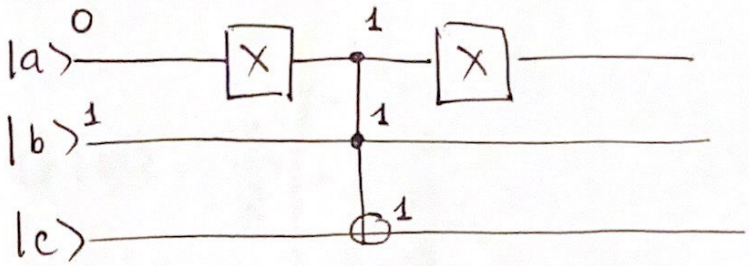
Question 1

$U_f =$



a, $U_f |ab\rangle|c\rangle = |ab\rangle|c \oplus f(a,b)\rangle$

$f(a,b) = 1$ when $a = 0$, $b = 1$

$= 0$ ow

b) Marked element is $|01\rangle$

$$2|\varphi\rangle\langle\varphi| - I = 2\frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} - I$$

$$= \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

c) $O_f = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \Rightarrow G = \frac{1}{2}\begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}$

d, $H^{\otimes 2}|0\rangle^{\otimes 2} = |\varphi\rangle$

$$\Rightarrow \quad GH^{\otimes 2}|0\rangle^{\otimes 2} = G|\varphi\rangle = \frac{1}{2}\begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$= \frac{1}{4}\begin{pmatrix} 0 \\ 4 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle \leftarrow \text{marked element}$$

e, $$|\alpha\rangle = \frac{1}{\sqrt{3}}\left(|00\rangle + |10\rangle + |11\rangle\right)$$

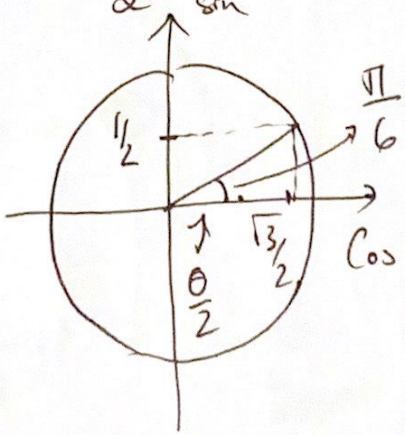
$$|\beta\rangle = \frac{1}{1}|01\rangle$$

$$\Rightarrow \quad |\varphi\rangle = \frac{1}{2}\left(\underbrace{\left(|00\rangle + |10\rangle + |11\rangle\right)}_{\sqrt{3}|\alpha\rangle} + \underbrace{|01\rangle}_{|\beta\rangle}\right)$$

$$\rightarrow \quad |\varphi\rangle = \frac{\sqrt{3}}{2}|\alpha\rangle + \frac{1}{2}|\beta\rangle$$

f, $$\cos\frac{\theta}{2} = \frac{\sqrt{3}}{2}$$

$$\sin\frac{\theta}{2} = \frac{1}{2}$$



$$\rightarrow \frac{\theta}{2} = \frac{\pi}{6}$$

$$\theta = \frac{\pi}{3}$$

g) $G = \frac{1}{2}\begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}$

$$|\alpha\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \qquad |\beta\rangle = \frac{1}{2}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$G|\alpha\rangle = \frac{1}{2\sqrt{3}}\begin{pmatrix} 1 \\ 3 \\ 1 \\ 1 \end{pmatrix} \qquad G|\beta\rangle = \frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ -1 \\ -1 \end{pmatrix}$$

thus; $G|\alpha\rangle = \frac{1}{2\sqrt{3}}\left(\sqrt{3}|\alpha\rangle + 3|\beta\rangle\right)$

$$= \frac{1}{2}|\alpha\rangle + \frac{\sqrt{3}}{2}|\beta\rangle$$

with $\theta = \frac{\pi}{3} \Rightarrow$ $G|\alpha\rangle = \cos\theta|\alpha\rangle + \sin\theta|\beta\rangle$

$$G|\beta\rangle = \frac{1}{2}\cdot\left(-\sqrt{3}|\alpha\rangle + |\beta\rangle\right) = \frac{1}{2}|\beta\rangle - \frac{\sqrt{3}}{2}|\alpha\rangle$$

$$\Rightarrow G|\beta\rangle = \frac{-\sqrt{3}}{2}|\alpha\rangle + \frac{1}{2}|\beta\rangle \rightarrow G = \underline{\text{Transformation Matrix}} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

$$= -\sin\theta|\alpha\rangle + \cos\theta|\beta\rangle$$

Question 2 $N = 143$; $n = 11$

- If $\gcd(a,N) \neq 1$ $\longrightarrow$ we have a "good" case of q
  (and also $a \neq 0,1$) Let p such that $p \mid N$
  and d $d \nmid N$

  we have $N' = N/d$; we can iterate the process with N' until we factorize $N = pq$

- $[a] \in \mathbb{Z}/N\mathbb{Z}^*$
  ↑
  $a \in [0, N-1]$
  $\gcd(a, N) = 1$

We have $N = 143 = 11 \times 13$; by Chinesse Remainder Theorem

$$\mathbb{Z}/_{N\mathbb{Z}} \simeq \mathbb{Z}/_{11\mathbb{Z}} \times \mathbb{Z}/_{13\mathbb{Z}}$$

thus; drawing $[a] \in \mathbb{Z}/_{N\mathbb{Z}}$ equivalent to drawing

$$(x,y) \in \left(\mathbb{Z}/_{11\mathbb{Z}}\right)^* \times \left(\mathbb{Z}/_{13\mathbb{Z}}\right)$$

- $|\mathbb{Z}/_{11\mathbb{Z}}^{*}| = \phi(11) = 11 - 1 = 10$ (11 is prime)

$|\mathbb{Z}/_{13\mathbb{Z}}^{*}| = \phi(13) = 13 - 1 = 12$

- Find $g_1 \in [0, 10]$ s.t $(\mathbb{Z}/_{11\mathbb{Z}})^{*} = \langle [g_1] \rangle$

$\Leftrightarrow$ g_1 satisfies $Ord_{11}(g_1) = 10$

Possible orders ~~(r)~~ are $d \mid 10$, $d > 0$ $\{1, 2, 5, 10\}$

Find g_1 s.t $g_1^{r} = 1 \mod 11$

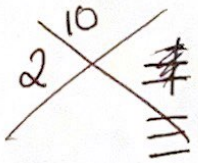
We have to check only 2, 5 and 10

r \ g_1	0	1	2	3	4	5
2	0	1	4	9	5	3
5	0	1	10	1	1	1
10	0	1	1	1	1	1

r \ g_1	6	7	8	9	10
2	3	5	9	4	1
5	10	10	10	1	10
10	1	1	1	1	1

We have $g_1 = 2^{\not 2} \not\equiv 1 \mod 11$ and $2^{10} \equiv 1 \mod 10$

$2^5 \not\equiv 1 \mod 11$



- $g_2 \in [0, 12]$ such that $\left(\mathbb{Z}/13\mathbb{Z}\right)^* = \langle [g_2] \rangle$

Possible orders are $\{1, 2, 3, 4, 6, 12\}$

g_2 st $\text{Ord}_{13}(g_2) = 12$

We only need to check order $\{4, 6, 12\}$ since

if $g_2^1 \not\equiv 1 \mod 13 \Rightarrow g_2^2 \not\equiv 1 \mod 13$

Similar to g_2^6 and g_2^3

q_2 \ r	4	6	12
0	0	0	0
1	1	1	1
2	3+	12	1
3	3	1	1
4	9	1	1
5	1	12	1
6	9	12	1
7	9	12	1
8	1	12	1
9	9	1	1
10	3	1	1
11	3	12	1
12	1	1	1

$q_2 = 2 \Rightarrow 2^4 \not\equiv 1 \mod 13$

$2^6 \not\equiv 1 \mod 13$

- We have $a \equiv g_1^{k_1} \bmod 11 \quad (0 \leq k_1 < 10)$

$$a \equiv g_2^{k_2} \bmod 13 \quad (0 \leq k_2 < 12)$$

$$\Leftrightarrow \begin{cases} g_1^{k_1 r} \equiv 1 \bmod 11 \\ g_2^{k_2 r} \equiv 1 \bmod 13 \end{cases}$$

$$\Leftrightarrow \begin{cases} 10 \mid k_1 r \\ 12 \mid k_2 r \end{cases} \quad \text{(By Fermat's Little Theorem)}$$

- $\begin{cases} 10 \mid k_1 r \\ 12 \mid k_2 r \end{cases} \Rightarrow \begin{cases} 2 \mid k_1 r \\ 2 \mid k_2 r \end{cases}$

If k_1 and k_2 is odd, r must be even

- From part (2), drawing $[a]$ from $\mathbb{Z}/N\mathbb{Z}^*$ uniformly random

equivalent to drawing $[g_1] \leftarrow \mathbb{Z}/11\mathbb{Z}^*$

$[g_2] \leftarrow \mathbb{Z}/13\mathbb{Z}^*$

$[g_1] \simeq k_1 \in [0, 9]$

$[g_2] \simeq k_2 \in [0, 11]$

So $\mathbb{P}\{k_1 \text{ or } k_2 \text{ is odd}\} = 1 - P(k_1 \text{ and } k_2 \text{ are even})$

$= \underset{\text{independent}}{1 - \frac{1}{2} \cdot \frac{1}{2}} = 1 - \frac{1}{4} = \frac{3}{4}$

- $a = 34$ then $g_1^{k_1} \equiv 34 \mod 11$

$\equiv 1 \mod 11$

$g_1 = 2 \Rightarrow k_1 = 0$

$g_2^{k_2} \equiv 34 \mod 13$; $g_2 = 2 \Rightarrow k_2 = 3$

$\equiv 8 \mod 13$

- Find $g_1^{k_1}$ that have order 1, 2, 5, 10 mod 11

⊕ $\text{Ord}_{11}(g_1^{k_1}) = \frac{11-1}{\gcd(10, k_1)} = \frac{10}{\gcd(10, k_1)}$

$g_1 \in [0, 9]$

Order	1	2	5	10
k_1	0	5	2, 4, 6, 8	1, 3, 7, 9

⊕ $\text{Ord}_{13}(g_2^{k_2}) = \frac{12}{\gcd(12, k_2)}$; $g_2 \in [0, 12]$

Order	1	2	3	4	6	12
k_2	0	6	4, 8	3, 9	2, 10	1, 5, 7, 11

- $Val_2(Ord_{11}(a_1))$

$= Val_2(1) := 2^\ell \mid 1 \iff \ell = 0$

$= Val_2(2) := 2^\ell \mid 2 \iff \ell = 1$

$= Val_2(5) := 2^\ell \mid 5 \iff \ell = 0$

$= Val_2(10) := 2^\ell \mid 10 \iff \ell = 1$

- $\mathbb{P}\left(Val_2(Ord_{11}(a_1)) = 0\right)$

$= \mathbb{P}\left(Val_2(Ord_{11}(a_1)) = 1\right) + \mathbb{P}(\text{---} = 5)$

$= \frac{1}{10} + \frac{4}{10} = \frac{5}{10} = \frac{1}{2}$

- $\mathbb{P}\left(Val_2(Ord_{11}(a_1)) = 1\right)$

$= \mathbb{P}\left(Val_2(Ord_{11} = 2\right) + \mathbb{P}(\text{---} = 10) = \frac{1}{10} + \frac{4}{10} = \frac{1}{2}.$

- For $a_2 \Rightarrow Val_2$

1	$2^1 \mid 1$	$\Rightarrow \ell = 0$
2	$2^\ell \mid 2$	$\Rightarrow \ell = 1$
3	$2^\ell \mid 3$	$\Rightarrow \ell = 0$
4	$2^\ell \mid 4$	$\Rightarrow \ell = 2$
6	$2^1 \mid 6$	$\Rightarrow \ell = 1$
12	$2^\ell \mid 12$	$\Rightarrow \ell = 2$

$$\mathbb{P}\left(Val_2\left(Ord_{13}(a_2)\right) = 0\right) = \mathbb{P}\left(Val_2(3)\right) + \mathbb{P}(Val_2(1))$$

$$= \frac{1}{12} + \frac{2}{12} = \frac{3}{12} = \frac{1}{4}$$

$$\mathbb{P}\left(Val_2\left(Ord_{13}(a_2)\right) = 1\right) = \mathbb{P}\left(Val_2(2)\right) + \mathbb{P}\left(Val_2(6)\right)$$

$$= \frac{1}{12} + \frac{2}{12} = \frac{3}{12} = \frac{1}{4}$$

$$\mathbb{P}\left(Val_2\left(Ord_{13}(a_2)\right) = 2\right) = \mathbb{P}\left(Val_2(4)\right) + \mathbb{P}\left(Val_2(12)\right)$$

$$= \frac{2}{12} + \frac{4}{12} = \frac{6}{12} = \frac{1}{2}$$

- We have $r_1 = Ord_{11}(a)$

$r_2 = Ord_{13}(a)$

$a^r \equiv 1 \mod (11 \times 13) \Rightarrow 13 \mid a^r - 1$

$11 \mid a^r - 1$

$$\Rightarrow \begin{cases} a^r \equiv 1 \mod 11 \rightarrow r_1 \mid r \\ a^r \equiv 1 \mod 13 \rightarrow r_2 \mid r \end{cases} \quad (1)$$

Let's assume that $r' = h_1 r_1 = h_2 r_2$

$$\Rightarrow a^{r'} = a^{h_1 r_1} \equiv 1 \mod 11$$

$$a^{h_2 r_2} \equiv 1 \mod 13$$

By CRT $\rightarrow$ $a^{r'} \equiv 1 \mod N$ so $r \mid r'$ and $\underline{\underline{r \leq r'}}$

$\Rightarrow$ r is less than any common multiple of r_1 and r_2 (2)

From (1), (2) $\Rightarrow$ $r = lcm(r_1, r_2)$

• ($\Leftarrow$) $r = \text{lcm}(r_1, r_2)$

If r_1 is even $\Rightarrow 2 \mid r_1 \Rightarrow 2 \mid r$
r_2 is even $\Rightarrow 2 \mid r_2 \Rightarrow 2 \mid r$
} r is even

($\Rightarrow$) If r_1 and r_2 are odd ; assume that

$r = 2r' \Rightarrow r_1 \mid r = 2r'$
$r_2 \mid r = 2r'$

$\Rightarrow$ $r_1 \mid r'$, $r_2 \mid r'$ } $\rightarrow$ r' is also a common ~~divisor~~ divisor.

However ; $r = \text{lcm}(r_1, r_2)$ contradict with $r = 2r'$

$\Rightarrow$ r musbe odd

• $P\left(\text{Val}_2(\text{Ord}_{11}(a)) = \text{Val}_2(\text{Ord}_{13}(a))\right)$

$= \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{2} = \frac{2}{8} = \frac{1}{4}$

$\Rightarrow P\left(\text{Val}_2(\text{Ord}_{11}(a)) \neq \text{Val}_2(\text{Ord}_{13}(a))\right) = \frac{3}{4}$

- $Ord_{11}(a) = 2^{t_1} k_1$
  $Ord_{13}(a) = 2^{t_2} k_2$
  $\left\{ \begin{array}{l} k_1, k_2 \text{ are odd} \\ t_1 \neq t_2 \end{array} \right.$

- $t_1 > t_2$, then $a^{r/2} \equiv -1 \mod 11$

$$a^{r/2} \equiv 1 \mod 13$$

We have $r = lcm(r_1, r_2) = r_1 k_1'$ ← odd
$= r_2 2^{t_2 - t_2} \cdot k_2'$ ←

$$\Rightarrow a^{r/2} = \left(a^{r_1/2}\right)^{k_1'} \equiv (-1)^{k_1} \mod 11$$

k_1 is odd $\Rightarrow$ $a^{r/2} \equiv (-1) \mod 11$

- $a^{r/2} = \left(a^{r_2}\right)^{2^{t_1 - t_2 - 1} \cdot k_2} = (1)^{2^{t_1 - t_2 - 1} k_2} \equiv 1 \mod 13$

thus for $t_1 > t_2 \Rightarrow \left\{ \begin{array}{l} a^{r/2} \equiv -1 \mod 11 \\ a^{r/2} \equiv 1 \mod 13 \end{array} \right.$

for $t_1 < t_2$; then

$$r = r_1 \, 2^{t_2 - t_1} \, k_1' \quad (k_1' \text{ odd})$$

$$= r_2 \, k_2' \quad (k_2' \text{ odd})$$

$$a^{r/2} = \left(a^{r_2/2}\right)^{k_2'} = (-1) \mod 13$$

$$2^{t_2 - t_1 - 1} \, k_1' = -1 \mod 13$$

$$a^{r/2} = \left(a^{r_1/2}\right)^{2^{t_2 - t_1 - 1} k_1'} = (1) = 1 \mod 11$$

thus, for $t_1 < t_2 \Rightarrow$

$$\begin{cases} a^{r/2} \equiv 1 \mod 11 \\ a^{r/2} \equiv -1 \mod 13 \end{cases}$$

- By CRT; we have

$$(I) \quad \begin{cases} a^{r/2} \equiv 1 \mod 11 \\ a^{r/2} \equiv -1 \mod 13 \end{cases} \Rightarrow a^{r/2} \not\equiv \begin{matrix} -1 \\ 1 \end{matrix} \mod 143$$

$$\Rightarrow 143 \mid a^{r/2} \pm 1$$

Condition (I) equivalent to the case $Val_2(Ord_{11}(a)) \neq Val_2(Ord_{13}(a))$

- $\mathbb{P}\left(r \text{ is even and } 143 \mid a^{r/2} \pm 1\right)$

$= \mathbb{P}\left(\text{Val}_2(\text{Ord}_{11}(a)) \neq \text{Val}_2(\text{Ord}_{13}(a))\right) = 3/4$

- With $a = 34$ $\quad n = 11$ qubits

$a^x \bmod N =$

x	0	1	2	3	4	5	6	7
	1	34	12	122	1	34	12	...

There are 4 different values

$\{1, 34, 12, 122\}$

- With $x = 2 \Rightarrow a^x \bmod 143 = 12 \Rightarrow b = 2$

$$mb = \left\lfloor \frac{2^2 - b - 1}{4} \right\rfloor = 511 \Rightarrow \frac{1}{\sqrt{mb}} \sum_{k=0}^{510} |y_0 + kr\rangle$$

the probability $\mathbb{P}(y = 2512) = \frac{1}{mb2^n} \left| \sum_{j=0}^{mb-1} \xi^j \right|^2$

where $\xi = e^{\frac{-2\pi i r y}{2^{11}}}$; $\xi_{512} = e^{\frac{-2\pi i \cdot 4 \cdot 512}{2^{11}}} = e^{-2\pi i} = 1$

$\xi_{1024} = e^{\frac{-2\pi i \cdot 4 \cdot 1024}{2^{11}}} = e^{-4\pi i} = 1$

$\xi_0 = 1$

$\xi_{1536} = e^{-6\pi i} = 1$

thus $\mathbb{P}(y=512) = \mathbb{P}(y=1024) = \mathbb{P}(y=1536)$

$$= \mathbb{P}(y=0) = \frac{511^2}{2^{11} \cdot 511} = \frac{511}{2^{11}} \simeq \frac{1}{4} - \frac{1}{2048}$$

- $\mathbb{P}$("Good" choice of a)

$$= \mathbb{P}\left(\gcd(a,N) \neq 1 \; ; \; a \neq 1\right) \quad (1)$$

$$+ \mathbb{P}\left(\gcd(a,N) = 1\right) \cdot \mathbb{P}\left(N \nmid a^{r/2} \pm 1\right) \quad (2)$$

$$(1) = \frac{N - \phi(N) - 1}{N} = \frac{143 - 120 - 1}{143} = \frac{2}{13}$$

$$(2) = \frac{\phi(N)}{N} \cdot \frac{3}{4} = \frac{120}{143} \cdot \frac{3}{4} = \frac{90}{143}$$

$$\Rightarrow \mathbb{P}(\text{——}) = \frac{112}{143}$$