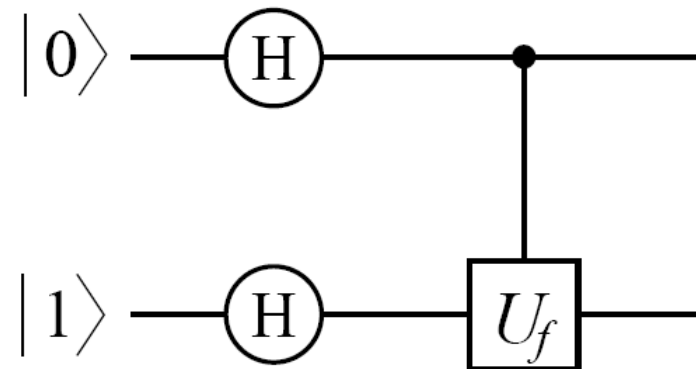




LECTURE FIVE: Introduction to Quantum Computation I

May 27,
2020



Harald Weinfurter

LMU München

Goals of This Lecture

- **Introduction to quantum computation**
 - bits – qubits – qubytes
 - operations
 - algorithms

conventional information processing



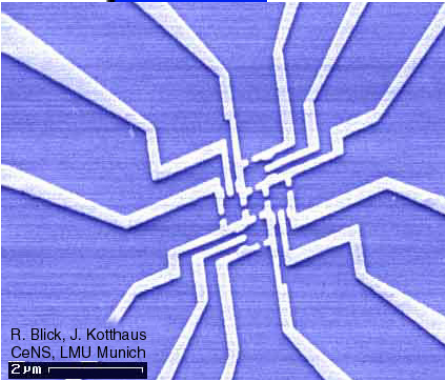
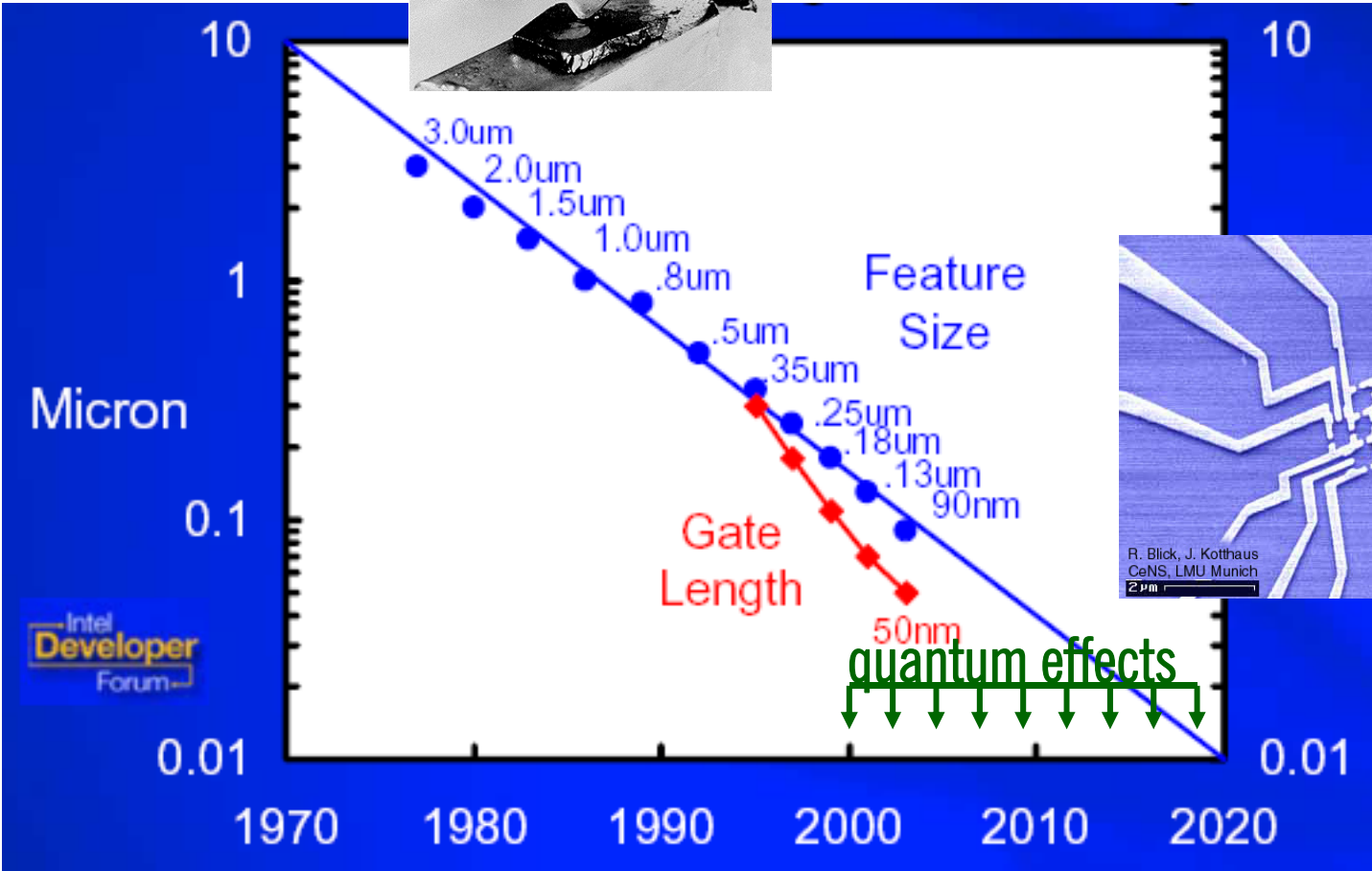
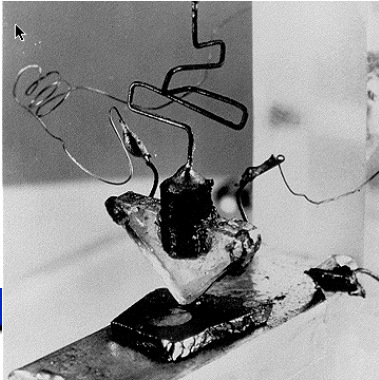
bit 0, 1

information carrier : light pulse, current, voltage, charge ...

increase in information processing power due to
miniaturization



Moore's Law

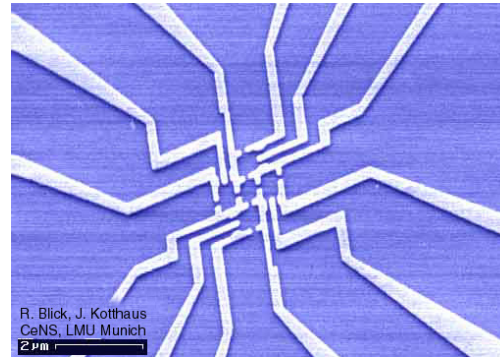
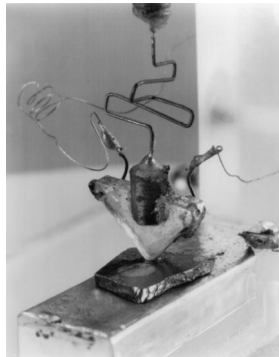


conventional information processing

bit 0, 1

information carrier : light pulse, current, voltage, charge ...

increase in information processing power due to
miniaturization



soon wires, contacts etc. will be only a few atoms wide

miniaturization results in quantum effects

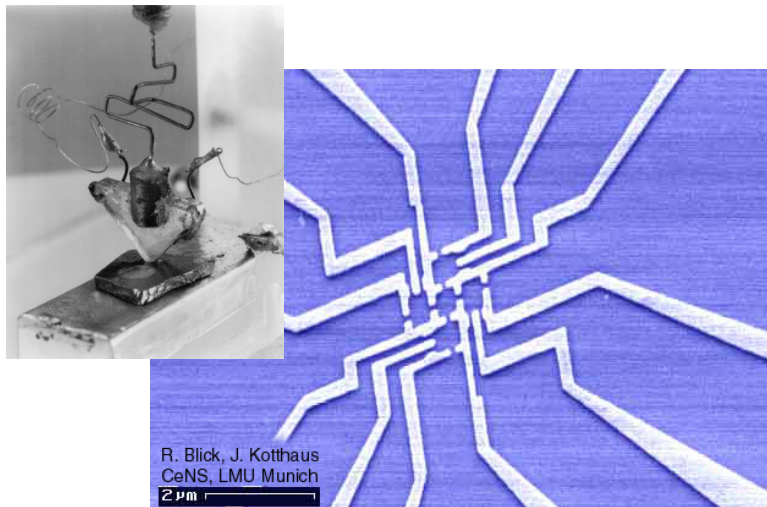
avoid quantum effects ?

USE THEM !

conventional Information – quantum information

bit 0, 1

information carrier : light pulse,
current, voltage, charge ...



minituriation

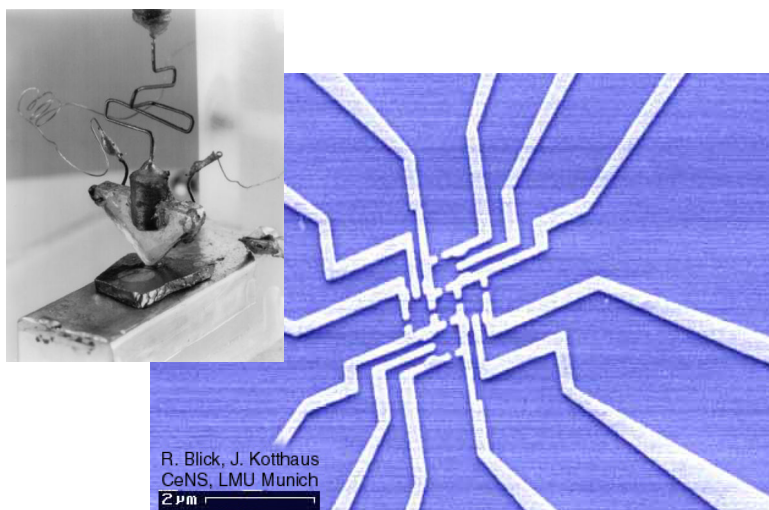
→ quantum effects
avoid ? use !

conventional information – quantum information



bit 0, 1

information carrier : light pulse, current, voltage, charge ...



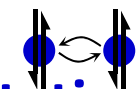
minituriazation

→ quantum effects
avoid ? use !

qubit $|\Psi\rangle = a_0|0\rangle + a_1|1\rangle$

information carrier: photons, atoms, electrons,...













- superposition
- uncertainty principle
random number generator
quantum cryptography
- entanglement
quantum teleportation
quantum computer











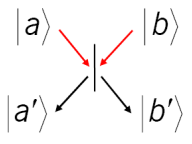


bit → qubit

- bit 0, 1
two possible values
- qubit $|0\rangle, |1\rangle$
any superposition of the
two states $|\Psi\rangle = a_0|0\rangle + a_1|1\rangle$

bit → qubit physical carriers

"0"	"1"	bit
		CD: <i>pattern</i>
no bump	bump	
		Pixel <i>brightness</i>
white	black	
		hard disk <i>magnetic orientation</i>
N	S	
		TTL-signals <i>voltage level</i>
0V	5V	
		high speed glass fiber connection <i>light</i>
off	on	
		RAM-memory <i>charge of capacitance</i>
not charged	charged	

"0"	"1"	qubit
		photon: <i>linear polarization</i>
$ V\rangle$	$ H\rangle$	
		superconducting current: <i>orientation</i>
$ L\rangle$	$ R\rangle$	
		electron, neutron, atomic nucleus: <i>spin</i>
$ +\frac{1}{2}\hbar\rangle$	$ -\frac{1}{2}\hbar\rangle$	
		atom, ion: <i>internal states</i>
$ g\rangle$	$ e\rangle$	
		quantum dots: <i>energy levels</i>
$ g\rangle$	$ e\rangle$	
		any particle: <i>directions at beam splitter</i>
$ a\rangle$	$ b\rangle$	
$ a'\rangle$	$ b'\rangle$	

bit → qubit

- bit 0, 1
two possible values

- strings {0,1,1,0}

- calculations
usually irreversible mapping

- readout gives result
"r"

- qubit $|0\rangle, |1\rangle$

any superposition of the two states

$$|\Psi\rangle = a_0|0\rangle + a_1|1\rangle$$

- strings of qubits $|0,1,1,0\rangle$
and any superposition of them

$$|\Psi\rangle = \sum_{i=0\dots00,\dots,1\dots11} a_i |i\rangle$$

- all unitary transformations

$$|\Psi\rangle \xrightarrow{\text{calculation}} U|\Psi\rangle$$

"quantum parallelism" !

- measurement gives only
one single result

new algorithms

- quantum computer can reduce complexity of a problem
 - complexity refers to the number of operations, memory size etc.
 - e.g.,

sum	$11+23=?$	$O(n)$
product	$11*23=?$	$O(n^2)$
factorization	$253=a*b$	$O(\exp(n^{1/3}))$
- **Advantage**, if **common properties** of all results (properties of the function) have to be calculated.
 - factorization, (search)

→ use quantum parallelism !

quantum operations – quantum logic gates



- single qubit gate

- unity

- NOT

- Hadamard

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{operate on} \quad \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$
$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

e.g.:

$$\mathbf{H} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} a_0 + a_1 \\ a_0 - a_1 \end{pmatrix}$$

$$\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

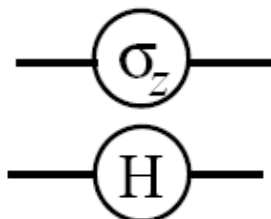
$$\mathbf{H}|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

quantum operations – quantum logic gates

- single qubit gate

- unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- NOT $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- Hadamard $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

operate on $\begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$

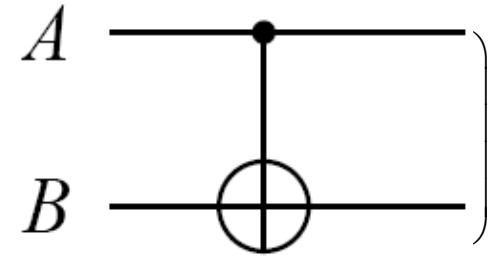


e.g.:

$$H \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} a_0 + a_1 \\ a_0 - a_1 \end{pmatrix}$$

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

- two qubit gate $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
- CNOT
- transform product state into entangled state



operate on $\begin{pmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{pmatrix}$

$$\text{CNOT} \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes |0\rangle \right] = \frac{1}{\sqrt{2}} (|0\rangle|0\rangle + |1\rangle|1\rangle)$$

all n-qubit gates can be decomposed in one- and two-qubit gates

Deutsch-Josza algorithm

- distinguish constant and balanced functions $f(x)$ (single bit)
- are the two sides of a coin equal ?
- i.e., **determine, whether function is constant or balanced**

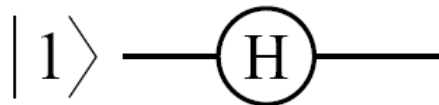
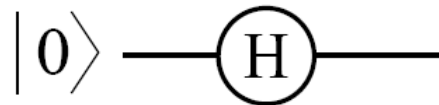
$f_1(0)=0$	$f_2(0)=1$	$f_3(0)=0$	$f_4(0)=1$
$f_1(1)=0$	$f_2(1)=1$	$f_3(1)=1$	$f_4(1)=0$
constant		balanced	

- classical solution: calculate function $2x$

Deutsch-Josza, quantum solution

- use two qubits, initially in state $|0,1\rangle$
- define function: $U_f|x,y\rangle = |x,y \oplus f(x)\rangle$
- apply Hadamard on both:

$$|\psi_1\rangle = H_a H_b |0,1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle)$$



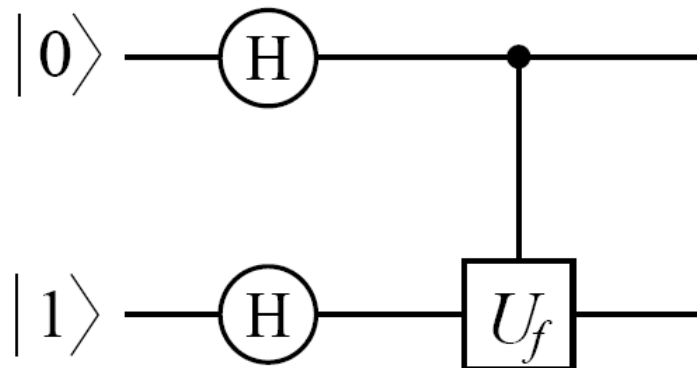
Deutsch-Josza, quantum solution

- use two qubits, initially in state $|0,1\rangle$
- define function: $U_f|x,y\rangle = |x,y \oplus f(x)\rangle$
- apply Hadamard on both:

$$|\psi_1\rangle = H_a H_b |0,1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle)$$

- evaluate function

$$|\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{2}(|0, f(0)\rangle + |0, f(1)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$$



Deutsch-Josza, quantum solution

- use two qubits, initially in state $|0,1\rangle$
- define function: $U_f|x,y\rangle = |x,y \oplus f(x)\rangle$
- apply Hadamard on both:

$$|\psi_1\rangle = H_a H_b |0,1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle)$$

- evaluate function

- $|\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{2}(|0, f(0)\rangle + |0, f(1)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$

$$f(1) = f(0)$$

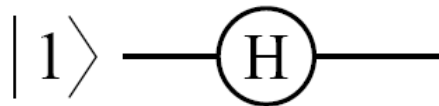
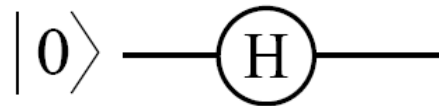
$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}(|0, f(0)\rangle + |0, f(0)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(0)\rangle) = \\ &= \frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |1 \oplus f(0)\rangle) \end{aligned}$$



Deutsch-Josza, quantum solution

- use two qubits, initially in state $|0,1\rangle$
- define function: $U_f|x,y\rangle = |x,y \oplus f(x)\rangle$
- apply Hadamard on both qubits:

$$|\psi_1\rangle = H_a H_b |0,1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle)$$

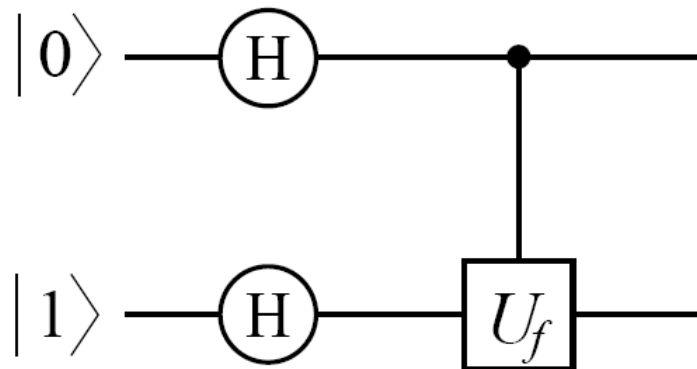


Deutsch-Josza, quantum solution

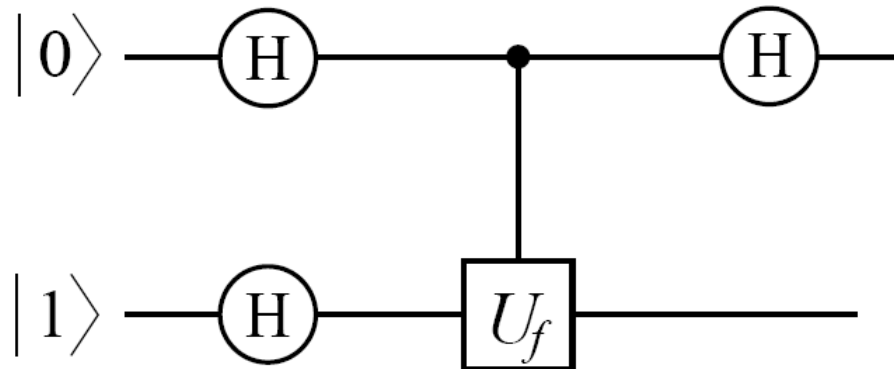
- use two qubits, initially in state $|0,1\rangle$
- define function: $U_f|x,y\rangle = |x,y \oplus f(x)\rangle$
- apply Hadamard on both qubits:

$$|\psi_1\rangle = H_a H_b |0,1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle)$$
- evaluate function

$$|\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{2}(|0, f(0)\rangle + |0, f(1)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$$



Deutsch-Josza, quantum solution



$$|\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{2} (|0, f(0)\rangle + |0, f(1)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$$

– two cases: **constant** $f(1) = f(0)$

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2} (|0, f(0)\rangle + |0, f(0)\rangle - |1, 1 \oplus f(0)\rangle + |1, 1 \oplus f(0)\rangle) = \\ &= \frac{1}{2} (|0\rangle + |1\rangle) (|f(0)\rangle - |1 \oplus f(0)\rangle) \end{aligned}$$

– **balanced** $f(1) = 1 \oplus f(0)$

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2} (|0, f(0)\rangle + |1, 1 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle - |1, f(0)\rangle) = \\ &= \frac{1}{2} (|0\rangle - |1\rangle) (|f(0)\rangle - |1 \oplus f(0)\rangle) \end{aligned}$$

→ **measure first qubit** (only one evaluation, also for many qubits)

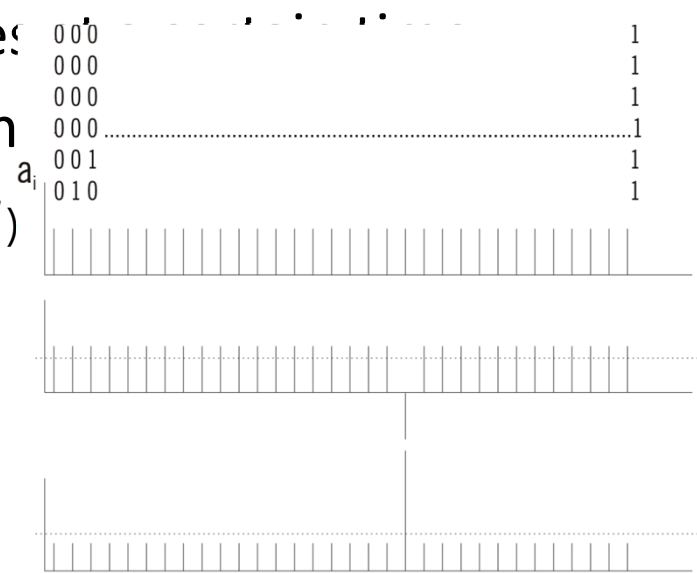
search algorithm (Grover)

- search unsorted database $f(x) = 1$ if x solution, $f(x) = 0$ otherwise
- manipulate amplitude of all possible data-elements (a_i), such that the correct one dominates:

1. prepare superposition of all elements

$$|\psi_1\rangle = H^{\otimes n} |00\dots 0\rangle = N^{-1/2} \sum_{x=0..N-1} |x\rangle \quad (N = 2^n)$$

2. apply oracle $U_f |x\rangle = (-1)^{f(x)} |x\rangle$



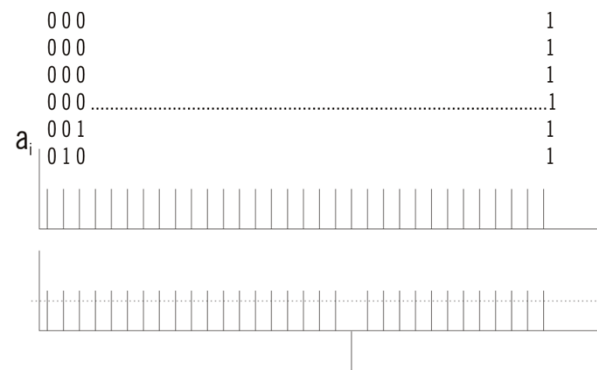
search algorithm (Grover)

- search unsorted database $f(x_s) = 1$ (if x_s solution), $f(x) = 0$ otherwise
- manipulate amplitude of all possible data-elements (a_i), such that the correct one dominates at a certain time

1. prepare superposition of all elements

$$|\psi_1\rangle = H^{\otimes n} |00\dots 0\rangle = N^{-1/2} \sum_{x=0..N-1} |x\rangle \quad (N = 2^n)$$

2. apply oracle $I_{x_s} : U_{f(x)} |x\rangle = (-1)^{f(x)} |x\rangle$

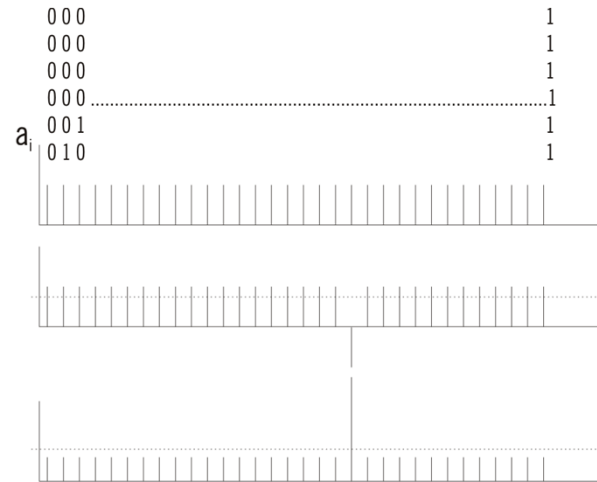


search algorithm (Grover)

- search unsorted database $f(x_s) = 1$ (if x_s solution), $f(x) = 0$ otherwise
- manipulate amplitude of all possible data-elements (a_i), such that the correct one dominates at a certain time

1. prepare superposition of all elements

$$|\psi_1\rangle = H^{\otimes n} |00\dots 0\rangle = N^{-1/2} \sum_{x=0..N-1} |x\rangle \quad (N=2^n)$$



2. apply oracle $I_{x_s} : U_{f(x)} |x\rangle = (-1)^{f(x)} |x\rangle$
3. apply inversion around the average

$$|\psi'\rangle = H^{\otimes n} I_0 H^{\otimes n} |\psi\rangle$$

$$I_0 |x\rangle = -(-1)^{\delta_{0,x}} |x\rangle$$

- repeat 2.,3., $|\psi_k\rangle = (H^{\otimes n} I_0 H^{\otimes n})^k |\psi_1\rangle = \cos \frac{2k+1}{2} \theta |x_s\rangle + \sin \frac{2k+1}{2} \theta |x_{others}\rangle$
with $|\psi_1\rangle = \cos \frac{\theta}{2} |x_{others}\rangle + \sin \frac{\theta}{2} |x_s\rangle$, if only 1 solution
- stop after about $\frac{\pi}{4} \sqrt{N}$ iterations

factorization

- difficult problem, best known classical algorithm $O(\exp(n^{1/3}))$
- fact that factorization is difficult, used in public-key encryption

factorization

- difficult problem, best known classical algorithm $O(\exp(n^{1/3}))$
- fact that factorization is difficult, used in public-key encryption
- a (not very fast) **factoring algorithm**:
 - choose y , coprime with N ; evaluate $F_N(a) = y^a \bmod N$
 - **find period** r of $F_N(a) \Rightarrow y^r \equiv 1 \bmod N$ $(y^r = kN + 1 \Rightarrow y^{r+1} = kNy + y \Rightarrow$
 - if r even, set $x = y^{r/2} \Rightarrow x^2 \equiv 1 \bmod N \Rightarrow$ $\Rightarrow y^{r+1} \bmod N = y \bmod N \Rightarrow r$ period of F_N)
 $\Rightarrow x^2 - 1 = (x-1)(x+1) \equiv 0 \bmod N$
 - $x-1$ or $x+1$ cannot be multiples of N , thus they must have a common factor
 $\Rightarrow p, q = \gcd(x \pm 1, N)$ are **factors of N**
- all tasks can be calculated efficiently except period of F_N

\Rightarrow Shor: use quantum Fourier transform

quantum Fourier transform

- use quantum parallelism to calculate $F_N(a)$ for many a
- use Fourier transform to calculate period r

– two registers: source register with K qubits, where
target register with

$$N^2 \leq Q := 2^K \leq 2N^2$$

1. initialize:

$$L \geq \log_2 N$$

2. calculate

all values are calculated in parallel and available for the next step

$$F_N(a): |\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{q=0..Q-1} |q\rangle |y^q \bmod N\rangle$$



quantum Fourier transform

- use quantum parallelism to calculate $F_N(a)$ for many a
- use Fourier transform to calculate period r
 - two registers: source register with K qubits, where $N^2 \leq Q := 2^K \leq 2N^2$
target register with $L \geq \log_2 N$

1. **initialize:** $|\psi_1\rangle = H^{\otimes K} |0\rangle|0\rangle = \frac{1}{\sqrt{Q}} \sum_{q=0..Q-1} |q\rangle|0\rangle$

2. **calculate** $F_N(q)$: $|\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{q=0..Q-1} |q\rangle |y^q \bmod N\rangle$

all values are calculated in parallel and available for the next step

3. **measure target register**, suppose result z , where $z = y^l \bmod N$.

Since $y^l \equiv y^{jr+l} \bmod N$, source register in state

$$|\phi_l\rangle = \frac{1}{\sqrt{A+1}} \sum_{j=0..A} |jr+l\rangle$$

measurement gives **one** value, e.g. $kr+l$, but l random, different in every run, not (yet) useful.

quantum Fourier transform II

4. **Fourier transform** to extract r : $U_{F_Q} : |q\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{q'=0..Q-1} \exp\left(2\pi i \frac{q'q}{Q}\right) |q'\rangle$

$$\begin{aligned} \Rightarrow |\phi'_l\rangle &= \frac{1}{\sqrt{Q(A+1)}} \sum_{q'=0..Q-1} \sum_{j=1..A} \exp\left(2\pi i \frac{q'(jr+l)}{Q}\right) |q'\rangle = \\ &= \frac{1}{\sqrt{Q(A+1)}} \sum_{q'=0..Q-1} \exp\left(2\pi i \frac{q'l}{Q}\right) \underbrace{\sum_{j=1..A} \exp\left(2\pi i \frac{q'jr}{Q}\right)}_{Q/r \text{ for } q' \text{ multiple of } Q/r; 0 \text{ otherwise}} |q'\rangle \end{aligned}$$

$$U_{F_Q} |\phi_l\rangle = \frac{1}{\sqrt{r}} \sum_{j=0..r-1} \exp\left(2\pi i \frac{lj}{r}\right) |j \frac{Q}{r}\rangle$$

5. **measure source register**, result $\lambda Q/r$, independent of l
6. **repeat 1...5**, several values of $\lambda_j Q/r \rightarrow$ determine r

example: factor $N=15$

- choose y , coprime with N , e.g. $y=7$, evaluate $F_N(a)$

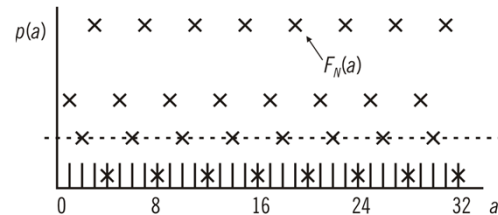
a	1	2	3	4	5	6	7
$F_N(a)$	7	4	13	1	7	4	13

$$r = 4 \Rightarrow x = 7^2 = 49$$

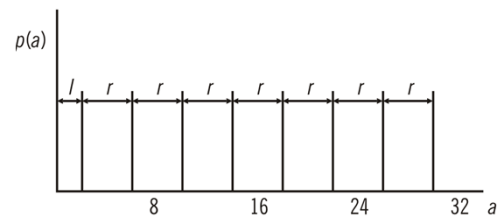
$$p = \gcd(49 - 1, N) = 3$$

$$q = \gcd(49 + 1, N) = 5$$

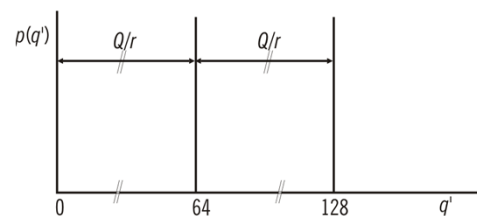
- quantum Fourier transform to find r :



initialize, evaluate $F_N(a)$



measure 2nd register, superposition in 1st register
random shift by l_j



QFT, measure first register \Rightarrow period $Q/r \Rightarrow r$

example: factor $N=15$

- choose y , coprime with N , e.g. $y=7$, evaluate $F_N(a)$

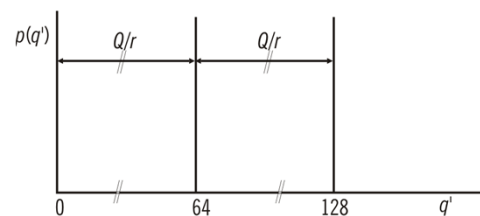
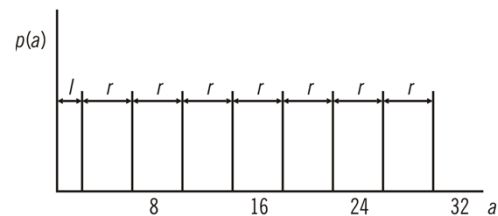
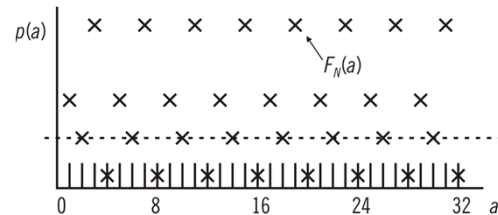
a	1	2	3	4	5	6	7
$F_N(a)$	7	4	13	1	7	4	13

$$r = 4 \Rightarrow x = 7^2 = 49$$

$$p = \gcd(49 - 1, N) = 3$$

$$q = \gcd(49 + 1, N) = 5$$

- quantum Fourier transform to find r :



initialize, evaluate $F_N(a)$

$$F_N(q): |\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{q=0..Q-1} |q\rangle |y^q \bmod N\rangle$$

measure 2nd register, superposition in 1st register
random shift by l_j

$$|\phi_l\rangle = \frac{1}{\sqrt{A+1}} \sum_{j=0..A} |jr + l\rangle$$

QFT, measure first register \Rightarrow period $Q/r \Rightarrow r$

summary

- quantum registers \Rightarrow quantum parallelism
- quantum gates \Rightarrow two qubit-gates suffice
- quantum algorithms
 - cleverly use quantum parallelism
 - amplify amplitudes (Grover)
 - analyze function over exponentially many input numbers to find global properties of the function (period in Shor algorithm)