Ali Alkadhim

Quantum Computing HW 3

3.1 P.3.8 :

a) using $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$,

$$\frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle)$$

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

$$= \frac{1}{2\sqrt{2}}(|0\rangle|0\rangle + \cancel{|0\rangle|1\rangle} + \cancel{|1\rangle|0\rangle} + |1\rangle|1\rangle + |0\rangle|0\rangle - \cancel{|0\rangle|1\rangle} - \cancel{|1\rangle|0\rangle} + |1\rangle|1\rangle)$$

$$= \frac{1}{\cancel{2}\sqrt{2}}(\cancel{2}|0\rangle|0\rangle + \cancel{2}|1\rangle|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

$\square$

b) using $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$,

$$\frac{1}{\sqrt{2}}(|i\rangle|i\rangle + |-i\rangle|-i\rangle)$$

$$= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\right]$$

$$= \frac{1}{2\sqrt{2}}\left[|0\rangle|0\rangle + \cancel{i|0\rangle|1\rangle} + \cancel{i|1\rangle|0\rangle} - |1\rangle|1\rangle + |0\rangle|0\rangle - \cancel{i|0\rangle|1\rangle} - \cancel{i|1\rangle|0\rangle} - |1\rangle|1\rangle\right]$$

$$= \frac{1}{2\sqrt{2}}\left[2|0\rangle|0\rangle - 2|1\rangle|1\rangle\right] = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \quad \square$$

Scanned with CamScanner

3.2 P. 3.12 : superposition w.r.t. standard basis but not entangled.

If a two-qubit state can be described as a tensor product of two single-qubit states, such as

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle),$$

then the state is not entangled. One can think of many two-qubit states that are a superposition w.r.t. the standard basis but are not entangled. For example

$$|\psi\rangle = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

$$= \underbrace{(a_1|0\rangle + b_1|1\rangle)}_{|\psi_1\rangle} \otimes \underbrace{(a_2|0\rangle + b_2|1\rangle)}_{|\psi_2\rangle}$$

for normalization requirement, we could have

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

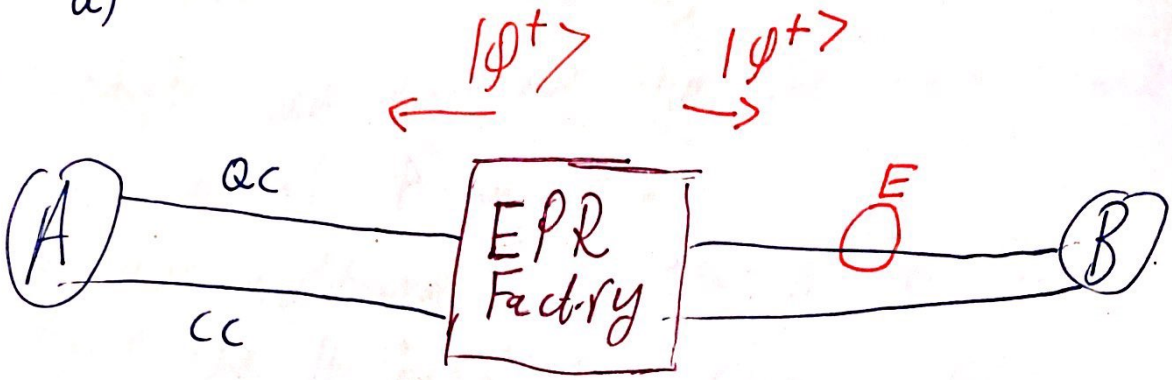
$$\Rightarrow |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$$

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

Scanned with CamScanner

3.3 P. 3.15:

a)



$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

i)

- Eve (E) always measures in the standard (S) basis.
- Alice (A) and Bob (B) randomly pick their bases they use for each qubit measurement.
- whoever measures the qubit "first" factorises the tensor product of the state

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

$$= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) + \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)\frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)\right]$$

- A and B communicate which bases they used after the measurement, and they throw away measurements in which their bases didn't match, which guarantees they both receive the same state.

Scanned with CamScanner

- Since E listens on the qubit before Bob, if she uses the same basis as A and B, she will get the correct state, and would not flip the state (and hence the bit value) of A and B.
- If she uses a different basis than A & B (i.e. A & B are using the H basis), then there is a 50% chance that the state (& hence the bit value) would flip. i.e,

	A	B	E	P(flip)
Basis	S	S	S	0
	S ⟷	H	S	$\frac{1}{2}$

Hence, since A & B also compare bit values, the probability that E is there <u>and</u> is detected is the same as $\sum P(\text{flip})$

$$P(E \text{ is there and detected})$$
$$= P(A \text{ and } B \text{ use } S \text{ basis})\, P(\text{flip})$$
$$+ P(A \text{ and } B \text{ use } H \text{ basis})\, P(\text{flip})$$
$$= \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$$

$\Rightarrow P(E \text{ is there but undetected}) = 1 - \frac{1}{4} = \frac{3}{4}$

for a <u>single</u> transmitted qubit.

Scanned with CamScanner

Hence, for <u>n qubits</u> (n = number of qubits transmitted),

$$P(E \text{ is there but undetected}) = \left(\frac{3}{4}\right)^n$$

The question is confusing/vague, especially in that it does not define S.

- If S is an arbitrary variable, then A and B can reach a probability 2^{-s} that E is undected by transmitting n qubits, according to

$$\left(\frac{3}{4}\right)^n = \left(\frac{1}{2}\right)^s$$

$$\Rightarrow n\log\left(\frac{3}{4}\right) = s\log(2) \Rightarrow n = \frac{s\log 2}{\log\left(\frac{3}{4}\right)} \quad (*)$$

- <u>If A & B know that E is using the standard basis</u>, they can reach a probabity 2^{-s} of having E be undetected by throwing away all of their H basis measurements, so that

$P(A \text{ and } B \text{ use } S \text{ basis}) = 0$, and
$P(A \text{ and } B \text{ use } H \text{ basis}) = 1$.

Scanned with CamScanner

so that

$P(E \text{ is there and undetected})$

$= P(A \,\&\, B \text{ use } S \text{ basis})\, P(\text{flip}) + P(A \,\&\, B \text{ use } H \text{ basis})\, P(\text{flip})$

$= \quad 0 \cdot 0 + 1 \cdot \frac{1}{2} = \underline{\frac{1}{2}}$

<u>for a single qubit.</u>

- If s refers to the number of qubits transmitted, then clearly this method will give them

$$P(E \text{ is there but undetected}) = \left(\frac{1}{2}\right)^s = 2^{-s} \qquad \square$$

- If s is a random variable and n is the number of qubits transmitted, then they can reach this probability by transmitting n qubits according to

$$\left(\frac{1}{2}\right)^n = \left(\frac{1}{2}\right)^s \longrightarrow n = \frac{s \log\left(\frac{1}{2}\right)}{\log\left(\frac{1}{2}\right)} = s$$

- If A & B don't know that E is using the standard basis, see pages 1-2 of this question's solution, resulting in equation ⊛.

Scanned with CamScanner

ii) What happens if Eve instead measures each qubit randomly in either the standard or Hadamard basis?

A	B	E	P(flip)

In analogy to the first part on the second page, this case just introduces another factor of $\frac{1}{2}$ for E choosing the same basis as E & B

P(E is undetected) = P

$= P(A \& B \text{ use } S \text{ basis})\, P(E \text{ uses } S \text{ basis})\, P(\text{flip})$

$+ P(A \& B \text{ use } S \text{ basis})\, P(E \text{ uses } H)\, P(\text{flip})$

$+ P(A \& B \text{ use } H)\, P(E \text{ uses } H)\, P(\text{flip})$

$+ P(A \& B \text{ use } H)\, P(E \text{ uses } S)\, P(\text{flip})$

$= \frac{1}{2}\cdot\frac{1}{2}\cdot 0 + \frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2}\cdot 0 + \frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}$

$\Rightarrow P(E \text{ is undetected}) = \frac{3}{4}$, giving eq. ⊛ again.

iii) If she picks a random state from all possible states,

Suppose Eve picks a random state $|\psi\rangle$ with an angle θ between the basis chosen by Eve & the one chosen by Bob

$|\psi\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$; $|\psi^{\perp}\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle$

Scanned with CamScanner

Since A & B throw away measurements in which their bases didn't match, we can consider one instance. Say A & B use the standard basis. Now since E measures first we have 2 cases corresponding to A sending $|0\rangle$:

1) E measures $|\psi\rangle$ & B.b measures $|0\rangle$

$$\text{Probability} = |\langle 0|\psi\rangle\langle\psi|0\rangle|^2$$

$$= |\langle 0|(\cos\theta|0\rangle + \sin\theta|1\rangle)(\cos\theta\langle 0| + \sin\theta\langle 1|)|0\rangle|^2$$

$$= \cos^4\theta$$

2) E measures $|\psi^+\rangle$ & B.b measures $|0\rangle$

$$\text{Probability} = |\langle 0|\psi^+\rangle\langle\psi^+|0\rangle|^2$$

$$= |\langle 0|(-\sin\theta|0\rangle + \cos\theta|1\rangle)(-\sin\theta\langle 0| + \cos\theta\langle 1|)|^2$$

$$= \sin^4\theta$$

Hence the probability the state does not flip

$$P(\text{not flip}) = \cos^4\theta + \sin^4\theta$$

Averaging over θ: $P(\text{not flip}) = \frac{1}{\pi/2}\int_0^{\pi/2} \cos^4\theta + \sin^4\theta \, d\theta = \frac{3}{4}$

$\Rightarrow P(E \text{ undetected}) = \frac{3}{4}$ for 1 bit

Scanned with CamScanner

b) Eve as the EPR Factory.

Eve can send any of $\{|00\rangle, |11\rangle, |+\rangle|+\rangle, |-\rangle|-\rangle\}$, then A and B can pick either the standard or Hadamard basis to make their measurement.
Say Eve sends $|00\rangle$.

$$A \xleftarrow{|00\rangle} E \xrightarrow{|00\rangle} B$$

Then their shared key's agree half of the time, since half of the time, since their bases agree half of the time. (Since they're entangled, if one measures using the same basis, the entire state becomes what was measured).

Now, Eve knows some of these bits.

Fraction of bits that Eve knows

$= P(\text{both pick } s)\, P(\text{it's the correct } s \text{ state})$

$= \frac{1}{2}\frac{1}{2} = \frac{1}{4}$

Scanned with CamScanner

3.4 P.4.1:

a) $|0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$

b) using $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$,

$|+\rangle\langle 0| - i|-\rangle\langle 1|$

$= \frac{1}{\sqrt{2}}\left(\left[\begin{pmatrix}0\\1\end{pmatrix} + \begin{pmatrix}1\\0\end{pmatrix}\right]\begin{pmatrix}0 & 1\end{pmatrix}\right) - i\frac{1}{\sqrt{2}}\left(\left[\begin{pmatrix}0\\1\end{pmatrix} - \begin{pmatrix}1\\0\end{pmatrix}\right]\begin{pmatrix}1 & 0\end{pmatrix}\right)$

$= \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} - i\begin{pmatrix}-1\\1\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix}\right]$

$= \frac{1}{\sqrt{2}}\left[\begin{pmatrix}0 & 1\\0 & 1\end{pmatrix} - i\begin{pmatrix}-1 & 0\\1 & 0\end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}i & 1\\-i & 1\end{pmatrix}$

c) $|00\rangle\langle 00|$, using S.B. ordering $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$,

$|00\rangle\langle 00| = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\\0 & 0 & 0 & 0\\0 & 0 & 0 & 0\\0 & 0 & 0 & 0\end{pmatrix}$

$|01\rangle\langle 01| = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}\begin{pmatrix}0 & 1 & 0 & 0\end{pmatrix} = \begin{pmatrix}0 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 0\\0 & 0 & 0 & 0\end{pmatrix}$

Scanned with CamScanner

$$\Rightarrow |00\rangle\langle 00| + |01\rangle\langle 01| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

d) $|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 01| + |10\rangle\langle 11|$

- $|11\rangle\langle 01| = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

- $|10\rangle\langle 11| = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

- $|00\rangle\langle 00|$ and $|01\rangle\langle 01|$ from the previous part of this question.

$$\Rightarrow |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 01| + |10\rangle\langle 11|$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Scanned with CamScanner

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

e) $|\psi^+\rangle\langle\psi^+|$; $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$\Rightarrow \langle\psi^+| = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)^+ = \frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)$$

$$\Rightarrow |\psi^+\rangle\langle\psi^+| = \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)$$

$$= \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$$

- $|00\rangle\langle 11| = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}(0\ 0\ 0\ 1) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

- $|11\rangle\langle 00| = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}(1\ 0\ 0\ 0) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

- $|11\rangle\langle 11| = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}(0\ 0\ 0\ 1) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Scanned with CamScanner

$$\Rightarrow |\psi^+\rangle\langle\psi^+| :$$

$$= \frac{1}{2}\left[\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\right]$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Scanned with CamScanner

3.5

a) $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Alice: $\{|\theta\rangle, |\theta_\perp\rangle\}$;

Basis: $|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$, $|\theta_\perp\rangle = \sin\theta|0\rangle - \cos\theta|1\rangle$

Result: $+1$, -1

Bob: $\{|\varphi\rangle, |\varphi_\perp\rangle\}$;

Basis: $|\varphi\rangle = \cos\varphi|0\rangle + \sin\varphi|1\rangle$, $|\varphi_\perp\rangle = \sin\varphi|0\rangle - \cos\varphi|1\rangle$

Result: $+1$, -1

$|\theta\rangle|\theta\rangle + |\theta_\perp\rangle|\theta_\perp\rangle$

$= (\cos\theta|0\rangle + \sin\theta|1\rangle)(\cos\theta|0\rangle + \sin\theta|1\rangle)$

$+ (\sin\theta|0\rangle - \cos\theta|1\rangle)(\sin\theta|0\rangle - \cos\theta|1\rangle)$

$= \cos^2\theta|0\rangle|0\rangle + \cos\theta\sin\theta|0\rangle|1\rangle + \sin\theta\cos\theta|1\rangle|0\rangle$

$+ \sin^2\theta|1\rangle|1\rangle + \sin^2\theta|0\rangle|0\rangle - \sin\theta\cos\theta|0\rangle|1\rangle$

$- \sin\theta\cos\theta|1\rangle|0\rangle + \cos^2\theta$

$= \sin^2\theta + \cos^2\theta(|0\rangle|0\rangle + |1\rangle|1\rangle)$

Scanned with CamScanner

And using $\sin^2\theta + \cos^2\theta = 1$

$$|\theta\rangle|\theta\rangle + |\theta_\perp\rangle|\theta_\perp\rangle = |0\rangle|0\rangle + |1\rangle|1\rangle$$

$$\Rightarrow |\varphi^+\rangle \equiv \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$$

b) Probability that they both attain $+1$:

$$P(\text{both get } +1) = |\langle\varphi|\theta\rangle|^2$$

$$= \Big|\underbrace{\left(\cos\varphi\langle 0| + \sin\varphi\langle 1|\right)}_{\text{Bob's state for } +1}\underbrace{\left(\cos\theta|0\rangle + \sin\theta|1\rangle\right)}_{\text{Alice's state for } +1}\Big|^2$$

$$= |\cos\varphi\cos\theta + \sin\varphi\sin\theta|^2$$

(since $\langle i|i\rangle = 1$ and $\langle i|j\rangle = 0$)

$$= |\cos(\theta - \varphi)|^2$$

(using the identity $\cos(\alpha - \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$)

$$= \cos^2(\theta - \varphi)$$

$\square$

Scanned with CamScanner