Solutions Homework 17 Oct 2013.

Exercice 1 *Bennett 1992 Protocol.*

Key Generation : From the explanation, it is clear that when $d_i = e_i$, Bob measures the qubit in the same basis that they are transmitted, i.e. the transmitted qbit state is $|0\rangle$ and the measurement is done in Z-basis which gives $|0\rangle$ with probability 1. A similar argument holds for $H|0\rangle$. Thus when $d_i = e_i$ we certainly have $y_i = 0$. In other words $\mathbb{P}(y_i = 0|d_i = e_i) = 1$ and $\mathbb{P}(y_i = 1|d_i = e_i) = 0$. However, when $d_i \neq e_i$ then for example the transmitted state is $|\psi\rangle = H|0\rangle$ but the measurement is done in the Z-basis which results in $|0\rangle$ or $|1\rangle$ with equal probability because $|\langle 0|\psi\rangle|^2 = |\langle 1|\psi\rangle|^2 = (1/\sqrt{2})^2 = 1/2$. In other words $\mathbb{P}(y_i = 0|d_i \neq e_i) = \frac{1}{2}$ and $\mathbb{P}(y_i = 1|d_i \neq e_i) = \frac{1}{2}$.

We observe that $y_i = 1$ only when $d_i \neq e_i$. The secret key is then generated as folllows : Alice and Bob reveal the y_i's and keep the $e_i = 1 - d_i$ such that $y_i = 1$ as a secret key. The other e_i and d_i are discarded. Indeed if $y_i = 1$ the Alice and Bob know that $e_i = 1 - d_i$ for sure. This can be proved from the Bayes rule :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = \frac{\mathbb{P}(y_i = 1|e_i = 1 - d_i)\mathbb{P}(e_i = 1 - d_i)}{\mathbb{P}(y_i = 1)} = \frac{\frac{1}{2} \times \frac{1}{2}}{\frac{1}{4}} = 1$$

In the last equalirty we used

$$\begin{aligned}\mathbb{P}(y_i = 1) &= \mathbb{P}(y_i = 1|e_i = d_i)\mathbb{P}(e_i = d_i) + \mathbb{P}(y_i = 1|e_i \neq d_i)\mathbb{P}(e_i \neq d_i) \\ &= 0 \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}.\end{aligned}$$

Here we have assumed that $\mathbb{P}(e_i \neq d_i) = \mathbb{P}(e_i = d_i) = \frac{1}{2}$.

The length of the resulting secret key is around $N\,\mathbb{P}(y_i = 1) = \frac{N}{4}$, a quarter of the length of the main sequence.

Security Check : Alice and Bob can do a security check by exchanging a small fraction of the secure bits via public channel. If the test is successful they keep the rest of the common substring secure : thus they have succeeded in generating a common secure string. If there is no attack from Eve's side and the transmission channel is perfect, then as we explained we have $e_i = 1 - d_i$ whenever $y_i = 1$. The test is :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = 1.$$

Eve's Attack : Here we discuss only the measurement attack. Alice sends the states $H^{e_i}|0\rangle$ through the optic fiber. Suppose Eve captures a photon and makes a measurement in the Z or the X basis. If she chooses the Z basis she finds the result of the measurement $|0\rangle$ or $|1\rangle$. If she finds $|0\rangle$ she sends this state to Bob. If she finds $|1\rangle$ she deduces that certainly Bob did not send the state $|0\rangle$, and that he must have sent the state $H|0\rangle$. She sends $H|0\rangle$ to Bob. If Eve chooses the X basis she finds the result of the measurement $H|0\rangle$ or $H|1\rangle$. If she finds $H|0\rangle$ she sends this state to Bob. If she finds $H|1\rangle$ she deduces that certainly Bob did not send the state $H|0\rangle$, and that he must have sent the state $|0\rangle$. She sends $|0\rangle$ to Bob. Let $E_i = 0, 1$ denote the choice of Z or X basis for Eve.

Note that we could devise other startegies for Eve but this will not help. If you wish you can devise your own strategy and see how the security criterion is affceted. Here we stick to the above strategy for Eve. Summarizing, we see that Bob receives the states $H^{e_i+E_i}|0\rangle$.

Now Bob decodes and finds the states $H^{d_i}|y_i\rangle$ ($d_i = 0, 1$ according to the basis chosen). From the measurement postulate

$$\mathbb{P}(y_i|e_i, d_i, E_i) = |\langle y_i|H^{e_i+d_i+E_i}|0\rangle|^2$$

2

In particular given $e_i = 1 - d_i$ we have

$$\mathbb{P}(y_i = 1|e_i = 1 - d_i, E_i) = |\langle y_i|H^{1+E_i}|0\rangle|^2$$

Thus

$$\begin{aligned}\mathbb{P}(y_i = 1|e_i = 1 - d_i) &= |\langle 1|H|0\rangle|^2 p(E_i = 0) + |\langle 1|H^2|0\rangle|^2 \mathbb{P}(E_i = 1)\\ &= \frac{1}{2}\mathbb{P}(E_i = 0)\end{aligned}$$

Now let us look at the security criterion. By Bayes rule :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = \frac{\mathbb{P}(y_i = 1|e_i = 1 - d_i)\mathbb{P}(e_i = 1 - d_i)}{\mathbb{P}(y_i = 1)}$$

For the denominator we use (we asume that Eve's choice of E_i is independent of Alice's and Bob's choices of e_i and d_i)

$$\begin{aligned}\mathbb{P}(y_i = 1) &= \sum_{E_i=0,1} \mathbb{P}(y_i = 1|e_i \neq d_i, E_i)\mathbb{P}(e_i \neq d_i, E_i) + \sum_{E_i=0,1} \mathbb{P}(y_i = 1|e_i = d_i, E_i)\mathbb{P}(e_i = d_i, E_i = 1)\\ &= \sum_{E_i=0,1} |\langle 1|H^{1+E_i}|0\rangle|^2\mathbb{P}(E_i) + \sum_{E_i=0,1} |\langle 1|H^{2+E_i}|0\rangle|^2\mathbb{P}(E_i)\\ &= |\langle 1|H|0\rangle|^2\mathbb{P}(E_i = 0) + |\langle 1|H|0\rangle|^2\mathbb{P}(E_i = 1)\\ &= \frac{1}{2}\end{aligned}$$

For the numerator,

$$\mathbb{P}(y_i = 1|e_i = 1 - d_i) = \sum_{E_i=0,1} |\langle 1|H^{1+E_i}|0\rangle|^2\mathbb{P}(E_i) = \frac{1}{2}\mathbb{P}(E_i = 0)$$

Putting these results alltogether we obtain :

$$\mathbb{P}(e_i = 1 - d_i|y_i = 1) = \frac{\frac{1}{2}\mathbb{P}(E_i = 0)\mathbb{P}(e_i = 1 - d_i)}{\frac{1}{2}} = \mathbb{P}(E_i = 0)\mathbb{P}(e_i = 1 - d_i)$$

Supposing that $\mathbb{P}(e_i \neq d_i) = \frac{1}{2}$ we see that $\mathbb{P}(e_i = 1 - d_i|y_i = 1) \leq \frac{1}{2}$ whatever is Eve's strategy for the choice of measurement basis $E_i = 0, 1$.

Exercice 2 : Production of Bell states.

a) One has to show that $\langle B_{x,y}|\, B_{x',y'}\rangle = \delta_{x,x'}\delta_{y,y'}$. We show it explicitly for two cases :

$$\begin{aligned}\langle B_{00}|\, B_{00}\rangle &= \frac{1}{2}(\langle 00| + \langle 11|)(|00\rangle + |11\rangle)\\ &= \frac{1}{2}(\langle 00|\, 00\rangle + \langle 00|\, 11\rangle + \langle 11|\, 00\rangle + \langle 11|\, 11\rangle).\end{aligned}$$

Now we have

$$\begin{aligned}\langle 00|\, 00\rangle = \langle 0|\, 0\rangle \langle 0|\, 0\rangle = 1, \langle 00|\, 11\rangle = \langle 0|\, 1\rangle \langle 0|\, 1\rangle = 0,\\ \langle 11|\, 00\rangle = \langle 1|\, 0\rangle \langle 1|\, 0\rangle = 0, \langle 11|\, 11\rangle = \langle 1|\, 1\rangle \langle 1|\, 1\rangle = 1.\end{aligned}$$

Thus we get that $\langle B_{00}|\, B_{00}\rangle = \frac{1}{2}(1+0+0+1) = 1$. Now let us consider

$$\begin{aligned}\langle B_{00}|\, B_{01}\rangle &= \frac{1}{2}(\langle 00| + \langle 11|)(|01\rangle + |10\rangle)\\ &= \frac{1}{2}(\langle 00|\, 01\rangle + \langle 00|\, 10\rangle + \langle 11|\, 01\rangle + \langle 11|\, 10\rangle)\\ &= \frac{1}{2}(0+0+0+0) = 0.\end{aligned}$$

b) The proof is by contradiction. Suppose there exist a_1, b_1 and a_2, b_2 such that

$$|B_{00}\rangle = (a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle).$$

Then we must have

$$\frac{1}{2}(|00\rangle + |11\rangle) = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + a_2 b_2 |11\rangle .$$

Since the states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ form a basis one has

$$\frac{1}{2} = a_1 a_2,\ \frac{1}{2} = b_1 b_2,\ a_1 b_2 = 0,\ b_1 a_2 = 0.$$

The third equality indicates that either $a_1 = 0$ or $b_2 = 0$ (or both). If $a_1 = 0$ we get a contradiction with the first equation. If on the other hand $b_2 = 0$, we get a contradiction with the second one. Therefore, there does not exist $|\psi_1\rangle$ and $|\psi_2\rangle$ such that $|B_{00}\rangle$ can be written as $|\psi_1\rangle \otimes |\psi_2\rangle$. Therefore, B_{00} is entangled.

c) By definition of the tensor product :

$$(H \otimes I)\,|x\rangle \otimes |y\rangle = H\,|x\rangle \otimes I\,|y\rangle = H\,|x\rangle \otimes |y\rangle .$$

Also, one can use that $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ to show that always

$$H\,|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x\,|1\rangle).$$

Thus,

$$(H \otimes I)\,|x\rangle \otimes |y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |y\rangle + (-1)^x\,|1\rangle \otimes |y\rangle).$$

Now we apply *'CNOT'*. By linearity, we can apply it to each term separately. Thus,

$$\begin{aligned}(CNOT)(H \otimes I)\,|x\rangle \otimes |y\rangle &= \frac{1}{\sqrt{2}}((CNOT)\,|0\rangle \otimes |y\rangle + (-1)^x (CNOT)\,|1\rangle \otimes |y\rangle)\\ &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |y\rangle + (-1)^x\,|1\rangle \otimes |y \oplus 1\rangle).\\ &= |B_{xy}\rangle .\end{aligned}$$

d) From the rule for the tensor product

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c \\ d \end{pmatrix} \\ \\ b \begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix},$$

we get for the basis states

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \qquad |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Thus,

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix},$$

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix},$$

$$|B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}.$$

Now we compute the Matrices involved in the

Let us first start with $H \otimes I$. We use the rule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{pmatrix},$$

Thus we have

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\otimes\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix}.$$

For (CNOT), we use the definition :

$$(CNOT)\,|x\rangle\otimes|y\rangle=|x\rangle\otimes|y\oplus x\rangle\,,$$

which implies that the matrix elements are

$$\langle x'y'|\,CNOT\,|xy\rangle=\langle x',y'|x,y\otimes x\rangle=\langle x'|\,x\rangle\,\langle y'|\,y\oplus x\rangle=\delta_{xx'}\delta_{y\oplus x,y'}.$$

We obtain the following table with columns xy and rows $x'y'$:

	00	01	10	11
00	1	0	0	0
01	0	1	0	0
10	0	0	0	1
11	0	0	1	0

For the matrix product $(CNOT)(H\otimes I)$, we find that

$$\begin{aligned}(CNOT)H\otimes I&=\frac{1}{\sqrt{2}}\begin{pmatrix}I & 0\\ 0 & X\end{pmatrix}\begin{pmatrix}I & I\\ I & -I\end{pmatrix}\\ &=\frac{1}{\sqrt{2}}\begin{pmatrix}I & I\\ X & -X\end{pmatrix},\end{aligned}$$

where $X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. Thus,

$$(CNOT)(H\otimes I)=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{pmatrix}.$$

One can check that for example $|B_{00}\rangle=(CNOT)(H\otimes I)\,|0\rangle\otimes|0\rangle$. Finally to check the unitarity, we have to check that $UU^\dagger=U^\dagger U=I$ for $U=H\otimes I$, $CNOT$ and $(CNOT)(H\otimes I)$. We leave this to the reader.

Problem 3: Useful properties of Bell states.

a) We have

$$|\gamma\rangle \otimes |\gamma\rangle = (\cos(\gamma)\,|0\rangle + \sin(\gamma)\,|1\rangle) \otimes (\cos(\gamma)\,|0\rangle + \sin(\gamma)\,|1\rangle)$$
$$= \cos^2(\gamma)\,|00\rangle + \cos(\gamma)\sin(\gamma)\,|01\rangle + \sin(\gamma)\cos(\gamma)\,|10\rangle + \sin^2(\gamma)\,|11\rangle\,.$$

Similarly,

$$|\gamma_\perp\rangle \otimes |\gamma_\perp\rangle = \cos^2(\gamma_\perp)\,|00\rangle + \cos(\gamma_\perp)\sin(\gamma_\perp)\,|01\rangle + \sin(\gamma_\perp)\cos(\gamma_\perp)\,|10\rangle + \sin^2(\gamma_\perp)\,|11\rangle\,.$$

A picture shows that $\cos(\gamma_\perp) = -\sin(\gamma)$ and $\sin(\gamma_\perp) = \cos(\gamma)$ (this also allows to check that $\langle\gamma|\,\gamma_\perp\rangle = 0$). Therefore, $\cos^2(\gamma_\perp) = \sin^2(\gamma)$, $\sin^2(\gamma_\perp) = \cos^2(\gamma)$ and $\cos(\gamma_\perp)\sin(\gamma_\perp) = -\cos(\gamma)\sin(\gamma)$. We find that

$$|\gamma\rangle \otimes |\gamma\rangle + |\gamma_\perp\rangle \otimes |\gamma_\perp\rangle = (\cos^2(\gamma) + \sin^2(\gamma))\,|00\rangle + (\sin^2(\gamma) + \cos^2(\gamma))\,|11\rangle\,,$$

and the terms $|01\rangle$ and $|10\rangle$ cancel. Finally,

$$\frac{1}{\sqrt{2}}(|\gamma\rangle \otimes |\gamma\rangle + |\gamma_\perp\rangle \otimes |\gamma_\perp\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |B_{00}\rangle\,.$$

b) Same type of calculations.

c) Let us first compute the norm:

$$\| \,|\phi\rangle \otimes |\psi\rangle - |B_{xy}\rangle \|^2$$
$$= \langle\phi|\phi\rangle\langle\psi|\psi\rangle - (\langle\phi| \otimes \langle\psi|)|B_{xy}\rangle$$
$$- \langle B_{xy}|(|\phi\rangle \otimes |\psi\rangle) + \langle B_{xy}|B_{xy}\rangle$$
$$= 2 - 2\,\mathrm{Re}(\langle\phi\otimes\psi|B_{xy}\rangle).$$

So we have to prove that

$$\max_{\phi,\psi} \mathrm{Re}\left(\langle \phi \otimes \psi \mid B_{xy} \rangle \right) = \frac{\sqrt{2}}{2}.$$

$$\langle \phi \otimes \psi \mid B_{xy} \rangle = \frac{1}{\sqrt{2}} \left(\langle \phi | 0 \rangle \langle \psi | 0 \rangle + \langle \phi | 1 \rangle \langle \psi | 1 \rangle \right).$$

Set $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$

$|\psi\rangle = \gamma |0\rangle + \delta |1\rangle, \quad |\gamma|^2 + |\delta|^2 = 1.$

Then we find

$$\langle \phi \otimes \psi \mid B_{xy} \rangle = \frac{1}{\sqrt{2}} (\alpha\gamma + \beta\delta).$$

$$= \frac{1}{\sqrt{2}} (\alpha, \beta) \cdot \begin{pmatrix} \gamma \\ \delta \end{pmatrix}.$$

Since $|\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\delta|^2 = 1$, by Schwartz inequality we see that

$$\max_{\alpha,\beta,\gamma,\delta} \left| \langle \phi \otimes \psi \mid B_{xy} \rangle \right| \leq \frac{1}{\sqrt{2}}.$$

and the bound is attained for say $(\gamma, \delta) = (\bar{\alpha}, \bar{\beta})$.

This proves (use $\mathrm{Re}\, z \leq |z|$ also).

$$\max_{\phi,\psi} \mathrm{Re} \langle \phi \otimes \psi \mid B_{xy} \rangle = \frac{\sqrt{2}}{2}.$$

Problem 4 : Entanglement Swapping

a). The local Bell basis at O is given by

$$\{ |B_{xy}\rangle\langle B_{xy}| \ , \ (x,y) = (0,0); (1,0); (0,1); (1,1) \}$$

The total measurement basis (projectors) is found by tensoring with identity matrices for the photons at A and B, since no measurement acts on these ones:

$$P_{xy} = \underbrace{I_A}_{2\times 2 \text{ matrix}} \otimes \underbrace{|B_{xy}\rangle\langle B_{xy}|}_{4\times 4 \text{ matrix}} \otimes \underbrace{I_B}_{2\times 2 \text{ matrix}} .$$

There are 4 matrices that are 16×16 dimensional.
Note that in Dirac notation

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| .$$

b) To compute the outcoming state after the measurement we project the initial state, So we find (up to normalization)

$$P_{xy} \ \left(|00\rangle_{AO} + |11\rangle_{AO} \right) \otimes \left(|00\rangle_{OB} + |11\rangle_{OB} \right) .$$

Let us compute this. The photons at A and B are untouched. We have

$$P_{xy}\{\,|0\,0\,0\,0\rangle + |0\,0\,1\,1\rangle + |1\,1\,0\,0\rangle$$

$$+\,|1\,1\,1\,1\rangle\,\}$$

$$= |0\rangle\,|B_{xy}\rangle\langle B_{xy}|00\rangle\,|0\rangle$$
$$+\,|0\rangle\,|B_{xy}\rangle\langle B_{xy}|01\rangle\,|1\rangle$$
$$+\,|1\rangle\,|B_{xy}\rangle\langle B_{xy}|10\rangle\,|0\rangle$$
$$+\,|1\rangle\,|B_{xy}\rangle\langle B_{xy}|11\rangle\,|1\rangle$$

$$= \langle B_{xy}|00\rangle\quad |0\rangle_A\otimes|B_{xy}\rangle_{00}\otimes|0\rangle_B$$
$$+\,\langle B_{xy}|01\rangle\quad |0\rangle_A\otimes|B_{xy}\rangle_{00}\otimes|1\rangle_B$$
$$+\,\langle B_{xy}|10\rangle\quad |1\rangle_A\otimes|B_{xy}\rangle_{00}\otimes|0\rangle_B$$
$$+\,\langle B_{xy}|11\rangle\quad |1\rangle_A\otimes|B_{xy}\rangle_{00}\otimes|1\rangle_B\,.$$

We see that in any case the two photons at O become entangled in the state $|B_{xy}\rangle$. Let us look more closely the state of photons at A and B.

Take the special case $|B_{xy}\rangle = |B_{00}\rangle$. This means the photons at O have collapsed in the state $|B_{00}\rangle$. Then the full outgoing state is

$$= \frac{1}{\sqrt{2}} |0\rangle_A \otimes |B_{00}\rangle_{OO} \otimes |0\rangle_B$$

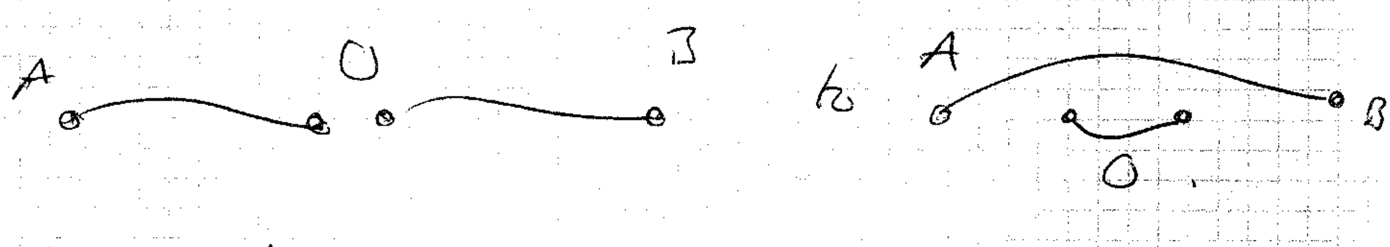
$$+ \frac{1}{\sqrt{2}} |1\rangle_A \otimes |B_{00}\rangle_{OO} \otimes |1\rangle_B .$$

$$\approx |B_{00}\rangle_{OO} \otimes |B_{00}\rangle_{AB} .$$

We see that photons at O are entangled and photons at AB are entangled.

The entanglement has been swapped from

AO and OB to AB and OO.



There are plans to use this in order to increase the distance between EPR pairs (between sattelites and earth for example).

Solutions Homework October 31. - 2013.

Problem 1. Bell for non-maximally entangled state.

We compute all averages of the form

$$\langle \psi_\alpha | A \otimes B | \psi_\alpha \rangle$$

$$\langle \psi_\alpha | A \otimes B' | \psi_\alpha \rangle$$

$$\langle \psi_\alpha | A' \otimes B | \psi_\alpha \rangle$$

$$\langle \psi_\alpha | A' \otimes B' | \psi_\alpha \rangle$$

as in the notes. For the first one we have

$$\alpha^2 \langle 00 | A \otimes B | 00 \rangle + \alpha (1-\alpha^2)^{1/2} \langle 00 | A \otimes B | 11 \rangle$$

$$+ \alpha (1-\alpha^2)^{1/2} \langle 11 | A \otimes B | 00 \rangle + (1-\alpha^2) \langle 11 | A \otimes B | 11 \rangle$$

Take $A = |a\rangle\langle a| - |a_\perp\rangle\langle a_\perp|$

$B = |b\rangle\langle b| - |b_\perp\rangle\langle b_\perp|$.

and

$$A \otimes B = |ab\rangle\langle ab| - |a b_\perp\rangle\langle a b_\perp|$$

$$- |a_\perp b\rangle\langle a_\perp b| + |a_\perp b_\perp\rangle\langle a_\perp b_\perp|$$

Then one uses:

$$\begin{cases} \langle 0 | a \rangle = \langle 0 | (\cos a |0\rangle + \sin a |1\rangle) \\ \qquad\quad = \cos a \\ \langle 1 | a \rangle = \langle 1 | \cos a |0\rangle + \sin a |1\rangle) \\ \qquad\quad = \sin a \\ \langle 0 | a_\perp \rangle = \langle 0 | (\sin a |0\rangle - \cos a |1\rangle) \\ \qquad\quad = \sin a \\ \langle 1 | a_\perp \rangle = \langle 1 | (\sin a |0\rangle - \cos a |1\rangle) \\ \qquad\quad = - \cos a . \end{cases}$$

and the same for $\langle 0 | b \rangle, \langle 1 | b \rangle, \langle 0 | b_\perp \rangle, \langle 1 | b_\perp \rangle$.

Putting everything together and with no sign mistakes one find

$$X = \langle \psi_\alpha | A \otimes B | \psi_\alpha \rangle + \langle \psi_\alpha | A \otimes B' | \psi_\alpha \rangle - \langle \psi_\alpha | A' \otimes B | \psi_\alpha \rangle$$
$$+ \langle \psi_\alpha | A' \otimes B' | \psi_\alpha \rangle .$$

Maximizing over a, b, a' and b' one find the maximal value of X in terms of α.

Note: use mathematica if you want.

Problem 2. Tsirelson inequality.

a). Check the commutation relations by doing the matrix products. Trivial.

b) Let $Q = \vec{q} \cdot \vec{\sigma}$ and $R = \vec{r} \cdot \vec{\sigma}$.

Then $[Q, R] = [\vec{q} \cdot \vec{\sigma}, \vec{r} \cdot \vec{\sigma}]$

Expanding the commutator one finds terms

$$q_x r_x [\sigma_x, \sigma_x] + q_y r_y [\sigma_y, \sigma_y] + q_z r_z [\sigma_z, \sigma_z]$$

$$= 0 + 0 + 0 = 0$$

and terms of the form

$$q_x r_y [\sigma_x, \sigma_y] + q_y r_x [\sigma_y, \sigma_x]$$
$$+ q_x r_z [\sigma_x, \sigma_z] + q_z r_x [\sigma_z, \sigma_x]$$
$$+ q_y r_z [\sigma_y, \sigma_z] + q_z r_y [\sigma_y, \sigma_z].$$

Using the commutation relations one finds ~~easily~~ that this equals

$$2i (\vec{q} \times \vec{r}) \cdot \vec{\sigma}$$

c). We start with the left hand side

$$\left(Q \otimes S + R \otimes S + R \otimes T - Q \otimes T\right)^2$$

$$= Q^2 \otimes S^2 + R^2 \otimes S^2 + R^2 \otimes T^2 + Q^2 \otimes T^2$$

$$+ QR \otimes S^2 + RQ \otimes S^2$$

$$+ QR \otimes ST + RQ \otimes TS$$

$$- Q^2 \otimes ST - Q^2 \otimes TS$$

$$+ R^2 \otimes ST + R^2 \otimes TS$$

$$- RQ \otimes ST - QR \otimes TS$$

$$- RQ \otimes T^2 - QR \otimes T^2 .$$

Using $S^2 = T^2 = R^2 = Q^2 = I$ since for example

$$S^2 = \sum_{i,j} s_i s_j \sigma_i \sigma_j = s_x^2 \sigma_x^2 + s_y^2 \sigma_y^2 + s_z^2 \sigma_z^2$$

$$= (s_x^2 + s_y^2 + s_z^2) I$$

$$= I$$

because $|\vec{s}|^2 = 1$; we get finaly :

$$(Q \otimes S + R \otimes S + R \otimes T - Q \otimes T)^2 = 4I + QR \otimes ST$$

$$+ RQ \otimes TS - RQ \otimes ST - QR \otimes TS$$

$$= 4I + [Q, R] \otimes [S, T] .$$

To deduce the inequality we note that the matrix

$$[Q, R] \otimes [S, T]$$

is equal (by question e)) to

$$-4 \, (\vec{q} \times \vec{r}).\vec{\sigma} \otimes (\vec{s} \times \vec{t}).\vec{\sigma}$$

Each matrix in the tensor terms has eigenvalues ± 1 so the max eigenvalue of the total matrix is $+4$. To this we add $4I$.

Thus the max eigenvalue of $(Q\otimes S + R\otimes S + R\otimes T - Q\otimes T)^2$ is $4+4 = 8$. Thus ~~the~~ the max eigenvalue of $Q\otimes S + R\otimes S + R\otimes T - Q\otimes T$ is $\sqrt{8} = 2\sqrt{2}$.

Thus for any $|\psi\rangle$ we have

$$|\langle\psi| \, Q\otimes S + R\otimes S + R\otimes T - Q\otimes T \, |\psi\rangle| \leq 2\sqrt{2}.$$

d). For a tensor product state $|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$

the left hand side is equal to:

$$(\langle\varphi_1|Q|\varphi_1\rangle + \langle\varphi_1|R|\varphi_1\rangle)(\langle\varphi_2|S|\varphi_2\rangle)$$

$$+ (\langle\varphi_1|Q|\varphi_1\rangle - \langle\varphi_1|R|\varphi_1\rangle)(\langle\varphi_2|T|\varphi_2\rangle).$$

Now since $|\langle\varphi_1|R|\varphi_1\rangle| \leq +1$ (again use an eigenvalue argument; ~~___~~ e.v of $\vec{r}\cdot\vec{\sigma}$ is ± 1.

this is of the form

$$(x + y)z + (x - y)z'$$

with $x, y, z \in [-1, +1]$. It is not difficult to show this is $\in [-2, +2]$.

We know the upper bound $2\sqrt{2}$ is saturated by $|\psi\rangle = |B_{00}\rangle$ and $\vec{t}, \vec{r}, \vec{s}, \vec{\rho}$ arranged like in the course notes.

Problem 3 : GHZ states.

a) Using $X\,|\uparrow\rangle = |\downarrow\rangle$, $X|\downarrow\rangle = +|\uparrow\rangle$

and $Y\,|\uparrow\rangle = -i\,|\downarrow\rangle$, $Y|\downarrow\rangle = i\,|\uparrow\rangle$

This is straightforward calculatio, for example:

$$Y\otimes Y\otimes X\ |GHZ\rangle$$

$$= \frac{1}{\sqrt{2}}\left(Y\otimes Y\otimes X\ |\uparrow\uparrow\uparrow\rangle - Y\otimes Y\otimes X\,|\downarrow\downarrow\downarrow\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(Y|\uparrow\rangle\otimes Y|\uparrow\rangle\otimes X|\uparrow\rangle - Y|\downarrow\rangle\otimes Y|\downarrow\rangle\otimes X|\downarrow\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left((-i)^2\,|\downarrow\downarrow\downarrow\rangle - i^2\,|\uparrow\uparrow\uparrow\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\ |GHZ\rangle .$$

$\Rightarrow$ $Y\otimes Y\otimes X$ has eigenstate $|GHZ\rangle$ with eigenvalue $+1$.

For the others its similar

b) Since $|GHZ\rangle$ is an eigenstate of the observable it is not perturbed and the result for the observables is given by the eigenvalue with probability 1.

Then the measurement results are with probability one!

	Alice	Bob	Charlie		eigenvalue	state
exp 1	$Y \otimes$	$Y \otimes$	X	$\longrightarrow$	$+1$	$\lvert GHZ\rangle$
exp 2	$Y \otimes$	$X \otimes$	Y	$\longrightarrow$	$+1$	$\lvert GHZ\rangle$
exp 3	$X \otimes$	$Y \otimes$	Y	$\longrightarrow$	$+1$	$\lvert GHZ\rangle$
exp 4	$X \otimes$	$X \otimes$	X	$\longrightarrow$	-1	$\lvert GHZ\rangle$.

c) Now we suppose that each observable has a definite value indep of wether we perform an experiment. When Alice Bob or Charlie measures Y ~~they~~ they would think that the outcome is $F_{A,B,C}(Y, \lambda) = \pm 1$ and when ~~they~~ they measures X ~~they~~ they would think the outcomes is $F_{A,B,C}(X, \lambda) = \pm 1$ where F and λ are a function and hidden variables of the classical theory. So the results (classically would be)

	Alice	Bob	Charlie	
exp 1	$F_A(Y, \lambda)$	$F_B(Y, \lambda)$	$F_C(X, \lambda)$	?
exp 2	$F_A(Y, \lambda)$	$F_B(X, \lambda)$	$F_C(Y, \lambda)$	?
exp 3	$F_A(X, \lambda)$	$F_B(Y, \lambda)$	$F_C(Y, \lambda)$	?
exp 4	$F_A(X, \lambda)$	$F_B(X, \lambda)$	$F_C(X, \lambda)$	?
Product	~~β~~ $+1$	$+1$	$+1$	$+1$.

The product along the columns is always +1 because F takes values ±1 and they occur in pairs along the columns.
Thus the product of all mean results is +1.

$$\{F_A(Y,\lambda)\,F_B(Y,\lambda)\,F_C(X,\lambda)\}\{F_A(Y,\lambda)\,F_B(X,\lambda)\,F_C(Y,\lambda)\}$$
$$\cdot\{F_A(X,\lambda)\,F_B(Y,\lambda)\,F_C(Y,\lambda)\}\{F_A(X,\lambda)\,F_B(X,\lambda)\,F_C(X,\lambda)\}$$
$$= +1.$$

But this is not what is obtained quantum mechanically. Indeed the product of the four quantum eigenvalues is -1 !

Thus there does not exist functions $F_{A,B,C}(W,\lambda)$ $W = X$ or Y that describe the quantum results!

Problem 4, Entanglement swapping with GHZ states.

The method of solution is similar to Problem 4 in previous homework. The entanglement $AA' \otimes BB' \otimes CC'$ SWAPS to $(ABC) \otimes (A'B'C')$. We do not write the details here.