ADDITIONS

to

Quantum computing

by Jozef Gruska

March 19, 2003

This is to acknowledge suggestions for additions and corrections in these Additions by Andris Ambainis, Helmut Fink and Chuzo Iwamoto.

Chapter 1 — Fundamentals

page 8, footnote 14, line -2 Add at the end of the sentence "As pointed out by Lloyd (1999), it is not clear at all whether von Neumann made such a statement — one does not find it in his collected works."

page 22, after Definition 1.4.6

Remark Proof that Hilbert spaces l_2 and L_2 are isomorphic played an important role in the development of quantum mechanics. It was used by Schrödinger to show that the first two approaches to quantum theory, see Section 9.1.1, due to Heisenberg and Schrödinger, in terms of sequences and functions, were equivalent.

page 23, add to Remark 1.4.12 There is a simple argument to show that there is no quantum way (evolution) to distinguish two non-orthogonal quantum states $|\phi\rangle$ and $|\psi\rangle$ without changing them (causing a disturbance to them). Indeed, the most general way of doing that would be to compose first the existing quantum system with another one in a predefined ancilla state $|\alpha\rangle$ and then to apply a unitary operator U to both $|\alpha\rangle \otimes |\phi\rangle$ and $|\alpha\rangle \otimes |\psi\rangle$ to produce $|\beta\rangle \otimes |\phi\rangle$ and $|\beta'\rangle \otimes |\psi\rangle$. Since no unitary evolution changes the value of scalar products we have

$$\langle \langle \alpha| \otimes \langle \phi| \,|\, |\alpha\rangle \otimes |\psi\rangle\rangle = \langle \langle \beta| \otimes \langle \phi| \,|\, |\beta'\rangle \otimes |\psi\rangle\rangle$$

and by the properties of the scalar product in a composed Hilbert space, page 28,

$$\langle \alpha|\alpha\rangle\langle \phi|\psi\rangle = \langle \beta|\beta'\rangle\langle \phi|\psi\rangle.$$

Since $\langle \phi|\psi\rangle \neq 0$ we have that $\langle \beta|\beta'\rangle = 1$ and therefore $|\beta\rangle = |\beta'\rangle$.

page 24, before Section 1.4.2 Each finite-dimensional Hilbert space has an orthogonal basis $\{|\psi_i\rangle\}_{i=1}^n$. Any basis $\{|\phi_i\rangle\}_{i=1}^n$ can be transformed into an orthogonal basis. For example, by the following Gram-Schmidt algorithm:

for $i = 1$ **to** n **do**
begin $|x_i\rangle \leftarrow |\phi_i\rangle - \sum_{j=1}^{k-1} \langle\psi_i|\phi_i\rangle|\phi_i\rangle$
$\quad |\psi_i\rangle \leftarrow \frac{|x_i\rangle}{||x_i\rangle|}$
end

Exercise 0.1 *Show correctness of the above algorithm.*

Remark Direct sum $H_1 \oplus H_2$ of two Hilbert spaces H_1 and H_2 can be defined in general as a Hilbert space with the following property: There exist linear injections $T_1 : H_1 \to H_1 \oplus H_2$, $T_2 : H_2 \to H_1 \oplus H_2$, such that if $\phi_1 \in T_1(H_1)$, $\phi_2 \in T_2(H_2)$, then $\langle\phi_1|\phi_2\rangle = 0$ and for every vector $\phi \in H_1 \oplus H_2$ there are unique $\phi_1 \in T_1(H_1)$, $\phi_2 \in T_2(H_2)$ such that $\phi = \phi_1 + \phi_2$.

page 25, before Exercise 1.4.21 **Exercise** A bounded linear operator $T : H \to H$ on a Hilbert space H is called **isometry** if $A^*A = I$. Show that the claim that A is isometry is equivalent to any of the following two conditions.

1. $\langle T\phi|T\psi\rangle = \langle\phi|\psi\rangle$ fpr every $\phi, \psi \in H$.
2. $||T\phi|| = ||\phi||$ for every $\phi \in H$.

page 24, add to line -5 of basic text: $A$is called **positive definite** if $\langle\phi|A|\phi\rangle > 0$ for all $|\phi\rangle \neq 0$. The **kernel** of A is the subspace spanned by its eigenvectors corresponding to the eigenvalue 0. The **support** of A is the subspace orthogonal to its kernel.

page 25, line +15 Replace "**self-adjoint**" by "**self-adjoint (Hermitian)**".

page 25, line +36 Add: "Hermitian operators play important role in quantum mechanics; they represent physical quantities and their eigenvalues represent possible values of these quantities."

page 26, line -21 Replace "POVM)." by "POVM or POM). (They are the most general type of quantum measurement. They are performed first by introducing a new quantum system, called ancilla, then by making unitary operations on the composed system and, finally, by making measurements on the resulting state of the new system. Technical details are discussed later, especially in Section 9.2.8.)"

page 27, after Exercise 1.4.28 Two relations between (sharp) observables are of special importance. The observable represented by Hermitian operators A and B are said to be: (a) **compatible** if $AB-BA=0$ – that is if the corresponding operators commute; (b) mutually transformable if $A=U^*BU$ for a unitary transformation U.

Example Observable corresponding to Pauli matrices σ_x and σ_z are not commutable because $\sigma_x\sigma_z=-\sigma_z\sigma_x$, but they are mutually transformable because $\sigma_z=H\sigma_xH$ for the Hadamard matrix H, see Figure 1.4d.

page 27, before Section 1.4.4

Remark

Slightly differently are sometimes treated measurements with respect to the so-called **filtration operator**

$$|\psi\rangle\langle\psi|,$$

where $|\psi\rangle$ is a pure state.

If such a filtration operator is applied to a state $|\phi\rangle$ the outcome is the state $|\psi\rangle$ with probability

$$|\langle\psi|\phi\rangle|$$

and with probability $1-|\langle|\psi|\phi\rangle|$ the outcome is no quantum state.

For example if photon in the state $\alpha|0\rangle+\beta|1\rangle$ is sent through a horizontal (vertical) filter – corresponding to the state $|0\rangle(|1\rangle)$, see pages 347-348, then the outcome of the measurement is with probability $|\alpha|^2$ ($|\beta|^2$) a photon with horizontal (vertical) polarization and with the remaining probability no photon gets through the polarizer.

page 28, add to line 1 Observe that $A\otimes B=(A\otimes I_m)(I_n\otimes B)$, where I_n (I_m) is the identity matrices of degree n (m).

page 28, before Section 1.4.5

Remark Let us list some additional less common matrix operations one encounters in quantum information processing literature. (a) **dot**

product of matrices A and B, notation $A \cdot B$, equals ABA^*; (b) **direct sum** of matrices of the same degree is the block matrix $\begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & B \end{pmatrix}$.

Exercise. (Gudder 2000) Let H_1 and H_2 be Hilbert spaces. Let H be a Hilbert space such that: (a) There is a bilinear mapping from $H_1 \times H_2$ to H, written as $(\phi_1, \phi_2) \to \phi_1 \otimes \phi_2$; (b) For any bilinear mapping B from $H_1 \times H_2$ to a Hilbert space H' there is a unique linear transformation $T : H_1 \times H_2 \to H'$ such that $T(\phi_1 \otimes \phi_2) = B(\phi_1, \phi_2)$). Show that if on H we define an inner-product by $\langle \phi_1 \otimes \phi_2 | \psi_1 \otimes \psi_2 \rangle = \langle \phi_1, \psi_1 \rangle \langle \phi_2 | \psi_2 \rangle$, then H is isomorphic to $H_1 \otimes H_2$. (This is actually another way how to define tensor product of two Hilbert spaces.)

page 28, line -10 In physics literature the term *mixed state* is often used to mean what is termed *density matrix* in the following and terms *mixture* or *ensemble* are used what is termed **mixed state** in this book. However, terminology is far from being unified.

page 29, after line +3 **Remark** It is often important to realize (and to make use of) the fact that any mixed state of a quantum system can be equivalently described by a pure state of a larger quantum system being a composition of the original system and an auxiliary system.

page 29, add to line -8 Add "**Support** of a density matrix ρ is the subspace generated by eigenvectors of ρ corresponding to non-zero eigenvalues."

page 29, after line -4

Remark To each density matrix ρ there exists a unitary transformation U such that $U^* \rho U$ is a diagonal matrix.

Remark There are several (equivalent) ways how to define functions $f(A)$ on operators (matrices) of a Hilbert space, where $f : \mathbf{C} \leftrightarrow \mathbf{C}$. For example: (1) If A is a linear operator with eigenvalues $\lambda_i, 1 \leq i \leq n$, and corresponding mutually orthogonal eigenvectors $|\lambda_i\rangle$, i.e. $A = \sum_{i=1}^{n} \lambda_i |\lambda_i\rangle\langle\lambda_i|$, then $f(A) = \sum_{i=1}^{n} f(\lambda_i)|\lambda_i\rangle\langle\lambda_i|$; (2) If $f(z) = \sum_{k=1}^{\infty} a_k z^k$, then $f(A) = \sum_{k=1}^{\infty} a_k A^k$.

In addition, if $g : \mathbf{C} \leftrightarrow \mathbf{C}$ is such that $g(z) = \frac{df(z)}{dz}$, then we define $\frac{df(A)}{dA} = g(A)$.

Example If ρ is a matrix, then we define

$$\lg \rho = \frac{1}{\ln 2} \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(\rho - I)^n}{n}.$$

This series converges provided ρ is close to the identity matrix I in the sence that

$$||\rho - I|| < 1$$

what is the case if ρ is a positive definite Hermitian operator of the trace 1.

In the case a density matrix is not positive-definite, only positive semi-definite (and it can have an eigenvalue 0), then $\lg\rho$ does not exist. However, in such a case there is a sequence $\{\rho_i\}_{i=1}^{\infty}$ of positive definite Hermitian operators of trace 1 such that $\rho = \lim_{i\to\infty}\rho_i$ and in such a case also the limit

$$\lim_{i\to\infty}\rho_i \lg \rho_i$$

exists. This means that von Neumann entropy is defined for all density matrices.

page 30, after line +19

Remark The rule to compute ρ_{H_A} given on page 30 of the book is neither very transparent nor easy to use. In the following we try to put more light on that rule and, in addition, following Bouda (2000), an easier to use rule.

Meaning of the tracing out operation. If $dim(H_A) = n$, $dim(H_B) = m$, then ρ is an $nm \times nm$ matrix which can be seen as an $n \times n$ matrix consisting of $m \times m$ blocks ρ_{ij} as follows:

$$\rho = \begin{pmatrix} \rho_{11} & \dots & \rho_{1n} \\ \vdots & \ddots & \\ \rho_{n1} & \dots & \rho_{nn} \end{pmatrix}$$

and in such a case

$$\rho_{H_A} = \begin{pmatrix} Tr(\rho_{11}) & \dots & Tr(\rho_{1n}) \\ \vdots & \ddots & \vdots \\ Tr(\rho_{n1}) & \dots & tr(\rho_{nn}) \end{pmatrix}$$

This can be easily seen from the formula for computing ρ_{H_A} once one realizes that

$$Tr(\rho_{ij}) = \sum_{|\psi\rangle\in\mathcal{B}_{H_B}} \langle\phi,\psi|\rho|\phi',\psi\rangle,$$

where $|\phi\rangle$ and $|\phi'\rangle$ are ith and jth vectors in $\mathcal{B}_{H_A}$.

A simpler rule for tracing out operation: The basic trick is to define, for states $|\psi\rangle_A \in H_A$, $|\psi'\rangle_B \in H_B$ and ${}_B\langle\phi| \in H_B^*$, the mapping, denoted also by ${}_B\langle\phi|$, from $H_A \times H_B$ to H_A, defined by

$${}_B\langle\phi|(|\psi\rangle_A \otimes |\psi'\rangle_B) = |\psi\rangle_{AB}\langle\phi||\psi'\rangle_B = |\psi\rangle_A\langle\phi|\psi'\rangle.$$

Analogically, the mapping $|\phi\rangle_B$ is defined. Using such mappings tracing out can be computed as follows

$$\rho_{H_A} = \sum_{|\phi\rangle\in\mathcal{B}_B} {}_B\langle\phi|\rho|\phi\rangle_B.$$

Remark In principle perhaps the simplest way to introduce tracing out operation is to say that it is a linear operation such that for any bipartite system $A\otimes B$, and any states $|\phi_1\rangle$ and $|\phi_2\rangle$ of A and any states $|\psi_1\rangle$ and $|\psi_2\rangle$ of B

$$Tr_B(|\phi_1\rangle\langle\phi_2| \otimes |\psi_1\rangle\langle\psi_2|) = |\phi_1\rangle\langle\phi_2|\, Tr(|\psi_1\rangle\langle\psi_2|) = |\phi_1\rangle\langle\phi_2|\langle\psi_2|\psi_1\rangle.$$

Examples Let $A\otimes B$ is a bipartite quantum system, $|\phi_i\rangle$ (will be states of A and $|\psi_i\rangle$ be states of B. 1) (a) $Tr_B(|\phi\rangle\otimes|\psi\rangle) = |\phi\rangle\langle\phi|$; (b) $Tr_B(\rho - 1\otimes\rho_2) = \rho_1$; (c) if $\rho = \sum_i \lambda_i\rho_i\otimes\sigma_i$, then $Tr_B\rho = \sum_i\lambda_i\rho_i$; (d) if $|\phi\rangle = \sum_i\sqrt{\lambda_i}|\phi_i\rangle|\psi_i\rangle$, then $Tr(|\phi\rangle) = \sum_i\lambda_i|\phi_i\rangle\langle\phi_i|$. **Remark** There is also a way to show that partial race is really the appropriate way to describe a part of a state of a bipartite system $A\otimes B$. The point is that one can show that partial trace is the only function on density matrices over $A\otimes B$ such that for any observable M on A and any density matrix ρ over $A\otimes B$ it holds

$$Tr(M(f(\rho)) = Tr((M\otimes I_B)\rho).$$

In other words, what is a plausible physical requirement, that measurments of averages are the same whether computed by ρ_A or ρ.

page 30, line -1, page 31, line +3 There are alternative ways to define fidelity. For example $F(\rho_1,\rho_2) = |\langle\phi_1|\phi_2\rangle|$ or $F(\rho_1,\rho_2) = \sqrt{|\langle\phi_1|\phi_2\rangle|}$ and similarly, $F(\phi_1,\rho_2) = |\langle\phi_1|\rho_2|\phi_1\rangle|$ or $F(\phi_1,\rho_2) = \sqrt{|\langle\phi_1|\rho_2|\phi_1\rangle|}$

page 31, before Remark 1.4.37 Why Hilbert space framework for quantum mechanics?

It is currently accepted that Hilbert spaces provide mathematical models for quantum systems and quantum theory.

The question "Why are Hilbert spaces the proper mathematical abstraction for quantum theory?" is often answered in a suggestive manner "Because the quantum world is that way".

However, this is not the only and not even the main answer the science provides. A more refined question "What is it about Hilbert space theory which makes it so well suitable for the representation of the physical world", or "Given the goal to find the mathematical framework to represent quantum world why Hilbert space theory has been chosen?" have been investigated intensively and Hughes (1997) provides a well readible treatment of this problem.

page 31, before Section 1.5 Notation and terminology concerning Hilbert spaces is far from being fixed. For example, instead of the "tensor product" one uses also the term "direct product". Instead of the "inner-product" the term "scalar-product".

Partial trace computation

As already mentioned, the definition of the partial trace operation given on page 30 is not only little transparent, but it is also not easy to use. Fortunately, there is also another simple rule how to compute the partial trace of density matrices (Lomonaco, 2000).

The very basic and useful fact is that for a general form of a density operator ρ over a tensor product $H^{(1)} \otimes H^{(2)}$

$$\rho = \sum_k \alpha_k |\phi_{1,k}\rangle\langle\psi_{2,k}|,$$

where $|\phi_{1,k}\rangle \in H^{(1)}$, $|\psi_{2,k}\rangle \in H^{(2)}$ is that it holds

$$Tr(\rho) = \sum_k \alpha_k \langle\psi_{2,k}|\phi_{1,k}\rangle$$

That is in order to determine trace of ρ the outer product has been replaced by the inner product.

The above method can be generalized for partial trace as follows:

Let

$$H = \bigotimes_{i=1}^{n} H^{(i)}$$

be the tensor product of n Hilbert spaces $H^{(i)}$, $i = 11, 2, \ldots, n\}$.

A general form of a density matrix over H is

$$\rho = \sum_k \alpha_k \bigotimes_{i=1}^{n} |\phi_{k,i}\rangle\langle\psi_{k,i}\rangle,$$

where states $|\phi_{k,i}\rangle$ and $|\psi_{k,i}\rangle, \in H^{(k)}$.

If now $I \subseteq J = \{1, 2, \ldots, n\}$ is a set of indices, then the **partial trace** over I can be computed by

$$Tr(\rho) = \sum_k \alpha_k \left(\prod_{j \in I} \langle\psi_{k,i}|\phi_{k,i}\rangle \right) \bigotimes_{J-I} |\phi_{k,j}\rangle\langle\psi k, j|$$

Example If $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, that is

$$\rho = \frac{1}{2}(|01\rangle\langle 01| - |01\rangle\langle 10| - |10\rangle\langle 01| + \langle 10\rangle\langle 10|)$$

and therefore

$$\rho_2 = \frac{1}{2}(\langle 1|0\rangle|1\rangle\langle 0| - \langle 0|0\rangle|1\rangle\langle 1| - \langle 1|1\rangle|0\rangle\langle 0| + \langle 0|1\rangle|0\rangle\langle 1|)$$

Hence,

$$\rho = -\frac{1}{2}(|1\rangle\langle 1| + |0\rangle\langle 1|) = -\frac{1}{2}I.$$

page 36, end of line +3 (To be more precise, the above phenomenon occurs only in the case the light produced has the wave length sufficiently small with respect to the distance between states. If this is the case, the light reflection causes that electrons obtain a momentum and can change their states and directions. In general, depending on the wave length of the light, the resulting interference picture is more or less disturbed and in the extreme cases either disappears completely or does not change at all. In addition, better we can observe through which hole an electron went less interference we can observe and vice versa.)

page 42, before Section 1.6.2 Of large importance is also the following principle.

Superposition principle. If $|\phi\rangle$ and $|\psi\rangle$ are pure states of a quantum system $\mathcal{S}$ and α, β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$, then the superposition $\alpha|\phi\rangle + \beta|\psi\rangle$ is also a state of $\mathcal{S}$.

For example, Dirac (1947) considered the main difference between the classical mechanics and quantum theory in the role the above superposition principle plays in quantum mechanics. On the other hand, others, for example von Neumann, considered Heisenberg's uncertainty principle, see Section 9.1.2, as the most specific one for quantum mechanics.

page 45, add to Remark 1.6.17 As pointed out by H. Fink "POVM have been used for decades for the description of open quantum systems (Davies 1976). From a fundamental point of view, POVM were established by Ludwig and collaborators in an axiomatic approach grounded on preparation and registration procedures. (Ludwig 1983, 1985) provides a coherent elaboration of this approach. An introduction of the basic notions can also be found in (Kraus 1983). While Ludwig strictly sticks to the view that quantum theory is a genuinely statistical theory yielding probability predictions only, Busch et al. (1997) claim to provide a realistic interpretation for quantum properties of individual systems based on unsharp observables. It remains true, however, that the empirical test of a quantum prediction in principle requires the comparison of relative frequencies of measurement results with the probability predicted. Hence, in general there is no operational justification of properties of individual quantum objects, regardless of whether sharp or unsharp observables are considered."

page 47, after Exercise 1.6.22

Exercice Let $\mathcal{B}$ be an orthonormal basis of a Hilbert space H and $\delta_{\phi,\psi} = 0$ if $\phi \neq \psi$ and 1 if $\phi = \psi$. Show that: (a) A bounded linear operator $U : H \rightarrow H$ is an isometry if and only if $\langle U\phi, U\psi\rangle = \delta_{\phi\psi}$ for all $\phi, \psi \in \mathcal{B}$; (b) A linear operator $U : H \rightarrow H$ is unitary if and only if U is an isometry and $||U^*\phi|| = 1$ for every $\phi \in \mathcal{B}$; (c) if H is finite dimensional, then a linear operator $U : H \rightarrow H$ is unitary if and only if $\langle U\phi|U\psi\rangle = \delta_{\phi\psi}$ if $\phi, \psi \in \mathcal{B}$.

page 49, before Section 1.7

1.6.6 Evolution and measurement of density operators

Schrödinger equation has in terms of density operators the form

$$i\hbar\frac{\partial\rho}{\partial t} = [H,\rho] = H\rho - \rho H.$$

If a unitary transformation U is the solution of the standard Schrödinger equation $i\hbar\frac{U(t)}{\partial t} = HU(t)$, then the evolution of ρ is according to the rule

$$\rho \rightarrow U\rho U^*.$$

If a density operator is measured with respect to an observable A with the spectral form $A = \sum_{i=1}^{k}\lambda_i P_i$, then with probability

$$Pr(\rho P_i)$$

the classical outcome is λ_i and the state ρ collapses into the state

$$\frac{P_i\rho P_i}{Tr(\rho P_i)}.$$

SCHRÖDINGER versus HEISENBERG PICTURE

An understanding of quantum evolution in terms of states and unitary operators, at which a quantum state $|\phi\rangle$ is changed by the rule

$$|\phi\rangle \rightarrow U|\phi\rangle$$

in the case of pure states $|\phi\rangle$ or by the rule

$$\rho \rightarrow U^*\rho U$$

in the case of mixed state ρ, where U is a unitary transformation, is called (at first sight quite puzzling) to be the **Schrödinger picture** because it represents Schrödinger's view of the quantum world.

At Schrödinger picture operators are stationary and states keep changing.

In an equivalent Heisenberg's view of the quantum world, called **Heisenberg picture**, the observables A keep changing under the rule

$$A \rightarrow U^*AU$$

and the (initial) states keep being stationary.

The equation for the change of observables has the form

$$i\hbar\frac{\partial A}{\partial t} = [A, H] = AH - HA.$$

page 52, before Section 1.7.2 A new type of universal reversible logic element, the so called *rotary memory* element, (RM), has been introduced by Morita et al. (1999). It is a 4-input/output reversible element which has two states and it is a kind of switching element that changes the path of an input signal depending on its state. Rotary memory elements and Fredkin gates can simulate each other. The main new features of RM is that when designing circuits with them one does not need synchronization elements for inputs, or a clock, as it is the case with Fredkin gates. Moreover RM is a very useful element when designing reversible two-dimensional cellular automata.

page 54, before Section 1.7.3 A variety of other results concerning simulation of one-tape Turing machines by reversible machines has been obtained by K. Morita and his collaborators. For example, Morita et al (1989) have shown that each one-tape Turing machine can be simulated, with at most quadratic increase of time, by one-tape two-symbol reversible Turing machine. Morita (1996) has also shown that each one-tape Turing machine can be simulated by reversible two-counter machine. Finally, Morita has recently shown, personal information, how to construct any reversible Turing machine as a closed circuit using only a new type of logic element, the so called rotary memory, see page 11, and therefore also out of Fredkin gates.

page 60, after line +7 Remark Observe that if $|\gamma| = 1$, then any two qubits $|\phi\rangle$ and $\gamma|\phi\rangle$ have the same representation on the Riemann sphere and that for any qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, with $|\alpha| = 1$ the qubit $\frac{\bar{\alpha}}{|\alpha|}|\phi\rangle$ can be represented as $\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$.

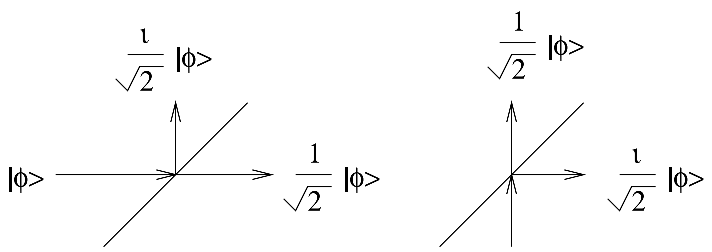
Chapter 2 — Elements

page 61, after Exercise 2.1.5 We show the best way to distinguish two nonorthogonal states $|\phi\rangle$ and $|\psi\rangle$ if the angle β between them is less then $\frac{\pi}{2}$. Let us orient the standard basis $\{|0\rangle, |1\rangle\}$ in such a way that that the angle between $|0\rangle$ and $|\phi\rangle$ is α, the angle between $|\phi\rangle$ and $|\psi\rangle$ is β and the between $|\psi\rangle$ and $|1\rangle$ is again α. In such a case $|\phi\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle$ and $|\psi\rangle = \sin\alpha|0\rangle + \cos\alpha|1\rangle$. If now one of the states $|\phi\rangle$ and $|\psi\rangle$ is measured with respect to the standard basis we get with probability $\cos^2\alpha$ the outcome 0 (1) if the measured state is $|\phi\rangle$ ($|\psi\rangle$).

page 63, after line -1 There are several other general forms of unitary matrices of degree 2. For example: (a) $U = e^{i\alpha}(\cos\phi\mathbf{I} + i\sin\psi(\bar{n}\cdot\bar{\sigma}))$, where $\bar{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ and $\bar{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\phi)$.

page 64, before Example 2.1.18

Remark The beam splitters used in Figure 2.5 is a device that transforms a single photon into a superposition of photons in a way shown in the following figure for the case that the photon enters either the horizontal input port or vertical one.



We say that the photones become an equally weighted superposition of reflected and transmitted photon with the phase shift 90°. The imaginary factor i is due to the relative phase shift that modifies the amplitude by the factor $e^{i\pi/2}$.

page 66, caption of Figure 2.6, add: . Instead of the term "singleton" also the following equivalents are used: "singlet", "singleton state", "singlet state". The remaining Bell states are called *triplets*

page 66, after Exercise 2.1.23

Remark "Magic basis" got it name because of having a variety of "magic" properties. For example:

- The set of states whose density matrices are real when expressed in the magic basis is the same as the set of mixtures of generalized Bell states.
- The set of unitary transformations that are rreal (except, perhaps, for an overall phase factor, when expressed in the magic basis is the

same as the set of transformations that act independently on the two qubits.

page 67, before Exercise 2.1.25 **Remark** The above matrix representation of the XOR operator refers to the standard basis. In different basis XOR has different representations. For example in the Bell basis XOR is represented by the matrix having value $-\frac{1}{2}$ in the main diagonal and $\frac{1}{2}$ in all other entries.

page 67, after Exercise 2.1.25

Exercise Show that XOR matrix is the solution of Schrödinger equation for Hamiltonian

$$H = \frac{\pi\hbar}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

paage 68, add to line +10 (See also reference Milonni and Hardies, 1982.)

page 68, before Exercise 2.1.29

Let us assume that also an ancilla in the state $|a\rangle$ is involved. Let U be an unitary transformation such that for any two unorthogonal states $|\phi\rangle$ and $|\psi\rangle$ it holds $U(|\phi\rangle|0\rangle|a\rangle) = |\phi\rangle|\phi\rangle|a_\phi\rangle$ and $U(|\psi\rangle|0\rangle|a\rangle) = |\psi\rangle|\psi\rangle|a_\psi\rangle$. Then it holds

$$\begin{aligned} \langle\phi|\psi\rangle &= \langle\phi, 0, a|a, 0, \psi\rangle & (1) \\ &= \langle\phi|\psi\rangle^2\langle a_\phi|a_\psi\rangle & (2) \end{aligned}$$

Therefore

$$\langle\phi|\psi\rangle = \frac{1}{\langle a_\phi|a_\psi\rangle}$$

what is impossible because $|\langle\phi|\psi\rangle|$ has to be smaller than 1.

page 72, after Example 2.1.38

Example (Design of symmetric states) In a variety of applications the following symmetric states (see, for example Section 7.3.1), are of importance

$$|s_k\rangle = \frac{1}{\sqrt{\binom{n}{k}}}\sum_{hw(x)=k}|x\rangle,$$

where $0 \leq k \leq n$ and $hw(x)$ is the Hamming weight of string x (number of 1's in x). A simple way to create such states is to use two register, one with n qubits and the second one, for an ancilla, with $\lceil \lg n \rceil$ qubits. By applying first the above Hadamard transformation H_n to the first register, and then the unitary mapping $|x, 0\rangle \to |x, hw(x)\rangle$ to the resulting state we get

$$|0^{(n)}\rangle|0^{\lceil \lg n \rceil)}\rangle \to \sum_{x \in \{0,1\}^n} |x\rangle|0^{(\lceil \lg n \rceil)}\rangle \to \sum_{x \in \{0,1\}^n} |x\rangle|hw(x)\rangle = \sum_{k=0}^{\lceil \lg n \rceil} \sqrt{\frac{\binom{n}{k}}{2^n}} |s_k\rangle|k\rangle$$

and therefore a measurement of the second register results in a $!s_k\rangle$ with probability $\binom{n}{k}/2^n$.

Exercise Show that the symmetric states $|S_k\rangle$ can be obtained in a better way by first applying to each qubit not Hadamard transformation, but the mapping $|0\rangle \to \sqrt{\frac{n-k}{n}}|0\rangle + \sqrt{\frac{k}{n}}|1\rangle$.

A more efficient method to design symmetric states has been developed by Kaye and Mosca (2000).

page 73, before Section 2.2

2.1.5 Bypassing quantum limitations

In a strict sense quantum limitations cannot be bypassed. However, these limitations are often to express extreme situations and ideal solutions. Once the problem is relaxed a bit, in some sense, it is meaningful to consider the task how to solve it in a best way. A variety of fundamental results have been obtained this way.

- **Limitation that an unknown state cannot be (fully) known.** A "relaxed problem" is how well (that is, with best fidelity) one can estimate an unknown quantum state $|\psi\rangle$ if n copies of $|\psi\rangle$ are available. The optimal fidelity $(\frac{n+1}{n+d}$, where d is dimension of the space), with which this can be done universally (i.e. in such a way that the resulting fidelity does not depend on $|\psi\rangle$), was determined by Massar and Popescu (1993) and Derka et al. (1998) have found a POVM to achieve the optimal fidelity.
- **No-cloning limitation.** A "relaxed" problem is to design an appropriate version of m new copies if n copies are available, the so-called $n \to m$ problem. By Werner (1999), the optimal achievable

fidelity is $\frac{m-n+n(m+d)}{m(n+d)}$, if a universal[1] cloning of d-dimensional states is done.

A better cloning performance can be expected if universal cloning of a restricted set of states is considered. For example, Bruß et al. (1999), show the best possible approximation cloning transformation for so-called "equatorial" qubits of the form $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$. (Actually cloning is in this case reduced to phase estimation.) They are called so because in the Bloch sphere they lie in the equator having z-component zero. (Equatorial states are of special interest because in all quantum cryptography experiments so far only such states have been used.) In such a case the achieved upper bound for fidelity is slightly higher, namely $2^{m-n}\frac{\sum_{i=0}^{n-1}\sqrt{\binom{n}{i}\binom{n}{i+1}}}{\sum_{j=0}^{m-1}\sqrt{\binom{n}{j}\binom{m}{j=1}}}$.

page 75, at the end

Remark An interesting and important observation has also been made by Peres (1999): " It is meaningless to assert that two particles are entangled without specifying in which state they are entangled, just as it is meaningless to assert that a quantum system is in a pure state without specifying that state.

If this simple rule is forgotten, or if we attempt to attribute an objective meaning to the quantum state of a single system, curious paradoxes appear: Quantum effects mimic not only instantaneous action-at-a-distance but also influence of future actions on past events, even after these events have been irrevocably recorded."

Remark Nonlocality is often identified with quantum entanglement. On one side, each entangled state violates a Bell type inequality and exhibits a nonlocality. However, a form of "nonlocality without entanglement" was demonstrated by Bennett et al. (1998). They created an orthogonal set of product states of two qutrits (states in H_3) that cannot be reliably distinguished by LQCC. (They have shown that there is a gap between mutual information obtained by any joint measurement on these states and a measurement at which only local operations are performed.)

page 76, add to line +16 Their method is of interest — they started with two pairs of entangled photons and transformed them via a special mea-

[1]Universality here means that quality (fidelity) of cloning does not depend on the state being cloned.

surement into three photons in a GHZ state and a fourth independent "trigger photon".

page 77, add new paragraph after line +19 There is a way to show that no entanglement is needed to implement quantum algorithms. Indeed, a manipulation with an n-qubit register, and therefore with n particles in qubit states, can be replaced by manipulation with one particle that can be in up to 2^n states. However, this is not considered a fully correct way out because it is believed that such a trick then requires some exponential physical resources either for realization of the corrsponding unitary operation, or/and quantum measurements.

On the other side, as shown by Meyer (2000), there is an algorithm to solve Bernstein-Vazirani problem, see page 109, using only one quantum query, even though any classical algorithm requires $\theta(n)$ queries, that employs no entanglement, only quantum superposition. However, it is not clear what kind of conclusions one should derive from this example concerning the power of entanglement. The point is that the number of queries may not be the best measure of (real) quantum complexity.

page 77, add to line -3 Popescu and Rohrlich (1997), as well as Vidal (1998), have shown that the above measure of entanglement of pure states is uniquely specified by certain "natural axioms".

page 77, add to line -1 A pure state of a bipartite system is called maximally entangled if the corresponding mixed states of subsystems are maximally mixed states.

page 78, add to line +19 (The main reason for this definition is that the $\sum_{i=1}^{n} p_i \rho_i \otimes \rho_i'$ is the most general form for a state at which quantum teleportation as discussed in Section 6.4, is not possible. In addition all separable mixed states can be created using LOCC.)

Observe also that the mixed state $\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ is separable inspite of the fact that it is correlated. Indeed, if the state of one particle is $|0\rangle$ so is the state of the other particle — the same for the state $|1\rangle$.

page 78, before Remark 2.2.7 So far there is no general and easy to use method to determine separability of density matrices and the search for such a method is a hot research subject. A simple necessary condition for a density matrix ρ to be separable is the *partial transpose condition* due to Peres (1996a): If a density matrix ρ of a composed (bipartite) quantum system $A \otimes B$ is separable, then its *partial transpose* $\bar{\rho}$ has to have positive eigenvalues. (A partial transpose $\bar{\rho}$ of ρ is obtained from ρ by making a transposition in ρ with respect to only one of the subsystems.) For example, the density matrix ρ for the Bell state Ψ^+ and its transpose $\bar{\rho}$ have the form

$$\rho = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \bar{\rho} = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

and $\bar{\rho}$ has $-\frac{1}{2}$ as one of the eigenvalues. There is a simple way to derive this criterion. Indeed, if a mixed state of a composed quantum system is separable, then it is a mixture of unentangled pure states, each of which is a tensor product of pure states of the subsystems. In such a case if a partial transposition on ρ is made the resulting matrix is again a density matrix and has therefore only positive eigenvalues. However, if ρ is not separable then $\bar{\rho}$ does not have to be a density matrix (and may have negative eigenvalues). Peres' criterion was shown by Horodecki et al. (1998c) to be a necessary and sufficient condition for density matrices of bipartite systems of dimension 2×2 and 2×3.

Several special types of density matrices play important role in investigation of entanglement.

- Werner states. This is a one parameter set of states, see page 334.
- Bell diagonal states. They are states of the form

  $$p_1|\Phi^+\rangle\langle\Phi^-| + p_2|\Phi^-\rangle\langle\Phi^-| + p_3|\Psi^+\rangle\langle\Psi^+| + p_4|\Psi^-\rangle\langle\Psi^-|,$$

  where $\sum_{i=1}^4 p_i = 1$ and all p_i are nonnegative.

page 81, before Section 2.3 Two entertaining puzzles discussed next are to illustrate power of entanglement to assist in creation of a sort of telepathy illusion – a pseudo telepathy. The first one is due to Hardy (1998). The second is actually a modification of the problem dealt with in Section 2.2.3.

Stage telepathy – puzzling behaviour of Alice and Bob

Alice and Bob are on a stage, very far from each other (so far that they cannot communicate), and they are simultaneously, but independently and randomly asked again and again either a "food question" or a "colour question".

- **FOOD question**: What is your favorite meal?
  ANSWER has to be either **carrot** or **peas**.

- **COLOUR question**: What is your favorite colour?
  ANSWER has to be either **green** or **red**.

The audience observes that their answers satisfy the following conditions:

- If both are asked colour-questions then in about 9% of the cases they both answer **green**
- If one of them is asked colour-question and answers **green** and the other is asked food-question then (s)he answers **peas**.
- If both are asked food-questions they never both answer **peas**.

It is not difficult to show that within the classical physics there is no way that Alice and Bob could invent a strategy for their answers before they went to stage in such a way that the above mentioned rules would be fulfilled. However, there is a quantum solution, and actually quite an easy one.

Let $|p\rangle$ and $|c\rangle$ be two arbitrary orthogonal states in H_2 and let

$$|r\rangle = a|p\rangle + b|c\rangle,$$

$$|g\rangle = b|p\rangle - a|c\rangle.$$

Let Alice and Bob at the very beginning, before they went to stage, create a sequence of two particles in the state

$$|\psi\rangle = N(|r\rangle|r\rangle - a^2|p\rangle|p\rangle),$$

where N is a normalization factor, and later each of them takes his/her particle with him/her to the stage.

If any of them is asked the colour-question, then (s)he measures his/her next particle with respect to the $\{|r\rangle, |g\rangle\}$-basis and answers in accordance with the result of measurement.

If any of them is asked the food-question (s)he measures his/her particle with respect to the $\{|p\rangle, |c\rangle\}$-basis and responds in accordance with the result of measurement.

It is a not difficult exercise to show that in this way Alice's and Bob's responses follow the rules described above (9% comes from an optimization in one case).

Guess my number puzzle

A very nice technical result concerning the communication power of entanglement, obtained by van Dam, Høyer and Tapp (1997), was attractively formulated into a puzzle, by Steane and van Dam (2000), as follows.

Alice, Bob and Charles are located in isolated booths and Alice is to guess, each time the moderator distributes secretly among them a number of apples, in total at most 4, potentially dividing some of the apples first into halves and distributing also halves, whether the total number of distributed apples was even or odd. If they guess correctly, they win.

The only communication allowed between the contestants, Alice, Bob and Charles, is that each of Alice's companions is allowed to send one bit to Alice (after seeing the portion of apples he got).

Contestants are allowed, before going to isolated booths, to agree on a strategy and to take with them whatever they want. However, once they are in booths, they are not allowed to communicate in some other way than sending to Alice one bit at each round of the game.

The basic question is whether it is possible that contestants always win? That Alice is always able to determine whether the number of apples distributed is even or odd?

There is no way for Alice, using only classical communications, to guess in more than 75% cases the correct answer. However, there is the following quantum solution.

- Before going to booths contestants create many triplets of particles in the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and each of them takes with him/her one of the particles from each triplets.
- In the case Alice, Bob, and Charles get x_a, x_b or x_c apples, respectively, where $x_a + x_b + x_c$ is an integer smaller than 5, then each of them applies to his/her particle the rotation

$$|0\rangle\langle 0| + e^{ix_i\pi}|1\rangle\langle 1|.$$

The resulting state is either

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \quad \text{if } x_a + x_b + x_c \text{ is even,}$$

or

$$\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), \quad \text{if } x_a + x_b + x_c \text{ is odd.}$$

- In order to enable Alice to determine parity of the number of apples, each of the contestants applies on his/her qubit the Hadamard transformation, getting together either the superposition of the basis states of the even parity

$$\frac{1}{2}(|000\rangle + |110\rangle + |101\rangle + |011\rangle),$$

or a superposition of states of the odd parity

$$\frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle).$$

.

- Each of them then measures his/her qubit in the standard basis and Bob and Charles communicate the outcomes to Alice. They always win.

One can show that in a generalization of the previous game to k contestants $\theta(k \lg k)$ bits are needed to be communicated if only classical communications are used, but if communication enhanced by quantum entanglement is used, only $k-1$ bits are needed to be communicated. This means that at the "entanglement assisted communication" one bit is "doing the work" of $\lg k$ bits. How is this possible?

One has to realize that what is transmitted is not, strictly speaking, an abstract bit, but rather a two-valued classical signal. In other words, a real physical entity is transmitted, and it is because this entity is coupled to the entangled system, at either end of each transmission, that such a gain can be obtained.

page 85, before Example 2.3.12

Exercise (a) Design unitary matrix U that corresponds to the swapping circuit in Figure 2.13b; (b) Design "square root" of the swapping matrix corresponding to the swapping circuit.

page 86, after Figure 2.15 Remark Of course, any permutation can be composed out of transpositions and therefore any permutation of qubits can be done by a circuit without ancilla qubits using technique shown in Figure 2.13b. For a permutation implemented on Figure 2.15 such a technique requires 6 columns of gates and therefore six time units comparing with the four in the circuit in Figure 2.15.

page 85, add to caption of Figure 2.12 Observe that by reversing the order of the left circuit one gets a circuit mapping Bell states into states $\{|ij\rangle \mid i,j \in \{0,1\}\}$ and this way Bell measurementcan be reduced to a bit measurement.

page 90, after Exercise 2.3.29 Observe also the following difference concerning universality of gates in the case of classical and quantum computing. In the classical case we usually say that the state of gates NOT and OR (and AND) form a universal set. However, we actually need also elements that duplicate (copy) outputs and these elements should be seen also as a sort of gates. However, in the quantum case such elements are not possible due to No-cloning theorem.

page 90, before section 2.3.3

Remark Concerning measurements in quantum circuits of large importance is also the so-called **principle of deferred measuremnt** that says that measurements can always be moved from an itermediate stage of a quantum circuit to the end of the ciruit in such a way that if the measurement results are used within the circuit, then the classically controlled operations can be replaced by conditional quantum operations. As a consequence measurements commute with quantum gates when the qubit measured is the control qubit.

page 97, before Definition 2.3.40

Definition If $\mathcal{L}(H_n)$ and $\mathcal{L}(H_m)$ are sets of linear operators on Hilbert spaces H_n and H_m. A map Λ from $\mathcal{L}(H_1)$ to $\mathcal{L}(H_2)$ is called positive, if it maps a positive operator to a positive operator. Λ is called completely positive if for all integers k also the mapping Λ_k from $\mathcal{L}(H_n \otimes H_k)$ to $\mathcal{L}(H_m \otimes H_k)$ defined by $\Lambda_k = \Lambda \otimes I_k$ is positive.

page 98, after line +5

Remark (1) Terminology concerning superoperators is not unique. Another possibility that is used is to call as *superoperators* linear mappings on matrices. *Positive superoperators* are then superoperators that map density matrices to density matrices and *completely positive superoperators (CPSO)* are positive superoperators G such that for any identity mapping I_k also $G \otimes I_k$ is a positive superoperator.

(2) Projection measurement in the standard basis of n qubits is n-qubits superoperator $\mathcal{M}$ such that for each density matrix ρ it holds $\mathcal{M}(\rho)_{ii} = \rho_{ii}$ and $\mathcal{M}(\rho)_{ij} = 0$ if $i \neq j$. Projection measurement in some other basis can be viewed as a projection measurement in the computational basis preceded by a unitary superoperator.

page 99, before Remark 2.3.47 Several additional useful properties of superoperators.

1. If a superoperator G is not constant and $G(\rho)$ is a pure state, then ρ is a pure state.
2. (**Equivalence of reversibility and unitarity**) If G is a superoperator in H_{2^n} and there exists in H_{2^n} a superoperator H such that $H \circ G$ is the identity mapping, then G is a unitary superoperator.

page 99, at the very end

2.3.6 Properties of completely positive maps

The concept of (completely) positive maps plays increasingly important role in the modern quantum information theory. We present here various characterizations and properties of these maps. For proofs see, for example, Donald et al. (2001).

Definition A **quantum operation** is positive map $\Lambda : \mathcal{L}(H_n) \to \mathcal{L}(H_m)$ sssuch that $\mathrm{Tr}(\Lambda(\rho)) \leq 1$ for any density matrix ρ of N_n.

The following four quantum operations are important examples of completely positive maps:

Adding ancilla It is the map $\Lambda_a : \mathcal{L}(H_n) \to \mathcal{L}(H_m \otimes H_k)$, defined $\Lambda_a(\rho) = \rho \otimes \sigma$, where σ is a density matrix on a H_k.

Tracing out operation (It is a mapping $\Lambda_t : \mathcal{L}(H_n \otimes H_k) \to H_n$ defined by $\Lambda_t(\rho) = \mathrm{Tr}_{H_k}(\rho)$.

Unitary transformation $\Lambda_u : \mathcal{L}(H_n) \to \mathcal{L}(H_n)$ defined by $\Lambda(\rho) = U\rho U^*$.

Generalized POVM measurement (Lüders-von Neumann measurement)
$\Lambda_m : \mathcal{L}(H_n) \to \mathcal{L}(H_n)$ defined by a sequence of pairwise orthogoanl projection operators P_i on H_n as follows: $\Lambda_m(\rho) = \sum_{i=1}^{r} P_i \rho P_i^*$.

The following theorem shows importance of the above set of four operations:

Theorem Let Λ be an operation from $\mathcal{L}(H_n)$ to $\mathcal{L}(H_m)$. Then

- If Λ is trace preserving, then Λ is completely positive iff Λ can be composed of the first three from the above set of operations.
- Λ is completely positive iff Λ can be composed from the above four operations.

Of importance is also the following characterization of completely positive maps.

Theorem (Chi-Kraus representation of completely positive maps) Any completely positive map $\Lambda : \mathcal{L}(H_n) \to \mathcal{L}(H_m)$ can be expressed in the form $\Lambda(A) = \sum_{i=1}^{nm} W_i A W_i^*$, for $A \in \mathcal{L}(L_n)$ and $H_i : \mathcal{L}(H_1) \to \mathcal{L}(H_2)$ for all i.

Chapter 3 — Algorithms

page 103, line +24, add (However, the statement that all values of f are computed in one step should be taken cautiously, because, as discussed later, there is in general no good way to get all values of f out of $|\phi\rangle$.)

Remark If we "measure" second register of the state

$$|\phi\rangle = \frac{1}{\sqrt{2^m}} \sum_{i=0}^{2^m-1} |i\rangle |f(i)\rangle$$

with respect to the standard basis $\{|z\rangle \mid z \in \{0,1\}^n\}$, then the state $|\phi\rangle$ collapses into one of the states

$$|\phi_y\rangle = \frac{1}{\sqrt{k}} \sum_{\{x \mid f(x)=y\}} |x\rangle |y\rangle,$$

where

- y is in the range of the values of the function f.

- $k = |\{x \mid f(x) = y\}|$.

The collapse into the state $|\phi_y\rangle$ happens with the probability

$$\frac{k}{2^m}$$

and into the classical world one gets information which of y in the range of f, in the second register, has been (randomly) chosen.

This fact we usually interpret that y is the (classical) result of the measurement of the second register of the state $|\phi\rangle$, with respect to the standard basis.

Remark Observe two paradoxical properties of quantum registers. (1) In general, the number of parameters needed to describe a state of n-qubit registers grows exponentially with n. (2) A quantum computer acting on quantum registers with just hundred of qubits is capable of performing tasks that could never be performed by classical computers.

page 109, add to line +5 (Show that such an algorithm never works with an entangled state if $n \leq 2$ and that for any $n > 2$ there is such a function f that the algorithm works with an entangled state (Collins et al. 1998).)

page 109, before Section 3.1.3 For implementations of algorithms to solve Deutsch-Jozsa problem see Jones and Mosca (1988), Chuang et al. (1998), Linden et al. (quant-ph/980839), Kim et al. (quant-ph/9910015)

page 111, before Section 3.2

Remark Let us sketch a different proof (see, for example, Shor, 2000) that solving Simon's problem on classical computers requires $\Omega(\sqrt{2^n})$ queries of f, in the worst case.

Let f be chosen randomly from all functions with the required property. By making k f-queries one can rule out $\frac{k(k-1)}{2}$ choices for s from the total 2^n possibilities. Hence, in the half of the cases for the choice of f $\theta(\sqrt{2^n})$ f-queries are required.

page 112, after line +4

Example For example, for $k = 8$ clasical FFT transforms a sequence with period r to a sequence with period $8/r$. An illustrative example:

$$\begin{array}{cccccccccccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \rightarrow & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \rightarrow & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \rightarrow & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \rightarrow & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

In addition, FFT transforms offsets in the input sequence into unique phase factors in the output sequence. An illustrative example:

$$\begin{array}{cccccccccccccccccc}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \rightarrow & 1 & 0 & 1 & 01 & 0 & 1 & 0 & \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & \rightarrow & 1 & 0 & -i & 0 & -1 & 0 & i & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \rightarrow & 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & \rightarrow & 1 & 0 & i & 0 & -1 & 0 & -i & 0
\end{array}$$

page 116, before line -6

Example (Generalized Deutsch-Jozsa problem – see Chi et al. (2000)) QFT can be used, for example, to solve also a natural generalization of the Deutsch-Jozsa problem with only one application of a given oracle function. The generalized Deutsch-Jozsa problem is defined as follows.

We say that a function $f : \mathbf{Z}_N \rightarrow \mathbf{Z}_M$ is **evenly distributed** if

$$\{f(x) \,|\, x \in \mathbf{Z}_N\} = \{j\mu + t \,|\, j \in \mathbf{Z}_k, M = \mu k \text{ and } k|N\},$$

and

$$|A_0| = |A_1| = |A_2| = \ldots = |A_{k-1}|,$$

where

$$A_j = \{x \in \mathbf{Z}_N \,|\, f(x) = j\mu + t\} \text{ for } j \in \mathbf{Z}_k.$$

In other words, f is evenly distributed if f has equally distributed k values and is ν-to-one function where $\nu = \frac{N}{k}$.

The **generalized Deutsch-Jozsa problem** is to decide, given a promise that a function f, given as an oracle, is either constant or evenly spaced distributed which of these two properties f has.

We show now how to solve the generalized Deutsch-Jozsa problem with just one applications of f if QFT is used.

For simplicity we assume $N = 2^n, M = 2^m$. Let

$$|\psi\rangle = QFT_{2^m}(|-\chi\rangle) = \frac{1}{2^m}\sum_{z=0}^{2^n-1} e^{-2\pi i\chi z/2^m}|z\rangle$$

for a $\chi \in \mathbf{Z}_{2^m}$.

In the following algorithm to the initial state

$$|0^{(n)}\rangle \otimes |\psi\rangle$$

at first the transformation $H_n \otimes I$ is applied, then the transformation U_f, transformations $z + f(x) \to z' \to z$, and, finally, again the trasformation $H_n \otimes I$. This way we get

$$\begin{aligned}
|0^{(n)}\rangle \otimes |\psi\rangle &\rightarrow \frac{1}{2^n}\sum_{x=0}^{2^n-1} |x\rangle \otimes |\psi\rangle && (3)\\
&\rightarrow \frac{1}{\sqrt{2^n 2^m}}\sum_{x=0}^{2^n-1}\sum_{z=0}^{2^m-1} e^{-2\pi i\chi z/2^m}|x\rangle|z+f(x)\rangle && (4)\\
&= \frac{1}{\sqrt{2^n 2^m}}\sum_{x=0}^{2^n-1}\sum_{z=0}^{2^m-1} e^{-2\pi i\chi (z-f(x))/2^m}|x\rangle|z\rangle && (5)\\
&= \frac{1}{2^n}\sum_{x=0}^{2^n-1} e^{2\pi i\chi f(x)/2^m}|x\rangle \otimes |\psi\rangle && (6)\\
&\rightarrow \sum_{y=0}^{2^n-1}\left(\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{x\cdot y}e^{2\pi i\chi f(x)/2^m}\right)|y\rangle|\psi\rangle && (7)
\end{aligned}$$

Let us now denote the inner summation in the last expression as

$$S_y = \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{x\cdot y}e^{2\pi i\chi f(x)/2^m},$$

Now it is easy to show that

- If f is constant then $S_y = 0$ if and only if $y \neq 0$.
- If f is evenly distributed, then $S_0 = 0$.

Hence, when f is constant the final state of the first register is $|0^{(n)}\rangle$, whereas when f is evenly distributed the state is orthogonal to $|0^{(n)}\rangle$. By one measurement of the first register we can therefore determine whether f is constant or evenly distributed.

Exercice (a) Show how to solve the Deutsch-Jozsa problem using an ancilla with an arbitrary qubit state $a|0\rangle + b|1\rangle$ and using the unitary operator U_f; (b) Show, using the experiences obtained with the solution of the exercises (a), that one can solve generalized Deutsch-Jozsa problem without using QFT by using bitwise operations between vectors in $\mathbf{Z}_2^m$ instead of $\mathbf{Z}_{2^m}$.

page 119, after line +2 Approximate QFT can be implemented, for example, by a circuit obtained from that in Figure 3.3 by deleting gates with very (exponentially) small amplitudes. The existence of such gates, that can hardly be seen as being realisable with arbitrary precision has been anyway an objection to feasibility of that circuit. Fortunately, even with approximate QFT one can have polynomial time quantum factorization.

page 122, after line +8

Remark Let us now sketch Shor's algorithm to compute the period of a function $f(x) = a^x \bmod n$ for the general case (see Shor (1997), Lomonaco (2000a)).

QFT_q is applied to the first register of the state $\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle|f(x)\rangle$ and afterward the measurement is performed on the first register to provide an $y_0 \in \{0,\ldots,q-1\}$.

To get the period r the following algorithm is realized where $\xi = \frac{y_0}{q}$, $a_0 = \lfloor \xi \rfloor$, $\xi_0 = \xi - a_0$, $p_0, q_0 = 1$, $p_1 = a_1 a_0 + 1, q_1 = a_1$

for $j = 1$ **until** $\xi_j = 0$ **do**

- compute p_j and q_j using the recursion (for the case $\xi_j \neq 0$);

$$a_j = \left\lfloor \frac{1}{\xi_{j-1}} \right\rfloor, \xi_j = \frac{1}{\xi_{j-1}} - a_j,$$

$$p_j = a_j p_{j-1} + p_{j-2}, \qquad q_j = a_j q_{j-1} + q_{j-2}$$

- Test whether $q_j = r$ by computing $m^{q_j} = \prod_i (m^{2^i})^{q_{j,i}} \bmod n$, where $q_j = \sum_i q_{j,i} 2^i$ is the binary expansion of q_n.
  If $a^{q_j} = 1 \bmod n$, then exit with $r = q_j$; if not continue the loop.

The non-easy task is to show (see for example Lomonaco (2000)) that the above algorithm provides the period r with sufficient probability ($> \frac{0.232}{\lg\lg n}(1-\frac{1}{n})^2$).

page 125, after line +15

Remark The above result has been generalized by Boneh and Lipton (1995). They have shown, generalizing Shor's method, that discrete logarithm over any group for which group operations can be computed effectively (including Galois fields and elliptic curves) is computable in quantum polynomial time. Their results imply that any cryptosystem based on what they refer to as a "hidden linear form" can be broken in quantum polynomial time. In particular, this implies that also currently so popular elliptic curve (discrete logarithm) cryptosystems would be breakable with powerful quantum computers.

Open problem It is an important open problem to find out whether there are fast quantum algorithms to break the following cryptosystems: (a) Ajtai-Dwork cryptosystem (which requires to find short vectors in certain types of lattices); (b) cryptosystems based on classical linear error-correcting codes.

page 128, at the end Example For $n = 4$ Grover's algorithm needs only one step. Indeed, in this case the initial distribution of amplitudes is $(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ and after one step inversion about the average operator makes out of that the distribution with one amplitude equal 1 and all other equal 0.

page 134, before Remark 3.3.10

Generalized Grover algorithm

Biham et al. (2000) analyzed time-evolution of amplitudes, optimal number of iterations, and the probability of finding a (marked) state x such that $f(x) = 1$, for so far the most general version of Grover algorithm.

They consider an arbitrary initial state

$$|\psi_0\rangle = \sum_{x\in X_1} k_x|x\rangle + \sum_{x\in X_0} l_x|x\rangle.$$

In addition, instead, of the initial rotation $V_f = I_f^\pi = \sum_x e^{i\pi f(x)}|x\rangle\langle x|$ of marked states (x such that $f(x) = 1$) a rotation by an arbitrary phase γ

is considered

$$I_f^\gamma = \sum_x e^{i\gamma f(x)}|x\rangle\langle x|.$$

Moreover, in the rotation by the inversion $G = -H_n I_0^\pi H_n$, the Hadamard transformation H_n is replaced by an arbitrary unitary matrix U and, in addition, the rotation I_0^π, is replaced by the rotation of a fixed basis state $|s\rangle$ by an arbitrary angle β. G has now the form

$$G = -UI_s^\beta U^*,$$

where

$$I_s^\beta = I - (1-e^{i\beta})|s\rangle\langle s|$$

and therefore

$$G = (1-e^{i\beta})|\theta\rangle\langle\theta|,$$

where $|\theta\rangle = U|s\rangle$ and the Grover's iterate has therefore the form GI_f^γ.

The time evolution of amplitudes after k applications of generalized Grover iterate is expressed using the first order linear difference equations that can be solved exactly. The solution also provides the number of iterations t needed to have the highest probability p of finding a marked state. Both t and p are shown to depend on the averages and variances of the initial amplitude distributions in $|\psi_0\rangle$, but not on higher moments.

page 134, before Section 3.3.4

Exercise Create all vectors and matrices as well compute resulting probabilities for the case Grover's search is used for: (a) $2^n = 8$ and $x_0 = 5$; (b) $2^n = 16$ and there are two solutions $x_0 = 5$ and $x_0 = 13$; (c) $2^n = 32$ and $x_0 = 13$.

Chapter 4 — Automata

page 155 A nice example of a simple 1QFA, with $n+2$ states, recognizing the language $L_n = \{w \mid w \in \{0,1\}^*, n \text{ divides } |w|_0, n \text{ divides } |w|_1\}$, for which each DFA has at least n^2 states, with a nontrivial proof of the acceptance of L_n, is due to Kikusts (1998).

page 156, before Section 4.1.3 Ambainis et al. (2000) developed a series of sufficient conditions (or necessary and sufficient conditions) for (certain) regular languages not to be acceptable by 1QFA (with probability greater than $\frac{1}{2}$). These conditions generalized ones developed by Ambainis and Freivalds (1998) and Brodsky and Pippenger (1999). All these conditions are related to the existence of certain *forbidden constructions* in the minimal DFA accepting a given regular language. These conditions are depicted in Figure 1 where q's denote states and symbols $r, s, t, u, v, w, x, y, z$ denote words over the input alphabet Σ. Moreover q_a, q'_a (q_r, q'_r) represents accepting (rejecting) states. It holds.

Theorem (1) Let L be a regular language and $\mathcal{A}$ its minimal DFA. If $\mathcal{A}$ contains one of the forbidden constructions F1, F2 and F4, then L is not recognized by a 1QFA.

(2) Let L be a regular language and $\mathcal{A}$ its minimal DFA. If $\mathcal{A}$ does not contain the forbidden construction F3, then L is recognizable by a 1QFA if and only if $\mathcal{A}$ does not contain the forbidden constructions F1 and F2.

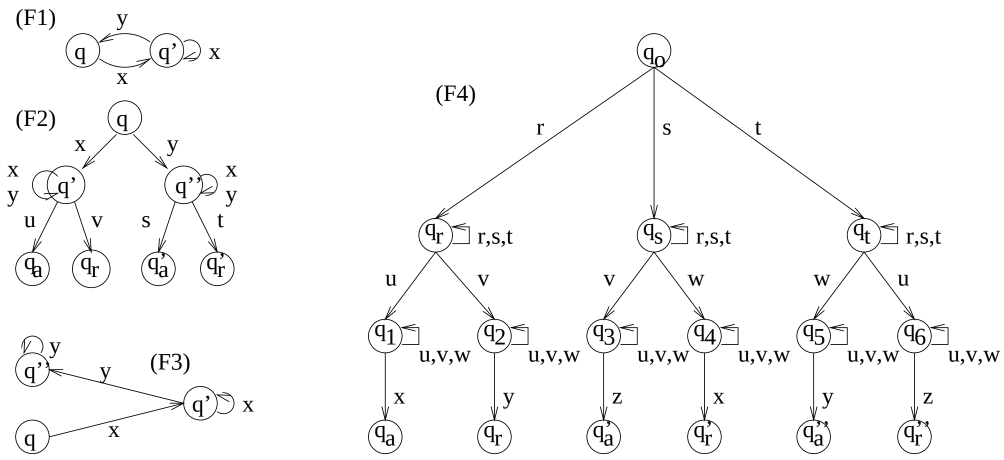


Figure 1: Forbidden constructions

Forbidden constructions F2 and F4 consists of several parts corresponding to different prefixes. Each part corresponds to a language recognizable by a 1QFA, but it is not possible to recognize by 1QFA (without violating unitarity) the union of these languages.

The key role in the proofs plays the following lemma (Ambainis and Freivalds (1998)) and its generalization.

Lemma If $x \in \Sigma^*$, then there are subspaces E_1 and E_2 of E_n such that $E_n = E_1 \oplus E_2$ and

1. If $|\psi\rangle \in E_1$, then $V'_x(\psi) \in E_1$ and $||V'_x(\phi)|| = ||\psi||$,
2. If $|\psi\rangle \in E_2$, then $||V'_{x^k}(\psi)|| \to 0$ when $k \to \infty$.

(This condition actually can be seen as a quantm counterpart of the classification of states of Markov chains (into ergodic sets, that are never left and into transient sets that are left with probability arbitrarily closed to one after sufficient number of steps).

Ambainis et al. (2000) described also a general *forbidden construction*

page 160, line -5 Add: "Morita (1990) has shown a simple way how to construct a 1RFA out of Fredkin gates in such a way that resulting circuit is "garbage-less"."

page 168, before Section 4.2

Remark A natural quantum generalization of the concept of multitape finite automata, with one head on each tape moving in the left-to-right direction, has been introduced by Ambainis et al. (1999a). Such quantum automata recognize relations of words of the same length. The most remarkable and non-easy result is that this model is provably stronger than its classical probabilistic version.

page 173, Exercise 4.2.11 Add "Actually a better bound 2ε can be shown."

page 183, before Exercise 4.3.4

Remark In addition, Morita and Hararo (1989) have shown computational universality of one-dimensional cellular automata. Moreover, Morita and Ueno (1992) have shown that there is universal two-dimensional 16-state reversible cellular automaton. An interesting problem is to construct a self-reproducible, universal and reversible cellular automaton. This problem is discussed in Morita (1998) and by Morita and Imai (1996).

Chapter 5 — Complexity

page 204, after line -15

Remark Robustness of complexity classes is in the case of quantum computing a more tricky issue as in the case of classical computing. This is due to several reasons. One of them is that at some suggested quantum computer architectures there are additional restriction than those in models considered in this book. In some cases this is not a problem. For example, it is required that a gate is applied only to neighbouring qubits. However, this does not change such classes as **P** or **BQP**, because, as shown, in Figure 2.13b, a transposition of two qubits can be done using only 3 gates.

On the other hand, it is not yet fully clear that if a unitary transformation is physically realisable that it cannot be used to accept languages not in **BQP**.

page 205, line +11 Last claim is not true, as pointed out by Mehdi Mhalla, Since both classes are between **P** and **PSPACE** inequality of these two classes would imply that **P** $\neq$ **PSPACE**. The error is due to the fact that what is countable in one case and uncountable in the other case is not the language being recognized, but the subclass of **BPQ**-'s Turing machines using only rational amplitudes. However, this does not mean that there is no other contable family of Turing machines that ecognize the class.)

page 205, footnote 6, line +3 For Kitaev's approach see Kitaev et al. (1999).

page 211, after line +11 Several lower bound techniques have been developed for C_b complexity, see Gruska (1997). One of them is the so-called **matrix rank method** due to Mehlhorn and Schmidt (1982).

Given a function $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$, let M_f be a matrix of degree 2^n such that $M_f(i,j) = f(i,j)$.

Theorem (Mehlhorn, Schmidt (1982)) For any function f $C_b(f) \geq \lg(Rank(M_f))$. It is not known how good this bound is. The so-called *LOG-Rank Conjecture* states that $C_b(f) = \mathcal{O}(poly(\lg(Rank(M_f))))$ for any f. A stronger conjecture even assumes that $C_b(f) \leq \lg^2(Rank(M_f))$. For an example of a function f such that $C_b(f) \geq \lg^{1.6}(Rank(M_f))$ see Nisan and Widgerson (1995).

page 213, at the end The disjointness problem discussed above is usually called DISJ_k function computation task and popularly interpreted as the appointment scheduling problem. Alice and Bob wants to find out, using their apointment books, when they have a free day so they can meet.

The method introduced by Ambainis at al. (1998) and discussed briefly above has turned out to be of a broader interest and importance for communication complexity in general and let us therefore discuss it in more details (see also Ta-Shma (1999)).

Definition A quantum communication protocol samples a quantum state (superposition) $|\psi\rangle = \sum_{x\in X}\sum_{y\in Y}\alpha(x,y)|x,y\rangle$, where $X =$

$\{0,1\}^n = Y$, to within ε error if starting with no inputs to Alice and Bob, it ends with both players having created a state $|\phi\rangle$ such that $\langle\phi|\psi\rangle \leq \varepsilon$ and $|\phi\rangle_{\text{Alice}}$ ($|\phi\rangle_{\text{Bob}}$) has support in X (Y). The number of communication qubits needed by the optimal algorithm is denoted $\bar{QC}_\varepsilon(\psi)$. In case $|\psi\rangle = \sum_{x\in X}\sum_{y\in Y}\frac{(-1)^{f(x,y)}}{4^n}|x,y\rangle$, then we use notation $\bar{QC}_\varepsilon(f)$.

The above concepts are of importance for several reasons:

(1) $\frac{1}{2}\bar{QC}_\varepsilon(f)$ provides a lower bound for randomized complexity (to within error ε for f.

(2) $\bar{QC}_\varepsilon(f)$ can be well characterized as follows. Let N_ψ be $2^n \times 2^n$ matrix such that $N_\psi(x,y) = \alpha(x,y)$ and let $M_\psi = N_\psi^* N_\psi$. All eigenvalues of N_ψ are nonnegative and let λ_i denotes the i-th largest of them. Let K_ε be the smallest integer such that $\sum_{i=1}^{K_\varepsilon}\lambda_i.1-\varepsilon$. It holds

Theorem For any state $|\psi\rangle$ and any $0 \leq \varepsilon \leq \frac{1}{2}$,

$$\lceil \lg K_{2\varepsilon}\rceil \leq \bar{QC}_\varepsilon(\psi) \leq \lceil \lg K_\varepsilon \rceil.$$

(3) In the case $\varepsilon = 0$ the following holds

$$\bar{QC}_0(f) = \theta(\lg(Rank(M_f)))$$

and we have a characterization of $\lg(Rank(M_f))$ in terms of communication complexity.

Chapter 6 — Cryptography

page 223, after line +18

3. **Collective attacks.** Their power is between that of individual (intercept-resent) attacks and coherent attacks. Eve brings each transmitted particle into an interaction within an auxiliary system and, at the end, after listening to all public discussions, she measures all auxiliary systems together.

Eavesdropper's attacks discussed above are inherently quantum, For a practical quantum cryptography several other types of attacks have been identified.

Trojan horse attack. This refers to the possibility that an entanglement with environment can "open the door" and let a "Trojan horse to get in to gather information about quantum communications in the protocol".

Beam splitter attacks. (Bennett et al., 1992), This attack and the next one refer to the fact that it seems to be beyond current technology to produce perfect single photon pulses. In the beam splitter attack some multi-photon signals are split. This allows to get some information about the key.

Photon number splitting attacks. (Lütkenhaus, personal information) An eavesdropper tests whether there are more photons in a pulse and if this is the case then, using a beam-splitter, gets always one of them. Under some situations this can be utilise to get full information about the polarization of transmitted photons and consequently about the key.

page 228, at the end In spite of the fact that the discovery of B92 protocol has been an important conceptual simplification and clarification of the limits of QKG, and several experimental QKG ssystems were based on the B92 protocol, it has turned out that that B92 protocol is not a good practical solution. The reason being (Gisin et al. (2001)) that although two non-orthogonal states can't be distinguished unambiguously without disturbation, they can be distinguished unambiguously at the cost of some loses (Ivanovic (1987), Peres (1988)), what has eeven been demonstrated experimentally (Huttner et al. (1996), Clarke et al. (2000)).

page 235, at the end Mayers and Yao's proof is a good opportunity to demonstrate difference between purely theoretical and pragmatical approach to security proofs for cryptographic protocols. From purely theoretical point their proof is fine. From a pragmatical point of view, as pointed out by Bennett and Shor (1998), one would need also a method to determine the safe rate of the key generation depending on the noise levels observed by the key generation parties.

page 247, line -9 Yao (1995) was first to claim that assuming unconditionally secure quantum bit commitment one can design an unconditionally secure quantum oblivious transfer protocol.

page 254, before the end of Section 6.4.1 It is easy to see that at the quantum teleportation Bob cannot learn more about the state of his particle after Alice's measurement step (but before she sends two classical bits), than before her measurement step. Indeed, in both cases the density matrix corresponding to the state of his particle is the same — $\frac{1}{2}I$. In the first case it is an equiprobable mixture of the states $|0\rangle$ and $|1\rangle$

and in the second case an equally probable mixture of four states, from (6.5), page, 253, that are variations of the original state $\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)$.

page 256, before Section 6.4.3

Remark The following facts concerning quantum teleportation are worth to observe: (a) There is no need to know the state in order to be able to teleport it; (b) All quantum operations performed during teleportation are local; (c) All operations performed during teleportation are independent of the state being teleported; (d) Quantum teleportation can be seen as "real teleportation" at which an object is at first dematerialized, then transfered and finally reassembled, at a different place — Bob 's particle at the end of the teleportation is undistinguishable from Alice's particle at the beginning of teleportation; (e) In spite of the fact that maximally entangled state that Alice and Bob share is publicaly known, teleportation represents an absolutely secure way of transferring quantum information at which no eavesdropping is possible — because no particle is transfered; (f) Since quantum particles are indistinguishable anyway, quantum teleportation can be seen as real teleporation.

page 258, after line -6 Add "3. Observe that the particle Alice sends to Bob is in the totally mixed state $\frac{1}{2}I$ and therefore a potential eavesdropper cannot learn anything about bits being transmitted this way."

page 258, at the end

Remark Quantum teleportation can be also seen as providing a fully quantum version of the calssical one-time pad cryptosystem with perfect secrecy. Indeed, provided Alice and Bob share n Bell states than any quantum message encoded using n qubits can be transmitted, using teleportation protocol n-times, in an absolutely secure way. Quantum teleportation can tehrefore be seen an ultimate form of quantum cryptography at which one even does not need to know where the receiver is located.

Chapter 7 — Processors

page 270, before Section 7.3.2

Remark The subspace of symmetric states of H_{2^n} has dimension $n + 1$ and its important basis consists of the states

$$|s_k\rangle = \frac{1}{\sqrt{\binom{n}{k}}} \sum_{hw(x)=k} |x\rangle$$

that is an equally weighted superposition of the standard basis states x having Hamming weight hw(k), for $0 \leq k \leq n$.

An efficient method to design the above symmetric states $|s_k\rangle$ is due to Kaye and Mosca (2000). These symmetric states are of importance in a variety of applications.

page 272, at the bottom If a codeword $u \in \Sigma_2^n$ is sent through a noisy channel $\mathcal{N}$ and it is changed by the channel to v, then $e = v - u$ is called error (error word).

A binary code C is said to correct a set $\mathcal{E}$ of errors if for any two distinct $e_i, e_j \in \mathcal{E}$

$$u + e_i \neq v + e_j, \text{ if } u, v \in C, u \neq v.$$

Example. The code $C = \{00, 01\}$ corrects errors from the set $\{00, 11\}$ and the code $C = \{000, 111\}$ corrects set of errors $\{000, 001, 010, 100\}$.

A code C is said to correct up to t (bit) errors if it can correct the set of errors from the set $\{w \mid hw(t) \leq t\}$.

page 272, line -3 Replace "**code**" by "**(block) code**[2]

page 274, line -16 Add "A code C is **weakly self-dual** if $C \subseteq C^{\perp}$.

page 274, after exercise 7.4.13 Of the key importance for the design of quantum error-correcting codes out of the classical codes is the following lemma (MacWilliams and Sloane, 1977).

Lemma If C is a binary linear $[n, k]$-code and $f : \{0,1\}^n \rightarrow \mathbf{R}$ is any mapping, then

$$\sum_{u \in C^{\perp}} f(u) = \frac{1}{|2^n|} \sum_{u \in C} \bar{f}(u),$$

where $\bar{f}(u) = \sum_{v \in \{0,1\}^n} (-1)^{u \cdot v} f(v)$ is the so-called Hadamard transform of f.

The proof of lemma is quite straightforward; one has only to use the fact that if $v \in C^{\perp}$, then $u \cdot v = 0$ exactly for half of $u \in \{0,1\}^n$.

[2]The adjective "block" refers to the fact that a block (a finite sequence) of symbols (messages) form a codeword. This adjective is often ommited. The adjective "code" is also used to distinguish this type of codes from other codes, practically very powerful, for example concatenated codes and tree codes, not considered here, that encode symbols of a message "continuously" without breaking them into blocks.

In addition, if f_C is the characteristic function of a $[n,k]$-code C,then

$$f_{C^\perp}(u) = \frac{1}{2^k} \sum_{v\in\{0,1\}^n} f_C(v)$$

and therefore $\bar{f}_C = 2^k f_{c^\perp}$.

page 277, after Theorem 7.4.8

Exercise Show the following properties of cyclic codes: (a) Dual of a cyclic code is also a cyclic code.

page 278, after line +8 Of importance are also the following **dual code theorems**.

$$H\sum_{u\in C}|u\rangle = \sum_{v\in C^\perp}|v\rangle$$

and for $w \notin C^\perp$

$$H\sum_{v\in C^\perp}|u+w\rangle = \sum_{v\in C}(-1)^{w\cdot v}|v\rangle.$$

page 278, before Section 7.4.2 For $[n,k,t]$-linear binary codes Hamming bound becomes

$$k \leq n - \lg(\sum_{i=0}^{t}\binom{n}{i})$$

what implies that

$$\frac{k}{n} \leq (1-H(\frac{t}{n}))(1-\varepsilon),$$

where $\varepsilon \to 0$ if $n \to \infty$ and H is entropy function (page 317).

The above bound shows to which degree an error correcting code can achieve high $\frac{k}{n}$ rate.

The problem how good can a linear code be is not yet fully solved. Of importance is **Gilbert-Varshamov bound** that a linear $[n,k,t]$ code exists if

$$2^k\sum_{i=0}^{t-2}\binom{n-1}{i} < 2^n,$$

what implies

$$(1-H(\frac{2t}{n}))(1-\varepsilon) \leq \frac{k}{n},$$

where $\varepsilon \to 0$ if $n \to \infty$.

page 282, line -4 Such codes are more easy to deal with and most of the codes developed so far are non-degenerate.

page 283, after Exercise 7.4.34

Remark The basic general principles of quantum error correction presented above have been formulated on a general level, without any reference to qubits. Error correction can indeed be considered also in terms of other primitives as qubits. However, for several reasons, for example in order to be able to make use of classical error correcting techniques, error-correction in terms of qubits is of special interest and importance.

page 286, after Exercise 7.4.37 In addition to quantum error correction of importance is also **error prevention**. An error correction procedure can be used for error protection if it is applied very often. Sometimes an error correction procedure can be simplified if used only for error prevention. For example, by omitting the correction step, Vaidman et al. (1996) have shown that in order to be useful for error prevention Shor's 9 qubit error correction code can be simplified to use only a 4 qubit-code.

page 294, after line +13 Generators for Steane's code can be easily derived from the parity check matrix for $\mathrm{Ham}(3,2)$ code. They actually corresponde to the row of that matrix with 1's replace alway either with X's or with Z's. Indeed, the codewords for which operators M_4 to M_6 have eigenvalue 1 are those that satisfy parity checks. Operators M_1 to M_3 are derived similarly once one realizes that dual error code in which sign errors are corrected is a subset of the Hamming code and therefore the same parity checks apply.

page 294, after line -5 If a stabilizer over n qubits has k generators then the code encodes $n-k$ qubits. This follows from the fact that each generator has equal number of eigenvactors with eigenvalue $+1$ and -1, so that specifying its eigenvalue reduces the dimension of the space by half. Therefore the code space has dimension 2^{n-k} - therefore it encodes $n-k$ qubits.

The following general results holds:

Theorem Let $\mathcal{S}$ be an Abelian subgroup of $\mathcal{G}_n$ of an order 2^k and let $-1 \notin \mathcal{L}$. Let d be the minimum weight of operators in $\mathcal{C}(\mathcal{S}) - \mathcal{S}$. Then the stabilizer code generated by $\mathcal{S}$ is an $[[n, n-k, d]]$-code.

page 297, add to line -1 Another way to see backward propagation of errors with XOR gate is to realize how XOR operates on dual basis:

$\text{XOR}(|i'\rangle, |j'\rangle) = (|(i \oplus j)'\rangle, |j'\rangle)$.

page 299, after line +11 The key point now is that if $|\psi\rangle = \sum_{i\in\{0,1\}^4} \alpha_i|i\rangle$, and

$$XoR = XOR_{1,5} \otimes XOR_{2,6} \otimes XOR_{3,7} \otimes XOR_{4,8}$$

then

$$|\theta\rangle = XoR|\psi\rangle|\phi_0\rangle = |\psi_0\rangle|\phi_0\rangle + |\psi_1\rangle|\phi_1\rangle,$$

where

$$|\psi_0\rangle = \sum_{i\in\{0,1\}^4} (1 - parity(i))\alpha_i|i\rangle \quad |\psi_1\rangle = \sum_{i\in\{0,1\}^4} (parity(i))\alpha_i|i\rangle$$

If therefore $|\psi\rangle = |\psi_0\rangle$ or $|\psi\rangle = |\psi_1\rangle$, then the state $|\theta\rangle$ is not entangled and the measurement of the ancilla does not change it.

page 308, line -4 Add:

8. Scalability. To be of a larger potential interest a quantum processor technology should scale sufficiently well. (For example, current NMR liquid state technology at room temperature was considered as one that does not scale well and 12 qubits seems to be its maximum.) On the other hand the recent experimental successes (see Kielpinski et al. (2001), created a hope that ion traps with thousands of ions are a feasible goal).

Chapter 8 — Information

page 319, after line +6 **Remark** Actually we can "derive" the expression for von Neumann entropy as follows. In the case of an observable with spectral representation $A = \sum_i a_i P_i$ the probability of having outcome a_i if a mixed state ρ is measured is $p_i = \text{Tr}(\rho P_i)$. It is then natural to consider (quantum) entropy of ρ as the minimum of $-\sum_i p_i \lg p_i$ for all probabilities obtained by measurement of ρ with respect to an observable. In the case $\rho = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$, where λ_i are eigenvalues of ρ and measurement of ρ is done with respect to eigenvectors of ρ we have, we get that quantum entropy is, by definition, not larger than $-\sum_i \lambda_i \lg \lambda_i$. In the case that measurement of ρ is given by an orthonormal basis $\{\psi_i\}_i$ (or orthogonal projection operators) $|\psi_i\rangle\langle\psi_i|$ the corresponding probabilities are $\Pr(a_i) = \sum_j \lambda_j |\langle\psi_i|\phi_j|^2 = \sum_j \lambda_j p_{ji}$. It can then be shown that $S(\sum_j \lambda_j p_{j1}, \sum_j \lambda_j p_{j2}, \ldots,) \geq S(\lambda_1, \lambda_2, \ldots)$. The measurement in the basis of eigenvectors of the density matrices is then optimal in the sense that entropy of the probability distribution of outcomes is the minimal. In this sense $QS(\rho) = \text{Tr}(\rho \lg \rho)$.

page 319, addition after line +12 (vi) $QS(\rho) = -\sum_{i=1}^{n} \lambda_i \lg \lambda_i$, where $\{\lambda_i \,|\, 1 \leq i \leq n\}$ is the multiset of eigenvalues of ρ. Hence $QS(\rho)$ is the Shannon entropy of the distribution induced by the eigenvalues of ρ on the corresponding eigenvectors; (vii) If $\rho = \sum_{i=1}^{k} p_i |\phi_i\rangle\langle\phi_i|$, for a mixed state $\bigoplus_{i=1}^{k}(p_i, |\phi_i\rangle)$, and the space spanned by the states $\{\phi_i\}_{i=1}^{n}$ has dimension d, then $QS(\rho) \leq \lg d$; (viii) **Insensitivity** If a sequence of density matrices $\{\rho_i\}_{i=1}^{\infty}$ has limit $\lim_{i\to\infty} \rho_i = \rho$, then also $\lim_{i\to\infty} QS(\rho_i) = QS(\rho)$, where convergence of density matrices is with respect to some norm of density matrices that is continuous in matrix entries; (ix) (**Triangle inequality (Araki-Lieb inequality)** if ρ is a density matrix of a bipartite quantum system $A \otimes B$ and ρ_A and ρ_B are defines as above, then $QS(\rho) \geq |QS(\rho_A) - QS(\rho_B)|$; (x) (**Strong subaditivity**) For a density matrix ρ of a three-partite system $A \otimes B \otimes C$ $QS(\rho) + QS(\rho_B) \leq QS(\rho_{AB}) + QS(\rho_{BC})$.

page 319, line +14 Add "Quantum relative entropy has the following properties: (a) Quantum relative entropy can be infinite; (b) **Join convexivity of relative entropy**: If p_i and q_i are probability distributions and ρ_i, σ_i are density matrices, then

$$QS(\sum_i p_i\rho_i || \sum_i q_i\sigma_i) \leq \sum_i p_i QS(\rho_i||\sigma_i) + S(p_i||q_i),$$

(c) $QS(\rho|\sigma) \geq \frac{1}{4\ln 2}||\rho - \sigma||_1$."

page 320, after line -5

Example The so called **Pauli channel** is realised by the superopertor specified by the matrices $A_1 = \sqrt{1-p}I$, $A_2 = \sqrt{p_x}\sigma_x$, $A_3 = \sqrt{p_y}\sigma_y$ and $A_4 = \sqrt{p_z}\sigma_z$, where $p = p_x + p_y + p_z$, and p, p_x, p_y, p_z are non-negative. Pauli channel performs the following mapping of an arbitrary state ρ:

$$\rho \to (1-p)\rho + p_x\sigma_x\rho\sigma_x + p_y\sigma_y\rho\sigma_y + p_z\sigma_z\rho\sigma_z.$$

Since $\sum_{i=1} A_i^* A_i = 1$, we have indeed a superoperator.

A special case of the Pauli channel, if $p_x = p_y = p_z = \frac{p}{3}$ is the so-called depolarizing channel discussed on page 332.

page 320, after line -1 **Definition** Let ρ be a mixed state of a Hilbert space H. A **purification** of ρ is any pure state $|\phi\rangle \in H \otimes H'$ of any extended Hilbert space $H \otimes H'$ such that $\rho = \mathrm{Tr}_{H'}|\phi\rangle\langle\phi|$.

page 331, after line -4 It is actually easy to see why two-way classical communication could increase channel capacity. One idea how to achieve it is that the quantum channel is not used to transmit the input state $|\psi\rangle$ directly. It is first used to transmit halves of several pure EPR pairs. Of course, in a noisy channel they can become this way impure. However, one can now use local operations and classical two-way communication to purify them, see Section 8.3.2, and to distill out of them some smaller number of (nearly) pure pairs. They are then used, together with classical communication, to "teleport" $|\psi\rangle$ with high fidelity.

page 331, at the end Of interest and importance is also to consider several capacities of quantum channels for transmission of classical data. The basic one is so-called **classical capacity**, denoted QC_C, which is defined by

$$QC_C(\mathcal{N}) = \lim_{\varepsilon\to 0}\limsup_{n\to\infty}\{\frac{n}{m} \mid \exists_{m,\mathcal{E},\mathcal{D}}\forall_{\psi\in\{|0\rangle,|1\rangle\}^n}(\langle\psi|\mathcal{D}\mathcal{N}^{\oplus m}\mathcal{E}(|\psi\rangle\langle\psi|)|\psi\rangle > 1-\varepsilon\}$$

and the difference to the definition of $QC(\mathcal{N})$, on page 330, is that instead of taking the universal quantifier over an arbitrary state $\psi \in H_{2^n}$ only states $\psi \in \{|0\rangle, |1\rangle\}^n$ are considered, i.e. universal quantification is only over all "classical states".

There are actually several variants of the classical capacity depending on whether encoding/decoding operators are allowed to be quantum or have to be classical

$$QC_C(\mathcal{N}) = QC_{C-QQ}(\mathcal{N}),\ QC_{C-QC}(\mathcal{N}),\ QC_{C-CQ}(\mathcal{N}),\ QC_{C-CC}(\mathcal{N}) = C(\mathcal{N}),$$

where the notation $QC_{C-ED}(\mathcal{N})$ is used with E (D) denoting the type of the encoder (decoder) allowed — quantum (Q) or classical (C). Investigation of these capacities and their computations (or estimations) is an intensive area of current research. (For some channels, for example for the erasure channel introduced on page 332, all four classical capacities are equal.) Channels $\mathcal{N}$ are known for which $QC_{C-CQ}(\mathcal{N}) > QC_{C-cc}(\mathcal{N})$. In addition, we have trivial inequalities:

$$QC_{C-CC}(\mathcal{N}) \leq QC_{C-QC}(\mathcal{N}), QC_{C-CQ}(\mathcal{N}) \leq QC_{C-QQ}(\mathcal{N}),$$

for any channel N.

page 332, after line +19 Another way of defining a p-depolarizing channel is as a channel transmitting the input qubit faithfully with probability $1-p$ and replacing it by a random qubit with probability p.

page 333, at the end of Section 8.3.1

Remark In quantum information literature one often considers manipulations with bipartite systems at which only local operations and classical communications are allowed (by two parties, one in the possession of one subsystem, second in the possession of the second subsystem). For this cases the following acronyms start to be used:

LOCC — local unitary operations and (two- way) classical communication.

LQCC — local quantum operations (any, including superoperators and POVM measurements) and (two-way) classical communications.[3,4]

ELQCC — entanglement-assisted local (general) quantum operations and classical communication (Jonathan and Plenio, 1999) — (or LOCCSE — local operation, classical communication and shared entanglement). Communicating parties are allowed, in addition to features offered by LQCC, at first to "borrow" some shared entanglement, then to use it for local operations and classical communication, but without consuming it.

(By a "local unitary operator" it is meant here a unitary operator that acts in one of the subsystems and at other subsystems acts as a unitary operators. Similarly, by a local measurement it is meant a measurement that is specified by a self-adjoint operator that acts on one of the subspaces and behaves as a unitary operator on other subspaces.)

The following examples illustrate what can be achieved with such operation s.

1. The singleton state can be transformed to any other Bell state by a local Pauli operator (matrix). This has been used at quantum superdense coding.
2. Local Bell measurement and classical communication (of 2 bits) are the basis of quantum teleportation.

[3] All these operations can be composed from the following ones: (a) appending an ancilla (not entangled with the other subsystem); (b) unitary operations; (c) performing a projection measurement; (d) tracing out a subsystem. Mathematically, we can represent these operations by multilocal superoperators — completely positive linear mappings that do not increase the trace and can be implemented locally, with classical coordination among the parties.

[4] A word of caution, the acronym LOCC is also used instead of LQCC.

3. If $|\psi\rangle$ is a bipartite pure state of a quantum system $A \otimes B$, $\rho = Tr_B|\psi\rangle\langle\psi|$ and $[\Phi\rangle = \bigoplus_{i=1}^{r}(p_i, |\phi_i\rangle)$ be a mixed state of A such that $\rho = \rho_{[\Phi\rangle}$, then there is a local measurement on B whose outcomes make A to collapse to one of the states $\{|\phi_i\rangle\}_{i=1}^{r}$ — and to the state $|\phi_i\rangle$ with probability p_i.

page 334, before line -8 The following facts concerning Werner states W_F are of interest and importance: (a) If $F \geq \frac{1}{4}$, then W_F can be created by transmitting the Bell state Φ^+ through a $(\frac{4}{3}(1-F))$-depolarizing channel (see page 332); (b) W_F is entangled if and only if $F \geq \frac{1}{2}$ (see Bennett et al. 1996b); (c) No Werner state violates a Bell inequality (d) Each two qubit state can be reduced to a Werner state by LQCC (the so-called *depolarization process*); (e) Mutual information of the Werner state is given by $QI(W_p) = QI(W_{p,A} : W_{p,B} = 2 + f\lg f + (1-f)\lg(\frac{1-f}{3})$, where $f = \frac{3p+1}{4}$ and for the relative entropy it holds $E_r(W_f) = 1 + f\lg f + (1-f)\lg(1-f)$; (f) For $F = \frac{1}{2}$ we have totally mixed state.

Remark There are several equivalent definitions of Werner states in $H_2 \otimes H_2$: (a) $W_p = p|\Psi^-\rangle\langle\Psi^-| + \frac{1-p}{4}\mathbf{I}$; $\frac{1}{3} \leq p \leq 1$; (b) Werner states are those states that do not change if subjected to the same unitary transformation to both systems.

Remark In $H_d \otimes H_d$ Werner states have the form $W_q = \frac{1}{d^2-qd}(I + qV)$, where $-1 \leq q \leq 1$ and V is the flip operator $V(\phi \otimes \psi) = \psi \otimes \phi$.

Remark In more details the above two-way purification procedure can be described and analysed as follows. If Alice and Bob share two pairs of non-maximally entangled mixed states, then Alice first transforms her particles into the circular basis and Bob performs the inverse of this basis changing transformations on his particles. After that both of them perform XOR operation on both particles and the measurements on the second particles. They inform each other about the results of the measurement and keep the first pair if the results are the same.

This purification step creates from two pairs of particles in a state ρ with fidelity coefficients

$$A = \langle\Phi^+|\rho|\Phi^+\rangle,\ B = \langle\Psi^-|\rho|\Psi^-\rangle,\ C = \langle\Psi^+|\rho|\Psi^+\rangle,\ D = \langle\Phi^-|\rho|\Phi^-\rangle$$

two particles in the state with coefficients

$$\bar{A} = \frac{A^2+B^2}{P},\ \bar{B} = \frac{2CD}{P},\ \bar{C} = \frac{C^2+D^2}{P}\ \bar{D} = \frac{2AB}{P},$$

where $P = (A+B)^2 + (C+D)^2$ is the probability that Alice and Bob obtain the same results when they measure the second pair of particles. It can be shown that if $A > \frac{1}{2}$, then the above process converges either to the attractor $(A,B,C,D) = (1,0,0,0)$ or $(A,B,C,D) = (0,0,1,0)$.

Remark Entanglement fidelity is also defined as follows:

$$F(\rho) = \max_{\text{all max. ent. } \psi} \langle\psi|\rho|\psi\rangle.$$

page 337, line +6 Instead of the term 'quantum entropy" in this case the terms "quantum partial entropy" or "reduced entropy" start to be used.

page 337, add to line +11 "Maximally entangled pure states are therefore such states that all their amplitudes in Schmidt decomposition are identical."

page 337, after line +17 Entropy (reduced entropy) $E(\phi)$ of a pure bipartite state $|\phi\rangle$ provides also an asymptotically achievable upper bound on the numer of singletons that can be produced from $|\phi\rangle$ by LQCC. Namely, from n states $|\phi\rangle$ the asymptotically achievable maximu of singleton produced is $nE(\phi)$.

Entropy (reduced quantum entropy) of entanglement of a pure bipartite state can also be interpreted as the achievable upper bound on the number of singletons interconvertible to the given state by LQCC.

Entropy (partial entropy) of entanglement has also the following properties (Bennett et al. (1996a), that make it to be a natural measure of entanglement: (a) additivity — $E(|\phi\rangle \otimes |\psi\rangle) = E(|\phi\rangle) + E(|\psi\rangle)$ for any two pure states $|\phi\rangle$ and $|\psi\rangle$; (b) it is preserved under local unitary operations; (c) the expectation value of the entanglement cannot be increased by local non-unitary operations (such as measurements).

page 338, after line +10 Entanglement of creation, E_{cr} is dual to entanglement of distillation. Entanglement of creation of a state ρ, $E_{cr}(\rho)$ can be defined as follows: Alice and Bob wish to create an n copies of ρ having no preshared entanglement, but having possibility to communicate qubits (at a cost) and perform classical communication (at no cost). The entanglement of creation is then defined to be asymptotically minimal value for the ratio of the number of qubits m they transmit to the number n of good (as $n \to \infty$) copies of ρ they create.

page 337, line -6 Add "(Entanglement of formation is also un achievable upper bound on the efficient of entanglement purification procedure.)"

page 338, after line +19

Remark The basic idea behind the entanglement of relative entropy of a state ρ is to define the amount of entanglement in ρ by a "minimal distance" between ρ and separable (unentangled) mixed states. The relative entropy $E(\rho||\sigma) = Tr(\rho \ln \rho - \rho \ln \sigma)$ seems to serve this purpose quite well even if it is not really distance in the mathematical sense (for example it is not even symmetric).

page 338, after line +16 Several other measures of entanglement of density matrices have been defined and explored. For example:

Total entanglement, E_t, (Horodecki et al. (1998b), defined by

$$E_t(\rho) = \lim_{n\rightarrow\infty} \frac{E_f(\rho^{\otimes n})}{n},$$

where $\rho^{\otimes n} = \overbrace{\rho \otimes \ldots \otimes \rho}^{ntimes}$. $E_t(\rho)$ can be interpreted as the least number of singletons asymptotically required to prepare ρ by means of local quantum operations and classical communications (LQCC). It can also be seen as dual to the entanglement of distillation, which can be considered as as the greatest number of singletons that can asymptotically be prepared by means of LQCC. (It is an open problem whether $E_t = E_f$. To show this equality it would be enough to show an identity $E_f(\rho \otimes \rho) = 2E_f(\rho)$, which holds for E_t.)

page 339, an addition after the last line Of interest and importance is also to search for analogies between basic concepts of physics and new concepts of quantum information processing. An analogy **energy — entanglement** has been explored by Horodecki et al. (1998b). They identify and analyse the following quantum information theoretical counterparts of the thermodynamic concepts: free energy — free entanglement, bound energy — bound entanglement, internal energy — total entanglement (see page 45 of these *Additions*).

page 339, at the end As pointed out by Plenio and Vedral (1998), it is useful to see "no entanglement increase by local operations principle (law)" in two forms.

Principle 1 There is no way, with no matter how small probability, to get an entangled bipartite state out of unentangled states by LQCC.

Principle 2 There is no way to increase the expectation amount of entanglement of a bipartite state by LQCC.

Observe, that the second formulation leaves a space to increase entanglement with some probability if it gets decreased with another probability and in the average it does not get increased.

Chapter 9, Appendix

page 343, line +11 Replace "constant" by "constant and $h \approx 6.62 \times 10^{-34}$ Joule $\times$ second".

page 344, new paragraph before Remark 9.1.1 Quantum theory as described above is nowadays termed mainly *quantum mechanics* — a theory of matter. Quantum physics ectually encompasses also *quantum field theory* — a theory of fields (the word "field" reflects the fact that the theory deals with some quantum anlogues of the electric and magnetic field).

The first steps in creating quantum field theory were due to Dirac in 1926. Quantum field theory was motivated by the question how an atom radiates light if electrons "jump" from an excited state to the ground state. Actually, quantum field theory was developed to make compatible quantum mechanics and the special theory of reality.

Important steps in the development of quantum field theory were approaches represented by quantum electrodynamics (QED), due to Feynman, Schwinger and Tomonaga and quantum chromodynamics (QCD).

QED and QCD can be seen as cornstones of the so-called *standard model* that has been able succesfuly to explained every particle experiment carried on so far.

The development of quantum physics can hardly be considered as finished yet beacause physics remains to be empirical. Basic properties of particles need still to be measured. What is needed is a theory that could derive and predict them.

For a short, well readible and insightfull account of the hundred years of quantum theory is due to Kleppner and Jackiw (2000). Especially worth to note is an observation that even though quantum mechanics can be seen as being born in 1900, and its fathers were quite sceptic to see what came out of their theories, it took 20 more years and a new generation of physicists were required to create fully modern quantum mechanics. (Current situation in quantum theory, especially in connection with QIPC, seems to be quite similar to that one hundred years ago.)

page 345, line +9 Add: "That are also reasons why, as it seems, von Neumann, one of the fathers of modern quantum mechanics and also of modern computers, did not (or could not) discover quantum computing."

page 362, after line +7

Remark A variety of "hidden-variable theories (interpretations)" of quantum mechanics has been developed. The first such approaches have been already due to Born and Brogglie (in 1927).

The common idea of these theories is the postulate that alongside of measurable quantities (as position, momentum spin, ...) dealt with by the (current) theory, there are further quantities (called *hidden variables*), (currently) inaccessible to measurements, whose values determine fully the values provided by the individual measurements (of the observable). The quantum mechanics statistics are then obtained by making an average over the values of the hidden variables. The inaccessability of the hidden variables may be a temporary matter and can change as new theoretical knowledge or experimental techniques emerge; or these quantities may be inaccessible in principle.

No-go theorems are theorems to show that no hidden variable theory satisfying certain constraints can reproduce quantum mechanics statistics. The first such theorem was due to von Neumann (1932). However, his constraints are now considered as too severe and theorems due to Bell (1964) and Kochen and Spencer (1967) are now considered as much more convincing.

Hidden variable theory developed by Bohm, and called also *Bohmian mechanics*, is also sometimes considered as one of the simplest *pilot-wave theories*. In such theories quantum mechanics is fundamentally about the behaviour of particles (described by their positions) and fields (described by their configurations) and only secondary about quantum states (wave-functions).

page 362, end

Remark Let us at least list some other interpretation that either received larger attention or are very recent.

- Coherent histories interpretation initiated by R. Griffiths (1984) and R. Omnès (1992, 1994). This interpretation is primarily concerned with histories of observables (and not of the states). It tries to assign probabilities to observables histories. Currently this approach seems to be seen as not well defined but still as an option to consider (for the development of a quantum theory without observers).

page 364 at the end

Remark Well readable recent analyses of the Bell theorem testing experiments are due to Hardy (1998) and Percival (2000). Here are some main points of the analysis.

- All experiments performed till recently made use of an untestable suplementary "fair sampling assumption" (the exception is experiment reported by Kielpinski et al. (2001)). Its basic idea is that "the detectors sample the ensemble in a fair way so that those events in which both photons are detected are representable of the whole ensemble" and or "that detector efficiency is not dependent on local "hidden variables".
- Without the above assumptions the detectors used in the experiments need to have some efficiency (estimated to be at least 67%) what is far more than what has been achieved so far.
- It is far from clear whether we can performed Bell experiments with ever increasing precision and whether we do not discover some laws of nature that prevents us of doing that.

Experiment reported by Kielpinski et al. (2001) closed detection loophole for the first time, but non-locality loophole remained open for their experiment because detection events on two ions occured within each other's lightcones.

9.1.9 Detailed proofs of Bell theorem

Two detailed proofs of the Bell theorem will now be presented (see Hardy (1998)). The first one is just a more detailed and complete version of the one sketched in the previous section in the book and the second one is without "Bell inequalities".

A photon with linear polarization along a direction θ to the vertical axis (to vector $|1\rangle$) is represented by the state

$$|\theta\rangle = \cos\theta|1\rangle + \sin\theta|0\rangle.$$

A photon with orthogonal polarization has then the state

$$|\theta^\perp\rangle = \sin\theta|1\rangle - \cos\theta|0\rangle.$$

From that it follows that:

$$|1\rangle = \cos\theta|\theta\rangle + \sin\theta|\theta^{\perp}\rangle,$$

$$|0\rangle = \sin\theta|\theta\rangle - \cos\theta|\theta^{\perp}\rangle.$$

Let us now assume that two photons are in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle,$$

and we want to measure the first (second) photon with respect to the polarization θ (ϕ). Corresponding probabilities can be determined easily once we represent state of photons with respect to the polarization chosen and this way we get:

$$\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) && (8)\\
&= \frac{1}{\sqrt{2}}([\cos\theta|\theta\rangle + \sin\theta|\theta^{\perp}\rangle][\sin\phi|\phi\rangle - \cos\phi|\phi\rangle] && (9)\\
&- [\sin\theta|\theta\rangle - \cos\theta|\theta^{\perp}\rangle][\cos\phi|\phi\rangle + \sin\phi|\phi^{\perp}\rangle]) && (10)\\
&= \frac{1}{\sqrt{2}}[\cos\theta\sin\phi - \sin\theta\cos\phi]|\theta\rangle|\phi\rangle && (11)\\
&+ \frac{1}{\sqrt{2}}[\cos\theta\cos\theta - \sin\theta\sin\phi]|\theta\rangle|\phi^{\perp}\rangle && (12)\\
&+ \frac{1}{\sqrt{2}}[\sin\theta\sin\phi + \cos\theta\cos\phi]|\theta^{\perp}\rangle|\phi\rangle && (13)\\
&+ \frac{1}{\sqrt{2}}[-\sin\theta\cos\phi + \cos\theta\sin\phi]|\theta^{\perp}\rangle|\phi^{\perp}\rangle. && (14)
\end{aligned}$$

From that it follows, for example, that the probability that the measurement produces particles in the state $|\theta\rangle|\phi^{\perp}\rangle$ is

$$|\alpha\cos\theta\cos\phi - \beta\sin\theta\sin\phi|^2.$$

Let us now assume that instead of the Gedanken experiment with electrons we perform one with polarized photons, with two separated photons in the state $\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$ that are sent in two opposite directions and then measured with respect to polarizations θ and ϕ

Let us define the correlation function

$$E(\theta,\phi) = \text{Average}(A(\theta)B(\phi)),$$

where $A(\theta) = +1(=-1)$ if the left photon comes out polarized as $|\theta\rangle$ (polarized as $|\theta^{\perp}\rangle$). Similarly for $B(\phi)$.

Let now the average is taken over many experiments. Probabilities $\Pr(\theta,\phi)$ and $\Pr(\theta^{\perp},\phi^{\perp})$ contribute to $A(\theta)B(\phi) = +1$ and the probabilities $\Pr(\theta,\phi^{\perp})$ and $\Pr(\theta^{\perp},\phi)$ contribute to $A(\theta)B(\phi) = -1$.

Therefore

$$E(\theta,\phi) = \Pr(\theta,\phi) + \Pr(\theta^{\perp},\phi^{\perp}) - \Pr(\theta,\phi^{\perp}) - \Pr(\theta^{\perp},\phi).$$

Using the formulas obtained before we get that

$$E(\theta,\phi) = -\cos(2(\theta-\phi)).$$

Let us now assume now that before two photon separate they exchange instructions how to behave (which way to get out) at different measurements.

This instruction code, denoted λ and called *hidden variable*, can be anything we want. These hidden variables can be different at distinct runs of the experiment. We can assume that, over a large number of runs of the experiment, that they are distributed according to a probability density function ρ and therefore

$$\int \rho(\lambda)\, d\lambda = 1.$$

The values of $A(\theta)$ and $B(\phi)$ will also depend on λ, notation $A(\theta,\lambda)$ and $B(\phi,\lambda)$. We assume that these functions do not depend on the setting at the other end of the experiment and that distribution $\rho(\lambda)$ does not depend on θ,ϕ.

In a local hidden variable theory the correlation function can be written as follows:

$$E(\theta,\phi) = \int A(\theta,\lambda)B(\phi,\lambda)\rho(\lambda)\, d\lambda.$$

Let C, D, A, B be variables taking on values ± 1, then, as discussed in the book,

$$C(A+B) + D(A-B) = \pm 2 \tag{15}$$

If we put $C = A(\theta, \lambda)$, $D = A(\theta', \lambda)$, $A = B(\phi, \lambda)$ and $B = B(\phi', \lambda)$ into equation (15), multiply by $\rho(\lambda)$ and then integrate over λ we get the so-called **Bell inequalities** (actualy a version of the Bell inequalities derived by Cluster et al.)

$$-2 \leq E(\theta, \phi) + E(\theta, \phi') + E(\theta', \phi) - E(\theta', \phi') \leq +2.$$

These inequalities express a constraint that all local variable theories should satisfy.

Observe that in order to derive thse inequalities we did not use quantum mechanics. Bell inequalities are therefore not about quantum mechanics.

In order to drive the above inequalities we have used onlythe so called local realism assumptions about physical world. namely that observable quantities have values independent of observations and that ,easurements performed one of the party could not perform a non-local influence on the measuremnt process performed by another party.

However, if we take

$$\theta = 0^\circ,\ \theta' = 45^\circ, \quad \phi = 22.5^\circ, \quad \phi' = -22.5^\circ$$

and the value of the average E derived from quantum mechanics (that is $E(\theta, \phi) = -\cos(2(\theta - \phi)))$ we get that

$$E(\theta, \phi) + E(\theta, \phi') + E(\theta', \phi) - E(\theta', \phi') = 2\sqrt{2}$$

what violates Bell inequalities.

Corollary: Quantum predictions cannot be reproduced by a local hidden variable mode

Proof of Bell Theorem without Bell inequalities (Greenberger et al. 1990)

Let us assume that three photons are created in the state

$$\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$$

and photons move in three different directions where they are measured with respect to the standard ($\mathcal{B}$) or the dual basis ($\mathcal{D}$). If we take results of the measurement as being 1 for $|0\rangle$ or $|0'\rangle$ and -1 for $|1\rangle$ or $|1'\rangle$ and $A(., \lambda)$, $B(., \lambda)$ and $C(., \lambda)$ denotes the results of the measurement of the first, second and third photon in the appropriate basis submitted for the first parameter (with λ standing again for hidden variables), then it is easy to see that the product of the values of A, B and C at different measurements have the following values

$$\begin{aligned} A(\mathcal{B},\lambda)B(\mathcal{B},\lambda)C(\mathcal{B},\lambda) &= +1, \\ A(\mathcal{B},\lambda)B(\mathcal{D},\lambda)C(\mathcal{D},\lambda) &= -1, \\ A(\mathcal{D},\lambda)B(\mathcal{B},\lambda)C(\mathcal{D},\lambda) &= -1, \\ A(\mathcal{D},\lambda)B(\mathcal{D},\lambda)C(\mathcal{B},\lambda) &= -1. \end{aligned}$$

In the case there are no nonlocal influences the result of one measurement cannot influence the other two and therefore we can assume that values of variables A, B and C appearing in different equations for the same basis are the same. We can then multiply the left and the right sides of all four equalities. However, the product of the left sides gives the value 1 because each value appears there twice and the product of the right sides gives the value -1. A contradiction.

page 369, after line +3

Remark An important related concept is that of **operator monotones**. It is a function f on operators such that for all Hermitean operators $A \geq B$ implies $f(A) \geq f(B)$. An important example of operator monotones is $f(x) = \lg x$.

page 371, before Section 9.2.3

Remark The set of Hermitian operators on H_2 forms a four-dimensional vector space over reals and $\{\sigma_x, \sigma_y, \sigma_z, I\}$ is the orthonormal basis of this space with respect to the inner product $\langle A|B\rangle = \frac{1}{2}Tr(AB)$.

page 372, after line -15

Remark Density matrices are often defined as *trace class operators with trace* 1. By "trace class operators" positive operators with finite trace are meant.

page 373, after line -13

Remark In general, if $\{P_i\}_{i=1}^k$ is a sequence of projection operators, $\{a_i\}_{i=1}^k$ is a sequence of non-negative integers with $\sum a_i = 1$, then $D = \sum_{i=1}^k a_i P_i$ is a density matrix.

As already discussed, there is, in general, no unique decomposition of density matrices into sums of projection operators.

In particular, if P_1 and P_2 are projection operators representing pure states, and $\lambda_1 \geq 0$, $\lambda_2 \geq 0$, $\lambda_1 + \lambda_2 = 1$, then $\lambda_1 P_1 + \lambda_2 P_2$ is a density operator (mixed state). That is why it is often said that the set of mixed states is convex.

page 374, after line +4

Remark Several additional useful, interesting properties of density matrices:

- Each density matrix ρ can be expressed in the form $\rho = \sum_{i=1}^{k} p_i|\phi_i\rangle\langle\phi_i|$, where $\sum_{i=1}^{k} p_i = 1$ and states in $\{\phi_i\}_{i=1}^{k}$ form an orthonormal basis. If this is the case $\sqrt{\rho} = \sum_{i=1}^{k} \sqrt{p_i}|\phi_i\rangle\langle\phi_i|$
- Density matrices corresponding to mixtures of basis states are diagonal.
- A density matrix of degree 2^n represents a pure states iff it has two eigenvalues: 0 with multiplicity $2^n - 1$ and 1 with multiplicity 1.
- Density matrices ρ in H_2 have the following **Bloch vector representation**
$$\rho = \frac{1}{2}[I + \bar{\lambda} \cdot \bar{\sigma}],$$
where $\bar{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is a (Pauli) vector of Pauli matrices, $\bar{\lambda} = (\lambda_1, \lambda_2, \lambda_3)$ is a real vector such that $|\lambda| = \lambda_1^2 + \lambda_2^2 + \lambda_3^2 \leq 1$ and $\bar{\lambda} \cdot \bar{\sigma} = \lambda_1\sigma_x + \lambda_2\sigma_y + \lambda_3\sigma_z$. ρ is a pure state, that is $\rho = |\phi\rangle\langle\phi|$ for a pure state $|\phi\rangle$, if and only if $|\lambda| = 1$. $\bar{\lambda}$ is called **Bloch vector** and this vector is on unit sphere in the 3-dimensional real space if the state is pure; otherwise it is inside of the sphere. Bloch vector representation of density matrices is often useful. (Observe that Bloch vector has only three components and they are real – they are sufficient to represent a 4-element density matrix).
- Determinants of density matrices in H_2 have values between 0 and $\frac{1}{4}$.
- (van Dam et al. (1999)) Each such density matrix can be written in the form
$$\rho = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1| + \alpha|1\rangle\langle 0| + \alpha^*|0\rangle\langle 1|,$$
where $0 \leq p \leq 1$ and α is a complex number such that $|\alpha|^2 \leq p(1-p)$. Representation of a density matrix in such a form will be

denoted by $\rho(p,\alpha)$. $\rho(p,\alpha)$ is a pure state iff $|\alpha|^2 = p(1-p)$. Projection measurement in the standard basis maps a density matrix $\rho(p,\alpha)$ into $\rho(p,0)$.

In $\rho(p,\alpha)$ notation for density matrices the trace norm for the difference between two density matrices $\rho(p,\alpha)$ and $\rho(q,\beta)$ has an elegant form

$$||\rho(p,\alpha)-\rho(q,\beta)||_1 = ||\overline{\rho(p,\alpha)}-\overline{\rho(q,\beta)}|| = 2\sqrt{(p-q)^2+|\alpha-\beta|^2}.$$

Moreover, if G is a superoperator in H_2 and if ρ_1,ρ_2 are density matrices over H_2, then

$$||G(\rho_1)-G(\rho_2)||_1 \leq ||\rho_1-\rho_2||_1.$$

- (van Wim et al. (1999) Density matrices in H_2 can be represented by points in the unit radius Bloch Ball. Each such point (vector) $\overline{u}$ can be specified by its norm (length of the corresponding vector) $r>0$, *latitude* — the angle between the x-axis and the vector $\overline{u}$ — $\theta \in [0,\pi]$ and *longitude* — the angle between the x-axis and the orthogonal projection of $\overline{u}$ in the plane defined by $z=0$ — $\phi \in [0,2\pi)$. If $\bar{u}=(x,y,z)$, then $x=r\sin\theta\cos\phi$, $y=r\sin\theta\sin\phi$, $z=r\cos\theta$. In such a case to any density matrix ρ there is a unique point $\bar{\rho}=(x,y,z)$ in the Bloch Ball such that

  $$\rho = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ z+iy & 1-z \end{pmatrix}.$$

  and in iddition,

  $$\bar{\rho(p,\alpha)} = (2Re(\alpha), 2Im(\alpha), 2p-1).$$

  For each superoperator G on density matrices over H_2 there exists a unique affine transformation $\bar{G}$ over $\mathbf{R}^3$ which maps Bloch Ball into itself and for all density matrices ρ over H_2 it holds $\bar{G}(\bar{\rho}) = \overline{G(\rho)}$.

  The affine transformation in $\mathbf{R}^3$ corresponding to projection measurement in the standard basis is the orthogonal projection to the z-axis. It maps $\bar{\rho}=(x,y,z)$ into $(0,0,z)$.

- Each density matrix ρ in H_4 has a unique decomposition $\rho = \lambda|\phi\rangle\langle\phi| + (1-\lambda)\rho_s$, where ϕ is a pure entangled state and ρ_s is a separable density matrix (Lewenstein and Sanpera, 1997).

page 374, line -1 Add: "Trace-preserving completely positive superoperators capture all physically allowed transformations: unitary transformations, tracing out operations, tensoring with constant qubits and general measurement.

Of importance are also norms on density matrices. Let us list some of them and their properties:

Trace norm $||\rho||_1 = \mathrm{Tr}(\sqrt{\rho^*\rho})$. Properties:

1. $||\rho||_1 = \sup_{B\neq 0} \frac{|\mathrm{Tr}AB|}{||B||}$;
2. $||\rho-\sigma||_1 = \max_{\mathcal{O}}\{||p_\rho^{\mathcal{O}} - p_\sigma^{\mathcal{O}}||\}$ where $p_\rho^{\mathcal{O}}$ is the probability distribution on the outcomes of the measurement on ρ with respect to observable $\mathcal{O}$.
3. $||\rho||_1 \geq ||F(\rho)||_1$ for any trace-preserving completely positive superoperator F;
4. $||\rho_1-\rho_2||_1 \leq ||F(\rho_1)-F(\rho_2)||_1$ for any density matrices ρ_1, ρ_2 and any superoperator F.
5. $||\rho-\sigma||_1 \leq 4\ln 2QS(\rho|\sigma)$
6. If ρ is a density matrix of a bipartite system $A\otimes B$, $\rho_a = \mathrm{Tr}_B\rho$ and $\rho_B = \mathrm{Tr}_A\rho$, then (1) $0 \leq ||\rho - \rho_A\otimes\rho_B||_1 \leq 2$; (b) $||\rho-\rho_A\otimes\rho_B||_1 \leq \sqrt{3QI(A:B)}$.
7. For any density matrices $\rho(p,\alpha)$ and $\rho(q,\beta)$ for qubits, see page 54, it holds
$$||\rho(p,\alpha)-\rho(q,\beta)||_1 = 2\sqrt{(p-q)^2+|\alpha-\beta|^2}.$$

page 375, after line -12

Remark As discussed above pure states and mixed states (density matrices) define probability measures on subspaces of a Hibert space. The so-called *Gleason theorem* says that all probability measures on subspaces of a Hibert space can be obtained this way.

page 376, before Section 9.2.5 Spin-$\frac{1}{2}$ observables

In the case of spin-$\frac{1}{2}$ particles, it is well known how to represent in H_2 observables S_α, which has two values (spin-up and for any direction of the spin, given by a point α on the unit sphere) and how to determine the probability with which this observable observes a direction represented by a point β on the unit sphere (see, for example, Hughes (1997), for details).

In the case α is represented by the cartesian coordinates (x, y, z), with $x^2 + +y^2 + z^2 = 1$, then

$$S_\alpha = \begin{pmatrix} z & x - iy \\ x + iy & -z \end{pmatrix}$$

and therefore $S_\alpha = x\sigma_x + y\sigma_y + z\sigma_z$.

In the case α is given by spherical coordinates (ϕ, θ) with the azimutal angle ϕ and the longitude θ (where $-\pi \leq \phi \leq \pi$ and $-\frac{\pi}{2} \leq \theta \leq \frac{\pi}{2}$), the corresponding projection operator is represented by the matrix

$$P(\alpha) = \begin{pmatrix} \cos^2(\frac{\phi}{2}) & \cos\frac{\phi}{2}\sin\frac{\phi}{2}e^{-i\theta} \\ \cos\frac{\phi}{2}\sin\frac{\phi}{2}e^{i\theta} & \sin^2(\frac{\phi}{2}) \end{pmatrix}$$

and the projection is into the subspace spanned by the vector $(\cos\frac{\phi}{2}e^{-i\theta/2}, \sin\frac{\phi}{2}e^{i\theta/2})$.

The probability $Pr_\alpha(\beta)$ with which a direction β is projected into α is then given by

$$Pr_\alpha(\beta) = \cos^2\frac{1}{2}\widehat{\alpha\beta}.$$

As demonstrated by Hughes (1997) the above results can be obtained on the basis of several basic principles concerning such observables and the probabilities they assign to various spin directions.

page 376, before Section 9.2.6 Another very basic question concerning quantum mechanics is whether we can show that evolution of quantum systems is indeed described by the Schrödinger equation.

To a certain extent this question can be answered positively. The following technical result is the basis for that.

Stone theorem. If transformations $U(t)$ form the so-called weakly continuous group of evolution operators on a Hilbert space H, parametrized by all real numbers t, then there is a unique Hermitian operator A on H such that for all t, $U(t) = e^{-At}$.

It is then possible to show, see for example Hughes (1997), from very general postulates which quantum evolution should satisfy, that the quantum evolution operators $U(t)$ satisfy conditions of the Stone theorem. The Schrödinger equation is therefore the one describing dynamics of quantum mechanics. However, such arguments do not reveal why the corresponding Hermitian operator should be the Hamiltonian of the quantum system.

Chapter 9, Exercises

page 394, Exercise 42 Show that any two-qubit state $|\psi\rangle$ can be expressed in the form

$$|\psi\rangle = \alpha|\phi_1\rangle|\psi_1\rangle + \beta|\phi_2\rangle|\psi_2\rangle,$$

where $\{|\phi_1\rangle, |\phi_2\rangle\}$ and $\{|\psi_1\rangle, |\psi_2\rangle\}$ are orthonormal bases in H_2.

page 394, Exercise 43 (Bruß et al. 1999) Show for operators $A_0 = \frac{1}{2}\sqrt{1+3\theta}I$, $A_i = \frac{1}{2}\sqrt{1-\theta}\sigma_i$, $i \in \{x, y, z\}$: (a) $\sum_{i\in\{0,x,y,z\}} A_i A_i^* = 1$; (b) $\sum_{i\in\{0,x,y,z\}} A_i\sigma_k A_i = \theta\sigma_k$ for any $k \in \{x, y, z\}$.

page 394, Exercise 44 Show unitarity of the following matrices: (a) (Kikusts, 1999)

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \dots & a_{n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{pmatrix}, \text{ where } a_j = \frac{1}{\sqrt{n}} e^{\frac{2\pi i}{n} j^2}.$$

(b) $\frac{1}{\sqrt{3}}\begin{pmatrix} 1 & -\sqrt{2} \\ \sqrt{2} & 1 \end{pmatrix}$; (c) $\frac{1}{\sqrt{2}}\begin{pmatrix} \omega & -\omega \\ \omega^2 & \omega^2 \end{pmatrix}$, where $\omega = e^{2\pi i/3}$.

page 394, Exercise 45 (Ambainis and Freivalds, 1998) Let L be a regular language and $\mathcal{A}$ its minimal DFA with the transition function δ. Let there be no two states q_1, q_2 of $\mathcal{A}$ and no word w such that: (a) $q_1 \neq q_2$, (b) $\delta(q_1, w) = q_2$ and $\delta(q_2, w) = q_2$, (c) q_2 does not accept (reject) all words. Show that L can be accepted by a MM-1QFA with probability at least $\frac{7}{9} + \varepsilon$, $\varepsilon > 0$.

page 394, Exercise 46 Show that if a language can be recognized by a MM-1QFA with n states, then it can be recognized by a DFA with $2^{\mathcal{O}(n)}$ states.

page 394, Exercise 47 Show that a pure state $|\psi\rangle$ of a composed Hilbert space $A \otimes B$ is entangled if and only if $\rho_A^2 = \rho_A$ for $\rho_A = Tr_B|\psi\rangle\langle\psi|$. (On the other hand, it is one of the basic open problems how to determine whether a given mixed state (density matrix) is entangled.)

page 394, Exercise 48 Show that the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$ is the eigenvector of the following matrices: (a) $\sigma_y \otimes \sigma_y \otimes \sigma_x$; (b) $\sigma_y \otimes \sigma_x \otimes \sigma_y$; (c) $\sigma_x \otimes \sigma_y \otimes \sigma_y$; (d) $\sigma_x \otimes \sigma_x \otimes \sigma_x$ and determine the corresponding eigenvalues.

page 394, Exercise 49 There is a simple argument demonstrating that cloning could be used to transfer signals at the speed larger than the speed of the light. Develop this argument.

page 394, Exercise 50 (Cleve, 1999; Boykin et al., 1999) Let $V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, $W = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/4)} \end{pmatrix}$. Show: (a) Toffoli gate can be simulated by a circuit consisting only of Hadamard gates, XOR gates and controlled-V and $-V^*$ gates (7 of such gates should be enough); (b) controlled-V gate can be simulated by a circuit consisting of W, W^* and XOR gates.

page 394, Exercise 51 Construct density matrices and determine their eigenvalues, eigenvectors and von Neumann entropy for the following mixed states: (a) $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, \cos\phi|0\rangle + \sin\phi|1\rangle)\}$; (b) $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, \alpha|0\rangle + \beta|1\rangle)\}$; (c) $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}(\frac{1}{\sqrt{2}}, (|0\rangle + |1\rangle)\}$.

page 394, Exercise 52 Show that the following code (Bennett and Shor, 1998) can be used to correct any one bit or/and phase error.

$$|0\rangle \rightarrow \frac{1}{2}(|000000000\rangle + |111111000\rangle + |111000111\rangle + |000111111\rangle)$$

$$|1\rangle \rightarrow \frac{1}{2}(|111111111\rangle + |000000111\rangle + |000111000\rangle + |111000000\rangle).$$

page 394, Exercise 53 Show, using no cloning theorem, that for $p = \frac{1}{2}$ neither erasure nor depolarizing channel have nonzero unassisted quantum capacity.

page 394, Exercise 54 Determine in which Hilbert space there is an orthonormal basis with the following properties (if there is some, then construct one): (a) all basis states are maximally entangled; (b) all basis states are bound entangled.

page 394, Exercise 55 (Bose et al. 1997) Show that multipartite entanglement can allow one party to read bit-messages of other parties through a single measurement.

page 394, Exercise 56 Show how to create a GHZ state from two singlets.

page 394, Exercise 57 (a) Let particles P_1 and P_2 as well as P_3 and P_4 are in the entangled state $\cos\theta|00\rangle + \sin\theta|11\rangle$. Let the Bell measurement be applied to particles P_2 and P_3. What are the resulting states and with which probabilities are they obtained? (b) Let particles P_1 with P_2 and P_3 with P_4 be in the entangled states $\cos\theta_1|00\rangle + \sin\theta_1|11\rangle$ and $\cos\theta_2|00\rangle + \sin\theta_2|11\rangle$. Again let the Bell measurement be applied to particles P_2 and P_3. What are the resulting states and their probabilities?

page 394, Exercise 58 Determine the difference between the case that on a 2-qubit state XOR operation is applied or the following unitary matrix:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1+i & 0 & 0 & 0 \\ 0 & 1-i & 0 & 0 \\ 0 & 0 & 0 & 1+i \\ 0 & 0 & 1-i & o \end{pmatrix}.$$

page 394, Exercise 59 (Brassard et al., 1999) Find eigenvalues and eigenvectors of the following matrices:
(a) $\begin{pmatrix} \cos\phi & \sin\phi \\ sin\phi & -\cos\phi \end{pmatrix}$; (b) $\begin{pmatrix} \cos\phi & e^{\psi i}\sin\phi \\ e^{\psi i}\sin\phi & -\cos\phi \end{pmatrix}$.

page 394, Exercise 60 (Brassard et al., 1999) Determine the probabilities of four possible results of the two consecutive measurements of the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, with respect to the observables $R(x)$ and then $R(y)$, where $R(x) = \begin{pmatrix} \cos x & \sin x \\ \sin x & -\cos x \end{pmatrix}$.

page 394, Exercise 61 Show that each unitary matrix U can be decomposed as $U = PDP^*$, where D is the diagonal matrix of the eigenvalues of U and P is a unitary matrix.

page 394, Exercise 62 (Brodsky, Pippenger, 1999) Show that if U is a unitary matrix, then to any $\varepsilon > 0$ there is an n_ε such that $||(I - U^{n_\varepsilon}x||^2 < \varepsilon$ for all vectors x such that $||x|| \leq 1$.

page 394, Exercise 63 (Moore, 1999) Let us call "modulo-2 gate" the gate $(x_1,\ldots,x_n) \rightarrow (x_1,\ldots,x_{n-1},x_n \oplus ((x_1+\ldots+x_{n-1}) \bmod 2)$ and by n-ary "fanout gate" the gate $(x_1,\ldots,x_n) \rightarrow (x_1, x_1\oplus x_2, x_1\oplus x_3,\ldots,x_1\oplus x_n)$. Show that each of these two gates can be realized by a quantum circuit of depth 3 consisting of the other gate and the Hadamard gates.

page 394, Exercise 64 (Moore, 1999) Show that n-ary modulo-2 gate can be realised by a circuit of depth 3 consisting of the Hadamard gates and the control shift gates $(x,y) \rightarrow (x,(-1)^{xy}y)$.

page 394, Exercise 65 What is the operational meaning of the gate represented by the following matrices: (a)

$$\begin{pmatrix} I &&&&&&& \\ & X &&&&&& \\ && X &&&&& \\ &&& I &&&& \\ &&&& X &&& \\ &&&&& I && \\ &&&&&& I & \\ &&&&&&& X \end{pmatrix} \quad \text{where } X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

page 394, Exercise 66 Show that error matrices, page 272, line -2, are "trace-orthogonal", i.e. $Tr(M^{(i)}M^{(j)}) = 2^n\delta_{ij}$.

page 394, Exercise 67 Let EXCH be a degree four unitary matrix representing the transformation realized by the qubit exchanging circuit in Fig. 2.13b. (a) Determine elements of EXCH; (b) show that EXCH.$(X \otimes Y) = Y \otimes X$ for any two matrices of degree 2.

page 394, Exercise 68 (Tucci, 1999) Denote $X\bar{O}R$ the unitary matrix realizing transformation $(x, y) \rightarrow (x, \bar{x} \oplus y)$. (a) Show four different quantum circuits consisting of XOR and $X\bar{O}R$ gates that realize the unitary mapping EXCH.; (b) Show four different quantum circuits consisting of XOR and $X\bar{O}R$ gates implementing unitary transformation given by the matrix

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

page 394, Exercise 69 (Golovkins, 1999) Show that for infinite matrices with only finitely many non-zero elements in each column and row the following properties hold. (a) multiplication of matrices is associative; (b) if $UU^* = 1$, then the norm of any row vector of U does not exceed 1; (c) if $UU^* = 1$, then row vectors of U are orthogonal if and only if every row vector of the matrix has norm 0 or 1; (d) U is unitary if and only if $UU^* = 1$ and its row vectors are orthonormal.

page 394, Exercise 70 Show that if f is "nice", then also two definitions $f(A)$, where A is a matrix, presented on page 4 are equivalent.

page 394, Exercise 71 Show that the following relations hold for arbitrary linear operators and commutators: (a) $[AB,C] = A[B,C]+[A,C]B$; (b) $[A,BC] = [A,B]C+B[A,C]$; (c) $0 = [A,[B,C]]+[B,[C,A]]+[C,[A,B]]$.

page 394, Exercise 72 Let A, B be operators on a Hilbert space such that $[A,B] = I$. Then it holds: (a) $[B,A^i] = i[B,A^{i-1}]$ if $i > 1$; (b) $[B,f(A)] = \frac{df(A)}{dA}$.

page 394, Exercise 73 (Smolin, 2000) Show that the mixed state $\bigoplus_{i,j=0}^{1}(\frac{1}{4},\Phi_{ij}\otimes\Phi_{ij})$, where Φ_{ij} stands for all four Bell states, forms a four-party state with the following properties: (a) it is an entangled state; (b) it is the state with bound entanglement — no pure entanglement can be distilled from it by LQCC operations; (c) whenever any two parties get together they can perform a measurement which enables the other two parties to create a pure maximally entangled state between them without coming together.

page 394, Exercise 74 Show that the matrix iXOR can be realized by a circuit consisting of 5 out of the matrices

$$\begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \quad \begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix} \quad \begin{pmatrix} e^{i\theta} & 0 & 0 & 0 \\ 0 & e^{-i\theta} & 0 & 0 \\ 0 & 0 & e^{-i\theta} & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}$$

for proper choices of θ and α.

page 394, Exercise 75 (a) Let a two-input/output quantum gate is represented by a unitary matrix $A = \{a_{ij}\}_{i.j=1}^{4}$. Describe the unitary matrix for the gate with reverse inputs; (b) Let a 3-input/output quantum gate is represented by a unitary matrix $A = \{a_{ij}\}_{i,j=1}^{8}$. Let π be a permutation on the set $\{0,1,2\}$. Describe unitary matrix for the gate obtained using permutation π of inputs.

page 394, Exercise 76 Let P be a projection and c a real number. Show that $e^{cP} = e^cP + I - P$.

page 394, Exercise 77 (Gudder, 2000) Let P_1 and P_2 are projection matrices such that $P_1P_2 = 0 = P_2P_1$ and $P_1 + P_2 = I$ and θ is a real number. Show that $e^{i\theta P_1 - i\theta P_2} = e^{i\theta}P_1 + e^{-i\theta}P_2$.

page 394, Exercise 78 Determine matrix representation of XOR operator in (a) dual basis; (b) magic basis.

page 394, Exercise 79 Show that the following operators are projections; (a) $\frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$; (b) $\frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$

page 394, Exercise 80 (Morita 2000) Design a universal reversible one-tape two symbol Turing machine producing output $0^\infty 1^n 0 1^{2n} 0^\infty$ for a given input $0^\infty 1^n 0^\infty$.

page 394, Exercise 81 Find an orthonormal basis of H_4 in which the XOR operator has diagonal form.

page 394, Exercise 82 Let C be a quantum circuit with n input and output qubits and a single gate acting on ith and jth qubits and represented by a unitary matrix A of degree 4. Describe the output of the circuit if applied to a basis state $|x\rangle$ of H_{2^n}.

page 394, Exercise 83 Show that by chossing a proper basis each qubit state can be written in the form: (a) $\cos\alpha|0\rangle + \sin\alpha|1\rangle$; (b) $\sqrt{\frac{k}{n}}|0\rangle + \sqrt{\frac{n-k}{n}}|1\rangle$.

page 394, Exercise 84 Let us call a quantum state symmetric if it is not changed under permutation of qubits. The set of symmetric states of each Hilbert space H_{2^n} spans a subspace.(a) Determine dimension of this subspace for H_{2^n}; (b) Find a basis for this subspace.

page 394, Exercise 85 Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two bases of H_4. Design a quantum circuit containing only unitary gates and controlled unitary gates that transform basis $\mathcal{B}_1$ into $\mathcal{B}_2$.

page 394, Exercise 86 Design a quantum circuit to realize the mapping

$$\sum_{x\in\{0,1\}^n} |x\rangle|0\rangle \to \sum_{x\in\{0,1\}^n} |x\rangle|H(x)\rangle,$$

where $H(x)$ is the Hamming weight of the string x.

page 394, Exercise 87 Depict the following matrices where I_j denotes unitary matrix of degree j: (a) XOR$\otimes I_2$; (b) $I_2\otimes$ XOR; (c) $H\otimes I_4$.

page 394, Exercise 88 Determine a necessary and sufficient condition, in terms of subspaces, for two projection operators of a Hilbert space to commute.

page 394, Exercise 89 Determine the matrix form of the projection operator in $\mathbf{R}_2$ onto the line at an angle θ to the x-axis.

page 394, Exercise 90 Determine in H_2 the projection operators that make projection into the subspace spanned by the vectors: (a) $(1, 1+i)$; (b) $(1-i, -1)$.

page 394, Exercise 91 Show that $e^{i\tau A} = \cos\tau I + i\sin\tau A$ for (a) $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$; (b) $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

page 394, Exercise 92 Can it be the case that the same density matrix corresponds to two different pure states?

CHAPTER 9 — BIBLIOGRAPHICAL COMMENTS

page 398, line +18 the first quantum cryptography apparatus was build mainly by Ch. Bennett and John Smolin.

page 398, a new paragraph after the second one Ch. Bennett holds also the first patents in quantum information processing (cryptography) from 1994. United States Patents Number 5307410 (Interferometric quantum cryptographic key distribution system) and 5515438 (with S. Wiesner — Quantum key distribution using nonorthogonal macroscopic signals). Both patents expire in 2013.

References

[1] Technical report.

[2] Andris Ambainis, Richard Bonner, Rusins Freivalds, Marats Golovkins, and Marek Karpinski. Quantum finite multitape automata vs. probabilistic finite automata. Technical report, quant-ph/9905026, 1999.

[3] Andris Ambainis, Arnolds Kikusts, and Maris Valdats. On the class of languages recognizable by 1-way quantum finite automata. Technical report, quant-ph/0009004, 2000.

[4] Charles H. Bennett and Peter W. Shor. Quantum information theory. *IEEE Transactions on Information Theory*, 44:2724–2742, 1998.

[5] Eli Biham, Ofer Biham, David Biron, Markus Grassl, Daniel A. Lidar, and Daniel Shapira. Analysis of generalized Grover's quantum search algorithms using recursion equations. Technical report, quant-ph/0010077, 2000.

[6] Dan Boneh and Richard J. Lipton. Quantum cryptoanalysis of hidden linear functions. In *Advances in Cryptology, Proceedings of CRYPTO'95*, pages 424–437, 1995.

[7] Sugato Bose, Vlatko Vedral, and Peter L. Knight. Purification via entanglement swapping and conserved entanglement. Technical report, quant-ph/9812013, 1997.

[8] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing. Technical report, quant-ph/9900054, 1999.

[9] Dagmar Bruß, Mirko Cinchetti, G. Mauro D'Ariano, and Chiara Macchiavello. Phase covariant quantum cloning. Technical report, quant-ph/9909046, 1999.

[10] Dagmar Bruß, Lara Faoro, Chiara Macchiavello, and G. Massimi Palma. Quantum entanglement and classical communication through a depolarizing channel. Technical report, quant-ph/9903033, 1999.

[11] Dong Pyo Chi, Jinsoo Kim, and Soojoon Lee. Quantum algorithm for generalized Deutsch-Jozsa problem. Technical report, quant-ph/0005059, 2000.

[12] M. Clarke, A. Chefles, S. M. Barnett, and E. Riis. Experimental demonstration of optimal unambiguous state discrimination. Technical report, quant-ph/0007063, 2000.

[13] R. Derka, Vladimír Bužek, and Arthur Ekert. Universal algorithm for optimal estimation of quantum states from finite ensembles via reiterable generalized measurement. *Physical Review Letters*, 80:1571–1575, 1998.

[14] R. Griffiths. Consistent histories and the interpretation of quantum mechanics. *Journal of Statistical physics*, 36:219–272, 1984.

[15] Lucien Hardy. Spooky action at a distance in quantum mechanics. *Contemporary physics*, 39(6):419–429, 1998.

[16] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223:1–8, 1998c. quant-ph/9605038.

[17] Pawel Horodecki, Ryszard Horodecki, and Michal Horodecki. Entanglement and thermodynamical analogies. *Acta Physica Slovaca*, 48(3):141–156, 1998b.

[18] R. I. G. Hughes. *The structure and interpretation of quantum mechanics.* Harward University Press, 1997.

[19] B. Huttner, J. D. Gautier, A. Muller, H. Zbinden, and N. Gisin. Unambiguous quantum measurement of non-orthogonal states. *Physics Review A*, 54:3783–3789, 1996.

[20] I. D. Ivanovic. How to differentiate between nonorthogonal states. *Physics Letter A*, 123:257–259, 1987.

[21] Daniel Jonathan and Martin Plenio. Entanglement-assisted local manipulation of pure quantum states. Technical report, quant-ph/9905071, 1999.

[22] Samuel J. Lomonaco Jr. A lecture on Shor's quantum factoring algorithm. Technical report, quant-ph/0010034, 2000a.

[23] Arnolds Kikusts. A small 1-way quantum finite automaton. Technical report, quant-ph/9810065, 1998.

[24] Alexei Kitaev, A Shen, and M. Vialyj. *Classical and quantum computations.* MCNMO, 1999. In Russian, ISBN 5-900916-35-9.

[25] Daniel Kleppner and Roman Jackiw. One hundred years of quantum physics. Technical report, quant-ph/0008092, 2000.

[26] Simon B. Kochen and Ernst P. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17:59–87, 1967.

[27] Karl Kraus. *States, effects and operations.* Lecture Notes in Physics 190, Springer, 1983.

[28] Seth Lloyd. Ultimate physical limits to computation. Technical report, quant-ph/9908043, 1999.

[29] Samuel J. Lomonaco. A Roseta stone for quantum mechanics with an introduction to quantum computation. Technical report, quant-ph/0007045, 2000.

[30] Günter Ludwig. *Foundations of quantum mechanics I/II*. Springer, Berlin, 1983,1985.

[31] Serge Massar and Sandu Popescu. Optimal extraction of information from finite quantum ensembles. *Physical Review Letters*, 74:1259–1265, 1995.

[32] Kurt Mehlhorn and Erik M. Schmidt. Las Vegas is better than detrminism in VLSI and distributed computing. In *Proceedings of 14th ACM STOC*, pages 330–337, 1982.

[33] David A. Meyer. Sophisticated quantum search without entanglement. Technical report, quant-ph/0007070, 2000.

[34] P. W. Milonni and M. L. Hardies. Photons cannot be always replicated. *Physics Letters A*, 92:321–322, 1982.

[35] Cristopher Moore. Quantum circuits: fanout, parity, and counting. Technical report, quant-ph/9903046, 1999.

[36] Kenichi Morita. A simple construction method of a reversible finite automaton out of Fredkin gates, and its related problems. *The Transactions of the IEICE*, E73(6):978–984, 1990.

[37] Kenichi Morita. Universality of a reversible two-counter machine. *Theoretical Computer Science*, 168:303–320, 1996.

[38] Kenichi Morita. Cellular automata and artificial life. In *Proceedings FISTA'98*, pages 1–40, 1998.

[39] Kenichi Morita and Masateru Harao. Computational universality of one-dimensional reversible (injective) cellular automata. *The Transactions of IEICE*, E72(6):758–762, 1989.

[40] Kenichi Morita and Katsunobu Imai. Self-reproduction in a reversible cellular space. *Theoretical Computer Science*, 168:337–366, 1996.

[41] Kenichi Morita, Akihiko Shirasaki, and Yoshifumi Gono. A 1-tape 2-symbol reversible Turing machine. *The Tranasactions of IEICE*, E72(3):223–228, 1989.

[42] Kenichi Morita, Yasuyuki Tojima, and Katsunobu Imai. A simple computer embedded in a reversible and number-conserving two-dimensional cellular space. *Multiple-valued logic*, ??(??):?, 2000. To appear.

[43] Kenichi Morita and Satoshi Uneo. Computation-universal models of two-dimensional 16-state reversible cellular automata. *IEICE Transaction on Information and Systems*, E75-D(1):141–147, 1992.

[44] Noam Nissan and Avi Wigderson. On rank versus communication complexity. *Combinatorica*, 15:557–565, 1995.

[45] Robert Omnés. Consistent interpretations of quantum mechanics. *Reviews of Modern Physics*, 64:339–382, 1992.

[46] Robert Omnès. *The interpretation of quantum mechanics.* Princeton University Press, 1994.

[47] Asher Peres. How to differentiate between two non-orthogonal states. *Physics Letter A*, 128:19–??, 1988.

[48] Asher Peres. Separability criterion for density matrices. *Physical Review Letters*, 77:1413–1415, 1996a.

[49] Asher Peres. Delayed choice for entanglement swapping. Technical report, quant-ph/9904042, 1999.

[50] Martin B. Plenio and Vlatko Vedral. Teleportation, entanglement, and thermodynamics in the quantum world. Technical report, quant-ph/9804075, 1998.

[51] Sandu Popescu and D. Rohrlich. ??? *Physical Review Letters*, 79:3319–, 1996.

[52] Peter Shor. Inroduction to quantum algorithms. Technical report, quant-ph/0005003, 2000.

[53] John A. Smolin. A four-party unlockable bound entangled state. Technical report, quant-ph/0000101, 2000.

[54] Amnon Ta-Shma. Classical versus quantum communication complexity. *SIGACT News*, ??(?):25–34, 1999.

[55] Robert R. Tucci. A rudimentary quantum compiler. Technical report, quant-ph/9902062, 1999.

[56] Lev Vaidman, Lev Goldenberg, and Stephen Wiesner. Error prevention scheme with four particles. *Physical Review A*, 54(3):1745–1748, 1996.

[57] G. Vidal. Entanglement monotonnes. Technical report, quant-ph/9807077, 1998.

[58] Reinhard F. Werner. Optimal clonning of pure states. *Physical Review A*, 58:1827–1831, 1998.

[59] Andrew C.-C. Yao. Security of quantum cryptography against coherent measurement. In *Proceedings of 26th ACM STOC*, pages 67–75, 1995.