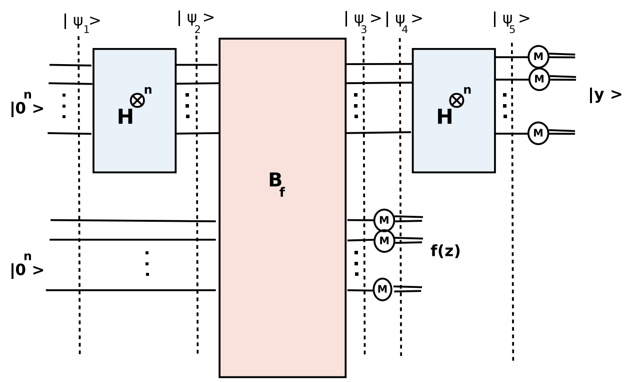

Figure 1: The circuit for the Simon's algorithm

- We have applied Simon's algorithm to a 4-bit input. Given that we have $|\psi_5\rangle = \frac{|0101\rangle - |1001\rangle + |1100\rangle + |0000\rangle + |0010\rangle - |1110\rangle - |1011\rangle + |0111\rangle}{\sqrt{8}}$. Assuming that you have the same $|\psi_5\rangle$ repeatedly, what is the secret message s? Please clearly show your calculations. [**5 Marks**]

  I have to randomly choose (by measurement) 3 linearly independent vectors.

  I choose $|1001\rangle$, $|1100\rangle$, and $|1011\rangle$.

  I solve the equation $A\vec{s} = \vec{0}$. To that end, we will be using Gaussian elimination method.

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

  We apply elementary row operations and get resultant matrix of

$$\begin{pmatrix} 1 & 0 & 0 & 1 & | & 0 \\ 0 & 1 & 0 & 1 & | & 0 \\ 0 & 0 & 1 & 0 & | & 0 \\ 0 & 0 & 0 & 0 & | & 0 \end{pmatrix}$$

  Solving it using back substitution. We get $s_4 = 1$, $s_3 = 0$, $s_2 = 1$, $s_1 = 1$. Thus, my $s = 1101$.

- U_f is defined as $U_f\left|x\right\rangle\left|y\right\rangle = \left|x\right\rangle\left|f(x)\oplus y\right\rangle$. Given $f(01) = 11$, what is $U_f\left|01\right\rangle\left|--\right\rangle$? [**5 Marks**]

$$\left|--\right\rangle = \frac{1}{2}\left|00\right\rangle - \left|01\right\rangle - \left|10\right\rangle + \left|11\right\rangle$$
$$U_f\left|01\right\rangle\left|--\right\rangle = \frac{1}{2}\left|01\right\rangle\Bigg(\left|11\oplus 00\right\rangle - \left|11\oplus\left|01\right\rangle\right\rangle - \left|11\oplus 10\right\rangle + \left|11\oplus 11\right\rangle\Bigg)$$
$$U_f\left|01\right\rangle\left|--\right\rangle = \frac{1}{2}\left|01\right\rangle\Bigg(\left|11\right\rangle - \left|10\right\rangle - \left|01\right\rangle + \left|00\right\rangle\Bigg)$$

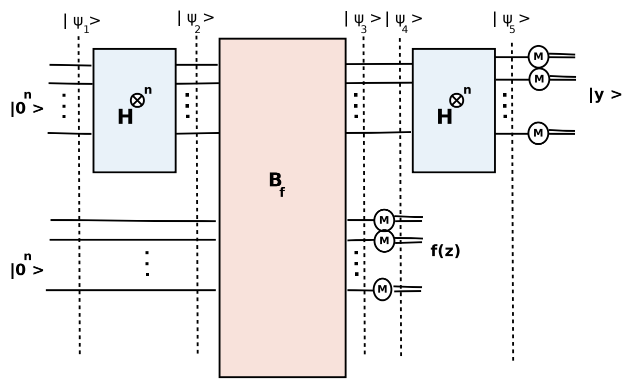

Figure 2: The circuit for the Simon's algorithm

- U_f is defined as $U_f\left|x\right\rangle\left|y\right\rangle = \left|x\right\rangle\left|f(x)\oplus y\right\rangle$. Given $f(10) = 11$, what is $U_f\left|10\right\rangle\left|-+\right\rangle$? [**5 Marks**]

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

$$U_f\left|10\right\rangle\left|-+\right\rangle = \frac{1}{2}\left|01\right\rangle\Big(\left|11\oplus 00\right\rangle + \left|11\oplus\left|01\right\rangle\right\rangle - \left|11\oplus 10\right\rangle - \left|11\oplus 11\right\rangle\Big)$$

$$U_f\left|01\right\rangle\left|-+\right\rangle = \frac{1}{2}\left|01\right\rangle\Big(\left|11\right\rangle + \left|10\right\rangle - \left|01\right\rangle - \left|00\right\rangle\Big)$$

- We have applied Simon's algorithm to a 4-bit input. Given that we have $|\psi_5\rangle = \frac{|0000\rangle - |0010\rangle + |1100\rangle + |0101\rangle + |1001\rangle - |1110\rangle + |1011\rangle - |0111\rangle}{\sqrt{8}}$. Assuming that you have the same $|\psi_5\rangle$ repeatedly, what is the secret message s? Please clearly show your calculations. [**5 Marks**]

  I have to randomly choose (by measurement) 3 linearly independent vectors.

  I choose $|1001\rangle$, $|1100\rangle$, and $|1011\rangle$.

  I solve the equation $A\vec{s} = \vec{0}$. To that end, we will be using Gaussian elimination method.

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

  We apply elementary row operations and get resultant matrix of

$$\begin{pmatrix} 1 & 0 & 0 & 1 & | & 0 \\ 0 & 1 & 0 & 1 & | & 0 \\ 0 & 0 & 1 & 0 & | & 0 \\ 0 & 0 & 0 & 0 & | & 0 \end{pmatrix}$$

  Solving it using back substitution. We get $s_4 = 1$, $s_3 = 0$, $s_2 = 1$, $s_1 = 1$. Thus, my $s = 1101$.