LECTURE NOTES
IN PHYSICS

L. Diósi

A Short Course in Quantum Information Theory

An Approach From Theoretical Physics

Springer

Lajos Diósi

A Short Course in Quantum Information Theory

An Approach From Theoretical Physics

Springer

Author

Dr. Lajos Diósi
KFKI Research Institute for
Partical and Nuclear Physics
P.O.Box 49
1525 Budapest
Hungary
E-mail: diosi@rmki.kfki.hu

L. Diósi, *A Short Course in Quantum Information Theory*, Lect. Notes Phys. 713 (Springer, Berlin Heidelberg 2007), DOI 10.1007/b11844914

Library of Congress Control Number: 2006931893

ISSN 0075-8450
ISBN-10 3-540-38994-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-38994-1 Springer Berlin Heidelberg New York

Typesetting: by the author and techbooks using a Springer LaTeX macro package
Cover design: WMXDesign GmbH, Heidelberg

Printed on acid-free paper SPIN: 11844914 54/techbooks 5 4 3 2 1 0

Lecture Notes in Physics

The Lecture Notes in Physics

The series Lecture Notes in Physics (LNP), founded in 1969, reports new developments in physics research and teaching – quickly and informally, but with a high quality and the explicit aim to summarize and communicate current knowledge in an accessible way. Books published in this series are conceived as bridging material between advanced graduate textbooks and the forefront of research to serve the following purposes:

- to be a compact and modern up-to-date source of reference on a well-defined topic;
- to serve as an accessible introduction to the field to postgraduate students and nonspecialist researchers from related areas;
- to be a source of advanced teaching material for specialized seminars, courses and schools.

Both monographs and multi-author volumes will be considered for publication. Edited volumes should, however, consist of a very limited number of contributions only. Proceedings will not be considered for LNP.

Volumes published in LNP are disseminated both in print and in electronic formats, the electronic archive is available at springerlink.com. The series content is indexed, abstracted and referenced by many abstracting and information services, bibliographic networks, subscription agencies, library networks, and consortia.

Proposals should be sent to a member of the Editorial Board, or directly to the managing editor at Springer:

Dr. Christian Caron
Springer Heidelberg
Physics Editorial Department I
Tiergartenstrasse 17
69121 Heidelberg/Germany
christian.caron@springer.com

Preface

Quantum information has become an independent fast growing research field. There are new departments and labs all around the world, devoted to particular or even complex studies of mathematics, physics, and technology of controlling quantum degrees of freedom. The promised advantage of quantum technologies has obviously electrified the field which had been considered a bit marginal until quite recently. Before, many foundational quantum features had never been tested or used on single quantum systems but on ensembles of them. Illustrations of reduction, decay, or recurrence of quantum superposition on single states went to the pages of regular text-books, without being experimentally tested ever. Nowadays, however, a youngest generation of specialists has imbibed quantum theoretical and experimental foundations "from infancy".

From 2001 on, in spring semesters I gave special courses for under- and post-graduate physicists at Eötvös University. The twelve lectures could not include all standard chapters of quantum information. My guiding principles were those of the theoretical physicist and the believer in the unity of physics. I achieved a decent balance between the core text of quantum information and the chapters that link it to the edifice of theoretical physics. Scholarly experience of the passed five semesters will be utilized in this book.

I suggest this thin book for all physicists, mathematicians and other people interested in universal and integrating aspects of physics. The text does not require special mathematics but the elements of complex vector space and of probability theories. People with prior studies in basic quantum mechanics make the perfect readers. For those who are prepared to spend many times more hours with quantum information studies, there have been exhaustive monographs written by Preskill, by Nielsen and Chuang, or the edited one by Bouwmeester, Ekert, and Zeilinger. And for each of my readers, it is almost compulsory to find and read a second thin book "Short Course in Quantum Information, approach from experiments"...

Acknowledgements I benefited from the conversations and/or correspondence with Jürgen Audretsch, András Bodor, Todd Brun, Tova Feldmann, Tamás Geszti, Thomas Konrad, and Tamás Kiss. I am grateful to them all for the generous help and useful remarks that served to improve my manuscript.

It is a pleasure to acknowledge financial support from the Hungarian Scientific Research Fund, Grant No. 49384.

Budapest,
February 2006

Lajos Diósi

Symbols, acronyms, abbreviations

$\{\ ,\ \}$	Poisson bracket	$\circ$	composition
$[\ ,\ ]$	commutator	$\times$	Cartesian product
$\langle\ \rangle$	expectation value	$\otimes$	tensor product
$\hat{O}$	matrix	tr	trace
$\hat{O}^\dagger$	adjoint matrix	tr_A	partial trace
$\oplus$	modulo sum		

$x, y, \ldots$	phase space points	w	weight in mixture
Γ	phase space	$\|\uparrow\rangle, \|\downarrow\rangle$	spin-up, spin-down basis
$\rho(x)$	phase space distribution, classical state	$\boldsymbol{n}, \boldsymbol{m} \ldots$	Bloch unit vectors
		$\|\boldsymbol{n}\rangle$	qubit state vector
$\mathrm{x}, \mathrm{y} \ldots$	binary numbers	$\boldsymbol{s}$	qubit polarization vector
$\mathrm{x}_n \ldots \mathrm{x}_2\mathrm{x}_1$	binary string	$\hat{\sigma}_x, \hat{\sigma}_y\hat{\sigma}_z$	Pauli matrices
$\rho(\mathrm{x})$	discrete classical state	$\hat{\boldsymbol{\sigma}}$	vector of Pauli matrices
$\mathcal{M}$	operation	$\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\alpha}, \ldots$	real spatial vectors
$\mathcal{T}$	polarization reflection	$\boldsymbol{ab}$	real scalar product
$\mathcal{I}$	identity operation	$\hat{\mathrm{x}}$	qubit hermitian matrix
$\mathcal{L}$	Lindblad generator	X, Y, Z	one qubit Pauli gates
$A(x), A(\mathrm{x})$	classical physical quantities	H	Hadamard gate
$H(x)$	Hamilton function	$T(\varphi)$	phase gate
P	indicator function	F	fidelity
$\Pi(x), \Pi(\mathrm{x})$	classical effect	E	entanglement measure
$\mathcal{H}$	Hilbert space	$S(\rho), S(p)$	Shannon entropy
d	vector space dimension	$S(\hat{\rho})$	von Neumann entropy
$\|\psi\rangle, \|\varphi\rangle, \ldots$	state vectors	$S(\rho'\|\rho), S(\hat{\rho}'\|\hat{\rho})$	relative entropy
$\langle\psi\|, \langle\varphi\|, \ldots$	adjoint state vectors	$\|\Psi^\pm\rangle, \|\Phi^\pm\rangle$	Bell basis vectors
$\langle\psi\|\varphi\rangle$	complex inner product	$\|\mathrm{x}\rangle$	computational basis vector
$\langle\psi\|\hat{O}\|\varphi\rangle$	matrix element	$\hat{M}_n$	Kraus matrices
$\hat{\rho}$	density matrix, quantum state	$\|n; E\rangle$	environmental basis vector
$\hat{A}$	quantum physical quantity	$X, Y, \ldots$	classical message
$\hat{H}$	Hamiltonian	$H(X), H(Y)$	Shannon entropy
$\hat{P}$	hermitian projector	$H(X\|Y)$	conditional Shannon entropy
$\hat{I}$	unit matrix	$I(X{:}Y)$	mutual information
$\hat{U}$	unitary map	C	channel capacity
$\hat{\Pi}$	quantum effect	$\rho(\mathrm{x}\|\mathrm{y})$	conditional state
p	probability	$\rho(\mathrm{y}\|\mathrm{x})$	transfer function

q-	quantum	LO	local operation
cNOT	controlled NOT	LOCC	local operation and classical communication

Lecture Notes in Physics

For information about earlier volumes
please contact your bookseller or Springer
LNP Online archive: springerlink.com

Vol.667: W. D. Heiss (Ed.), Quantum Dots: a Doorway to Nanoscale Physics

Vol.668: H. Ocampo, S. Paycha, A. Vargas (Eds.), Geometric and Topological Methods for Quantum Field Theory

Vol.669: G. Amelino-Camelia, J. Kowalski-Glikman (Eds.), Planck Scale Effects in Astrophysics and Cosmology

Vol.670: A. Dinklage, G. Marx, T. Klinger, L. Schweikhard (Eds.), Plasma Physics

Vol.671: J.-R. Chazottes, B. Fernandez (Eds.), Dynamics of Coupled Map Lattices and of Related Spatially Extended Systems

Vol.672: R. Kh. Zeytounian, Topics in Hyposonic Flow Theory

Vol.673: C. Bona, C. Palenzula-Luque, Elements of Numerical Relativity

Vol.674: A. G. Hunt, Percolation Theory for Flow in Porous Media

Vol.675: M. Kröger, Models for Polymeric and Anisotropic Liquids

Vol.676: I. Galanakis, P. H. Dederichs (Eds.), Half-metallic Alloys

Vol.677: A. Loiseau, P. Launois, P. Petit, S. Roche, J.-P. Salvetat (Eds.), Understanding Carbon Nanotubes

Vol.678: M. Donath, W. Nolting (Eds.), Local-Moment Ferromagnets

Vol.679: A. Das, B. K. Chakrabarti (Eds.), Quantum Annealing and Related Optimization Methods

Vol.680: G. Cuniberti, G. Fagas, K. Richter (Eds.), Introducing Molecular Electronics

Vol.681: A. Llor, Statistical Hydrodynamic Models for Developed Mixing Instability Flows

Vol.682: J. Souchay (Ed.), Dynamics of Extended Celestial Bodies and Rings

Vol.683: R. Dvorak, F. Freistetter, J. Kurths (Eds.), Chaos and Stability in Planetary Systems

Vol.684: J. Dolinšek, M. Vilfan, S. Žumer (Eds.), Novel NMR and EPR Techniques

Vol.685: C. Klein, O. Richter, Ernst Equation and Riemann Surfaces

Vol.686: A. D. Yaghjian, Relativistic Dynamics of a Charged Sphere

Vol.687: J. W. LaBelle, R. A. Treumann (Eds.), Geospace Electromagnetic Waves and Radiation

Vol.688: M. C. Miguel, J. M. Rubi (Eds.), Jamming, Yielding, and Irreversible Deformation in Condensed Matter

Vol.689: W. Pötz, J. Fabian, U. Hohenester (Eds.), Quantum Coherence

Vol.690: J. Asch, A. Joye (Eds.), Mathematical Physics of Quantum Mechanics

Vol.691: S. S. Abdullaev, Construction of Mappings for Hamiltonian Systems and Their Applications

Vol.692: J. Frauendiener, D. J. W. Giulini, V. Perlick (Eds.), Analytical and Numerical Approaches to Mathematical Relativity

Vol.693: D. Alloin, R. Johnson, P. Lira (Eds.), Physics of Active Galactic Nuclei at all Scales

Vol.694: H. Schwoerer, J. Magill, B. Beleites (Eds.), Lasers and Nuclei

Vol.695: J. Dereziński, H. Siedentop (Eds.), Large Coulomb Systems

Vol.696: K.-S. Choi, J. E. Kim, Quarks and Leptons From Orbifolded Superstring

Vol.697: E. Beaurepaire, H. Bulou, F. Scheurer, J.-P. Kappler (Eds.), Magnetism: A Synchrotron Radiation Approach

Vol.698: S. Bellucci (Ed.), Supersymmetric Mechanics – Vol. 1

Vol.699: J.-P. Rozelot (Ed.), Solar and Heliospheric Origins of Space Weather Phenomena

Vol.700: J. Al-Khalili, E. Roeckl (Eds.), The Euroschool Lectures on Physics with Exotic Beams, Vol. II

Vol.701: S. Bellucci, S. Ferrara, A. Marrani, Supersymmetric Mechanics – Vol. 2

Vol.702: J. Ehlers, C. Lämmerzahl, Special Relativity

Vol.703: M. Ferrario, G. Ciccotti, K. Binder (Eds.), Computer Simulations in Condensed Matter Systems: From Materials to Chemical Biology Volume 1

Vol.704: M. Ferrario, G. Ciccotti, K. Binder (Eds.), Computer Simulations in Condensed Matter Systems: From Materials to Chemical Biology Volume 2

Vol.705: P. Bhattacharyya, B.K. Chakrabarti (Eds.), Modelling Critical and Catastrophic Phenomena in Geoscience

Vol.706: M.A.L. Marques, C.A. Ullrich, F. Nogueira, A. Rubio, K. Burke, E.K.U. Gross (Eds.), Time-Dependent Density Functional Theory

Vol.707: A.V. Shchepetilov, Calculus and Mechanics on Two-Point Homogenous Riemannian Spaces

Vol.708: F. Iachello, Lie Algebras and Applications

Vol.709: H.-J. Borchers and R.N. Sen, Mathematical Implications of Einstein-Weyl Causality

Vol.710: K. Hutter, A.A.F. van de Ven, A. Ursescu, Electromagnetic Field Matter Interactions in Thermoelastic Solids and Viscous Fluids

Vol.711: H. Linke, Controlled Nanoscale Motion in Biological and Artifical Systems

Vol.712: W. Pötz, J. Fabian, U. Hohenester (Eds.), Modern Aspects of Spin Physics

Vol.713: L. Diósi, A Short Course in Quantum Information Theory

Contents

1 Introduction

Classical physics — the contrary to quantum — means all those fundamental dynamical phenomena and their theories which became known until the end of the 19th century, from our studying the macroscopic world. Galileo's, Newton's, and Maxwell's consecutive achievements, built one on the top of the other, obtained their most compact formulation in terms of the classical canonical dynamics. At the same time, the conjecture of the atomic structure of the microworld was also conceived. By extending the classical dynamics to atomic degrees of freedom, certain microscopic phenomena also appearing at the macroscopic level could be explained correctly. This yielded indirect, yet sufficient, proof of the atomic structure. But other phenomena of the microworld (e.g., the spectral lines of atoms) resisted to the natural extension of the classical theory to the microscopic degrees of freedom. After Planck, Einstein, Bohr, and Sommerfeld, there had formed a simple constrained version of the classical theory. The naively *quantized* classical dynamics was already able to describe the non-continuous (discrete) spectrum of stationary states of the microscopic degrees of freedom. But the detailed dynamics of the transitions between the stationary states was not contained in this theory. Nonetheless, the successes (e.g., the description of spectral lines) shaped already the *dichotomous* physics world concept: the microscopic degrees of freedom obey to other laws than macroscopic ones do. After the achievements of Schrödinger, Heisenberg, Born, and Jordan, the *quantum theory* emerged to give the complete description of the microscopic degrees of freedom in perfect agreement with experience. This quantum theory was not a mere quantized version of the classical theory anymore. Rather it was a totally new formalism of completely different structure than the classical theory, which was applied professedly to the microscopic degrees of freedom. As for the macroscopic degrees of freedom, one continued to insist on the classical theory.

For a sugar cube, the center of mass motion is a macroscopic degree of freedom. For an atom, it is microscopic. We must apply the classical theory to the sugar cube, and the quantum theory to the atom. Yet, there is no sharp boundary of where we must switch from one theory to the other. It is, furthermore, obvious that the center of mass motion of the sugar cube should be derivable from the center of mass motions of its atomic constituents. Hence a specific inter-dependence exists between the classical and the quantum theories, which must give consistent resolution for the above dichotomy. The von Neumann "axiomatic" formulation of the quantum theory represents, in the framework of the dichotomous physics world concept, a

Lajos Diósi: *A Short Course in Quantum Information Theory*, Lect. Notes Phys. **713**, 1–3 (2007)
DOI 10.1007/3-540-38996-2_1

description of the microworld maintaining the perfect harmony with the classical theory of the macroworld.

Let us digress about a natural alternative to the dichotomous concept. According to it, all macroscopic phenomena can be reduced to a multitude of microscopic ones. Thus in this way the basic physical theory of the universe would be the quantum theory, and the classical dynamics of macroscopic phenomena should be deducible from it, as limiting case. But the current quantum theory is not capable of holding its own. It refers to genuine macroscopic systems as well, thus requiring classical physics as well. Despite of the theoretical efforts in the second half of 20th century, there has not so far been consensus regarding the (universal) quantum theory which would in itself be valid for the whole physical world.

This is why we keep the present course of lectures within the framework of the dichotomous world concept. The "axiomatic" quantum theory of von Neumann will be used. Among the bizarre structures and features of this theory, discreteness (quantumness) was the earliest, and the theory also drew its name from it. Yet another odd prediction of quantum theory is the inherent randomness of the microworld. During the decades, further surprising features have come to light. It has become "fashion" to deduce paradoxical properties of quantum theory. There is a particular range of paradoxical predictions (Einstein-Podolski-Rosen, Bell) which exploits such correlations between separate quantum systems which could never exist classically. Another cardinal paradox is the non-clonability of quantum states, meaning the fidelity of possible copies will be limited fundamentally and strongly.

The initial role of the paradoxes was better knowledge of quantum theory. We learned the *differenciae specificae* of the quantum systems with respect to the classical ones. The consequences of the primarily paradoxical quantumness are understood relatively well and also their advantage is appreciated with respect to classical physics (see, e.g., semiconductors, superconductivity, superfluidity). By the end of the 20th century the paradoxes related to *quantum-correlations* have come to the front. We started to discover their advantage only in the past decade. The keyword is: *information*! Quantum correlations, consequent upon quantum theory, would largely extend the options of classical information manipulation including information storage, coding, transmitting, hiding, protecting, evaluating, as well as algorithms, game strategies. All these represent the field of quantum information theory in a wider sense. Our short course covers the basic components only, at the introductory level.

Chapters 2–4 summarize the classical, the semiclassical, and the quantum physics. The two Chaps. 2 and 4 look almost like mirror images of each other. I intended to exploit the maximum of existing parallelism between the classical and quantum theories, and to isolate only the essential differences in the present context. Chapter 5 introduces the text-book theory of abstract two-state quantum systems. Chapter 6 discusses their quantum informatic manipulations and presents two applications: copy-protection of banknotes and of cryptographic keys. Chapter 7 is devoted to composite quantum systems and quantum correlations (also called entanglement). An insight into three theoretical antecedents is discussed, finally I show

two quantum informatic applications: superdense coding and teleportation. Chapter 8 introduces us to the modern theory of quantum operations. The first parts of Chaps. 9 and 10 are anew mirror images of each other. The foundations of classical and quantum information theories, based respectively on the Shannon and von Neumann entropies, can be displayed in parallel terms. This holds for the classical and quantum theories of data compression as well. There is, however, a separate section in Chap. 10 to deal with the entanglement as a resource, and with its conversions which all make sense only in quantum context. Chapter 11 offers simple introduction into the quintessence of quantum information which is quantum algorithms. I present the concepts that lead to the idea of the quantum computer. Two quantum algorithms will close the Chapter: solution of the oracle and of the searching problems. A short section of divers Problems and Exercises follow each Chapter. This can, to some extent, compensate the reader for the laconic style of the main text. A few number of missing or short-spoken proofs and arguments find themselves as Problems and Exercises. That gives a hint how the knowledge, comprised into the economic main text, could be derived and applied.

For further reading, we suggest the monograph [1] by Nielsen and Chuang which is the basic reference work for the time being, together with [2] by Preskill and [3] edited by Bouwmeester, Ekert and Zeilinger. Certain statements or methods, e.g. in Chaps. 10 and 11, follow [1] or [2] and can be checked from there directly. Our bibliography continues with textbooks [4]–[10] on the traditional fields, like e.g. the classical and quantum physics, which are necessary for the quantum information studies. References to two useful reviews on q-cryptography [11] and on q-computation are also included [12]. The rest of the bibliography consists of a very modest selection of the related original publications.

2 Foundations of classical physics

We choose the classical canonical theory of Liouville because of the best match with the q-theory — a genuine statistical theory. Also this is why we devote the particular Sect. 2.4 to the measurement of the physical quantities. Hence the elements of the present Chapter will most faithfully reappear in Chap. 4 on Foundations of q-physics. Let us observe the similarities and the differences!

2.1 State space

The state space of a system with n degrees of freedom is the phase space:

$$\Gamma = \{(q_k, p_k); k = 1, 2, \ldots, n\} \equiv \{x_k; k = 1, 2, \ldots, n\} \equiv \{x\} \ , \tag{2.1}$$

where q_k, p_k are the canonically conjugate coordinates of each degree of freedom in turn. The *pure* state of an individual system is described by the phase point $\bar{x}$. The generic state state is *mixed*, described by normalized distribution function:

$$\rho \equiv \rho(x) \geq 0, \quad \int \rho \mathrm{d}x = 1 \ . \tag{2.2}$$

The generic state is interpreted on the statistical ensemble of identical systems. The distribution function of a pure state reads:

$$\rho_{\mathrm{pure}}(x) = \delta(x - \bar{x}) \ . \tag{2.3}$$

2.2 Mixing, selection, operation

Random mixing the elements of two ensembles of states ρ_1 and ρ_2 at respective rates $w_1 \geq 0$ and $w_2 \geq 0$ yields the new ensemble of state:

$$\rho = w_1\rho_1 + w_2\rho_2; \quad w_1 + w_2 = 1 \ . \tag{2.4}$$

A generic mixed state can always be prepared (i.e. decomposed) as the mixture of two or more other mixed states in infinite many different ways. After mixing, however, it is totally impossible to distinguish which way the mixed state was prepared.

Lajos Diósi: *A Short Course in Quantum Information Theory*, Lect. Notes Phys. **713**, 5–13 (2007)
DOI 10.1007/3-540-38996-2_2