# 1 Introduction and Survey

## 1.1 Motivation: why quantum computers

Over the past twenty years, much of the world economy has been driven by the development in microelectronics and information technology.

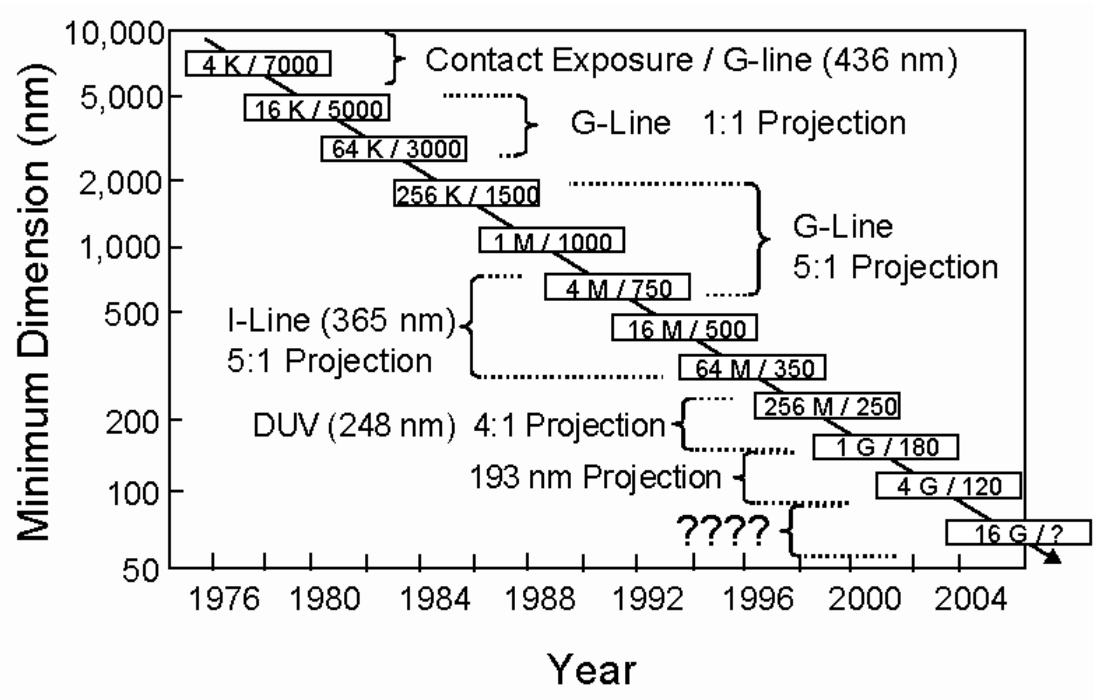



Figure 1: Prospective evolution of feature size in microelectronics circuits.

**Roadmap** – The feature size of electronic devices is now in the range of $100\,\mathrm{nm} = 100 \times 10^{-9}$ m and decreasing at a rate of some 12% per year. According to this roadmap, feature sizes of 50 nm will be reached in the year 2013. At the same time the operational voltage decreases to less than one Volt.

**Number of electrons** – The capacity of a spherical capacitor is $C = 4\pi\epsilon_0 r$. For a spherical capacitor with radius 50 nm, the capacity is therefore of the order of $5 \cdot 10^{-18} C$. A change in the voltage of 0.1 V will then move less than four electrons in such a device. While intelligent designs will be able to avoid problems from such effects, the quantization of charge will certainly become noticeable in electronic devices around the year 2020. By that time, quantum mechanics will have to be considered explicitly when the design and function of electronic devices is analyzed.

**Quantum information** – While this may appear as a nuisance to many engineers, it also represents an enormous potential, since devices that incorporate quantum mechanical effects into their principle of operation may be much more powerful than conventional (classical) devices. The emerging research field of quantum information processing (qiv) studies the possibilities provided by such an approach and tries to develop algorithms and implementations to harness this potential.

## 1.2 History of quantum information processing

**Quantum dynamics vs. electro-dynamics** – Quantum mechanics has always been the basis for understanding the properties of semiconductor materials, which form the basis of today's computers. However, if one is not interested in the first principles derivation of these materials properties, it is well possible to describe the operation of todays computers by classical electrodynamics.

It was soon recognized that the situation might be different when the components keep shrinking in size, thus approaching atomic dimensions. In such a situation, quantum mechanics will certainly have to be taken into account explicitly. Quantum effects may prevent current electronic circuits from functioning, e.g. when the Coulomb blockade prevents current from flowing.

**Quantum dynamics vs. boolean logics** – On a more fundamental level, one may ask how quantum mechanics can describe Boolean logic. In particular, logical gates like AND are clearly not reversible, since it is not possible to calculate the input from the output. Quantum mechanics, on the other hand, describes all time evolution with unitary operators, such as $\exp(iHt)$, which are obviously time-reversible ($\exp(iHt)\exp(-iHt) = 1$).

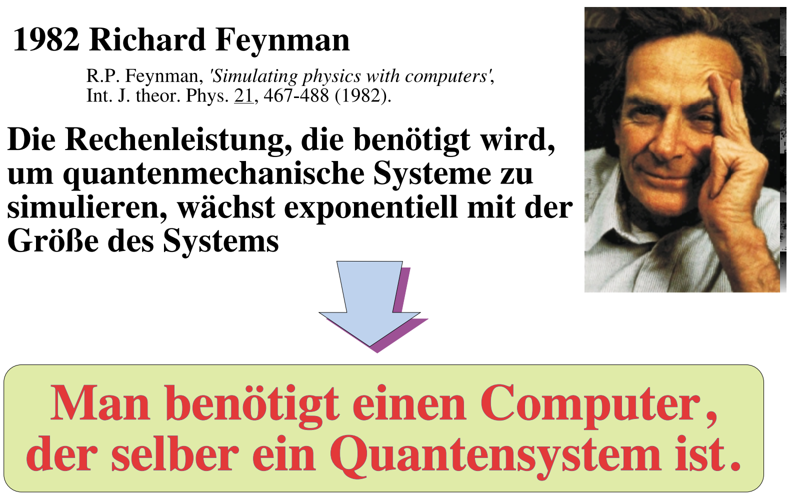
**Quantum simulation of Boolean logics** – Several people, such as Bennett, Fredkin, and Toffoli started to discuss the possibility of describing computer operation quantum mechanically. They showed, e.g., that algorithms based on Boolean logic can also be adapted to reversible logic. In 1982, Benioff [9] showed that quantum mechanical systems can efficiently simulate classical systems. This proved that quantum mechanical systems are at least as powerful as classical systems.

**Classical simulation of quantum systems** – In the same year, Richard Feynman asked the opposite question: Can classical computers efficiently simulate quantum mechanical systems [11].

**Exponentionally increasing Hilbert-space** – He noted that the number of variables required to describe the system grows exponentially with its size. As an example consider a system of N spins 1/2. The size of the corresponding Hilbert space is $2^N$ and a specification of its wavefunction therefore requires $2^{2N} - 1$ real numbers. On any given (classical) computer, the duration of a simulation will therefore grow exponentially with the number of particles in the quantum system. He concluded that classical computers will never be able to exactly simulate quantum mechanical systems containing more than just a few particles.

**Exactly solvable many-body problems** – Of course, these considerations only take the general case into account. If the particles (or at least the majority) do not interact, e.g., it is always possible to perform the computation in a smaller Hilbert space, thus reducing the computational requirements qualitatively. Another special case of great interest in solid-state physics is given by the class of exactly solvable many-body systems (Bethe-Ansatz), where the exponentially large number of degrees of freedom can be mapped onto a set of integral-equations.

**The Feynman conjecture** – The best solution to quantum-mechanical many-body problem is provided by nature, i.e. by experiments of physical realizations of the model Hamiltonian. Alternatively, Feynman offered the insight: "Quantum computers - universal quantum simulators". He shows that the drastic increase in the computation time is a direct consequence of the large amount of information in the quantum mechanical system. This implies that quantum systems are efficient processors of information. He states "I therefore believe it is true that with a suitable class of quantum machines you could imitate any quantum system, including the physical world." As an open question he asks which systems could actually be simulated and where it would be useful.




**Universal quantum simulators** – A first proof of the Feynman conjecture was given in 1993 by Bernstein, Vazirani, and Yao. They showed that a quantum mechanical Turing machine was capable of simulating other quantum mechanical systems in polynomial time. In the following years, several people developed algorithms that would run more efficiently on quantum computers than on classical machines. However, these examples were relatively artificial and of little practical relevance.

**Specialized "quantum" algorithms** – The first example of an algorithm that used the power of quantum computers and may have practical relevance was provided by Peter Shor in 1994 [12]. He discusses (amongst other problems) an algorithm for the factorization of prime numbers. The best classical algorithms for factorization of an $l$ digit number use a time that grows as $\exp(cl^{(1/3)}(\log l)^{(2/3)})$, i.e. exponentially with the number of digits. He proposes a model for quantum computation and an algorithm that solves the factorization problem in a time proportional to $O(l^2 \log l \log \log l)$, i.e. polynomially in time.

**NP-hard vs. polynomial** – This is a qualitative difference: algorithms that are polynomial in time are considered "efficient", while exponential algorithms (NP-hard) are not usable for large systems. The different behavior will always make classical computers slower than quantum computers at some system size, independent of the speed at which individual operations are performed. This can be seen by putting in some numbers for the above example. We will assume that a fast classical computer can factorize a 50 digit number in one second, while the quantum computer may take as much as an hour for the same operation. Setting the constant c in the above formula to 1 (it was not specified in Shor's paper),

If the number of digits increases to 300, both computers require some 2.5 days to solve the problem. A further increase to 1000 digits requires 42 days on the quantum computer, while the classical computer would need some 19000 years - clearly too long for any practical purposes. With 2000 digits, the quantum computer needs half a year, while the computation time on the classical computer becomes roughly equal to the age of the universe.

## 1.3 Quantum communication

**Classical encoding** – One of the most active areas of quantum information processing is quantum communication, i.e. the transfer of information encoded in quantum mechanical degrees of freedom. Semiclassically, a photon can carry a bit: it can be transmitted or not, thus corresponding to a logical 0 or 1. Other encoding schemes include the polarization of the photon, which may be vertical or horizontal.

**Quantum-mechanical encoding** – Quantum mechanically, a photon has to be described by a vector in Hilbert space. If we consider polarization, e.g., the relevant part of Hilbert space is the spinor

$$\psi \;=\; a\psi_x + b\psi_y \;, \qquad\qquad |a|^2 + |b|^2 = 1 \;,$$

, where $\psi_x$ and$\psi_y$ describe linear polarization states in the two direction. The two parameters a and b are both complex numbers. Taking normalization into account, the system is therefore described by three continuous variables (the angles $\varphi,\ \alpha,\ \beta$):

$$a = \cos(\varphi)\, e^{i\alpha} \;, \qquad\qquad b = \sin(\varphi)\, e^{i\beta} \;.$$

**Information vs. measurement** – This does not mean, however, that it is possible to store an infinite amount of information in a single photon. To obtain the information content, one has to take the measurement process into account: it is never possible to exactly measure the quantum state of a single photon. A single measurement can only measure one degree of freedom and returns a single bit (particle found or not). A complete measurement of the state of a single photon would thus require repeated measurements, which were possible if one could prepare copies of the actual quantum mechanical state. However, this is prohibited by the “no cloning theorem”, which states that no process can duplicate the exact quantum state of a single particle.

**Two-level system: two classical bits** – While the details of the calculation are rather involved, it is possible to show that a single quantum mechanical two-level system can transfer up to two classical bits of information. This is just one example that proves the by now famous saying “information is physical”, which means that information is not just an abstract concept, but must always be related to the physical system carrying the information. Quantum communication has evolved into a very active field. Besides the fundamental interest, it promises a number of possible applications: taking quantum mechanics into account may improve the information content of communication channels, as discussed above.

**Secure quantum communication** – It has been shown that communication with individual photons may be made secure, i.e. it is impossible to tap into such a communication without the users of the communication line noticing it. This is a consequence of the no-cloning theorem: While it is conceivable that an eavesdropper intercepts a photon, thus detecting that information is being transferred, and re-emitting the photon to the original receiver, he cannot send an exact copy of the original photon. If the communication protocol were to use only the presence or absence of the photon as the information, the eavesdropper would be able to use QND (=quantum nondemolition detection) to observe the passage of the photon. Such experimental schemes can measure a given quantum mechanical variable (such as light intensity) without affecting this variable (i.e. changing the number of photons). They must, however, change the conjugate variable, in this example the phase of the photon, thus allowing the original recipient to detect the presence of the eavesdropper.

## 1.4 Quantum computer: principle of operation

**Qubits and quantum registers** – A quantum computer, i.e. a programmable quantum information processing device, encodes the information in the form of a quantum register, consisting of a labeled series of quantum bits or qubits. Each qubit is represented by a quantum mechanical two level system, such as a spin 1/2. While today’s quantum registers are limited to 7 qubits, a useful quantum computer will require several hundred to 1000 qubits. Before an actual computation, the quantum register must be initialized into a well defined state, typically the ground state $|0, 0, ...0>$.

**Quantum gates** – Quantum gates operate on quantum registers (many-body

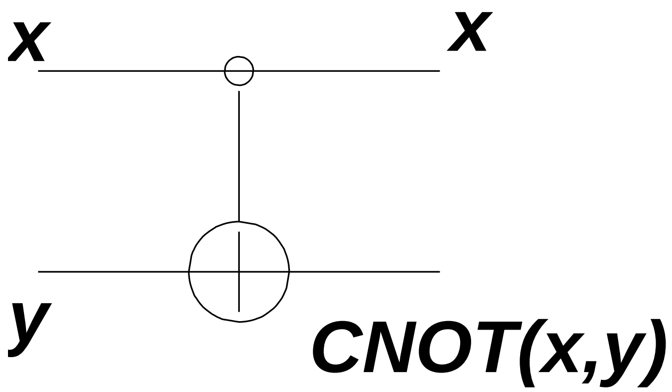



Figure 2: The controlled-not gate.

wavefunctions); the sequence of quantum gates required depends on the specific algorithm. The sequence of operations, i.e. the program, may be stored in a classical device associated with the quantum computer, such as a classical computer. These operations can be represented as unitary transformations, typically of the form $\exp(-iHt)$.

**Minimum gates** – It has been shown that a general purpose computer can be built on the basis of the following quantum gates:

- single qubit operations, corresponding to arbitrary rotations $R(\theta, \phi)$
- one type of 2-qubit operations, e.g. the "controlled not" or CNOT

The CNOT 2-qubit operation corresponds to the following truth table:

| control-qubit | target-qubit | result |
|---|---|---|
| 0 | 0 | 00 |
| 0 | 1 | 01 |
| 1 | 0 | 11 |
| 1 | 1 | 10 |

**What a QC needs** – Any implementation of a quantum computer must therefore provide the possibility of performing one-qubit operations on arbitrary qubits, without affecting other qubits. It must therefore include a means of addressing individual qubits. The 2-qubit operations must also be applied to arbitrary pairs of qubits. It is possible, however, to decompose a 2-qubit operation between any pair into a series of 2-qubit operations between nearest neighbors. Such schemes are often much easier to implement than schemes with interactions between arbitrary pairs. The number of 2qubit operations is larger, but increases only linearly with the number of qubits. The overall process therefore remains efficient.

## 1.5 Some quantum mechanics

The following material (compare, for example, Chapter 2 of Ref. [8] ) should be a mere recapitulation of the quantum mechanics course for everybody how has attended one. We will touch on

- Vectors in Hilbert space
- Operators in Hilbert space
- Dynamics: the Schrödinger equation
- The two-dimensional Hilbert space: Spins and single qubits
- Two qubits and the density matrix

### 1.5.1 Vectors in Hilbert space

**Finite number of degrees of freedom** – Systems with a finite number of particles in a bounded region of space (non-ionized atoms, for example) have a *discrete spectrum* of energy eigenvalues. For the time being we *neglect* the continuous spectrum which may exist in other systems. It will later make its appearance in a cumbersome way anyway ($\rightarrow$ dissipation, decoherence).

For mathematical simplicity we will even assume that the dimension $d$ of the Hilbert space is *finite*. $d = 2$ will be the important special case of a single qubit.

**Hilbert space** – The Hilbert space is a $d$-dimensional complex linear space: every linear combination of allowed states (Hilbert space vectors) is an allowed state too; scalar product, norm, etc can be defined as usual:

$d$-dimensional (column) vector: $|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ . \\ . \\ a_d \end{pmatrix}$

corresponding (row) vector $\langle a| = (a_1^*, a_2^*, \ldots, a_d^*)$ (*: complex conjugation)

**Dirac notation** – The notation $|a\rangle$ (ket) and $\langle a|$ (bra) is called the Dirac notation. It makes life simple since the bra- and the ket-vectors are coordinate independent representations, the $a_1$ are the amplitudes. The scalar product is

$$\langle a|b\rangle \; = \; \sum_{i=1}^{d} a_i^* \, b_i \; .$$

It suffices to consider normalized states $|\psi\rangle$, that is, $\langle\psi|\psi\rangle = 1$.

**Phase factors** – The states $|\psi\rangle$ and $e^{i\alpha}|\psi\rangle$($\alpha$ real) are physically equivalent: overall phase factors do not matter. However, *relative* phases between components of a state are *extremely* important:$|\phi\rangle + |\psi\rangle$ and $|\phi\rangle + e^{i\alpha}|\psi\rangle$ may have completely different physical properties.

### 1.5.2 Operators in Hilbert space

*Operators* map states (*linearly*) to each other; they thus are $d \times d$ complex matrices operating on the $d$-dimensional Hilbert space.

$$\mathbf{A}|\psi\rangle = |\phi\rangle , \qquad \sum_{\mathbf{j}=\mathbf{1}}^{\mathbf{d}} (\mathbf{A})_{\mathbf{ij}} \, \psi_{\mathbf{j}} = \phi_{\mathbf{i}}$$

*Observables*, that is, measurable quantities correspond to *self-adjoint* or *Hermitian* matrices, that is,

$$\mathbf{A}^\dagger = \mathbf{A}; \quad (\mathbf{A}^\dagger)_{\mathbf{ij}} := (\mathbf{A})^*_{\mathbf{ji}}$$

Self-adjoint operators have real eigenvalues (measurable quantities!); their eigenstates are pairwise orthogonal (or can be orthogonalized in the case of degeneracy). Thus they form a *basis* in Hilbert space.

$$\mathbf{A}|\mathbf{a_i}\rangle = \mathbf{a_i}|\mathbf{a_i}\rangle \quad (\mathbf{i} = \mathbf{1}, \ldots, \mathbf{d})$$

$$\langle a_i | a_j \rangle = 0 \text{ for } i \neq j$$

... and for normalized states we have

$$\langle a_i | a_j \rangle = \delta_{ij} \quad (\text{ Kronecker-}\delta)$$

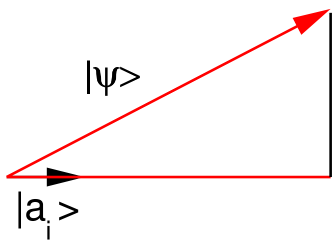
**Projection operators** – Eigenstates and eigenvalues characterize an operator completely, because any arbitrary state can be expanded in eigenstates of **A**. This leads to the *spectral representation* of **A**. To define that representation we need a further class of operators: *projection operators* or *projectors* for short.

$$\mathbf{P_i} := |\mathbf{a_i}\rangle\langle\mathbf{a_i}|$$

Action on an arbitrary state $|\psi\rangle$

$$\mathbf{P_i}|\psi\rangle = |\mathbf{a_i}\rangle\langle\mathbf{a_i}|\psi\rangle = \underbrace{\langle a_i|\psi\rangle}_{\text{a number}} \; |\mathbf{a_i}\rangle$$

$|\langle a_i|\psi\rangle|$is the length of the projection of $|\psi\rangle$ on the unit vector $|a_i\rangle$:




For orthonormal $|a_i\rangle$ (i.e. $\langle a_i|a_j\rangle = \delta_{ij}$) we have

$$\mathbf{P_i P_j} = \delta_{\mathbf{ij}} \mathbf{P_j}; \qquad \text{especially} \qquad \mathbf{P_i^2} = \mathbf{P_i},$$

and as the $\mathbf{P_i}$ cover "all directions" of Hilbert space:

$$\sum_{i=1}^{d} \mathbf{P_i} = \sum_{\mathbf{i=1}}^{\mathbf{d}} |\mathbf{a_i}\rangle\langle\mathbf{a_i}| = \mathbf{1}$$

(completeness). Now we can define the *spectral representation* of $\mathbf{A}$:

$$\mathbf{A} = \sum_{\mathbf{i=1}}^{\mathbf{d}} \mathbf{a_i}\mathbf{P_i} = \sum_{\mathbf{i=1}}^{\mathbf{d}} \mathbf{a_i}|\mathbf{a_i}\rangle\langle\mathbf{a_i}|$$

An arbitrary state is decomposed into components along eigenstates, each such component is treated accordingly.

**Quantum mechanical measurement** – A POSTULATE of quantum mechanics states :

(i) A (single) *measurement* of the observable $\mathbf{A}$ in the (normalized) state $|\psi\rangle$ yields one of the eigenvalues $a_i$ of $\mathbf{A}$ with probability $|\langle a_i|\psi\rangle|^2$ $(\sum_i |\langle a_i|\psi\rangle|^2 = 1$ due to normalization).

(ii) Immediately after the measurement the system is in the (normalized) state

$$\frac{\mathbf{P_i}|\psi\rangle}{||\mathbf{P_i}|\psi\rangle||}.$$

(iii) In general it is not possible to predict the outcome of a measurement. A measurement of $\mathbf{A}$ on an ensemble of systems prepared in the same state $|\psi\rangle$ yields the *average* (expectation value)

$$\langle\mathbf{A}\rangle := \langle\psi|\mathbf{A}|\psi\rangle$$

with deviations described by the *variance*

$$\langle(\mathbf{A} - \langle\mathbf{A}\rangle)^{\mathbf{2}}\rangle \geq \mathbf{0} \qquad (\text{ "=" for an eigenstate })$$

(Note that we have just discussed two different kinds of measurement.)

### 1.5.3 Dynamics: The Schrödinger equation

A state $|\psi(t)\rangle$ evolves according to the "time-dependent" *Schrödinger equation*

$$\frac{d}{dt}|\psi(t)\rangle = -\frac{i}{\hbar}\mathbf{H}|\psi(\mathbf{t})\rangle$$

Where $\mathbf{H}$ is the Hamiltonian. $\mathbf{H}$ is a $d \times d$ matrix, as every operator and it is hermitian since it represents the ENERGY OPERATOR and the energy can be measured. The for of the Hamilton operator depends on the physical settings.

**Eigenstates** – If $|\phi_i\rangle$ is an eigenstate of the Hamiltonian with energy eigenvalue $\varepsilon_i$:

$$\mathbf{H}|\phi_\mathbf{i}\rangle = \varepsilon_\mathbf{i}|\phi_\mathbf{i}\rangle$$

("time-independent Schrödinger equation") then

$$|\psi(t)\rangle = \exp\left(-i\frac{\varepsilon_i t}{\hbar}\right)|\phi_i\rangle$$

is a solution of the time-dependent Schrödinger equation with initial condition

$$|\psi(t=0)\rangle = |\phi_i\rangle.$$

Obviously this is a *stationary* state, as a global phase factor has no physical significance. As any initial state $|\psi(t=0)\rangle$ can be expressed as a linear combination of eigenstates $|\phi_i\rangle$ of $\mathbf{H}$, the initial value problem is solved (at least in principle).

**Time evolution operator** – Formally the solution for TIME-INDEPENDENT $\mathbf{H}$ can be written as

$$|\psi(t)\rangle = \exp\left(-i\frac{\mathbf{Ht}}{\hbar}\right)|\psi(t=0)\rangle.$$

The *time evolution operator* $\mathbf{U}(\mathbf{t}) := \exp\left(-\mathbf{i}\frac{\mathbf{Ht}}{\boldsymbol{\hbar}}\right)$ may be defined/interpreted in two ways:

i) as a power series

$$\exp\left(-i\frac{\mathbf{Ht}}{\hbar}\right) = \mathbf{1} + \left(-i\frac{\mathbf{Ht}}{\hbar}\right) + \frac{1}{2}\left(-i\frac{\mathbf{Ht}}{\hbar}\right)^2 + \frac{1}{6}\left(-i\frac{\mathbf{Ht}}{\hbar}\right)^3 + \cdots$$

ii) by means of the spectral representation

$$\exp\left(-i\frac{\mathbf{Ht}}{\hbar}\right) = \sum_{i=1}^{d}\exp\left(-i\frac{\varepsilon_i t}{\hbar}\right)|\phi_i\rangle\langle\phi_i|$$

For *time-dependent* $\mathbf{H}(\mathbf{t})$ the time-evolution operator $\mathbf{U}(\mathbf{t})$ is still well defined: $|\psi(t)\rangle = \mathbf{U}(\mathbf{t})|\psi(\mathbf{0})\rangle$. It is then solution of an operator differential equation; for completely general time dependence the solution of that equation is not even known for $d=2$.

**Properties of U** – All eigenvalues $\exp\left(-i\frac{\varepsilon_i t}{\hbar}\right)$ of $\mathbf{U}(\mathbf{t})$ have unit modulus; operators with this property are called **unitary**. $\mathbf{U}$ preserves all scalar products, that is, the scalar product of $|\psi\rangle$ and $|\chi\rangle$ equals that of $|\psi'\rangle = \mathbf{U}|\psi\rangle$ and $|\chi'\rangle = \mathbf{U}|\chi\rangle$:

$$\langle\chi'|\psi'\rangle \;=\; \langle\chi|\mathbf{U}^\dagger\,\mathbf{U}|\psi\rangle \;=\; \langle\chi|\psi\rangle\ .$$

Consequently *norms* are preserved too. Thus unitary operators are *rotations* in Hilbert space. The general property characterizing unitarity is

$$\mathbf{U}^\dagger \mathbf{U} = \mathbf{1} \qquad \Leftrightarrow \qquad \mathbf{U}^\dagger = \mathbf{U}^{-1}.$$

For time-independent $\mathbf{H}$ we have

$$(\mathbf{U}(\mathbf{t}))^{-1} = \mathbf{U}(-\mathbf{t}),$$

that is, unitary time evolution is reversible.

**State changes** – Up to now we know two kinds of change of state:
i) unitary time evolution: deterministic and reversible
ii) measurement: probabilistic and irreversible.
Why is the measurement different from another physical process governed by a Hamiltonian? This can by microscopically not correct, since all the world and also the measurement is governed by quantum mechanics, i.e. by unitary time evolution operators. The measurement process looks irreversible only because the measurement apparatus is *macroscopic*.

### 1.5.4 The two-dimensional Hilbert space: Qubits and Spins

In many situations only two states of a system are important, for example, the ground and first excited states; a single spin 1/2 possesses only two states. In order to keep the analogy to classical bits as close as possible those systems are most suitable for the discussion of quantum computing.

The Hilbert space of a single spin-1/2 particle is spanned by the states

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\uparrow\rangle = |0\rangle$$

and

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |\downarrow\rangle = |1\rangle.$$

(The identification with $|0\rangle$ and $|1\rangle$ follows the convention of [3].) All operators in this Hilbert space can be combined from the four fundamental operators

$$\mathbf{P}_\uparrow = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |\uparrow\rangle\langle\uparrow|$$

$$\mathbf{P}_\downarrow = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = |\downarrow\rangle\langle\downarrow|$$

$$\mathbf{S}^+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = |\uparrow\rangle\langle\downarrow|$$

$$\mathbf{S^-} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = |\downarrow\rangle\langle\uparrow|.$$

More convenient for the purposes of physics are the following combinations:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{P_\uparrow} + \mathbf{P_\downarrow}$$

$$\mathbf{S_z} = \frac{\mathbf{1}}{\mathbf{2}}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \frac{\mathbf{1}}{\mathbf{2}}(\mathbf{P_\uparrow} - \mathbf{P_\downarrow}) = \frac{\mathbf{1}}{\mathbf{2}}\mathbf{Z}$$

$$\mathbf{S_x} = \frac{\mathbf{1}}{\mathbf{2}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \frac{\mathbf{1}}{\mathbf{2}}(\mathbf{S^+} + \mathbf{S^-}) = \frac{\mathbf{1}}{\mathbf{2}}\mathbf{X}$$

$$\mathbf{S_y} = \frac{\mathbf{1}}{\mathbf{2}}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \frac{\mathbf{i}}{\mathbf{2}}(\mathbf{S^-} - \mathbf{S^+}) = \frac{\mathbf{1}}{\mathbf{2}}\mathbf{Y}$$

$$\mathbf{S_x}^{\mathbf{2}} = \mathbf{S_y}^{\mathbf{2}} = \mathbf{S_z}^{\mathbf{2}} = \frac{\mathbf{1}}{\mathbf{4}}\mathbf{1}.$$

The matrices $\mathbf{S}_\alpha$ $\alpha = x, y, z$ are the spin-matrices of a spin-1/2 particle.

**Quantum gates** – It is evident why $\mathbf{X}$ is also often called the "NOT gate" in the language of quantum computing. Any unitary $2 \times 2$ matrix is a valid quantum gate, for example the $\mathbf{Z}$ gate which generates a $\pi$ relative phase. We will also frequently encounter the Hadamard gate

$$\mathbf{H} \;=\; \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(\mathbf{X} + \mathbf{Z}) \;=\; \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

$\mathbf{H}$ (hopefully not to be confused with the Hamiltonian) is at the same time unitary and Hermitian, implying that $\mathbf{H^2} = \mathbf{1}$. Nevertheless $\mathbf{H}$ is often called the "square root of NOT" gate, because it turns $|0\rangle$ into a state "halfway between" $|0\rangle$ and $|1\rangle$ and similarly for $|1\rangle$. (Exercise: Find the genuine square root of NOT. Hint: Try to write NOT as $\exp i\alpha\mathbf{S_x}$.)

**Spin in a magnetic field** – A spin-1/2 particle (fixed in space) in an external field with components $B_x, B_y, B_z$ has the Hamiltonian

$$\mathbf{H} \;=\; -\vec{\mathbf{B}} \cdot \vec{\mathbf{S}} \;=\; -(\,\mathbf{B_x S_x} + \mathbf{B_y S_y} + \mathbf{B_z S_z}\,)\;,$$

where all $g$ factors etc have been absorbed in the units of $\vec{B}$.

We consider the initial state $|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and determine the time evolution operator $\mathbf{U(t)}$ for a $\vec{B}$ field along one of the coordinate axes $\alpha = x, y, z$.

$$\mathbf{U(t)} = \exp\left(-\frac{\mathbf{iHt}}{\hbar}\right) = \exp\left(\frac{\mathbf{iB_\alpha t}}{\mathbf{2\hbar}}\underbrace{2\mathbf{S}_\alpha}_{\text{square}=\mathbf{1}}\right)$$

$$= \cos\left(\frac{B_\alpha t}{2\hbar}\right)\mathbf{1} + i\sin\left(\frac{B_\alpha t}{2\hbar}\right)2\mathbf{S}_\alpha.$$

For $\alpha = z$ we have

$$\mathbf{U(t)} = \begin{pmatrix} \exp\left(i\frac{B_\alpha t}{2\hbar}\right) & 0 \\ 0 & \exp\left(-i\frac{B_\alpha t}{2\hbar}\right) \end{pmatrix}$$

$$\Rightarrow |\psi(t)\rangle = \exp\left(i\frac{B_\alpha t}{2\hbar}\right)|\psi(0)\rangle$$

which is a stationary state, as expected, because the initial state was an eigenstate of $\mathbf{S_z}$(and thus of $\mathbf{H}$).

The case $\alpha = x$ is different:

$$\mathbf{U(t)} = \begin{pmatrix} \cos\left(\frac{B_\alpha t}{2\hbar}\right) & i\sin\left(\frac{B_\alpha t}{2\hbar}\right) \\ i\sin\left(\frac{B_\alpha t}{2\hbar}\right) & \cos\left(\frac{B_\alpha t}{2\hbar}\right) \end{pmatrix},$$

consequently

$$|\psi(t)\rangle = \begin{pmatrix} \cos\left(\frac{B_\alpha t}{2\hbar}\right) \\ i\sin\left(\frac{B_\alpha t}{2\hbar}\right) \end{pmatrix} = \cos\left(\frac{B_\alpha t}{2\hbar}\right)|\uparrow\rangle + i\sin\left(\frac{B_\alpha t}{2\hbar}\right)|\downarrow\rangle.$$

Runs through a continuum of states periodically: "uniform rotation in Hilbert space" (similar for $\alpha = y$).

**Qubits** – A (pure) *qubit* state is an arbitrary normalized linear combination of $|\uparrow\rangle$ and $|\downarrow\rangle$ which may be parametrized, for example, by two angles:

$$|\theta,\varphi\rangle = \exp\left(-i\frac{\varphi}{2}\right)\cos\frac{\theta}{2}|\uparrow\rangle + \exp\left(i\frac{\varphi}{2}\right)\sin\frac{\theta}{2}|\downarrow\rangle$$

$$(0 \leq \theta \leq \pi; 0 \leq \varphi \leq 2\pi).$$

Thus a qubit is able to store two (bounded) *real* numbers. The question how to read, write, and manipulate this information will keep us busy for the rest of this semester (and longer, maybe).

It is easy to check that the above qubit is an eigenstate of the operator

$$\cos\theta\mathbf{S_z} + \sin\theta\cos\varphi\mathbf{S_x} + \sin\theta\sin\varphi\mathbf{S_y}$$

with eigenvalue $+1/2$. We therefore recognize $(\theta,\varphi)$ the angle of spherical coordinates. Thus, in order to prepare this qubit, one "only" needs to align the spin along the $(\theta,\varphi)$ direction by a sufficiently strong field.

### 1.5.5 Two qubits and the density matrix

"Much that is weird and wonderful about quantum mechanics can be appreciated by considering the properties of the quantum states of two qubits." (John Preskill [8])

**Quantum mechanics and the environment** – In the real world there are no isolated spins 1/2; quantum systems always couple to the "environment" which we often cannot or do not want to take into account in our quantum mechanical considerations. If we want to take the environment nevertheless is same "average" way into account, we have to modify the description of the quantum mechanics of the accessible system. If we consider a quantum system which is in reality only part of a larger system, we will therefore have to abandon some of our dogmas, because

- states are no longer vectors in Hilbert space,
- measurements are no longer orthogonal projections on to the final state
- and time evolution is no longer unitary.

The simplest example of a coupled system is given by one qubit $A$ = "system" (accessible) and another qubit $B$ = "environment" (inaccessible). $\{|\uparrow\rangle_A, |\downarrow\rangle_A\}$ and $\{|\uparrow\rangle_B, |\downarrow\rangle_B\}$ are orthonormal bases for the two subsystems.

**Partial measurement** – A *correlated* or *entangled* state of two qubits:

$$|\psi\rangle \;=\; a\,|\uparrow\rangle_A \otimes |\uparrow\rangle_B \;+\; b\,|\downarrow\rangle_A \otimes |\downarrow\rangle_B.$$

A measurement of the state of qubit $A$ (that is, a projection on to the $A$ basis) yields $|\uparrow\rangle_A \otimes |\uparrow\rangle_B$ with probability $|a|^2$ and $|\downarrow\rangle_A \otimes |\downarrow\rangle_B$ with probability $|b|^2$. In both cases after the measurement on $A$ the state of $B$ is *fixed*.

A measurement of an observable $\mathbf{M}_A$ which acts only on $A$ is given by

$$\mathbf{M}_A \otimes \mathbf{1}_B \;.$$

The expectation value of this observable in the state $|\psi\rangle$ is

$$\langle \mathbf{M}_A\rangle = \langle\psi|\mathbf{M}_A \otimes \mathbf{1}_B|\psi\rangle =$$

$$\Big[a^*\ {}_A\langle\uparrow|\otimes_B\langle\uparrow| + b^*\ {}_A\langle\downarrow|\otimes_B\langle\downarrow|\Big]\,\mathbf{M}_A\otimes\mathbf{1}_B\,\Big[a\,|\uparrow\rangle_A\otimes|\uparrow\rangle_B + b\,|\downarrow\rangle_A\otimes|\downarrow\rangle_B\Big] \;=\; \cdots$$

$\mathbf{1}_B$ does *not* change $|...\rangle_B$ states; ${}_B\langle\uparrow|\downarrow\rangle_B = 0 \Rightarrow$ only two terms survive.

$$\cdots \;=\; |a|^2\ {}_A\langle\uparrow|\mathbf{M}_A|\uparrow\rangle_A \;+\; |b|^2\ {}_A\langle\downarrow|\mathbf{M}_A|\downarrow\rangle_A \;=$$

$$= \mathrm{Tr}\left(|a|^2\,\mathbf{P}_{\uparrow A}\,\mathbf{M}_A + |b|^2\,\mathbf{P}_{\downarrow A}\,\mathbf{M}_A\right) =$$

$$= \mathrm{Tr}\left(\left[|a|^2\,\mathbf{P}_{\uparrow A} + |b|^2\,\mathbf{P}_{\downarrow A}\right]\mathbf{M}_A\right) \;\equiv\; \mathrm{Tr}\left(\rho_A \mathbf{M}_A\right).$$

Here

$$\mathbf{P}_{\uparrow\mathbf{A}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathbf{P}_{\downarrow\mathbf{A}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

are projectors on to the $\uparrow, \downarrow$ subspaces of $A$; Tr denotes the trace (sum of the diagonal elements) in the Hilbert space of $A$, that is,

$$\mathrm{Tr}\mathbf{X} \;=\; {}_A\langle\uparrow|\mathbf{X}|\uparrow\rangle_A + {}_A\langle\downarrow|\mathbf{X}|\downarrow\rangle_A .$$

**Density operator** – The quantity

$$\rho_A \;=\; |a|^2\,\mathbf{P}_{\uparrow A} + |b|^2\,\mathbf{P}_{\downarrow A} = \begin{pmatrix} |a|^2 & 0 \\ 0 & |b|^2 \end{pmatrix}$$

is the *density operator* (density matrix); it is Hermitian, positive and its trace is unity. It is important to note that *every* operator with these properties is a possible density operator, irrespective of its being diagonal or not in the basis which we have chosen accidentally or thoughtfully!

**Pure and mixed states** – If $\rho_{\mathbf{A}}^{\mathbf{2}} = \rho_{\mathbf{A}}$ ( for example if $|a| = 1$ in our example) $\rho_{\mathbf{A}}$ is a projector on a vector in Hilbert space: *pure* state; otherwise: *mixed* state; often called "incoherent superposition" by people who like optics better than quantum mechanics. The above $\rho_{\mathbf{A}}$ is obviously a mixed state.

**Uncorrelated states** – The initial $|\psi\rangle$ above was a vector in the "large" Hilbert space; the two subsystems were correlated (entangled). Let us now consider an *uncorrelated* state:

$$|\Phi\rangle \;=\; \Big(a|\uparrow\rangle_A + b|\downarrow\rangle_A\Big) \otimes \Big(c|\uparrow\rangle_B + d|\downarrow\rangle_B\Big)$$

with $|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1$. For that state we quickly end up with

$$\langle\mathbf{M}_A\rangle \;=\; \langle\Phi|\,\mathbf{M}_A \otimes \mathbf{1}_B\,|\Phi\rangle \;=\; \Big[a^*\;{}_A\langle\uparrow| + b^*\;{}_A\langle\downarrow|\Big]\,\mathbf{M}_A\,\Big[a\,|\uparrow\rangle_A + b\,|\downarrow\rangle_A\Big]\cdot$$

$$\cdot\Big[c^*\;{}_B\langle\uparrow| + d^*\;{}_B\langle\downarrow|\Big]\,\mathbf{1}_B\,\Big[c\,|\uparrow\rangle_B + d\,|\downarrow\rangle_B\Big]\;.$$

The "$B$ part" of course yields unity and we obtain

$$\langle\mathbf{M}_A\rangle \;=\; |a|^2\;{}_A\langle\uparrow|\mathbf{M}_A|\uparrow\rangle_A \;+\; |b|^2\;{}_A\langle\downarrow|\mathbf{M}_A|\downarrow\rangle_A \;+$$

$$+\; a^*b\;{}_A\langle\uparrow|\mathbf{M}_A|\downarrow\rangle_A \;+\; b^*a\;{}_A\langle\downarrow|\mathbf{M}_A|\uparrow\rangle$$

$$=\; \mathrm{Tr}\Big(\mathbf{M}_A\Big[|a|^2\mathbf{P}_{\uparrow A} + |b|^2\mathbf{P}_{\downarrow A} + a^*b|\downarrow\rangle_{AA}\langle\uparrow| + b^*a|\uparrow\rangle_{AA}\langle\downarrow|\Big]\Big) \;=\; \mathrm{Tr}\left(\mathbf{M}_A\rho_A\right)\;.$$

Again $\rho_A$ is Hermitian and of unit trace, but obviously *not* diagonal; in the usual basis it is

$$\rho_{\mathbf{A}} = \begin{pmatrix} |a|^2 & a^*b \\ b^*a & |b|^2 \end{pmatrix}.$$

Nevertheless ${\rho_{\mathbf{A}}}^{\mathbf{2}} = \rho_{\mathbf{A}}$, as we can easily calculate. We conclude

i) The density matrix of $A$ is a pure state if the initial state of the combined system $A + B$ is a product state (that is, uncorrelated, not entangled).

ii) If the state of the combined system $A + B$ is entangled, the summation over all possibilities for the state of $B$ ("partial trace over the Hilbert space of $B$") leads to the loss of the phases of $a$ and $b$ and we end up with a mixed state for $\rho_A$.

**Loss of coherence by time-evolution** – The following picture for the loss of coherence thus arises: in the beginning, system and environment are uncorrelated. The system's density matrix is initially pure. By interaction, system and environment become entangled (we will soon see examples for this) and the system's density matrix becomes mixed.

**Bloch sphere** – The general density matrix of a qubit is:

$$\rho(\vec{P}) \;=\; \frac{1}{2}\left(\mathbf{1} + 2\vec{P}\cdot\vec{\mathbf{S}}\right) \;; \qquad |\vec{P}| \le 1$$

The possible $\vec{P}$ form the so-called *Bloch sphere*; pure states have $|\vec{P}| = 1$.

**Exercise** – Distinguish the pure state

$$|\chi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$$

from the mixed state

$$\rho = \frac{\mathbf{1}}{\mathbf{2}}(\mathbf{P}_\uparrow + \mathbf{P}_\downarrow)$$

by determining the expectation values and variances of the operators $\mathbf{S}_\alpha$. Furthermore, determine the polarization vector $\vec{P}$ in both cases.

**Further concepts** – Further important theoretical concepts which could be discussed at this point are

- the time evolution of the density matrix (generalization from the Schrödinger equation to the Liouville / von Neumann equation)
- more formal definition of entanglement.

The first item is treated in many quantum mechanics texts, whereas the second one is still a topic of research, see [8]. Here we will just discuss the *"no cloning theorem"*, since we wil encouter if ofter in the further discussion.

### 1.5.6 No cloning theorem

A basic difference between classical and quantum information is that while classical information can be copied perfectly, quantum cannot. his follows from the no-cloning theorem of Wootters and Zurek [38]. The statement is the following:

Let $U_{\rm QCM}$ be the linear (unitary) operator representing the action of an alleged *quantum copier machine*:

$$U_{\rm QCM}: \quad |\Psi\rangle_{\rm orig}|\phi_0\rangle \quad \mapsto \quad |\Psi\rangle_{\rm orig}|\Psi\rangle_{\rm copy} \ , \quad \forall|\Psi\rangle \ ,$$

where $|\phi_0\rangle$ is the "blank" state of the copy.

Such a machine cannot exist. This is a remarkably simple application of the linearity of quantum mechanics. For a contradiction, suppose it does exist. Assume for simplicity that the object to copy is just a single qubit, and let $|\Psi\rangle_{\rm orig} = \alpha_0|0\rangle + \alpha_1|1\rangle$. Then, linearity implies

$$U_{\rm QCM}|\Psi\rangle|\phi_0\rangle \ = \ \alpha_0\, U_{\rm QCM}|0\rangle|\phi_0\rangle + \alpha_1\, U_{\rm QCM}|1\rangle|\phi_0\rangle \ = \ \alpha_0|0\rangle|0\rangle + \alpha_1|1\rangle|1\rangle \quad (1)$$

whereas the definition of a quantum copier yields

$$U_{\rm QCM}|\Psi\rangle|\phi_0\rangle \ \equiv \ |\Psi\rangle|\Psi\rangle \ = \ \alpha_0^2|0\rangle|0\rangle + \alpha_0\alpha_1|0\rangle|1\rangle + \alpha_1\alpha_0|1\rangle|0\rangle + \alpha_1^2|1\rangle|1\rangle \quad (2)$$

The results (1), (2) are in general incompatible, what proves the assertion.

# References


[1] Michael Brooks. *Quantum Computing and Communications*. Springer, New York, 1999. 152 pp.

[2] Jozef Gruska. *Quantum computing*. McGraw-Hill, London, 2000. 439 pp.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge Univ. Press, Cambridge, 2001. 676 pp.

[4] Colin P. Williams and Scott H. Clearwater. *Explorations in quantum computing*. Springer, New York, 1998. 307 pp, CD-ROM, DM 98.00.

[5] A. Steane. Quantum computing. *Rep. Prog. Phys.*, 61:117–173, 1998.

[6] Dorit Aharonov. Quantum computation. In Dietrich Stauffer, editor, *Annual Reviews of Computational Physics VI*, pages 259–346. World Scientific, 1999. Preprint quant-ph/9812037.

[7] A. Galindo and M. A. Martin-Delgado. Information and computation: Classical and quantum aspects, 2002. Rev. Mod. Phys., to appear. Preprint quant-ph/0112105.

[8] John Preskill. Quantum computation. http://theory.caltech.edu/ preskill/ph229/, 1997. 413 pp.

[9] Paul Benioff. Quantum mechanical Hamiltonian models of Turing machines. *J. Stat. Phys.*, 29:515, 1982.

[10] Y. Lecerf. Machines de Turing reversibles. Compters Rendus **257**, 1597, 1963.

[11] Richard P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.

[12] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, Piscataway, NJ, 1994. IEEE Press.

[13] Stephan Mertens. Computational complexity for physicists. Lecture given at the DPG school on "Quantum Computing", 2000. Preprint cond-mat/0012185.

[14] Barenco, A., C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter. *"Elementary gates for quantum computation"*, Phys. Rev. A **52**, 3457-3467 (1995).

[15] Barenco, A., D. Deutsch, A. Ekert and R. Jozsa. *"Conditional quantum dynamics and logic gates"*, Phys. Rev. Lett. **74**, 4083-6 (1995).

[16] Alonzo Church. An unsolvable problem of elementary number theory. *Am. J. Math.*, 58:345–363, 1936.

[17] Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc. Ser.*, 42:230, 1936. See also ibidem 43, 544.

[18] Douglas R. Hofstadter. *Gdel, Escher, Bach: An Eternal Golden Braid*. Basic Books, New York, 1979. 777 pp.

[19] Leo Szilard. ber die Entropieverminderung in einem thermodynamischen System bei Eingriffen intelligenter Wesen. *Z. Physik*, 53:840–856, 1929.

[20] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal Res Dev*, 5:183–191, 1961.

[21] Seth Lloyd. Ultimate physical limits to computation. *Nature*, 406:1047–1054, 2000.

[22] N. Margolus and L.B. Levitin. title. In T. Toffoli, M. Biafore, and J. Le?o, editors, *Proceedings of the Fourth Workshop on Physics and Computation PhysComp96 (New England Complex Systems Institute, Boston, MA, 1996)*. North-Holland, 1998. Physica D Vol. 120.

[23] Richard P. Feynman. *Feynman Lectures on Computing*, chapter 6, Quantum Mechanical Computers. Addison-Wesley, 1996. Originally published in Optics News, February 1985, pp. 11-20; see also Found. Phys. **16**, 507-532 (1986).

[24] P. Jordan and E. Wigner. Über das Paulische Äquivalenzverbot. *Z. Physik*, 47:631–651, 1928.

[25] Jian-Wei Pan, Dik Bouwmeester, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. *Nature*, 403:515–519, 2000.

[26] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe. Experimental entanglement of four particles. *Nature*, 404:256–259, 2001.

[27] Rainer Blatt. Push-button entanglement. *Nature*, 404:231–232, 2001.

[28] Brian Julsgaard, Alexander Kozhekin, and Eugene S. Polzik. Experimental long-lived entanglement of two macroscopic objects. *Nature*, 413:400–403, 2001.

[29] J. Ignacio Cirac. Quantum physics: Entangled atomic samples. *Nature*, 413:375–377, 2001.

[30] L. Grover. (title). In *Proc. 28th Annual ACM Symposium on the Theory of Computation*, pages 212–219, New York, 1996. ACM Press.

[31] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, 1997. Preprint quant-ph/9706033.

[32] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing, 1999. Preprint quant-ph/9906054.

[33] D.P. DiVincenzo. The physical implementation of quantum computation. *Fortschr. Phys.*, 48:771–783, 2000. Preprint quant-ph/0002077.

[34] C.E. Hughes and S. Wimperis. Bounds on spin dynamics and the design of multiple-pulse NMR experiments. *J. Chem. Phys.*, 106:2105–2117, 1997.

[35] J. Stoustrup, O. Schedletzky, S.J. Glaser, C. Griesinger, N.C. Nielsen, and O.W. Sorensen. Generalized bound on quantum dynamics: efficiency of unitary transformations between non-hermitian states. *Phys. Rev. Lett.*, 74:2921–2924, 1995.

[36] J. H. Smet, R. A. Deutschmann, F. Ertl, W. Wegscheider, G. Abstreiter, and K. von Klitzing. Gate-voltage control of spin interactions between electrons and nuclei in a semiconductor. *Nature*, 415:281–286, 2002.

[37] J. Kikkawa. Eavesdropping on spin talk. *Nature*, 415:273–274, 2002.

[38] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[39] D. Dieks. Communication by EPR devices. *Phys. Lett. A*, 92:271–271, 1982.

[40] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[41] C.H. Bennettr. Logical reversability of computation. *IBM J. Res. Dev.* **17**, 525-532, 1973.

[42] C.H. Bennett and S.J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992.

[43] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India, December 1984)*, pages 175–179, New York, 1984. IEEE.

[44] H. Zbinden, J.D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittle. Interferometry with Faraday mirrors and quantum cryptography. *Electron. Lett.*, 33:586–588, 1997.

[45] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[46] G.M. Palma, K.-A. Suominen, and A.K. Ekert. Quantum computers and dissipation. *Proc. Roy. Soc. A*, 452:567–584, 1996.

[47] D.A. Lidar, I.L. Chuang, and K.B. Whaley. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.*, 81:2594–2597, 1998.

[48] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, 2000.

[49] L. Viola, E.M. Fortunato, M.A. Pravia, E. Knill, R. Laflamme, and D.G. Cory. Experimental realization of noiseless subsystems for quantum information processing. *Science*, 293:2059–2063, 2001.