Quantum Computing

Carl August Gjørsvik

April 2020

Contents

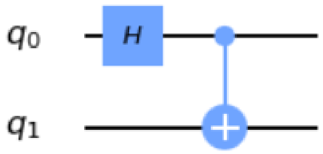
1 Superposition of a multiparticle qubit state

A multiparticle qubit can be in a state superposed of both its possible observable states, the superposition can be expressed as a linear combination of states. A common example is the use of the spin (up or down) of a single electron to represent bit states 0 and 1. If the electron is in a superposition of its states, it can be expressed as $\alpha|0\rangle + \beta|1\rangle$ where α and β are the (possibly complex) probability amplitudes of the states. When measuring the spin, state $|0\rangle$ will be observed with probability $|\alpha|^2$ and state $|1\rangle$ with probability $|\beta|^2$.

2 Quantum entanglement

For a pair or set of qubits to be entangled means that for any entangled qubit, its quantum state cannot be expressed separately from the state of the others.

A simple example of an entangled 2-qubit system is the Bell state, which can be produced with the following circuit:



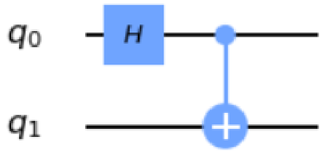
Initially the qubits q_0, q_1 are in the state $|0\rangle$. The combined state can be expressed as $|00\rangle$, but is still separable (each qubit is independent of the other). Applying the Hadamard-gate to q_0 changes its state to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ while q_1 is unchanged and the combined state becomes $\frac{|00\rangle+|10\rangle}{\sqrt{2}}$. After the controlled-NOT gate, q_1 will be *flipped* if q_0 is in state $|1\rangle$, and unchanged otherwise.
The final combined state becomes $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, and here we can see that if one of the qubits is measured, the state of the other will also be decided. The state of the single qubits can no longer be expressed independent of the other.

This phenomenon is not affected by physical distance, which is why some have argued that in this case, information is exchanged at a speed faster than the speed of light, and Einstein famously referred to it as “spooky action at a distance”.

3 Bell states

The Bell states are the four maximally entangled states of a two-qubit system. When in a Bell state, if either of the two qubits are measured, it has an equal probability of being measured in either possible observable state, while the other qubit will also at this point be determined to be either in the same state or the opposite, depending on which Bell state they were in.

The Bell states can be created with the simple circuit



Which corresponds to the equation:

$$|\beta_{xy}\rangle = \frac{|0,y\rangle + (-1)^x|1,\bar{y}\rangle}{\sqrt{2}}$$

Such that:

$$|00\rangle \quad \Rightarrow \quad \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|01\rangle \quad \Rightarrow \quad \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|10\rangle \quad \Rightarrow \quad \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|11\rangle \quad \Rightarrow \quad \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

4 The No-cloning Theorem

The idea of the No-Cloning theorem is that an unknown quantum state $|\psi\rangle$ is impossible to copy. One can only copy qubits in their orthonormal states, e.g. $|0\rangle$ or $|1\rangle$.

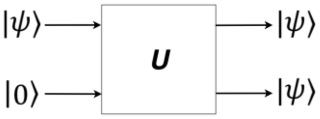
To copy a qubit, the CNOT-gate can be applied to the source $|\psi\rangle$ and the target qubit initialized in the zero state $|0\rangle$.

$$CNOT([\alpha|0\rangle + \beta|1\rangle] \otimes |0\rangle) = \alpha|00\rangle + \beta|11\rangle$$

Now if $\alpha = 0$ or $\beta = 0$, the state has been effectively copied, but in any other case, the qubits are now entangled, and the target qubit is not a copy of the initial state. For it to be a true copy of the state, we should have the un-entangled state:

$$|\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

To show that a unitary quantum operator U which can copy a quantum state $|\psi\rangle$ cannot exist, consider:



If U could copy the state $|\psi\rangle$, then:

$$[\alpha|0\rangle + \beta|1\rangle] \otimes |0\rangle \quad \overset{U}{\Rightarrow} \quad [\alpha|0\rangle + \beta|1\rangle] \otimes [\alpha|0\rangle + \beta|1\rangle]$$

And U must logically transform the following states:

$$|00\rangle \overset{U}{\Rightarrow} |00\rangle$$

$$|10\rangle \overset{U}{\Rightarrow} |11\rangle$$

$$|01\rangle \overset{U}{\Rightarrow} |00\rangle$$

$$|11\rangle \overset{U}{\Rightarrow} |11\rangle$$

Applying the above transformations to the state we wanted to copy:

$$\alpha|00\rangle + \beta|10\rangle \quad \overset{U}{\Rightarrow} \quad \alpha U|00\rangle + \beta U|10\rangle$$

$$= \alpha|00\rangle + \beta|11\rangle$$

Which is not the required result.

5 The Pauli matrices

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

As with all quantum gates, these matrices are unitary.

The X-matrix

Also known as the quantum “bit flip” gate, or the quantum NOT gate.

Applying X to a qubit $\alpha_0|0\rangle + \alpha_1|1\rangle$ results in $\overset{X}{\Rightarrow} \ \alpha_1|0\rangle + \alpha_0|1\rangle$.
When applied to a qubit in a certain state, e.g. $|0\rangle$, we get:

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

The matrix is unitary:

$$X^\dagger X = XX^\dagger = I \quad ?$$

$$X^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X \quad \Rightarrow \quad X^\dagger X = XX^\dagger = X^2$$

$$X^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

The Y-matrix

This Pauli matrix can be described as a simultaneous application of the “bit flip” and “phase flip”.

$$\alpha_0|0\rangle + \alpha_1|1\rangle \quad \overset{Y}{\Rightarrow} \quad i(-\alpha_1|0\rangle + \alpha_0|1\rangle)$$

$$Y|\Psi\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = i \begin{pmatrix} -\alpha_1 \\ \alpha_0 \end{pmatrix}$$

$$Y^\dagger Y = YY^\dagger = I \quad ?$$

$$Y^\dagger = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = Y \qquad \Rightarrow \qquad Y^\dagger Y = YY^\dagger = Y^2$$

$$Y^2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

The Z-matrix

Referred to as the “phase flip” gate. When working in the computational basis, it flips the sign of the probability amplitude of $|1\rangle$: $\alpha_0|0\rangle + \alpha_1|1\rangle \overset{Z}{\Rightarrow} \alpha_0|0\rangle - \alpha_1|1\rangle$.

A qubit in the $|+\rangle$ state is “flipped” to $|-\rangle$ and vice versa. E.g.

$$Z|+\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$$

$$Z^\dagger Z = ZZ^\dagger = I \quad ?$$

$$Z^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z \qquad \Rightarrow \qquad Z^\dagger Z = ZZ^\dagger = Z^2$$

$$Z^2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

6 How the Pauli matrices are stabilized by H and N

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad N = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}$$

$$HXH = Z$$

$$HXH = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$

$$HZH = X$$

$$HZH = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X$$

$$HYH = -Y$$

$$HYH = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} = -Y$$

$$NXN^{-1} = -Y$$

$$NXN^{-1} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} = -Y$$

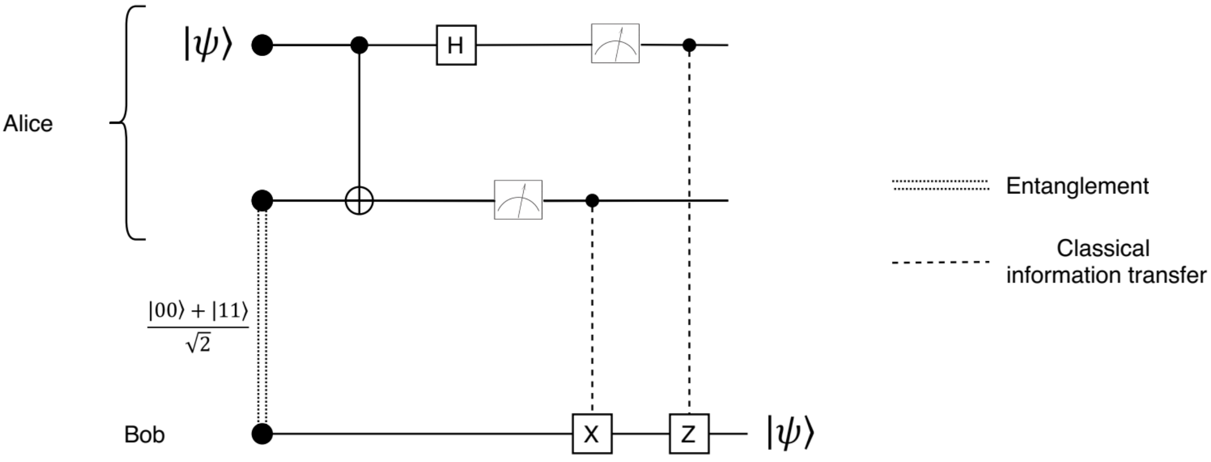
$$NYN^{-1} = -Z$$

$$NYN^{-1} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = -Z$$

$$NZN^{-1} = X$$

$$NZN^{-1} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X$$

7 A quantum teleportation protocol


Alice
$|\psi\rangle$
H
X
Z
$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$
Bob
$|\psi\rangle$
Entanglement
Classical information transfer

a. Establish an initial state where Alice has a qubit q_0 in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, which is the state they want to *teleport*. In addition, they share an entangled pair q_1, q_2 in the Bell state $|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. The state of all the qubits can be expressed: $|\psi\rangle \otimes \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ or

$$\frac{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle}{\sqrt{2}}$$

b. Alice applies a CNOT-gate on her qubits q_0, q_1 such that the state becomes

$$\frac{\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle}{\sqrt{2}}$$

c. Alice measures q_1, which will decide the state of the remaining qubits. Depending on what she measures, these are the possible states:

$$Measure\ 0 \ \Rightarrow \ q_0, q_2 = \frac{\alpha|00\rangle + \beta|11\rangle}{\sqrt{2}}$$

$$Measure\ 1 \ \Rightarrow \ q_0, q_2 = \frac{\alpha|01\rangle + \beta|10\rangle}{\sqrt{2}}$$

d. Alice informs Bob whether she measured 0 or 1 for q_1 by classical communication. If Alice measured 1, Bob performs a *bit-flip* (Pauli X-gate) on q_2 such that the state of q_0, q_2 is $\frac{\alpha|00\rangle+\beta|11\rangle}{\sqrt{2}}$ in any case.

e. Alice applies a Hadamard gate to q_0 to measure it in the +/- basis. As these qubits are entangled, this operation might best be described as applying $H \otimes I$ to q_0, q_2, where

$$H \otimes I = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

Applying this to the state:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}\alpha\\ 0\\ 0\\ \beta\end{bmatrix} = \frac{1}{2}[\alpha, \beta, \alpha, -\beta]$$

$$= \alpha|00\rangle + \beta|01\rangle + \alpha|10\rangle - \beta|11\rangle$$

And now that Alice measures her qubit q_0, we get these results:

$$Measure\ 0 \ \Rightarrow\ q_2 = \alpha|0\rangle + \beta|1\rangle$$

$$Measure\ 1 \ \Rightarrow\ q_2 = \alpha|0\rangle - \beta|1\rangle$$

f. Alice informs Bob by classical information transfer whether she measured 0 or 1. If she measured 1, Bob applies the *phase flip* gate (Pauli Z-gate)

$$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\alpha\\ -\beta\end{bmatrix} = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$$

Now Bob's qubit is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

7.1 If the distance between Alice and Bob is large, why does this not contradict the speed of light limit?

As described in the quantum teleportation protocol above, Alice and Bob must exchange information through a classical communication channel limited by the speed of light for there to be any teleportation. Without the classical communication, no information is transferred (or *teleported*). Which means the quantum teleportation protocol does not contradict the limitation of the speed of light.

8 The quantum factoring algorithm

Shor's algorithm can be used to find the factors of a number N.
It starts with a guess $1 < g < N$, and if g is or shares a factor with N, which can be determined by calculating gcd (g, N) using Euclid's algorithm, a factor is found and the algorithm is done. When N becomes an increasingly large number, the chance of guessing a factor becomes too small for this to be feasible.

The next step is to use a "wrong" guess to find a factor using the following mathematical property:

For any A, B coprime, $\exists p$ s.t. $A^p = mB + 1$

$$\Rightarrow g^p = mN + 1$$

$$\Rightarrow g^p - 1 = mN \qquad |\ rearranging\ g^p - 1$$

$$\Rightarrow \left(g^{\frac{p}{2}}+1\right)\left(g^{\frac{p}{2}}-1\right)=mN$$

Which means $\left(g^{\frac{p}{2}}+1\right)$ and $\left(g^{\frac{p}{2}}-1\right)$ share factors with N, except in the case where either is a multiple of N. Also note that p must be even. Then if p is known, we can again use Euclid's algorithm to find the shared factors.

But just like guessing g, guessing p becomes infeasible for sufficiently large N.

Again, we need to find the value p such that $g^p = mN + 1$, or in other words $g^p \equiv 1(mod\ N)$. This p is the period of the function such that for every guess x, if $g^x \equiv r(mod\ N)$, then for any multiple of p this also follows: $g^{x+mp} \equiv r(mod\ N)$. The remainder r repeats with period p.

Shor's algorithm uses this property and the inverse Quantum Fourier Transform (QFT) to find the period efficiently.

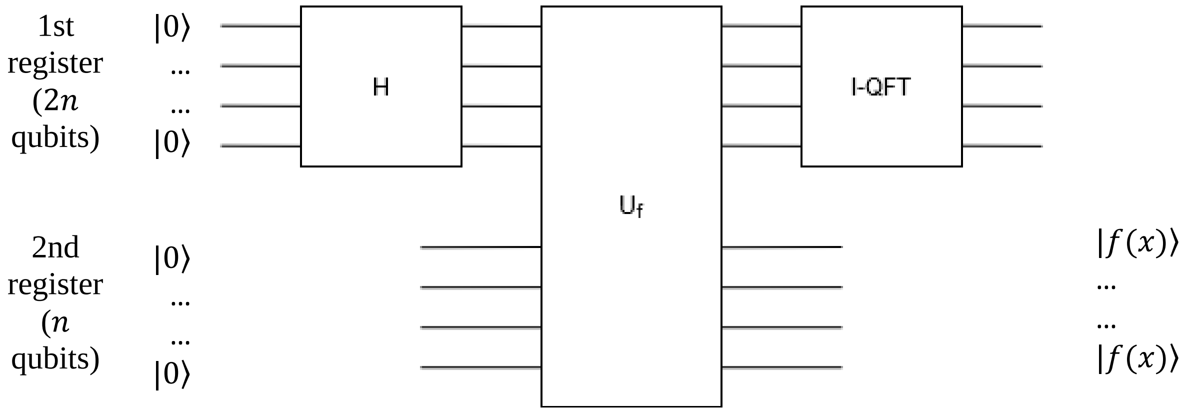
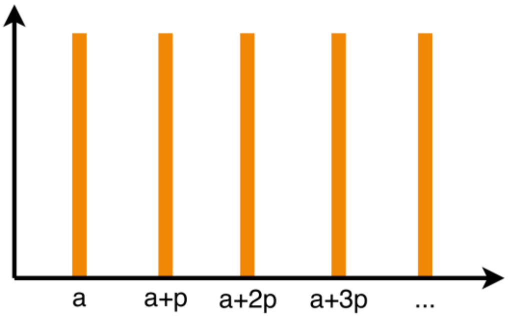


Illustration of period finding circuit

Initialize the first register as a tensor in the $|0\rangle$ state of length $2n$, where $n = \lceil \log_2 N \rceil$ and the second register of length n.

Apply Hadamard transformation to the first register, resulting in a tensor of each qubit in the superposition $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$.

Construct a Controlled-U gate with the function $f(x) = g^x(mod\ N)$, such that the function result is output to the second register. The first register is used as input (x) to the function. Now the registers have become entangled. Measuring the output of the second register will *collapse* the register superpositions to one of the possible remainders r of the function $g^x(mod\ N) \equiv r$ (though this measurement is not necessary and does not affect the following steps). The first register has become a periodic superposition:



Probability amplitude distribution of first register after U_f

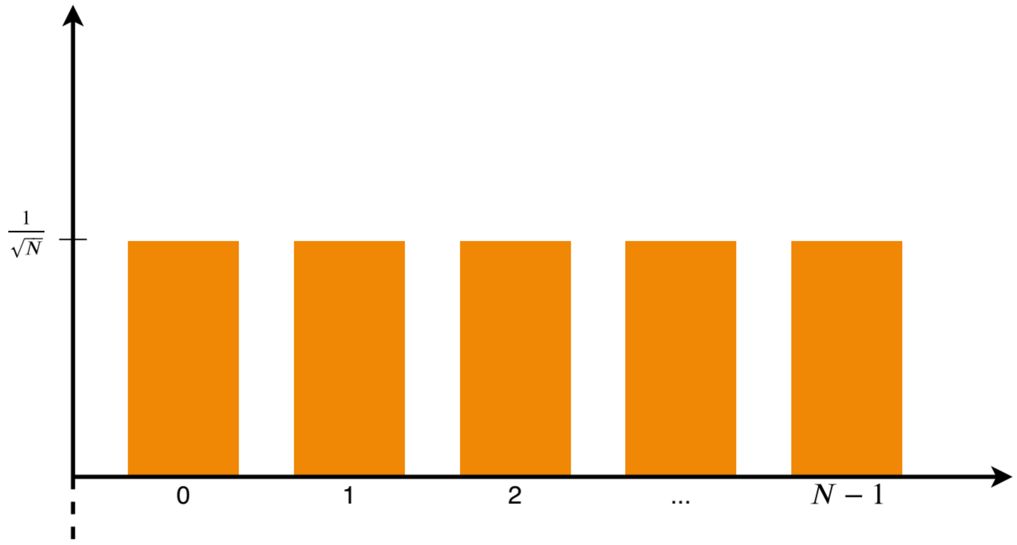
This periodic superposition can be shifted such that $a = 0$ and the peaks are then at multiples of p. After the QFT, one can measure an output which will be a random multiple of $\frac{N}{p}$. It might be necessary to measure more than once, but p can now be calculated using continued fraction – and if p is odd, just try a new guess. If p is even, we can calculate $\left(g^{\frac{p}{2}} + 1\right)$ and $\left(g^{\frac{p}{2}} - 1\right)$ and find shared factors with N by Euclid's algorithm. When a factor a of N is found, divide $\frac{N}{a} = b$ to find the other factor.

The complexity of this algorithm is polynomial over $\log N$ with it's complexity being approximately $O((\log N)^3)$, which is the product of the complexity of the Quantum Fourier Transform ($O((\log N)^2)$) and the modular arithmetic.

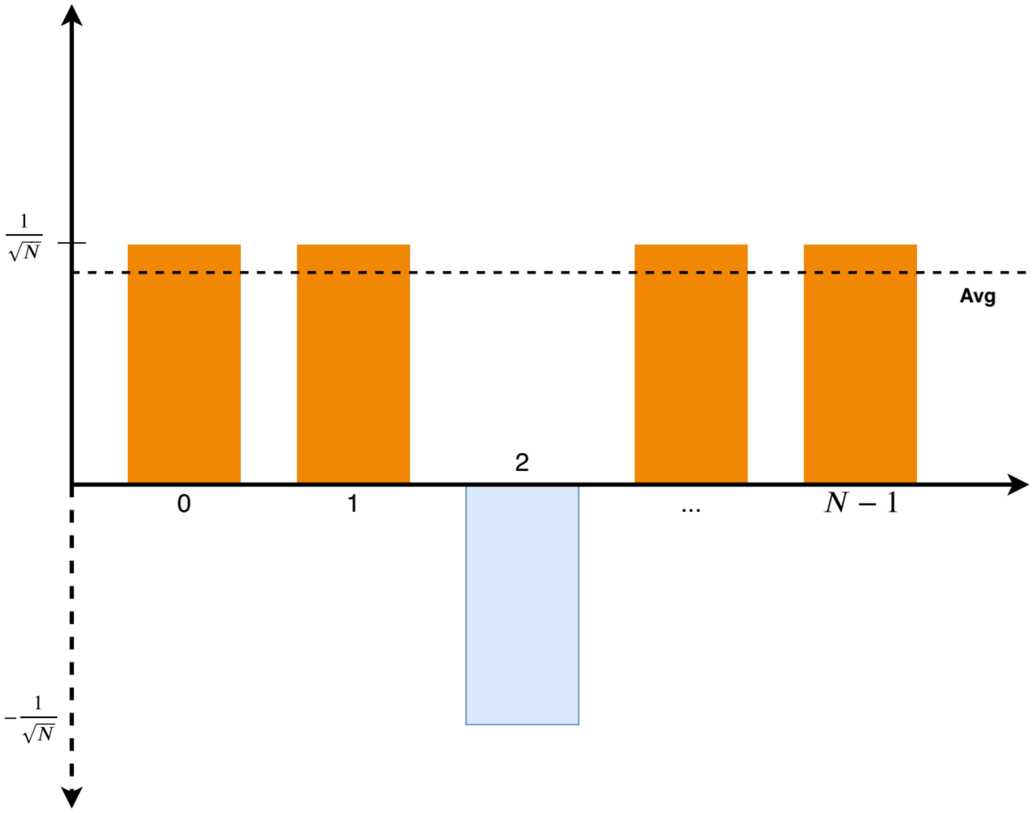
9 The quantum search algorithm

Grover's algorithm can find the target of a search in $O\left(\sqrt{N}\right)$ time if the search can be expressed as an *oracle function*, i.e. the result of the function is zero for every input except the search target, which result is 1.

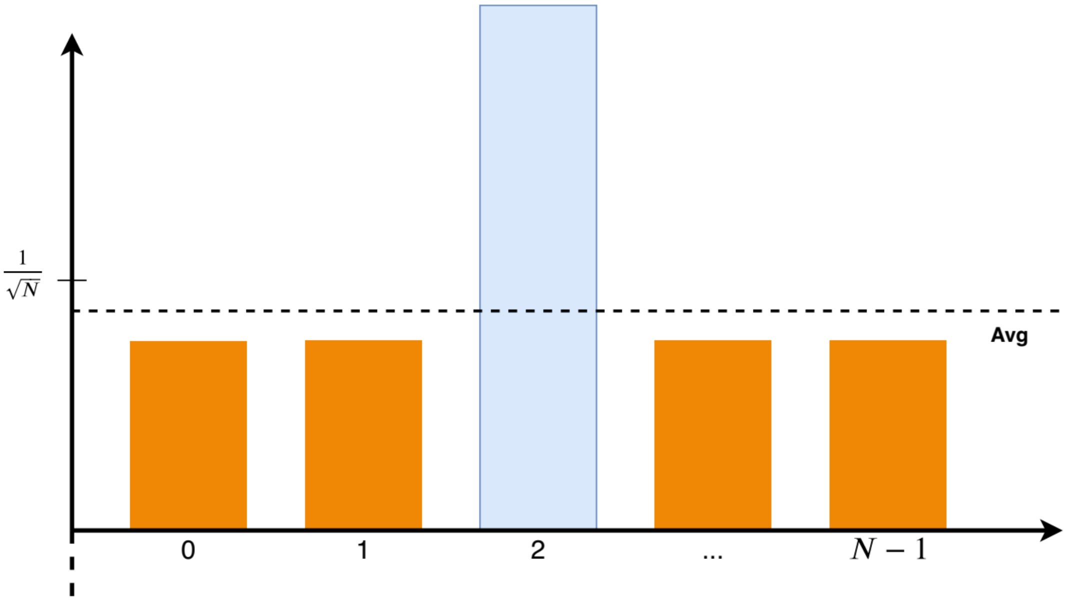
To perform the search, we need the input to be a superposition of all possible values in N. Then the first step of the algorithm is to apply a function U_f such that the probability amplitude of the search target x^* is inverted (sign changed). This will reduce the average probability amplitude slightly below $\frac{1}{\sqrt{N}}$. Now we can apply the second step, to "flip" each probability amplitude around the average – resulting in a reduction for all the *incorrect* values and an increase for x^*. Repeat these two steps $\sqrt{N}$ times such that the probability to measure x^* approaches 1.



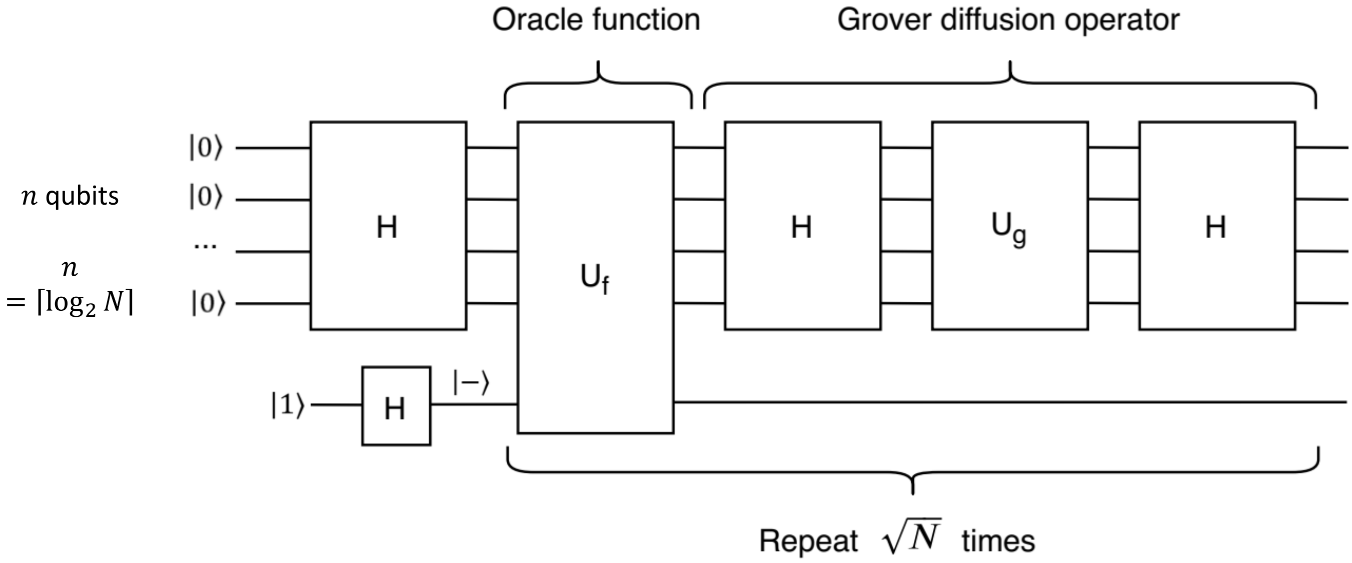
Initial state



Visualization of probability amplitude distribution after step 1 (oracle function) with e.g. $x^* = 2$



Visualization of probability amplitude distribution after step 2 (Grover diffusion operator)



Sketch of circuit implementing Grover's algorithm

To implement Grover's algorithm, Hadamard gates are used to create a superposition of possible x, as input to the oracle function. The oracle function U_f must invert probability amplitudes for which $f(x) = 1$ while leaving others unchanged – i.e. $U_f = (-1)^{f(x)}|x\rangle$. This can be implemented using a "control" qubit in the $|-\rangle$ state:

$$U_f(|x\rangle \oplus |-\rangle) = \frac{1}{\sqrt{2}}\big(U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle\big)$$

$$= \frac{1}{\sqrt{2}}(|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle)$$

$$= \begin{cases} \frac{1}{\sqrt{2}}(|x\rangle|1\rangle - |x\rangle|0\rangle) = -|x\rangle \oplus |-\rangle & if\ f(x) = 1 \\ \frac{1}{\sqrt{2}}(|x\rangle|0\rangle - |x\rangle|1\rangle) = |x\rangle \oplus |-\rangle & if\ f(x) = 0 \end{cases}$$

The Grover diffusion operator used to “flip the amplitudes around the mean” can be implemented as follows:

$$H^{\oplus n}(2|0\rangle\langle 0| - I)H^{\oplus n}$$

$$= 2|\Psi\rangle\langle\Psi| - I$$

Where Ψ is the superposition of possible states.

This algorithm achieves a quadratic advantage over classical systems as the computation procedures only needs to be repeated $\sqrt{N}$ times for the probability of finding the search target to approach 1 with a negligible margin, as opposed to the classical approach which is a sequential search of $O(N)$.