Quantum Computing - Grover's Algorithm

Programming Quantum Computers:
A Primer with IBM Q and D-Wave Exercises

Patrick Dreher
NC State University

Chief Scientist - NCSU IBM Q Hub

Demo of the Grover Algorithm Using the Quirk Simulator

Grover Algorithm

- Classically, searching an unsorted database requires a linear search that is of *O(N)* in time.
- Grover's quantum search algorithm finds the unique input to a black box function that produces a particular output value, with only $\bigcirc(N^{1/2})$ evaluations of the function with high probability
- It is the fastest possible quantum algorithm for searching an unsorted database and provides a quadratic speedup
- Reference:
  - Quantum Algorithm Implementation for Beginners https://arxiv.org/pdf/1804.03719

Grover Algorithm

- Find a unique item in an unstructured search among N items
- Classically worst case requires check of N boxes
- In quantum computer
  - Prepare of superposition of initial states that are

$$|+>=\frac{|0>+|1>}{\sqrt{2}} \qquad |->=\frac{|0>-|1>}{\sqrt{2}}$$

  - Oracle on |-> reverses the amplitude of that state

$$O|x^*>\frac{|f(x^*)\oplus|0>-|f(x^*)\oplus 1>-|f(x^*)\oplus 1>}{\sqrt{2}}=|x^*>\frac{|1>-|0>}{\sqrt{2}}=-|x^*>\frac{|0>-|1>}{\sqrt{2}}$$

Grover Algorithm

- Define Grover operator G and initial uniform superposition of states $|\Psi>$ and $G = [2|\Psi><\Psi| - I]$ ◎
- The amplitude of each state is flipped about the mean

$$G = [2|\Psi><\Psi| - I] \sum_i a_i |i> = \sum_i [2 < a > - a_i]|i>$$

- Applying $G = [2|\Psi><\Psi| - I]$ makes |x*> have amplitude above the mean while all other states have an amplitude below the mean

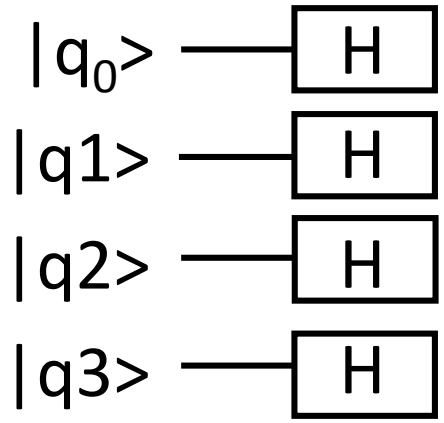
Implementation of the Algorithm

1. Use the Quirk simulator (https://algassert.com/quirk)
2. Initialization
   - Initialize the qubits in a superposition with $N^{-1/2}$ normalization (.25 for N=4)
3. Oracle
   - Implement the Oracle function
4. Amplification
   - Phase flip the amplitude about the average amplitude
   - Inverting the target state amplitude while keeping all other amplitudes unchanged causes the target amplitude to increase while all other states decrease
5. Measurement
   - Perform a readout of the final qubit states

Initialization of 4 Qubit System

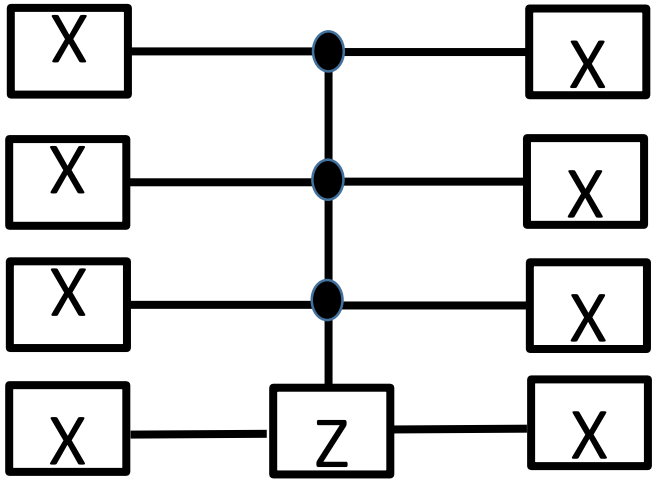
- Quantum computing platforms are normally initialized as $|\mathbf{0}\rangle = \begin{pmatrix} \mathbf{1} \\ \mathbf{0} \end{pmatrix}$

- The procedure is to apply Hadamard gates to each qubit

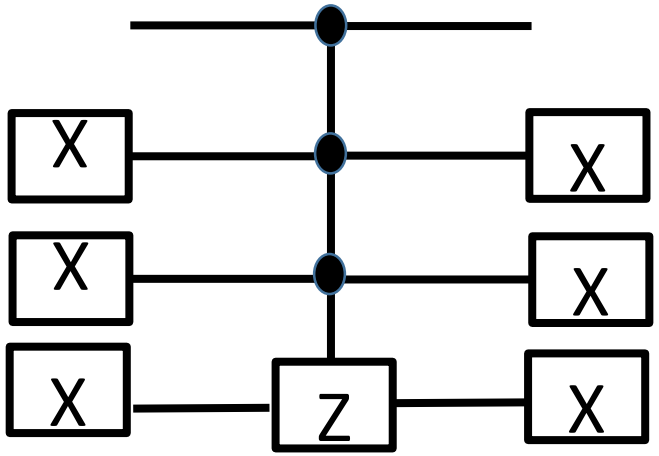


Possible Oracle Configurations with 4 Qubits

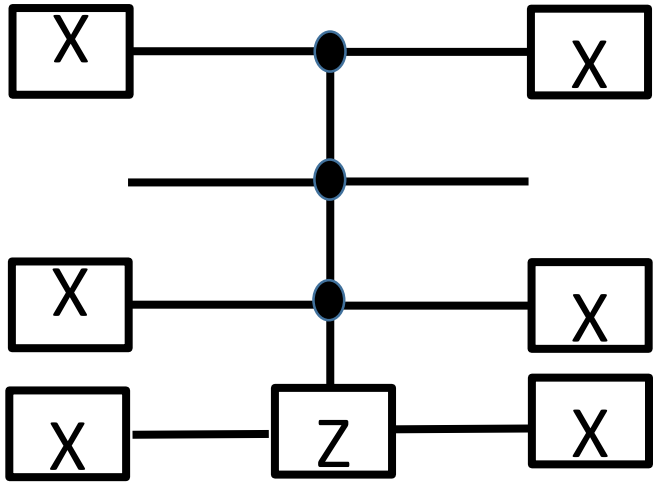
- With 4 qubits there are 16 possible oracle configurations
- States are initialized on QC platforms in the $|\mathbf{0}\rangle = \begin{pmatrix}\mathbf{1}\\\mathbf{0}\end{pmatrix}$ state
- Recall that the Z gate has the matrix representation $\begin{pmatrix}\mathbf{1} & \mathbf{0}\\\mathbf{0} & \mathbf{-1}\end{pmatrix}$
- Recall that the T gate has the matrix representation $\begin{pmatrix}\mathbf{1} & \mathbf{0}\\\mathbf{0} & \boldsymbol{e^{i\frac{\pi}{4}}}\end{pmatrix}$



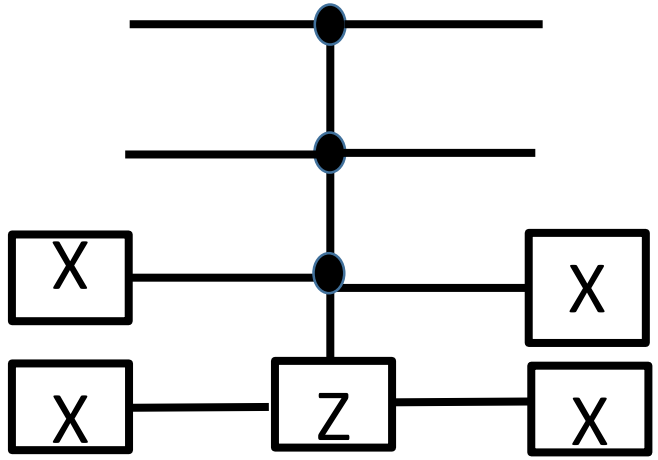
0000



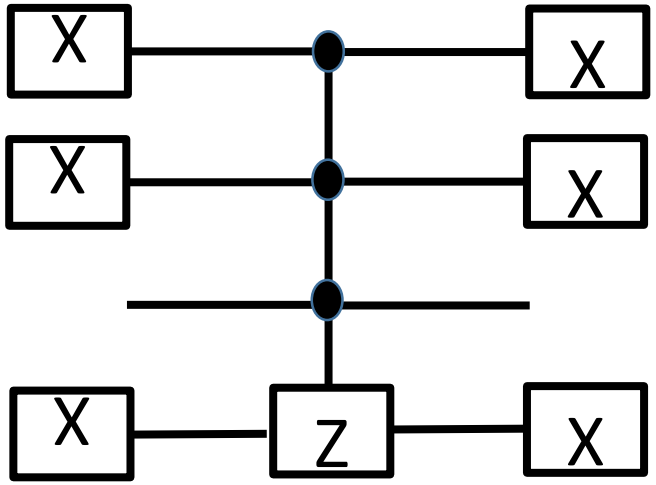
0001



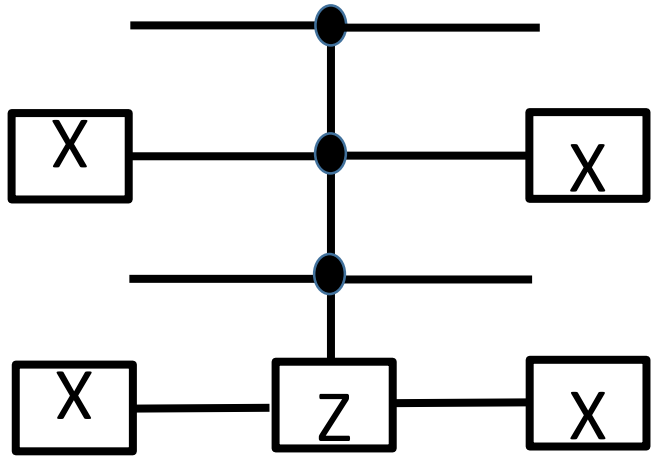
0010



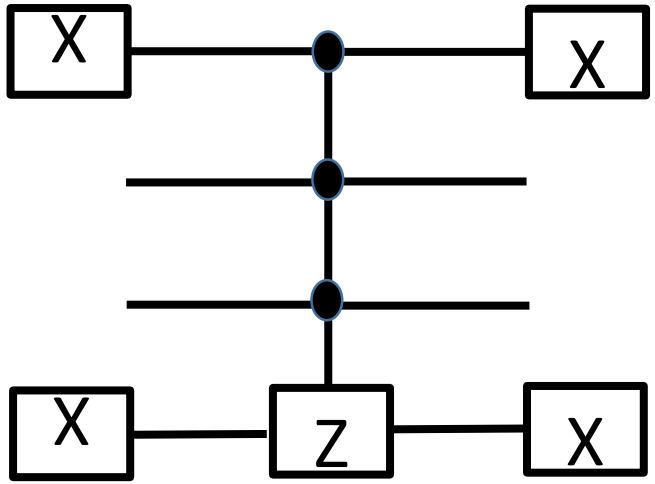
0011



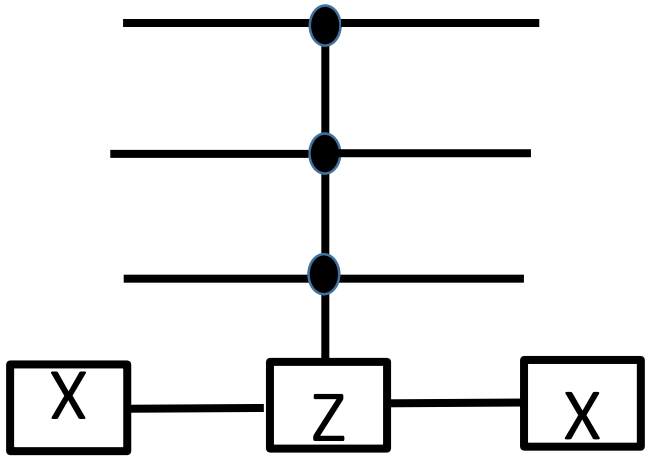
0100



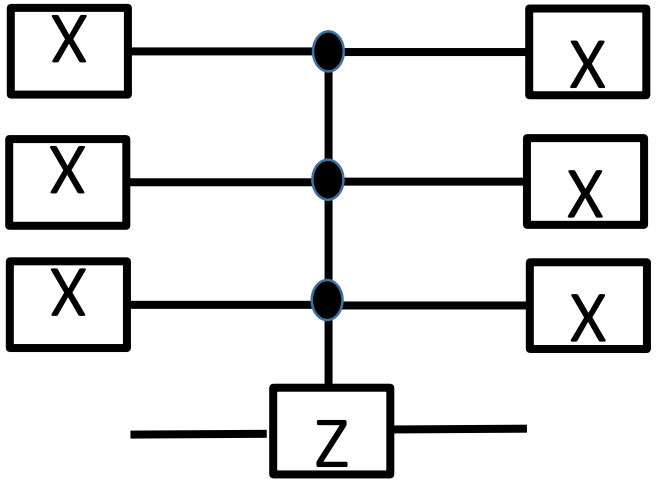
0101



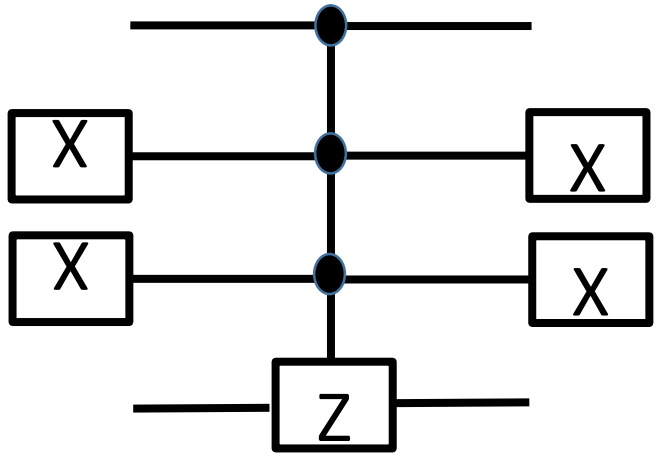
0110



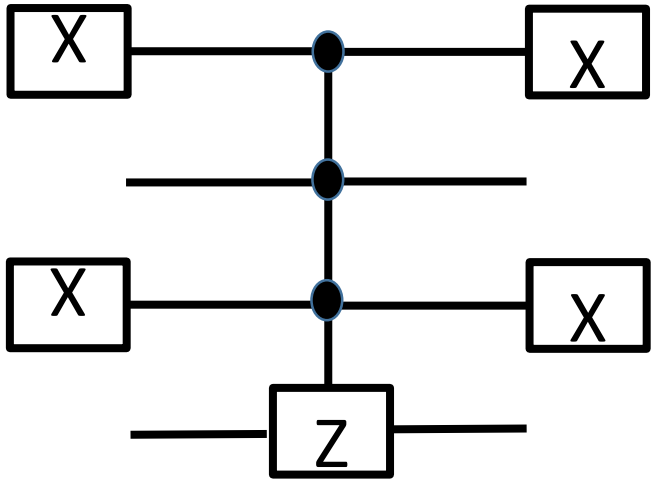
0111



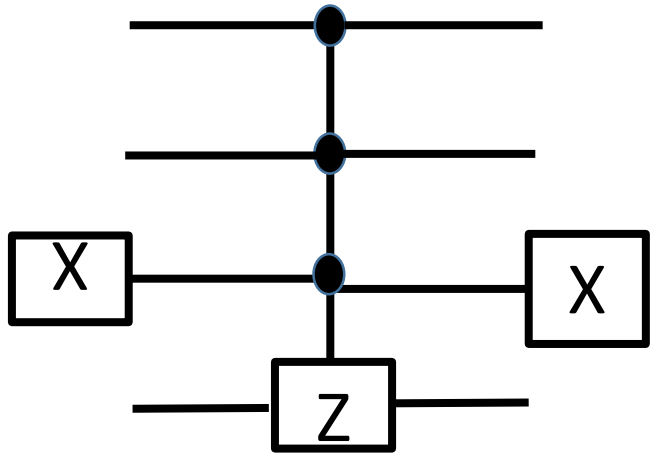
1000



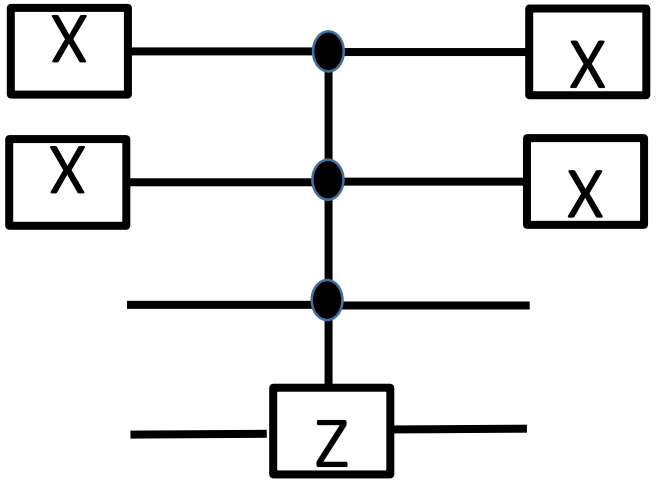
1001



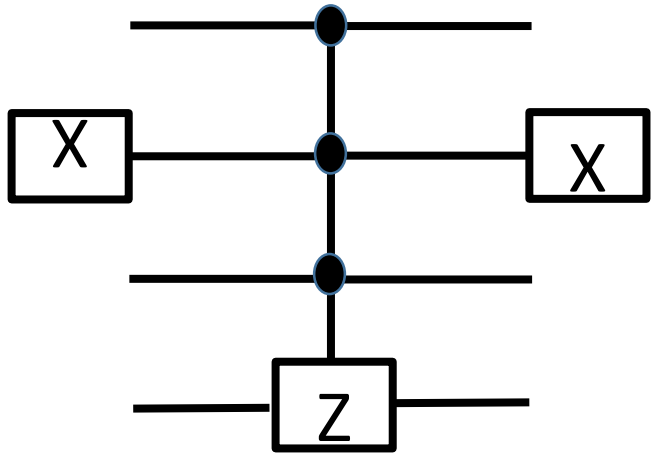
1010



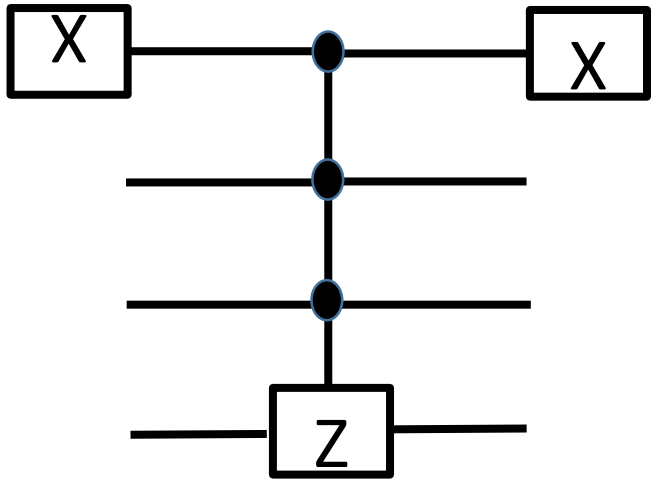
1011



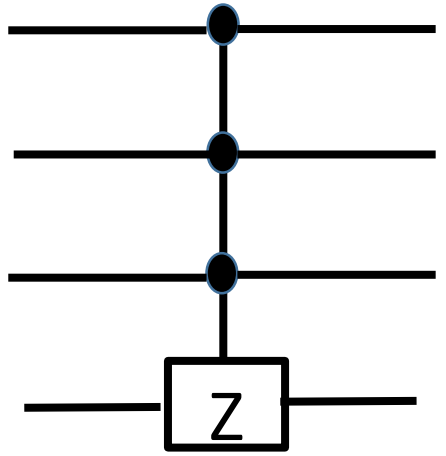
1100



1101



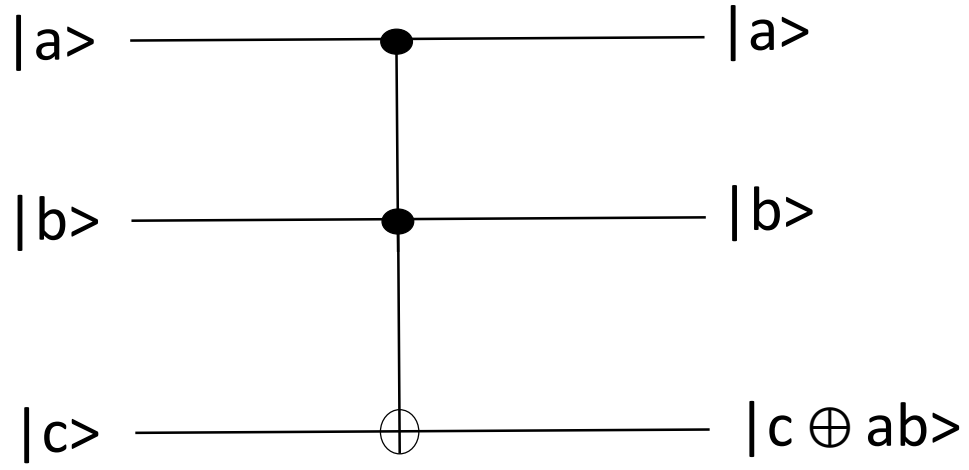
1110



1111

Reference The Toffoli Gate Construction

- The Toffoli gate is a 3-bit gate, which is universal for classical computation
- If the first two bits are in the state |1>, it applies a Pauli-X (NOT) on the third bit, otherwise the state is left unchanged

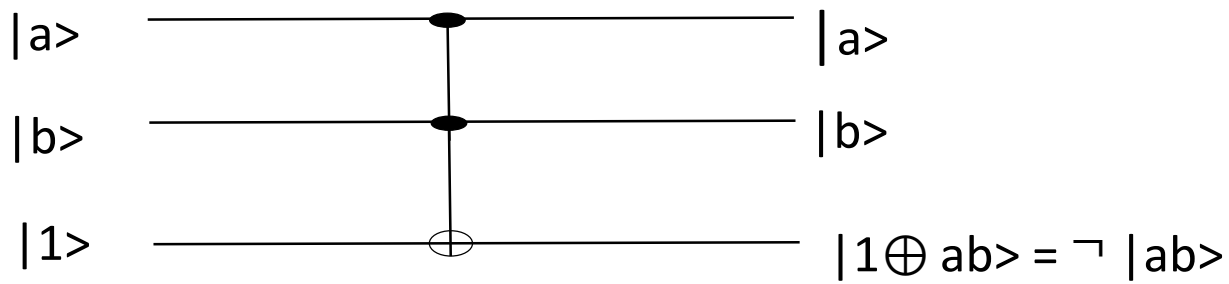


Properties of Toffoli Gates

- Toffoli Gate is a reversible gate (i.e. $U_T^{-1}U_T=I$) or
- Toffoli gate is used to replace a classical circuit with the equivalent reversible gate
- Two bits are control bits (|a> and |b>) and target bit |c> is flipped as per the truth table

$$(a, b, c) \rightarrow (a, b, c \oplus ab) \rightarrow (a, b, c)$$

- Toffoli gate and be used to simulate a NAND Gate



Toffoli Gate Truth Table and Matrix

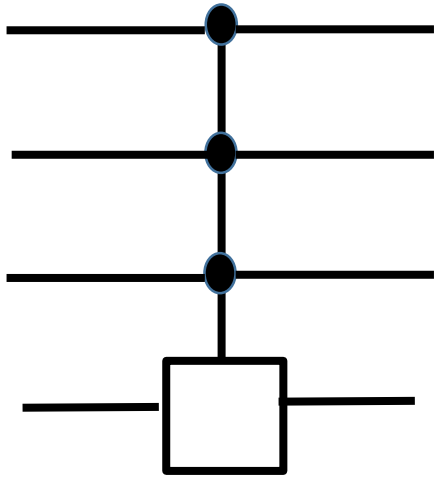
INPUT			OUTPUT		
a	b	c	a’	b’	c’
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

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

X Gate
Pauli σ_x rotation matrix

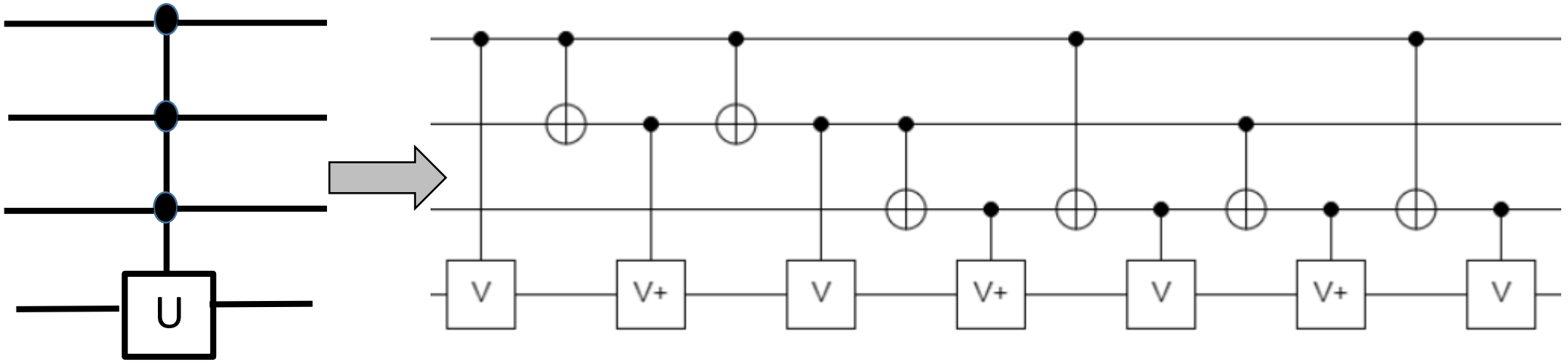
4 Qubit Control-Z Gate

- Within the Oracle there is multi-connected gate that as similar characteristics to the Toffoli Gate



CCC-Not Gate Construction

- It should be possible to construct a CCC-Not gate using an array of CC-Not gates combined with a sequence of 1 bit gates
- Any 4-bit gate that has 3 controlled and one unitary transformation can be represented* as where V is tuned such that $V^4 = U$



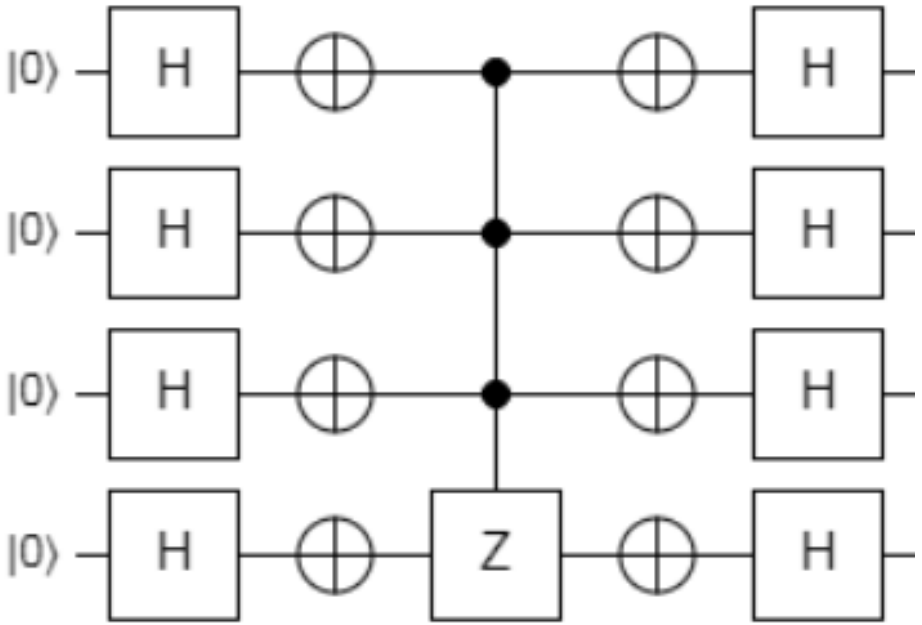
*A. Barenco, C. Bennett, R. Cleve, D. P. DeVincenzo, N. Margolus, P. W. Shor, "Elementary Gates for Quantum Computation", Phys. Rev A, March 1995

Amplification

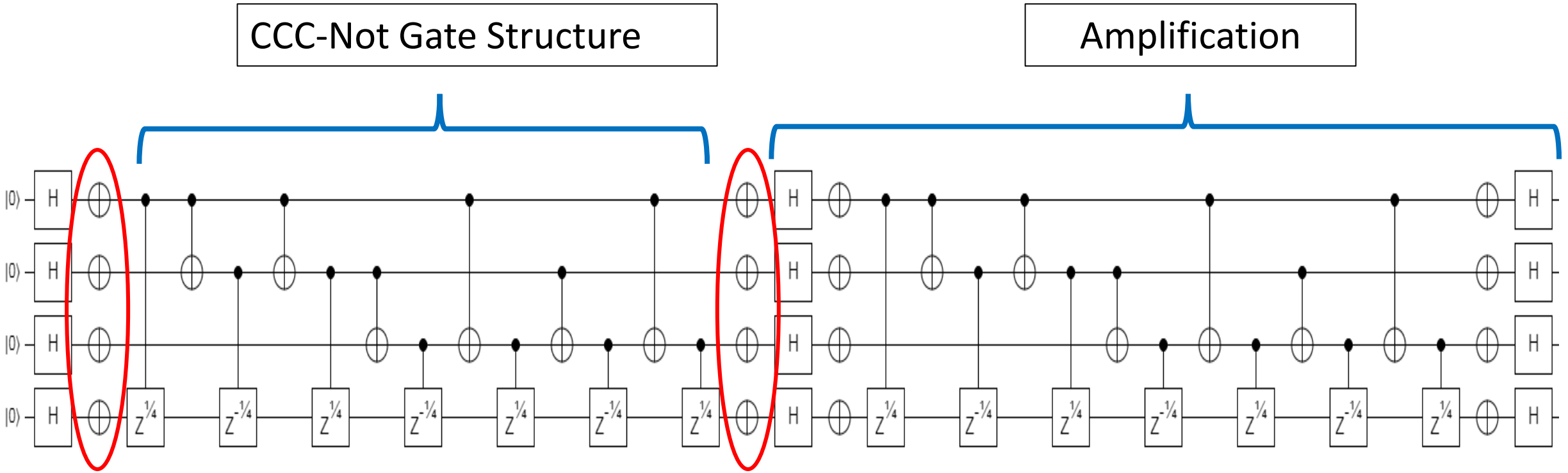
- This stage performs an inversion of the amplitudes about the average
- From the initialization step the amplitude is .25 ($N^{-1/2}$ where N=4)
- Avg_{amp} = [(15)(0.25)+(-0.25)]/16 = 0.21875
- Ind_{amp} = 0.21875-(-0.25) = 0.46875
- The inversion of the Ind_{amp} about the average is

  0.21875+0.46875 = 0.6875
- The amplitudes of the other states are 0.21875 - 0.25 = -0.03125
- The other states have a value 0.21875 - 0.03125 = 0.1875

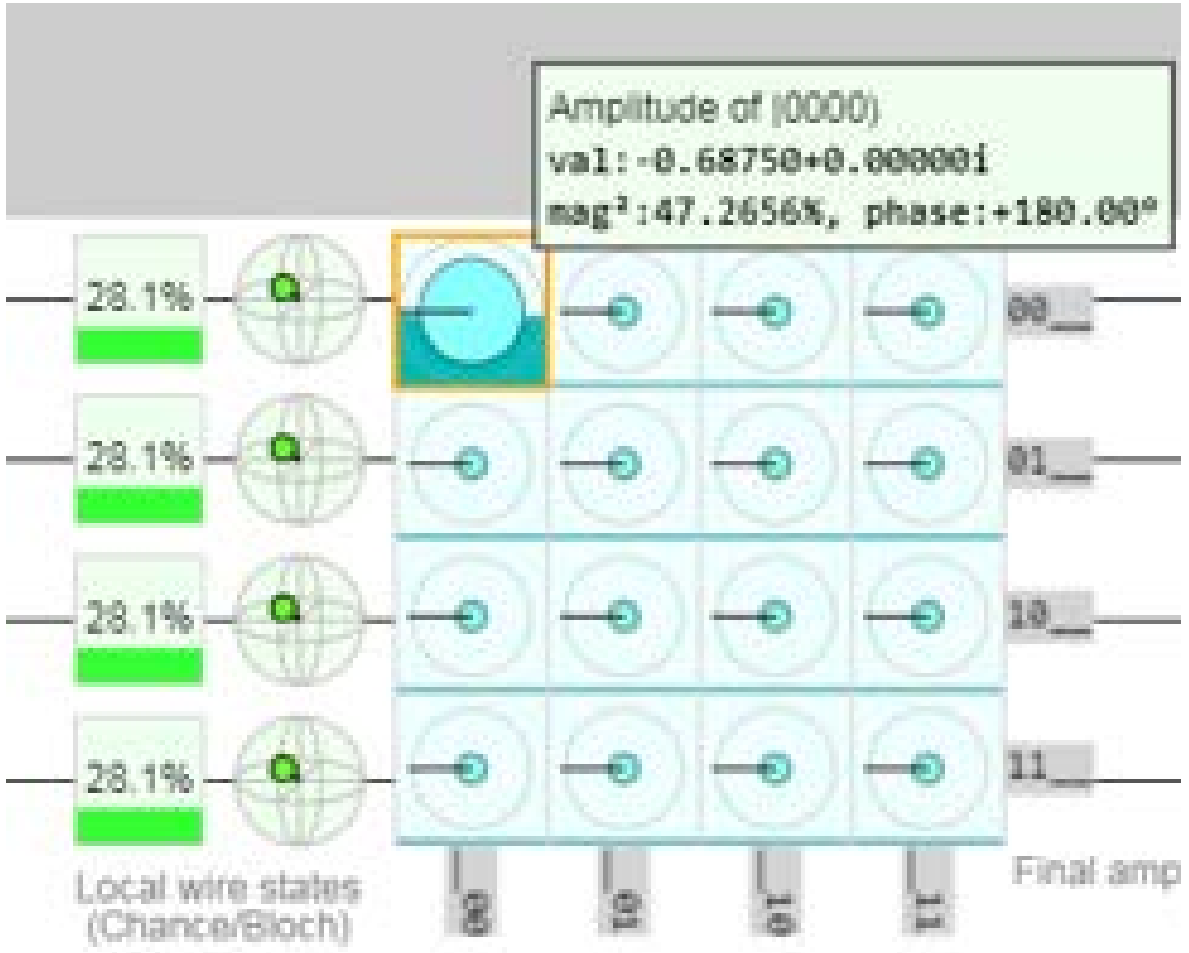
Amplification Gate Structure



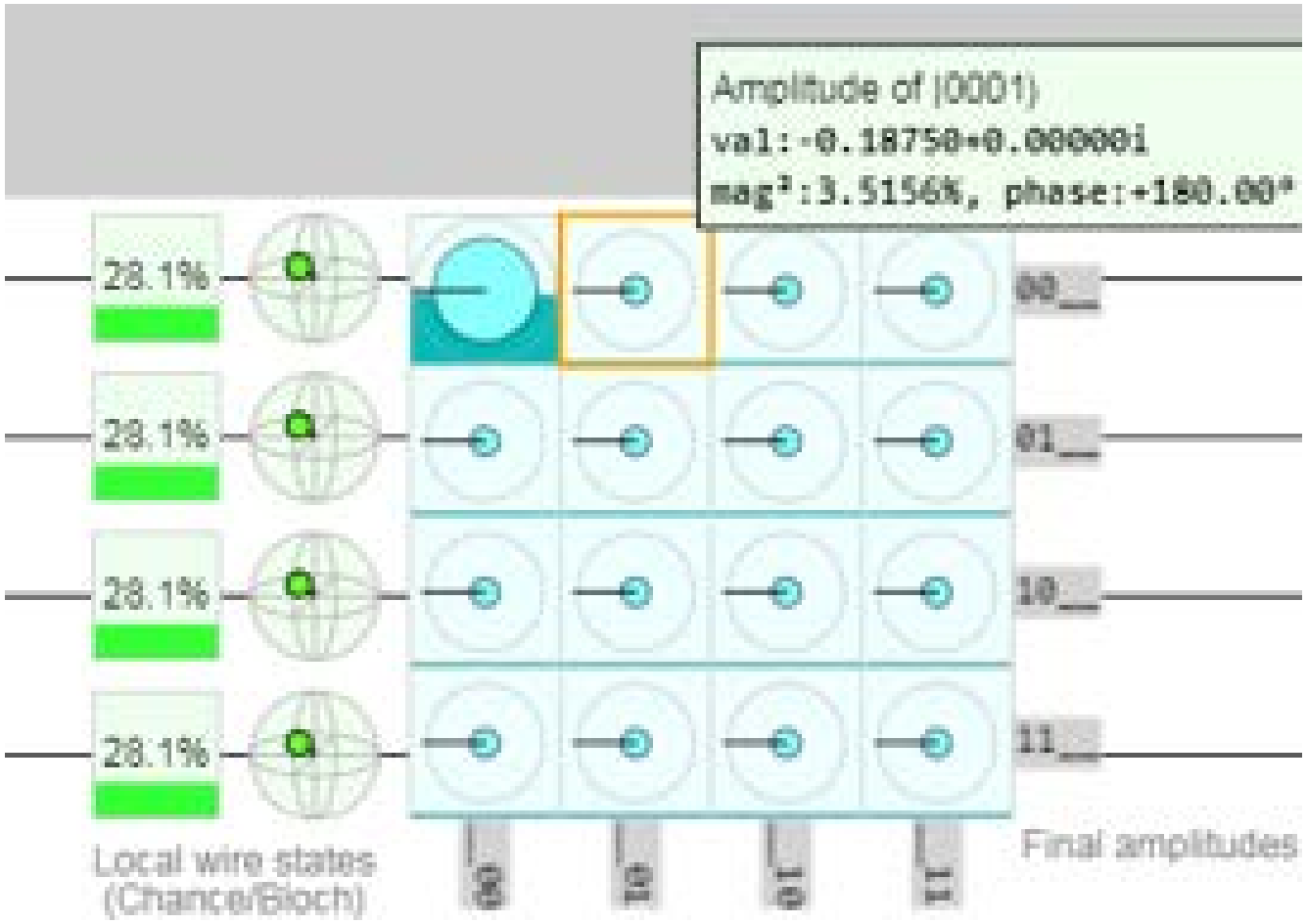
Quantum Computing Circuits for |0000> Oracle

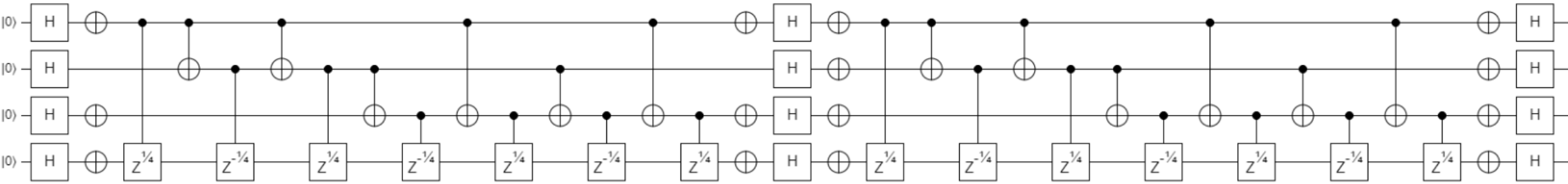


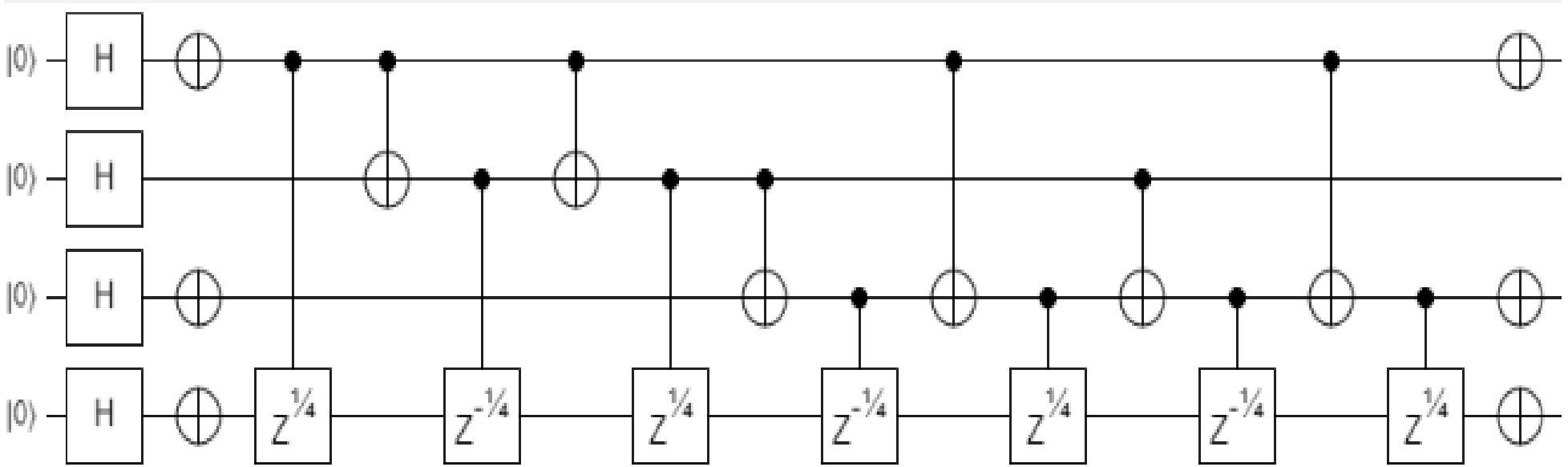
Final Measurement



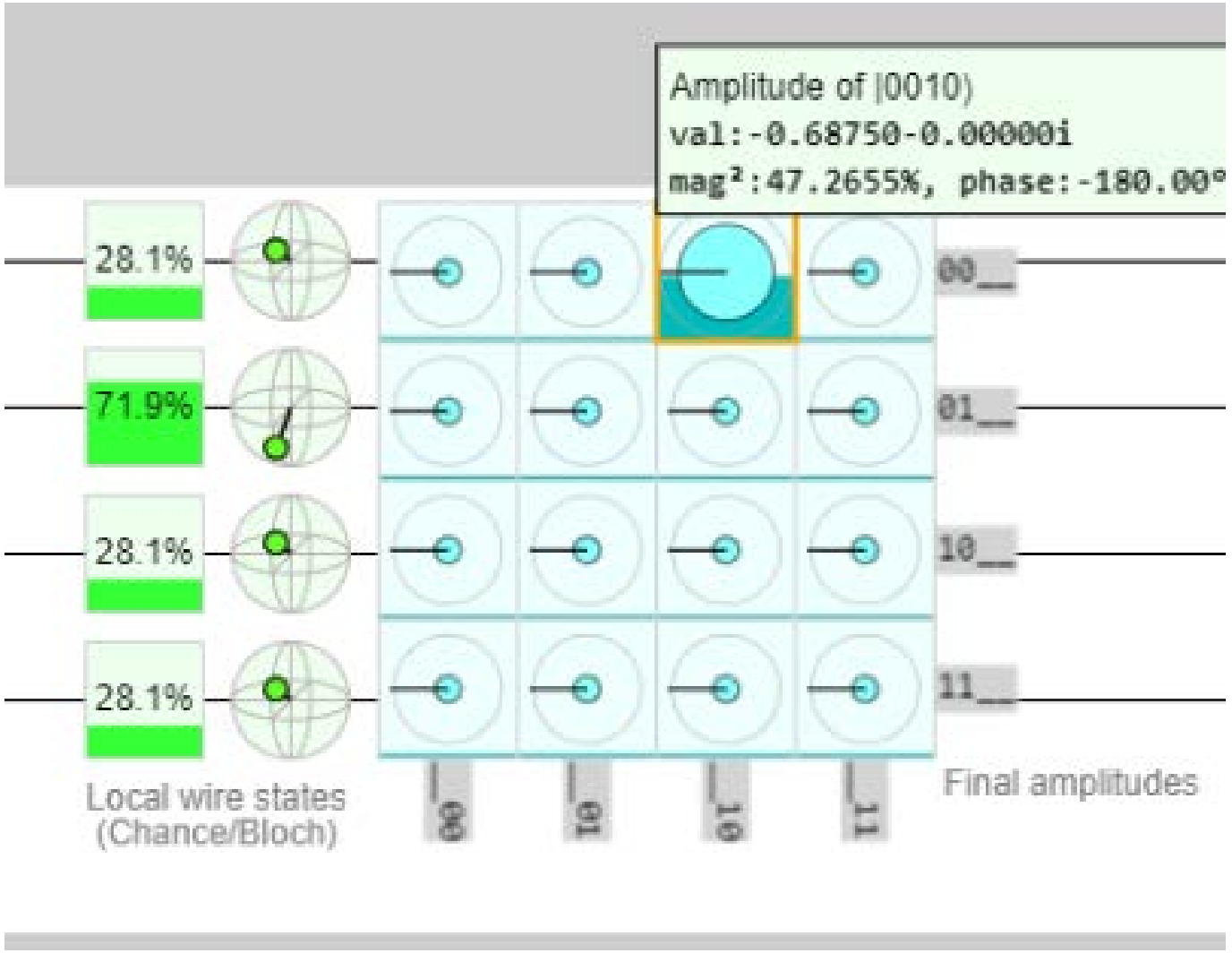
Final Measurement



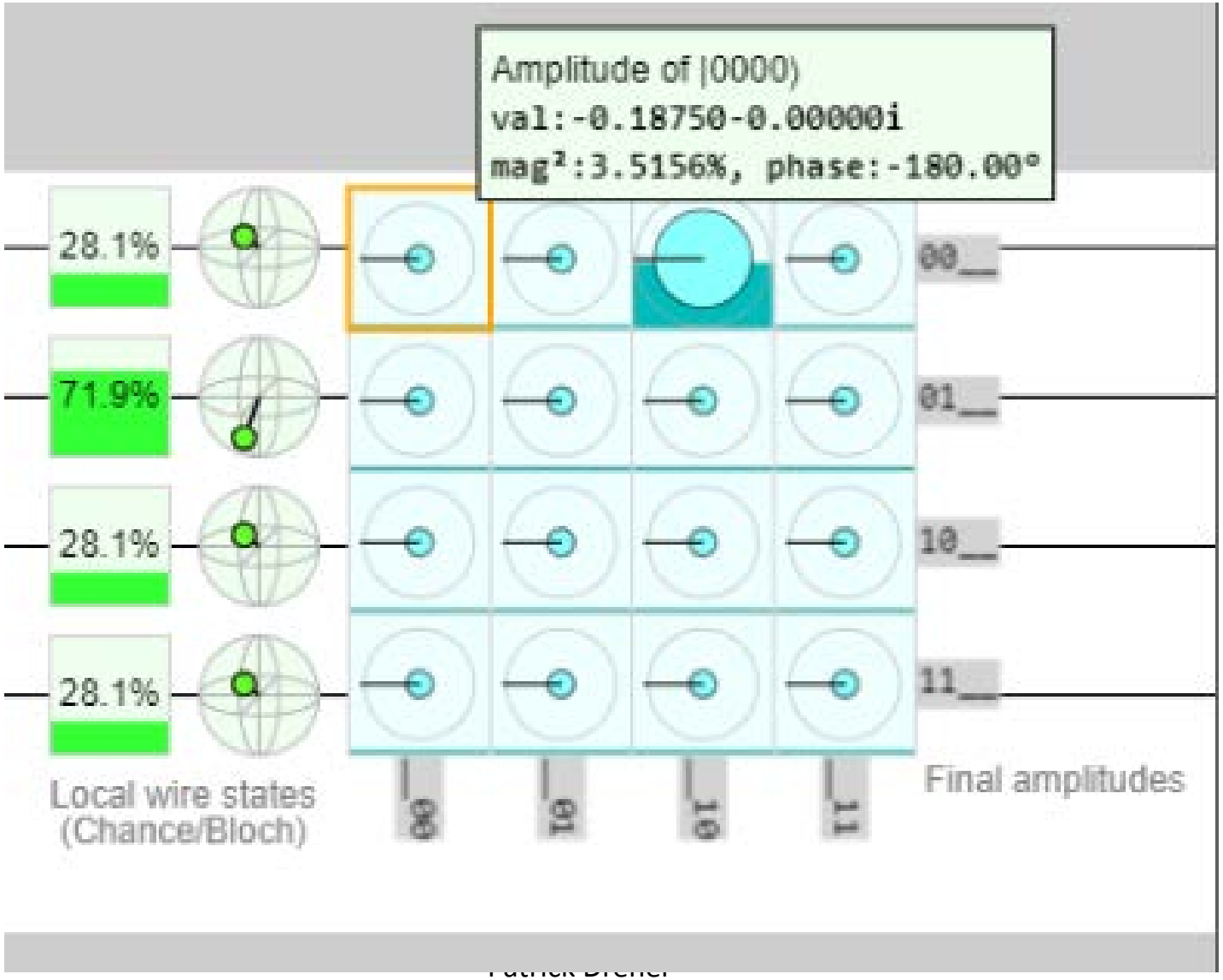

|0⟩
|0⟩
|0⟩
|0⟩
H
H
H
H
Z^¼
Z^-¼


|0⟩
H
|0⟩
H
|0⟩
H
|0⟩
H
Z^1/4
Z^-1/4
Z^1/4
Z^-1/4
Z^1/4
Z^-1/4
Z^1/4

Final Measurement



Final Measurement



Last Slide