06-22457 *Quantum Computing and Cryptography*
Spring Semester 2011
Steve Vickers

The University of Birmingham
School of Computer Science
19 January, 2011

Exercises 1
Cbits and vectors

1. Write as many notations as you can for the ket $|9\rangle_4$.

2. Calculate the matrices for the following operators.

   (a) The 2-Cbit operator $\mathsf{X}_1\mathsf{X}_0$ that flips both Cbits. (Note – don't confuse this with the swap operator.)

   (b) The 3-Cbit operator S_{21} that swaps the states of Cbits 2 and 1.

3. Design a 3-Cbit gate A_{210} that flips Cbit 0 if at least one of Cbits 1,2 has state $|1\rangle$. (It leaves Cbits 1 and 2 unchanged.)

   (a) Write down an expression for $\mathsf{A}_{210}|xyz\rangle$.

   (b) Show that it is reversible.

   (c) Write down its matrix.

   (d) Draw a circuit diagram to construct it using NOT gates and Toffoli gates. (Use as many of each as you need).

   (e) Show that that configuration of gates really does compute A_{210}.

   Hint: Think of the bits 0 and 1 as logical **false** and **true**. Then multiplication xy is logical "and", $x \wedge y$; addition $x \oplus y$ modulo 2 is "exclusive or"; $x \oplus 1$ is the same as complementation $\widetilde{x}$ and gives logical "not". If "inclusive or" is written $x \vee y$ then de Morgan's law says that $\widetilde{x \vee y} = \widetilde{x} \wedge \widetilde{y}$.

Solutions

1. $|9\rangle$, $|1001\rangle$, $|1\rangle|0\rangle|0\rangle|1\rangle$, $|1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle$ and

$$\begin{pmatrix} 0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0 \end{pmatrix}.$$

2. (a) $\mathsf{X}_1\mathsf{X}_0$ exchanges $|00\rangle = |0\rangle$ with $|11\rangle = |3\rangle$, and $|01\rangle = |1\rangle$ with $|10\rangle = |2\rangle$. Its matrix is

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

   (b) S_{21} exchanges $|2\rangle$ with $|4\rangle$ and $|3\rangle$ with $|5\rangle$ and fixes all the rest. Its matrix is

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

3. (a)

$$\mathsf{A}_{210}|xyz\rangle = |x\rangle|y\rangle|z \oplus (x \vee y)\rangle$$

(b) A_{210} is its own inverse.

$$\mathsf{A}_{210}\mathsf{A}_{210}|xyz\rangle = \mathsf{A}_{210}|x\rangle|y\rangle|z \oplus (x \vee y)\rangle = |x\rangle|y\rangle|z \oplus (x \vee y) \oplus (x \vee y)\rangle = |xyz\rangle$$

(c) A_{210} fixes (leaves unchanged) those states $|xyz\rangle$ in which $x = y = 0$. These two fixed states $|000\rangle = |0\rangle_3$ and $|001\rangle = |1\rangle_3$ correspond to 1s on the diagonal of the matrix. If either of x, y is 1 then it exchanges the two states $|xy0\rangle$ and $|xy1\rangle$: thus $|2\rangle \leftrightarrow |3\rangle$, $|4\rangle \leftrightarrow |5\rangle$ and $|6\rangle \leftrightarrow |7\rangle$. These exchanges correspond to six 1s off the diagonal. The matrix is

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

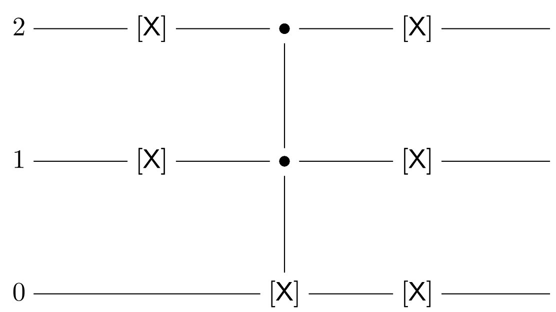
(d) Using de Morgan's law we can calculate

$$z \oplus (x \vee y) = z \oplus \widetilde{\tilde{x} \wedge \tilde{y}} = z \oplus (\tilde{x}\tilde{y} \oplus 1)$$

and so

$$\begin{aligned} \mathsf{A}_{210}|xyz\rangle &= |x\rangle|y\rangle|z \oplus (\tilde{x}\tilde{y}) \oplus 1\rangle \\ &= \mathsf{X}_0|x\rangle|y\rangle|z \oplus (\tilde{x}\tilde{y})\rangle \\ &= \mathsf{X}_2\mathsf{X}_1\mathsf{X}_0|\tilde{x}\rangle|\tilde{y}\rangle|z \oplus (\tilde{x}\tilde{y})\rangle \\ &= \mathsf{X}_2\mathsf{X}_1\mathsf{X}_0\mathsf{T}_{210}|\tilde{x}\rangle|\tilde{y}\rangle|z\rangle \\ &= \mathsf{X}_2\mathsf{X}_1\mathsf{X}_0\mathsf{T}_{210}\mathsf{X}_2\mathsf{X}_1|x\rangle|y\rangle|z\rangle. \end{aligned}$$

(Note that because X and T are reversible, so is A.)
Hence A_{210} can be implemented using the following circuit diagram. Remember that the operations $\mathsf{X}_2\mathsf{X}_1\mathsf{X}_0\mathsf{T}_{210}\mathsf{X}_2\mathsf{X}_1$ are applied from right to left, while the diagram is read from left to right.



(e) We have already shown this.