Introduction to quantum computing

Bijan Chokoufe Nejad

Vortrag zur Vorlesung Informationstheorie

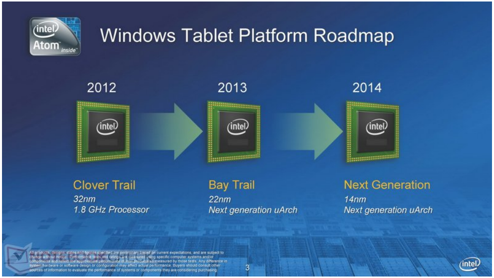
July 3, 2012

Table of contents

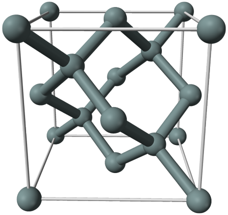
Cbits and Qbits

Why do we need/want a quantum computer?

End of *Moore's law* is within reach:



vs



$a = 0.543\,\mathrm{nm}$

Urge for technological progress needs new ideas.

Why do we need/want a quantum computer?

- 1994 Peter Shor introduced an quantum computing algorithm which can factorize numbers N in polynomial time

$$\mathcal{O}(\log N^3)$$

- The best known factoring algorithm on classical computers are superpolynomial:

$$\mathcal{O}\left(e^{C(\log N)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}}\right)$$

- RSA encryption, which depends on the nonpolynomial factorization time, could be broken using quantum computers.

- Simulations of other quantum systems which are still poorly understood due to complexity.. and much more?

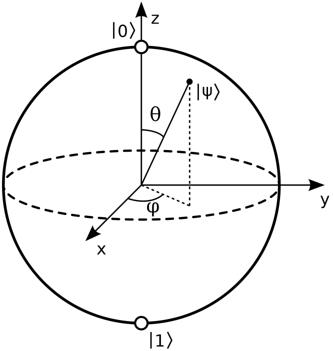
Classical computing (CC)

Classical bits Cbits

Only two discrete values for each Cbit: 1,0.

Quantum computing (QC)

Quantum bits Qbits



Why should we use unitary operators?

- Due to the unreasonable success of quantum mechanics and quantum field theories, e.g.

  $$g_{\text{el, theor}} = 2{,}002\,319\,304\,8(8)\,, \quad g_{\text{el, exp}} = 2{,}002\,319\,304\,361\,53(53),$$

  we think that the time evolution of the universe is given by a unitary operator

  $$U(t,t_0) = \mathrm{e}^{-\mathrm{i}H(t-t_0)}, \qquad |\Psi(t)\rangle = U(t,t_0)\,|\Psi(t_0)\rangle\,.$$

- For QC, we insist that a subblock of the unitary matrix is unitary and decoupled from the rest of the world.
  $\rightarrow$ Experimental problems. Other topic.

- Unitarity also means conservation of probability, i.e. we stay on our Bloch sphere and don't lose states during computation.

Why should we use unitary operators?

- Due to the unreasonable success of quantum mechanics and quantum field theories, e.g.

$$g_{\text{el, theor}} = 2{,}002\,319\,304\,8(8)\,, \quad g_{\text{el, exp}} = 2{,}002\,319\,304\,361\,53(53),$$

  we think that the time evolution of the universe is given by a unitary operator

$$U(t, t_0) = \mathrm{e}^{-\mathrm{i}H(t-t_0)}, \qquad |\Psi(t)\rangle = U(t, t_0)\,|\Psi(t_0)\rangle\,.$$

- For QC, we insist that a subblock of the unitary matrix is unitary and decoupled from the rest of the world.
  $\rightarrow$ Experimental problems. Other topic.

- Unitarity also means conservation of probability, i.e. we stay on our Bloch sphere and don't lose states during computation.

- Introduce Dirac notation: $|0\rangle_3 = |000\rangle, |7\rangle_3 = |111\rangle$.
- Here 1 and 0 represent physical systems with two unambiguously distinguishable states.
- For QC, only unitary operations are relevant. Classical counterpart: reversible operations.
- Only nontrivial reversible operation on one Cbit is NOT:

$$X : |x\rangle \mapsto |\tilde{x}\rangle ; \quad \tilde{1} = 0, \quad \tilde{0} = 1.$$

- $X^2 = 1 \to X$ is reversible and it's own inverse.

- Introduce Dirac notation: $|0\rangle_3 = |000\rangle\,, |7\rangle_3 = |111\rangle$.
- Here 1 and 0 represent physical systems with two unambiguously distinguishable states.
- For QC, only unitary operations are relevant.
  Classical counterpart: reversible operations.
- Only nontrivial reversible operation on one Cbit is NOT:

$$X : |x\rangle \mapsto |\tilde{x}\rangle\,; \quad \tilde{1} = 0, \quad \tilde{0} = 1.$$

- $X^2 = 1 \to X$ is reversible and it's own inverse.

- In our favourite basis of the 2D vector space:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \quad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}, \quad X = \sigma_x \equiv \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$$

- On a pair of Cbits we can also permute or swap:

$$S_{10}\,|xy\rangle = |yx\rangle$$

- Or apply the controlled-NOT or cNOT C_{ij} (aka XOR). Apply NOT on target Cbit j iff the control Cbit i is true.

$$\text{e.g.} \quad C_{01}\,|xy\rangle = |x\rangle\,|(x+y)\text{mod}_2\rangle$$

In matrix representation with the usual tensor product:

$$C_{01} = \begin{bmatrix}\mathbb{1}_{2x2} & 0\\0 & \sigma_x\end{bmatrix} \quad |00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \text{etc.}$$

SWAP and cNOT

- In our favourite basis of the 2D vector space:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad X = \sigma_x \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- On a pair of Cbits we can also permute or swap:

$$S_{10} |xy\rangle = |yx\rangle$$

- Or apply the controlled-NOT or cNOT C_{ij} (aka XOR). Apply NOT on target Cbit j iff the control Cbit i is true.

$$\text{e.g.} \quad C_{01} |xy\rangle = |x\rangle \, |(x + y)\text{mod}_2\rangle$$

  In matrix representation with the usual tensor product:

$$C_{01} = \begin{bmatrix} \mathbb{1}_{2x2} & 0 \\ 0 & \sigma_x \end{bmatrix} \quad |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \text{etc.}$$

Number operator

$$n\,|x\rangle = x\,|x\rangle \qquad \tilde{n} = 1 - n$$

With this, we can rewrite the cNOT as

$$C_{ij} = \tilde{n}_i + X_j n_i$$

and construct $$Z = \tilde{n} - n = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \sigma_z$$

Or by linear combination with the $\mathbb{1}$:

$$n = \frac{1}{2}(\mathbb{1} - \sigma_z) \quad \tilde{n} = \frac{1}{2}(\mathbb{1} + \sigma_z)$$

Number operator

$$n\,|x\rangle = x\,|x\rangle \qquad \tilde{n} = 1 - n$$

With this, we can rewrite the cNOT as

$$C_{ij} = \tilde{n}_i + X_j n_i$$

and construct $$Z = \tilde{n} - n = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \sigma_z$$

Or by linear combination with the $\mathbb{1}$:

$$n = \frac{1}{2}(\mathbb{1} - \sigma_z) \quad \tilde{n} = \frac{1}{2}(\mathbb{1} + \sigma_z)$$

Plugging this in:

$$\begin{aligned} C_{ij} &= \tilde{n}_i + X_j n_i \\ &= \frac{1}{2}\left\{(1 + \sigma_z^i) + \sigma_x^j(1 - \sigma_z^i)\right\} \\ &\overset{i \neq j}{=} \frac{1}{2}\left\{(1 + \sigma_x^j) + \sigma_z^i(1 - \sigma_x^j)\right\} \end{aligned}$$

Which makes it obvious that a swap $i \leftrightarrow j$ can be achieved by $X \leftrightarrow Z$.

The corresponding operator is the Hadamard transformation

$$H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Plugging this in:

$$\begin{aligned} C_{ij} &= \tilde{n}_i + X_j n_i \\ &= \frac{1}{2}\left\{(1 + \sigma_z^i) + \sigma_x^j(1 - \sigma_z^i)\right\} \\ &\stackrel{i \neq j}{=} \frac{1}{2}\left\{(1 + \sigma_x^j) + \sigma_z^i(1 - \sigma_x^j)\right\} \end{aligned}$$

Which makes it obvious that a swap $i \leftrightarrow j$ can be achieved by $X \leftrightarrow Z$.

The corresponding operator is the Hadamard transformation

$$H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Applying the transformation

$H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$

Using $\sigma_x^2 = \sigma_z^2 = 1$ and $\sigma_x\sigma_z = -\sigma_z\sigma_x$ immediately follows:

$$H^2 = \frac{1}{2}\left(1 + \sigma_x\sigma_z + \sigma_z\sigma_x + 1\right) = 1 \qquad \rightarrow H = H^{-1}$$

and

$$H\sigma_x H = \frac{1}{2}\left(\sigma_x + \sigma_z\right)\left(1 + \sigma_x\sigma_z\right) = \sigma_z, \qquad H\sigma_z H = \sigma_x$$

which is the wanted transformation.

Therefore

$$\begin{aligned} C^{ji} &= S^{ij} C^{ij} S^{ij} \\ &= \left(H^i H^j\right) C^{ij} \left(H^i H^j\right) \end{aligned}$$

and we only need a product of two 1-Cbit operators to interchange control and target Cbit.

Applying the transformation

$H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$

Using $\sigma_x^2 = \sigma_z^2 = 1$ and $\sigma_x \sigma_z = -\sigma_z \sigma_x$ immediately follows:

$$H^2 = \frac{1}{2}\left(1 + \sigma_x\sigma_z + \sigma_z\sigma_x + 1\right) = 1 \quad \rightarrow H = H^{-1}$$

and

$$H\sigma_x H = \frac{1}{2}\left(\sigma_x + \sigma_z\right)\left(1 + \sigma_x\sigma_z\right) = \sigma_z, \qquad H\sigma_z H = \sigma_x$$

which is the wanted transformation.

Therefore

$$\begin{aligned} C^{ji} &= S^{ij} C^{ij} S^{ij} \\ &= \left(H^i H^j\right) C^{ij} \left(H^i H^j\right) \end{aligned}$$

and we only need a product of two 1-Cbit operators to interchange control and target Cbit.

Let the general state of n Qbits be any complex superposition of the 2^n different Cbits (classical or computational basis)

$$|\Psi\rangle = \sum_{0 \le x < 2^n} \alpha_x |x\rangle_n ,$$

$$\sum_{0 \le x < 2^n} |\alpha_x|^2 = 1, \qquad \alpha_x \in \mathbb{C}$$

Keep in mind that

$$\begin{aligned} |\Psi\rangle &= |\psi\rangle \otimes |\phi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \\ &= \alpha_0\beta_0 |0\rangle_2 + \alpha_0\beta_1 |1\rangle_2 + \alpha_1\beta_0 |2\rangle_2 + \alpha_1\beta_1 |3\rangle_2 \\ \text{in general} &\neq \alpha_0 |0\rangle_2 + \alpha_1 |1\rangle_2 + \alpha_2 |2\rangle_2 + \alpha_3 |3\rangle_2 \end{aligned}$$

Let the general state of n Qbits be any complex superposition of the 2^n different Cbits (classical or computational basis)

$$|\Psi\rangle = \sum_{0\leq x<2^n} \alpha_x |x\rangle_n ,$$

$$\sum_{0\leq x<2^n} |\alpha_x|^2 = 1, \qquad \alpha_x \in \mathbb{C}$$

Keep in mind that

$$\begin{aligned} |\Psi\rangle &= |\psi\rangle \otimes |\phi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \\ &= \alpha_0\beta_0 |0\rangle_2 + \alpha_0\beta_1 |1\rangle_2 + \alpha_1\beta_0 |2\rangle_2 + \alpha_1\beta_1 |3\rangle_2 \\ \text{in general} &\neq \alpha_0 |0\rangle_2 + \alpha_1 |1\rangle_2 + \alpha_2 |2\rangle_2 + \alpha_3 |3\rangle_2 \end{aligned}$$

Let the general state of n Qbits be any complex superposition of the 2^n different Cbits (classical or computational basis)

$$|\Psi\rangle = \sum_{0 \le x < 2^n} \alpha_x |x\rangle_n ,$$

$$\sum_{0 \le x < 2^n} |\alpha_x|^2 = 1, \qquad \alpha_x \in \mathbb{C}$$

Keep in mind that

$$\begin{aligned} |\Psi\rangle &= |\psi\rangle \otimes |\phi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \\ &= \alpha_0\beta_0 |0\rangle_2 + \alpha_0\beta_1 |1\rangle_2 + \alpha_1\beta_0 |2\rangle_2 + \alpha_1\beta_1 |3\rangle_2 \\ \text{in general} &\neq \alpha_0 |0\rangle_2 + \alpha_1 |1\rangle_2 + \alpha_2 |2\rangle_2 + \alpha_3 |3\rangle_2 \end{aligned}$$

Since $2 + 2 \neq 6$. The general 2-Qbit state doesn't have to be a product of 1-Qbit states which is called entanglement.

Basics of quantum computing

Now on a single Qbit, all unitary transformations are possible

$$uu^{\dagger} = u^{\dagger}u = \mathbb{1}$$

For n Qbits, we could imagine any 2^n-dimensional unitary transformation $U \in \mathrm{U}(2^n)$.

Extend the classical, reversible operations (gates)

NOT SWAP cNOT

by linearity to all complex Qbits since $\{T_{\mathrm{rev}}(n)\} \subset \mathrm{U}(n)$.

Other possibilities are e.g. Z or H.

Now on a single Qbit, all unitary transformations are possible

$$uu^\dagger = u^\dagger u = \mathbb{1}$$

For n Qbits, we could imagine any 2^n-dimensional unitary transformation $U \in \mathrm{U}(2^n)$.

Extend the classical, reversible operations (gates)

NOT SWAP cNOT

by linearity to all complex Qbits since $\{T_{\mathrm{rev}}(n)\} \subset \mathrm{U}(n)$.

Other possibilities are e.g. Z or H.

- It is quite hard to construct an gate/transformation which acts on three quantum states or even more.
- '80 Toffoli has shown that AND and XOR can be made reversible by using 3-Cbit gates. The extra third Cbit is also called garbage.
- Based on this, '89 Deutsch expanded the concept to the whole Hilbert space. $\rightarrow$ Any unitary transformation can be performed using 3-Qbit gates.
- '94 DiVincenzo reduced it to 2-Qbit gates.

- It is quite hard to construct an gate/transformation which acts on three quantum states or even more.
- '80 Toffoli has shown that AND and XOR can be made reversible by using 3-Cbit gates. The extra third Cbit is also called garbage.
- Based on this, '89 Deutsch expanded the concept to the whole Hilbert space. $\rightarrow$ Any unitary transformation can be performed using 3-Qbit gates.
- '94 DiVincenzo reduced it to 2-Qbit gates.

- General idea: Decompose $U(N, \mathbb{C})$ into phases and rotations in $SO(N/2) \to SO(N)$.

- $U(N, \mathbb{C})$ is a Lie group (diff. manifold) with elements like

$$U_\lambda = \begin{bmatrix} \mathbb{1}_{6x6} & & \\ & \cos\lambda & \mathrm{i}\sin\lambda \\ & \mathrm{i}\sin\lambda & \cos\lambda \end{bmatrix} = \mathbb{1}_{6x6} \oplus U_\lambda^2 \neq \mathbb{1}_{4x4} \otimes U_\lambda^2$$

  which is a complex rotation in the plane of $|110\rangle$ and $|111\rangle$.

- Using the concept of infinitesimal generators

$$U = \mathrm{e}^{\mathrm{i}\epsilon H} = \mathbb{1} + \mathrm{i}\epsilon H + \mathcal{O}(\epsilon^2)$$

  and the Lie algebra of the group ($[\circ, \circ] : V \times V \to V$):

$$[H_i, H_j] = \sum_k f_{ijk} H_k$$

- General idea: Decompose $U(N,\mathbb{C})$ into phases and rotations in $SO(N/2) \to SO(N)$.

- $U(N,\mathbb{C})$ is a Lie group (diff. manifold) with elements like

$$U_\lambda = \begin{bmatrix} \mathbb{1}_{6x6} & & \\ & \cos\lambda & \mathrm{i}\sin\lambda \\ & \mathrm{i}\sin\lambda & \cos\lambda \end{bmatrix} = \mathbb{1}_{6x6} \oplus U_\lambda^2 \neq \mathbb{1}_{4x4} \otimes U_\lambda^2$$

  which is a complex rotation in the plane of $|110\rangle$ and $|111\rangle$.

- Using the concept of infinitesimal generators

$$U = \mathrm{e}^{\mathrm{i}\epsilon H} = \mathbb{1} + \mathrm{i}\epsilon H + \mathcal{O}(\epsilon^2)$$

  and the Lie algebra of the group ($[\circ,\circ] : V \times V \to V$):

$$[H_i, H_j] = \sum_k f_{ijk} H_k$$

We may as well express each H_k as commutator of some H_i, H_j. For example

$$\mathrm{e}^{\mathrm{i}\epsilon H_3} = \mathrm{e}^{\mathrm{i}\epsilon(\mathrm{i}[H_1,H_2])} \qquad \left[e^{-X}e^{-Y}e^{X}e^{Y} = e^{[X,Y]}\right]$$
$$\approx \mathrm{e}^{-\mathrm{i}\sqrt{\epsilon}H_1}\mathrm{e}^{-\mathrm{i}\sqrt{\epsilon}H_2}\mathrm{e}^{\mathrm{i}\sqrt{\epsilon}H_1}\mathrm{e}^{\mathrm{i}\sqrt{\epsilon}H_2} + \mathcal{O}(\epsilon^2)$$

using the Baker-Campbell-Hausdorff formula, where

$$\mathrm{e}^{\mathrm{i}\epsilon H_1} = \begin{bmatrix} \mathbb{1}_{4\times 4} & & \\ & A(\epsilon) & \\ & & A(\epsilon) \end{bmatrix} = \begin{bmatrix} \mathbb{1}_{2\times 2} & \\ & A(\epsilon) \end{bmatrix} \otimes \mathbb{1}_{2\times 2}$$

and $A(\epsilon) = \begin{bmatrix} \cos\epsilon & \sin\epsilon \\ -\sin\epsilon & \cos\epsilon \end{bmatrix}$. The rest is mere commutator algebra to obtain all of Deutsch's transformations.

We may as well express each H_k as commutator of some H_i, H_j. For example

$$
\begin{aligned}
\mathrm{e}^{\mathrm{i}\epsilon H_3} &= \mathrm{e}^{\mathrm{i}\epsilon(\mathrm{i}[H_1,H_2])} \qquad\qquad \left[e^{-X}e^{-Y}e^{X}e^{Y} = e^{[X,Y]}\right] \\
&\approx \mathrm{e}^{-\mathrm{i}\sqrt{\epsilon}H_1}\mathrm{e}^{-\mathrm{i}\sqrt{\epsilon}H_2}\mathrm{e}^{\mathrm{i}\sqrt{\epsilon}H_1}\mathrm{e}^{\mathrm{i}\sqrt{\epsilon}H_2} + \mathcal{O}(\epsilon^2)
\end{aligned}
$$

using the Baker-Campbell-Hausdorff formula, where

$$
\mathrm{e}^{\mathrm{i}\epsilon H_1} = \begin{bmatrix} \mathbb{1}_{4\times 4} & & \\ & A(\epsilon) & \\ & & A(\epsilon) \end{bmatrix} = \begin{bmatrix} \mathbb{1}_{2\times 2} & \\ & A(\epsilon) \end{bmatrix} \otimes \mathbb{1}_{2\times 2}
$$

and $A(\epsilon) = \begin{bmatrix} \cos\epsilon & \sin\epsilon \\ -\sin\epsilon & \cos\epsilon \end{bmatrix}$. The rest is mere commutator algebra to obtain all of Deutsch's transformations.

Since this was an first order calculation, we obtain the full unitary operation as

$$U_\lambda = \left(U_{\lambda/n}\right)^n + \mathcal{O}(1/\sqrt{n})$$

similar to ordinary rotations. However this means that arbitrary, unitary transformations on N Qbits need infinitely many 2-Qbit gates or accepting a small error.

We might be better off just restricting ourselves to 2-Qbit gates and leaving the general case for future problems.

Since this was an first order calculation, we obtain the full unitary operation as

$$U_\lambda = \left(U_{\lambda/n}\right)^n + \mathcal{O}(1/\sqrt{n})$$

similar to ordinary rotations. However this means that arbitrary, unitary transformations on N Qbits need infinitely many 2-Qbit gates or accepting a small error.

We might be better off just restricting ourselves to 2-Qbit gates and leaving the general case for future problems.

Circuit diagrams

The initial state is on the left and the result after some transformation on the right.

$$|\Psi\rangle \qquad -\boxed{\mathbf{u}}- \qquad \mathbf{u}\,|\Psi\rangle$$

Applying a 1-Qbit gate u.

$$|\Psi\rangle \qquad -\boxed{\mathbf{U}}- \qquad \mathbf{U}\,|\Psi\rangle$$

Or an n-Qbit gate U.

$$|\Psi\rangle \qquad -\boxed{\mathbf{V}}-\boxed{\mathbf{U}}- \qquad \mathbf{UV}\,|\Psi\rangle$$

Be aware of the order!

Making a von Neumann measurement of the n-Qbit state

$$|\Psi\rangle = \sum_{0 \le x < 2^n} \alpha_x \, |x\rangle_n$$

Collapse of the wave functions. From the measurement, we only get a probabilistic result.

No additional information may be gained.

The initial state is on the left and the result after some transformation on the right.

$|\psi\rangle \quad —\boxed{\mathbf{u}}— \quad \mathbf{u}\,|\psi\rangle$

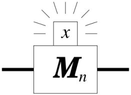
Applying a 1-Qbit gate *u*.

$|\Psi\rangle \quad —\boxed{\mathbf{U}}— \quad \mathbf{U}\,|\Psi\rangle$

Or an *n*-Qbit gate *U*.

$|\Psi\rangle \quad —\boxed{\mathbf{V}}—\boxed{\mathbf{U}}— \quad \mathbf{UV}\,|\Psi\rangle$

Be aware of the order!

$|\Psi\rangle_n = \sum a_x\,|x\rangle_n$  $|x\rangle_n \qquad p = |a_x|^2$

Making a von Neumann measurement of the *n*-Qbit state

$$|\Psi\rangle = \sum_{0\le x<2^n} \alpha_x\,|x\rangle_n$$

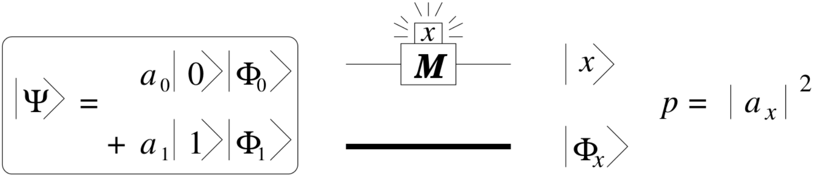
Collapse of the wave functions. From the measurement, we only get a probabilistic result.

No additional information may be gained.

Any state can be expressed as

$$|\Psi\rangle_{n+1} = a_0\,|0\rangle\,|\phi_0\rangle_n + a_1\,|1\rangle\,|\phi_1\rangle_n \qquad |a_0|^2 + |a_1|^2 = 1$$

which allows to formulate the generalized Born rule:



So unentangled states $|\Psi\rangle = |\psi\rangle\,|\phi\rangle$ correspond to $|\phi_0\rangle = |\phi_1\rangle$.

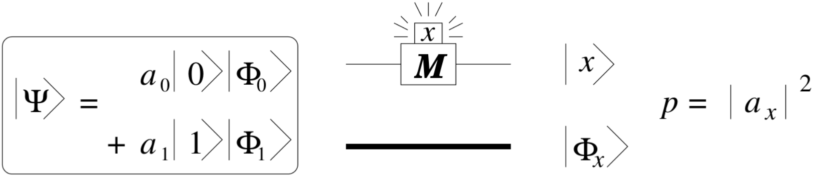
After the measurement, the state will be a product state.

Consequent application of 1-Qbit measurements gives the same result as the *n*-Qbit measurement.
$\rightarrow$ Only 1-Qbit measurement gates.

Any state can be expressed as

$$|\Psi\rangle_{n+1} = a_0 |0\rangle |\phi_0\rangle_n + a_1 |1\rangle |\phi_1\rangle_n \quad |a_0|^2 + |a_1|^2 = 1$$

which allows to formulate the generalized Born rule:



So unentangled states $|\Psi\rangle = |\psi\rangle |\phi\rangle$ correspond to $|\phi_0\rangle = |\phi_1\rangle$.

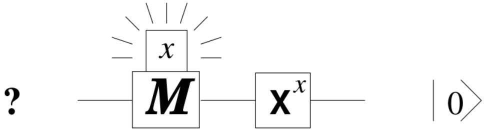
After the measurement, the state will be a product state.

Consequent application of 1-Qbit measurements gives the same result as the *n*-Qbit measurement.
$\rightarrow$ Only 1-Qbit measurement gates.

If Qbits are realized by atoms, $|0\rangle$ might be the lowest-energy state and $|1\rangle$ the first excited.

$\rightarrow |0\rangle_n$ could be realized by cooling down.

For the general case, $|0\rangle_n$ can always be realized with measurement gates:



NOT is applied if $|\psi\rangle = |1\rangle$.

Simple applications

We want to compute a number $f(x)$ represented by m-bit integers from a given number x represented by n-bit integers.

We need $n + m$ Qbits, the input and the output register:

$$U_f\left(|x\rangle_n |0\rangle_m\right) = |x\rangle_n |f(x)\rangle_m$$

So the input remains in its initial state. With the Hadamard transformation $H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$ we can make a trick:

$$\begin{aligned}(H \otimes H)(|0\rangle \otimes |0\rangle) &= (H|0\rangle)(H|0\rangle) \\ &= \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2)\end{aligned}$$

which generalizes clearly: $H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} |x\rangle_n$.

We want to compute a number $f(x)$ represented by m-bit integers from a given number x represented by n-bit integers.

We need $n + m$ Qbits, the input and the output register:

$$U_f\left(|x\rangle_n |0\rangle_m\right) = |x\rangle_n |f(x)\rangle_m$$

So the input remains in its initial state.With the Hadamard transformation $H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$ we can make a trick:

$$\begin{aligned}(H \otimes H)(|0\rangle \otimes |0\rangle) &= (H|0\rangle)(H|0\rangle) \\ &= \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2)\end{aligned}$$

which generalizes clearly: $H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} |x\rangle_n$.

$$H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} |x\rangle_n$$

The *n*-fold Hadamard transformation gives an equally weighted superposition of all possible inputs.

$$\to U_f \left(H^{\otimes n} \otimes \mathbb{1}_m\right) |0\rangle_n |0\rangle_m = \frac{1}{2^{n/2}} \sum_x |x\rangle_n |f(x)\rangle_m$$

If we had $|0\rangle_{100}$ in the input and apply a hundred Hadamard gates before applying U_f, we get a state containing 2^{100} evaluations of f. This is called quantum parallelism.

But there is no way to find out what this state is.

By applying measurement gates, we get with equal probability a certain $|x_0\rangle |f(x_0)\rangle$, similar to a Monte Carlo simulation.

$$H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{0\leq x<2^n} |x\rangle_n$$

The *n*-fold Hadamard transformation gives an equally weighted superposition of all possible inputs.

$$\to U_f\left(H^{\otimes n}\otimes \mathbb{1}_m\right)|0\rangle_n|0\rangle_m = \frac{1}{2^{n/2}}\sum_x |x\rangle_n |f(x)\rangle_m$$

If we had $|0\rangle_{100}$ in the input and apply a hundred Hadamard gates before applying U_f, we get a state containing 2^{100} evaluations of f. This is called quantum parallelism.

But there is no way to find out what this state is.

By applying measurement gates, we get with equal probability a certain $|x_0\rangle\,|f(x_0)\rangle$, similar to a Monte Carlo simulation.

Easy way to avoid this problem:
Copy the result and measure many times.

But the no-cloning theorem states, there is no unitary transformation which takes $|\psi\rangle_n |0\rangle_n \to |\psi\rangle_n |\psi\rangle_n$.

Proof:
If $\quad U(|\psi\rangle |0\rangle) = |\psi\rangle |\psi\rangle \qquad U(|\phi\rangle |0\rangle) = |\phi\rangle |\phi\rangle,$
we get from linearity

$$\begin{aligned} U\,(a\,|\psi\rangle + b\,|\phi\rangle)\,|0\rangle &= a\,U\,|\psi\rangle\,|0\rangle + b\,U\,|\phi\rangle\,|0\rangle \\ &= a\,|\psi\rangle\,|\psi\rangle + b\,|\phi\rangle\,|\phi\rangle \end{aligned}$$

and if U clones arbitrary inputs:

$$\begin{aligned} U\,(a\,|\psi\rangle + b\,|\phi\rangle)\,|0\rangle = a^2\,|\psi\rangle\,|\psi\rangle + b^2\,|\phi\rangle\,|\phi\rangle \\ + ab\,|\psi\rangle\,|\phi\rangle + ba\,|\phi\rangle\,|\psi\rangle \end{aligned}$$

Easy way to avoid this problem:
Copy the result and measure many times.

But the no-cloning theorem states, there is no unitary transformation which takes $|\psi\rangle_n |0\rangle_n \to |\psi\rangle_n |\psi\rangle_n$.

Proof:
If $\quad U(|\psi\rangle |0\rangle) = |\psi\rangle |\psi\rangle \qquad U(|\phi\rangle |0\rangle) = |\phi\rangle |\phi\rangle$,
we get from linearity

$$\begin{aligned} U\,(a\,|\psi\rangle + b\,|\phi\rangle)\,|0\rangle &= a\,U\,|\psi\rangle\,|0\rangle + b\,U\,|\phi\rangle\,|0\rangle \\ &= a\,|\psi\rangle\,|\psi\rangle + b\,|\phi\rangle\,|\phi\rangle \end{aligned}$$

and if U clones arbitrary inputs:

$$\begin{aligned} U\,(a\,|\psi\rangle + b\,|\phi\rangle)\,|0\rangle = a^2\,|\psi\rangle\,|\psi\rangle + b^2\,|\phi\rangle\,|\phi\rangle \\ + ab\,|\psi\rangle\,|\phi\rangle + ba\,|\phi\rangle\,|\psi\rangle \end{aligned}$$

Easy way to avoid this problem:
Copy the result and measure many times.

But the no-cloning theorem states, there is no unitary transformation which takes $|\psi\rangle_n |0\rangle_n \to |\psi\rangle_n |\psi\rangle_n$.

Proof:
If $\quad U(|\psi\rangle\,|0\rangle) = |\psi\rangle\,|\psi\rangle \qquad U(|\phi\rangle\,|0\rangle) = |\phi\rangle\,|\phi\rangle$,
we get from linearity

$$\begin{aligned} U\,(a\,|\psi\rangle + b\,|\phi\rangle)\,|0\rangle &= a\,U\,|\psi\rangle\,|0\rangle + b\,U\,|\phi\rangle\,|0\rangle \\ &= a\,|\psi\rangle\,|\psi\rangle + b\,|\phi\rangle\,|\phi\rangle \end{aligned}$$

and if U clones arbitrary inputs:

$$\begin{aligned} U\,(a\,|\psi\rangle + b\,|\phi\rangle)\,|0\rangle = a^2\,|\psi\rangle\,|\psi\rangle + b^2\,|\phi\rangle\,|\phi\rangle \\ + ab\,|\psi\rangle\,|\phi\rangle + ba\,|\phi\rangle\,|\psi\rangle \end{aligned} \qquad \square$$

There are more clever things one can do in QC. Especially if one is interested in relations between different $f(x)$.

Let's take an 1-Qbit input and an 1-Qbit output register. In the basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, there are four possible distinct functions $f_j(x)$:

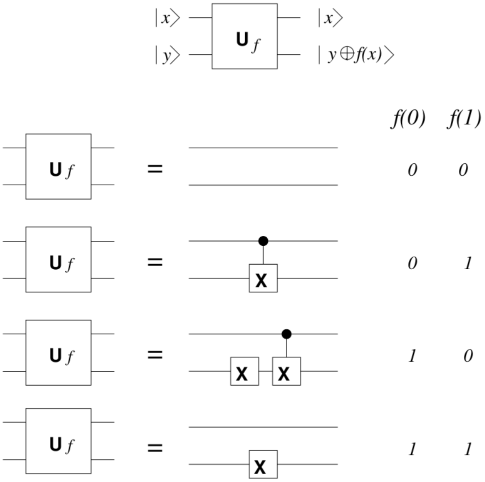
$$U_{f_0} = \mathbb{1}_{4\times 4}, \quad U_{f_1} = C_{io}, \quad U_{f_2} = C_{io}X_o, \quad U_{f_3} = X_o$$

	$x=0$	$x=1$
f_0	0	0
f_1	0	1
f_2	1	0
f_3	1	1

$$U_f\left(|x\rangle\,|y\rangle\right) = |x\rangle\,|(y+f(x))\mathrm{mod}_2\rangle$$

Pretend, we have a black box that executes one U_f but we are not told which one. What can we learn?

Deutsch's problem



If we want to know if f is constant ($f(0) = f(1)$), satisfied by f_0 and f_3, ...

On a classical computer, we have to run U_f twice and compare results.

On a quantum computer, we may apply some additional transformations.

$$
\begin{aligned}
&U_f\,(H\otimes H)\,(X\otimes X)\,(|0\rangle\,|0\rangle)\\
&\quad= U_f\,(H\otimes H)\,(|1\rangle\,|1\rangle)\\
&\quad= U_f\frac{1}{2}\big(|0\rangle-|1\rangle\big)\big(|0\rangle-|1\rangle\big)\\
&\quad= \frac{1}{2}\Big(U_f\,|00\rangle-U_f\,|10\rangle-U_f\,|01\rangle+U_f\,|11\rangle\Big)\\
&\quad= \frac{1}{2}\left(|0f(0)\rangle-|1f(1)\rangle-\left|0\tilde{f}(0)\right\rangle+\left|1\tilde{f}(1)\right\rangle\right)
\end{aligned}
$$

where $\tilde{f}(x)=(1+f(x))\mathrm{mod}_2$. So for $f(0)=f(1)$ we have

$$\frac{1}{2}\big(|0\rangle-|1\rangle\big)\left(|f(0)\rangle-\left|\tilde{f}(0)\right\rangle\right)$$

and for $f(0)\neq f(1)$

$$\frac{1}{2}\big(|0\rangle+|1\rangle\big)\left(|f(0)\rangle-\left|\tilde{f}(0)\right\rangle\right)$$

$$
\begin{aligned}
& U_f\,(H \otimes H)\,(X \otimes X)\,(|0\rangle\,|0\rangle) \\
&\quad = U_f\,(H \otimes H)\,(|1\rangle\,|1\rangle) \\
&\quad = U_f \frac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|0\rangle - |1\rangle\right) \\
&\quad = \frac{1}{2}\Big(U_f\,|00\rangle - U_f\,|10\rangle - U_f\,|01\rangle + U_f\,|11\rangle\Big) \\
&\quad = \frac{1}{2}\left(|0f(0)\rangle - |1f(1)\rangle - \left|0\tilde{f}(0)\right\rangle + \left|1\tilde{f}(1)\right\rangle\right)
\end{aligned}
$$

where $\tilde{f}(x) = (1 + f(x))\mathrm{mod}_2$. So for $f(0) = f(1)$ we have

$$\frac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|f(0)\rangle - \left|\tilde{f}(0)\right\rangle\right)$$

and for $f(0) \neq f(1)$

$$\frac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|f(0)\rangle - \left|\tilde{f}(0)\right\rangle\right)$$

So with one more Hadamard transform on the input, we get

$$(H \otimes \mathbb{1})\, U_f\, (H \otimes H)\, (X \otimes X)\, (|0\rangle\, |0\rangle) =$$
$$\begin{cases} |1\rangle \frac{1}{\sqrt{2}} \left(|f(0)\rangle - \left|\tilde{f}(0)\right\rangle \right), & f(0) = f(1) \\ |0\rangle \frac{1}{\sqrt{2}} \left(|f(0)\rangle - \left|\tilde{f}(0)\right\rangle \right), & f(0) \neq f(1) \end{cases}$$

The input register tells us in a single run if $f(0) = f(1)$ or not. But we lost every information what value $f(0)$ or $f(1)$ actually is.

f(x) could characterize any two-valued property of the output of an subroutine. E.g. the millionth bit in the expansion of $\sqrt{2+x}$.

Deutsch's problem becomes the nontrivial question of wether the millionth bits of $\sqrt{2}$ and $\sqrt{3}$ agree or not.

So with one more Hadamard transform on the input, we get

$$(H \otimes \mathbb{1})\, U_f\, (H \otimes H)\, (X \otimes X)\, (|0\rangle\, |0\rangle) = \begin{cases} |1\rangle\, \frac{1}{\sqrt{2}} \left(|f(0)\rangle - \left| \tilde{f}(0) \right\rangle \right), & f(0) = f(1) \\ |0\rangle\, \frac{1}{\sqrt{2}} \left(|f(0)\rangle - \left| \tilde{f}(0) \right\rangle \right), & f(0) \neq f(1) \end{cases}$$

The input register tells us in a single run if $f(0) = f(1)$ or not.
But we lost every information what value $f(0)$ or $f(1)$ actually is.

f(x) could characterize any two-valued property of the output of an subroutine. E.g. the millionth bit in the expansion of $\sqrt{2 + x}$.

Deutsch's problem becomes the nontrivial question of wether the millionth bits of $\sqrt{2}$ and $\sqrt{3}$ agree or not.

Conclusion

- Quantum gates are represented by unitary transformations
- Quantum computing allows completely new algorithms
- Important topics which haven't been covered:
  - Experimental realization
  - Shor algorithm
  - Quantum-error correction
  - Elaboration of entanglement
  - Grover-Search algorithm

Conclusion

- Quantum gates are represented by unitary transformations
- Quantum computing allows completely new algorithms
- Important topics which haven't been covered:
  - Experimental realization
  - Shor algorithm
  - Quantum-error correction
  - Elaboration of entanglement
  - Grover-Search algorithm

Literature

N. David Mermin
Quantum Computer Science.

David P. DiVincenzo
Two-bit gates are universal for quantum computation
Phys. Rev. A 51, 1995 **1015-1022**