Introduction to Quantum Computation

Gil Harel

Spinoza Institute
Universiteit Utrecht

adapted from

"Quantum computation tutorial"

Samuel Braunstein

Department of Physics
University of Wales, Bangor

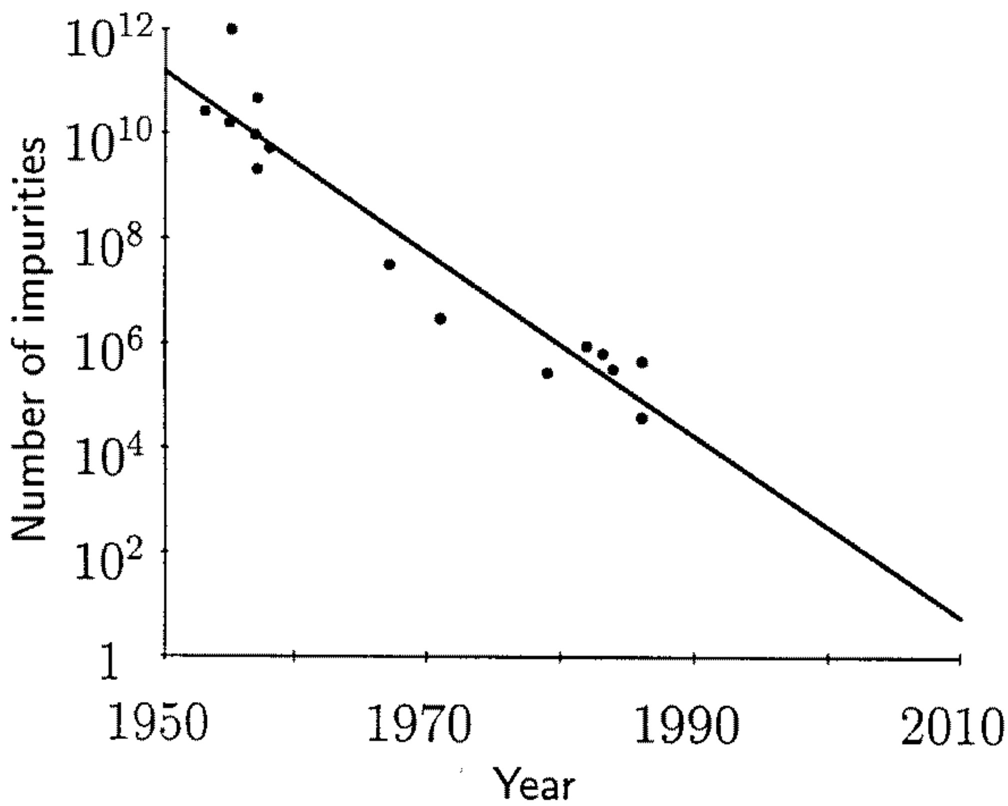
Quantum Computation:

computation theory + quantum mechanics

- Motivation
- Hardware: quantum logic
- Software: quantum algorithms
- Current research in QC
- References

Motivation

- Miniaturization limit



Number of dopant impurities in bases of bipolar transistors involved in logic versus year.

From: R. W. Keyes, IBM J. Res. Develop. **32**, 24 (1988), "Miniaturization of electronics and its limits".

- Massive parallel processing to solve hard computational problems

P problem: solvable in polynomial running time:
n data bits take poly(n) $\sim$ n^k steps (k fixed).
eg: n-bit Fast Fourier Transform: $\sim$ $n \log n$ steps.

NP (nondeterministic polynomial) problem: guess-solution can be checked in polynomial running time.
eg: decomposing an integer into its prime factors.

By definition: P $\subseteq$ NP

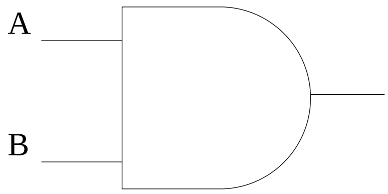
Open question: P $=$ NP ?

NP-complete: NP problem that is general enough:
any other NP problem can be reduced to it in polynomial running time.
eg: Traveling Salesman Problem.

Classical Logic Gates

Boolean logic (1847):

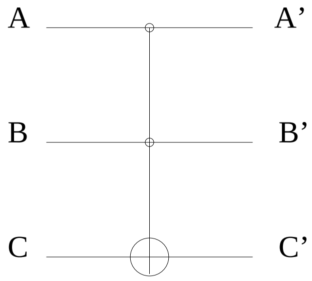
A	B	NOT	AND	OR	XOR
0	0	1	0	0	0
0	1	0	0	1	1
1	0	1	0	1	1
1	1	0	1	1	0
A	B	$\bar{B}$	$A.B$	$A+B$	$A \oplus B$



Universal sets:
{AND, NOT}; {OR, NOT}; {AND, XOR}

Reversible logic: Toffoli gate (1980):

A	B	C	A'	B'	$C' = C \oplus (A.B)$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



Universal reversible gate:
$C = 0 \;\Rightarrow\; C' = A.B$ AND gate
$B = 1 \;\Rightarrow\; C' = C \oplus A$ XOR gate

Quantum Logic

- Quantum bit: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ $\quad |\alpha|^2 + |\beta|^2 = 1$

eg: photons in a cavity; two-level atom; electron spin; nuclear spin; quantum dot; SQUID (superconductor).

- Quantum register (3 qubits)

Disentangled state:

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle$$
$$=$$
$$[\,\alpha_1\,|0\rangle + \beta_1\,|1\rangle\,] \otimes [\,\alpha_2\,|0\rangle + \beta_2\,|1\rangle\,] \otimes [\,\alpha_3\,|0\rangle + \beta_3\,|1\rangle\,]$$
$$=$$
$$a_0\,|000\rangle + a_1\,|001\rangle + a_2\,|010\rangle + a_3\,|011\rangle +$$
$$a_4\,|100\rangle + a_5\,|101\rangle + a_6\,|110\rangle + a_7\,|111\rangle$$

$$a_0 = \alpha_1\alpha_2\alpha_3 \quad a_1 = \alpha_1\alpha_2\beta_3 \quad a_2 = \alpha_1\beta_2\alpha_3 \quad a_3 = \alpha_1\beta_2\beta_3$$
$$a_4 = \beta_1\alpha_2\alpha_3 \quad a_5 = \beta_1\alpha_2\beta_3 \quad a_6 = \beta_1\beta_2\alpha_3 \quad a_7 = \beta_1\beta_2\beta_3$$

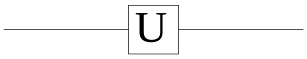
Entangled state: $a_0\,|000\rangle + a_7\,|111\rangle$

Classically: n bits $\Rightarrow$ 2^n states of the register.

Quantum mechanically: n qubits $\Rightarrow$ ∞^{2^n} states: superpositions of 2^n basic states of the register.

- Quantum gates

One-qubit gate:



$$\alpha\,|0\rangle + \beta\,|1\rangle \;\rightarrow\; \alpha'\,|0\rangle + \beta'\,|1\rangle$$

$$\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

(u_{ij}) unitary

Two-qubit gate:

$$a_0\,|00\rangle + a_1\,|01\rangle + a_2\,|10\rangle + a_3\,|11\rangle$$

$$\rightarrow\; a_0'\,|00\rangle + a_1'\,|01\rangle + a_2'\,|10\rangle + a_3'\,|11\rangle$$

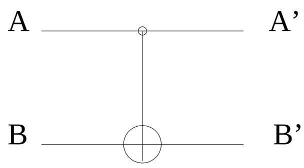
$$\begin{pmatrix} a_0{}' \\ a_1{}' \\ a_2{}' \\ a_3{}' \end{pmatrix} = \begin{pmatrix} v_{00} & v_{01} & v_{02} & v_{03} \\ v_{10} & v_{11} & v_{12} & v_{13} \\ v_{20} & v_{21} & v_{22} & v_{23} \\ v_{30} & v_{31} & v_{32} & v_{33} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

(v_{ij}) unitary

Controlled-NOT (XOR) gate:

A	B	A'	$B' = B \oplus A$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



Universal set: { all 1-qubit gates, Controlled-NOT }

ie: $$\left\{ \text{all unitary} \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix},\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \right\}$$

- Quantum parallel processing

Given any function: $f : \{0,1,\ldots,7\} \rightarrow \{0,1,\ldots,7\}$

assemble a twin 3-qubit register $|\,\_\ \_\ \_\ ;\_\ \_\ \_\,\rangle$

and connect quantum gates to get a unitary (64×64)

transformation U_f on the register, such that:

$$U_f\ :\ |\,m\,;\,0\,\rangle \ \rightarrow\ |\,m\,;\,f(m)\rangle \qquad\qquad m = 0,1,\ldots,7.$$

Then: $\sum_{m=0}^{7} a_m\,|\,m\,;\,0\,\rangle \ \rightarrow\ \sum_{m=0}^{7} a_m\,|\,m\,;\,f(m)\rangle$

that is: $2^3 = 8$ calculations at once:

$$a_0\,|000;000\rangle + a_1\,|001;000\rangle + a_2\,|010;000\rangle + a_3\,|011;000\rangle +$$
$$a_4\,|100;000\rangle + a_5\,|101;000\rangle + a_6\,|110;000\rangle + a_7\,|111;000\rangle$$
$$\rightarrow$$
$$a_0\,|000;f(0)\rangle + a_1\,|001;f(1)\rangle + a_2\,|010;f(2)\rangle + a_3\,|011;f(3)\rangle +$$
$$a_4\,|100;f(4)\rangle + a_5\,|101;f(5)\rangle + a_6\,|110;f(6)\rangle + a_7\,|111;f(7)\rangle$$

Deutsch (1985):

For n qubits get 2^n calculations at once !

How to exploit this massive parallelism ?

Quantum Algorithms

- Factoring numbers: $N = p \times q$? $\qquad n \equiv \ln N$

Shor's quantum algorithm (1994):
factoring N in $\sim$ $(\ln N)^3$ steps. $\qquad \sim\ n^3$

Best classical algorithm:
$\sim$ $\exp[\, a\,(\ln N)^{1/3}(\ln\ln N)^{2/3}\,]$ steps. $\qquad \sim\ {}_{523}{}^{n^{1/3}}$

RSA-155 (512 bits) factorization:

109417386415705274218097073220403576120037329454492059909138421314763499842889347847179972578912673324976257528997818337970765372440271467435315933543
33897

=

102639592829741105772054196573991675900716567808038066803341933521790711307779

$\times$

106603488380168454820927220360012878679207958575989291522270608237193062808643

(A.K. Lenstra and H.J.J. te Riele, CWI, August 1999).

Example: $91 = p \times q$?

try 3: compute $f(m) = 3^m \pmod{91}$:

m :	0	1	2	3	4	5	6	7 ...
3^m :	1	3	9	27	81	243	729	2187 ...
$3^m \pmod{91}$:	1	3	9	27	81	61	1	3 ...

"quantum see at once:" 3 has period 6
(quantum compute the values $f(m)$ in parallel; find the period by Fourier transform and measurement)

$\Rightarrow \quad 3^6 - 1 \equiv 0 \pmod{91}$
$\Rightarrow \quad (3^3 - 1)(3^3 + 1) \equiv 0 \pmod{91}$
$\Rightarrow \quad 26 \times 28 \equiv 0 \pmod{91}$
$\Rightarrow \quad \gcd(26, 91) > 1$ or $\gcd(28, 91) > 1$

in fact:

$\gcd(26, 91) = 13 \qquad \gcd(28, 91) = 7 \qquad 91 = 13 \times 7$

Quantum Fourier transform modulo M $\quad (M \geq N^2)$:

$|a\rangle \;\rightarrow\; \frac{1}{\sqrt{M}} \sum_{c=0}^{M-1} \exp(2\pi i\, ac/M)\, |c\rangle \quad a = 0, 1, \ldots, M-1$

$\sum_{a=0}^{M-1} g(a)\, |a\rangle \;\rightarrow\; \sum_{c=0}^{M-1} \tilde{g}(c)\, |c\rangle$

$\tilde{g}(c) = \frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} g(a) \exp(2\pi i\, ac/M)$

Finding the period r of $f(a) = y^a$ (mod N):

choose $y < N$ at random
$\Rightarrow$ Prob[gcd$(y, N) = 1$, r even, $y^{r/2} \not\equiv \pm 1 (\mathrm{mod} N)] \geq \frac{1}{2 \ln N}$

$|0; 0\rangle \;\rightarrow\; \frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a; 0\rangle \;\rightarrow\; \frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a; f(a)\rangle$

measure second part: $|\; ; z\rangle \quad z = f(b) \quad b$ minimal

$\rightarrow\; \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |b + jr; f(b)\rangle \qquad A = \lceil (M-b)/r \rceil \approx M/r$

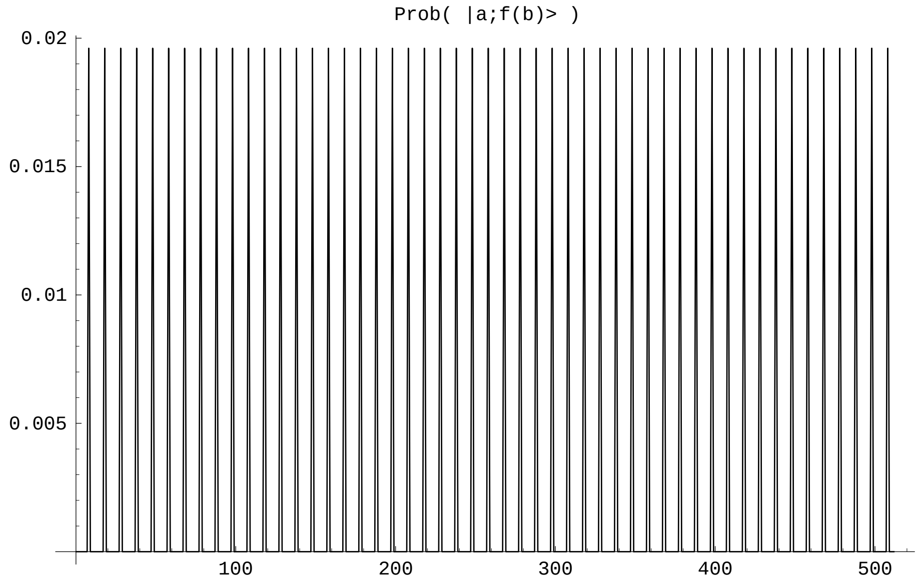
$\rightarrow\; \frac{1}{\sqrt{MA}} \sum_{c=0}^{M-1} \sum_{j=0}^{A-1} \exp(2\pi i (b + jr) c/M)\, |c; f(b)\rangle$

$\Rightarrow$ Prob($|c; f(b)\rangle$) $= \frac{1}{MA} |\sum_{j=0}^{A-1} \exp(2\pi i\, j\, \frac{rc}{M})|^2$

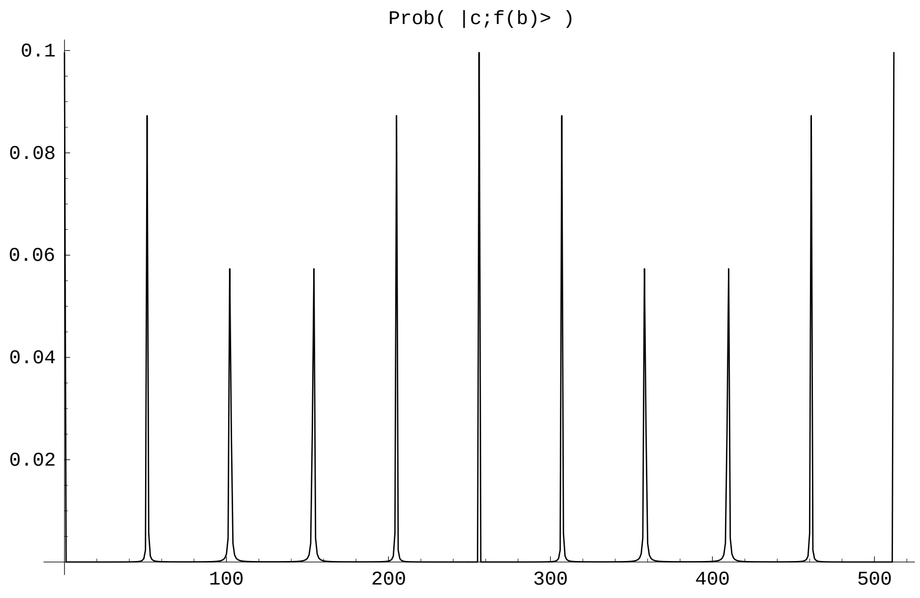
$\Rightarrow$ peaks at c with $|rc - c'M| \leq \frac{r}{2}$ ie $|\frac{c}{M} - \frac{c'}{r}| \leq \frac{1}{2M}$

$\Rightarrow$ Prob(the measured c identifies r) $> \frac{4}{\pi^2 \ln N}$

Probability distribution after measuring second part:
$|\,;z\rangle \quad z = f(b) \quad b = 8 \quad r = 10 \quad M = 512 \quad A = 51$:



Probability distribution after Fourier transform:



Prob(measuring c at a peak) $> \frac{4}{\pi^2}$

• Database search: find the unique item satisfying a given condition among N unsorted items.

Grover's quantum algorithm (1996): $\sim \sqrt{N}$ steps.

Best classical algorithm: $\frac{1}{2}N$ steps on average.

```
% GROVER'S ALGORITHM:
```

prepare initial state: $\sum_{m=0}^{N-1} a_m^{(0)} |m\rangle = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} |m\rangle$

`FOR` $i = 0$ `TO` $\sim \sqrt{N}$ `DO`

phase rotate the states selectively:

$\sum_{m=0}^{N-1} a_m^{(i)} |m\rangle \rightarrow \sum_{m=0}^{N-1} b_m^{(i)} |m\rangle$

$b_m^{(i)} = (-1)^{C(m)} a_m^{(i)} \quad C(m) \equiv \delta_{mm_0}$ one database read

invert the amplitudes about their average:

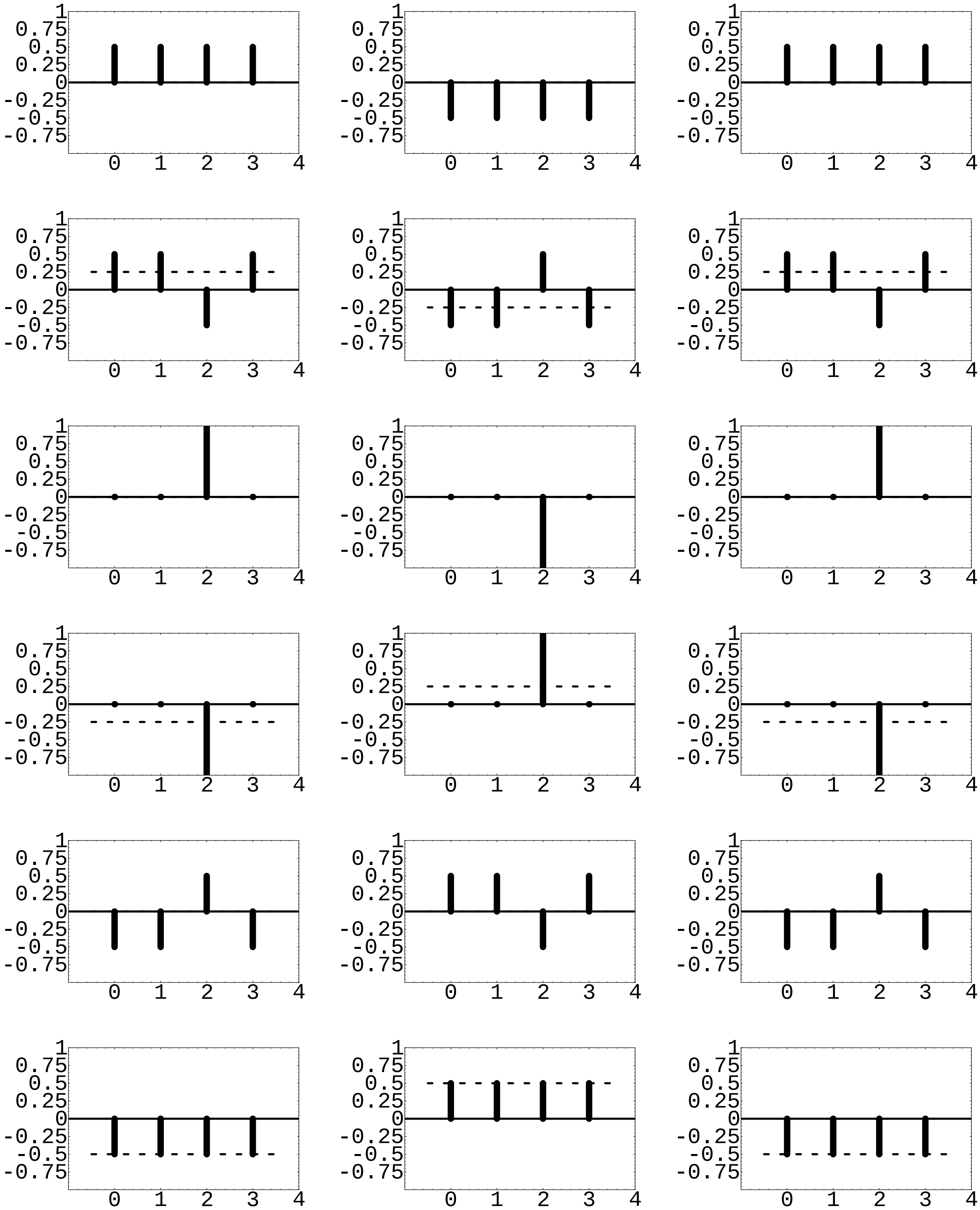
$\sum_{m=0}^{N-1} b_m^{(i)} |m\rangle \rightarrow \sum_{m=0}^{N-1} a_m^{(i+1)} |m\rangle$

$a_m^{(i+1)} = \frac{1}{N} \sum_{j=0}^{N-1} b_j^{(i)} - \left[b_m^{(i)} - \frac{1}{N} \sum_{j=0}^{N-1} b_j^{(i)} \right]$

`NEXT` i

measure the value of m; get Prob$(m{=}m_0) \geq \frac{1}{2}$

```
% END
```



$$\text{phase rotation} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{array}{l} C(0) = 0 \\ C(1) = 0 \\ C(2) = 1 \\ C(3) = 0 \end{array}$$

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$M \otimes M = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Walsh-Hadamard transformation: $W = \overbrace{M \otimes \ldots \otimes M}^{n \text{ terms}}$

$$W_{ij} = \frac{1}{\sqrt{N}} (-1)^{\overline{i} \cdot \overline{j}} \qquad N = 2^n \qquad WW = I$$

$$|0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} |m\rangle \qquad W \text{ unitary}$$

Inversion about average: $D = P - (I - P)$

$$P = \left(\frac{1}{N}\right) = W(\delta_{i0}\delta_{j0})W \qquad I = W(\delta_{ij})W$$

$$D = 2P - I = \left(\frac{2}{N} - \delta_{ij}\right) = W(2\delta_{i0}\delta_{j0} - \delta_{ij})W = WRW$$

$$D = \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \qquad R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Convergence:

$$\left(\frac{C}{\sqrt{N}}, \cdots, \frac{C}{\sqrt{N}}, -\sqrt{1 - C^2(1 - \frac{1}{N})}, \frac{C}{\sqrt{N}}, \cdots, \frac{C}{\sqrt{N}}\right) \quad \frac{1}{2} \leq C \leq 1$$

$$\text{amplitude increase} = 2\left[\frac{C}{\sqrt{N}} - \frac{\sqrt{1 - C^2(1 - \frac{1}{N})} + \frac{C}{\sqrt{N}}}{N}\right] \approx \frac{1}{\sqrt{N}}$$

stop when $\sqrt{1 - C^2(1 - \frac{1}{N})} \geq \frac{1}{\sqrt{2}}$ get Prob $\geq \frac{1}{2}$

Current research in QC

- Experimental realizations of quantum logic:
qubit; quantum register; quantum gates.

- Quantum computer architecture:
effective computing devices; networking.

- Quantum algorithms:
how to exploit the quantum advantage.

- Quantum error correction:
software and hardware schemes.

- Decoherence control:
experimental measurements; theoretical modeling.

References

- Historical milestones

P. Benioff, J. Stat. Phys. **22**, 563 (1980), "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines".

R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982), "Simulating [quantum] physics with computers".

D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985), "Quantum theory, the Church-Turing principle and the universal quantum computer".

S. Lloyd, Science **261**, 1569 (1993), "A potentially realizable quantum computer".

P. W. Shor, in *Proceedings of the 35th annual symposium on foundations of computer science*, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos CA, 1994), p. 124, "Algorithms for quantum computation: discrete logarithms and factoring".

P. W. Shor, Phys. Rev. A **52**, R2493 (1995). "Scheme for reducing decoherence in quantum computer memory".

L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997). "Quantum Mechanics Helps in Searching for a Needle in a Haystack".

- Reviews

A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996), “Quantum computation and Shor’s factoring algorithm”.

S. L. Braunstein, “Quantum computation tutorial”: www.sees.bangor.ac.uk/~schmuel

J. Preskill, “Quantum Computing: Pro and Con”: arXiv.org/abs/quant-ph/9705032

Physics World, March 1998, “Quantum information” physicsweb.org/toc/11-03

B.M. Terhal, *Quantum algorithms and quantum entanglement*, PhD. thesis, Universiteit van Amsterdam, 1999.

- Books

R. P. Feynman, *Feynman lectures on computation*, ed. by A. J. G. Hey and R. W. Allen (Addison-Wesley, Reading MA, 1996).

C. P. Williams and S. H. Clearwater, *Explorations in quantum computing* (TELOS, New York, 1998).

H.-K. Lo, T. Spiller, and S. Popescu (eds.), *Introduction to quantum computation and information*, (World Scientific, Singapore, 1998).

D. Bouwmeester, A. Ekert, and A. Zeilinger (eds.) *The physics of quantum information* (Springer, Berlin, 2000).

M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, (Cambridge University Press, New York, 2000).

- Links

CQC Oxford:
Centre for Quantum Computation:
www.qubit.org

QIPC projects:
EU R&D in Information Society Technologies,
Quantum Information Processing & Communications:
www.cordis.lu/ist/fetqipc.htm

QUIC Caltech, MIT, USC:
Quantum Information and Computation:
theory.caltech.edu/~quic

IQI Caltech:
Institute for Quantum Information:
www.iqi.caltech.edu

RSA (Rivest, Shamir, Adleman):
searchable cryptography FAQs and glossary:
www.rsasecurity.com

CWI Amsterdam: H.M. Buhrman, P.M.B. Vitányi
UvA WINS: B. Nienhuis
Quantum Computing and Advanced Systems Research:
dbs.cwi.nl:8080/cwwwi/owa/cwwwi.print_themes?ID=6

RU Groningen: H. De Raedt
Computational Physics: Quantum Computation:
rugth30.phys.rug.nl/compphys0/quantum.htm

TU Delft: L.P. Kouwenhoven, J.E. Mooij
U Utrecht: P.C.E. Stamp
Applied Physics: Quantum Transport:
vortex.tn.tudelft.nl