1. Alice and Bob wish to use 30 Qbits in order to agree a one-time pad. Bob receives 30 Qbits from Alice, and for each one he randomly applies 1 or H before measuring it. Subsequently Alice tells him what type she used for preparing each Qbit. The results are as follows. The four rows in each block show the Qbit number, Bob’s measurement type, Bob’s result and Alice’s preparation type.

<table>
<thead>
<tr>
<th>Qbit</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>B type</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td>1</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>result</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>A type</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>H</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>H</td>
<td>1</td>
<td>1</td>
<td>H</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Qbit</th>
<th>16</th>
<th>17</th>
<th>18</th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
<th>28</th>
<th>29</th>
<th>30</th>
</tr>
</thead>
<tbody>
<tr>
<td>B type</td>
<td>1</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>result</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>A type</td>
<td>1</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td>H</td>
<td>1</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td>H</td>
<td>H</td>
<td>1</td>
<td>H</td>
</tr>
</tbody>
</table>

(a) How long is their one-time pad, and what is it? What message does Bob send back to Alice?

Before they use their pad, they remember they should have checked to see if the Qbits were intercepted. They decide they will sacrifice half of their useful Qbits: the first, third, fifth and so on. When Alice tells Bob how she prepared them, it turns out that they were indeed just as Bob measured them.

(b) What can they deduce about interception? What one-time pad do they end up with?

(c) Suppose they want 20 bits in their one-time pad, and 99.9% certainty that Eve is not intercepting every Qbit. How many Qbits do they need to use? (You can use a calculator, but also try to estimate the answer without one, using \( \log_2 3 \approx 1.6 \).)

(d) Suppose they still want 20 bits for the one-time pad, but this time they want 95% certainty that Eve is intercepting no more than 10% of the Qbits. How many Qbits do they need?

2. (a) Calculate all four Bell states \( |\psi_{xy}\rangle \) as linear combinations of \( |00\rangle, |01\rangle \) etc.

(b) Show that the four Bell states \( |\psi_{xy}\rangle \) are orthonormal, and hence form a basis (the Bell basis).

(c) Calculate \( H_1 H_0 |\psi_{xy}\rangle \) in terms of the Bell basis for \( xy = 01, 10, 11 \). Write down the matrix of \( H_1 H_0 \) with respect to that basis.
1. (a) The one-time pad has 16 bits. It is
\[ 0011100111001001 \]
Bob sends a message to Alice saying which are the useful bits. There are various ways he can do this.
Qbit numbers of useful bits:
\[ 3, 4, 7, 10, 11, 16, 17, 18, 19, 24, 25, 26, 27, 28, 29, 30 \]
Complete list of measurement types:
\[ \text{HH11H11HHH1HH1HHH1H1HH11HH1HH1} \]

(b) Eight useful Qbits were sacrificed for interception checking. Suppose they were all intercepted, so there would be a probability of 25% for each Qbit that it gave the wrong measurement for Bob. Hence the probability of no discrepancies, i.e. the probability that Eve was lucky, is \( \left( \frac{3}{4} \right)^8 \approx 0.1 \). In practice Alice and Bob would want to use more Qbits to get a better estimate of the risk, but if they went ahead with these their eight non-sacrifice Qbits (the even numbered ones) would give a one-time pad of
\[ 01011001 \]

(c) If Eve is intercepting every Qbit, then on average 25% of the Qbits will show a discrepancy if Alice and Bob compare values. For \( n \) check Qbits, the probability that Eve will not be detected for any of them is \( \left( \frac{3}{4} \right)^n \). For the 99.9% certainty we are looking for \( n \) large enough that \( \left( \frac{3}{4} \right)^n < 0.001 \). With a calculator we find we need \( n \geq 25 \). (Without: \( \log_2 \left( \frac{3}{4} \right) = \log_2 3 - 2 \approx -0.4 \). Also, \( 2^{10} = 1024 \), so \( \log_2 0.001 \approx -10 \), so we want \( n \geq 25 \).) It follows that Alice and Bob need 45 useful Qbits: 20 for the pad and 25 sacrificed for detecting interceptions. Since on average only half the Qbits are useful, they need 90 Qbits altogether.

(d) If Eve intercepts more than 10%, then on average at least 2.5% of the Qbits will show a discrepancy. The probability of no discrepancy in \( n \) check Qbits is 0.975\(^n\), so for 95% certainty we want 0.975\(^n\) < 0.05. By a calculator, \( n > \frac{\log_{0.975} 0.05}{\log_{0.975} 0.999} \approx 120 \). For 140 useful Qbits (20 for the pad, 120 to check), Alice and Bob need 280 Qbits.

2. (a) Use \( |\psi_{xy}\rangle = Z_1 X_0^n |\psi_{00}\rangle \)
\[ |\psi_{00}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \] (from lectures)
\[ |\psi_{01}\rangle = X_0 |\psi_{00}\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) \]
\[ |\psi_{10}\rangle = Z_1 |\psi_{00}\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) \]
\[ |\psi_{11}\rangle = Z_1 X_0 |\psi_{00}\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \]

(b) Using the fact that \( Z \) and \( X \) are self-adjoint, we have
\[ \langle \psi_{x' y'} | \psi_{x y} \rangle = \langle \psi_{00} | Z_1^x X_0^y Z_1^x X_0^y | \psi_{00} \rangle \]
\[ = \langle \psi_{00} | Z_1^x \otimes x X_0^y \otimes y | \psi_{00} \rangle = \langle \psi_{00} | \psi_{x' y'} \rangle. \]
Hence it suffices to show that \( \langle \psi_{00} | \psi_{x y} \rangle = 0 \) if \( xy \) is 01, 10 or 11. For the cases \( y = 1 \) this is obvious, because \( |01\rangle \) and \( |10\rangle \) are both orthogonal to \( |00\rangle \) and \( |11\rangle \). For \( xy = 10 \) we have
\[ \langle \psi_{00} | \psi_{10} \rangle = \frac{1}{2} \left( \langle 00 | + \langle 11 | \langle 00 | - \langle 11 | \right) \]
\[ = \frac{1}{2} \left( \langle 00 |00 \rangle + \langle 11 |00 \rangle - \langle 00 |11 \rangle - \langle 11 |11 \rangle \right) \]
\[ = \frac{1}{2} (1 + 0 - 0 - 1) = 0. \]
Alternatively, writing
\[ |\psi_{00}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + 0|01\rangle + 0|10\rangle + \frac{1}{\sqrt{2}} |11\rangle) \]
\[ |\psi_{10}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + 0|01\rangle + 0|10\rangle - \frac{1}{\sqrt{2}} |11\rangle) \]
the inner product can be calculated as
\[
\left( \frac{1}{\sqrt{2}} \right)^* \left( \frac{1}{\sqrt{2}} \right) + 0^*0 + 0^*0 + \left( \frac{1}{\sqrt{2}} \right)^* \left( -\frac{1}{\sqrt{2}} \right) = \frac{1}{2} - \frac{1}{2} = 0.
\]

(c) Using \( HZ = XH \) we see
\[
H_1H_0|\psi_{xy}\rangle = H_1H_0Z_x^yX_0^y|\psi_{00}\rangle \\
= X_x^yZ_0^yH_1H_0|\psi_{00}\rangle \\
= X_x^yZ_0^y|\psi_{00}\rangle \\
= S_{10}X_x^yZ_0^yS_{10}|\psi_{00}\rangle \\
= S_{10}X_x^yZ_0^y|\psi_{00}\rangle \\
= S_{10}S_{10}|\psi_{xy}\rangle.
\]

Hence,
\[
H_1H_0|\psi_{01}\rangle = S_{10}|\psi_{10}\rangle = |\psi_{10}\rangle \\
H_1H_0|\psi_{10}\rangle = S_{10}|\psi_{01}\rangle = |\psi_{01}\rangle \\
H_1H_0|\psi_{11}\rangle = S_{10}|\psi_{11}\rangle = -|\psi_{11}\rangle
\]
The matrix is
\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & -1
\end{pmatrix}
\]