Quantum Information
- an introduction -

WS 2017/2018

0. Introduction
1. Quantum theory: some reminders
2. Entanglement: definition, measures, elementary applications
3. Quantum information transfer and error correction
4. Quantum cryptography
5. Quantum computing and algorithms
6. Experimental realizations

potential add-ons:

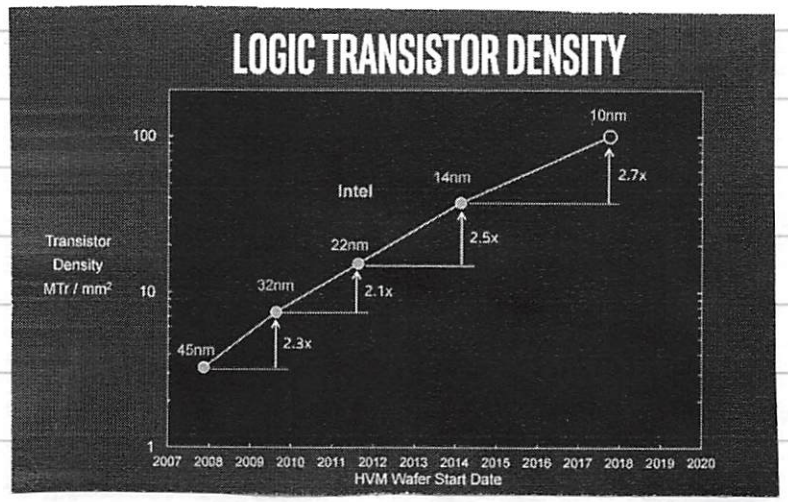
7. topological quantum computing
8. one-way quantum computing

0. Introduction

0.1. Why quantum information processing ?

- Moor's law: (Gerald Moore, co-founder of Intel)
  number of transistors on a computer chip increases by a factor of 2 every 18-24 month

between 2015-2020 each transistor has the size of few atoms
⇒ quantum effects!



logical operations such as "and" or "or" are irreversible and thus lead to production of heat
⇒ need for reversible elementary operations

> Future computer technology requires elementary processes which are revevsible and obay rules of quantum physics

➤ are quantum effects marely a technological barrier of information technology? no!

• Richard Feynman: 1st conference on the physics of computation (1981) in a side remark

simulation of dynamics of a general quantum system on classical computers is exponentially slower than the actual quantum dynamics, i.e. the time needed for the computation grows exponentially with the "size" of the quantum system

illustration: System of N spin 1/2; basis: $\{|0\rangle, |1\rangle\}$

dimension of Hilbert space $d = 2^N$

assume initial state $|\psi(t_0)\rangle$ product state

(1) $|\psi(t_0)\rangle = \underbrace{|0\rangle|1\rangle|0\rangle \cdots |0\rangle|1\rangle}_{N \text{ binary numbers}}$ N bit

(2) $|\psi(t)\rangle = \sum_{i=0}^{2^N-1} \alpha_i(t)\,|i\rangle$

$|i\rangle \in \begin{cases} |10000\ldots\rangle \\ |11000\ldots\rangle \\ |10100\ldots\rangle \\ \vdots \\ |111\ldots\rangle \end{cases}$ 2^N different states

classical simulation requires storage and processing of 2^N complex numbers with sufficient accuracy!

$N = 100$ $\quad 2^{100} \sim 10^{30}$!!!

classical computers can simulate quantum many-body problems in general only inefficient

reversion of argument (Feynman): a quantum mechanical experiment replaces an exponentially costly classical calculation

⇒ a computation machine physically realized by a quantum system could outperform a classical computer

0.2 potentials of quantum information processing

(i) secure information transfer (cryptography)
- BB84 protocol (Bennet, Brasad 1984)
- Deutsch-Ekert Protocol (Ekert et al. 1992)

- uses properties of q.m. measurement process (measurement changes quantum state)
- no-cloning theorem

$$|\varphi\rangle|0\rangle \not\longrightarrow |\varphi\rangle|\varphi\rangle$$

in general impossible

(ii) data super compression ("dense coding")
a quantum bit can transfer two classical bits

(iii) quantum algorithms

- Grovers search algorithm
  L. Grover PRL 78, 325 (1997)

search in unsorted list (telephone book backwards)

- classical: $N/2$ inquiries needed
- q.m. $\sqrt{N}$ tests sufficient

rem: $N = 2^{\log N}$ $\quad \sqrt{N} = 2^{\frac{1}{2}\log N}$

both scale exponentially with $\log N \hat{=}$ number of classical bits to encode N

- Shors factorization (1994)

given: $N \in \mathbb{N}$ task: find $k \neq 1, N$ $k \in \mathbb{N}$ such that k is divider of N

- naive approach: test all numbers from $k=1$ to $\sqrt{N}$
  $\Rightarrow$ on average $\sqrt{N}/2$ trials needed $= 2^{\frac{1}{2}\log N}$

- best classical prime-number sieve

$$\exp\{(\log N)^{1/3}(\log\log N)\}$$

- Shore: $O(\text{poly}(\log N))$!!

factorization is believed to be an NP problem and Shore's quantum algorithm turns this into a P problem

NP problem: - solution difficult (effort to solve scales exponentially with size of problem ($\log N$))

- verification simple (an efficient algorithm exists)

Example $5 \times 7 \Rightarrow \boxed{35}$ $\quad 49 \Rightarrow \boxed{7} \times \boxed{7}$

$17 \times 29 \Rightarrow \boxed{435}$ $\quad 589 \Rightarrow \boxed{19} \times \boxed{31}$

simple $\quad$ difficult

Shores algorithm could be used to break the RSA code used in todays cryptographic schemes

0.3 Potential problems of quantum information processing

- controlled coherent manipulation of large number of microscopic quantum systems needed $\Rightarrow$ difficult!
- Rolf Landauer: processing of quantum information requires coupling of a quantum system to its environment. This leads necessarily to unwanted decoherence

- note: "amplification" of quantum information is not possible (as we will see); there is however a way out ⇒ quantum error correction

Literature

- older but still good reviews as introduction
  - A. M. Steane "quantum computing" quant-ph/9708022
  - A. Ekert, R. Jozsa Rev. Mod. Phys. 68, 733 (1996)
  - J. Preskill "Lecture notes for physics 229: quantum information & computation" (1998)
- books
  - M. A. Nielsen, I. L. Chuang "Quantum Computation and Quantum Information" Cambridge Univ Press 2000