Quantum Computing

Prof. Dr. Jean-Pierre Seifert
jpseifert@sec.t-labs.tu-berlin.de
http://www.sec.t-labs.tu-berlin.de/
Outline for this lecture

Simon’s Problem
Recap from last lecture
Deutsch-Jozsa Promise Problem

- Given a function \( f : \{0, 1\}^n \rightarrow \{0, 1\} \), as a black box, that is (promised to be) balanced or constant. Decide which property \( f \) has.

- Classical deterministic computers need, in the worst case, exponential time to solve the problem.

- Surprisingly, there is a quantum algorithm to solve the problem by applying \( f \) only once.
Deutsch-Jozsa Promise Problem

- Let us consider one quantum register with \( n \) qubits and apply the Hadamard transformation \( H_n \) to this register. This yields

\[
|0^n\rangle \xrightarrow{H_n} |\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle
\]

- By applying now the transformation \( V_f \) (only on this register?!) we get

\[
V_f |\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} |i\rangle \overset{\text{def}}{=} |\phi_1\rangle
\]

- What has been achieved by these operations?
  - The values of \( f \) were transferred to their amplitudes.
Deutsch-Jozsa Promise Problem

- The former fact can be utilized, through the power of quantum superposition and a proper observable, as follows.
- Let us consider the observable $\mathcal{D} = \{E_a, E_b\}$, where $E_a$ is the one-dimensional subspace spanned by the vector $|\Psi_a\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$.
- and $E_b = (E_a)\perp$. The projection of $|\phi_1\rangle$ onto $E_a$ and $E_b$ has the form
  $$|\phi_1\rangle = \alpha |\Psi_a\rangle + \beta |\Psi_b\rangle \text{ with } |\alpha|^2 + |\beta|^2 = 1,$$
  where $|\Psi_b\rangle$ is a vector in $E_b$ such that $|\Psi_b\rangle \perp |\Psi_a\rangle$.
- Thus, a measurement by $\mathcal{D}$ provides “the value $a$ or $b$” with probability $|\alpha|^2$ or $|\beta|^2$. 
Deutsch-Jozsa Promise Problem

- It is easy to determine $\alpha$ from

$$|\phi_1\rangle = \alpha |\Psi_a\rangle + \beta |\Psi_b\rangle \quad \text{with} \quad |\alpha|^2 + |\beta|^2 = 1,$$

using the above projection of $|\phi_1\rangle$ onto $E_a$ by the computation

$$\alpha = \langle \Psi_a | \phi_1 \rangle.$$
Indeed

\[ \alpha = \langle \Psi_a \mid \phi_1 \rangle \]

\[ = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \langle i \mid \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{f(j)} | j \rangle \]

\[ = \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} (-1)^{f(j)} \langle i \mid j \rangle \]

\[ = \frac{1}{2^n} \sum_{j=0}^{2^n-1} (-1)^{f(j)} \]

because \( \langle i \mid j \rangle = 1 \) if and only if \( i = j \) and \( 0 \) otherwise.
Deutsch-Jozsa Promise Problem

- Yet, we have
  \[ \alpha = \frac{1}{2^n} \sum_{j=0}^{2^n-1} (-1)^{f(j)}. \]

- If \( f \) is balanced, then the sum for \( \alpha \) contains the same number of 1s and \( -1 \)s and therefore \( \alpha = 0 \). A measurement of \( |\phi_1\rangle \) with respect to \( D \), therefore provides, for sure, the outcome \( b \).

- If \( f \) is constant, then either \( \alpha = 1 \) or \( \alpha = -1 \) and therefore the measurement of \( |\phi_1\rangle \) with respect to \( D \) always gives the outcome \( a \).

- A single measurement of \( |\phi_1\rangle \), with respect to \( D \), therefore provides the solution of the problem with probability 1.
Deutsch-Jozsa – second solution

- If the Hadamard transformation is applied to the state $|\phi_1\rangle$ we get

$$H_n |\phi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} |u\rangle = \frac{1}{\sqrt{2^n}} \sum_{u=0}^{2^n-1} (-1)^u |i\rangle (-1)^{f(i)} |u\rangle$$

- If $f$ is constant, then

$$\sum_{i=0}^{2^n-1} (-1)^{u \cdot i} = \begin{cases} 0 & \text{if } u \neq 0 \\ 2^n & \text{if } u = 0 \end{cases}$$

- If $f$ is balanced, then

$$\sum_{i=0}^{2^n-1} (-1)^{u \cdot i}(-1)^{f(i)} = 0 \text{ if and only if } u = 0.$$  

- One measurement therefore shows with prob. 1 whether $f$ is balanced or not.

I.e., $H_n |\phi_1\rangle = |0\rangle$ with prob. 1 iff. $f$ is constant.
Deutsch-Jozsa – randomized solution

- It is easy to show that though deterministic algorithms to solve the Deutsch-Jozsa problem for $n = 2^k$ require $2^{k-1} + 1$ queries in the worst case, there are probabilistic algorithms to solve this problem relatively fast, if we are willing to tolerate some error.
  - Indeed, a randomized algorithm can solve the Deutsch-Jozsa problem with probability of error at most $1/3$ with only two queries.
  - The probability of error can be reduced to less than $1/2^k$ with only $k + 1$ queries.

- Therefore, in spite of the fact that there is an exponential gap between deterministic classical and exact quantum query complexity, the gap between randomized classical complexity and quantum query complexity is in this case constant in the case of constant error.
The next milestone in QC was

Simon’s Problem
Simon’s Problem

- Simon has discovered a simple problem with an expected quantum polynomial time algorithm, but having no polynomial time randomized algorithm.

- Let $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a function such that either $f$ is one-to-one or $f$ is two-to-one and there exists a single $0 \neq s \in \{0, 1\}^n$ such that

  $$\forall x \neq x' \ (f(x) = f(x') \iff x' = x \oplus s).$$

- The task is to determine which of the above conditions holds for $f$ and, in the second case, to determine also $s$.

- To solve the problem two registers are used, both with $n$ qubits, and the initial states $|0^n\rangle$, and (expected) $O(n)$ repetitions of the following version of the so-called Hadamard-twice scheme:
Simon’s Problem

- Apply the Hadamard transformation on the first register with the initial value $|0^n\rangle$, to produce the superposition

$$|0^n, 0^n\rangle \xrightarrow{H_n} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x, 0^n\rangle .$$

- Apply $U_f$ to compute $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x, f(x)\rangle$.

- Apply Hadamard transformation on the first register to get

$$\frac{1}{2^n} \sum_{x, y \in \{0, 1\}^n} (-1)^{x \cdot y} |y, f(x)\rangle .$$

- Observe the resulting state to get a pair $(y, f(x))$. 
Case 1:

- \( f \) is one-to-one. After performing the first three steps of the above procedure all possible states \(|y, f(x)\rangle\) in the superposition are distinct and the absolute value of their amplitudes is the same, namely \(2^{-n}\).

- \( n - 1 \) independent applications of the above scheme (Hadamard-twice) therefore produce \( n - 1 \) pairs \((y_1, f(x_1)), \ldots, (y_{n-1}, f(x_{n-1}))\), distributed uniformly and independently over all \(2^n\) possible pairs \((y, f(x))\).
Case 2:

- \( f \) is two-to-one. I.e., there is some \( 0 \neq s \in \{0, 1\}^n \) such that
  \[ \forall x \neq x' \ ( f(x) = f(x') \iff x' = x \oplus s ). \]

- In such a case for each \( y \) and \( x \) the states \( |y, f(x)\rangle \) and \( |y, f(x \oplus s)\rangle \) are identical. Their total amplitude \( \alpha(x, y) \) has the value
  \[ \alpha(x, y) = 2^{-n} ( (-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y} ). \]

- If \( y \cdot s \equiv 0 \mod 2 \),
  - then \( x \cdot y \equiv (x \oplus s) \cdot y \mod 2 \) and therefore \( |\alpha(x, y)| = 2^{-n+1} \);
  - otherwise \( \alpha(x, y) = 0 \).

- \( n - 1 \) independent applications of the above scheme (Hadamard-twice) therefore yield \( n - 1 \) independent pairs \( (y_1, f(x_1)), \ldots, (y_{n-1}, f(x_{n-1})) \) such that \( y_i \cdot s \equiv 0 \mod 2 \), for all \( 1 \leq i \leq n - 1 \).
In both cases, after \( n - 1 \) repetitions of the above scheme (Hadamard-twice), \( n - 1 \) vectors \( y_i, 1 \leq i \leq n - 1 \), are obtained.

If these vectors are linearly independent, then the system of \( n - 1 \) linear equations over \( \mathbb{Z}_2 \), i.e.,
\[
y_i \cdot s \equiv 0 \mod 2
\]
can be solved to obtain \( s \).

- \( f \) is two-to-one, \( s \) obtained in such a way is the one to be found.
- \( f \) is one-to-one, \( s \) obtained in such a way is a random string.

To distinguish these two cases, it is enough to compute \( f(0) \) and \( f(s) \).

- If \( f(0) \neq f(s) \), then \( f \) is one-to-one.

If the vectors obtained by this scheme are not linearly independent, then the whole process has to be repeated.
Show that each classical algorithm needs to perform $\Omega(\sqrt{2^n})$ queries to solve Simon’s problem.
Computational Power of Entanglement

- As illustrated in the following examples, in some cases there is a clever way to make use of quantum entanglement to compute efficiently some global properties of a function.

- Let a function \( f : \{1, \ldots, n\} \rightarrow \{0, 1\} \) be given as a black box.

- To determine \( f \) classically, \( n \) calls of \( f \) are needed - to get the string \( w_f = f(1) \, f(2) \, \ldots \, f(n) \).

- Quantumly, this can be done, with probability greater than 0.95, using \( n/2 + \sqrt{n} \) quantum calls of \( f \).

- Indeed, on the base of equality

\[
|w_f\rangle = H_n \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} (-1)^{x \cdot w_f} |x\rangle,
\]

- in order to compute \( x \cdot w_f \) one needs \( \text{hw}(x) \) calls of \( f \), where \( \text{hw}(x) \) is the Hamming weight of \( x \).
The trick is to compute the former identity but only for \( x \) such that \( h_w(x) \leq k \), for a suitable \( k \).

If \( F_k \) is such a function that for \( x \in \{0, 1\}^n \),

\[
F_k(x) = \begin{cases} 
  x \cdot w_f & \text{if } h_w(x) \leq k \\
  0; & \text{otherwise}
\end{cases}
\]

then

\[
V_{F_k}|x\rangle = \begin{cases} 
  (-1)^x \cdot w_f |x\rangle & \text{if } h_w(x) \leq k \\
  |x\rangle; & \text{otherwise}
\end{cases}
\]

Therefore, if \( V_{F_k} \) is applied to the (initial) state

\[
|\psi_k\rangle = \frac{1}{\sqrt{M_k}} \sum_{x \in \{0,1\}^n} |x\rangle,
\]

where \( M_k = \sum_{i=0,...,k} \binom{n}{i} \),
Then

$$|\psi'_k\rangle = V_{F_k} |\psi_k\rangle = \frac{1}{\sqrt{M_k}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot w_f} |x\rangle.$$ 

In order to compute $|\psi'_k\rangle$, at most $k$ calls of $f$ are needed. Let us now measure all $n$ qubits of $|\psi''_k\rangle = H_n |\psi'_k\rangle$.

The probability that this way we get $w_f$ is

$$\Pr[|\psi''_k\rangle \text{ yields at measurement } w_f] = |\langle w_f | \psi''_k\rangle|^2$$

$$= M_k / 2^n$$

$$= \sum_{i=0,\ldots,k} \binom{n}{i} / 2^n$$

and, as one can easily calculate, this probability is more than 0.95 if $k = n/2 + \sqrt{n}$. 

21
The Quantum Fourier Transform is a quantum variant of the Discrete Fourier Transform (DFT).

It maps a discrete function to another discrete one with equally distant points as its domain.

For example it maps a $q$-dimensional complex 

$$(f(0), f(2), \ldots, f(q-1))$$

into $(\bar{f}(0), \bar{f}(2), \ldots, \bar{f}(q-1))$ where

$$\bar{f}(c) = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} e^{2\pi i ac/q} f(a)$$

and $c \in \{0, \ldots, q-1\}$. 
The quantum version of DFT (QFT) is the unitary transformation

\[
\text{QFT}_q : |x\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} e^{2\pi i ax/q} |a\rangle,
\]

\(x \in \{0, \ldots, q-1\}\) for the unitary matrix

\[
F_q = \frac{1}{\sqrt{q}} \begin{pmatrix}
1 & 1 & 1 & \ldots & 1 \\
1 & \omega & \omega^2 & \ldots & \omega^{(q-1)} \\
1 & \omega^2 & \omega^4 & \ldots & \omega^{2(q-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{(q-1)} & \omega^{2(q-1)} & \ldots & \omega^{(q-1)^2}
\end{pmatrix},
\]

and \(\omega = e^{2\pi i/q}\) is the \(q^{th}\) root of unity.
Property of QFT

- If applied to a quantum superposition, $\text{QFT}_q$ performs as

$$\text{QFT}_q : \sum_{a=0}^{q-1} f(a) \ket{a} \rightarrow \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \overline{f}(c) \ket{c},$$

$$= \frac{1}{\sqrt{q}} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \sum_{a=0}^{q-1} e^{2\pi i ac/q} f(a) \ket{c}$$

where $\overline{f}(c)$ is as defined as before.

- Note that

$$\text{QFT}_q : \ket{0^n} \rightarrow \frac{1}{\sqrt{q}} \sum_{i=0}^{q-1} \ket{i}.$$
Outline for next lecture

QFT and Shor’s factoring algorithm
Questions?