z_3|\psi_{\text{Steane}}\rangle$ (phase flip), $X_3Z_3|\psi_{\text{Steane}}\rangle$ (bit-phase flip).

   We will use that the operations on different qubits commute and $X_3Z_3 = -Z_3X_3$. For example, if we have phase flip and apply stabilizer $X_1X_2X_3X_7$, we obtain that corrupted code $Z_3|\psi_{\text{Steane}}\rangle$ is an eigenstate with eigenvalue -1 :

$$X_1X_2X_3X_7\left(Z_3|\psi_{\text{Steane}}\rangle\right) = -Z_3\left(X_1X_2X_3X_7|\psi_{\text{Steane}}\rangle\right) = -\left(Z_3|\psi_{\text{Steane}}\rangle\right).$$

   Similarly, we can obtain:

   - bit-flip: measurement of stabilizers $Z_1Z_2Z_3Z_7$, $Z_2Z_3Z_4Z_5$ will give -1, others 1. If we identify it, we apply X_3 to the channel output.
   - phase-flip: measurement of stabilizers $X_1X_2X_3X_7$, $X_2X_3X_4X_5$ will give -1, others 1. If we identify it, we apply Z_3 to the channel output.
   - bit-phase flip: measurement of stabilizers $Z_1Z_2Z_3Z_7$, $Z_2Z_3Z_4Z_5$, $X_1X_2X_3X_7$, $X_2X_3X_4X_5$ will give -1, others 1. If we identify it, we apply X_3Z_3 to the channel output.

5. **(7pts)** Stabilizers can be constructed as products of Pauli matrices X_i, Z_i. The codewords should be the eigenstates of stabilizers with eigenvalue 1 and stabilizers must be commutative so we can make the simultaneous measurement of them.