



©Jens Eisert

# Quantum Information

martin wilkens

These are lecture notes for my courses on quantum information. The notes are being developed as we proceed. They are posted (and removed) somewhere in the directory “Teaching” on <http://www.quantum.physik.uni-potsdam.de>



The notes are neither complete nor original. They are full of mistakes, misprints and misconceptions. Their mere purpose is to remind me of what should be improved for the next course . . .

In preparing the notes I found the following material useful

- Preskill lecture notes “Quantum Information and Computation”  
<http://www.theory.caltech.edu/people/preski11/ph219/>.
- Mackay lecture notes “Information theory, inference, and learning algorithm”  
<http://wol.ra.phy.cam.ac.uk/mackay/itprnm/book.html>
- Werner lecture notes “Quantum Information and Quantum Computing”  
<http://www.imaph.tu-bs.de/qi>.

Recommended reading for *quantum information theory*:

- *Quantum Computation and Quantum Information* by Michael A. Nielsen and Isaac L. Chuang, Cambridge University Press 2000 [ISBN 0 521 63503 9]. With 650 pages(!) truly an in-depth treatment of the subject. Comparable to J.D. Jackson “Classical Electrodynamics”, the book is likely to become *the* reference for the next couple of years.

Recommended reading for *classical information theory*:

- *Codes and Cryptography* by Dominic Welsh, Oxford Science Publications, Oxford University Press 1988 [ISBN 0 19 853287 3].

Recommended reading for *Quantum mechanics*

- *Quantum Theory: Concepts and Methods* by Asher Peres, Kluwer Academic Pub. 1995 [ISBN 0-7923-2549-4 (HB), -3632-1 (PB)]

Recommended reading for *fun*:

- *The Emperor's New Mind* by Roger Penrose, Oxford University Press 1989; reprint in Vintage Books, Random House, London 1990 [ISBN 0 09 977170 5]. A marvel on computers, minds and the laws of physics. Recommended source for easy-to-read material on Turing machines, Gödel's incompleteness theorem, and its relation to physics in general and quantum mechanics in particular.

Further references will be given as the course proceeds ... just to start with one: *Information* is a many-facet notion with an interesting history of meaning and use from the old greeks to our times. A fair amount of references and even some own investigations may be found in the dissertation thesis

- *Quantentheorie der Information* by Holger Lyre, Springer 1998 [ISBN 3-211-83204-1].

The subtitle *Zur Naturphilosophie der Theorie der Ur-Alternativen und einer abstrakten Theorie der Information. Mit einem Geleitwort von Carl Friedrich von Weizsäcker* indicates what it is: a philosophically inclined reconstruction of a notion of information in the framework of a certain Neu-Kantian programme which was originally initiated by C.F. von Weizsäcker. The “Ur-Alternative” is what we call qubit these days. The Weizsäcker programme on the *Aufbau der Physik* could not really revive the natural philosophy – yet Lyres’ thesis is still a valuable piece of work.



# Contents

<b>1</b>	<b>Information and Quantum Information</b>	<b>13</b>
1.1	Information is not a thing . . . . .	13
1.2	Information is physical . . . . .	16
1.3	Complement: Probability in a nutshell . . . . .	18
1.4	Complement: Physics and Probability . . . . .	21
<b>2</b>	<b>A little bit of information theory</b>	<b>29</b>
2.1	Hartley's postulate . . . . .	29
2.2	Shannon Entropy . . . . .	31
2.3	Relative entropy . . . . .	36
2.4	Complement: Convex analysis – the basics . . . . .	37
<b>3</b>	<b>Source coding</b>	<b>39</b>
3.1	Significance of Shannon Entropy . . . . .	39

3.2	Shannon source coding theorem . . . . .	40
3.3	Huffman coding algorithm . . . . .	44
3.4	Supplement: Codes – an overview . . . . .	46
3.4.1	Symbol codes . . . . .	47
3.4.2	Block codes . . . . .	48
3.4.3	Errors and Decoding rules . . . . .	48
3.4.4	Linear Codes . . . . .	49
<b>4</b>	<b>Channel Coding</b>	<b>51</b>
4.1	The discrete memoryless channel . . . . .	51
4.2	Mutual Information . . . . .	52
4.3	Channel Capacity, Rates and Errors . . . . .	56
4.4	Channel coding theorem . . . . .	58
<b>5</b>	<b>Quantum vs Classical Information</b>	<b>61</b>
5.1	The qubit . . . . .	61
5.2	The power of linear superposition . . . . .	63
5.3	The benefit of the impossible . . . . .	65
5.4	The novel type of information . . . . .	66
<b>6</b>	<b>Preparation and Measurement</b>	<b>69</b>
6.1	Pauli operators . . . . .	70

---

6.2 Stern-Gerlach magnet . . . . .	71
<b>7 Qubit codes and cryptography</b>	<b>75</b>
7.1 Qubit codes . . . . .	75
7.2 Quantum Cryptography . . . . .	76
7.3 Quantum public key distribution (BB84-protocol) . . . . .	78
7.4 B92 protocol . . . . .	80
<b>8 Qubit manipulation and control</b>	<b>81</b>
8.1 Qubit Schrödinger equation . . . . .	81
8.2 Single qubit gates . . . . .	83
<b>9 Composite Systems</b>	<b>85</b>
9.1 Hilbert space of a composite system . . . . .	85
9.2 Schmidt decomposition . . . . .	87
9.3 Bases for two qubits . . . . .	88
9.4 Operators for two qubits . . . . .	89
9.5 Entanglement and Correlations . . . . .	90
<b>10 EPR Paradox and Bell inequalities</b>	<b>91</b>
10.1 The facts . . . . .	92
10.2 The Paradox . . . . .	92

10.3 Bohr response . . . . .	94
10.4 Bell theorem . . . . .	94
10.5 The solution of the paradox . . . . .	96
<b>11 The power of entanglement</b>	<b>99</b>
11.1 Quantum dense coding . . . . .	99
11.2 Quantum teleportation . . . . .	101
11.3 Quantum public key distribution (E91 protocol) . . . . .	103
11.4 No Cloning Theorem . . . . .	104
11.5 Yes Cloning Theorem . . . . .	105
<b>12 Entanglement is the rule</b>	<b>107</b>
12.1 Entanglement and measurement . . . . .	108
<b>13 States and channels</b>	<b>113</b>
13.1 The qubit state operator . . . . .	113
13.2 States of composite systems . . . . .	118
13.3 Preparation and Measurement revisited . . . . .	119
13.4 Qubit Liouville-von Neumann equation . . . . .	121
13.5 Channels . . . . .	123
<b>14 Entropy and information</b>	<b>127</b>



---

14.1	State estimation . . . . .	129
14.2	Information gain . . . . .	131
14.3	Entropy and measure of entanglement . . . . .	136
14.4	Measure of Non-Separability . . . . .	137
<b>15</b>	<b>Models of Computation</b>	<b>139</b>
15.1	The Turing machine . . . . .	142
15.2	The circuit model . . . . .	144
15.2.1	Elementary gates . . . . .	145
15.2.2	Reversible gates . . . . .	146
15.3	Complexity . . . . .	148
15.4	Energy of computation . . . . .	149
15.5	DNA Computing . . . . .	151
<b>16</b>	<b>Quantum Computer</b>	<b>153</b>
16.1	Single qubit gates . . . . .	153
16.2	Two-qubit gates . . . . .	154
16.3	Quantum circuit . . . . .	156
<b>17</b>	<b>Quantum Algorithm</b>	<b>159</b>
17.1	The Deutsch algorithm . . . . .	159
17.2	Shor's factoring algorithm . . . . .	161

17.3	Quantum discrete Fourier transform . . . . .	165
17.4	Grover Algorithm . . . . .	167
<b>18 Doing it</b>		
18.1	The Cirac-Zoller ion trap computer . . . . .	169
18.2	NMR computer . . . . .	169
<b>19 Fighting errors</b>		
19.1	Sources of errors . . . . .	171
19.2	Error-correction schemes . . . . .	171
<b>A Probabilities – the basics</b>		
A.1	Ensembles and such . . . . .	173
A.2	Observables and Measurement . . . . .	176
A.3	Composite ensembles . . . . .	180
A.4	Convex analysis – the basics . . . . .	181
A.5	Entropies . . . . .	182
<b>B Codes – an overview</b>		
B.1	Symbol codes . . . . .	186
B.2	Block codes . . . . .	187
B.3	Errors and Decoding rules . . . . .	187

---

B.4	Linear Codes . . . . .	189
<b>C Quantum mechanics</b>		
C.1	Quantum mechanics punch lines . . . . .	191
C.2	Hilbert space and vectors . . . . .	193
C.3	Operators . . . . .	194
C.4	Qubit specifics I . . . . .	196
C.5	Composite Systems . . . . .	197
C.6	Qubit specifics II . . . . .	199
<b>D Quantum Statistics</b>		
D.1	States . . . . .	201
D.2	Entropies and Monotones . . . . .	203
D.3	Measurement . . . . .	205
D.4	Maps and channels . . . . .	206
<b>E Elements of number theory</b>		
E.1	Divisibility . . . . .	209
E.2	Arithmetics $+$ , $-$ , $\times$ and $\div$ is easy . . . . .	210
E.3	GCD and Euclid's Algorithm . . . . .	211
E.4	Congruences . . . . .	214
E.5	Chinese Remainder Theorem . . . . .	216

E.6 Factorization and order finding . . . . .	216
<b>F Mathematical concepts</b>	<b>219</b>
F.1 A little bit of number theory . . . . .	222