Quantum Computation 101 for Physicists

Class exercise 6

1 Grover with k correct answers

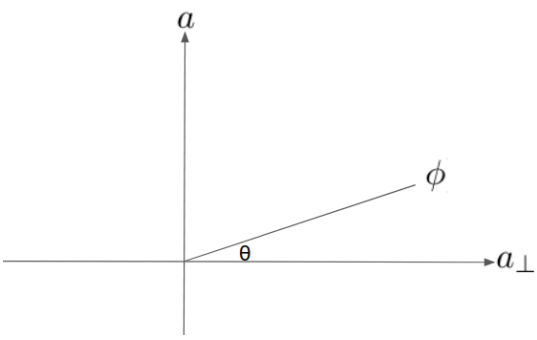
Assume we have a function f such that $f(x) = 1$ for exactly k special values of x, and $f(x) = 0$ otherwise.

1. Generalize Grover's algorithm for $k \ll N$. How does the number of necessary iterations change?
2. What happens if we perform j iterations more than the optimal number?

1.1 Solution

1. Recall the two component's used for Grover's iteration: The first one is V or the phase kickback, $V|x\rangle = \begin{cases} |x\rangle & f(x) = 0, \\ -|x\rangle & f(x) = 1. \end{cases} = (\mathbb{I} - 2\sum_{i=1}^{k} |x_i\rangle\langle x_i|)|x\rangle$ where the x_is are the special xs. In class this set contained only one value, but this generalization is natural for the case of k answers. The second component, $W = 2|\phi\rangle\langle\phi| - 1$ where $|\phi\rangle = \frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} |i\rangle$, does not need any special alterations for the case of multiple answers.

   We now define the sub-space parallel to $|a\rangle, |\phi\rangle$ we saw in class. We define $|a\rangle = \frac{1}{\sqrt{k}} \sum_{i=1}^{k} |x_k\rangle$ and $|a_\perp\rangle = \frac{1}{\sqrt{1-k/2^n}}(|\phi\rangle - \langle a|\phi\rangle|a\rangle)$. We start from the state $|\phi\rangle$, which is in an angle $\theta = \arcsin(\sqrt{\frac{k}{N}})$ from $a_\perp$ as in the drawing below.

   From here, the rest of the algorithm goes the same way: Applying V reflects the state around the $a_\perp$ and applying W reflects the state around $|\phi\rangle$, so applying WV rotates the state by 2θ. Since k is still very small, we can approximate $\theta \approx \sqrt{\frac{k}{N}}$, and after $\frac{\pi}{4}/\theta = O(\sqrt{N/k})$ iterations, we are as close as possible to $|a\rangle$.

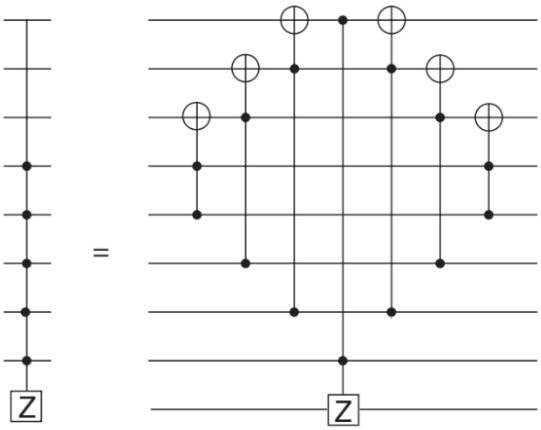
2. If we perform more iterations than we should, we keep rotating away from the state $|a\rangle$. If we perform j additional rotations the space will be rotated approximately $2j\sqrt{k}/\sqrt{N}$ from $|a\rangle$. If j is smaller than half the necessary iterations, the probability to measure $|a\rangle$ is still larger than $1/2$.

2 Implementing the W gate

In class we saw the implementation for the W gate:

$$-W = H^{\otimes n} X^{\otimes n} c^{n-1} Z X^{\otimes n} H^{\otimes n},$$

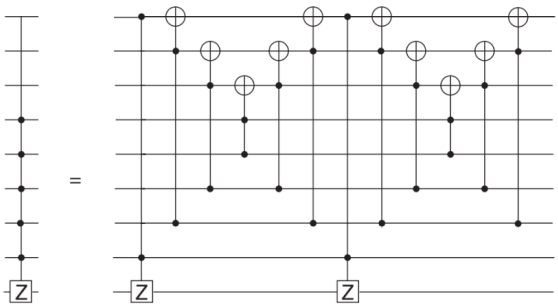
which requires a $c^{n-1}Z$ gate. We also saw how to implement such a gate with $n-3$ qubits initiated at $|0\rangle$:



We see that if at least one of the control qubits is in the zero states, the top ancilla qubit will also be in the zero state and the Z gate will not be applied.

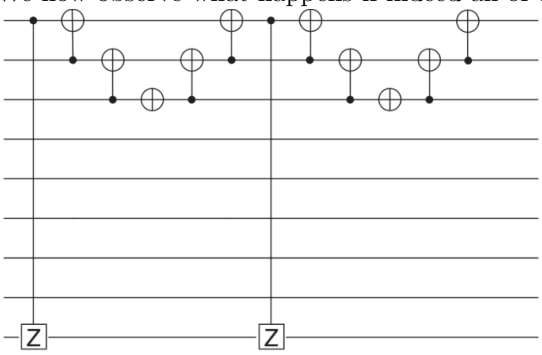
this is a bit waistful - it requires almost n ancillary qubits, but more importantly, it requires that they are 'cleaned' after every iteration, which is hard work. We now see how to implement the $c^{n-1}Z$ gate with only one ancilla qubit and a polynomial number of Toffoli gates.

We start by looking at the following circuit, and being persuaded that it implements the $c^{n-1}Z$ gate regardless of the initial state of the ancilla:



We see that if at least one of the control qubits is 0, then its Toffoli gate would not act, and two Toffoli identical gates act as the identity, the entire gate collapses into the identity as well. At the end we added the important uncompute gates.

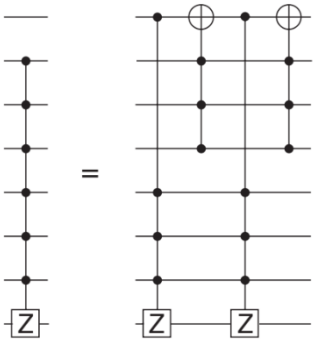
We now observe what happens if indeed all of the control qubits are in the one state:



and we note that

$$\mathrm{CNOT}_{ij} X_i \mathrm{CNOT}_{ij} = X_i X_j.$$

So in fact, we don't need all of the ancillary qubits, we only need one:



Here we use $c^{n-3}Z$, $c^{n-4}X$ gates. But we just showed above that the ancila qubits may be in an arbitrary state, so when implementing such a gate, we can just use the rest of the control qubits as our ancilla.