

# Quantum Computing

Mathias Niepert

## Final Exam

### Problem 1

$$1) D = 2P - I = \frac{2}{N} \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & \dots & 1 & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & \dots & 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

$$R = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix} = 2|0\rangle^{\otimes n} \langle 0|^{\otimes n} - I^{\otimes n} = 2|0\dots 0\rangle \langle 0\dots 0| - I^{\otimes n}$$

Show that  $D = H^{\otimes N} \cdot R \cdot H^{\otimes N}$ .

$$\begin{aligned} H^{\otimes n} \cdot R \cdot H^{\otimes n} &= H^{\otimes n} \cdot (2|0\dots 0\rangle \langle 0\dots 0| - I^{\otimes n}) \cdot H^{\otimes n} = \\ &= (H^{\otimes n} \cdot 2|0\dots 0\rangle \langle 0\dots 0| \cdot H^{\otimes n}) - (H^{\otimes n} \cdot I^{\otimes n} \cdot H^{\otimes n}) = \\ &= (H^{\otimes n} \cdot 2|0\dots 0\rangle \langle 0\dots 0| \cdot H^{\otimes n}) - (H^{\otimes n} \cdot H^{\otimes n}) = \\ &= (H^{\otimes n} \cdot 2|0\dots 0\rangle \langle 0\dots 0| \cdot H^{\otimes n}) - I^{\otimes n} = \end{aligned}$$

$$H^{\otimes n} \cdot 2 \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix} \cdot H^{\otimes n} - I^{\otimes n} = \mathbf{1}$$

$$\begin{aligned}
& H^{\otimes n} \cdot \frac{2}{\sqrt{2^n}} \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix} - I^{\otimes n} \stackrel{2}{=} \\
& \frac{2}{2^n} \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & \dots & 1 & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & \dots & 1 & 1 \end{pmatrix} - I^{\otimes n} = \frac{2}{N} \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & \dots & 1 & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & \dots & 1 & 1 \end{pmatrix} - I^{\otimes n} \\
& = \\
& 2P - I = D
\end{aligned}$$

<sup>1</sup> Because the first row of  $H^{\otimes n}$  contains only Ones.

<sup>2</sup> Because the first column of  $H^{\otimes n}$  contains only Ones.

2) Figure 1 implements the diffusion matrix  $D = -I + 2P = H^{\otimes n} \cdot R \cdot H^{\otimes n}$

It's easy to see that the first and last column of Hadamard-gates implements  $H^{\otimes n}$ . It remains to show that the inner circuit (within the dotted frame) implements  $R$ .

$$XX = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = I \quad (1)$$

$$HH = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = I \quad (2)$$

Assume we have n "inputs" (QuBits). The first n-1 (0...n-2) qubits remain always in the state in which they enter the circuit because of (1).

If only one of the first QuBits is not in the state  $|0\rangle$  all the QuBits remain unchanged because of (1) and (2). However, if **all** of these first n-1 qubits are in the state  $|0\rangle$  before entering the circuit, the operation  $X \cdot H \cdot X \cdot H \cdot X$  is performed on the last QuBit.

### Two possibilities:

1. If the last QuBit is in the state  $|1\rangle$ , then  $|1\rangle \rightarrow X|1\rangle \rightarrow |0\rangle \rightarrow H|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow X \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow H \frac{1}{\sqrt{2}}(|0\rangle +$



$|1\rangle \rightarrow |0\rangle \rightarrow X|0\rangle \rightarrow |1\rangle$

The qubit remains in the same state.

2. If the last QuBit is in the state  $|0\rangle$ , then  $|0\rangle \rightarrow X|0\rangle \rightarrow |1\rangle \rightarrow H|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow X \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) \rightarrow H \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) \rightarrow -|1\rangle \rightarrow -X|1\rangle \rightarrow -|0\rangle$

The qubit gets a negative phase which can be pulled to the front of the composite state  $|0\dots 0\rangle$ .

This shows, that the circuit is equivalent to R. It changes the (composite/ system-) state  $|0\dots 0\rangle$  to  $-|0\dots 0\rangle$  and leaves all other possible (composite/ system-) states unchanged.

The X-gate can be implemented with 4 phase gates in a row. The controlled NOT gate ( $C^{n-1}(X)$ ) can be implemented with  $2(n-1)$  Toffoli-gates and  $(n-1)$  work qubits like in Figure 4.10 in the textbook. The Toffoli gate can be implemented with 16 gates out of the standard gate set  $\{H, \sigma_z^{\pm\frac{1}{4}}, CNOT\}$ . (See textbook page 182, Figure 4.9.).

Hence we used overall  $16 \cdot 2(n-1) + 2n + 2$  (hadamard gates)  $+ 2(4n)$  (phase gates for the X-gates)  $= 32n - 16 + 2n + 2 + 8n = 42n - 14$  gates. This is  $\in poly(n)$ .

## Problem 2

- 1) If we want to measure in a basis other than the computational one, we need to find the unitary transformation which transforms from the basis we wish to perform the measurement in, to the computational basis and then finally measure in the computational basis.

In the given case, it's easy to see that the transformations we need to apply to the second qubit (which we want to measure) are the phase operator gate P and the Hadamard gate H. Proof:

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

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

(a) Apply phase gate P:

$$P \cdot |+\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ e^{i\phi} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$P \cdot |-\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -e^{i\phi} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

(a) Apply Hadamard gate H:

$$H \cdot \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = |0\rangle$$

$$H \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 0 \\ 2 \end{pmatrix} = |1\rangle \quad \square$$

We have a two-qubit system and we measure the second in the  $|+\rangle$ ,  $|-\rangle$  basis. Thus the two unitary operations we need to perform are  $I \otimes P$  (or  $P \otimes I$  which is the controlled phase gate and has the same result on the given input state) and  $I \otimes H$ .

We start in the state  $(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|00\rangle + \beta|10\rangle$ . Now we perform the CNOT on the system. This gives us the state  $\alpha|00\rangle + \beta|11\rangle$ .

After applying  $I \otimes P$  we are in  $\alpha|00\rangle + \beta|1\rangle e^{-i\phi}|1\rangle = \alpha|00\rangle + \beta e^{-i\phi}|11\rangle$ .

Perform  $I \otimes H$  which results in  $\frac{1}{\sqrt{2}}\alpha|0\rangle(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}\beta e^{-i\phi}|1\rangle(|0\rangle - |1\rangle)$

$$= \frac{1}{\sqrt{2}}\alpha(|00\rangle + |01\rangle) + \frac{1}{\sqrt{2}}\beta e^{-i\phi}(|10\rangle - |11\rangle) =$$

$$\frac{1}{\sqrt{2}}\alpha|00\rangle + \frac{1}{\sqrt{2}}\alpha|01\rangle + \frac{1}{\sqrt{2}}\beta e^{-i\phi}|10\rangle - \frac{1}{\sqrt{2}}\beta e^{-i\phi}|11\rangle$$

Rearrange the state:

$$\frac{1}{\sqrt{2}}[(\alpha|0\rangle + \beta e^{-i\phi}|1\rangle)|0\rangle + (\alpha|0\rangle - \beta e^{-i\phi}|1\rangle)|1\rangle]$$

Now we measure the second qubit in the computational basis and get the outcomes  $\alpha|0\rangle + \beta e^{-i\phi}|1\rangle$  and  $\alpha|0\rangle - \beta e^{-i\phi}|1\rangle$ , respectively.

$$2) \wedge(e^{-i\phi}) \equiv P \otimes I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{-i\phi} & 0 \\ 0 & 0 & 0 & e^{-i\phi} \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{-i\phi}|10\rangle\langle 10| + e^{-i\phi}|11\rangle\langle 11|$$

- 3) We want the first qubit (the one which remains after the measurement) to be in the state  $\alpha|0\rangle + \beta e^{-i\phi}|1\rangle$  when we measure  $|1\rangle$  (because  $P \cdot |\psi\rangle = \alpha|0\rangle + \beta e^{-i\phi}|1\rangle$ ) and when we measure  $|0\rangle$  in the state  $\alpha|0\rangle + \beta|1\rangle$ .

When we measure  $|1\rangle$  we need to apply Z because

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ -\beta e^{-i\phi} \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta e^{-i\phi} \end{pmatrix} = \alpha|0\rangle + \beta e^{-i\phi}|1\rangle.$$

When  $|0\rangle$  is measured I don't know what to do. We would need to apply something like  $P$  but this is impossible to achieve only with multiplications of the Pauli matrices. Measurements commute with quantum gates when the qubit being measured is a control qubit. This is not the case here...?!? I hope I get the question right.

### Problem 3

- 1)  $N = 105; N^2 = 11025; 11025 \leq q = 2^m < 22050 \Rightarrow q = 2^{14} = 16384$

State before measurement:

$$\frac{1}{16384} \sum_{a=0}^{16383} \sum_{c=0}^{16383} e^{2\pi i ac/16384} |c\rangle |x^a \pmod{n}\rangle$$

- 2) Find all  $c$ 's such that  $-3 \leq 6c \pmod{q} \leq 3$

$$11^1 = 11 \pmod{15}$$

$$11^2 = 16 \pmod{15}$$

$$11^3 = 71 \pmod{15}$$

$$11^4 = 46 \pmod{15}$$

$$11^5 = 86 \pmod{15}$$

$$11^6 = 1 \pmod{15}$$

Possible candidates are integers nearest to  $\{0, 1, 2, 3, 4, 5\} \times \frac{q}{r}$  with  $r$  period of  $x \pmod{q}$ .  $\frac{q}{r} = 2730\frac{2}{3}$ .

$\Rightarrow c_1 = 0 = 0(\text{mod } q), c_2 = 2731 = 2(\text{mod } q), c_3 = 5461 = -2(\text{mod } q), c_4 = 8192 = 0(\text{mod } q), c_5 = 10923 = 2(\text{mod } q), c_6 = 13653 = -2(\text{mod } q).$

- 3) We want to compute the probability that the system ends in a particular state  $|c, x^k(\text{mod } n)\rangle$  with  $0 \leq k < r$ . Sum over all ways to reach the state  $|c, x^k(\text{mod } n)\rangle$ . This is

$$|\frac{1}{q} \sum_{a: x^a = x^k} e^{2\pi i ac/q}|^2 \text{ over all } a, 0 \leq a < q \text{ with } x^a = x^k(\text{mod } n).$$

Because  $a = br + k$  with  $r$  the period of  $x \text{ mod } n$  and  $b \in \{0, \dots, \lfloor (q - 1 - k)/r \rfloor\}$  we can rewrite the sum to :

$$\begin{aligned} |\frac{1}{q} \sum_{b=0}^{\lfloor (q-1-k)/r \rfloor} e^{2\pi i (br+k)c/q}|^2 &= |\frac{1}{q} \sum_{b=0}^{\lfloor (q-1-k)/r \rfloor} e^{2\pi i kc/q + 2\pi i brc/q}|^2 = \\ |\frac{1}{q} e^{2\pi i kc/q} \sum_{b=0}^{\lfloor (q-1-k)/r \rfloor} e^{2\pi i brc/q}|^2 &= |\frac{1}{q} \sum_{b=0}^{\lfloor (q-1-k)/r \rfloor} e^{2\pi i brc/q}|^2 \end{aligned}$$

Now insert particular values. Assume we measured 16 in the second register.  $\Rightarrow k = 2$ . We know that  $r = 6$  and  $q = 2^{14}$ .

$$P(c) = |\frac{1}{16384} \sum_{b=0}^{2730} (e^{12\pi i c/16384})^b|^2 = |\frac{1}{16384} \frac{1 - (e^{32772\pi i c/16384})}{1 - e^{12\pi i c/16384}}|^2$$

Particular Values (with Calculator):

$$P(1) \approx 4.13922e-10 \approx 0.0\%$$

$$P(123) \approx 4.16387e-10 \approx 0.0\%$$

$$P(1337) \approx 8.97445e-10 \approx 0.0\%$$

$$P(2730) \approx 0.00474804 \approx 0.47\%$$

$$P(2731) \approx 0.01900005 \approx 1.90\%$$

$$P(2732) \approx 0.00118806 \approx 0.12\%$$

- 4)  $P(0) \approx 0.0277642 \approx 2.7\%$

$$P(2731) \approx 0.01900005 \approx 1.9\%$$

$$P(5461) \approx 0.01900006 \approx 1.9\%$$

$$P(8192) \approx 0.0190006 \approx 1.9\%$$

$$P(10923) \approx 0.0190005 \approx 1.9\%$$

$$P(13652) \approx 0.00118805 \approx 0.1\%$$

5) Use  $c = 10923$ :

$\frac{c}{q} = \frac{10923}{16384} = \frac{1}{\frac{16384}{10923}} = \frac{1}{1 + \frac{5461}{10923}} = \frac{1}{1 + \frac{1}{2 + \frac{1}{5461}}}$ . Stop before the denominator exceeds 105. Thus  $\frac{c_1}{r_1} = \frac{1}{1 + \frac{1}{2}} = \frac{2}{3} \Rightarrow r_1 = 3$ . Try small multiples of  $r_1$  as possible values of  $r$  and check if  $x^r = 1 \pmod{105}$ . This is the case for  $r = 6$ . Thus  $r = 6$  is the period of 11 mod 105.

6) Test if  $r$  is even and  $x^{r/2} \neq -1 \pmod{105}$ :

$$6 \text{ is even and } x^3 = 71 \neq -1 \pmod{105}.$$

Now compute  $\gcd(x^3 - 1, 105)$  and  $\gcd(x^3 + 1, 105)$ :

$\gcd(1330, 105) = 7$  and  $\gcd(1332, 105) = 3$  which are both non-trivial factors of 105.

#### Problem 4

$$1) |u_o\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \equiv \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ \dots \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$U_f |u_o\rangle = \frac{1}{\sqrt{N}} ((\sum_{x=0; x \neq a}^{N-1} |x\rangle) - |a\rangle) = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ \dots \\ -1 \\ 1 \\ \dots \\ 1 \\ 1 \end{pmatrix}$$

Assume  $N = 2^n$ . A state is entangled if it's not a product state. The state  $U_f|u_0\rangle$  is not a product state because otherwise it would be possible to write it as  $\mathbb{C}^2 \otimes (\mathbb{C}^2)^{\otimes n-1}$ . Proof:

$$\text{Let } \mathbb{C}^2 = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \text{ with } |\alpha|^2 + |\beta|^2 = 1 \text{ and } (\mathbb{C}^2)^{\otimes n-1} = \begin{pmatrix} \lambda_1 \\ \dots \\ \dots \\ \dots \\ \lambda_{N/2} \end{pmatrix}$$

(also normalized). Let the  $k$ -th component in  $U_f|u_0\rangle$  be the negative one. Applying the kronecker product  $(\mathbb{C}^2 \otimes (\mathbb{C}^2)^{\otimes n-1})$  it must be:  $\alpha \cdot \lambda_i = \frac{1}{\sqrt{N}}$ , for  $i \neq k$  and  $-\frac{1}{\sqrt{N}}$  for  $i = k$  and  $\beta \cdot \lambda_i = \frac{1}{\sqrt{N}}$ , for all  $i$ . This is not possible in  $\mathbb{C}$ .

- 2) Find all vectors  $v_i$  which are linear combinations of  $|u_0\rangle$  and  $U_f|u_0\rangle$  and with  $U_f v_i = \lambda v_i$ ,  $\lambda \in \mathbb{C}$ .  $U_f$  takes  $|a\rangle$  (the  $a$ -th element  $x$  in the vector-representation) to  $-|a\rangle$  (to  $-x$ ) and leaves everything else as it is. So either the  $a$ -th element must be 0 or all other elements, except  $a$ , must be 0 to hold the condition  $U_f v_i = \lambda v_i$ ,  $\lambda \in \mathbb{C}$ . Thus the normalized eigenvectors are

$$v_1 = |a\rangle = \begin{pmatrix} 0 \\ \dots \\ 1 \\ 0 \\ \dots \\ 0 \end{pmatrix} \text{ and } v_2 = \frac{1}{\sqrt{N-1}} \sum_{x=0; x \neq a}^{N-1} |x\rangle = \frac{1}{\sqrt{N-1}} \begin{pmatrix} 1 \\ \dots \\ 0 \\ 1 \\ \dots \\ 1 \end{pmatrix}$$

- 3)  $|u_0\rangle = \frac{\sqrt{N-1}}{\sqrt{N}} v_2 + \frac{1}{\sqrt{N}} v_1 = \frac{\sqrt{N-1}}{\sqrt{N}} \frac{1}{\sqrt{N-1}} \sum_{x=0; x \neq a}^{N-1} |x\rangle + \frac{1}{\sqrt{N}} |a\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$
- 4) Let  $\cos(\varphi/2) = \sqrt{\frac{N-1}{N}}$  for some  $\varphi$ . Thus  $|u_0\rangle = \cos(\varphi/2)v_2 + \sin(\varphi/2)v_1$ .

The Grover iteration performs a reflection about the vector  $|v_2\rangle$  and then about the vector  $|u_0\rangle$  itself, in the  $v_1, v_2$  plane. With the given representation of  $|u_0\rangle$  this is a rotation of  $|u_0\rangle$  by  $\varphi$  radians. (See Figure 6.3 in the textbook).

Thus  $G|u_0\rangle = \cos(\varphi/2 + \varphi)v_2 + \sin(\varphi/2 + \varphi)v_1 = \cos(3\varphi/2)v_2 + \sin(3\varphi/2)v_1$ . Continued application of  $G$  takes the state to

$$G^k|u_0\rangle = \cos(\frac{2k+1}{2}\varphi)v_2 + \sin(\frac{2k+1}{2}\varphi)v_1.$$

- 5) The initial state is  $|u_0\rangle = \sqrt{\frac{N-1}{N}}v_2 + \sqrt{\frac{1}{N}}v_1 = \cos(\varphi/2)v_2 + \sin(\varphi/2)v_1$  with  $v_1 = |a\rangle$ .

Because all the vectors are normalized (unit circle) the projection of a vector onto the  $|v_1\rangle$  axis is the sinus of the angle of this vector and the projection onto the  $|v_2\rangle$  axis is the cosinus of the angle of the vector. At the beginning of the iteration the vector  $|u_0\rangle$  has the angle  $\varphi/2$  with the  $|v_2\rangle$  axis and  $\sin(\varphi/2) = \frac{1}{\sqrt{N}}$ . Now we want to move the vector  $|u_0\rangle$  as close as possible to the axis  $|v_1\rangle$  (through  $\sim \pi/2 - \varphi/2$  radians). This is the angle of the unit vector whose cosinus (projection to the  $|v_2\rangle$  axis) is  $\frac{1}{\sqrt{N}}$ .

Hence, rotating through  $\arccos(\frac{1}{\sqrt{N}})$  radians rotates the system ( $G^k|u_0\rangle$ ) to  $|v_1\rangle = |a\rangle$ . Every iteration of Grover's algorithm rotates the system through  $\varphi$  radians. Thus we need  $k = \lfloor \frac{\arccos(\frac{1}{\sqrt{N}})}{\varphi} \rfloor$  iterations.

### Problem 5

- 1) Alice's answers for question  $j$  may be  $a_1^j, a_2^j, a_3^j$  and Bob's answers for question  $k$  may be  $b_1^k, b_2^k, b_3^k$ .

It must be  $a_1^j a_2^j a_3^j = -1$  and  $b_1^k, b_2^k, b_3^k = 1$  for all  $j, k$ . Thus

$$a_1^1 a_2^1 a_3^1 a_1^2 a_2^2 a_3^2 a_1^3 a_2^3 a_3^3 = -1 \text{ and}$$

$$b_1^1 b_2^1 b_3^1 b_1^2 b_2^2 b_3^2 b_1^3 b_2^3 b_3^3 = 1$$

If they want to win the game, it has to be  $a_k^j = b_j^k$  for all  $j, k$  which is impossible because at least one of them has to be different (because one product is 1 and the other is -1).  $\Rightarrow$  There is a probability ( $\geq 1/9$ ) that  $a_k^j \neq b_j^k$

- 2) a) The product of the operators in each row is -I and the product in each column is I:

$$(\sigma^{m_1} \otimes \sigma^{n_1})(\sigma^{m_2} \otimes \sigma^{n_2})(\sigma^{m_3} \otimes \sigma^{n_3}) = (\sigma^{m_1} \sigma^{m_2} \sigma^{m_3} \otimes \sigma^{n_1} \sigma^{n_2} \sigma^{n_3})$$

$$XYZ = i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, YXZ = -i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, XZY = -i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$ZXY = i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, ZYX = -i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, YZX = i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{Row 1: } XYZ \otimes XYZ = i^2(I \otimes I) = -\mathbf{I}$$

$$\text{Row 2: } YZX \otimes ZXY = i^2(I \otimes I) = -\mathbf{I}$$

$$\text{Row 3: } ZXY \otimes YZX = i^2(I \otimes I) = -\mathbf{I}$$

$$\text{Column 1: } XYZ \otimes XZY = -ii(I \otimes I) = \mathbf{I}$$

$$\text{Column 2: } YZX \otimes YXZ = -ii(I \otimes I) = \mathbf{I}$$

$$\text{Column 3: } ZXY \otimes ZYX = -ii(I \otimes I) = \mathbf{I}$$

It has to be  $\sigma^m \sigma^o \otimes \sigma^n \sigma^p = \sigma^o \sigma^m \otimes \sigma^p \sigma^n$  for all given combinations of  $m, n, o, p \in \{X, Y, Z\}$ . Because then  $(\sigma^m \otimes \sigma^n)(\sigma^o \otimes \sigma^p) - (\sigma^o \otimes \sigma^p)(\sigma^m \otimes \sigma^n) = 0$

If it's possible to prove that  $\sigma^m \sigma^o = -\sigma^o \sigma^m$  and  $\sigma^n \sigma^p = -\sigma^p \sigma^n$  for all given combinations, we are done! (Because we can pull out both -1s which gives the coefficient 1).

Indeed, it is  $XY = -YX$ ,  $YZ = -ZY$  and  $ZX = -XZ$   $\square$

b) Textbook page 88:

Choose the EPR pair  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Because of (a) and because we measure  $\sigma_i$  in the state of the  $i$ -th qubit we can write:

$$\langle (\sigma_1^m \otimes \sigma_3^n) \otimes (\sigma_2^m \otimes \sigma_4^n) \rangle = \langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} | \sigma_1^m \otimes \sigma_2^m | \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rangle \langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$| \sigma_3^n \otimes \sigma_4^n | \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rangle$$

For the state  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$   $X \otimes X, Y \otimes Y$

and  $Z \otimes Z$  is like the identity. Thus

$$\langle (\sigma_1^m \otimes \sigma_3^n) \otimes (\sigma_2^m \otimes \sigma_4^n) \rangle = \langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rangle \langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rangle.$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = 1 \cdot 1 = 1.$$

c) Lack of time...