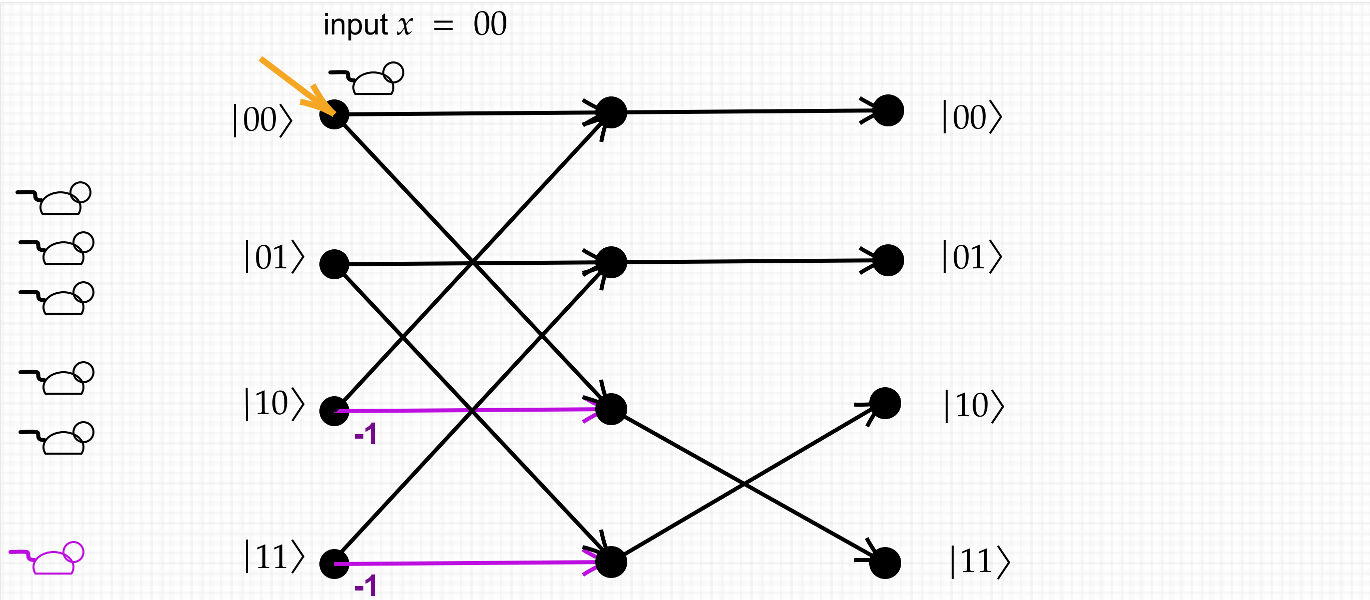
CSE491/596 Lecture Fri. 12/01/23: Working Out Circuits and Measurements

There are basically three ways to "reckon" a quantum circuit computation:

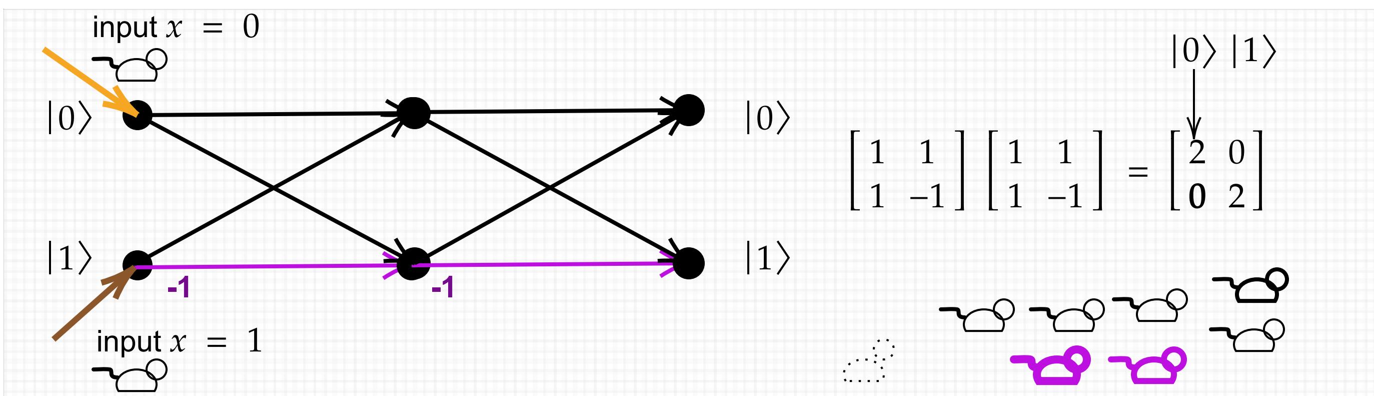
1. Multiply the $Q \times Q$ matrices together---using *sparse-matrix techniques* as far as possible. If BQP $\neq$ P and you try this on a problem in the difference then the sparse-matrix techniques must blow up at some (early) point. The downside is that the exponential blowup is paid early; the upside is that once you pay it, the matrix multiplications don't get any worse, no matter how more complex the gates become. This is often called a "Schrödinger-style" simulation.
2. Any product of s-many $Q \times Q$ matrices can be written as a single big sum of s-fold products. For instance, if A, B, C, D are four such matrices and u is a length-Q vector, then
$$ABCDu\,[i] \;=\; \sum_{j,k,l,m=1}^{Q} A[i,j]\cdot B[j,k]\cdot C[k,l]\cdot D[l,m]\cdot u[m].$$
Every (*nonzero*) product of this form can be called a (*legal*) **path** through the system. [As hinted before, in a quantum circuit, u will be at left---on an input x, it will be the basis vector $\mathbf{e}_{x0^{r+m}} = |x0^{r+m}\rangle$ under the convention that 0s are used to initialize the output and ancilla lines---and D will be the first matrix from gate(s) in the circuit as you read left-to-right. Thus the output will come out of A, which is why it is best to visualize the path as coming in from the top of the column vector u, going out at some row m (where u_m is nonzero---for a standard basis vector, there is only one such m), then coming in at column m of D, choosing some row l to exit (where the entry $D[l,m]$ is nonzero), then coming in at column l of C, and so on until exiting at the designated row i of A. This is the discrete form of Richard Feynman's **sum-over-paths** formalism which he originally used to represent integrals over quantum fields (often with respect to infinite-dimensional Hilbert spaces). The upside is that each individual path has size $O(s)$ which is linear not exponential in the circuit size. The downside is that the number of nonzero terms in the sum can be far worse than Q and doubles each time a Hadamard gate (or other nondeterministic gate) is added to the circuit.
3. Find a way to formulate the matrix product so that the answer comes out of symbolic linear algebra---if possible!

For the textbook, I devised a way to combine the *downsides* of 1 and 2 by making an exponential-sized "maze diagram" up-front but evaluating it Feynman-style. Well, the book only uses it for $1 \leq Q \leq 3$ and I found that the brilliant Dorit Aharonov had the same idea. All the basic gate matrices have the property that all nonzero entries have the same magnitude---and when normalizing factors like $\frac{1}{\sqrt{2}}$ are collected and set aside, the Hadamard, **CNOT**, Toffoli, and Pauli gates (ignoring the global i factor in $\mathbf{Y}$) give just entries $+1$ or -1, which become the only possible values of any path. That makes it easier to sum the results of paths in a way that highlights the properties of **amplification** and **interference** in the "wave" view of what's going on. The index values $m, l, k, j, i, \ldots$ become "locations" in the wavefront as it flows for time s, and since it is discrete, the text pictures packs of...well...spectral lab mice running through the maze.

One nice thing is that you can read the mazes left-to-right, same as the circuits. Here is the $\mathbf{H} + \mathbf{CNOT}$ entangling circuit example:



No interference or amplification is involved here---the point is that if you enter at $|00\rangle$, then $|00\rangle$ and $|11\rangle$ are the only places you can come out---and they have equal weight. To see interference, you can string the "maze gadgets" for two Hadamard gates together:



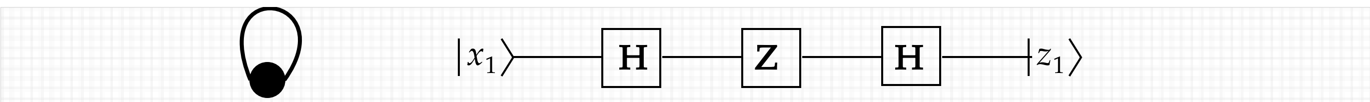
In linear-algebra terms, all that happened at lower right was $1 \cdot 1 + -1 \cdot 1$ giving 0. But the wave interference being described that way is a real physical phenomenon. Even more, according to Deutsch the two serial Hadamard gates branch into 4 universes, each with its own "Phil the mouse" (which can be a photon after going through a beam-splitter). One of those universes has "Anti-Phil", who attacks a "Phil" that tries to occupy the same location (coming from a different universe) and they fight to mutual annihilation. (I am skeptical about the reality of such "branches of the multiverse" because this way of viewing things seems to entail exponential collective effort by those universes. They seem to do our bidding in our one universe too complicitly.)

Visualizing Small Quantum Systems

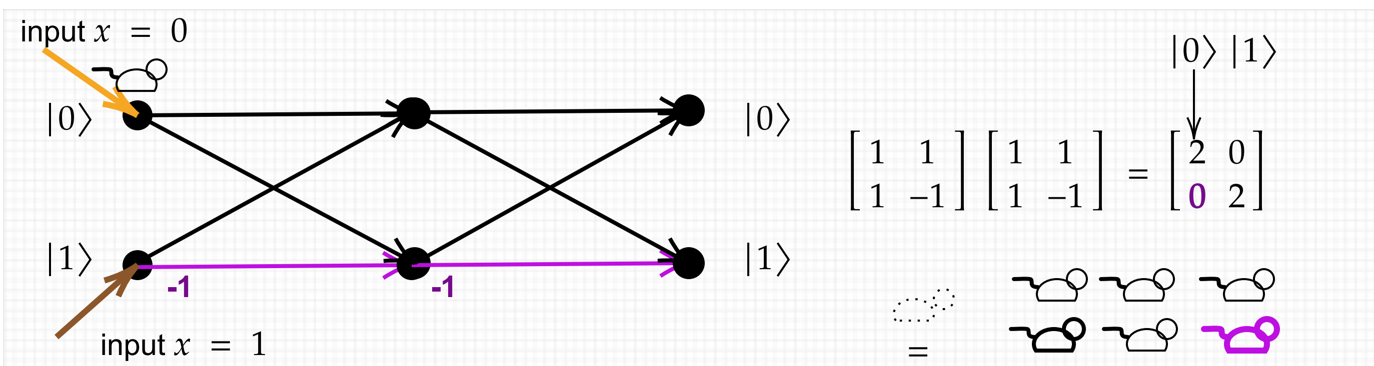
Can we build any interesting things with just a few qubits? Yes, in fact. We have already modeled graphs that way. To state this formally:

Definition: A **graph state circuit** on n qubits consists of an n-qubit Hadamard transform (i.e., $\mathbf{H}^{\otimes n}$), then some number of $\mathbf{Z}$ and $\mathbf{CZ}$ gates, then a final $\mathbf{H}^{\otimes n}$.

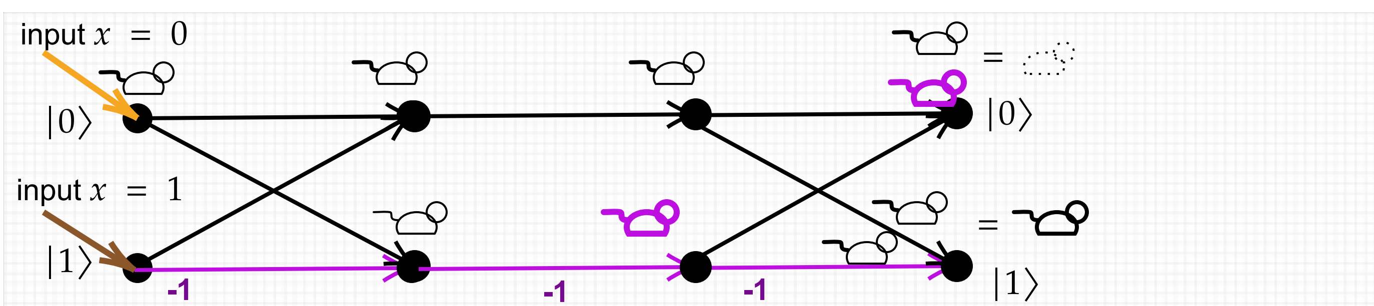
Each qubit is a node. A $\mathbf{CZ}$-gate connecting qubits i and j gives an undirected edge between nodes i and j. A $\mathbf{Z}$-gate on line i denotes a self-loop at node i. The simplest nonempty graph has just one node with a self-loop:



We have seen the equation $\mathbf{HZH} = \mathbf{X}$. How is this reflected when we visualize the quantum properties? There is onlyone change from the "maze" for two $\mathbf{H}$-gates canceling, which was:



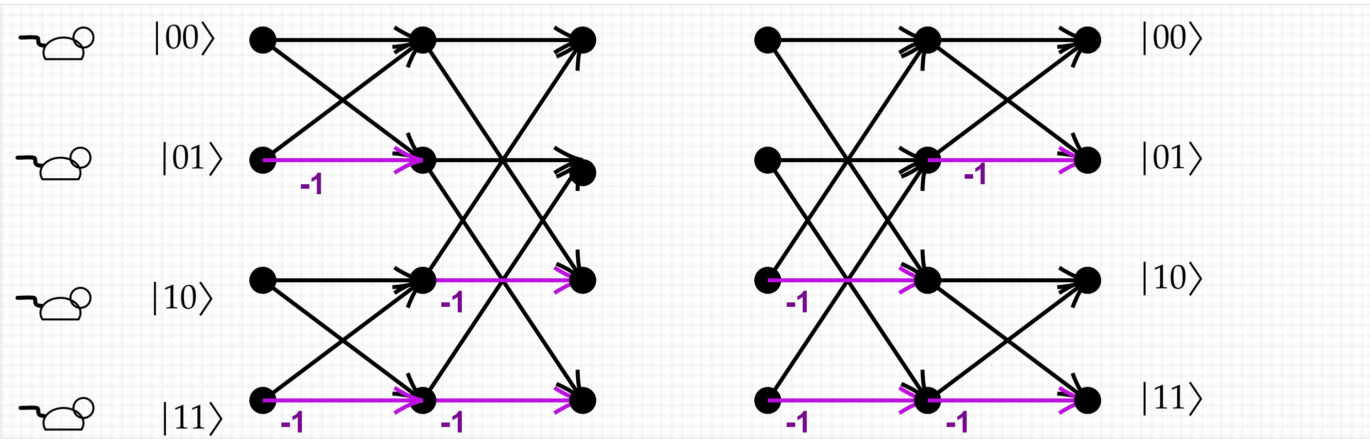
The change is to insert a stage that again has a -1 on the $|1\rangle$ basis value but no "crossover":



This time, when "Phil" starts running from $|0\rangle$ at left, the "mice" cancel at $z = |0\rangle$ and amplify at $z = |1\rangle$. And on input $x = |1\rangle$ they output the basis state $|0\rangle$. The result is Boolean NOT, i.e., $\mathbf{X}$.

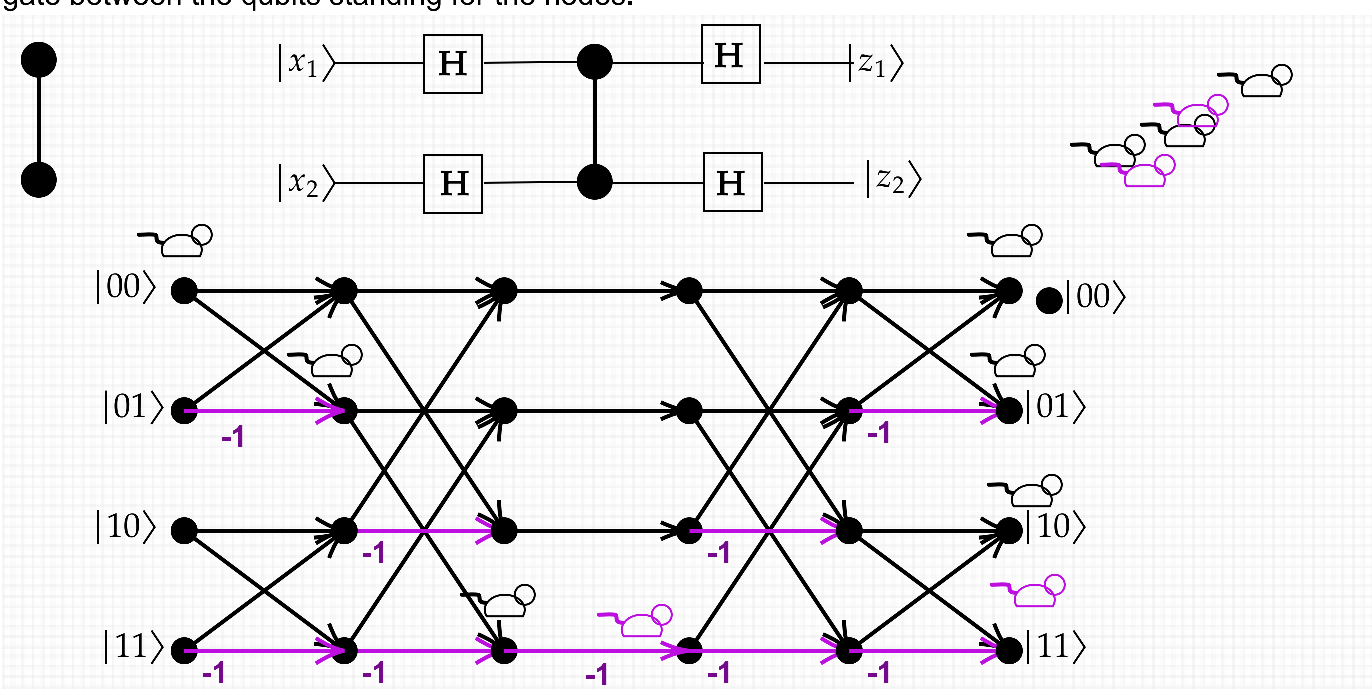
[Footnotes: A basic outcome $|z\rangle$ for the circuit C on input x has amplitude $\langle z|U_C|x\rangle$, not $\langle x|U_C|z\rangle$. Perhaps the diagrams should write the bra-form, $\langle 0|$ and $\langle 1|$ and so on, for z at right to emphasize this. The diagrams that follow show the "mice" in final positions---they will be reset in lecture.]

For graph state circuits of 2 nodes we need 2 qubits. The Hadamard transform of two qubits is diagrammed as at left and right. It does not matter what order the two $\mathbf{H}$ gates go in.



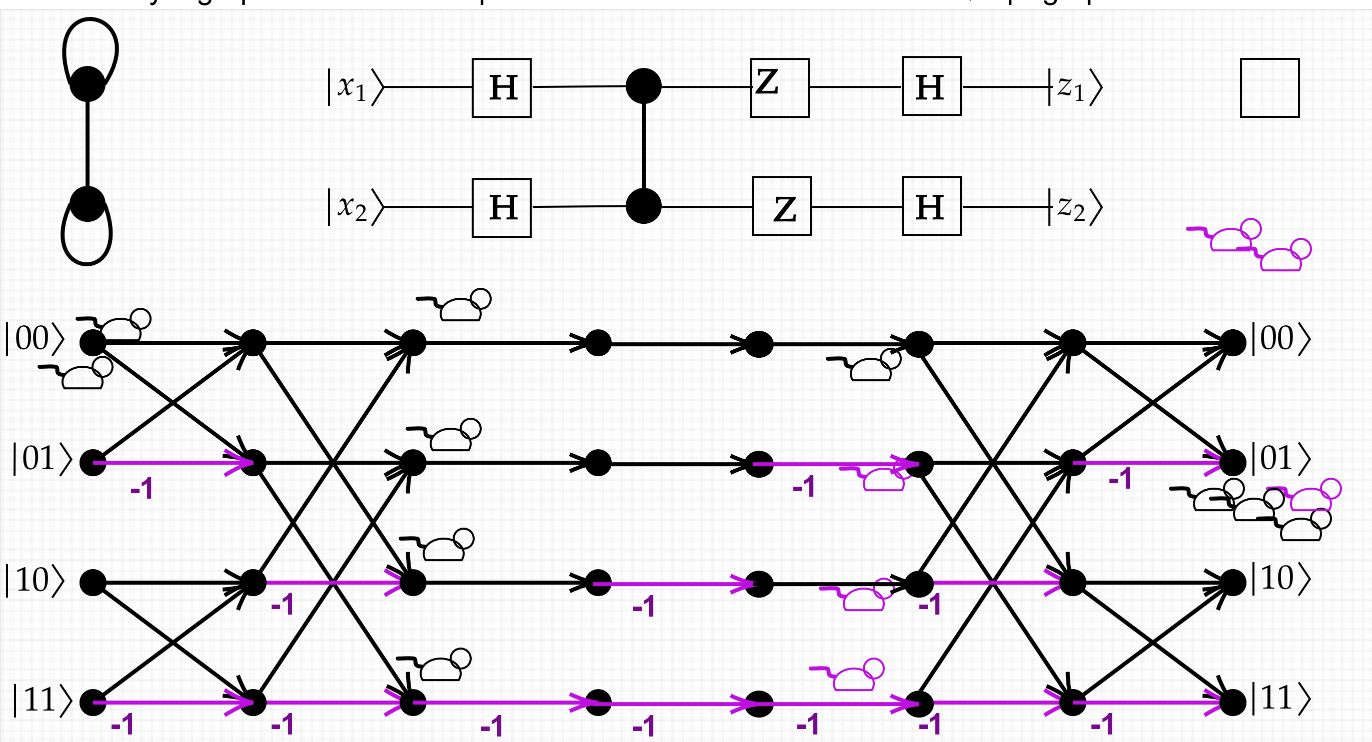
Note that the mouse running from $|00\rangle$ encounters no phase change, nor mice ending at $|00\rangle$ regardless of origin. This simply expresses that the Hadamard transform (and the QFT too) have every entry $+1$ (divided by the normalizing constant $R = \sqrt{2^n}$) in the row and column for $|00\rangle$. We will focus on the amplitude of getting $|00\rangle$ as output given $|00\rangle$ as input. If G is the graph, C_G the graph-state circuit, and U_G the unitary operator it computes, then the amplitude we want is $\langle 00|U_G|00\rangle$.

The simplest two-node G has a single edge connecting the two nodes. This introduces a single $\mathbf{CZ}$ gate between the qubits standing for the nodes.



If we take the two Hadamard gates away from line 1, then we have $\mathbf{H}\,2\,\mathbf{CZ}\,1\,2\,\mathbf{H}\,2$, which is equivalent to $\mathbf{CNOT}$. But with them, we get equal superpositions once again. Most in particular, the amplitude of $\langle 00|U_G|11\rangle$ (= $\langle 11|U_G|00\rangle$) is nonzero. [The lecture also noted how $\frac{1}{2}[1,1,1,-1]^T$ is a fixed point of $\mathbf{H}^{\otimes 2}$ and found some other fixed points of parts of the circuit, including one that was equal up to multiplication by the unit scalar -1.]

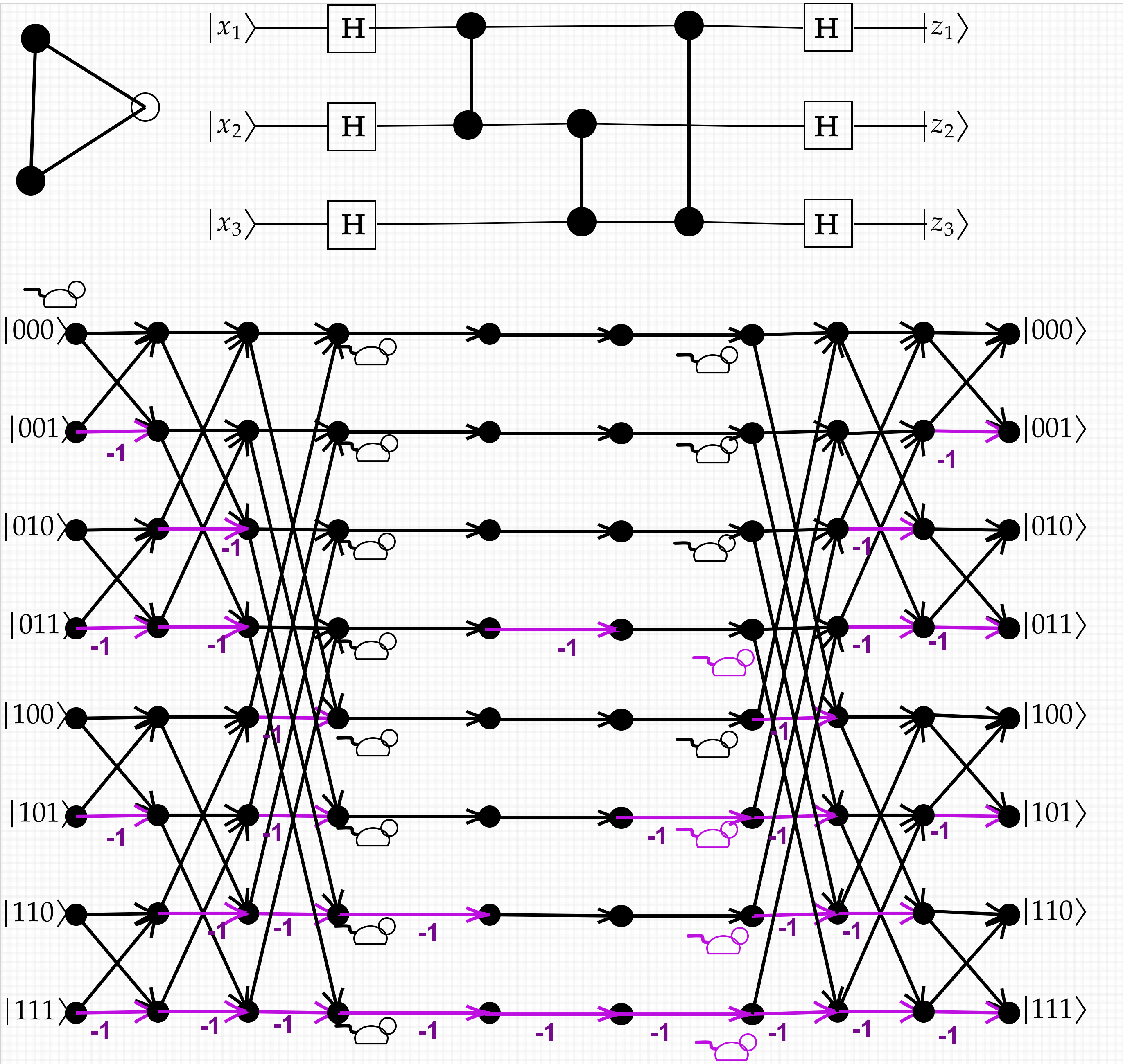
Now let's try a graph that adds a loop at each node. We can call it the "Q-Tip" graph:



The -1 phase shifts for the $\mathbf{Z}$ gates go on the basis states that have a 1 on line 1 or 2, respectively. Now the amplitude value $\langle 00|U_G|00\rangle$ is negative. Its sign does not affect the probability and the state still gives an equal superposition.

It does not matter whether we put the $\mathbf{Z}$ gates "before" or "after" the $\mathbf{CZ}$. The diagonal matrices all commute, and this is clear from how the paths go straight across without branching. We could simply make the whole graph into one diagonal gate with phase shifts that multiply the -1 factors along each row. A related thing to note is that if we repeat an edge or loop, then the two cancel completely. It's as if we have a graph with edges defined by even-odd parity rather than number.

Now let's try a three-node graph, the triangle:



For computing the amplitude $\langle 000 | U_G | 000 \rangle$ it is not necessary to follow the "mice" through the Hadamard parts of the "maze". The mice entering the graph part from $x = |000\rangle$ are all positive, and the mice going to $z = |000\rangle$ will not change color once they leave the graph. So we need only track the middle portion and count how many mice are $+$ and how many are $-$. For the triangle graph, the answer is: four of each. They **cancel**. So $\langle 000 | U_G | 000 \rangle = 0$.