Problem Sheet 5

1. Balanced functions

(a) $f : B_2 \to B_1$

$$\{00, 01, 10, 11\} \to \{0, 1\}$$

Balanced function must have equal number zero outputs as one outputs

x_1	x_2	$f_1(x_1,x_2)$	$f_2(x_1,x_2)$	$f_3(x_1,x_2)$	$f_4(x_1,x_2)$	$f_5(x_1,x_2)$	$f_6(x_1,x_2)$
0	0	0	1	1	1	0	0
0	1	0	1	0	0	1	1
1	0	1	0	1	0	1	0
1	1	1	0	0	1	0	1

(b) $f : B_2 \to B_1$ again.

$$|f\rangle = \frac{1}{2} \sum_{x_1, x_2 = 0}^{1} (-1)^{f(x_1, x_2)} |x_1, x_2\rangle$$

To be orthogonal, we must have $\langle f_1 | f_2 \rangle = 0$.
Since $|f_1\rangle$ and $|f_2\rangle$ are in the same basis, we may choose

$$f_1(x_1,x_2) = \begin{cases} 0 & x_1 x_2 = 00 \\ 0 & x_1 x_2 = 01 \\ 1 & x_1 x_2 = 10 \\ 1 & x_1 x_2 = 11 \end{cases}$$

$$\gamma_2(x_1, x_2) = \begin{cases} 0 & x_1x_2 = 00 \\ 1 & x_1x_2 = 01 \\ 1 & x_1x_2 = 10 \\ 0 & x_1x_2 = 11 \end{cases}$$

Then

$$|\gamma_1(x_1x_2)\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle - |10\rangle - |11\rangle\right)$$

$$|\gamma_2(x_1x_2)\rangle = \frac{1}{2}\left(|00\rangle - |01\rangle - |10\rangle + |11\rangle\right)$$

$$\therefore \langle \gamma_1|\gamma_2\rangle = \frac{1}{4}\left(\langle 00|00\rangle - \langle 01|01\rangle + \langle 10|10\rangle - \langle 11|11\rangle\right)$$

$$= \frac{1}{4}\left(1 - 1 + 1 - 1\right) = 0$$ $\therefore$ hence $|\gamma_1\rangle$ and $|\gamma_2\rangle$ orthogonal

To find one pair such that their states are <u>not</u> orthogonal we could modify $|\gamma_2\rangle$ to become

$$\gamma_2(x_1, x_2) \longrightarrow \begin{cases} 1 & x_1x_2 = 00 \\ 1 & x_1x_2 = 01 \\ 0 & x_1x_2 = 10 \\ 0 & x_1x_2 = 11 \end{cases}$$

and hence

$$|\gamma_2\rangle = \frac{1}{2}\left(-|00\rangle - |01\rangle + |10\rangle + |11\rangle\right)$$

and so

$$\langle \gamma_1|\gamma_2\rangle = \frac{1}{4}\left(-\langle 00|00\rangle - \langle 01|01\rangle - \langle 10|10\rangle - \langle 11|11\rangle\right)$$

$$= -1$$ $\therefore$ γ_1 and γ_2 <u>not</u> orthogonal.

(c) Constant function will have the form

$$g_0(x_1, x_2) = \begin{cases} 0 & x_1x_2 = 00 \\ 0 & x_1x_2 = 01 \\ 0 & x_1x_2 = 10 \\ 0 & x_1x_2 = 11 \end{cases}$$

$$\therefore \; |g_0\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

A state associated to a balenced function will have two positive states and two negative states, for example

$$|g\rangle = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle)$$

Lets label the coefficients a, b, c and d as

$$|g\rangle = \frac{1}{2}(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle)$$

where $a, b, c, d \in \{+1, -1\}$. Then

$$\langle g|g\rangle = \frac{1}{4}(a + b + c + d)$$

Given that for a balenced function, two of a, b, c and d must be +1, with the other two −1, we can clearly see that in any permutation, the sum $a+b+c+d = 0$. Hence $|g_0\rangle$ is orthogonal to all balenced functions.

(d)

$x_1x_2x_3$	g_1	g_2	g_3	g_4
000	0	0	0	0
100	1	0	0	1
010	1	0	0	1
001	0	0	0	1

110	0	1	1	0
101	1	0	1	0
011	1	0	1	0
111	0	1	1	1
	balanced	not balanced	balanced	balanced

2. Functions from one trit to one trit

$f : \{0,1,2\} \to \{0,1,2\}$

(a) $0\to 0,\ 0\to 1,\ 0\to 2,\ 1\to 0,\ 1\to 1,\ 1\to 2,\ 2\to 0,\ 2\to 1,\ 2\to 2$

<u>9</u> such functions exist.

(b) $f_1(x) = (x+2) \bmod 3$

$f_1(0) = (0+2) \bmod 3 = 2$

$f_1(1) = (1+2) \bmod 3 = 0$

$f_1(2) = (2+2) \bmod 3 = 1$

f_1 takes <u>three values</u>

(c) $f_2(0) = 1,\ f_2(1) = 0,\ f_2(2) = 2$

we want in form $f_2(x) = (ax^2 + bx + c) \bmod 3$

$f_2(0) = 1 = c \bmod 3 \qquad (1)$

$f_2(1) = 0 = (a+b+c) \bmod 3 \qquad (2)$

$$f_2(2) = 2 = (4a + 2b + c) \bmod 3 \quad (3)$$

From (1) $\rightarrow$ $c \bmod 3 = 1$ $\rightarrow$ $c = 3n + 1 \quad n \in \mathbb{Z}$

But $c \in \{0, 1, 2\}$ $\therefore$ $\underline{\underline{c = 1}}$ $(n = 0)$

$\therefore$ (2) $\rightarrow$ $(a + b + 1) \bmod 3 = 0$

(3) $\rightarrow$ $(4a + 2b + 1) \bmod 3 = 2$

From (2) $a + b + 1 = 3n \Rightarrow a + b = 3n - 1$

From (3) $4a + 2b + 1 = 3n + 2 \Rightarrow 4a + 2b = 3n + 1$

$$\therefore 4a + 2b - 2 = a + b$$

$$\Rightarrow 3a + b = 2$$

$$\Rightarrow b = 2 - 3a \qquad (a, b \in \{0, 1, 2\})$$

Therefore $a = 0$ (any other value would mean that b is negative) and hence $b = 2$.

$$a = 0,\ b = 2,\ c = 0 \rightarrow f_2(x) = (2x + 1) \bmod 3$$

Verify: $f_2(0) = 1 \bmod 3 = 1$ ✓ $f_2(1) = 3 \bmod 3 = 0$ ✓

$f_2(2) = 5 \bmod 3 = 2$ ✓

(d) $f_3(x) = x^3 \bmod 3$; $f_4(x) = x^4 \bmod 3$

Begin with f_3:

$f_3(0) = 0$; $f_3(1) = 1$; $f_3(2) = \overset{8 \bmod 3}{2}$

$\therefore \quad \underline{f_3(x) = x \bmod 3}$ (form above with $a=c=0$, $b=1$)

Now $f_4(x)$:

$$f_4(0) = 0 \bmod 3 = 0$$

$$f_4(1) = 1 \bmod 3 = 1$$

$$f_4(2) = 16 \bmod 3 = 1$$

$\underline{f_4(x) = x^2 \bmod 3}$ (form above with $b=c=0$, $a=1$).

3. Identifying Functions

B_2 : set of all 2 bit strings $(00, 01, 10, 11)$
$B_1 = \{0,1\}$

$$g : B_2 \to B_1$$

has property

$$V_g(x) = (-1)^{g(x)} |x\rangle \qquad x = x_1 x_2, \ |x\rangle = |x_1 x_2\rangle$$

Define 4 functions

$$f_{00}(x) = 0 \quad \forall x$$

$$f_{01}(x) = \begin{cases} 0 & \text{if } x = 00, 01 \\ 1 & \text{otherwise} \end{cases}$$

$$f_{10}(x) = \begin{cases} 0 & \text{if } x = 00, 10 \\ 1 & \text{otherwise} \end{cases}$$

$$f_{11}(x) = \begin{cases} 0 & \text{if } x = 00, 11 \\ 1 & \text{otherwise} \end{cases}$$

(a) Insert $x = 00$ into $f_a = f_{00}$ or f_{01} or f_{10} or f_{11}.

into f_{00} $\rightarrow$ returns 0

into f_{01} $\rightarrow$ returns 0

into f_{10} $\rightarrow$ returns 0

into f_{11} $\rightarrow$ returns 0

Since all functions return the same value, we gain no information from this query.

Consider querying at first 00 as above - we learn no new information.

We might then query $x = 01$. In this case, if we get $f_a(01) = 0$ then it could be f_{00} $\underline{\text{or}}$ f_{01}, and if we get $f_a(01) = 1$, then it could be f_{10} $\underline{\text{or}}$ f_{11}. Hence we need one more query (11 or 10) to properly determine the function.

Hence we need 3 queries $(2^{n-1}+1$ in general$)$.

(b) For an arbitrary function g, we have

$$V_g = (-1)^{g(00)}|00\rangle\langle 00| + (-1)^{g(01)}|01\rangle\langle 01|$$
$$+ (-1)^{g(10)}|10\rangle\langle 10| + (-1)^{g(11)}|11\rangle\langle 11|$$

Check if unitary: $\quad g \in \mathbb{R}$ (maps $\{00, 01, 10, 11\} \mapsto \{0, 1\}$)

$$V_g^\dagger V = \Big((-1)^{g(00)}|00\rangle\langle 00| + (-1)^{g(01)}|01\rangle\langle 01|$$
$$+ (-1)^{g(10)}|10\rangle\langle 10| + (-1)^{g(11)}|11\rangle\langle 11|\Big)$$

$$\times \Big((-1)^{g(00)} |00\rangle\langle 00| + (-1)^{g(01)} |01\rangle\langle 01| + (-1)^{g(10)} |10\rangle\langle 10| + (-1)^{g(11)} |11\rangle\langle 11| \Big)$$

$$= \left[(-1)^{g(00)}\right]^2 |00\rangle\langle 00| + \left[(-1)^{g(01)}\right]^2 |01\rangle\langle 01| + \left[(-1)^{g(10)}\right]^2 |10\rangle\langle 10| + \left[(-1)^{g(11)}\right]^2 |11\rangle\langle 11|$$

We can see that

$$\left[(-1)^{g(x)}\right]^2 = (-1)^{2g(x)} = 1^{g(x)} = 1$$

and hence

$$V_g^\dagger V = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11| = I$$

Hence V_g is unitary in general.

(c) $|g\rangle = V_g (H \otimes H)|00\rangle$

$$= V_g |+\rangle|+\rangle = V_g \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{2} V_g \big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\big)$$

$$= \frac{1}{2}\Big((-1)^{g(00)}|00\rangle + (-1)^{g(01)}|01\rangle + (-1)^{g(10)}|10\rangle + (-1)^{g(11)}|11\rangle \Big)$$

So, for each function the signs in front of the states i.e. the phase will be different.

However, for all possible phase permutations, we will measure $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ with equal probability, so we still learn nothing about the original function.

(d) Start with two qubits in $|00\rangle$

$$|q\rangle = |00\rangle$$

Apply $H \otimes H$

$$H \otimes H |q\rangle = |+\rangle|+\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$$

Apply V_{f_a}:

$$V_{f_a}(H \otimes H)|q\rangle = \frac{1}{2}\sum_{x} (-1)^{f_a(x)}|x\rangle \qquad \left(x \in \{00, 01, 10, 11\}\right)$$

Apply $H \otimes H$

$$(H \otimes H)V_{f_a}(H \otimes H)|q\rangle = \frac{1}{2}(H \otimes H)\sum_{x} (-1)^{f_a(x)}|x\rangle$$

$$= \frac{1}{2}(H \otimes H)\Big[(-1)^{f_a(00)}|00\rangle + (-1)^{f_a(01)}|01\rangle + (-1)^{f_a(10)}|10\rangle + (-1)^{f_a(11)}|11\rangle\Big]$$

$$|m\rangle = \frac{1}{2}\Big[(-1)^{f_a(00)}|++\rangle + (-1)^{f_a(01)}|+-\rangle + (-1)^{f_a(10)}|-+\rangle + (-1)^{f_a(11)}|--\rangle\Big]$$

$$|++\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{2}\Big[|00\rangle + |01\rangle + |10\rangle + |11\rangle\Big]$$

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

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

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

n.b. I'm using this to add them in my head - its a lot to write out :)

$$|m_{00}\rangle = \frac{1}{2}\Big[2|00\rangle\Big] = |00\rangle$$

$$|m_{01}\rangle = \frac{1}{2}\Big[2|10\rangle\Big] = |10\rangle$$

$$|m_{10}\rangle = \frac{1}{2}\Big[2|01\rangle\Big] = |01\rangle$$

all collapse onto single states (measurement outcome is certain)

$$|m_{11}\rangle = \frac{1}{2}\left[2|11\rangle\right] = |11\rangle$$

Hence

measurement	function (with certainty)
00	f_{00}
01	f_{10}
10	f_{01}
11	f_{11}

4. Periodic States

$$QFT|a\rangle = \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} \exp\left(\frac{2\pi i ab}{N}\right)|b\rangle \qquad 0 \le a \le N-1$$

$$e^{\frac{\pi i ab}{3}} = w^{ab}$$

(a) in $N=6$ dimensions

$$QFT|a\rangle = \frac{1}{\sqrt{6}} \sum_{b=0}^{5} w^{ab}|b\rangle$$

$$= \frac{1}{\sqrt{6}}\left[|0\rangle + w^{a}|1\rangle + w^{2a}|2\rangle + w^{3a}|3\rangle + w^{4a}|4\rangle + w^{5a}|5\rangle\right]$$

$$= \frac{1}{\sqrt{6}}\begin{bmatrix} 1 \\ w^{a} \\ w^{2a} \\ w^{3a} \\ w^{4a} \\ w^{5a} \end{bmatrix} \quad //$$

(b) periodic if $|a\rangle + |a+r\rangle + |a+2r\rangle + \dots$

with period $= r$

$|\tau\rangle$ is either

$$\frac{1}{\sqrt{6}}\left[|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle \right] \qquad r=1$$

or

$$\frac{1}{\sqrt{3}}\left[|0\rangle + |2\rangle + |4\rangle \right] \qquad r=2$$

or

$$\frac{1}{\sqrt{3}}\left[|1\rangle + |3\rangle + |5\rangle \right] \qquad r=2$$

We measure $|\tau\rangle$ in the standard basis $\{ |0\rangle \dots |N-1\rangle \}$

As we only measure once, we can only learn one state. This means that there is no way to measure the period. If we measured say $|2\rangle$, this tells us nothing about our period - it could be 1 or 2 still.

(c) In $|\tau\rangle$ again

Apply QFT_6

$$QFT_6 |\tau\rangle = \frac{1}{\sqrt{6}} \sum_{b=0}^{5} w^{\tau b} |b\rangle$$

$$QFT|\tau\rangle_1 = \frac{1}{\sqrt{6}}\left(QFT|0\rangle + QFT|1\rangle + \dots + QFT|5\rangle \right)$$

$$= \frac{1}{6}\left[\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ w \\ w^2 \\ w^3 \\ w^4 \\ w^5 \end{bmatrix} + \begin{bmatrix} 1 \\ w^2 \\ w^4 \\ w^6 \\ w^8 \\ w^{10} \end{bmatrix} + \begin{bmatrix} 1 \\ w^3 \\ w^6 \\ w^9 \\ w^{12} \\ w^{15} \end{bmatrix} + \begin{bmatrix} 1 \\ w^4 \\ w^8 \\ w^{12} \\ w^{16} \\ w^{20} \end{bmatrix} + \begin{bmatrix} 1 \\ w^5 \\ w^{10} \\ w^{15} \\ w^{20} \\ w^{25} \end{bmatrix} \right]$$

$$= \frac{1}{6}\begin{bmatrix} 6 \\ 1+w+w^2+w^3+w^4+w^5 \\ 1+w^2+w^4+w^6+w^8+w^{10} \\ 1+w^3+w^6+w^9+w^{12}+w^{15} \\ 1+w^4+w^8+w^{12}+w^{16}+w^{20} \\ 1+w^5+w^{10}+w^{15}+w^{20}+w^{25} \end{bmatrix} = \frac{1}{6}\begin{bmatrix} 6 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |0\rangle$$

summing powers $w = e^{i\pi/3}$

$$\text{QFT}|\tau\rangle_2 = \frac{1}{3\sqrt{2}}\begin{bmatrix} 3 \\ 1+w^2+w^4 \\ 1+w^4+w^8 \\ 1+w^6+w^{12} \\ 1+w^8+w^{16} \\ 1+w^{10}+w^{20} \end{bmatrix} = \frac{1}{3\sqrt{2}}\begin{bmatrix} 3 \\ 0 \\ 0 \\ 3 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle+|3\rangle\right)$$

$$\text{QFT}|\tau\rangle_3 = \frac{1}{3\sqrt{2}}\begin{bmatrix} 3 \\ w+w^3+w^5 \\ w^2+w^6+w^{10} \\ w^3+w^9+w^{15} \\ w^4+w^{12}+w^{20} \\ w^5+w^{15}+w^{25} \end{bmatrix} = \frac{1}{3\sqrt{2}}\begin{bmatrix} 3 \\ 0 \\ 0 \\ -3 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle-|3\rangle\right)$$

So being able to measure $|3\rangle$ is in indicator of periodicity 2. However, we wont always measure this.

If the period is actually 2 then we will either be in state 2 or 3.

Then, there is a 50% chance in each to measure $|0\rangle$, in which case we are not certain.

5. Quantum Cryptography

(a) $|0\rangle$, $|u\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + w|1\rangle\right)$

$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$

$C = |u\rangle\langle u| - |u^\perp\rangle\langle u^\perp|$ (orthogonal state $|u^\perp\rangle$)

In Z we measure in $\{|0\rangle, |1\rangle\}$ basis

$\langle u^\perp|u\rangle = \frac{1}{2}\left(\langle 0|0\rangle - w^2\langle 1|1\rangle\right) = 0$

In C we measure in $\{|u\rangle, |u^\perp\rangle\}$ basis

$|u^\perp\rangle$ must be orthogonal to $|u\rangle$, can use $|u^\perp\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - w^*|1\rangle\right)$

We need $|0\rangle$ in this basis

$$|0\rangle = A|u\rangle + B|u^\perp\rangle$$

$$\langle u|0\rangle = A = \frac{1}{\sqrt{2}} \qquad \langle u^{\perp}|0\rangle = B = \frac{1}{\sqrt{2}}$$

$$\therefore\ |0\rangle = \frac{1}{\sqrt{2}}\left(|u\rangle + |u^{\perp}\rangle\right)$$

So Alice can send $|0\rangle = \frac{1}{\sqrt{2}}\left(|u\rangle + |u^{\perp}\rangle\right)$ or $|u\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \omega|1\rangle\right)$

If Bob measures Z, he can get (in $\{|0\rangle, |1\rangle\}$)

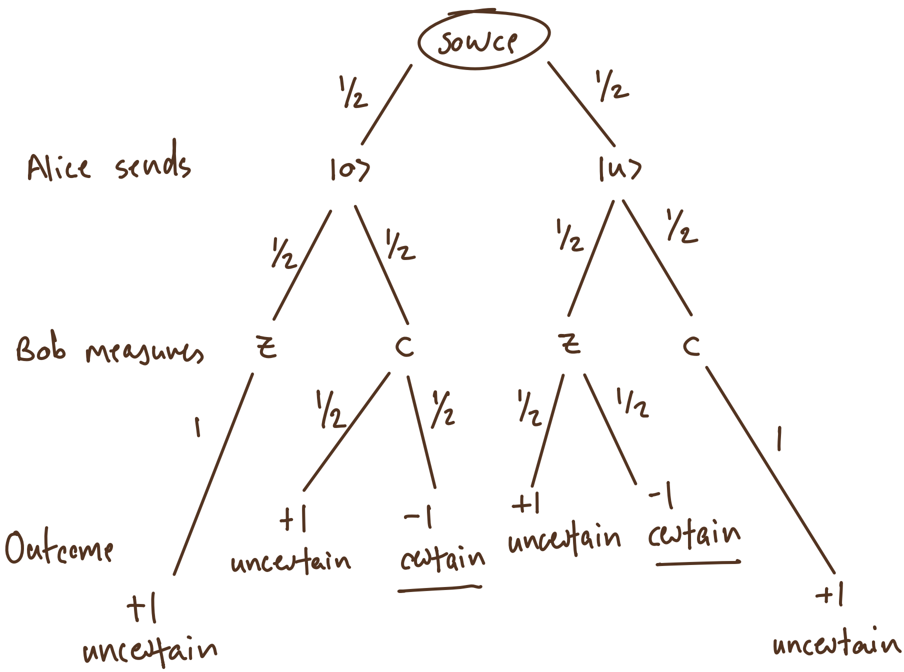
$+1 \to$ outcome is $|0\rangle \to$ uncertain, both $|0\rangle$ and $|u\rangle$ have $|0\rangle$

$-1 \to$ outcome is $|1\rangle \to$ certain, only $|u\rangle$ contains $|1\rangle$

If Bob measures C, he can get (in $\{|u\rangle, |u^{\perp}\rangle\}$)

$+1 \to$ outcome is $|u\rangle \to$ uncertain, both $|0\rangle$ and $|u\rangle$ have $|u\rangle$

$-1 \to$ outcome is $|u^{\perp}\rangle \to$ certain, only $|0\rangle$ has $|u^{\perp}\rangle$ term.



So the probability that Bob is certain what Alice sent is

$$\left(\frac{1}{2}\right)^3 + \left(\frac{1}{2}\right)^3 = \underline{\underline{\frac{1}{4}}}$$

(b) we must now encode <u>trits</u> since Alice can send three different bits.

However, we will run into an issue.

Imagine that Alice sends $|0\rangle$, and then Bob measures Z. Previously, to be certain that Alice sent the "other" state, Bob would need to measure -1. However, since $|+\rangle$ and $|y+\rangle$ are superpositions of $|0\rangle$ and $|-1\rangle$, we can now only <u>rule out</u> $|0\rangle$, but we still have two options on what the state could be. Hence, we can never know with certainty what state Alice sent, so this process is <u>not</u> useful for quantum cryptography.

Bob could then randomly measure <u>another</u> operator on the state he has left ($\frac{1}{\sqrt{2}}(|+\rangle + |y+\rangle)$ <u>here</u>) and he then <u>might</u> learn the state.

However, the probability of "guessing the right operator" <u>twice</u> now becomes very low.