Interlude: Graphs and Graph States

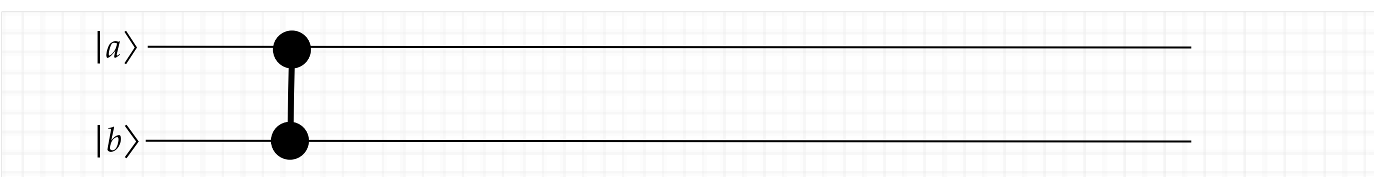
Related to the **CNOT** gate is the controlled version of the Z gate. Recall $\mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. The controlled version of any matrix A (in the standard basis) is the block matrix

$$\mathbf{C}A \;=\; \begin{array}{c|c|c} & 0u & 1u \\ \hline 0u & \mathbf{I} & 0 \\ \hline 1u & 0 & A \end{array},$$

where the hierarchical quantum indexing scheme is also shown. If the first qubit is 0 then the effect ios the identity, while if it is 1, then the effect on the remainder $|u\rangle$ is to apply A. So

$$\mathbf{CZ} \;=\; \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

Although the control is nominally on the first qubit, with **CZ** the effect on base states is to multiply the global state by -1 if and only if *both* qubits are 1. Hence it is really symmetric---the second qubit could equally be said to be controlling the first. The standard diagram for it is just two black dots connected by themselves:



Since a general vector $[u_1, u_2, u_3, u_4]^T$ becomes $[u_1, u_2, u_3, -u_4]^T$ after going through **CZ**, it follows, upon writing $|a\rangle = [a_1, a_2]^T$ and $|b\rangle = [b_1, b_2]^T$, that

$$\mathbf{CZ} \cdot \big(|a\rangle \otimes |b\rangle\big) \;=\; \mathbf{CZ} \cdot [a_1b_1, a_1b_2, a_2b_1, a_2b_2] \;=\; [a_1b_1, a_1b_2, a_2b_1, -a_2b_2]\ .$$

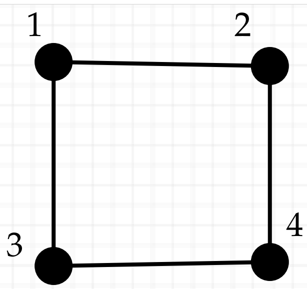
Is this ever entangled, and if so, when? Note that if $|a\rangle$ and $|b\rangle$ are both $|1\rangle$, then $\mathbf{CZ} \cdot \big(|a\rangle \otimes |b\rangle\big) \;=\; \mathbf{CZ}|11\rangle \;=\; \mathbf{CZ} \cdot [0,0,0,1]^T \;=\; [0,0,0,-1]$. To try to represent this as a tensor product $\begin{bmatrix} e \\ f \end{bmatrix} \otimes \begin{bmatrix} g \\ h \end{bmatrix} = [eg, eh, fg, fh]^T$, we need both e and g to be 0, so we are left with $fh = -1$. This is easy to solve with $f = 1$ and $h = -1$, or even $f = h = i$ since we can use complex numbers. But now let $|a\rangle$ and $|b\rangle$ both be $|+\rangle$. Then we get

$$\mathbf{CZ}|{+}{+}\rangle = \mathbf{CZ}\cdot\tfrac{1}{2}[1,1,1,1]^T = \tfrac{1}{2}[1,1,1,-1]^T .$$

For determining entanglement we can ignore the $\frac{1}{2}$ factor. So the equations become $eg = 1$, $eh = 1$, $fg = 1$, and $fh = -1$. The first three combine to give $g = \frac{1}{e} = h$, so $fg = fh = 1$, but that contradicts the fourth equation $fh = -1$. Thus $\mathbf{CZ}|{+}{+}\rangle$ is entangled. It follows that

It is possible for a quantum gate to leave one separable state separable while making another separable state become entangled.

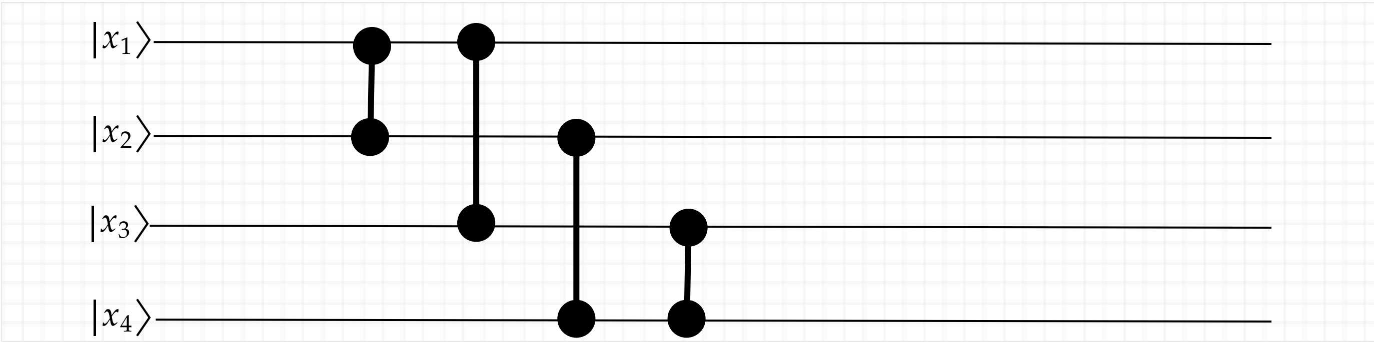
Now CZ gates are especially neat because they look like edges in a **graph** $G = (V, E)$, specifically an **undirected** graph because the gates are symmetric. Let's first see some examples of graphs. The *cycle graphs* C_k have k **vertices** (also called **nodes**) and k edges connecting them in a ring, for $k \geq 3$. The four-cycle graph has the following picture and **adjacency matrix**:



$$A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad A' = \tfrac{1}{2}A \qquad A'' = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{bmatrix}$$

Note: This differs from the text only in the labels 3 and 4. This makes it maybe easier to see that not only is A not unitary, it isn't even invertible: rows 2 and 3, and rows 1 and 4, are identical. But:

- A is a real symmetric matrix, so it is Hermitian.
- A' is a matrix of nonnegative entries each of whose rows and columns sums to 1, which makes it **doubly stochastic**. This is an analogue of "unitary" for classical probability.
- In fact, for any **regular** graph, meaning that all vertices have the same **degree** d, dividing the adjacency matrix by d always gives a doubly-stochastic matrix.
- We can in fact make a unitary matrix A'' by flipping the sign of the two 1s at lower right and dividing by $\sqrt{2}$ rather than by 2. This is, however, more of a coincidence than a general feature. The text shows that in the case of the regular *prism graph* ($n = 6$, $d = 3$), there is no sensible way to make it into a unitary matrix.
- The general way to encode graphs into quantum circuits via the $\mathbf{CZ}$ gate yield much bigger underlying matrices---and some surprises. Here we go:



When put on four qubits, the first gate gives the matrix $\mathbf{CZ} \otimes \mathbf{I} \otimes \mathbf{I}$, which we know how to build: replace every entry of the CZ matrix by the 4×4 identity matrix, to get the 16×16 matrix

$$\left|\begin{array}{c} 0000 \\ 0001 \\ 0010 \\ 0011 \\ 0100 \\ 0101 \\ 0110 \\ 0111 \\ 1000 \\ 1001 \\ 1010 \\ 1011 \\ 1100 \\ 1101 \\ 1110 \\ 1111 \end{array}\right| : \quad \mathbf{CZ} \otimes \mathbf{I} \otimes \mathbf{I} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix} = diag\left(\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ -1 \\ -1 \\ -1 \\ -1 \end{bmatrix}\right)$$

At far left I've put the labels of the underlying coordinates by the sixteen basis strings of length 4. The point is that the -1 entries go in all the places where the first two bits of the string are 1 as shown in pink. This is because the first CZ gate is on the first two bits. Next, for the gate on qubits 1 and 3, we follow the same rule but for the coordinates where the first and third bit are 1:

$$\left|\begin{matrix}0000\\0001\\0010\\0011\\0100\\0101\\0110\\0111\\1000\\1001\\1010\\1011\\1100\\1101\\1110\\1111\end{matrix}\right| : \quad diag\left(\begin{bmatrix}1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\-1\\-1\\1\\1\\-1\\-1\end{bmatrix}\right).$$

Here is the product of all four gate matrices that we get. I've "properly" put the matrix for the first gate on the right now, but actually this doesn't matter---they are all diagonal matrices so they commute with each other. To multiply them, we can just multiply the entries in each of the sixteen rows. The blue 1s show cases where an even number of -1 entries multiplied to give $+1$:

$$\left|\begin{matrix}0000\\0001\\0010\\0011\\0100\\0101\\0110\\0111\\1000\\1001\\1010\\1011\\1100\\1101\\1110\\1111\end{matrix}\right| : \quad diag\left(\begin{bmatrix}1\\1\\1\\-1\\1\\1\\1\\-1\\1\\1\\1\\-1\\1\\1\\1\\-1\end{bmatrix}\right) \cdot diag\left(\begin{bmatrix}1\\1\\1\\1\\1\\-1\\1\\-1\\1\\1\\1\\1\\1\\-1\\1\\-1\end{bmatrix}\right) \; diag\left(\begin{bmatrix}1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\-1\\-1\\1\\1\\-1\\-1\end{bmatrix}\right) \cdot diag\left(\begin{bmatrix}1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\-1\\-1\\-1\\-1\end{bmatrix}\right) = diag\left(\begin{bmatrix}1\\1\\1\\-1\\1\\-1\\1\\1\\1\\1\\-1\\1\\-1\\1\\1\\1\end{bmatrix}\right).$$

A word to the wise: The matrix for the fourth gate, which comes leftmost just above, is the tensor product $(\mathbf{I} \otimes \mathbf{I}) \times \mathbf{CZ}$. The matrices for the middle two gates, however, are technically not tensor products, because one identity comes "between the two arms" of the $\mathbf{CZ}$ gate. They are "morally" tensor products, though. The assigned exercise 4.11 makes a different case of this point. The rule about places with two particular 1s, however, applies in all cases. And the surviving -1 entries in the product at right mark four of the strings that gave exactly two 1s, the four corresponding to the edge set $E = \{(1,2),(1,3),(2,4),(3,4)\}$ of the graph.

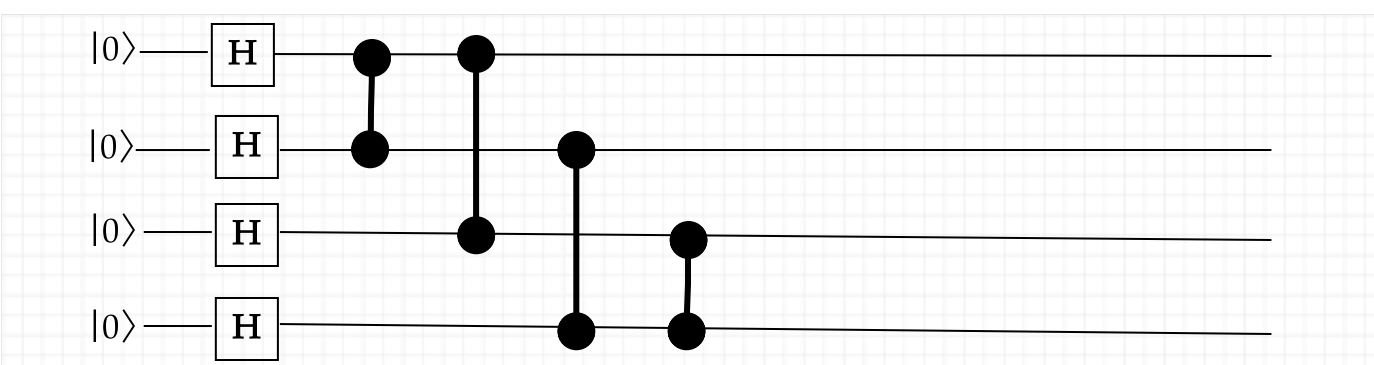
If we apply our diagonal matrix to the all-1 unit vector, here $[1,1,1,1]\frac{1}{2} = |{+}{+}\rangle$, then we get the column vector of the diagonal entries at right (again, divided by 2 to normalize it). Does that column vector faithfully preserve all information about the given graph? A question to ponder...

General Quantum Circuits and Computations

If there are n qubits, then the underlying matrices we get are $N \times N$ with $N = 2^n$. It is much harder to handle 2^n-sized stuff than n-sized stuff. Happily, we can always break the basic gates down to constant size---3 at most with the Toffoli gate in practice---and there are theorems that guarantee constant size gates working in general. One important case of using n single-qubit gates is the **Hadamard transform** $\mathbf{H} \otimes \mathbf{H} \otimes \cdots \otimes \mathbf{H}$ (n times), which can be abbreviated $\mathbf{H}^{\otimes n}$:

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \quad H^{\otimes 3} = \frac{1}{2\sqrt{2}}\left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right]$$

We always have $H^{\otimes n}|0^n\rangle = |+\rangle^{\otimes n} = |+^n\rangle =$ the all-1 vector of length $N = 2^n$ divided by $\sqrt{N} = \sqrt{2^n} = 2^{n/2}$. Often this is the first step of a quantum circuit, for example:



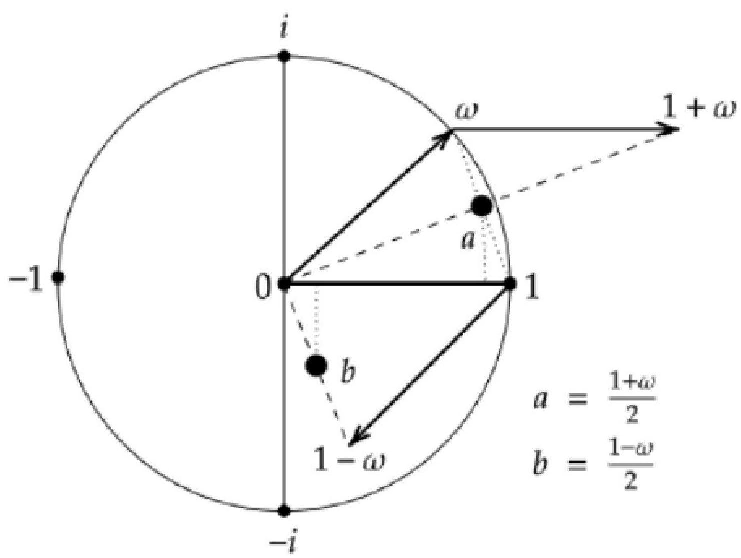
Putting the same Hadamard transform also at the end creates what is called a **graph state circuit**; we will analyze them later.

We will call an $N \times N$ matrix that arises from a single small gate---or a tensor product of small gates---a **succinct** matrix. Thus a **quantum computation** of **length** s is formally a composition of s succinct matrices applied to some input vector. The text draws allusion to a classical computation on a binary string x of length n, such as $x = 10100010$, say. The quantum circuit starts with input the basis state $|x\rangle = |10100010\rangle$. We could actually start with $|0^8\rangle$ but then **prepare** the state $|x\rangle$ by making the first column of the circuit be the tensor product

$$\mathbf{X} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{I} \text{ ,}$$

which has a NOT gate where x has a 1. This is why we often suppose ("without loss of generality") that the circuit starts with the all-zero basis vector.

The $\mathbf{Z}$ and $\mathbf{CZ}$ gates are the heads of an important family of basic gates having to do with rotations of **phase**, which is a curious but definitely physical property. When a complex number $x + iy$ is rewritten in polar form as $re^{i\theta}$, the angle θ is the phase. The magnitude is r, so when $r = 1$ we have a unit complex number. Note that i itself is the same as $e^{i\pi/2}$ since $\frac{\pi}{2}$ means 90° phase. Then $i^2 = e^{i\pi} = -1$ and if we put $\omega = e^{i\pi/4}$ then $\omega^2 = i$. In Cartesian coordinates, $\omega = \frac{1+i}{\sqrt{2}}$. Here is some more geometry:



The vector $\mathbf{u} = [a, b]^T$ is a funky unit vector. To see that it is a unit vector, note that

$$||\mathbf{u}||^2 = \langle \mathbf{u}, \mathbf{u} \rangle = \mathbf{u}^* \mathbf{u} = a^* a + b^* b = \left(\frac{1+\overline{\omega}}{2}\right)\left(\frac{1+\omega}{2}\right) + \left(\frac{1-\overline{\omega}}{2}\right)\left(\frac{1-\omega}{2}\right).$$

In polar form, the complex conjugate of $e^{i\theta}$ is always $e^{-i\theta} = e^{i(2\pi-\theta)}$, so $\overline{\omega} = e^{i7\pi/4} = \omega^7$. In Cartesian coordinates,

$$\frac{1+\omega}{2} = \frac{1}{2}\left(1+\frac{1+i}{\sqrt{2}}\right) = \frac{\sqrt{2}+1+i}{2\sqrt{2}} \quad \text{and} \quad \frac{1-\omega}{2} = \frac{1}{2}\left(1-\frac{1+i}{\sqrt{2}}\right) = \frac{\sqrt{2}-1-i}{2\sqrt{2}}$$

So

$$\frac{1+\overline{\omega}}{2} = \frac{1}{2}\left(1+\frac{1-i}{\sqrt{2}}\right) = \frac{\sqrt{2}+1-i}{2\sqrt{2}} \quad \text{and} \quad \frac{1-\overline{\omega}}{2} = \frac{1}{2}\left(1-\frac{1-i}{\sqrt{2}}\right) = \frac{\sqrt{2}-1+i}{2\sqrt{2}}.$$

Then

$$\left(\frac{1+\overline{\omega}}{2}\right)\left(\frac{1+\omega}{2}\right) = \frac{1}{8}\left(\sqrt{2}+1+i\right)\left(\sqrt{2}+1-i\right) = \frac{1}{8}\left[\left(\sqrt{2}+1\right)^2+1\right] = \frac{1}{8}\left(2+1+2\sqrt{2}+1\right) = \frac{2+\sqrt{2}}{4}$$

and

$$\left(\frac{1-\overline{\omega}}{2}\right)\left(\frac{1-\omega}{2}\right) = \frac{1}{8}\left(\sqrt{2}-1-i\right)\left(\sqrt{2}-1+i\right) = \frac{1}{8}\left[\left(\sqrt{2}-1\right)^2+1\right] = \frac{1}{8}\left(2+1-2\sqrt{2}+1\right) = \frac{2-\sqrt{2}}{4}\ .$$

These squared values add to 1 as promised, so $\mathbf{u} = [a, b]^T$ is a unit vector. How do we get it? Here is the start of an infinite family of gates:

$$\mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ \mathbf{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},\ \mathbf{T} = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix},\ \mathbf{T}_{\pi/8} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}.$$

The controlled versions to go with $\mathbf{CZ}$ are $\mathbf{CS}$, $\mathbf{CT}$, etc. They, too, are symmetric---indeed, all of these gates are controlled phase shifts conditioned on the basis-state 1 of all of the (one or two) qubits involved. (Here I must note global inconsistency and confusion in notation, especially about rotations, which we will try to resolve when we cover the **Bloch Sphere** next week.)

Now we have all the background we need to read **quantum circuits**. Lecture will go on to illustrate them, both out of section 4.5 and (the same examples) on QC web applets.