

This paper follows Alessandro Berti and his didactical access to Grover's algorithm:

<https://towardsdatascience.com/behind-oracles-grovers-algorithm-amplitude-amplification-46b928b46f1e>

### SAT problem

We have a set of Boolean variables that should fulfill a given combination, e. g.:

$$(x \vee y) \wedge \bar{y} = 1$$

The solution:

$$x = 1, y = 0$$

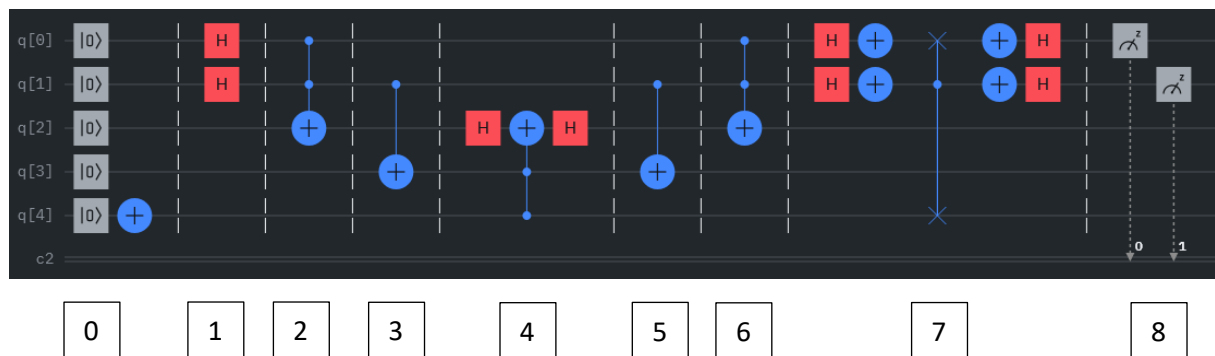
Quantum circuits can handle "  $\wedge$  " better than "  $\vee$  ", so we use the de Morgan formula:

$$\overline{(x \vee y)} = \bar{x} \wedge \bar{y}$$

We get the equivalent to our problem  $(x \vee y) \wedge \bar{y} = 1$

$$\overline{(\bar{x} \wedge \bar{y})} \wedge \bar{y} = 1$$

### The Quantum circuit

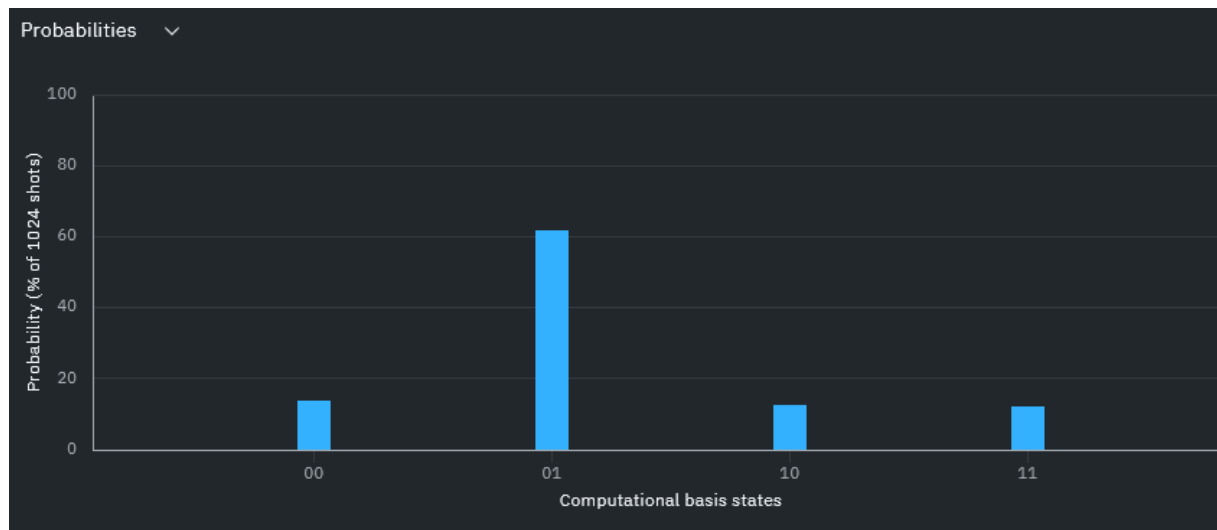


### Details

- 0 We use five qubits to calculate the correct values for  $x$  and  $y$ .  
 These are the qubit  $q[0]$  and  $q[1]$ . We set them to  $|0\rangle$  as start value.  
 We need two working qubits,  $q[2]$  and  $q[3]$ . We set them to  $|0\rangle$  as start value. The working qubits store intermediate results.  
 We need a "checker" qubit  $q[4]$ . We set it to  $|1\rangle$  via the swap as start value. The checker qubit transports the solution to the superposition in 8.
- 1 We bring the input qubits  $q[0]$  and  $q[1]$  into superposition by help of the *Hadamard* gate.
- 2 We calculate the first part of the logic problem,  $(\bar{x} \wedge \bar{y})$  by help of a *CCNOT* gate:  
 The *CCNOT* performs a not on line three if the values on line one and line two are "1". The working qubit  $q[2]$  then holds the result of the first operation.
- 3 In the same way we calculate the second part of the logic problem,  $\bar{y}$  and store the result in the working qubit  $q[3]$ .
- 4 Now we apply a *CCZ* to the working qubit  $q[2]$ .

5 and 6 are needed to undo 2 and 3. This is a property of quantum computing.  
 1 through 6 form the oracle.

- 7 We use the diffuser to apply the solution in search to the qubits  $x$  and  $y$ . We apply the Hadamards to both qubits again, invert them and perform a  $CSWAP$  to the checker qubit. This brings the solution searched into contact with the superposition of the input qubits  $x$  and  $y$ . We then undo the invert and the Hadamards.
- 8 We measure both qubits. With a single measurement we will get either 0 or 1. We must repeat the whole process for e. g. 100 times and get a sample of results:



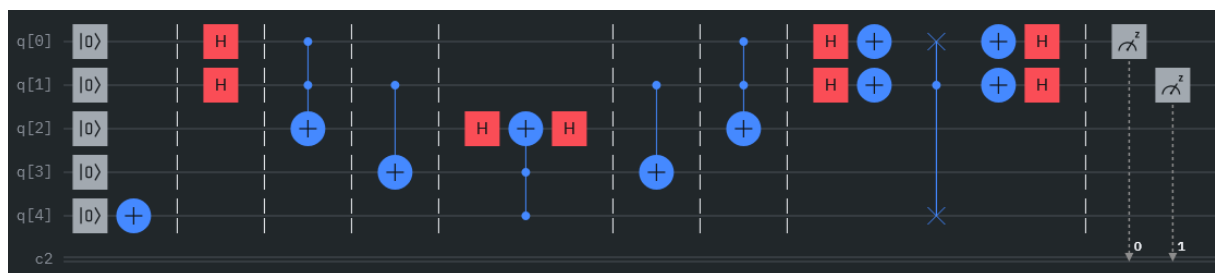
The measurement result with the highest probability is the combination  $x = 1, y = 0$ , the solution for our problem. Please note that the composer uses little endian.

Remark: We did not insert the solution into our circuit but we inserted the Boolean formula for it.

We take a look at the whole process on conceptual level.

### Conceptual level

We used the circuit:



- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8

- 0 We have five input qubits we write as  $|00001\rangle$  (the 1 made by the *NOT*).
- 1 We apply the *Hadamard* to qubits one and two. The *Hadamard* applied to  $|0\rangle$  gives  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ , the *Hadamard* applied to  $|1\rangle$  gives  $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ .

$$|00001\rangle \rightarrow H|0\rangle H|0\rangle|001\rangle =$$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot |001\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|001\rangle =$$

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)|001\rangle = \frac{1}{2}(|00001\rangle + |01001\rangle + |10001\rangle + |11001\rangle)$$

2 Then we apply the *CCNOT* from lines one and two to line three. The *CCNOT* swaps position three if positions one and two both are  $|1\rangle$ .

$$\frac{1}{2}(|00001\rangle + |01001\rangle + |10001\rangle + |11101\rangle)$$

3 We apply the *CNOT*-gate from position two to position four:

$$\frac{1}{2}(|00001\rangle + |01011\rangle + |10001\rangle + |11111\rangle)$$

4 We apply the *CCZ*-gate from position four and three to qubit 2:

$$\frac{1}{2}(|00001\rangle + |01011\rangle + |10001\rangle - |11111\rangle)$$

Note: The circuit shown represents the *CCZ* as the *CCZ* is not directly available in IBM composer.

Note: This is the sign-swap wanted.

5 We undo operations 2 and 3 by applying them again:

Operation 2 was a *CCNOT* from lines one and two to line three. The *CCNOT* swaps position three if positions one and two both are  $|1\rangle$ .

$$\frac{1}{2}(|00001\rangle + |01011\rangle + |10001\rangle - |11011\rangle)$$

6 Operation 3 was a *CNOT*-gate from position two to position four:

$$\frac{1}{2}(|00001\rangle + |01001\rangle + |10001\rangle - |11001\rangle)$$

Note: The first two qubits are in the same state as in the beginning after the first Hadamard.

7 The diffusor with the application of the *Hadamard*, *X*-gate, *CSWAP* and the undo.

The *Hadamards*:

$$\frac{1}{2}(H|0\rangle H|0\rangle|001\rangle + H|0\rangle H|1\rangle|001\rangle + H|1\rangle H|0\rangle|001\rangle - H|1\rangle H|1\rangle|001\rangle) =$$

$$\frac{1}{4}((|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|001\rangle + (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)|001\rangle + (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)|001\rangle - (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)|001\rangle) =$$

$$\frac{1}{4}(|00001\rangle + |01001\rangle + |10001\rangle + |11001\rangle + |00001\rangle - |01001\rangle + |10001\rangle - |11001\rangle + |00001\rangle + |01001\rangle - |10001\rangle - |11001\rangle - |00001\rangle + |01001\rangle + |10001\rangle - |11001\rangle) =$$

$$\frac{1}{4}(2|00001\rangle + 2|01001\rangle + 2|10001\rangle - 2|11001\rangle)$$

The  $X$ -gates:

$$\frac{1}{4}(2|11001\rangle + 2|10001\rangle + 2|01001\rangle - 2|00001\rangle)$$

The  $CSWAP$  from position two swaps position zero and four:

$$\frac{1}{4}(2|11001\rangle + 2|10001\rangle + 2|11000\rangle - 2|00001\rangle)$$

The  $X$ -gates:

$$\begin{aligned} &\frac{1}{4}(2|00001\rangle + 2|01001\rangle + 2|00000\rangle - 2|11001\rangle) = \\ &\frac{1}{2}(|00001\rangle + |01001\rangle + |00000\rangle - |11001\rangle) = \end{aligned}$$

The  $Hadamards$ :

$$\begin{aligned} &\frac{1}{4}((|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|001\rangle + (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)|001\rangle + (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|000\rangle \\ &\quad - (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)|001\rangle) = \\ &\frac{1}{4}(|00001\rangle + |01001\rangle + |10001\rangle + |11001\rangle + |00001\rangle - |01001\rangle + |10001\rangle - |11001\rangle \\ &\quad + |00000\rangle + |01000\rangle + |10000\rangle + |11000\rangle - |00001\rangle + |01001\rangle + |10001\rangle \\ &\quad - |11001\rangle) = \\ &\frac{1}{4}(|00001\rangle + |01001\rangle + 3|10001\rangle - |11001\rangle + |00000\rangle + |01000\rangle + |10000\rangle + |11000\rangle) = \end{aligned}$$

8 We measure qubits one and two. The probabilities are:

$ 00xxx\rangle$	$\frac{1}{16} + \frac{1}{16} = \frac{1}{8}$
$ 01xxx\rangle$	$\frac{1}{16} + \frac{1}{16} = \frac{1}{8}$
$ 10xxx\rangle$	$\frac{1}{16} + \frac{9}{16} = \frac{5}{8}$
$ 11xxx\rangle$	$\frac{1}{16} + \frac{1}{16} = \frac{1}{8}$

Note: When measuring target qubits in a sequence of qubits, we concentrate on the target and ignore the rest.

Note: The sum of probabilities is 1.

This shows that the distribution of the probability for  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$ ,  $|11\rangle$  that was  $\frac{1}{4}$  after the first *Hadamard*. The probabilities for  $|00\rangle$ ,  $|01\rangle$ ,  $|11\rangle$  lowered to  $\frac{1}{8}$ , the probability for  $|10\rangle$  raised to  $\frac{5}{8}$ .