COLLÈGE DE FRANCE 1530

Chaire de Physique Mésoscopique
Michel Devoret
Année 2010, 11 mai - 22 juin

INTRODUCTION AU CALCUL QUANTIQUE

INTRODUCTION TO QUANTUM COMPUTATION

Première Leçon / *First Lecture*

What is a quantum computer?

Aren't all computers quantum?

Each bit of ordinary computer information is physically represented by thousands of quantum particles.

Only the average behavior of these particles encodes information, and it is described by classical physics.

Quantum computer differs from classical computer in 2 respects:
- each bit of information is physically carried by only one particle
- superposition principle of quantum mechanics is exploited

This course can be followed both by physicists and computer scientists

CONTENT OF THIS YEAR'S LECTURES

QUANTUM COMPUTATION FROM THE PERSPECTIVE OF MESOSCOPIC CIRCUITS

1. Introduction, c-bits versus q-bits
2. The Pauli group and quantum computation primitives
3. Stabilizer formalism for state representation
4. Clifford calculus
5. Algorithms
6. Error correction

NEXT YEAR: QUANTUM FEEDBACK OF ENGINEERED QUANTUM SYSTEMS

10-I-3

VISIT THE WEBSITE OF THE CHAIR OF MESOSCOPIC PHYSICS

http://www.college-de-france.fr

then follow
Enseignement > Sciences Physiques > Physique Mésoscopique > Site web

or

http://www.physinfo.fr/lectures.html

PDF FILES OF ALL LECTURES ARE POSTED ON THESE WEBSITES

Questions, comments and corrections are welcome!

write to "phymeso@gmail.com"

10-I-4

CALENDAR OF SEMINARS

May 11: Cristian Urbina, (Quantronics group, SPEC-CEA Saclay)
Josephson Effect in Atomic Contacts and Carbon Nanotubes

May 18: Benoît Douçot (LPTHE / Université Pierre et Marie Curie)
Emergence de symétries discrètes locales dans les réseaux de jonctions Josephson

June 1: Takis Kontos (LPA / Ecole Normale Supérieure)
Points quantiques et ferromagnétisme

June 8: Cristiano Ciuti (MPQ, Université Paris - Diderot)
Ultrastrong coupling circuit QED : vacuum degeneracy and quantum phase transitions

June 15: Leo DiCarlo (Yale)
Preparation and measurement of tri-partite entanglement in a superconducting quantum circuit

June 22: Vladimir Manucharian (Yale)
The fluxonium circuit: an electrical dual of the Cooper-pair box?

NOTE THAT THERE IS NO LECTURE AND NO SEMINAR ON MAY 25 !

10-I-5

LECTURE I : C-BITS vs Q-BITS

1. Information and physics
2. Quantum bits
3. Classical information processing
4. Reversible logical circuits
5. Error correction
6. Linear vs non-linear processing

10-I-6

OUTLINE

1. Information and physics
2. Quantum bits
3. Classical information processing
4. Reversible logical circuits
5. Error correction
6. Linear vs non-linear processing

10-I-6a

INFORMATION AS SEQUENCE OF SYMBOLS

:

Geometric shapes: ♠♣♥♠♦♣♥♠♦♣♥♣♣♦♦♠♣♥♦♠♥♥♠♦♣♥♣♠♣♦♠♠♥♠♣♥♠♦♣

Letters: LES□SANGLOTS□LONGS□DES□VIOLONS□DE□L’AUTOMNE

Digits (decimal): 31415926535897932384626433832795028841971693993

<u>Digits (binary):</u> 11001001000011111101101010100010001000010110100

ALL INFORMATION CAN BE REDUCED TO SERIES OF BITS (Shannon)

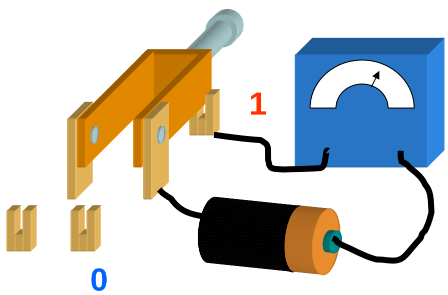
INFORMATION HAS TWO SIDES: LOGICAL AND PHYSICAL

SYMBOLS:
- Mathematical entities combined by abstract operations
- States of a physical system that evolves dynamically

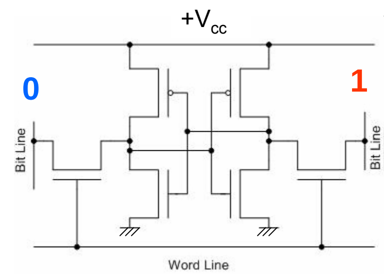
10-I-7

PHYSICAL BIT = BISTABLE SYSTEM

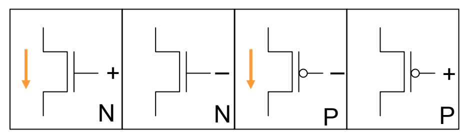
Mechanical system with electrical readout: switch



Electrical system with electrical readout: RAM cell



CMOS Transistors:



10-I-8

REGISTER = SET OF ACTIVE BITS

REGISTER WITH N=10 BITS:

0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	1	0
⋮				⋮					⋮
1	1	1	1	1	1	1	1	1	0
1	1	1	1	1	1	1	1	1	1

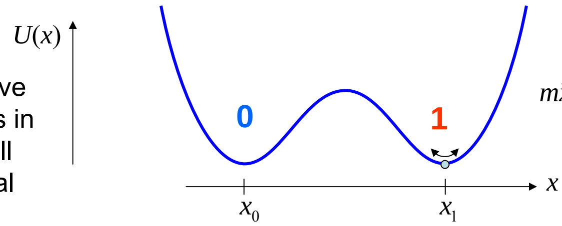
2^N = 1024 POSSIBLE CONFIGURATIONS

represents one number between 0 et 1023

10-I-9

PHYSICAL C-BITS ARE STRONGLY DISSIPATIVE

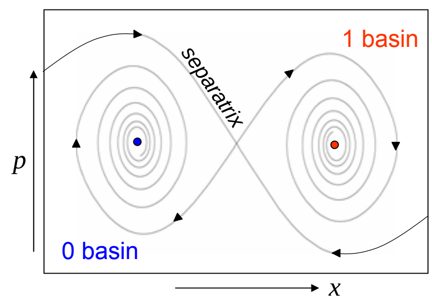
dissipative dynamics in two-well potential



$$m\ddot{x} + \eta\dot{x} + \frac{\mathrm{d}}{\mathrm{d}x}U(x) = 0$$

friction coef., interaction w/ many d.o.f.

phase-space portrait:



logical states correspond to <u>attractors</u>

stability comes at a price

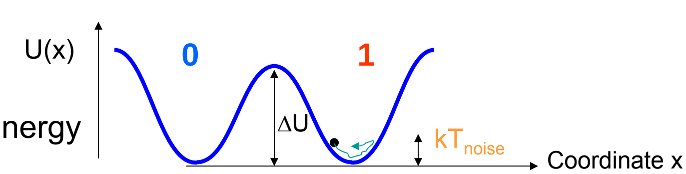
10-I-10

DISSIPATION = INTERACTION WITH MANY DEGREES OF FREEDOM

$$m\ddot{x} + \eta\dot{x} + \frac{\mathrm{d}}{\mathrm{d}x}U(x) = 0 \quad \Longleftrightarrow \quad \begin{cases} m\ddot{x} + m\sum_i c_i^2\omega_i^2\left(x - \frac{y_i}{c_i}\right) + \frac{\mathrm{d}}{\mathrm{d}x}U(x) = 0 \\ \ddot{y}_i + \omega_i^2\left(y_i - c_i x\right) = 0 \\ \eta = \frac{\pi}{2}m\left\langle \frac{c_i^2\omega_i^2}{\omega_i - \omega_{i-1}} \right\rangle \end{cases}$$

(Caldeira & Leggett, 1982)

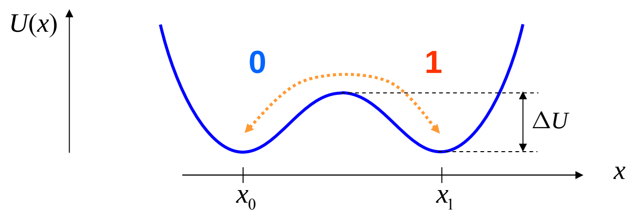
FLUCTUATION-DISSIPATION THEOREM

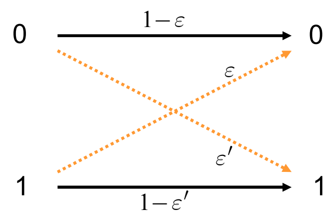


Bit state is either 0 or 1: 1) strong dissipation and 2) $kT_{noise} \ll \Delta U$

10-I-11

BIT ERRORS





if symmetric well, 1 eff^{tive} temp^{re}:

$$\varepsilon = \varepsilon' = \omega_a \tau \exp\left(-\frac{\Delta U}{k_B T_{eff}}\right)$$

Dissipation implies noise, but bit error rate can be made exponentially small.

Higher barriers mean larger energy is needed to change state.

QUESTIONS INFORMATION PHYSICS ATTEMPTS TO ANSWER

HOW CAN BITS BE BEST REPRESENTED PHYSICALLY?

WHAT CONSTRAINTS DO THE LAWS OF PHYSICS IMPOSE ON SPEED AND COMPLEXITY OF INFORMATION PROCESSING?

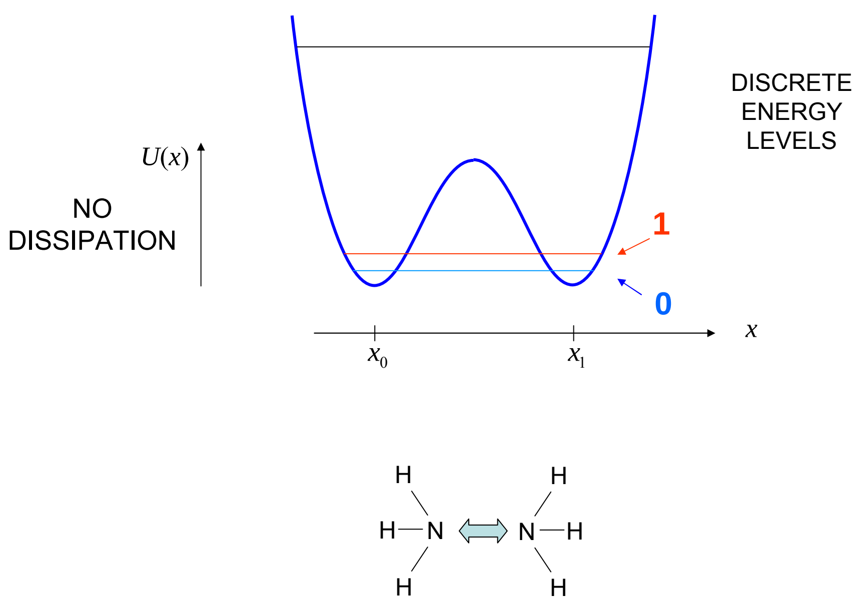
WHAT ARE THE LINKS BETWEEN THE LOGICAL PROPERTIES OF INFORMATION AND THE LAWS OF THE PHYSICAL WORLD?

OUTLINE

1. Information and physics
2. Quantum bits
3. Classical information processing
4. Reversible logical circuits
5. Error correction
6. Linear vs non-linear processing

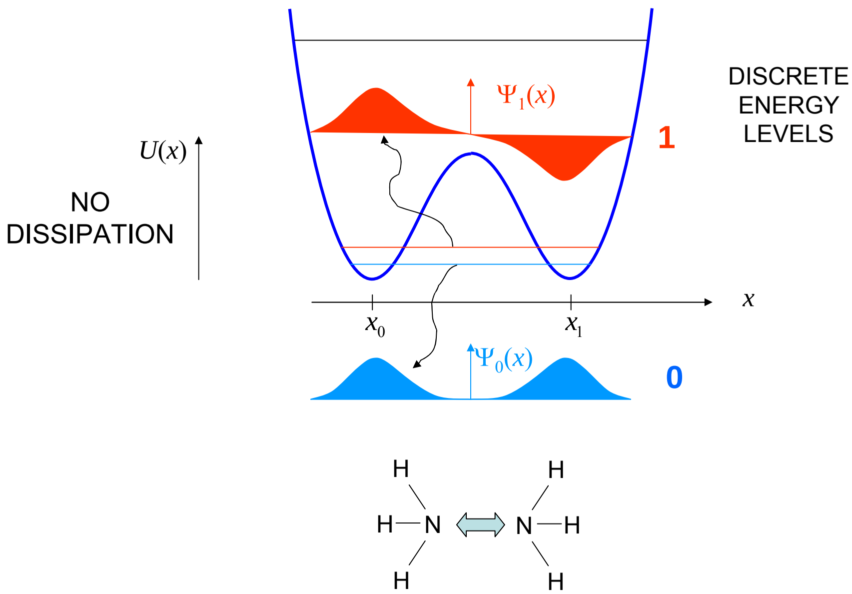
10-1-6b

FROM CLASSICAL BIT TO QUANTUM BIT



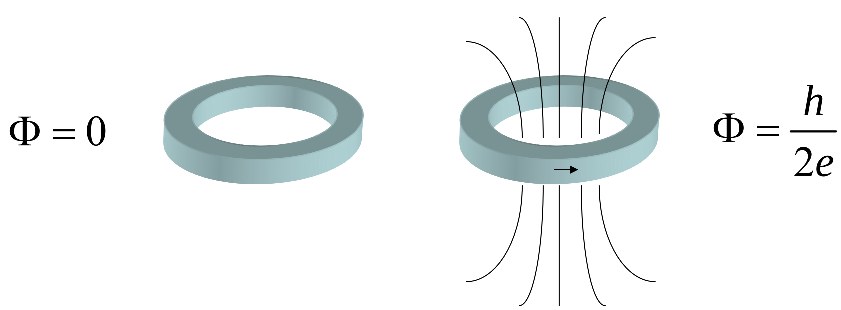
10-I-14

FROM CLASSICAL BIT TO QUANTUM BIT



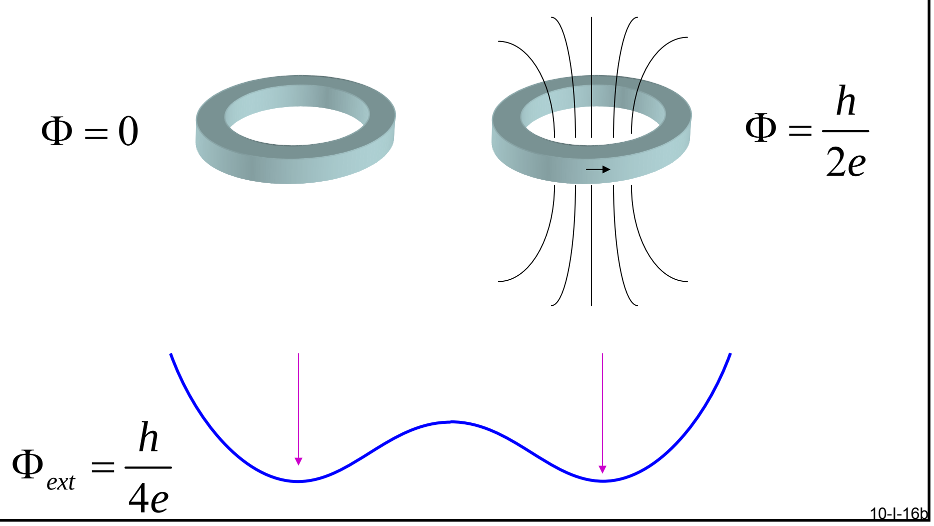
10-I-15

TWO FLUX STATES OF A SUPERCONDUCTING RING



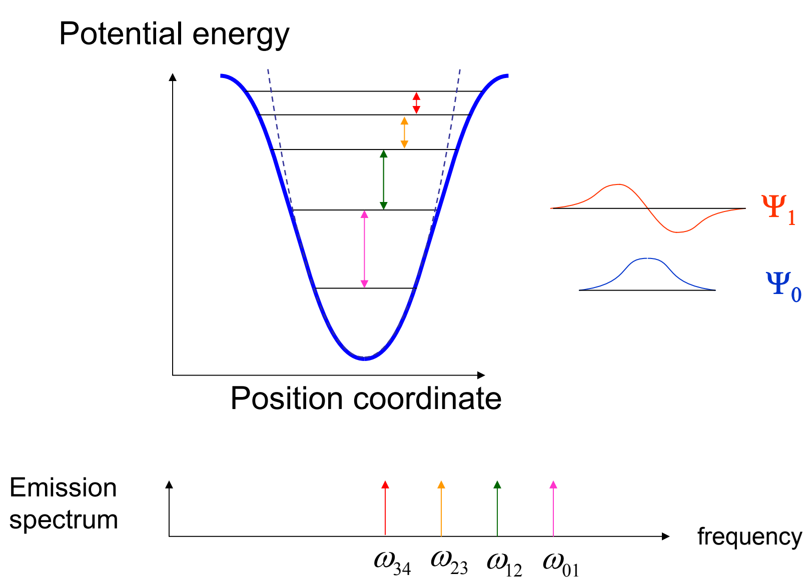
10-I-16

TWO FLUX STATES OF A SUPERCONDUCTING RING



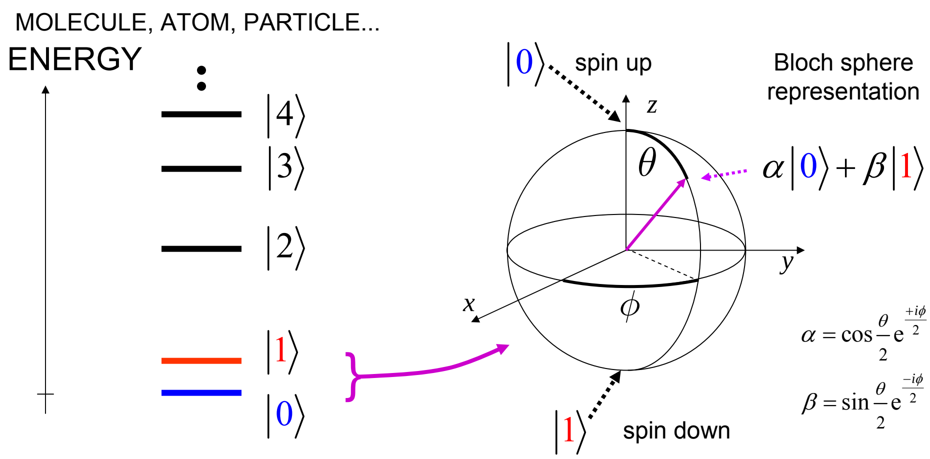
10-I-16b

ANY POTENTIAL BUT QUADRATIC



10-I-17

QUANTUM BIT: 2 LEVELS FORMING EFFECTIVE SPIN 1/2



Qubit state can be 0 "and" 1: 1) no dissipation and 2) $kT_{noise} \ll \hbar\omega_{01}$

10-I-18

OUTLINE

1. Information and physics
2. Quantum bits
3. Classical information processing
4. Reversible logical circuits
5. Error correction
6. Linear vs non-linear processing

10-1-6c

BOOLEAN CALCULUS

Boolean field $\mathbb{B} = \{\{0,1\};\oplus;\bullet\}$ A.K.A. $\mathbb{Z}/2\mathbb{Z}$

- $\{0,1\}$: 2 binary digits = 2 numbers
- $\oplus$: addition modulo 2
- $\bullet$: multiplication (modulo 2)

10-I-19

BOOLEAN CALCULUS

Boolean field $\mathbb{B} = \{\{0,1\};\oplus;\bullet\}$

- $\{0,1\}$: 2 binary digits = 2 numbers
- $\oplus$: addition modulo 2
- $\bullet$: multiplication (modulo 2)

$b_1 \oplus b_2$		$b_1 = 0$	$b_1 = 1$
b_2	0	0	1
	1	1	0

$b_1 \bullet b_2$		$b_1 = 0$	$b_1 = 1$
b_2	0	0	0
	1	0	1

10-I-19b

LOGICAL OPERATIONS

Boolean field $\mathbb{B} = \{\{0,1\}; \oplus; \bullet\}$

False = 0
True = 1

addition modulo 2

multiplication (modulo 2)

Notations and functions:

$$\mathrm{NOT}(x) = \overline{x} = x \oplus 1$$

$$\mathrm{XOR}(x,y) = x \;\mathrm{XOR}\; y = x \oplus y \quad \text{A.K.A. CNOT}$$

$$\mathrm{AND}(x,y) = x \;\mathrm{AND}\; y = x \bullet y$$

$$\mathrm{OR}(x,y) = x \;\mathrm{OR}\; y = \overline{\overline{x} \bullet \overline{y}} = x \bullet y \oplus x \oplus y$$

See also formal logic, predicate calculus, etc...

10-I-20

LOGICAL REGISTERS AND THEIR MAPPINGS

N bits $\quad \vec{x} = (x_{N-1}, \ldots, x_2, x_1, x_0) \in \mathbb{B}^N$ Boolean vector

This vector can also be seen as an non-negative integer $x \in \{0,1,2,\ldots,2^N - 1\}$

used when no confusion: $x = \sum_{i=0}^{N-1} x_i 2^i$

$\vec{y} = \mathbf{A}\vec{x} \oplus \vec{b}$: affine function of a Boolean vector $\quad$ $\mathbf{A}$: Boolean matrix

Boolean scalar product of two Boolean vectors: (Boolean sum)

$$\vec{y} \odot \vec{x} = y_0 \cdot x_0 \oplus y_1 \cdot x_1 \oplus \ldots \oplus y_i \cdot x_i \oplus \ldots \oplus y_{N-1} \cdot x_{N-1}$$

Hamming scalar product of two Boolean vectors: (integer sum)

$$\vec{y} \cdot \vec{x} = y_0 \cdot x_0 + y_1 \cdot x_1 + \ldots + y_i \cdot x_i + \ldots + y_{N-1} \cdot x_{N-1}$$

$\|\vec{x}\| = \vec{x} \cdot \vec{x}$: Hamming norm $\quad$ $\|\vec{y} \oplus \vec{x}\|$: Hamming distance

10-I-21

THE MEASURE OF INFORMATION

(Shannon, 1948)

Consider a string of symbols x. Each string is a register content.
A higher level, we also define an ensemble of strings of the type of x, which defines a random variable X, from which x is a realization.

Entropy: $$H(X) = -\sum_{x \in \mathbb{X}} p(x) \log_2 \left[p(x) \right]$$

measures how uncertain X is (conversely, how much choice is represents, depending on point of view)

Mutual information: $$I(X;Y) = H(X) + H(Y) - H(X,Y)$$
$$= \sum_{x \in \mathbb{X}} \sum_{y \in \mathbb{Y}} p(x,y) \log_2 \left[\frac{p(x,y)}{p(x)\,p(y)} \right]$$

measures the mutual dependence of the two random variables X and Y.

10-I-22

INFORMATION CONSERVATION

General bijective (reversible) function:

$$\vec{x} \neq \vec{y} \Rightarrow f(\vec{x}) \neq f(\vec{y})$$

(permutation of first 2^N integers)

We can also say that f conserves information

Information is conserved by a process $X \rightarrow Y$ if

$$\forall X, I(X;Y)/H(X) = 1$$

(generalization of phase space volume conservation)

Hamiltonian evolution is information conserving.
We thus limit ourselves to reversible functions.

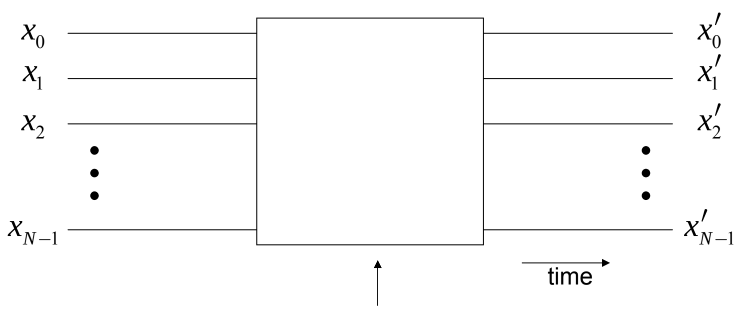
10-I-23

OUTLINE

1. Information and physics
2. Quantum bits
3. Classical information processing
4. Reversible logical circuits
5. Error correction
6. Linear vs non-linear processing

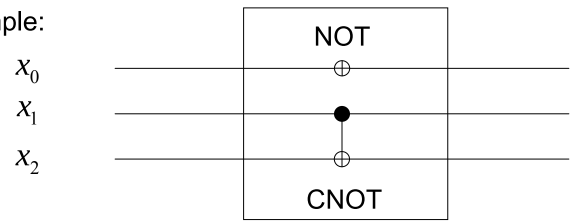
10-1-6d

STRUCTURE OF REVERSIBLE LOGICAL CIRCUITS



information preserving function, a.k.a. reversible computation

Example:



$x_0' = x_0 \oplus 1$

$x_1' = x_1$

$x_2' = x_2 \oplus x_1$

10-I-24

TRUTH TABLE

reversible function → CNOT

all register configurations:

c	t	c'	t'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

before | after

compact vector notation:

$$\begin{bmatrix} \vec{x}_0\,' \\ \vec{x}_1\,' \\ \vec{x}_2\,' \\ \vec{x}_3\,' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \vec{x}_0 \\ \vec{x}_1 \\ \vec{x}_2 \\ \vec{x}_3 \end{bmatrix}$$

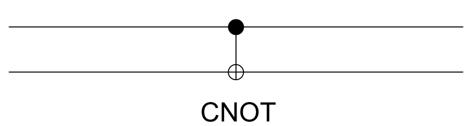
10-I-25

COPY, SWAP AND ERASE

COPY OPERATION

x_1 → $x_1' = x_1$

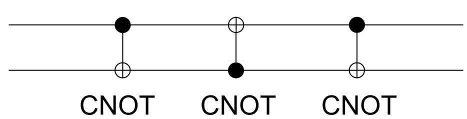
$x_2 = 0$ (ancilla bit) → $x_2' = x_1$



SWAP OPERATION

x_1 → $x_1' = x_2$

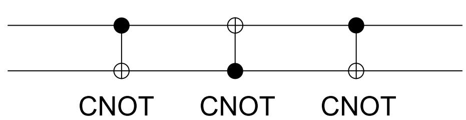
x_2 → $x_2' = x_1$



ERASE OPERATION

x_1 → $x_1' = 0$

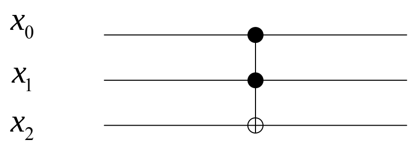
$x_2 = 0$ (ancilla bit) → $x_2' = x_1$



10-I-26

NON-LINEAR REVERSIBLE FUNCTIONS

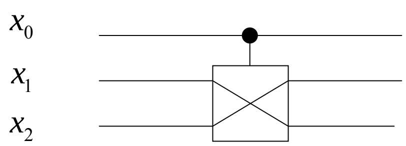
REVERSIBLE **AND** GATE



$x_0' = x_0$
$x_1' = x_1$
$x_2' = x_2 \oplus x_1 \bullet x_0$

CCNOT (a.k.a.Toffoli gate)

FREDKIN GATE



$x_0' = x_0$
$x_1' = x_1 \oplus (x_1 \oplus x_2) \bullet x_0$
$x_2' = x_2 \oplus (x_1 \oplus x_2) \bullet x_0$

CSWAP

10-I-27

UNIVERSAL SET OF GATES

The Toffoli and Fredkin gates are universal:
a series of either one of these gates can be used
to compute any reversible function.

The CNOT gate by itself is not universal.
It can only compute a linear reversible
function.

10-I-28

CONSERVATIVE REVERSIBLE FUNCTIONS

A conservative gate conserves the Hamming norm. It verifies:

$$\left\| f\left(\vec{x}\right)\right\| = \left\|\vec{x}\right\|$$

If 0 and 1 correspond to 2 different energies, a conservative gate conserves energy.

The SWAP and FREDKIN gates are conservative.

Neither the CNOT nor the CCNOT (Toffoli) are conservative.

Do not mix the notions of reversible gate and conservative gate!

10-I-29

OUTLINE

1. Information and physics
2. Quantum bits
3. Classical information processing
4. Reversible logical circuits
5. Error correction
6. Linear vs non-linear processing

10-1-6e

PARITY CHECK CODES

N+1 bits $\quad \vec{x}_C = \left(x_N, x_{N-1}, ..., x_2, x_1, x_0\right) \in \mathbb{B}^{N+1}$

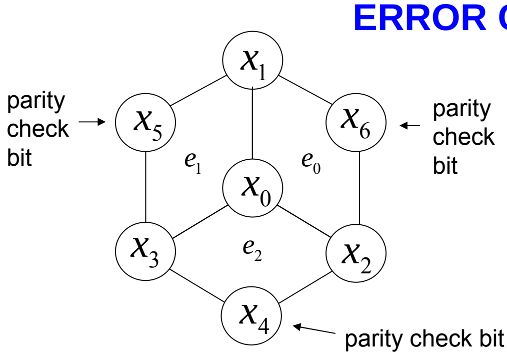
constraint: $\quad x_N = \sum_{i=0}^{N=1} \oplus x_i \quad \longleftarrow$ Boolean sum

↑ parity bit

If 1 or an odd number of errors occur, constraint is violated.
It is possible to detect that an error has occurred,
it is but impossible to correct it.

10-I-30

ERROR CORRECTING CODES



Example of Hamming code:
4 bits protected with 3 parity check bits

Constraints:

$$x_0 \oplus x_1 \oplus x_2 \oplus x_6 = 0$$
$$x_0 \oplus x_1 \oplus x_3 \oplus x_5 = 0$$
$$x_0 \oplus x_2 \oplus x_3 \oplus x_4 = 0$$

can be written as: $\mathbf{A}\vec{x}_C = 0$

where: $\quad i \longleftarrow$

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{matrix} f \\ g \\ h \end{matrix}$$

After one error:

$$\mathbf{A}\vec{x}_C' = \vec{e}$$

The error syndrome matrix $\mathbf{A}$ detects which error has occurred and corrects it

$$x_i \to x_i \oplus \left(e_0 \oplus \overline{f}[i]\right)\left(e_1 \oplus \overline{g}[i]\right)\left(e_2 \oplus \overline{h}[i]\right)$$

Requires 7 3-way AND + linear gates

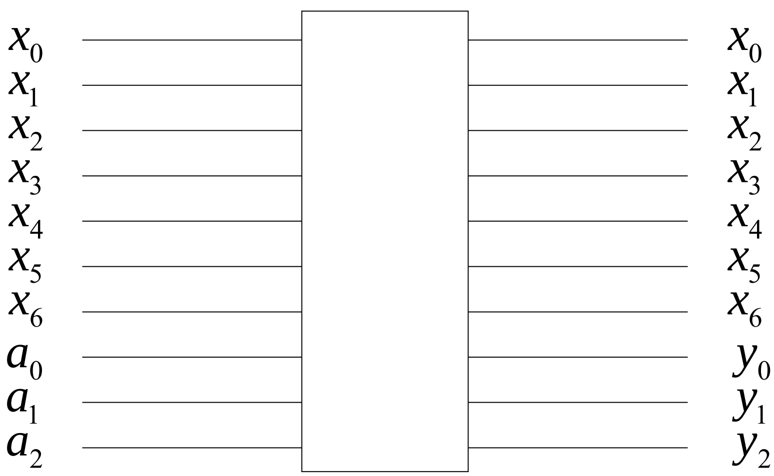
10-I-31

OUTLINE

1. Information and physics
2. Quantum bits
3. Classical information processing
4. Reversible logical circuits
5. Error correction
6. Linear vs non-linear processing

10-1-5a

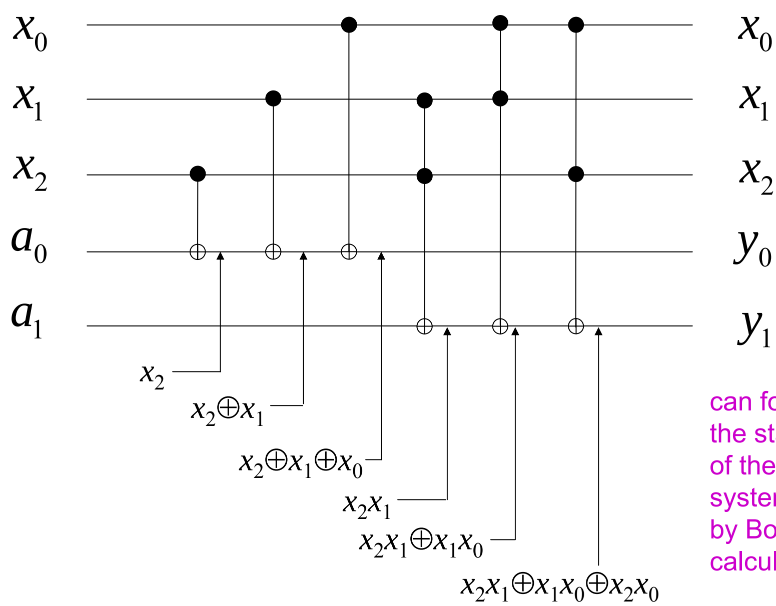
INTEGER ADDITION (HAMMING NORM EVALUATION) IS A NON-LINEAR OPERATION



$$s = \sum_{i=0}^{6} x_i = \|\vec{x}\| \qquad y_0 = s \bmod 2;\ y_1 = \left(\frac{s - y_0}{2}\right) \bmod 2;\ y_2 = \left(\frac{s - y_0 - 2y_1}{4}\right)$$

10-I-32

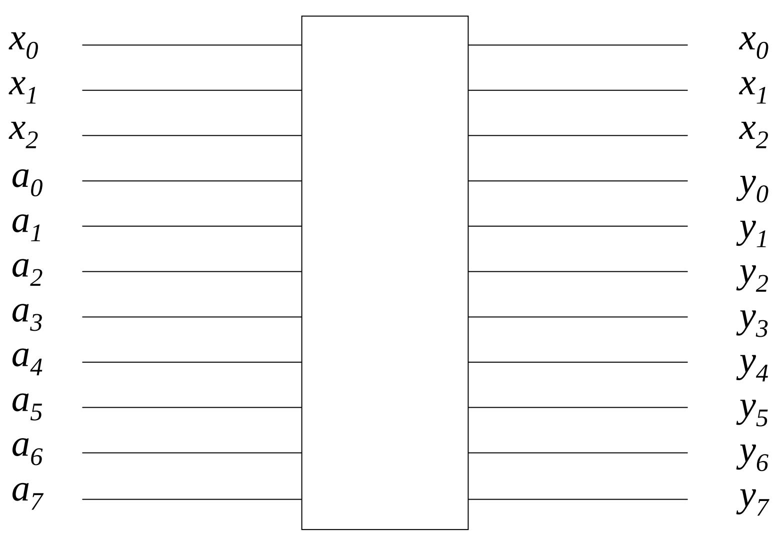
LOGICAL CIRCUIT FOR 3-BIT INTEGER ADDITION



can follow the state of the system by Boolean calculus!

10-I-33

ADDRESS DECODE IS ALSO AN IMPORTANT NON-LINEAR OPERATION



$$y_{b_0+2b_1+4b_2} = (b_0 \oplus x_0 \oplus 1)(b_1 \oplus x_1 \oplus 1)(b_2 \oplus x_2 \oplus 1)$$

10-I-34

WHAT ARE ALL THE LINEAR OPERATIONS ON TWO BITS?

Linear operation: group isomorphism $f(g_1 \cdot g_2) = f(g_1) \bullet f(g_2)$

transforms identity into identity

1 bit: only one trivial isomorphism $F \longrightarrow F$

where $F: \; b \rightarrow b \oplus 1$ is the flip operation on 1 bit

2 bits: 6 different isomorphisms:

Id	
IF	IF
FI	FI

$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$CNOT_{tc}$	
IF	IF
FI	FF

$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$CNOT_{ct}$	
IF	FF
FI	FI

$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$

$SWAP$	
IF	FI
FI	IF

$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$SWCN_{tc}$	
IF	FI
FI	FF

$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$

$SWCN_{ct}$	
IF	FF
FI	IF

$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

10-I-35

LINEAR OPERATIONS OF A REGISTER ARE GENERAL GROUP ISOMORPHISMS

Example: CNOT operation

$II\mathbf{IF}FIIIFIIIF \longleftarrow$ series of bit flips applied to register

$\downarrow$

$II\mathbf{FF}FIIIFIIIF \longleftarrow$ resulting series of bit flip after operation

The Toffoli or Fredkin gate do not share this property

They are “exterior” to the group structure of the register

QUANTUM INFORMATION ABOLISHES THESE CLASS DISTINCTIONS!

10-I-36

SELECTED BIBLIOGRAPHY

Books
Brillouin, L., "Science and Information Theory" (Academic Press, 1962)
Cover, T., and Thomas, J.A., "Elements of Information Theory" (Wiley, 2006)
Esteve, D., Raimond, J-M., and Dalibard J., "Quantum Entanglement and Information Processing" (Elsevier, Amsterdam, 2004)
Jaeger, G., "Quantum Information" (Springer, Berlin, 2007)
Kitaev, D. M., Shen A.H., and Vyalyi, M.N., "Classical Quantum Computation" (American Mathematical Soc., 2002)
Mermin, D., "Quantum Computer Science" (Cambridge University Press, 2007)
Nielsen, M. and Chuang, I., "Quantum Information and Quantum Computation" (Cambridge, 2001)
Shannon C. and Weaver W., M. "Mathematical theory of communication" (University of Illinois, 1949, 1998)
Walls, D.F., and Milburn, G.J. "Quantum Optics" (Springer, Berlin, 2008)

Review articles and theses
Bennett, Ch., Int. J. Theor. Phys. 21, 906 (1982) http://www.research.ibm.com/people/b/bennetc/chbbib.htm
Clarke, J. and Wilhelm, F. K., "Superconducting quantum bits". Nature 453, 1031–1042 (2008).
Dennis, E., Kitaev, A., Landahl A., and Preskill, J., "Topological quantum memory", quant-ph/0110143
Devoret, M. H., Wallraff A., and Martinis J. M., e-print cond-mat/0411174
Gottesman, D., "Stabilizer codes and quantum error correction" Caltech PhD thesis (1997) quant-ph/9705052
Gottesman, D., "Heisenberg representation of quantum information", quant-ph/9807006
Hein, M., Dur, W., Raussendorf, J., Van den Nest, R., and Briegel, H.,"Entanglement in Graph States and its Applications" quant-ph/0602096
Blais A., Gambetta J., Wallraff A., Schuster D. I., Girvin S., Devoret M.H., Schoelkopf R.J. Phys. Rev. (2007) A 75, 032329
Rigetti, C., Mosseri, R. and Devoret, M.H., "Digital quantum information", J. Quant. Infor. Proc. 3, 163-203
Schoelkopf, R.J., and Girvin, S.M., Nature **451**, 664 (2008).

10-I-37

END OF LECTURE