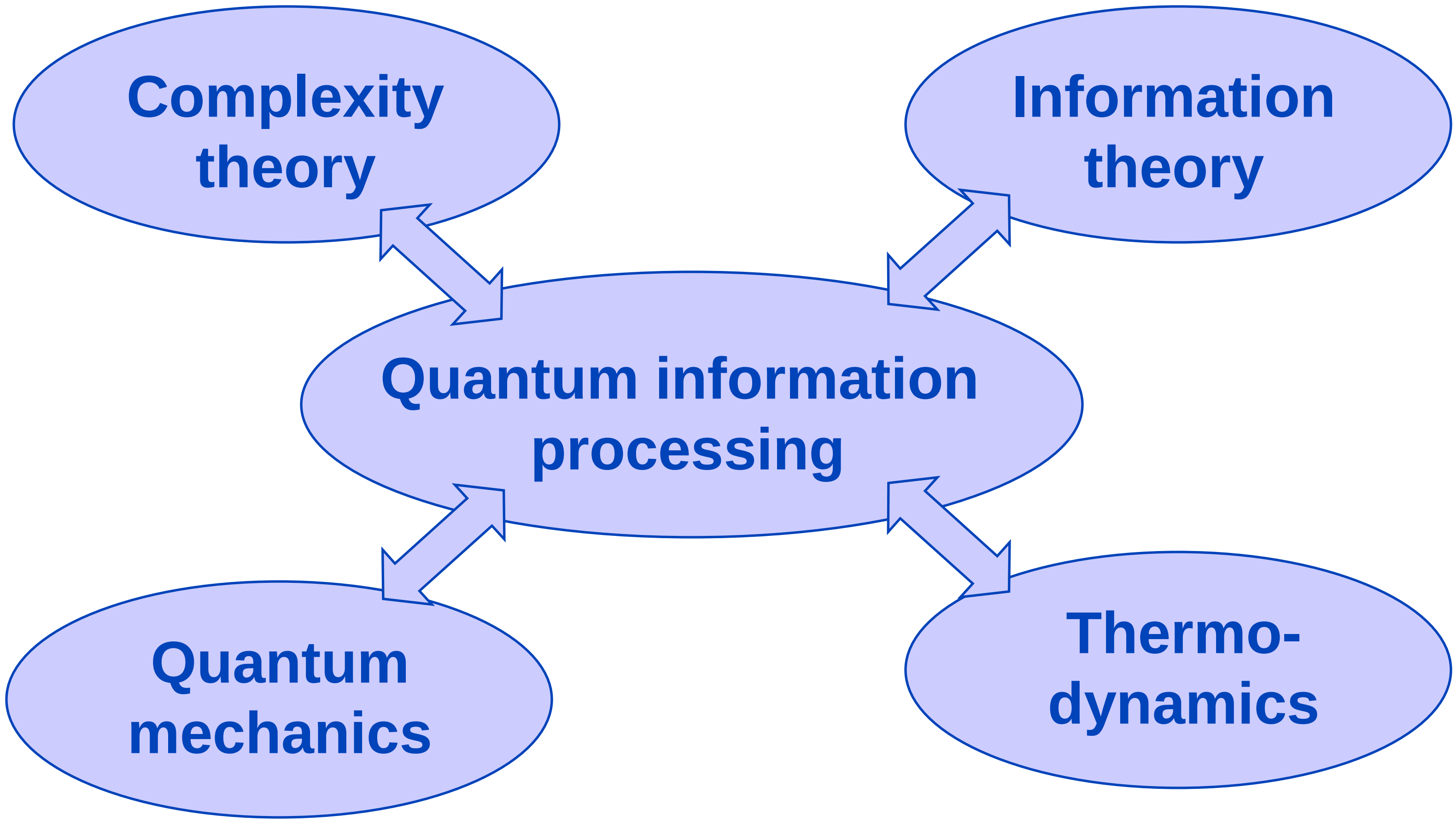
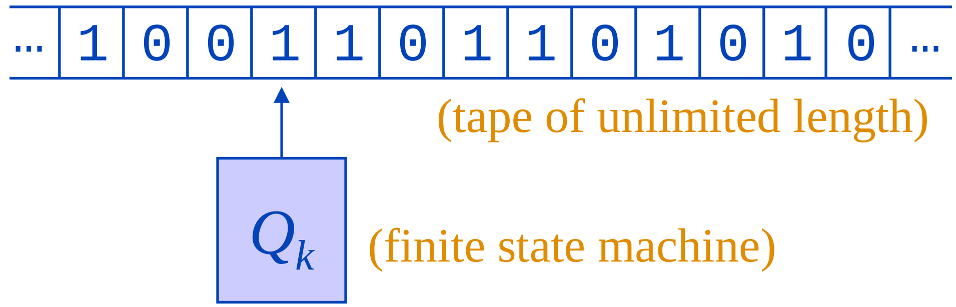

Complexity theory
Information theory
Quantum information processing
Quantum mechanics
Thermo-dynamics

Turing Machines (1936)

Alan M. Turing (1912-1954)

Enigma, theory of computability, UTM

Is there a universal model for computation?



$$< State_0, Symbol, State_{next}, New\ Symbol, Action >$$

Actions: (1) move left
(2) move right

⇒ Try designing a Turing machine for adding two numbers

Universal Turing machine

A universal Turing machine can mimic the operation of *any* Turing machine!

- Feed the UTM a tape with (1) description of the Turing machine T
  (2) the input string to T
- The UTM will then produce the same output string as T would produce, given the input
- Description of T can be given in the form of a binary string reflecting

$$< State_0, Symbol, State_{\text{next}}, New\ symbol, Action >$$

Is your PC a universal Turing machine?

Computability

A universal Turing machine can compute all functions computable on any machine

(Church-Turing thesis)

Are all functions computable?

NO:

1. There are uncountably many real numbers but only countably many Turing machines

2. Halting problem (related to Godel's theorem)

Complexity theory

A universal Turing machine can *efficiently* simulate any algorithmic process

(strong Church-Turing thesis)

No essential difference between an abacus and a supercomputer!
(they are polynomially equivalent)

"Efficient": the effort grows at most polynomially in the problem size
"Inefficient": … superpolynomially (e.g. expontially) …

Note: effort = time x size x precision (or energy)

Tractable versus intractable!

Information theory (1948)

Information contained in n equally likely messages?

$I = \log 2\, n$ bits

What about not equally likely messages?
By how much can we compress a bit string?

001010010100100011001…

000111111000000000111…

1000011000000010000010…

$H = p(0) \log_2 p(0) + p(1) \log_2 p(1)$ (for i.i.d rand var)

$p(0) = p(1) = 1/2$ -> $H = 1$ (bit)

The more random a state, the higher the entropy, the more information it can contain!

H(p) gives the maximum compression ratio possible

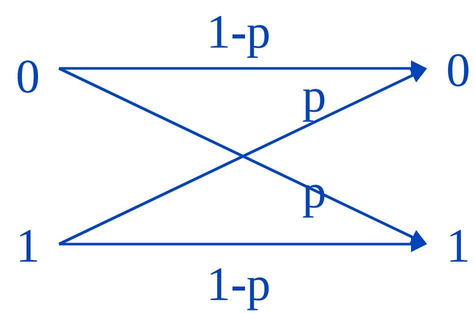
Claude Shannon (1916-2001)

Information theory (1948)

How much information can we transmit over a noisy channel?

Define channel capacity $C = I(X,Y) = H(Y) - H(Y|X)$

Example:



$C = 1 - H(p)$

Need redundancy for reliable data transmission

C gives the maximum (asymptotically) error-free data rate possible

Thermodynamics and computation

How much energy does it cost to compute ?
Is it possible to compute reversibly *?*

Note: Computers generates heat!
(N)AND gate is irreversible!

In	out
00	0
01	0
10	0
11	1

In	out
00	00
01	00
10	10
11	11

Fredkin gate

In	out
0**00**	**0**00
0**01**	**0**01
0**10**	**0**10
0**11**	**1**01
100	100
101	011
110	110
111	111

Computation costs no energy - erasing information does

Landauer's principle:

Bit erasure dissipates (kT ln2) to the environment

OR

Bit erasure increases entropy by (k ln2)

In reversible computation, no bits are erased and no energy is dissipated

Rolf Landauer
1927 - 1999

Information vs physics

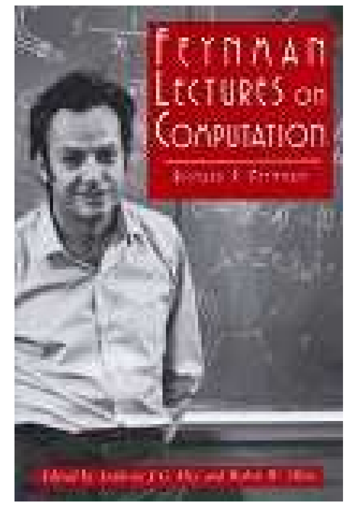
computation	⟷	physical process
computer	⟷	physical system
input	⟷	initial state
rules (algorithm)	⟷	laws of motion
output	⟷	final state

Deep questions about complexity theory, information theory, thermodynamics, are revisited when physical systems obey the laws of quantum mechanics

Computation with quantum systems

Paul Benioff:

prescription for classical computation
with quantum systems (unitary evolution)
(lecture 2)



Richard Feynman:

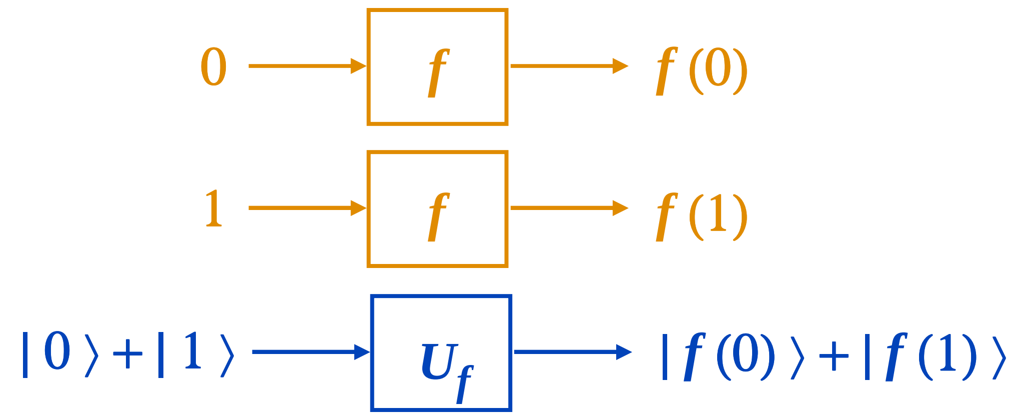
couldn’t we efficiently simulate quantum
systems using a “quantum computer” ?
(lecture 8)

David Deutsch:

a universal Turing machine cannot efficiently
simulate a quantum computer

(e.g. Deutsch’ problem , lecture 3)

Quantum Parallelism

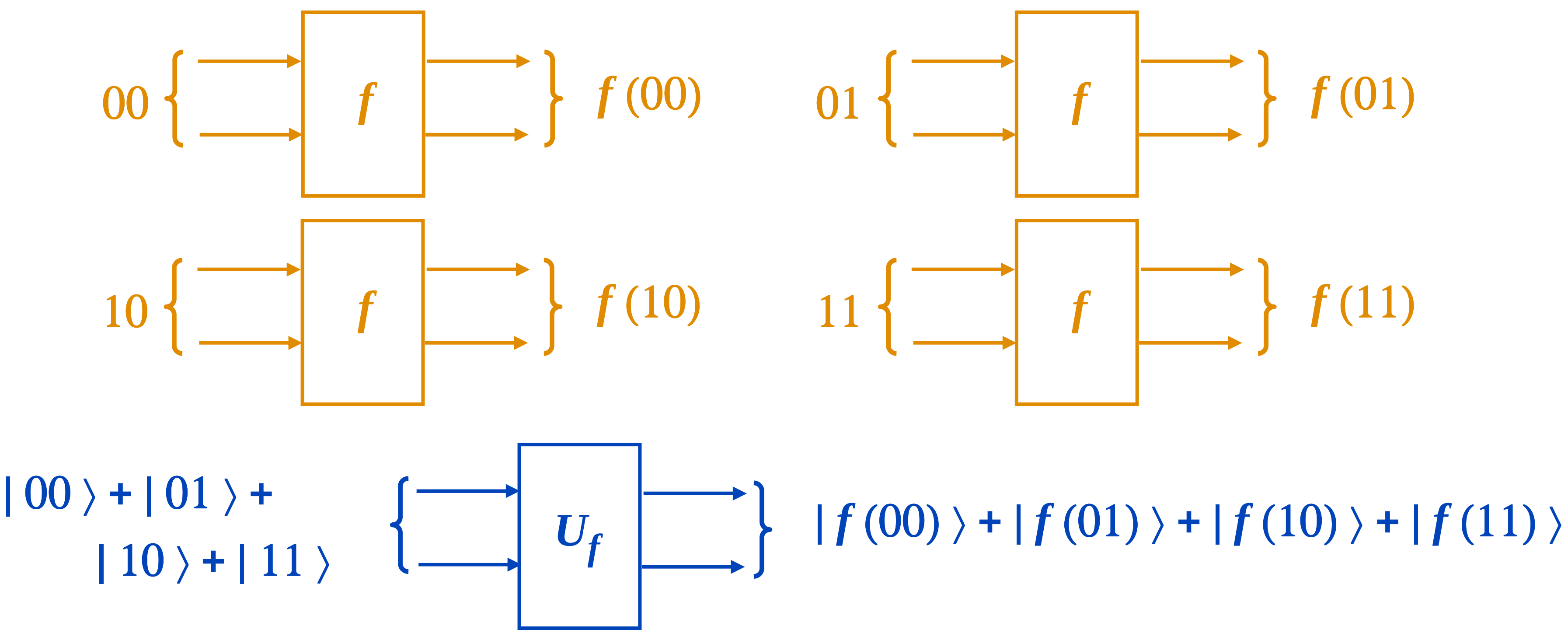


Computational power

classically $\propto n$

quantum $\propto 2^n$

D. Deutsch, 1985



Quantum algorithms

Measurement of $|\, f(0)\,\rangle + |\, f(1)\,\rangle$ gives either $f(0)$ or $f(1)$.

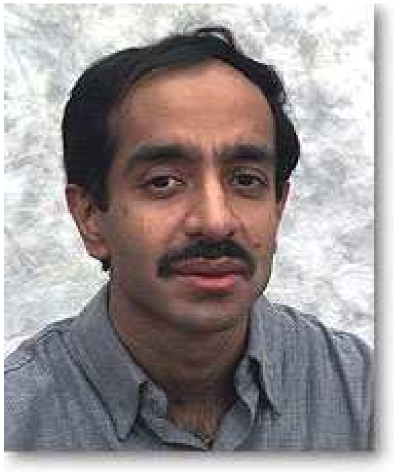
(lecture 5)

The exponential power appears inaccessible ...

Nevertheless: quantum algorithms make computational speed-ups possible !

Peter Shor (1994)
factoring (lecture 7)

Lov Grover (1996)
searching (lecture 8)



Quantum error correction

Decoherence destroys quantum parallelism.

(lecture 4,5)

⬇

The exponential power appears limited in time ...

Nevertheless: quantum error correction makes arbitrarily long quantum computations possible !

- Quantum error correction (P. Shor 1996, A. Steane 1996)
- Accuracy threshold (D. Aharonov 1997, A. Kitaev 1997, ...)

(lecture 6,9)

Quantum information and communication

How much information can
a quantum state contain?

Holevo bound (1973)

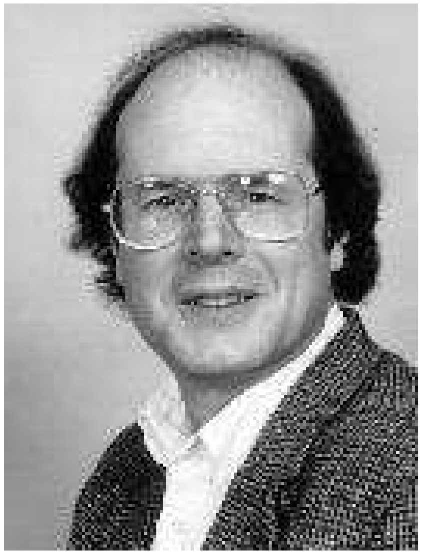
Can we copy unknown quantum states?

No-cloning theorem (1982)

(lecture 11)

Can quantum mechanics enhance
the channel capacity?

Superdense coding (1992)



Charles Bennett

Can quantum mechanics enhance security?

Quantum cryptograpy (1984) (lecture 10)

Can we transmit states without transmitting particles?

Quantum teleportation (1993) (lecture 3)

Practicalities

- Format:
  - lectures (15%)
  - presentations/discussion of experiments (25%)
  - homework (25%) – ok to discuss with others, not to copy
  - final exam (35%)
  - required reading: weekly discussion paper
  - optional reading: Nielsen & Chuang
  - ask commitment! it’s not a seminar series
- Website: http://qt.tn.tudelft.nl/~lieven/qip
  - schedule
  - problem sets and solutions
  - lecture notes and powerpoints
- Credit
  - 5 ECTS points, CRS, NS 3621
- Email list participants

	Date	Lecture	Discussion paper
1	14-sep	History, Q states and operations	-
2	21-sep	Hamiltonian, Universal quantum gates	Bell's inequalities
3	28-sep	Q circuit examples (teleportation)	DiVincenzo requirements
4	5-oct	Density matrix, non-unitary processes	Cavity QED
5	12-oct	Decoherence and q measurement	Ion trap - CZ gate
6	26-oct	Tomography and fidelities	NMR
7	2-nov	Shor’s algorithm	Q Measurement
8	9-nov	Grover’s algorithm + Q simulation	Optical lattices
9	23-nov	Quantum error correction	Meas. Based QC
10	30-nov	Quantum cryptography	Teleportation
11	7-dec	Quantum communication	Q cryptography