Quantum Computing

Introduction & recent developments

Stephan Spindler Janos Tapolczai Dominik Theuerkauf

May 12, 2014

Contents

1. Mathematics
    - Representation of qubits
    - Several qubits
    - Quantum gates
    - Deutsch's problem
    - No-cloning theorem
2. Algorithms
    - Shor's algorithm
    - Grover's algorithm
    - Element distinctness problem
3. How to buld a quantum computer?
4. Recent developments

Mathematics

What is . . . ?

- **Quantum Information**
  It is physical information being held in the state of a **quantum system**.
- **Quantum Computing**
  The idea behind quantum computing is using **superposition** of **quantum states** for massively parallel **computing**.
- **Qubit**
  It is a unit of **quantum information** — analogue to the classical bit.

Mathematics

What is . . . ?

- **Quantum state**
  In a physical point of view, it is any state in a **quantum-mechanical system**, such as movement of an electron in an hydrogen-atom. Mathematically, it is described by an abstract "ket"-vector $|\psi\rangle$ with $|\psi\rangle \in L^2$ (Hilbertspace).
- **Superposition**
  This is a fundamental principle of **quantum mechanics** that a physical system exists partly in all its theoretically possible **states** simultaneously. However, when the system gets measured (observed), the superposition collapses into only one of the possible configurations.

Representation of **vectors** in **Dirac-notation**

- Quantum states written as "bra-ket"
  bra-vector $\psi^* \dots \langle\psi|$
  ket-vector $\Phi \dots |\Phi\rangle$
- Easy to use: a physical view of e^- **Spins**
  Spin **up**: $\dots |\uparrow\rangle$ or $|0\rangle$
  Spin **down**: $\dots |\downarrow\rangle$ or $|1\rangle$
- 2-dim. basis states: $|\uparrow\rangle$, $|\downarrow\rangle \in \mathcal{H}$
  (comparably: unit vectors $\vec{e_i} \in \mathbb{R}^n$)

Some **properties** of **bra-kets** in **Dirac-notation** of spin-vectors

- Hermitian conjugation (dual vector space)
  with $c \in \mathbb{C}$

$$c^* \langle\psi| = (c\,|\psi\rangle)^\dagger \tag{1}$$

$$c\,|\psi\rangle = (c^* \langle\psi|)^\dagger \tag{2}$$

- Orthonormality

$$\langle n|m\rangle = \delta_{nm} \tag{3}$$

$$\|\ \langle n|\ \| = \|\ |n\rangle\ \|\ = 1 \tag{4}$$

- Completeness

$$\sum_n |n\rangle \langle n| = \hat{\mathbb{1}} \tag{5}$$

Representation of **qubits**

- Superposition of quantum state (1 qubit) with α, $\beta \in \mathbb{C}$

  $$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{6}$$

  A **qubit** can be represented as a linear combination of **basis states** $|0\rangle$ and $|1\rangle$. Due to orthonormality eqn. (3), it must be granted

  $$\langle\psi|\psi\rangle = 1 \tag{7}$$

  That means

  $$|\alpha|^2 + |\beta|^2 = 1 \tag{8}$$

  So α, β can be interpreted as **probability amplitudes**.

Sample pure **qubit** visualisation by a **Bloch sphere**

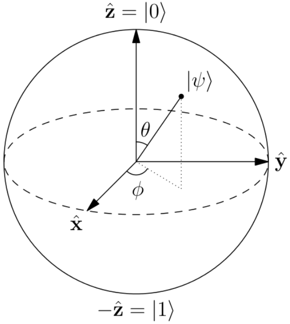


Figure 1 : Unit sphere S^2 with spherical coordinates θ, ϕ.

$$|\psi\rangle = \cos\frac{\theta}{2}e^{-i\phi}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle \tag{9}$$

Measurement of **quantum states**

- **Projection operator**: $\hat{P}_n = |n\rangle \langle n|$, idempotent

$$\langle n| \hat{P}_n |\psi\rangle = \alpha_n \tag{10}$$

- **Density operator** describes a quantum system in **mixed state** (statistical ensemble of several quatum states)

$$\hat{\rho} = \sum_n p_n |\psi_n\rangle \langle\psi_n| \tag{11}$$

Pure state only if $Tr(\hat{\rho}^2) = 1$ or $\hat{\rho}$ is idempotent.

Measurement of **quantum states**

- **Expectation value**: Let $\hat{A}$ be an **observable** of a quantum system, assuming the ensemble is in mixed state such that each pure state $|\psi_n\rangle$ occurs with a probability p_n, the density operator is like in eqn.(11). The expection value of the measurement calculates as

$$\begin{aligned}\langle\hat{A}\rangle &= \sum_n p_n \langle\psi_n|\hat{A}|\psi_n\rangle = \sum_n Tr\left(p_n |\psi_n\rangle\langle\psi_n| \hat{A}\right) \\ &= Tr\left(\sum_n p_n |\psi_n\rangle\langle\psi_n| \hat{A}\right) = Tr\left(\hat{\rho}\hat{A}\right)\end{aligned} \tag{12}$$

Tensor product in **Hilbert space**

- Let $\mathcal{H}_j \subseteq \mathcal{H}$ be a Hilbert space and with basis vectors $\left|n\right\rangle_j \in \mathcal{H}_j$ representing a complete orthonormal system. Then, the Tensor product $\left|ij\right\rangle$ will be $\left|ij\right\rangle \in \mathcal{H}_i \bigotimes \mathcal{H}_j$

$$\left|nm\right\rangle := \left|n\right\rangle_i \left|m\right\rangle_j = \left|n\right\rangle_i \otimes \left|m\right\rangle_j \tag{13}$$

- Example, using presentation of spins (2 Qubits) obtaining following set

$$\{\left|0\right\rangle \otimes \left|0\right\rangle, \left|0\right\rangle \otimes \left|1\right\rangle, \left|1\right\rangle \otimes \left|0\right\rangle, \left|1\right\rangle \otimes \left|1\right\rangle\}$$

$$\left|01\right\rangle = \left|0\right\rangle \left|1\right\rangle = \left|0\right\rangle_1 \left|1\right\rangle_2 = \left|0\right\rangle_1 \otimes \left|1\right\rangle_2$$

Qubits

- **Superposition**: composition of 2 qubits
  Consider $|\vartheta\rangle_1 = \alpha\,|0\rangle_1 + \beta\,|1\rangle_1$, $|\phi\rangle_2 = |1\rangle_2$, $\alpha, \beta \in \mathbb{C}$

$$|\psi\rangle = |\vartheta\phi\rangle = (\alpha\,|0\rangle_1 + \beta\,|1\rangle_1)\,|1\rangle_2 = \alpha\,|01\rangle + \beta\,|11\rangle$$

- **Entanglement**: Quantum state is not reachable by tensor product. Examples:

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{|\alpha|^2 + |\beta|^2}}\,(\alpha\,|00\rangle + \beta\,|11\rangle) \\ |\phi\rangle_\pm &= \frac{1}{\sqrt{2}}\,(|01\rangle \pm |10\rangle) \end{aligned} \tag{14}$$

Measurement of Spins of m-qubits

- Assuming observable operator $\hat{E}_j$ with $\{j \in \mathbb{N} | 0 \leqslant j \leqslant m\}$
  Projection on standard basis $\{|0\rangle, |1\rangle\}^n$

$$\hat{E}_j |n_0 n_1 \dots n_m\rangle = n_j |n_0 n_1 \dots n_m\rangle$$

- Example: 2 qubits

quantum state $\lvert\psi\rangle$	measurement $\hat{E}_1$	measurement $\hat{E}_2$
$\lvert 01\rangle$	0	1
$\lvert 10\rangle - \lvert 11\rangle$	1	$0 \vee 1$
$\lvert 00\rangle + \lvert 10\rangle$	$0 \vee 1$	0
$\lvert 00\rangle + \lvert 11\rangle$	$0 \vee 1$	$0 \vee 1$

Unitary operations with **gates**

- To compute on quantum states, we will use unitary operations. Input qubits $\longrightarrow$ compute $\longrightarrow$ output qubits (measurement).
- **Unitary operators** preserve the norm of the quantum system. It executes a rotation of $|\psi\rangle$ in spin-space **surface of Blochsphere**.

$$\| \hat{U} |\psi\rangle \| = \| |\psi\rangle \| \tag{15}$$

- properties: $\hat{U}^\dagger = \hat{U}^{-1}$

$$\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \hat{U}^{-1}\hat{U} = \hat{U}\hat{U}^{-1} = \hat{\mathbb{1}} \tag{16}$$

Not-gate

- A **not-gate** converts one basis state into another: $|0\rangle \longrightarrow |1\rangle$ and $|1\rangle \longrightarrow |0\rangle$. Mathematically written

$$\begin{aligned} \hat{N}\,|0\rangle &= |1\rangle \\ \hat{N}\,|1\rangle &= |0\rangle \end{aligned} \tag{17}$$

With superposition $|\psi\rangle_\pm = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right)$ the output of the not-gate is

$$\hat{N}\,|\psi\rangle_\pm = \frac{1}{\sqrt{2}}\hat{N}\left(|0\rangle \pm |1\rangle\right) = \frac{1}{\sqrt{2}}\left(|1\rangle \pm |0\rangle\right) = \pm\,|\psi\rangle_\pm \tag{18}$$

Controlled not-gate

- A **controlled not-gate** takes effect on a 2-qubit state and only if the first qubit is in state $|1\rangle$ the second qubit becomes changed.

$$\hat{N}_c |n\rangle |m\rangle = |n\rangle |(n+m) \mod 2\rangle \tag{19}$$

- Examples:

$$\begin{aligned} \hat{N}_c |00\rangle &= |00\rangle \\ \hat{N}_c |11\rangle &= |10\rangle \\ \hat{N}_c \left(\frac{1}{\sqrt{2}}(|00\rangle \pm |10\rangle) \right) &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \end{aligned} \tag{20}$$

Hadamard transform

- The Hadamard transform is needed to create superposition states out of basis states. It can be written as

$$\hat{H}\left|n\right\rangle = \frac{1}{\sqrt{2}}\sum_{m}(-1)^{nm}\left|m\right\rangle \tag{21}$$

- the affect on basis states $\left|0\right\rangle, \left|1\right\rangle$

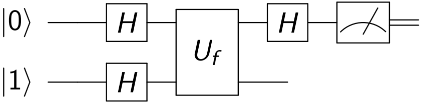
$$\begin{aligned} \hat{H}\left|0\right\rangle &= \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) \\ \hat{H}\left|1\right\rangle &= \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) \end{aligned} \tag{22}$$

Deutsch's problem

- Deutsch's algorithm for distinguishing between constant and balanced functions: For each arbitrary function $f : \{0, 1\} \longrightarrow \{0, 1\}$, we define the unitary operation

$$\hat{U}_f \left|n\right\rangle \left|m\right\rangle = \left|n\right\rangle \left|(m + f(n)) \mod 2\right\rangle \tag{23}$$

- using a quantum circuit which solves the problem:



Deutsch's problem

- Compute with input $|0\rangle\,|1\rangle$

$$
\begin{aligned}
|01\rangle &\to \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\
&\to \frac{1}{2}\left((-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle\right)(|0\rangle - |1\rangle) \\
&\to \frac{1}{2}\Big[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \\
&\qquad + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\Big]\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}
\tag{24}
$$

- Measuring the first qubit, we find the outcome $|0\rangle$ with probability 1 if $f(0) = f(1)$ (**const.** func.) and the outcome $|1\rangle$ with expection value 1 if $f(0) \neq f(1)$ (**balanced** func.)

No cloning theorem

- Important for quantum informatics, as no classical error correction codes are possible-
- Is the basis for quantum cryptography.
- Proof: Assuming perfect copies by an unitary operation of arbitrary qubits. 2 arbitrary quantum states $|\phi\rangle, |\psi\rangle \rightarrow$ transferred to independent state $|\lambda\rangle$
  Copying:

$$\hat{U}(|\phi\rangle \otimes |\lambda\rangle) = |\phi\rangle \otimes |\phi\rangle \tag{25}$$

$$\hat{U}(|\psi\rangle \otimes |\lambda\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{26}$$

No cloning theorem

- Scalar product:

$$\begin{aligned}\langle(\phi\otimes\lambda)|(\psi\otimes\lambda)\rangle &= \langle(\phi\otimes\lambda)|\hat{U}^{\dagger}\hat{U}|(\psi\otimes\lambda)\rangle \\ &= \langle(\phi\otimes\phi)|(\psi\otimes\psi)\rangle\end{aligned} \tag{27}$$

$$\begin{aligned}\langle(\phi\otimes\lambda)|(\psi\otimes\lambda)\rangle = \langle\phi|\psi\rangle\,\langle\lambda|\lambda\rangle = \langle\phi|\psi\rangle \\ \langle(\phi\otimes\phi)|(\psi\otimes\psi)\rangle = \langle\phi|\psi\rangle\,\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^{2}\end{aligned} \tag{28}$$

- So $\langle\phi|\psi\rangle^2 = \langle\phi|\psi\rangle$, $\Rightarrow$ solutions: $\langle\phi|\psi\rangle = 0$ or $\langle\phi|\psi\rangle = 1$ $\Rightarrow$ $|\phi\rangle$ is an orthogonal state of $|\psi\rangle$ or $|\phi\rangle = |\psi\rangle$.
- It is not possible to copy **arbitrary states**.

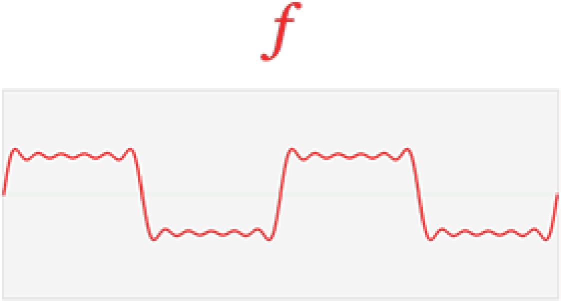
Algorithms

Algorithms

- Quantum algorithms use a number of techinques, e.g.
  - Quantum Fourier Transform (QFT)
  - Amplitude Amplification
  - Quantum Walks
- These often take $\Omega(2^n)$ time on classical computers,
- but often only $O(n^k)$ on quantum computers*.
  - * given certain assumptions.

Fourier Transform

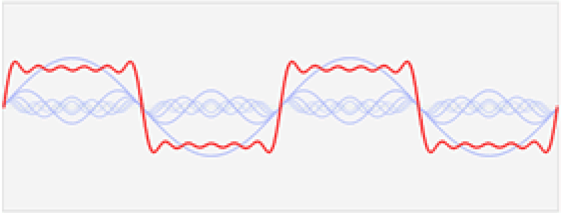
- The Fourier series decomposes a function $f : \mathbb{R} :\to \mathbb{C}$ into periodic components.



Fourier Transform

- The Fourier series decomposes a function $f : \mathbb{R} :\to \mathbb{C}$ into periodic components.

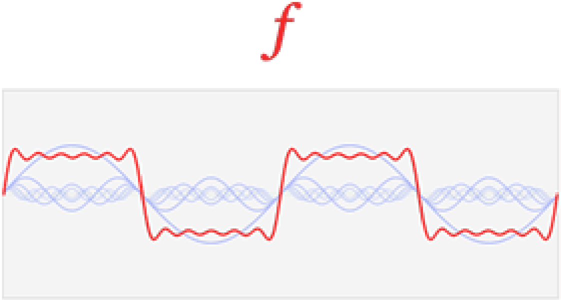
$$f$$



$$a_n \cos(nx) + b_n \sin(nx)$$

Fourier Transform

- The Fourier series decomposes a function $f : \mathbb{R} :\rightarrow \mathbb{C}$ into periodic components.

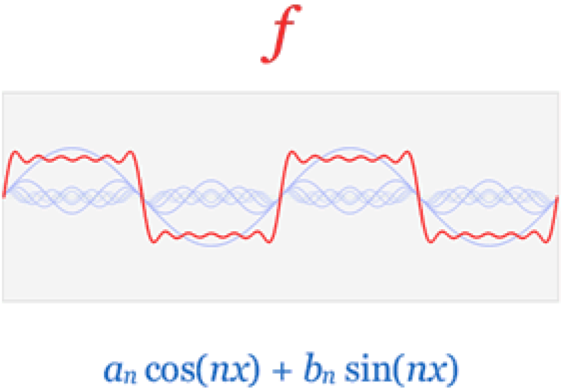


$$a_n \cos(nx) + b_n \sin(nx)$$

- Any function f can be approximated by a number of sinusoidal functions.

Fourier Transform

- The Fourier series decomposes a function $f : \mathbb{R} :\to \mathbb{C}$ into periodic components.



- Any function f can be approximated by a number of sinusoidal functions.
- The *discrete* Fourier Transform (DFT) does the same, but operates on a list $[x_1, \ldots, x_n]$ of equally spaced samples.

Quantum Fourier Transform

- DFT is computed as
  $dft : (x_1, \ldots, x_n) \mapsto (a_1, \ldots, a_{\frac{n}{2}}, b_1, \ldots, b_{\frac{n}{2}})$ with

$$a_m = \sum_{i=0}^{n-1} \frac{2\pi}{n} f(x_i) \cos(m x_i)$$

$$b_m = \sum_{i=0}^{n-1} \frac{2\pi}{n} f(x_i) \sin(m x_i)$$

- QFT, equivalently, maps quantum states $|x_1 x_2 \ldots x_n\rangle$.

Quantum Fourier Transform

- For simplicity, let us assume $n = 2^m$ for some m.
- $|X\rangle = |x_1 \dots x_n\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$ where $X = x_1 2^{n-1} + \cdots + x_n 2^0$
- QFT can be implemented as follows:

$$|X\rangle \mapsto \frac{1}{\sqrt{N}} (\mathrm{vec}(n) \otimes \cdots \otimes \mathrm{vec}(1))$$

where

$$\mathrm{vec}(i) = |0\rangle + e^{2\phi i \exp(i)} |1\rangle$$

$$\exp(i) = \sum_{k=i}^{n} \frac{x_k}{2^k} = \frac{x_i}{2} + \cdots + \frac{x_n}{2}$$

- $(\mathrm{vec}(n) \otimes \cdots \otimes \mathrm{vec}(1))$ is the tensor product of n single-qubit operations.
- Each operation canbe implemented using a Hadamard gate.

Definition (Integer factorization (IF))

$\texttt{factor} : \mathbb{N} \to \mathsf{Set}[\mathbb{N} \times \mathbb{N}]$

Input: $n \in \mathbb{N}$

Output: $P \subseteq \mathbb{N} \times \mathbb{N}$ s.t. $[\forall (p, e) \in P]$ prime(p) and $\prod_{(p,e) \in P} p^e = n$

Example

$2448 = 2^4 * 3^2 * 17^1 \quad \Rightarrow \quad \texttt{factor}(2448) = \{(2,4),(3,2),(17,1)\}$

- Best known classical algorithm: generalized prime number sieve (GPNS).
    - $O(e^{1.9 \log(n)^{\frac{1}{3}} (\log\log(n))^{\frac{2}{3}}}) = O(e^{f(n)})$ for sub-exponential f.
- **Shor's algorithm** runs in **polylogarithmic** time.
    - $O(\log(n)^3)$

- Shor's algorithm has a **classical** and a **quantum** part.

Code (Classical part)

```
//Definitions
let a = random number < n
    func(x) = $a^x \bmod n$
    r = period(func) //use QFT

//We correctly guessed a factor
case gcd(a, n) $\neq 1$               ⇒ return a

//We use the quantum part (period)
case r is odd                    ⇒ repeat
case $a^{\frac{r}{2}} \bmod n = n - 1$ ⇒ repeat
case otherwise                   ⇒ return gcd($a^{\frac{r}{2}} \pm 1$, n)
```

- `period(x)` is the quantum part and uses QFT to determine the period of $a^x \mod n$.
- Using number-theoretical results (the Chinese Remainder Theorem and Bézout's identity), we can derive factors from the period.
- The function problem **IF** can be reduced to a decision problem thus:

Definition (Integer factorization decision (IF-dec))

$\texttt{hasFactor} : \mathbb{N} \to \mathbb{N} \to \mathsf{Bool}$

Input: $n \in \mathbb{N}$ and bound $k \in \mathbb{N}$

Output: true iff n as a non-trivial factor $< k$.

- Through binary search on k, we can find the factors of n with polynomially many calls to `hasFactor`.

Definition (Unsorted search)

`elem` : $T \to \text{List}[T] \to \text{Bool}$
Input: $e \in T, \textit{list} \in \text{List}[T]$
Output: true iff e occurs in $\textit{list}$.

Example

$\textit{elem}\ 5\ [2, 1, 7, 3, 9] = \text{false}$
$\textit{elem}\ 5\ [2, 1, 7, 3, \mathbf{5}, 9] = \text{true}$

- Classical search takes $\Theta(n)$ time ($n = \text{length}(\textit{list})$): one has to iterate through the whole list.
- **Grover's algorithm** takes only $O(\sqrt{n})$ steps.

Code

```
initialize the system $S$ to the distribution
$\left(\frac{1}{\sqrt{n}}, \cdots, \frac{1}{\sqrt{n}}\right)$

repeat $O(\sqrt{n})$ times:
    case $C(S) = 1 \Rightarrow$ rotate the phase by $\pi$ radians
    case $C(S) = 0 \Rightarrow$ leave $S$ unaltered

    apply the matrix $D$ where
        $m = \frac{2}{n}$
        $D = \begin{bmatrix} (-1+m) & m & \dots & m \\ m & (-1+m) & \dots & m \\ \vdots & & \ddots & \vdots \\ m & \dots & m & (-1+m) \end{bmatrix}$
```

Grover's Algorithm

Amplitude Amplification

- D can be implemented as $D = WRW$ where R is the rotation matrix and W is the Welsh-Hadamard matrix, defined as

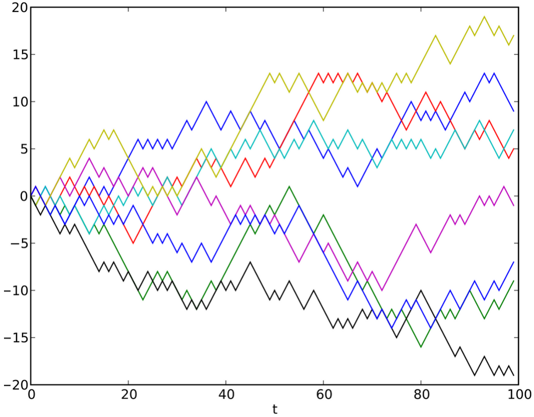
$$W_{ij} = 2^{\frac{-n}{n}} * (-1)^{\mathrm{bit}(i)\ \cdot\ \mathrm{bit}(j)} \qquad R = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & \dots & & 0 & -1 \end{bmatrix}$$

- In each iteration, the amplitude of the desired state is increased by $O(\frac{1}{\sqrt{n}})$.
- After $O(\sqrt{n})$ iterations, the amplitude of the desired state is 1.
- In the end, the system is sampled. If $\exists S_{\text{target}}$ s.t. $C(S_{\text{target}}) = 1$ then $P(S = S_{\text{target}}) \geq \frac{1}{2}$.

Quantum Walks

- A (discrete-time) random walk in n dimensions is an infinite series $[(0, \ldots, 0), (x_1^1, \ldots, x_n^1), (x_1^2, \ldots, x_n^2), \ldots]$ where, for all $k \in \mathbb{N}$, x_i^k is a sample of the random variable X_i.
- The random variables $X_1, \ldots, X_n$ are pairwise independent and $P(X_i = 1) = P(X_i = -1) = 0.5$ for $1 \leq i \leq n$.

- A (discrete-time) random walk in n dimensions is an infinite series $[(0,\ldots,0),(x_1^1,\ldots,x_n^1),(x_1^2,\ldots,x_n^2),\ldots]$ where, for all $k \in \mathbb{N}$, x_i^k is a sample of the random variable X_i.
- The random variables $X_1,\ldots,X_n$ are pairwise independent and $P(X_i = 1) = P(X_i = -1) = 0.5$ for $1 \leq i \leq n$.



Quantum Walks

- With random walks, the system is in state $(s_1, \ldots, s_n)$ at time t with a certain probability.
- With Quantums walks, the system is in a superposition of states.

Definition (All elements distinct)

$\texttt{distinct} : \text{List}[T] \to \text{Bool}$

Input: $\mathit{list} \in \text{List}[T]$

Output: true iff there are no i, j s.t. $i \neq j$ and $\mathit{list}[i] = \mathit{list}[j]$.

Example

$\mathit{distinct}\ [2, 1, 7, 3, 9] = \text{true}$

$\mathit{distinct}\ [2, \mathbf{1}, 7, 3, \mathbf{1}, 9] = \text{false}$

- Classical search takes $\Theta(n \log(n))$ time: sort the list and iterate, looking for identical consecutive elements.
- **Andris Ambainis** provides an $O(n^{\frac{2}{3}})$ algorithm.

Element distinctness problem

Quantum walks

Code

```
//Definitions
let ind = [1,...,length(list)]
    r = $n^{\frac{2}{3}}$
    $G = (V, E, mark)$ with $|V| = \binom{n}{r} + \binom{n}{r+1}$
        where
            $v_S \in V \Leftrightarrow S \subseteq ind$ with $r \leq |S| \leq r+1$;
            $(v_S, v_T) \in E \Leftrightarrow T = S \cup \{i\}$ for some $i \in list$
            $mark(v_S) = 1 \Leftrightarrow \{i,j\} \in ind \land list[i] = list[j]$

find_marked_vertex(G)
```

Element distinctness problem

Code (Finding a marked vertex)

```
1. start with a uniform superposition over $V$
2. Repeat $(N/r)$ times:
        2.1 Apply $|S\rangle |y\rangle |list\rangle \rightarrow -|S\rangle |y\rangle |list\rangle$
            for a marked $S$
            $x \in [1, \ldots, m]^r$
            $y \in ind - S$
        2.2 Perform $\sqrt{r}$ steps of a quantum walk
            through $G$.
```

m is reused accross queries: if we move from v_S to v_T, we set m to $|T - S|$.

BQP and NP

- The algorithms just discussed all lie in **BQP**:

Definition (Bounded error quantum polynomial time)

A language $X \in$ **BQP** iff $\exists f$: List[Qubit] $\rightarrow$ Bit for X s.t.

1. f takes n qubits of input,
2. f runs in $O(n^k$ time (for a constant k),
3. $x \in X \Rightarrow P(f(x) = 1) \geq \frac{2}{3}$,
4. $x \notin X \Rightarrow P(f(x) = 0) \geq \frac{2}{3}$.

- **BQP** is the quantum-analogue of **BPP**:

Definition (Bounded error polynomial time)

A language $X \in$ **BQP** iff $\exists f$: List[Bit] $\rightarrow$ Bit for X s.t.

1. f takes n *bits* of input,
2. f may make use of a true random number generator,
3. f runs in $O(n^k$ time (for a constant k),
4. $x \in X \Rightarrow P(f(x) = 1) \geq \frac{2}{3}$,
5. $x \notin X \Rightarrow P(f(x) = 0) \geq \frac{2}{3}$.

BQP and NP

- $\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE}$
- However, both $\mathbf{BQP} \overset{?}{\subseteq} \mathbf{NP}$ and $\mathbf{NP} \overset{?}{\subseteq} \mathbf{BQP}$ are unknown.
- Shor's algorithm solves the **NP**-problem **IF**, but $\mathbf{IF} \overset{?}{\in}$ **NP-complete** is not known.
- Hence, it is not known whether quantum computers can actually solve the class **NP** in polynomial time.

- Sources:
  - Shor's algorithm: `http://arxiv.org/abs/quant-ph/0303175`
  - Grover's algorithm: `http://arxiv.org/abs/quantph/9605043`
  - Ambainis's algorithm: `http://arxiv.org/abs/quantph/0311001`

How to build a quantum computer?

Requirements for a quantum computer

- A scalable physical system with well characterized quibits
- The ability to initialize the state of the qubits to a simple fiducial state such as $\langle 000 \ldots |$
- Long relevant decoherence times, much longer than the gate operation time
- A "universal" set of quantum gates
- A qubit-specific measurement capability

Problems

- **Relaxation** - falling back to state with lower energy.
- **Dekoherence** - superposition gets lost through external influence.

Possible Technological Candiates

- Bose-Einstein condensate (BEC)
- Ion Traps
- Super-conducting qubits
- Cold-atom optical lattices
- NV-centers in diamonds
- Semiconductor quantum dots

Bose-Einstein condensate (BEC)

- Temperature very close to 0 K
- Quantum effects manifest on macroscopic level
- Same quantum state over multiple atom
- Two-component BCE for qubits.

Ion Traps

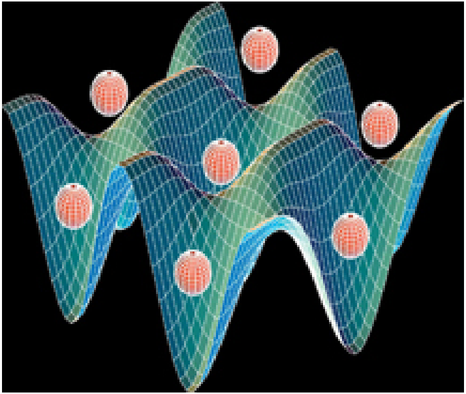
- Long storage of state
- Ions in vacuum
- Initialisation with optical pumping
- Measurement via laser
- Operations 97% successful

Super-conducting qubits

- Super-conducting circuit
- With Josephson junction
- Initialisation with microwaves

Cold-atom in opcial lattices

- Grid of laser beams
- Periodic potential traps neutral atoms



NV-centers in diamonds

- Nitrogen (N) replaces carbon (C) in diamond
- Initialisation with laser beams
- Diamond structure isolates qubits from external influence
- No cooling required

Semiconductor quantum dot

- 10^3 to 10^9 atoms
- Electrons cannot move
- Discrete electronic state
- Qubit as spin of electron
- Initialisation with magnetic fields

Recent developments

Recent developments

- At the TU:
  - http://www.tuwien.ac.at/aktuelles/news_detail/article/8744/