

Introduction to
Quantum Information Processing

—
Draft

Technical University of Clausthal
SS 2001 – SS 2005

W. Lücke

Preface

Quantum information processing is one of the most fascinating and active fields of contemporary physics. Its central topic is the coherent control of quantum states in order to perform tasks — like quantum teleportation, absolutely secure data transmission and efficient factorization of large integers — that do not seem possible by means of classical systems alone. The vast possibilities of physical implementations are currently being extensively studied and evaluated. Various proof-of-principle experiments have already been performed. However, in the present note only some possibilities can be indicated. Main emphasis will be on quantum optical methods, indispensable for transmission of quantum information.

For more complete information on achievements and latest proposals concerning quantum information processing the Los Alamos preprint server

<http://xxx.lanl.gov/archive/quant-ph>

is highly recommended.

Recommended Literature: (Alber et al., 2001; Bowmeester et al., 2000; Ekert et al., 2000; Nielsen and Chuang, 2001; Preskill, 01; Shannon, 1949; Bertlmann and Zeilinger, 2002; Audretsch, 2002; Bruß, 2003)

Contents

I	Idealized Quantum Gates and Algorithms	9
1	Basics of Quantum Computation	11
1.1	Classical Logic Circuits	11
1.2	Quantum Computational Networks	17
1.2.1	Quantum Gates	17
1.2.2	Quantum Teleportation	24
1.2.3	Universality	27
2	Quantum Algorithms	35
2.1	Quantum Data Base Search	35
2.1.1	GROVER's Algorithm	35
2.1.2	Network for GROVER's Algorithm	37
2.1.3	Details and Generalization	38
2.2	Factoring Large Integers	39
2.2.1	Basics	39
2.2.2	The Quantum FOURIER Transform	43
2.2.3	Quantum Order Finding	46
3	Physical Realizations of Quantum Gates	53
3.1	Quantum Optical Implementation	53
3.1.1	Photons	54
3.1.2	Photonic n-Qubit Systems	56
3.1.3	Nonlinear Optics Quantum Gates	60
3.1.4	Linear Optics Quantum Gates	62
3.2	Measurement-Based Quantum Computation	70
3.3	Cold Trapped Ions	73
3.3.1	General Considerations	74
3.3.2	Linear Paul Trap	75
3.3.3	Implementing Quantum Gates by Laser Pulses	81
3.3.4	Laser Cooling	90

II	Fault Tolerant Quantum Information Processing	91
4	General Aspects of Quantum Information	93
4.1	Introduction	93
4.2	Quantum Channels	95
4.2.1	Open Quantum Systems and Quantum Operations	95
4.2.2	Quantum Noise and Error Correction	103
4.3	Error Correcting Codes	105
4.3.1	General Aspects	105
4.3.2	Classical Codes	110
4.3.3	Quantum Codes	112
4.3.4	Reliable Quantum Computation	118
4.4	Entanglement Assisted Channels	122
4.4.1	Quantum Dense Coding	122
4.4.2	Quantum Teleportation	123
4.4.3	Entanglement Swapping	125
4.4.4	Quantum Cryptography	126
5	Quantifying Quantum Information	129
5.1	Shannon Theory for Pedestrians	129
5.2	Adaption to Quantum Communication	133
5.2.1	Von Neumann Entropy	133
5.2.2	Accessible Information	137
5.2.3	Distance Measures for Quantum States	139
5.2.4	Schumacher Encoding	145
5.2.5	A la Nielsen/Chuang	147
5.2.6	Entropy	147
6	Handling Entanglement	149
6.1	Detecting Entanglement	149
6.1.1	Entanglement Witnesses	149
6.1.2	Examples	152
6.1.3	Other Criteria	155
6.2	Local Operations and Classical Communication	158
6.2.1	General Aspects	158
6.2.2	Entanglement Dilution	164
6.2.3	Entanglement Distillation	164
6.3	Quantification of Entanglement	164
A		167
A.1	Turing's Halting Problem	167
A.2	Some Remarks on Quantum Teleportation	168
A.3	Quantum Phase Estimation and Order Finding	169
A.4	Finite-Dimensional Quantum Kinematics	173
A.4.1	General Description	173

CONTENTS

7

A.4.2 Qubits 177
A.4.3 Bipartite Systems 178

Bibliography 185

Index 202

Part I

**Idealized Quantum Gates and
Algorithms**

Chapter 1

Basics of Quantum Computation

1.1 Classical Logic Circuits

The smallest entity of classical information theory (Shannon, 1949) is the *bit* (binary digit), i.e. the decision on a classical binary alternative. Usually bits are identified with the numbers 0 (for *wrong*) or 1 (for *true*) and typically correspond to the position of some simple switch. Every definite statement may be encoded into a sufficiently long but finite sequence (b_1, \dots, b_n) of bits.¹ In this sense the essence of a calculations may be described as the transformations of a finite sequence of input bits (encoding the task) into a finite sequence of output bits (encoding the result). This suggests the following model for actual calculators:

1. An input register (array of switches) will be put into a state corresponding to the n_1 -tuple $(b_1, \dots, b_{n_1}) \in \{0, 1\}^{n_1}$ encoding the task.
2. A computational circuit, the elementary components of which are called *gates*,² transforms (b_1, \dots, b_{n_1}) into an n_2 -tuple (b'_1, \dots, b'_{n_2}) of bits encoding the result to be stored into an output register.

From the mathematical point of view it is only important which element of \mathcal{F}_{n_1, n_2} , denoting the set of all mappings from $\{0, 1\}^{n_1}$ into $\{0, 1\}^{n_2}$, is implemented by the circuit. Therefore, computational circuits implementing the same mapping are called *equivalent*.

Every element of \mathcal{F}_{n_1, n_2} can be implemented by some assembly of gates listed in Table 1.1:

DRAFT, June 26, 2009

¹An important consequence of this fact is the *halting problem* (see Appendix A.1).

²For simple hardware implementations see (Pütz, 1971, pp. 244–252).

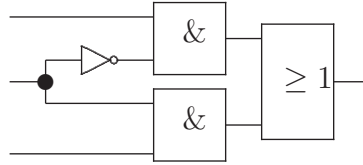
Name	Symbol	Class	Action
ID		$\mathcal{F}_{1,1}$	$b \mapsto b$
FANOUT		$\mathcal{F}_{1,2}$	$b \mapsto (b, b)$
NOT		$\mathcal{F}_{1,1}$	$b \mapsto 1 - b$
AND		$\mathcal{F}_{2,1}$	$(b_1, b_2) \mapsto b_1 b_2$
OR		$\mathcal{F}_{2,1}$	$(b_1, b_2) \mapsto b_1 + b_2 - b_1 b_2$

Table 1.1: Elementary gates

Lemma 1.1.1 For arbitrary positive integer n_1, n_2 all elements of \mathcal{F}_{n_1, n_2} can be represented as compositions of tensor products of functions from Tabular 1.1.

Proof: See below. ■

Thus every classical logic circuit corresponds to a graph consisting of symbols from Tabular 1.1. For instance, the graph



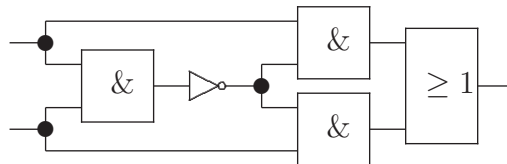
corresponds to the mapping

$$\text{SWITCH} \stackrel{\text{def}}{=} \text{OR} \circ (\text{AND} \otimes \text{AND}) \circ (\text{IDNOT} \otimes \otimes \text{ID} \otimes \text{ID}) \circ (\text{ID} \otimes \text{FANOUT} \otimes \text{ID}),$$

acting as

$$(b_0, s, b_1) \mapsto \begin{cases} b_0 & \text{if } s = 0, \\ b_1 & \text{if } s = 1. \end{cases}$$

Another example is the graph



corresponding to

$$\begin{aligned} \text{XOR} \stackrel{\text{def}}{=} & \text{OR} \circ (\text{AND} \otimes \text{AND}) \circ (\text{ID} \otimes \text{FANOUT} \otimes \text{ID}) \\ & \circ (\text{ID} \otimes (\text{NOT} \circ \text{AND}) \otimes \text{ID}) \circ (\text{FANOUT} \otimes \text{FANOUT}) \end{aligned}$$




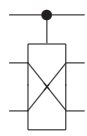
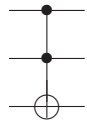
Name	Symbol	Class	Action
CNOT		$\mathcal{F}_{2,2}$	$(b_1, b_2) \mapsto (b_1, b_1 \oplus b_2)$
TCNOT		$\mathcal{F}_{2,2}$	$(b_1, b_2) \mapsto (b_1 \oplus b_2, b_2)$
SWAP		$\mathcal{F}_{2,2}$	$(b_1, b_2) \mapsto (b_2, b_1)$
CSWAP ³		$\mathcal{F}_{3,3}$	$(0, b_1, b_2) \mapsto (0, b_1, b_2)$ $(1, b_1, b_2) \mapsto (1, b_2, b_1)$
CCNOT ⁴		$\mathcal{F}_{3,3}$	$(b_1, b_2, b_3) \mapsto (b_1, b_2, b_1 b_2 \oplus b_3)$

Table 1.2: Some reversible gates

and acting as

$$\begin{aligned}
 (b_1, b_2) \mapsto b_1 \oplus b_2 &\stackrel{\text{def}}{=} \begin{cases} \text{NOT}(b_2) & \text{if } b_1 = 1 \\ b_2 & \text{if } b_1 = 0 \end{cases} \\
 &= b_1 + b_2 - 2b_1 b_2 \\
 &= b_1 + b_2 \pmod{2}.
 \end{aligned}$$

Of course, also for the gates listed in Table 1.2 there are equivalent networks, e.g.:⁵

$$\text{CNOT} = (\text{ID} \otimes \text{XOR}) \circ (\text{FANOUT} \otimes \text{ID}), \quad (1.1)$$

DRAFT, June 26, 2009

³The CSWAP gate is also called FREDKIN *gate*.

⁴The CCNOT gate is also called TOFFOLI *gate*.

⁵See (Tucci, 2004) for more equivalences of classical and/or quantum networks.

Diagram (1.2) shows a CNOT gate (control on top, target on bottom) is equivalent to a SWAP gate (two crossing lines) with a Hadamard gate (circle with a plus sign) on the target qubit.

$$\text{CNOT} \equiv \text{SWAP} \circ \text{Hadamard}_{\text{target}}, \quad (1.2)$$

Diagram (1.3) shows a SWAP gate is equivalent to two CNOT gates: one with control on the top qubit and target on the bottom qubit, followed by one with control on the bottom qubit and target on the top qubit.

$$\text{SWAP} \equiv \text{CNOT}_{\text{top} \rightarrow \text{bottom}} \circ \text{CNOT}_{\text{bottom} \rightarrow \text{top}}. \quad (1.3)$$

Diagram (1.4) shows a SWAP gate is equivalent to two CNOT gates with Hadamard gates on the target qubits: one with control on the top qubit and target on the bottom qubit, followed by one with control on the bottom qubit and target on the top qubit.

$$\text{SWAP} \equiv \text{CNOT}_{\text{top} \rightarrow \text{bottom}} \circ \text{Hadamard}_{\text{target}} \circ \text{CNOT}_{\text{bottom} \rightarrow \text{top}} \circ \text{Hadamard}_{\text{target}}. \quad (1.4)$$

Now we are prepared for the

Proof of Lemma 1.1.1: Thanks to FANOUT and SWAP it is sufficient to prove the lemma for *decision functions*, i.e. for $n_2 = 1$. Obviously, then, the statement of the lemma holds for $n_1 = 1$, since the four elements of $\mathcal{F}_{1,1}$ are ID,

$$\text{TRUE} \stackrel{\text{def}}{=} \text{OR} \circ (\text{ID} \otimes \text{NOT}) \circ \text{FANOUT},$$

and their compositions with NOT (applied last). Now, assume that the statement of the lemma has already been proved for $n_1 = n$ and consider an arbitrary $f \in \mathcal{F}_{n+1,1}$. Then both f_0 and f_1 , where

$$f_s(b_1, \dots, b_n) \stackrel{\text{def}}{=} f(b_1, \dots, b_n, s),$$

can be represented as compositions of tensor products of functions from Tabular 1.1. There is a composition of FANOUTs and SWAPs acting as

$$(b_1, \dots, b_n, s) \mapsto (b_1, \dots, b_n, s, b_1, \dots, b_n).$$

Composing this with

$$\text{SWITCH} \circ (f_0 \otimes \text{ID} \otimes f_1)$$

(to be applied last) gives f . This proves the statement of the lemma for $n_1 = n + 1$. ■

According to Lemma 1.1.1 we may perform arbitrarily complex computations by composing simple hardware components of very small variety. Of course, given $f \in \mathcal{F}_{n_1, n_2}$, there are infinitely many representations of f as composition of tensor products of elementary components. Therefore, the interesting problem arises how to simplify a given gate (*logic circuit*) without changing its action.⁶

From the technological point of view it is also of interest that

$$\text{NAND} \stackrel{\text{def}}{=} \text{NOT} \circ \text{AND}$$

———— DRAFT, June 26, 2009 ————

⁶See (Lindner et al., 1999, Sect. 8.2.3) for $n_1 \leq 6$, $n_2 = 1$ and (Lee et al., 1999; Shende et al., 2003) for quantum gates.

is **universal** in the sense that it can replace NOT, AND, and OR as elementary gates:⁷

$$\begin{aligned}\text{NOT} &= \text{NAND} \circ \text{FANOUT}, \\ \text{AND} &= \text{NOT} \circ \text{NAND}, \\ \text{OR} &= \text{NAND} \circ (\text{NOT} \otimes \text{NOT}).\end{aligned}$$

In the same sense

$$\text{NOR} \stackrel{\text{def}}{=} \text{NOT} \circ \text{OR}$$

is universal:

$$\begin{aligned}\text{NOT} &= \text{NOR} \circ \text{FANOUT}, \\ \text{AND} &= \text{NOR} \circ (\text{NOT} \otimes \text{NOT}), \\ \text{OR} &= \text{NOT} \circ \text{NOR}.\end{aligned}$$

Alternatively, in order to minimize dissipation of energy (Landauer, 1961; Landauer, 1998; Plenio and Vitelli, 2001; Bub, 2001; Parker and Walker, 2003), one may execute all calculations using only reversible networks⁸ (Toffoli, 1980a):

Since⁹

$$\text{CCNOT}_3(b_1, b_2, 1) = \text{NAND}(b_1, b_2) \quad \forall b_1, b_2 \in \{0, 1\}$$

and

$$\begin{pmatrix} \text{CCNOT}_1(b, 1, 0) \\ \text{CCNOT}_3(b, 1, 0) \end{pmatrix} = \text{FANOUT}(b) \quad \forall b \in \{0, 1\},$$

the CCNOT gate is universal for reversible classical computation in the following sense:

For every mapping $\phi \in \mathcal{F}_{n_1, n_2}$ there is a reversible n -bit network composed of only CCNOT gates,¹⁰ SWAP gates, and ID gates (*wires*) implementing a mapping $f \in \mathcal{F}_{n, n}$ ($n \geq n_1, n_2$) fulfilling

$$\begin{pmatrix} f_1(b_1, \dots, b_{n_1}, c_{n_1+1}, \dots, c_n) \\ \vdots \\ f_{n_2}(b_1, \dots, b_{n_1}, c_{n_1+1}, \dots, c_n) \end{pmatrix} = \phi(b_1, \dots, b_{n_1}) \quad \forall b_1, \dots, b_{n_1} \in \{0, 1\}$$

for suitably chosen constant bits c_{n_1+1}, \dots, c_n .

Of course, it is a nontrivial task to optimize such networks.¹¹

— DRAFT, June 26, 2009 —

⁷I.e., every classical logic circuit corresponds to a composition of tensor products of IDs, FANOUTs, and NANDs.

⁸**Reversible** classical networks (logic circuits) are those corresponding to bijections $f \in \mathcal{F}_{n, n}$ for some $n \in \mathbb{N}$.

⁹TOFFOLI called his gate the AND/NAND gate to indicate that also $\text{CCNOT}_3(j, k, 0) = \text{AND}(j, k)$ holds. Correspondingly, he called CNOT the XOR/FANOUT gate.

¹⁰The CNOT gate **cannot** fulfill this purpose for **classical** computation.

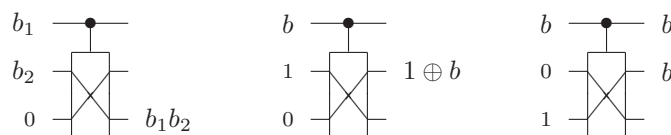
¹¹See (Shende et al., 2003) and (Tsai and Kuo, 2001; Younes and Miller, 2004; Shende et al., 2006), in this connection.

Theorem 1.1.2 (TOFFOLI) For all $n_1, n_2 \in \mathbb{N}$ and for every $\phi \in \mathcal{F}_{n_1, n_2}$ there is some $n \in (\max\{n_1, n_2\}, \dots, n_1 + n_2)$ and some bijection $f \in \mathcal{F}_{n, n}$ with

$$\begin{pmatrix} f_1(b_1, \dots, b_{n_1}, 0, \dots, 0) \\ \vdots \\ f_{n_2}(b_1, \dots, b_{n_1}, 0, \dots, 0) \end{pmatrix} = \phi(b_1, \dots, b_{n_1}) \quad \forall b_1, \dots, b_{n_1} \in \{0, 1\} .$$

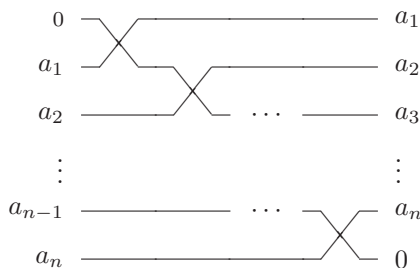
Proof: See (Toffoli, 1980b, Theorem 4.1). ■

Exercise 1 Show that CSWAP acts as indicated and, therefore, is universal for classical reversible computation:

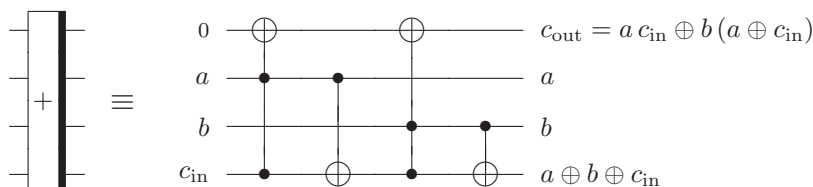


Exercise 2 Show that the following networks act as indicated.¹²

a) Multiplication by 2:



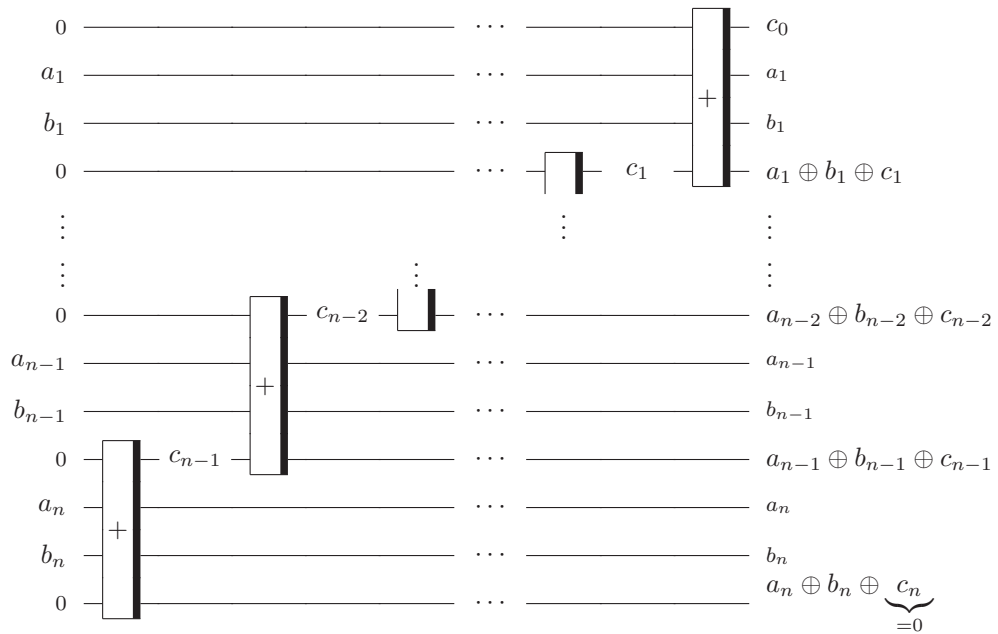
b) Adder¹³ for $a, b \in \{0, 1\}$:



¹²See also (Vedral et al., 1996; Draper, 2000; Tsai and Kuo, 2001; Cheng and Tseng, 2002).

¹³Note that $a c_{in} \oplus b(a \oplus c_{in}) = 0$ iff $a + b + c_{in} \leq 1$.

c) Adder for $\mathbf{a}, \mathbf{b} \in \{0, 1\}^n$:



$$\underbrace{\sum_{\nu=1}^n a_{\nu} 2^{n-\nu}}_x + \underbrace{\sum_{\nu=1}^n b_{\nu} 2^{n-\nu}}_y = c_0 2^n + \underbrace{\sum_{\nu=1}^n (a_{\nu} \oplus b_{\nu} \oplus c_{\nu}) 2^{n-\nu}}_{x+y}.$$

Exercise 3 Show that for every reversible classical 2-bit network there is an equivalent one composed only of CNOTs, TCMNOTs and NOTs.¹⁴

1.2 Quantum Computational Networks

1.2.1 Quantum Gates

If the computational registers are made smaller and smaller you will finally have to take into account the quantum behavior of the devices. Then a n -bit register has to be considered as an array of quantum mechanical systems to be ‘switched’ — for **classical** computation — into one of two selected (pure) states corresponding

¹⁴**Hint:** Check the action of $(\text{ID} \otimes \text{NOT}) \circ \text{TCNOT}$ on the ordered set of 2-bits.

to two orthonormal state vectors, usually denoted $|0\rangle$ and $|1\rangle$. This way the n -bit information (b_1, \dots, b_n) will be encoded into the state vector

$$|b_1, \dots, b_n\rangle \equiv |b_1\rangle \otimes \dots \otimes |b_n\rangle \quad (1.5)$$

corresponding to the situation:

‘Switch’ number ν being in the state corresponding to $|b_\nu\rangle$ for $\nu = 1, \dots, n$.

Then reversible classical n -bit gates correspond to permutations of the 2^n states corresponding to the orthonormal **computational basis**

$$\{|\mathbf{b}\rangle : \mathbf{b} \in \{0, 1\}^n\}$$

of the registers state space. Since such permutations are special unitary transformations there is a chance to implement them by mathematically simple quantum mechanical evolution (governed by some SCHRÖDINGER equation). Of course the interpolating states do no longer correspond to some element of the computational basis even if this is the case for both the input state and the output state. Moreover, quantum mechanics allows **coherent superpositions** as input states,¹⁵ corresponding to complex linear combinations of the elements of the computational basis. Then the gate causes the transition

$$\sum_{\mathbf{b} \in \{0, 1\}^n} \underbrace{\lambda_{\mathbf{b}}}_{\in \mathbb{C}} |\mathbf{b}\rangle \longmapsto \sum_{\mathbf{b} \in \{0, 1\}^n} \lambda_{\mathbf{b}} |f(\mathbf{b})\rangle ,$$

where $f \in \mathcal{F}_{n,n}$ is the mapping corresponding to the classical action of the gate. This means that, in a way, the gate is able to perform all the 2^n transitions

$$|\mathbf{b}\rangle \longmapsto |f(\mathbf{b})\rangle , \quad \mathbf{b} \in \{0, 1\}^n ,$$

simultaneously — thanks to quantum mechanical evolution. Of course, one would like to exploit this massive **quantum parallelism** for more efficient computation. Unfortunately quantum mechanics imposes severe restrictions:

1. Unknown coherent superpositions cannot be copied with arbitrary precision (Wootters and Zurek, 1982; Peres, 2002). Otherwise a device for superluminal communication could be constructed (Werner, 2001, Chapter 3).
2. Every measurement of an unknown state destroys most of the information carried by that state (*quantum state collapse*).
3. It is extremely difficult to correct errors caused by unwanted interaction with the environment.

Nevertheless quantum computational networks can be devised, at least in principle, which are much more efficient, for certain tasks, than classical computational networks. Their general structure is as follows:

DRAFT, June 26, 2009

¹⁵See (Long and Sun, 2001) for an efficient preparation of these superpositions.

- The information is usually processed on one and the same quantum register¹⁶ realized as an array of *qubits*,¹⁷ i.e. quantum mechanical systems with a preselected simple quantum alternative corresponding to orthonormal state vectors, usually denoted $|0\rangle$ and $|1\rangle$.
- The possible (pure) states of such an n -qubit register correspond to the (normalized) complex linear combinations of the elements (1.5) of the computational basis.
- ‘Simple’ quantum computational steps are depicted in the network model by *quantum gates* with an equal number ($\leq n$) of *quantum wires* (horizontal lines) attached on both sides. These quantum wires represent the qubits on which the gate acts.
- Several quantum gates may be assembled as in the classical reversible case (without loopbacks, of course).
- The whole network itself is a (more complicated) n -qubit quantum gate acting corresponding to some unitary operator \hat{U}_{net} .
- The action of this operator on the initial state vector $|b_1, \dots, b_n\rangle$ representing the task (encoded in the bit sequence (b_1, \dots, b_n)) has to be checked — i.e. the output state $\hat{U}_{\text{net}} |b_1, \dots, b_n\rangle$ has to be *measured* — to yield a *result*.

Even though only the probability of a certain outcome of a quantum computation is predictable (according to the rules of quantum mechanics) quantum computation may be very useful for problems of the type

“solution easy to check but difficult to find”.

This will be demonstrated by several quantum algorithms in Chapter 2.

Remarks:

1. We use the naive tensor product formalism of quantum mechanics to describe coupled systems. The latter is very problematic if the interaction of matter with radiation is to be described; see Section 6.2 of (Lücke, nlqo).
2. Of course, the network model described above is just the simplest model for quantum computing. Some possible generalizations, not to be discussed in this chapter, are:
 - Computation with non-unitarily evolving mixed states (Tarasov, 2002).
 - Quantum computation via application of sequences of one-qubit projective measurements to suitably prepared initial states (Raussendorf et al., 2002).
 - Use of *non-deterministic* gates, i.e. those succeeding only with probability (considerably) less than 1 (Ralph et al., 2002; Bartlett et al., 2002).

DRAFT, June 26, 2009

¹⁶Thanks to the SWAP gate this is not a necessity but this point of view simplifies the treatment.

¹⁷Usually qubits are treated as distinguishable, due to their localization in (essentially) disjoint regions; see (Eckert et al., 2002) for a refined description.


Name	Symbol	Operator	Matrix	Action
\hat{U} gate		\hat{U}	$\begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$	$ 0\rangle \mapsto u_{11} 0\rangle + u_{21} 1\rangle$ $ 1\rangle \mapsto u_{12} 0\rangle + u_{22} 1\rangle$

Table 1.3: General one-qubit gate ($\overline{u_{1j}} u_{1k} + \overline{u_{2j}} u_{2k} = \delta_{jk}$)




Name	Symbol	Operator	Matrix	Action
ID gate		\hat{I}	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$ b\rangle \mapsto b\rangle$
NOT gate		$\hat{\neg}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$ 0\rangle \rightleftharpoons 1\rangle$
phase shift gate		\hat{S}_δ	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}$	$ 0\rangle \mapsto 0\rangle$ $ 1\rangle \mapsto e^{i\delta} 1\rangle$
HADAMARD gate		\hat{U}_H	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$ 0\rangle \mapsto \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$ $ 1\rangle \mapsto \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$

Table 1.4: Special one-qubit gates

3. We are not going to discuss oddities like¹⁸ “quantum computation even before its quantum input is defined” (Brukner et al., 2003) or “counterfactual computation” (Mitchison and Jozsa, 2001). For quantum **programming** we refer to (Bettelli et al., 2001).

The elements $|b_1, \dots, b_n\rangle$ of the computational basis of an n -qubit system are naturally ordered by the corresponding integers

$$I(\mathbf{b}) \stackrel{\text{def}}{=} \sum_{\nu=1}^n b_\nu 2^{n-\nu} \quad \forall \mathbf{b} \in \{0, 1\}^n. \quad (1.6)$$

It is relative to this ordering that the actions of quantum gates are usually represented by unitary matrices as in Tables 1.3–1.5.

Remark: Note that every (complex) unitary 2×2 matrix corresponds to a spin rotation; see, e.g., Exercise 19 of (Lücke, tdst) and Sect. 4.2.1 of (Lücke, qft).

Note that a quantum gate may be used for classical computation iff the entries of its matrix take only values from $\{0, 1\}$. Whenever this is the case we use the same

¹⁸See 3.1.4, however.

Name	Symbol	Matrix	Action
$\Lambda_n(\hat{U})$ gate		$\begin{pmatrix} \mathbb{1}_{2^n} & 0 \\ 0 & \hat{U} \end{pmatrix}$	$ b_1, \dots, b_n, c\rangle \mapsto \begin{cases} b_1, \dots, b_n\rangle \otimes \hat{U} c\rangle & \text{if } b_1 = \dots = b_n = 1 \\ b_1, \dots, b_n, c\rangle & \text{else} \end{cases}$

Table 1.5: Special $(n + 1)$ -qubit gates

symbol and name for the quantum gate as for its classical analog. In this sense we have, e.g.,

$$\Lambda_1(\hat{\wedge}) = \text{CNOT} : \quad \begin{array}{c} \bullet \\ | \\ \square \hat{\wedge} \\ | \\ \oplus \end{array} = \begin{array}{c} \bullet \\ | \\ \oplus \\ | \\ \bullet \end{array},$$

$$\Lambda_2(\hat{\wedge}) = \text{CCNOT} : \quad \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \square \hat{\wedge} \\ | \\ \oplus \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \oplus \\ | \\ \bullet \end{array}, \quad (1.7)$$

i.e.

$$\oplus = \begin{array}{c} | \\ \square \hat{\wedge} \\ | \end{array}. \quad (1.8)$$

Obviously, the phase shift gate (for $\delta \neq 0 \pmod{\pi}$) and the HADAMARD gate have no classical analog.

Sometimes it is more convenient to sketch the action of a gate as done in Figure 1.1 for the f -CNOT gate.

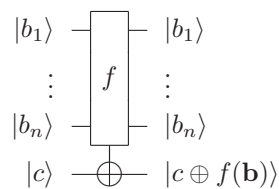
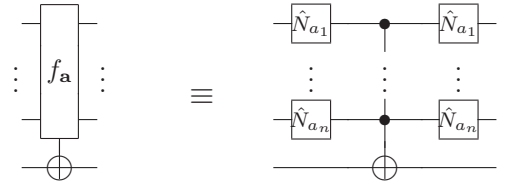


Figure 1.1: f -CNOT gate for $f \in \mathcal{F}_{n,1}$

Quantum computational networks are called *equivalent* if they implement the same mapping up to a phase factor.

Exercise 4

a) For arbitrary $\mathbf{a} \in \{0, 1\}^n$, $n \in \mathbb{N}$, show that



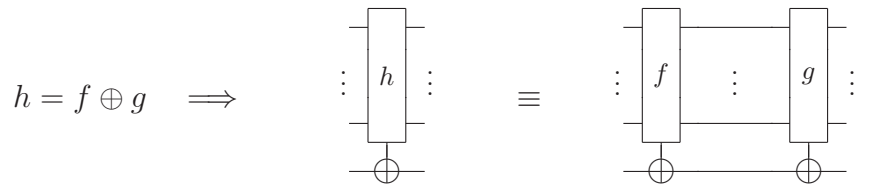
where

$$f_{\mathbf{a}}(\mathbf{b}) \stackrel{\text{def}}{=} \delta_{\mathbf{a},\mathbf{b}} \quad \forall \mathbf{b} \in \{0, 1\}^n$$

and

$$\hat{N}_b \stackrel{\text{def}}{=} \begin{cases} \hat{1} & \text{if } b = 0, \\ \hat{1} & \text{else.} \end{cases}$$

b) Show for arbitrary $f, g \in \mathcal{F}_{n,1}$ that



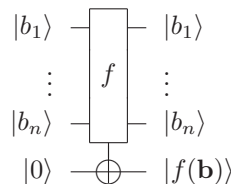
A first example showing the superiority of quantum networks is the DEUTSCH-JOZSA *problem*:

Assume you are given an $(n + 1)$ qubit gate which is only known to be the f -CNOT gate of some $f \in \mathcal{F}_{n,1}$ that is either constant or *balanced*, i.e. fulfills

$$\sum_{\mathbf{b} \in \{0,1\}^n} (-1)^{f(\mathbf{b})} = 0.$$

Find out by ‘asking’ this DEUTSCH-JOZSA *oracle* whether f is balanced or constant.

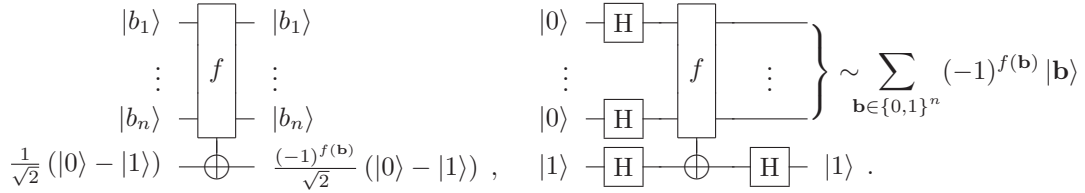
Note that in classical computation



you may have to ask the DEUTSCH-JOZSA oracle $2^{n-1} + 1$ times (in the worst case) to find the answer. Already for $n = 60$ that would take more than

$$\frac{2^{59}}{60 \cdot 60 \cdot 24 \cdot 365 \cdot 10^9} \text{ years} > 18 \text{ years}$$

to get the answer if the oracle is asked at a frequency of 1 GHz. In quantum computation, however, we may take advantage of coherent superpositions:



Since

$$\begin{aligned} \hat{U}_H |b\rangle &= \frac{1}{\sqrt{2}} (|0\rangle + (-1)^b |1\rangle) \\ &= \frac{1}{\sqrt{2}} \sum_{b' \in \{0,1\}} (-1)^{b'b} |b'\rangle \quad \forall b \in \{0,1\} \end{aligned}$$

and hence

$$\hat{U}_H^{\otimes n} |\mathbf{b}\rangle = 2^{-n/2} \sum_{\mathbf{b}' \in \{0,1\}^n} (-1)^{\mathbf{b}' \cdot \mathbf{b}} |\mathbf{b}'\rangle \quad \forall \mathbf{b} \in \{0,1\}^n \quad (1.9)$$

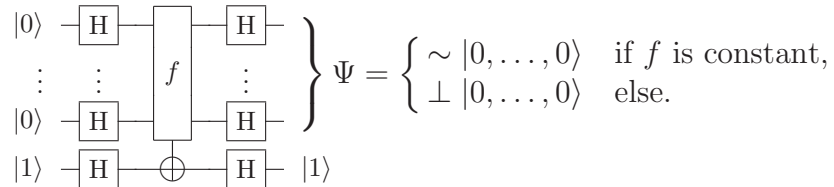
we have

$$\hat{U}_H^{\otimes(n+1)} \circ f\text{-CNOT} \circ \hat{U}_H^{\otimes(n+1)} |0, \dots, 0, 1\rangle = 2^{-n} \sum_{\mathbf{b}, \mathbf{b}' \in \{0,1\}^n} (-1)^{f(\mathbf{b}) + \mathbf{b}' \cdot \mathbf{b}} |\mathbf{b}', 1\rangle. \quad (1.10)$$

For the DEUTSCH-JOZSA oracle this means

$$\hat{U}_H^{\otimes(n+1)} \circ f\text{-CNOT} \circ \hat{U}_H^{\otimes(n+1)} |0, \dots, 0, 1\rangle = \begin{cases} \sim |0, \dots, 0, 1\rangle & \text{if } f \text{ is constant,} \\ \perp |0, \dots, 0, 1\rangle & \text{else.} \end{cases}$$

Therefore, the following quantum gate has to be used only¹⁹ once in order to solve the DEUTSCH-JOZSA problem (Cleve et al., 1998, Sect. 3):



DRAFT, June 26, 2009

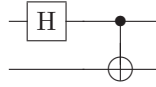
¹⁹Actually, since there is always some tiny probability for getting the wrong answer, the quantum test should be repeated a few times. For a physical realization of the algorithm see (Gulde et al., 2003).

Remark: (1.10) holds for every $f \in \mathcal{F}_{2,1}$ and can therefore be applied also to the BERNSTEIN-VAZIRANI *oracle*, i.e. the f -CNOT gate with $f(\mathbf{b}) = \mathbf{a} \cdot \mathbf{b}$ for some $\mathbf{a} \in \{0, 1\}^n$. Then Ψ becomes

$$2^{-n} \sum_{\mathbf{b}, \mathbf{b}' \in \{0,1\}^n} (-1)^{(\mathbf{a}+\mathbf{b}') \cdot \mathbf{b}} |\mathbf{b}'\rangle = |\mathbf{a}\rangle .$$

1.2.2 Quantum Teleportation

Obviously, the BELL *network*



acts according to²⁰

$$\begin{aligned} |0, 0\rangle &\longmapsto \Psi_{0,0} \stackrel{\text{def}}{=} \Phi_+ \stackrel{\text{def}}{=} \frac{|0, 0\rangle + |1, 1\rangle}{\sqrt{2}} = (\hat{U}_{0,0} \otimes \hat{1}) \Psi_{0,0}, \\ |0, 1\rangle &\longmapsto \Psi_{0,1} \stackrel{\text{def}}{=} \Psi_+ \stackrel{\text{def}}{=} \frac{|0, 1\rangle + |1, 0\rangle}{\sqrt{2}} = (\hat{U}_{0,1} \otimes \hat{1}) \Psi_{0,0}, \\ |1, 0\rangle &\longmapsto \Psi_{1,0} \stackrel{\text{def}}{=} \Phi_- \stackrel{\text{def}}{=} \frac{|0, 0\rangle - |1, 1\rangle}{\sqrt{2}} = (\hat{U}_{1,0} \otimes \hat{1}) \Psi_{0,0}, \\ |1, 1\rangle &\longmapsto \Psi_{1,1} \stackrel{\text{def}}{=} \Psi_- \stackrel{\text{def}}{=} \frac{|0, 1\rangle - |1, 0\rangle}{\sqrt{2}} = (\hat{U}_{1,1} \otimes \hat{1}) \Psi_{0,0}, \end{aligned}$$

where

$$\begin{aligned} \hat{U}_{0,0} &\stackrel{\text{def}}{=} +|0\rangle\langle 0| + |1\rangle\langle 1| = \hat{1}, \\ \hat{U}_{0,1} &\stackrel{\text{def}}{=} +|1\rangle\langle 0| + |0\rangle\langle 1| = \hat{\sigma}_x, \\ \hat{U}_{1,0} &\stackrel{\text{def}}{=} +|0\rangle\langle 0| - |1\rangle\langle 1| = \hat{S}_\pi, \\ \hat{U}_{1,1} &\stackrel{\text{def}}{=} -|1\rangle\langle 0| + |0\rangle\langle 1| = \hat{S}_\pi \hat{\sigma}_x. \end{aligned}$$

This indicates the possibility of *quantum dense coding*.²¹

———— DRAFT, June 26, 2009 ————

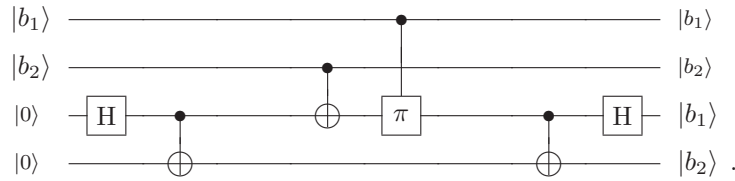
²⁰The states on the r.h.s are usually called BELL *states*. They exhibit maximal correlation between the two qubits. We use the notation $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}_\perp \stackrel{\text{def}}{=}} \begin{pmatrix} -\bar{\beta} \\ +\bar{\alpha} \end{pmatrix}$. Thus

$$\Psi_- = \frac{1}{\sqrt{2}} \left(\frac{\Psi}{\|\Psi\|} \otimes \frac{\Psi_\perp}{\|\Psi_\perp\|} - \frac{\Psi_\perp}{\|\Psi_\perp\|} \otimes \frac{\Psi}{\|\Psi\|} \right) \quad \forall \Psi \in \mathbb{C}^2 \setminus \{0\} .$$

²¹See (Mermin, 2002) for an interesting discussion of dense coding.

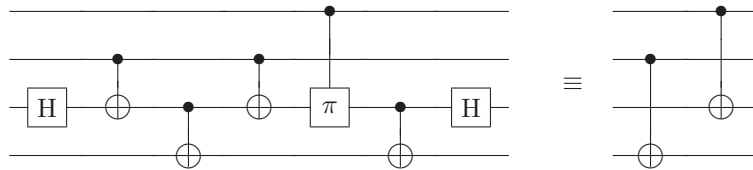
Bob prepares the *entangled*²² state $\Psi_{0,0}$ by applying the BELL network to the easily available state $|0, 0\rangle$ and sends his first qubit to Alice (arbitrarily far away). Now Alice may transfer a 2-bit message to Bob by applying one of the operators $\hat{U}_{0,0}, \hat{U}_{0,1}, \hat{U}_{1,0}, \hat{U}_{1,1}$ to this single qubit and sending it back to Bob. Bob can ‘read’ this message by performing a BELL measurement, i.e. checking whether the state of the 2-qubit system is $\Psi_{0,0}, \Psi_{0,1}, \Psi_{1,0},$ or $\Psi_{1,1}$.

The whole procedure is described by the following network action:



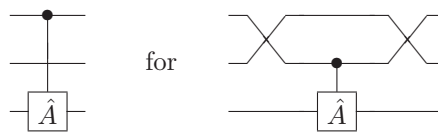
Remarks:

1. As pointed out in (Mermin, 2002), the network



— although unsuitable for dense coding — has the same effect on the considered special input.

2. We use abbreviations like



without explicit definition.

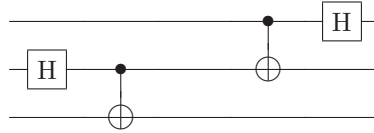
Moreover, checking the special cases $\Psi \in \{|0\rangle, |1\rangle\}$, we see that the *teleportation network*

———— DRAFT, June 26, 2009 ————

²²*Entanglement* of vector states Ψ means

$$\langle \Psi | \hat{A} \otimes \hat{B} | \Psi \rangle \stackrel{\text{i.g.}}{\neq} \langle \Psi | \hat{A} \otimes \hat{1} | \Psi \rangle \langle \Psi | \hat{1} \otimes \hat{B} | \Psi \rangle,$$

i.e. (non-classical) correlations between the subsystems. See (Brukner et al., 2001) in this context.



acts on $\psi \otimes |0, 0\rangle$ in the following way:

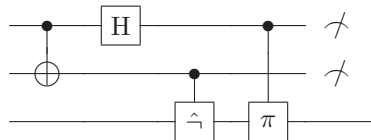
$$\psi \otimes |0, 0\rangle \mapsto \frac{1}{2} \sum_{\mathbf{b} \in \{0,1\}^2} |\mathbf{b}\rangle \otimes \hat{U}_{\mathbf{b}}^{-1} \psi.$$

(for every one-qubit state vector ψ). This indicates the possibility of *quantum teleportation*.²³

Qubits 2 and 3 are prepared in the state $\Phi_{0,0}$ (indicated by the BELL subnetwork on the left acting on $|0, 0\rangle$). Then qubit 2 is sent to Alice and qubit 3 to Bob (far apart). Since, now, Alice and Bob share an entangled pair of qubits, Alice may teleport the unknown state ψ of qubit 1 to Bob in the following way:

Alice performs a BELL measurement on the system formed by qubits 1 and 2 and sends Bob the classical 2-bit information \mathbf{b} if the result is $\Psi_{\mathbf{b}}$ (corresponding to the output $|\mathbf{b}\rangle$ of the teleportation network for qubits 1 and 2). After receiving this information Bob transforms the (collapsed) state of qubit 3 into ψ by applying $\hat{U}_{\mathbf{b}}$.

Note that the actions taken by Alice and Bob, sharing the entangled pair, have the same effect on qubits 1–3 as the following *post selection* scheme:²⁴



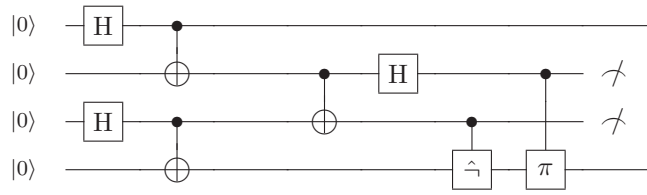
In this sense the following scheme describes teleportation of entanglement, also called

———— DRAFT, June 26, 2009 ————

²³The possibility of teleportation, further discussed in Appendix A.2, was first pointed out in (Bennet et al., 1993). Generalization to n -qubit states is straightforward (Díaz-Caro, 2005). Concerning the experimental realization of quantum teleportation see (Giacomini et al., 2002).

²⁴The symbol \nearrow represents an ideal test (projective measurement) whether the corresponding qubit is in state $|0\rangle$ or $|1\rangle$. It is instructive to study the BELL measurement as a two-step process, in this connection (Groisman, 2008).

entanglement swapping.²⁵



This possibility is very important for creating entanglement for teleportation over very large distances.

Exercise 5 Show that the entanglement swapping scheme prepares the subsystem formed by qubits 1 and 4 (arbitrarily far apart) in the state $\Psi_{0,0}$.

1.2.3 Universality

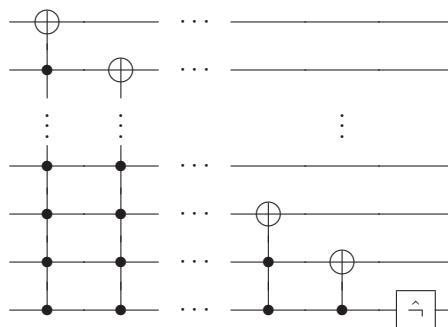
A 2-qubit gate corresponding to the unitary operator $\hat{U}^{(2)}$ is called *universal* if for every quantum network there is an equivalent one composed only of one-qubit gates and 2-qubit gates corresponding to $\hat{U}^{(2)}$.

Ordering the computational basis vectors

$$|I(\mathbf{b})\rangle_n \stackrel{\text{def}}{=} |\mathbf{b}\rangle \quad \forall \mathbf{b} \in \{0,1\}^n \tag{1.11}$$

as $|0\rangle_n, |1\rangle_n, \dots, |2^n - 1\rangle_n$ then $\lambda_{n-1}(\hat{\Lambda})$ just interchanges the last two of these vectors, the latter being $|1, \dots, 1, 0\rangle$ and $|1, \dots, 1, 1\rangle$. Also cyclic permutations of the computational basis vectors can be achieved by suitable composition of $\Lambda_\nu(\hat{\Lambda})$ gates, as the following exercise shows.

Exercise 6 Show that the n -qubit network



DRAFT, June 26, 2009
²⁵See (Bowmeester et al., 2000, Sect. 3.10) and (Gisin and Gisin, 2002).

acts according to

$$|x\rangle_n \mapsto |(x+1) \bmod 2^n\rangle_n \quad \forall x \in \{0, \dots, 2^n - 1\},$$

where

$$\left| \sum_{\nu=1}^n b_\nu 2^{\nu-1} \right\rangle_n \stackrel{\text{def}}{=} |\mathbf{b}\rangle \quad \forall \mathbf{b} \in \{0, 1\}^n. \quad (1.12)$$

Therefore:

For every quantum gate that has a classical analogue there is an equivalent quantum network composed only of $\Lambda_\nu(\hat{\cdot})$ (and ID) gates.

This together with the following theorem shows that the CNOT gate is universal if the following holds for every $\nu \in \mathbb{N}$:

For every $\hat{U} \in U(2)$ there is a network composed only of single qubit gates and CNOT gates (and ID gates) that is equivalent to the $\Lambda_\nu(\hat{U})$ gate. (1.13)

Theorem 1.2.1 *Let $2 < N \in \mathbb{N}$. Then every unitary $N \times N$ -matrix may be represented as a product of permutation matrices and $N \times N$ -matrices of the form*

$$\begin{pmatrix} \hat{1} & 0 \\ 0 & \hat{U} \end{pmatrix}, \quad \hat{U} \in U(2).$$

Outline of proof:²⁶ Given $2 < N \in \mathbb{N}$, choose some orthonormal basis $\{\mathbf{e}_1, \dots, \mathbf{e}_N\}$ of \mathbb{C}^N . Then, for arbitrary

$$\hat{U} = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \in U(2),$$

$N' \in \{2, \dots, N\}$, and $\nu \in \{1, \dots, N\}$ define

$$\hat{U}_{N'} \mathbf{e}_\nu \stackrel{\text{def}}{=} \begin{cases} u_{11} \mathbf{e}_{N'-1} + u_{21} \mathbf{e}_{N'} & \text{for } \nu = N' - 1, \\ u_{12} \mathbf{e}_{N'-1} + u_{22} \mathbf{e}_{N'} & \text{for } \nu = N', \\ \mathbf{e}_\nu & \text{else.} \end{cases}$$

Then, for arbitrary normed

$$\mathbf{z} = \sum_{\nu=1}^N z^\nu \mathbf{e}_\nu \in \mathbb{C}^N,$$

$N' \in \{2, \dots, N\}$, and $\zeta \in \mathbb{C}$ with

$$|\zeta|^2 + \sum_{\nu=N'+1}^N |z^\nu|^2 = 1$$

²⁶Compare (Reck et al., 1994; Diťă, 2001).

we have

$$\hat{U}_{N'}^{(N')} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \zeta \\ z^{N'+1} \\ \vdots \\ z^N \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \zeta' \\ z^{N'} \\ z^{N'+1} \\ \vdots \\ z^N \end{pmatrix}$$

for suitable $\hat{U}^{(N')} \in U(2)$ and $\zeta' \in \mathbb{C}$. Thus, by iteration, we see that there are $\hat{U}^{(N)}, \dots, \hat{U}^{(2)} \in U(2)$ with

$$\mathbf{z} = \hat{U}_2^{(2)} \dots \hat{U}_N^{(N)} \mathbf{e}_N$$

and hence

$$\left(\hat{U}_N^{(N)} \right)^{-1} \dots \left(\hat{U}_2^{(2)} \right)^{-1} \mathbf{z} = \mathbf{e}_N.$$

Identifying \mathbf{z} with the last column of an arbitrarily given unitary $N \times N$ -matrix \hat{U} we get

$$\left(\left(\hat{U}_N^{(N)} \right)^{-1} \dots \left(\hat{U}_2^{(2)} \right)^{-1} \hat{U} \right)_{\nu, N} = \delta_{\nu, N}.$$

Thanks to unitarity, the latter also implies

$$\left(\left(\hat{U}_N^{(N)} \right)^{-1} \dots \left(\hat{U}_2^{(2)} \right)^{-1} \hat{U} \right)_{N, \nu} = \delta_{N, \nu}.$$

Iteration of this argument, if necessary, proves the theorem. \blacksquare

That (1.13) holds for $\nu = 1$ is a simple consequence of the following lemma (Barenco et al., 1995):

Lemma 1.2.2 *For every²⁷ $\hat{U} \in \text{SU}(2)$ there are $\hat{A}, \hat{B}, \hat{C} \in \text{SU}(2)$ with*

$$\hat{A}\hat{B}\hat{C} = \hat{1}, \quad \hat{A}\hat{\leftarrow}\hat{B}\hat{\leftarrow}\hat{C} = \hat{U}.$$

Proof: Let $\hat{U} \in \text{SU}(2)$. Then one may easily show (see Exercise 28 of (Lücke, eine)) that there are angles ψ, θ, ϕ with

$$\hat{U} = \hat{R}_3(\psi) \hat{R}_2(\theta) \hat{R}_3(\phi),$$

where

$$\hat{R}_3(\psi) \stackrel{\text{def}}{=} \begin{pmatrix} e^{+i\frac{\psi}{2}} & 0 \\ 0 & e^{-i\frac{\psi}{2}} \end{pmatrix}, \quad \hat{R}_2(\theta) \stackrel{\text{def}}{=} \begin{pmatrix} +\cos\frac{\theta}{2} & +\sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & +\cos\frac{\theta}{2} \end{pmatrix}.$$

With the definitions

$$\hat{A} \stackrel{\text{def}}{=} \hat{R}_3(\psi) \hat{R}_2\left(\frac{\theta}{2}\right), \quad \hat{B} \stackrel{\text{def}}{=} \hat{R}_2\left(-\frac{\theta}{2}\right) \hat{R}_3\left(-\frac{\psi+\phi}{2}\right), \quad \hat{C} \stackrel{\text{def}}{=} \hat{R}_3\left(\frac{\phi-\psi}{2}\right)$$

DRAFT, June 26, 2009

²⁷As usual, we denote by $U(2)$ the set of all (complex) unitary 2×2 -matrices and by $SU(2)$ the set of all $\hat{U} \in U(2)$ with $\det \hat{U} = 1$.

this gives

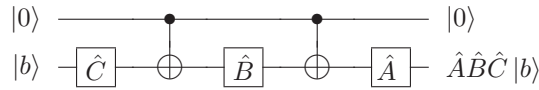
$$\begin{aligned}\hat{A}\hat{B}\hat{C} &= \hat{R}_3(\psi)\hat{R}_2\left(\frac{\theta}{2}\right)\hat{R}_2\left(-\frac{\theta}{2}\right)\hat{R}_3\left(-\frac{\psi+\phi}{2}\right)\hat{R}_3\left(\frac{\phi-\psi}{2}\right) \\ &= \hat{R}_3(\psi)\hat{R}_3(-\psi) \\ &= \hat{1}\end{aligned}$$

and

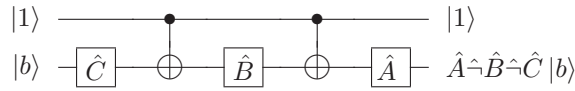
$$\begin{aligned}\hat{A}\hat{\smile}\hat{B}\hat{\smile}\hat{C} &= \hat{R}_3(\psi)\hat{R}_2\left(\frac{\theta}{2}\right)\hat{\smile}\hat{R}_2\left(-\frac{\theta}{2}\right)\hat{\smile}\hat{R}_3\left(-\frac{\psi+\phi}{2}\right)\hat{\smile}\hat{R}_3\left(\frac{\phi-\psi}{2}\right) \\ &= \hat{R}_3(\psi)\hat{R}_2\left(\frac{\theta}{2}\right)\left(\hat{\smile}\hat{R}_2\left(-\frac{\theta}{2}\right)\hat{\smile}\right)\left(\hat{\smile}\hat{R}_3\left(-\frac{\psi+\phi}{2}\right)\hat{\smile}\right)\hat{R}_3\left(\frac{\phi-\psi}{2}\right) \\ &= \hat{R}_3(\psi)\hat{R}_2\left(\frac{\theta}{2}\right)\hat{R}_2\left(\frac{\theta}{2}\right)\hat{R}_3\left(\frac{\psi+\phi}{2}\right)\hat{R}_3\left(\frac{\phi-\psi}{2}\right) \\ &= \hat{R}_3(\psi)\hat{R}_2(\theta)\hat{R}_3(\phi) \\ &= \hat{U}. \quad \blacksquare\end{aligned}$$

Remark: Note that ψ, θ, ϕ in the above proof correspond to the well-known EULER angles; see Sect. 2.1.1.3 of (Lücke, mech) and — for generalization — also (D'Alessandro, 2001).

Because of

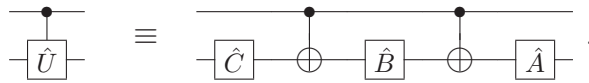


and

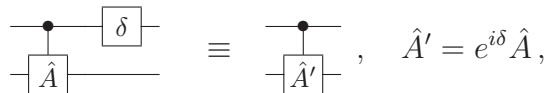


this has the following consequence:

Corollary 1.2.3 For $\hat{A}, \hat{B}, \hat{C}, \hat{U}$ according to Lemma 1.2.2 we have:

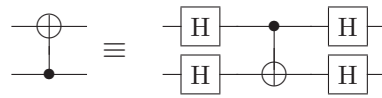


Corollary 1.2.3 together with

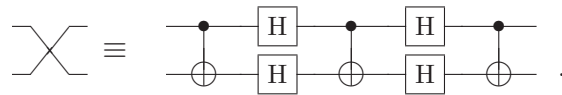


shows that that (1.13) holds for $\nu = 1$, indeed.

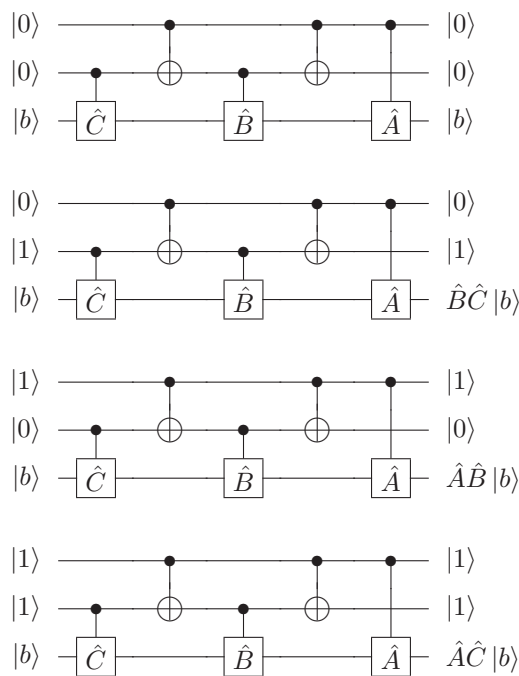
Exercise 7 Show that



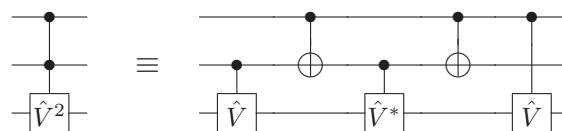
and²⁸



Moreover, because of

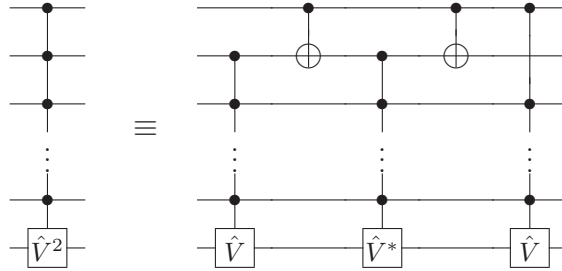


we have (Sleator and Weinfurter, 1994):



²⁸Recall (1.3).

This SLEATOR-WEINFURTER *construction* may be generalized for $\bigwedge_n(\hat{V}^2)$ with arbitrary $n \in \mathbb{N}$:²⁹



Since

$$U(2) = \left\{ \hat{V}^2 : \hat{V} \in U(2) \right\}$$

this that (1.13) holds for every $\nu \in \mathbb{N}$, hence:

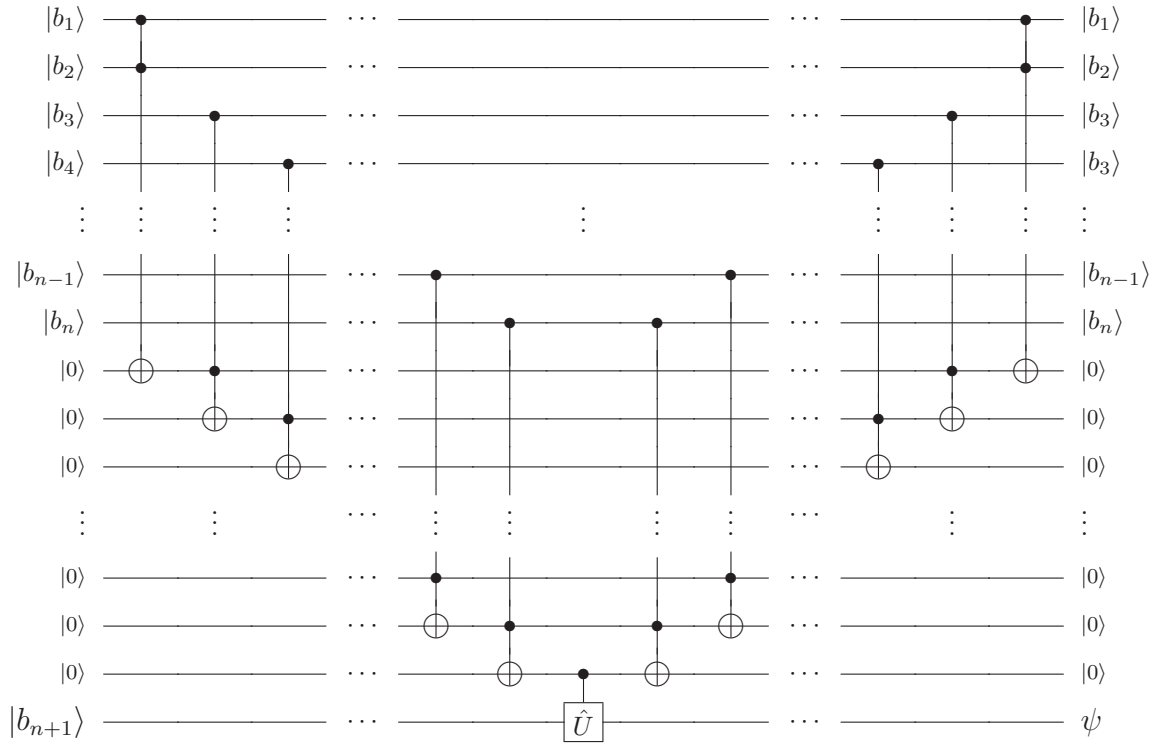
The CNOT gate is universal.³⁰

———— DRAFT, June 26, 2009 ————

²⁹Of course, one should look for more efficient implementations; see, e.g. Exercise 8 and (Aho and Svore, 2003; Vatan and Williams, 2004; Shende et al., 2004). For a nice introduction into the general theory of computational complexity see (Mertens, 2002).

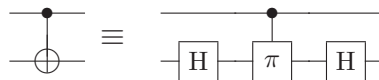
³⁰Therefore, if CNOT is implementable together with all one-qubit gates and projective measurements w.r.t. the computational basis, **all** observables can actually be measured.

Exercise 8 Show that the following network acts as indicated:

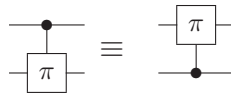


$$\psi = \begin{cases} \hat{U} |b_{n+1}\rangle & \text{if } b_1 = \dots = b_n = 1, \\ |b_{n+1}\rangle & \text{else.} \end{cases}$$

Exercise 9 Show that³¹



and that



acts according to

$$|j, k\rangle \mapsto (-1)^{\delta_{j,1}\delta_{k,1}} |j, k\rangle .$$

DRAFT, June 26, 2009

³¹This equivalence is exploited in most suggestions for physical realization of CNOT.

Chapter 2

Quantum Algorithms¹

So far, we have only discovered a few techniques which can produce speed up versus classical algorithms. It is not clear yet whether the reason for this is that we do not have enough intuition to discover more techniques, or that there are only a few problems for which quantum computers can significantly speed up the solution.

(Shor, 2000)

2.1 Quantum Data Base Search

2.1.1 GROVER'S Algorithm

Let us assume that the $\mathbf{b} \in \{0, 1\}^n$ are the indices of the entries of some unstructured data base. Moreover let us assume we are given a search machine that provides an implementation of the $f_{\mathbf{a}}$ -CNOT gate, where

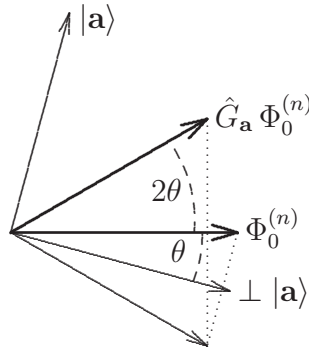
$$f_{\mathbf{a}}(\mathbf{b}) = \begin{cases} 1 & \text{if } \mathbf{b} = \mathbf{a} \\ 0 & \text{else} \end{cases} \quad \forall \mathbf{b} \in \{0, 1\}^n ,$$

when fed with a unique characterization of some entry indexed by \mathbf{a} . Now consider the following problem:

Find \mathbf{a} with probability $\geq 50\%$ by testing the behavior of the $f_{\mathbf{a}}$ -CNOT gate.

DRAFT, June 26, 2009

¹*Algorithms* are general, step-by-step procedures for solving general problems.

Figure 2.1: Action of \hat{G} on $\Phi_0^{(n)}$.

In classical computing (recall 1.2.2) one has to test $f_{\mathbf{a}}$ -CNOT at least 2^{n-1} -times² in order to find \mathbf{a} with probability of 50%. A substantial speedup,³ exploiting quantum parallelism, was suggested in (Grover, 1996). The basic ingredients of GROVER's algorithm are the initial state

$$\Phi_0^{(n)} \stackrel{\text{def}}{=} \hat{U}_H^{\otimes n} |0, \dots, 0\rangle = 2^{-n/2} \sum_{\mathbf{b} \in \{0,1\}^n} |\mathbf{b}\rangle = 2^{-n/2} \Phi_{1,1} \quad (2.1)$$

and the unitary operator

$$\hat{G}_{\mathbf{a}} \stackrel{\text{def}}{=} -\hat{R}_{\Phi_0^{(n)}} \hat{R}_{|\mathbf{a}\rangle}, \quad (2.2)$$

where

$$\hat{R}_{\Psi} \stackrel{\text{def}}{=} \hat{1} - 2\hat{P}_{\Psi} \quad \forall \Psi \in \mathcal{H}_n.$$

Since both reflections $\hat{R}_{|\mathbf{a}\rangle}$ and $\hat{R}_{\Phi_0^{(n)}}$ leave the $|\mathbf{a}\rangle$ - $\Phi_0^{(n)}$ -plane invariant, $\hat{G}_{\mathbf{a}}$ acts as a rotation in this plane. To determine this rotation it suffices to check its effect on $\Phi_0^{(n)}$.

As explained in Figure 2.1 this action is a rotation by the angle 2θ towards $|\mathbf{a}\rangle$, where $\pi/2 - \theta$ is the angle between $\Phi_0^{(n)}$ and $|\mathbf{a}\rangle$. Therefore:

Applying $\hat{G}_{\mathbf{a}}$ an appropriate number of times to $\Phi_0^{(n)}$ and testing the result with respect to the computational basis solves the posed problem.

———— DRAFT, June 26, 2009 ————

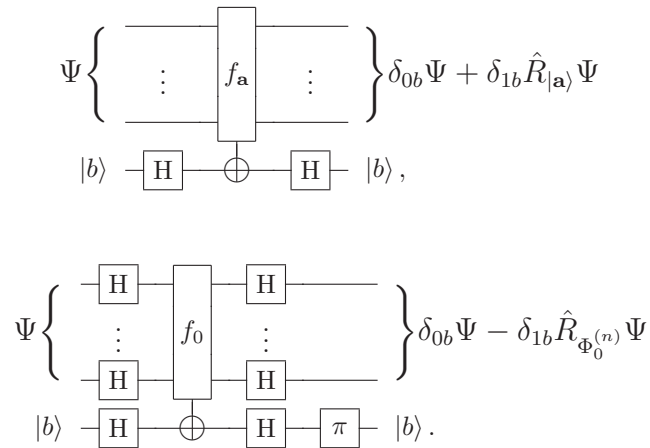
²Moreover, expectation value for the necessary number of tests for finding \mathbf{a} is

$$\overline{N} = \sum_{\nu=1}^{2^n} \frac{\nu}{N} = \frac{2^n + 1}{2}.$$

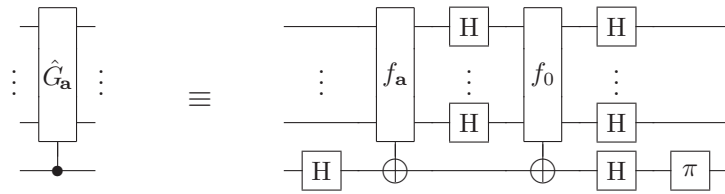
³See (Aaronson and Gottesman, 2004), however.

2.1.2 Network for GROVER's Algorithm

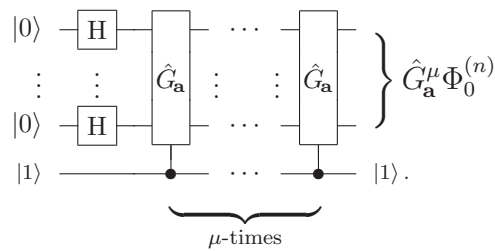
Exercise 10 Show that the following $(n + 1)$ -qubit networks act as indicated:⁴



Using the obvious notation and generalization of $\bigwedge_1(\hat{U})$ for n -qubit unitary operators \hat{U} , we get from Exercise 10



and therefore:



———— DRAFT, June 26, 2009 ————
⁴Recall Exercise 4a).

2.1.3 Details and Generalization

For actual application of GROVER's one has to know the number of times $G_{\mathbf{a}}$ should be applied. This can be read off from⁵

$$G_{\mathbf{a}}^{\mu} \Phi_0^{(n)} = \sin\left((2\mu + 1)\theta\right) |\mathbf{a}\rangle + \cos\left((2\mu + 1)\theta\right) \frac{1}{\sqrt{2^n - 1}} \sum_{\mathbf{b} \neq \mathbf{a}} |\mathbf{b}\rangle, \quad (2.3)$$

where

$$\theta \stackrel{\text{def}}{=} \arcsin\left(\frac{1}{\sqrt{2^n}}\right). \quad (2.4)$$

Since

$$\theta \approx 2^{-n/2} \quad \text{for } 2^{-n/2} \ll 1$$

we have

$$G_{\mathbf{a}}^{\mu} \Phi_0^{(n)} \approx |\mathbf{a}\rangle \quad \text{for } \mu = \left\lfloor \frac{\pi}{4} \sqrt{2^n} \right\rfloor \text{ and } 2^n \gg 1.$$

In this sense GROVER's algorithm provides a quadratic speedup compared to classical computation.

Let us now consider the case that there are exactly t data base entries,⁶ indexed by $\mathbf{a}_1, \dots, \mathbf{a}_t \in \{0, 1\}^n$, meeting the search criteria and that the search engine, therefore, provides an implementation of the $(f_{\mathbf{a}_1} + \dots + f_{\mathbf{a}_t})$ -CNOT gate. In order to find at least one of these \mathbf{a}_ν we just have to replace $\hat{G}_{\mathbf{a}}$ by

$$\hat{G}_{\mathbf{a}_1, \dots, \mathbf{a}_t} \stackrel{\text{def}}{=} -\hat{R}_{\Phi_0^{(n)}} \hat{R}_{|\mathbf{a}_1\rangle} \cdots \hat{R}_{|\mathbf{a}_t\rangle},$$

which may be implemented as described in 2.1.2 with the $f_{\mathbf{a}}$ -CNOT gate replaced by the $(f_{\mathbf{a}_1} + \dots + f_{\mathbf{a}_t})$ -CNOT gate. Correspondingly, (2.3)/(2.4) have to be replaced by

$$\hat{G}_{\mathbf{a}_1, \dots, \mathbf{a}_t}^{\mu} \Phi_0^{(n)} = \sin\left((2\mu + 1)\theta_t\right) \frac{|\mathbf{a}_1\rangle + \dots + |\mathbf{a}_t\rangle}{\sqrt{t}} + \cos\left((2\mu + 1)\theta_t\right) \frac{1}{\sqrt{2^n - t}} \sum_{\mathbf{b} \notin \{\mathbf{a}_1, \dots, \mathbf{a}_t\}} |\mathbf{b}\rangle \quad (2.5)$$

and

$$\theta_t \stackrel{\text{def}}{=} \arcsin\left(\frac{t}{\sqrt{2^n}}\right). \quad (2.6)$$

Choosing μ such that $\sin^2\left((2\mu + 1)\theta_t\right)$ is close to 1 we get a state that is essentially a superposition of only those states of the computational basis which correspond to data base entries meeting the search criteria. Performing a test we select one solution at random.

———— DRAFT, June 26, 2009 ————

⁵Formula (2.3) was presented first in (Boyer et al., 1998).

⁶For instance, we may be interested in only a subset of bit-values (Grover and Radhakrishnan, 2004)

Unfortunately, we only know how to choose μ if we know t . If t is unknown we find a solution after an expected number of $O\left(\sqrt{\frac{2^n-1}{t}}\right)$ applications of the described procedure with suitably chosen μ 's (Boyer et al., 1998, Sect. 4).

For interesting modifications of GROVER's algorithm see (Ambainis, 2005; Korepin and Grover, 2005; Tulsi et al., 2005) and references given there. For a few-qubit experimental implementation of the algorithm see (Walther et al., 2005) and references given there. For application to robots see (Dong et al., 2006).

Final Remark: Presumably GROVER's algorithm will **not** be useful for searching a **standard** database, because transferring the database to quantum memory would require too much effort (Deutsch and Ekert, 1998).

2.2 Factoring Large Integers

2.2.1 Basics

The greatest common divisor $\gcd(n_0, n_1)$ for given $n_0, n_1 \in \mathbb{Z}$ may be efficiently determined via EUCLID's *algorithm*.⁷

Defining

$$n_{\nu+2} \stackrel{\text{def}}{=} \begin{cases} n_\nu - n_{\nu+1} \lfloor \frac{n_\nu}{n_{\nu+1}} \rfloor & \text{if } n_{\nu+1} \neq 0 \\ 0 & \text{else} \end{cases} \quad (2.7)$$

successively for $\nu = 0, 1, 2, \dots$ we get

$$\gcd(n_0, n_1) = n_s \quad \text{for } s = \sup \{ \nu \in \mathbb{N} : n_\nu \neq 0 \} < \infty. \quad (2.8)$$

Thus, factoring a given product $N = p_1 p_2$ of unknown **large** integers p_1, p_2 is a task of the type

“A solution is easy to check but extremely difficult to find.”

Classical encryption schemes rely on this fact.

DRAFT, June 26, 2009

⁷As usual, we use the notation

$$\lfloor x \rfloor \stackrel{\text{def}}{=} \sup \{ n \in \mathbb{Z} : n \leq x \} \quad \forall x \in \mathbb{R}.$$

Thus, for $n_{\nu+1} \neq 0$, $n_{\nu+2}$ is the **remainder** of the integer division of n_ν by $n_{\nu+1}$. For details concerning EUCLID's algorithm see Section 2.2.3.

The most popular public-key encryption algorithm⁸ is RSA, named after its three inventors Ron Rivest, Adi Shamir, and Leonhard Adleman. It works as follows (Rivest et al., 1978):

- Messages and keys are represented by natural numbers corresponding to binary strings.
- Messages M are encoded as

$$C = M^e \pmod{N},$$

where $N > M$ and e are two **public keys** created in the following way:

1. Two large prime numbers p and q of comparable size are randomly chosen⁹ and kept secret. Only their product

$$N = p \cdot q$$

is publicly announced.

2. e is chosen as a large random number having 1 as largest common divisor with $(p - 1) \cdot (q - 1)$ — to be checked by EUCLID's algorithm.

- The message may be decrypted in the form

$$M = C^d \pmod{N}.$$

where $d \in \{1, \dots, (p - 1) \cdot (q - 1) - 1\}$ is the **private key** to be determined from¹⁰

$$e \cdot d = 1 \pmod{(p - 1) \cdot (q - 1)}.$$

Of course, d has to be kept secret as well as the prime numbers p, q which then may be forgotten.

The task of factorizing N in the form

$$N = p \cdot q \quad \text{with } p, q \in \{2, \dots, N - 1\}$$

is essentially solved if a factorization

$$n_+ \cdot n_- = 0 \pmod{N} \tag{2.9}$$

of an integer multiple of N is found that fulfills the conditions

$$n_{\pm} \neq 0 \pmod{N} \tag{2.10}$$

DRAFT, June 26, 2009

⁸See (Singh, 2002; Kahn, 1967) for the history of classical cryptography and (Schneier, 1996) for applications.

⁹See (Rivest et al., 1978, Section VII.B) how to find large prime numbers without testing primality by factorization.

¹⁰The essential point is that

$$(p - 1) \cdot (q - 1) = \varphi(p \cdot q),$$

where φ denotes the EULER function introduced in Theorem 2.2.1, below. d may be determined modulo $(p - 1) \cdot (q - 1)$ running EUCLID's algorithm (2.7) for $n_0 = (p - 1) \cdot (q - 1)$ and $n_1 = e$ and resubstituting iteratively the expressions for $n_s = 1$, s given by (2.8), using (2.7) to yield the representation $1 = e \cdot x + y \cdot N$ with certain integers x, y .

Then¹¹

$$\gcd(n_{\pm}, N) \in \{2, \dots, N-1\} \quad (2.11)$$

and these factors may be efficiently determined using EUCLID's algorithm.

Outline of proof for (2.11): Obviously, every prime factor of N must be a factor of either n_+ or n_- (or both) and neither n_+ nor n_- can be the product of all these (not necessarily pairwise different) factors. ■

Finding a factorization of type (2.9),(2.10) is facilitated by the following theorem.

Theorem 2.2.1 (EULER's Theorem) *Let $x, N \in \mathbb{N}$. If x and N are **coprime**, i.e. if $\gcd(x, N) = 1$, then*

$$x^{\varphi(N)} = 1 \pmod{N}$$

holds, where EULER's φ **function** is defined as¹²

$$\varphi(N) \stackrel{\text{def}}{=} \left| \{y \in \mathbb{N} : y < N, \gcd(y, N) = 1\} \right|.$$

Proof: See, e.g., (Schroeder, 1997, Sect. 8.3) or (Nielsen and Chuang, 2001, Theorem A4.9). ■

By EULER's theorem, for $N \in \mathbb{N}$ and

$$x \in \{2, \dots, N-1\}, \quad \gcd(x, N) = 1 \quad (2.12)$$

the function

$$f(\nu) \stackrel{\text{def}}{=} x^{\nu} \quad \forall \nu \in \mathbb{Z} \quad (2.13)$$

has a **minimal** period

$$r \stackrel{\text{def}}{=} \inf \{a \in \mathbb{N} : x^a = 1 \pmod{N}\}, \quad (2.14)$$

called the **order**¹³ of x modulo N . If r is **even** and

$$x^{r/2} \neq -1 \pmod{N} \quad (2.15)$$

then the conditions (2.9) and (2.10) are fulfilled for

$$n_{\pm} = x^{r/2} \pm 1.$$

¹¹As usual, we denote by $\gcd(n_1, n_2)$ the greatest common divisor of two integers n_1, n_2 .

¹²By $|M|$ we denote the number of elements of a finite set M .

¹³The numbers $x \in \{1, \dots, N-1\}$ form a group w.r.t. multiplication modulo N . Every element x of this group generates a cyclic subgroup of order r .

Outline of proof: (2.9) is a consequence of (2.14) and

$$(x^{r/2} + 1)(x^{r/2} - 1) = x^r - 1.$$

(2.10) follows from (2.15) and the corresponding property

$$x^{r/2} \not\equiv +1 \pmod{N}$$

implied by (2.14). ■

Summarizing, we have the following factoring algorithm:

1. Randomly choose some $x \in \{2, \dots, N - 1\}$.
2. If $\gcd(x, N) \neq 1$ then x is already a nontrivial factor of N .
3. If (2.12) holds, determine the order r of x modulo N .
4. If r is odd or $x^{r/2} \equiv -1 \pmod{N}$, restart the algorithm.
5. If r is even and $x^{r/2} \not\equiv -1 \pmod{N}$, determine the factors $\gcd(x^{r/2} \pm 1, N)$ using EULER's algorithm.

Thanks to the following theorem (and EULER's algorithm) the efficiency of this factoring algorithm depends solely on the available techniques for determining (2.14).

Theorem 2.2.2 *Let m be the number of different prime factors of the positive integer N and let $x \in \{1, \dots, N - 1\}$ be randomly chosen. If $\gcd(x, N) = 1$, then the (conditional) probability for (2.14) being even and $x^{r/2} \not\equiv -1 \pmod{N}$ is not smaller than $1 - 2^{-m}$.*

Proof: See, e.g., (Nielsen and Chuang, 2001, Theorem A.4.13). ■

In order to gain exponential speed up for the determination of (2.14), Peter W. Shor suggested the following (Shor, 1994):

Instead of calculating $x^a \pmod{N}$ for $a = 1, 2, \dots$ until the result is $1 \pmod{N}$, transform the state

$$\frac{1}{2^L} \sum_{a=0}^{2^{2L}-1} |a\rangle_{2L} \otimes |0\rangle_L,$$

where

$$L \stackrel{\text{def}}{=} \min \{l \in \mathbb{N} : N \leq 2^l\},$$

into the state¹⁴

$$\frac{1}{2^L} \sum_{a=0}^{2^{2L}-1} |a\rangle_{2L} \otimes |x^a \pmod{N}\rangle_L$$

(exploiting quantum parallelism) and evaluate the latter by means of the quantum FOURIER transform applied to the first $2L$ qubits..

2.2.2 The Quantum FOURIER Transform

In order to plot, over the interval $[-\Omega, +\Omega]$, the FOURIER transform

$$\tilde{f}(\omega) = \frac{1}{\sqrt{2\pi}} \int_0^{T_0} f(t) e^{i\omega t} dt$$

of a (sufficiently well-behaved) signal restricted to the time interval $[0, T_0]$ it is sufficient to have the discrete values

$$\tilde{f}\left(k \frac{2\pi}{T_0}\right), \quad k \in \mathbb{Z}, \quad \left|k \frac{2\pi}{T_0}\right| \leq \Omega,$$

if T_0 is large enough (depending on the required precision). In order to determine these values approximately it is sufficient to know the sampling values

$$f\left(j \frac{T_0}{N}\right), \quad j \in \{0, 1, \dots, N-1\},$$

for sufficiently large $N \in \mathbb{N}$ (depending on T_0 and Ω):

$$\tilde{f}\left(k \frac{2\pi}{T_0}\right) \approx \frac{1}{\sqrt{2\pi}} \sum_{j=0}^{N-1} f\left(j \frac{T_0}{N}\right) e^{ik \frac{2\pi}{N} j \frac{T_0}{N}} \quad \text{for } \left|k \frac{2\pi}{T_0}\right| \leq \Omega.$$

Remark: In order to estimate the quality of this approximation note that

$$\sum_{j=0}^{N-1} f\left(j \frac{T_0}{N}\right) e^{ik \frac{2\pi}{N} j} = \int_0^{T_0} \Delta_{T_0/N}(t) f(t) e^{i\omega t} dt,$$

where

$$\Delta_{T_0/N}(t) \stackrel{\text{def}}{=} \sum_{\nu \in \mathbb{Z}} \delta\left(t - \nu \frac{T_0}{N}\right)$$

and hence¹⁵

$$\tilde{\Delta}_{T_0/N}(\omega) = \sqrt{2\pi} \frac{N}{T_0} \sum_{\mu \in \mathbb{Z}} \delta\left(\omega - \underbrace{\mu \pi \frac{2N}{T_0}}_{\text{NYQUIST-frequency}}\right).$$

¹⁴An efficient implementation is described in (Vedral et al., 1996).

¹⁵See, e.g., (Lücke, musi, Anhang A.1).

Hence, using the so-called **discrete FOURIER transform**

$$\{x_j\}_{j \in \{0, \dots, N-1\}} \mapsto \left\{ \tilde{x}_k \stackrel{\text{def}}{=} \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{i k \frac{2\pi}{N} j} \right\}_{k \in \{0, \dots, N-1\}} \quad (2.16)$$

we get

$$\tilde{f}\left(k \frac{2\pi}{T_0}\right) \approx \frac{T_0}{\sqrt{2\pi N}} \tilde{x}_{k \pmod{N}} \quad \text{if } \left|k \frac{2\pi}{T_0}\right| \leq \Omega$$

for the sampling values

$$x_j = f\left(j \frac{T_0}{N}\right), \quad j \in \{0, \dots, N-1\}.$$

Since

$$\sum_{k=0}^{N-1} e^{i k \frac{2\pi}{N} m} = \frac{1 - e^{i 2\pi m}}{1 - e^{i \frac{2\pi}{N} m}} = 0 \quad \forall m \in \{1, \dots, N-1\}, \quad (2.17)$$

the inverse of the transformation (2.16) is

$$\{\tilde{x}_k\}_{k \in \{0, \dots, N-1\}} \mapsto \left\{ x_j \stackrel{\text{def}}{=} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \tilde{x}_k e^{-i k \frac{2\pi}{N} j} \right\}_{j \in \{0, \dots, N-1\}}. \quad (2.18)$$

Especially for $N = 2^n$ we define the **quantum FOURIER transform** \hat{F}_n by

$$\hat{F}_n \sum_{\mathbf{b} \in \{0,1\}^n} x(\mathbf{b}) |\mathbf{b}\rangle \stackrel{\text{def}}{=} \sum_{\mathbf{b} \in \{0,1\}^n} \tilde{x}(\mathbf{b}) |\mathbf{b}\rangle \quad \forall (x_0, \dots, x_{2^n-1}) \in \mathbb{C}^{2^n}, \quad (2.19)$$

where¹⁶

$$\left. \begin{aligned} x(\mathbf{b}) &\stackrel{\text{def}}{=} x_{I(\mathbf{b})} \\ \tilde{x}(\mathbf{b}) &\stackrel{\text{def}}{=} \tilde{x}_{I(\mathbf{b})} \end{aligned} \right\} \quad \forall \mathbf{b} \in \{0,1\}^n.$$

Obviously, \hat{F}_n is a linear operator on \mathbb{C}^{2^n} and, therefore,

$$(x(\mathbf{a}) = \delta_{\mathbf{a}, \mathbf{b}} \quad \forall \mathbf{a} \in \{0,1\}^n) \stackrel{(2.16)}{\implies} \left(\tilde{x}(\mathbf{a}) = \frac{1}{\sqrt{2^n}} e^{i I(\mathbf{a}) \frac{2\pi}{2^n} I(\mathbf{b})} \quad \forall \mathbf{a} \in \{0,1\}^n \right)$$

implies¹⁷

$$\begin{aligned} \sqrt{2^n} \hat{F}_n |\mathbf{b}\rangle &= \sum_{\mathbf{a} \in \{0,1\}^n} e^{i I(\mathbf{a}) \frac{2\pi}{2^n} I(\mathbf{b})} |\mathbf{a}\rangle \\ &= \sum_{\mathbf{a} \in \{0,1\}^n} \bigotimes_{\nu=1}^n \left(e^{i 2^{n-\nu} a_\nu \frac{2\pi}{2^n} I(\mathbf{b})} |a_\nu\rangle \right) \quad \forall \mathbf{b} \in \{0,1\}^n. \end{aligned} \quad (2.20)$$

DRAFT, June 26, 2009

¹⁶Recall the definition of $I(\mathbf{b})$ in (1.6).

¹⁷Note the ordering of

$$\bigotimes_{\nu=1}^n \chi_\nu \stackrel{\text{def}}{=} \chi_1 \otimes \dots \otimes \chi_n.$$

The latter implies¹⁸

$$\hat{F}_n |\mathbf{b}\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{\nu=1}^n \left(|0\rangle + e^{i2\pi 2^{-\nu} I(\mathbf{b})} |1\rangle \right) \quad \forall \mathbf{b} \in \{0, 1\}^n. \quad (2.21)$$

Thanks to

$$e^{i2\pi b_\mu 2^{n-\mu-\nu}} = 1 \quad \text{for } \mu \leq n - \nu$$

we may rewrite this as

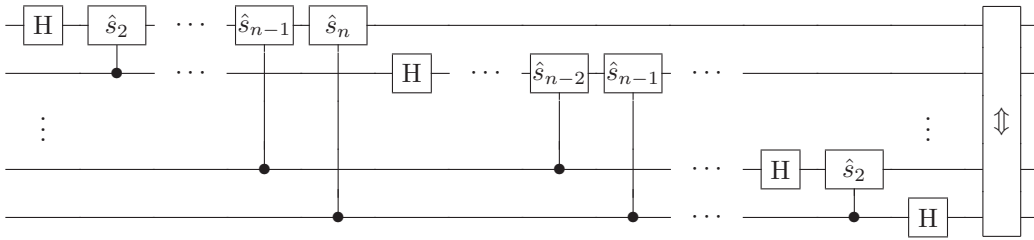
$$\hat{F}_n |\mathbf{b}\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{\nu=1}^n \left(|0\rangle + e^{i2\pi \sum_{\mu=n-\nu+1}^n b_\mu 2^{n-\mu-\nu}} |1\rangle \right) \quad \forall \mathbf{b} \in \{0, 1\}^n \quad (2.22)$$

or as

$$\hat{F}_n |\mathbf{b}\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{\nu=1}^n \left(|0\rangle + \left(\prod_{\alpha=1}^{\nu} e^{i2\pi 2^{-(\alpha-1)} b_{(n-\nu)+\alpha}} \right) |1\rangle \right) \quad \forall \mathbf{b} \in \{0, 1\}^n \quad (2.23)$$

showing, by the way, that \hat{F}_n is isometric.

Exercise 11 Using (2.23), show that the n -qubit network



with

$$\hat{s}_\nu \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^\nu} \end{pmatrix}, \quad \begin{array}{c} |b_1\rangle \\ \vdots \\ |b_n\rangle \end{array} \begin{array}{c} \boxed{\hat{s}_\nu} \\ \updownarrow \\ \boxed{\hat{s}_\nu} \end{array} \begin{array}{c} |b_n\rangle \\ \vdots \\ |b_1\rangle \end{array},$$

implements the quantum FOURIER transform.¹⁹ Moreover, using Corollary 1.2.3, show that

$$\begin{array}{c} \boxed{\hat{s}_\nu} \\ \bullet \end{array} \equiv \begin{array}{c} \boxed{\hat{C}_\nu} \oplus \boxed{\hat{C}_\nu^{-1}} \\ \bullet \quad \bullet \end{array} \begin{array}{c} \oplus \\ \oplus \end{array} \begin{array}{c} \delta_\nu \end{array}$$

holds for $\delta_\nu = -\pi/2^\nu$ and $\hat{C}_\nu = \hat{R}_3(\delta_\nu)$.


DRAFT, June 26, 2009

¹⁸An import special case is $\hat{F}_n |0\rangle = \hat{U}_H^{\otimes n} |0\rangle$.

¹⁹Note that

$$\frac{1}{\sqrt{2}} (|0\rangle + e^{i\pi b} |1\rangle) = \hat{U}_H |b\rangle \quad \forall b \in \{0, 1\}.$$

Remarks:

1. If the crossings  are ignored then the above implementation of the quantum FOURIER transform uses $n/2$ SWAP gates, n HADAMARD gates and $n^2/2$ $\Lambda_1(\hat{s}_\nu)$ gates.
2. Since

$$\begin{aligned} \tilde{x}_{I(\mathbf{a})} &\stackrel{(2.19)}{=} \sum_{\mathbf{b} \in \{0,1\}^n} x_{I(\mathbf{b})} \langle \mathbf{a} | \hat{F}_n \mathbf{b} \rangle \\ &= \sum_{\mathbf{b} \in \{0,1\}^n} x_{I(\mathbf{b})} \langle \hat{F}_n^{-1} \mathbf{a} | \mathbf{b} \rangle \quad \forall \mathbf{a} \in \{0,1\}^n, \end{aligned}$$

the above network implementation for \hat{F}_n yields a nice factorization of the matrix corresponding to the discrete FOURIER transformation. This factorization is the core of the radix-2 version of the **fast FOURIER transform** (FFT) algorithm.²⁰

Exercise 12 Prove the identities²¹

$$\begin{aligned} \sqrt{2} \mathcal{F}_{n'}(0, b_2, \dots, b_n) &= +\mathcal{F}_{n'-1}(b_2, \dots, b_{n'}, 0, b_{n'+1}, \dots, b_n) \\ &\quad + e^{i 2\pi \sum_{\nu=2}^{n'} b_\nu 2^{-\nu}} \mathcal{F}_{n'-1}(b_2, \dots, b_{n'}, 1, b_{n'+1}, \dots, b_n), \\ \sqrt{2} \mathcal{F}_{n'}(1, b_2, \dots, b_n) &= +\mathcal{F}_{n'-1}(b_2, \dots, b_{n'}, 0, b_{n'+1}, \dots, b_n) \\ &\quad - e^{i 2\pi \sum_{\nu=2}^{n'} b_\nu 2^{-\nu}} \mathcal{F}_{n'-1}(b_2, \dots, b_{n'}, 1, b_{n'+1}, \dots, b_n) \end{aligned}$$

for the partial discrete FOURIER transform $\mathcal{F}_{n'}$ defined by

$$(\mathcal{F}_{n'} x)(\mathbf{b}) \stackrel{\text{def}}{=} \sum_{\mathbf{b}' \in \{0,1\}^{n'}} x(b'_1, \dots, b'_{n'}, b_{n'+1}, \dots, b_n) \exp\left(+i 2\pi \sum_{\nu, \nu'=1}^{n'} b_\nu b_{\nu'} 2^{n'-\nu-\nu'}\right)$$

for $n' < n \in \mathbb{N}$ and

$$(\mathcal{F}_n x)(\mathbf{b}) \stackrel{\text{def}}{=} \tilde{x}(\mathbf{b}), \quad (\mathcal{F}_0 x)(\mathbf{b}) \stackrel{\text{def}}{=} x(\mathbf{b}).$$

2.2.3 Quantum Order Finding

———— DRAFT, June 26, 2009 ————

²⁰See, e.g., (Brigham, 1974; Nussbaumer, 1982).

²¹Let us point out that

$$e^{i 2\pi \sum_{\nu=2}^{n'} b_\nu 2^{-\nu}} = e^{i \pi \frac{I(b_2, \dots, b_{n'})}{2^{n'-1}}} \quad \forall b_2, \dots, b_{n'} \in \{0,1\}.$$

As already mentioned at the end of 2.2.1, to find the order (2.14) of a given integer $x \in \{2, \dots, N-1\}$, SHOR suggested to exploit the effectively implementable²² state

$$\begin{aligned} \Psi_{\text{Shor}} &\stackrel{\text{def}}{=} \frac{1}{2^L} \sum_{a=0}^{2^{2L}-1} \left(\hat{F}_{2^L} |a\rangle_{2^L} \right) \otimes |x^a \pmod{N}\rangle_L \\ &\stackrel{(2.19),(2.16)}{=} \frac{1}{2^{2L}} \sum_{a,c=0}^{2^{2L}-1} e^{i a \frac{2\pi}{2^{2L}} c} |c\rangle_{2^L} \otimes |x^a \pmod{N}\rangle_L . \end{aligned}$$

where

$$L \stackrel{\text{def}}{=} \min \{ l \in \mathbb{N} : N \leq 2^l \} .$$

The essential point is the following:

$$x^a \pmod{N} = x^{a'} \pmod{N} \iff a' = a \pmod{r} .$$

Therefore,

$$\begin{aligned} p(a, c) &\stackrel{\text{def}}{=} \left| \left\langle |c\rangle_{2^L} \otimes |x^a \pmod{N}\rangle_L \mid \Psi_{\text{Shor}} \right\rangle \right|^2 \\ &= \frac{1}{2^{4L}} \left| \sum_{a' \in M_a} e^{i a' \frac{2\pi}{2^{2L}} c} \right|^2 \quad \forall a, c \in \{0, \dots, 2^{2L}-1\} , \end{aligned}$$

where

$$M_a \stackrel{\text{def}}{=} \left\{ a' \in \{0, \dots, 2^{2L}-1\} : a' = a \pmod{r} \right\} ,$$

is negligible unless all the phases

$$2\pi \frac{b r c}{2^{2L}} \pmod{2\pi} \in [0, 2\pi)$$

with

$$b \in \left\{ 0, \dots, \left\lfloor (2^{2L}-1 - \min M_a) / r \right\rfloor \right\} ,$$

are predominantly almost the same, i.e. (assuming L sufficiently large) unless

$$[0, 2\pi) \ni 2\pi \frac{r c}{2^{2L}} \pmod{2\pi} = O\left(\frac{r}{2^{2L}}\right) .$$

The latter means that²³

$$\left| \frac{c}{2^{2L}} - \frac{d}{r} \right| = O\left(\frac{1}{2^{2L}}\right)$$

holds for some integer d .

———— DRAFT, June 26, 2009 ————

²²See also (Coppersmith, 1994), in this connection.

²³If, by chance, r divides 2^{2L} then b runs from 0 to $\frac{2^{2L}}{r} - 1$ and, therefore, an adaption of (2.17) shows that $p(a, c)$ vanishes exactly unless $\frac{r c}{2^{2L}} = d$ holds for some integer d .

More precisely, one can show:²⁴

A projective measurement of Ψ_{Shor} w.r.t. the computational basis is likely to find the first $2L$ -qubit register in a state $|c\rangle_{2L}$ with

$$\left| \frac{c}{2^{2L}} - \frac{d}{r} \right| \leq \frac{1}{2r^2}, \quad \gcd(d, r) = 1 \quad (2.24)$$

being fulfilled for integer d .

If we have found a fraction $c/2^{2L}$ fulfilling (2.24) for some (unknown) integer d with $\gcd(c, d) = 1$, then r may be efficiently determined using the continued fraction algorithm:²⁵

The motivation for the definition (2.7) — given $n_0, n_1 \in \mathbb{N}$ — is the observation that

$$\frac{n_\nu}{n_{\nu+1}} = \left\lfloor \frac{n_\nu}{n_{\nu+1}} \right\rfloor + \frac{1}{n_{\nu+1} \underbrace{\left(n_\nu - n_{\nu+1} \left\lfloor \frac{n_\nu}{n_{\nu+1}} \right\rfloor \right)}_{\text{remainder}}} \quad \forall n_\nu, n_{\nu+1} \in \mathbb{N}$$

since, then, we have

$$\begin{aligned} \frac{n_0}{n_1} &= \left\lfloor \frac{n_0}{n_1} \right\rfloor + \frac{1}{\left(\frac{n_1}{n_2} \right)} \\ &= \left\lfloor \frac{n_0}{n_1} \right\rfloor + \frac{1}{\left\lfloor \frac{n_1}{n_2} \right\rfloor + \frac{1}{\left(\frac{n_2}{n_3} \right)}} \\ &= \left\lfloor \frac{n_0}{n_1} \right\rfloor + \frac{1}{\left\lfloor \frac{n_1}{n_2} \right\rfloor + \frac{1}{\left\lfloor \frac{n_2}{n_3} \right\rfloor + \frac{1}{\left(\frac{n_3}{n_4} \right)}}} \\ &\quad \text{etc.,} \end{aligned}$$

hence the continued fraction expansion²⁶

$$\frac{n_0}{n_1} = \left\lfloor \frac{n_0}{n_1} \right\rfloor + \sum_{\mu=1}^{\nu-2} \frac{1}{\left\lfloor \frac{n_\mu}{n_{\mu+1}} \right\rfloor} + \frac{1}{\left\lfloor \frac{n_{\nu-1}}{n_\nu} \right\rfloor} \quad \forall \nu \in \{1, \dots, s\} \quad (2.25)$$

with s given by (2.8).

———— DRAFT, June 26, 2009 ————

²⁴See (Shor, 1997, Section 5) for details and Appendix A.3 for an improved search algorithm. Note that $r \leq \varphi(N) < N$.

²⁵Otherwise the prescription will yield an integer r' that fails the test $x^{r'} = 1 \pmod{N}$ almost certainly. Then the whole procedure has to be repeated.

²⁶Note that the continued fraction expansion does not change if n_0 and n_1 are replaced by $n'_0 = pn_0$ and $n'_1 = pn_1$, where $p \in \mathbb{N}$.

Remark: Formally, i.e. without specification of the a_μ and b_μ , finite *continued fractions*²⁷

$$b_0 + \frac{a_1}{|b_1|} + \frac{a_2}{|b_2|} + \dots + \frac{a_\nu}{|b_\nu|},$$

are recursively defined by

$$b_0 + \frac{a_1}{|b_1|} \stackrel{\text{def}}{=} b_0 + \frac{a_1}{b_1}$$

and

$$b_0 + \frac{a_1}{|b_1|} + \frac{a_2}{|b_2|} + \dots + \frac{a_{\nu+1}}{|b_{\nu+1}|} \stackrel{\text{def}}{=} b_0 + \frac{a_1}{|b_1|} + \frac{a_2}{|b_2|} + \dots + \frac{a_\nu}{\left|b_\nu + \frac{a_{\nu+1}}{b_{\nu+1}}\right|}.$$

Due to

$$n_{\nu+1} \neq 0 \quad \stackrel{(2.7)}{\implies} \quad n_{\nu+2} < n_{\nu+1} < n_{\nu+1}$$

s must be finite and fulfill the equation $\left\lfloor \frac{n_{s-1}}{n_s} \right\rfloor = \frac{n_{s-1}}{n_s}$. Since

$$\gcd(n_{\nu-1}, n_\nu) \neq 0 \quad \iff \quad \gcd(n_{\nu+1}, n_\nu)$$

we see that $\gcd(n_0, n_1)$ divides n_s and that n_s , dividing n_{s-1} , also divides n_0 and n_1 . Hence (2.8) holds, indeed.

Given $c, L \in \mathbb{N}$ fulfilling (2.24), the set of possible fractions $\frac{d}{c}$ is strongly restricted by the following lemma.

Lemma 2.2.3 *Given $n_0, n_1, d, r \in \mathbb{N}$ fulfilling*

$$\left| \frac{n_0}{n_1} - \frac{d}{r} \right| < \frac{1}{2r^2},$$

using definition (2.7) and (2.8), we have²⁸

$$\frac{d}{r} = \left\lfloor \frac{n_0}{n_1} \right\rfloor + \sum_{\mu=1}^t \frac{1}{\left\lfloor \frac{n_\mu}{n_{\mu+1}} \right\rfloor}$$

for some $t \in \{1, \dots, s-1\}$.

Proof: See (Nielsen and Chuang, 2001, Theorem A4.16). ■

———— DRAFT, June 26, 2009 ————

²⁷See, e.g., (Perron, 1954; Perron, 1957) or (Brezinski, 1991) for the general theory of continued fractions. See also (Baladi and Vallee, 2003).

²⁸Note, however, that

$$a_t = 1 \quad \implies \quad \sum_{\mu=1}^t \frac{1}{|a_\mu|} = \sum_{\mu=1}^{t-1} \frac{1}{|a_\mu|} + \frac{1}{|a_{t-1} + 1|} \quad \forall a_0, \dots, a_t \in \mathbb{N}.$$

Therefore, using (2.7) for

$$n_0 = c, \quad n_1 = 2^{2L}$$

and determining — for $t = 1, 2, \dots, s$ — the numbers $A_t, B_t \in \mathbb{N}$ characterized by

$$\left\lfloor \frac{n_0}{n_1} \right\rfloor + \sum_{\mu=1}^t \frac{1}{\left\lfloor \frac{n_\mu}{n_{\mu+1}} \right\rfloor} = \frac{A_t}{B_t} \quad \gcd(A_t, B_t) = 1,$$

we have

$$\boxed{r = B_t \text{ for some } t \leq s.}$$

Also these A_t, B_t can be efficiently determined via EUCLID's algorithm:

If

$$b_0 + \frac{a_1}{|b_1|} + \frac{a_2}{|b_2|} + \dots + \frac{a_n}{|b_n|},$$

is well-defined then

$$b_0 + \sum_{\mu=1}^{\nu+1} \frac{a_\mu}{|b_\mu|} = b_0 + \sum_{\mu=1}^{\nu-1} \frac{a_\mu}{|b_\mu|} + \frac{a_\nu b_{\nu+1}}{|b_\nu b_{\nu+1} + a_{\nu+1}|} \quad \forall \nu = 1, \dots, n-1$$

and, therefore,

$$b_0 + \frac{a_1}{|b_1|} + \frac{a_2}{|b_2|} + \dots + \frac{a_\nu}{|b_\nu|} = \frac{A_\nu(a_1, \dots, a_\nu; b_0, \dots, b_\nu)}{B_\nu(a_1, \dots, a_\nu; b_0, \dots, b_\nu)} \quad \forall \nu = 1, \dots, n,$$

if the A_ν and B_ν are recursively defined by²⁹

$$\left. \begin{aligned} A_\nu &\stackrel{\text{def}}{=} b_\nu A_{\nu-1} + a_\nu A_{\nu-2} \\ B_\nu &\stackrel{\text{def}}{=} b_\nu B_{\nu-1} + a_\nu B_{\nu-2} \end{aligned} \right\} \text{ for } \nu = 1, 2, \dots, n,$$

where

$$A_{-1} \stackrel{\text{def}}{=} 1, \quad A_0 \stackrel{\text{def}}{=} b_0, \quad B_{-1} \stackrel{\text{def}}{=} 0, \quad B_0 \stackrel{\text{def}}{=} 1.$$

Fortunately, these definitions also imply

$$\left. \begin{aligned} a_\mu = 1 \quad \forall \mu \in \{1, \dots, n\} \\ b_\mu \in \mathbb{N} \quad \forall \mu \in \{0, \dots, n\} \end{aligned} \right\} \implies \gcd(A_\nu, B_\nu) = 1 \quad \forall \nu \in \{1, \dots, n\}.$$

Outline of proof:

$$\begin{aligned} A_{\nu+1} B_\nu &= b_{\nu+1} A_\nu B_\nu + A_{\nu-1} B_\nu \\ &= b_{\nu+1} A_\nu B_\nu + A_{\nu-1} B_{\nu-2} + b_\nu A_{\nu-1} B_{\nu-1} \end{aligned}$$

———— DRAFT, June 26, 2009 ————

²⁹Thus

$$(b_\nu b_{\nu+1} + a_{\nu+1}) A_{\nu-1} + (a_\nu b_{\nu+1}) A_{\nu-2} = b_{\nu+1} A_\nu + a_{\nu+1} A_{\nu-1}$$

and similarly for the B_μ .

and the corresponding equation with A, B interchanged imply

$$A_{\nu+1} B_{\nu} - B_{\nu+1} A_{\nu} = -(A_{\nu} B_{\nu-1} - B_{\nu} A_{\nu-1}).$$

By induction, starting from

$$A_0 B_{-1} - B_0 A_{-1} = -1,$$

this gives

$$A_{\nu} B_{\nu-1} - B_{\nu} A_{\nu-1} = (-1)^{\nu+1} \quad \forall \nu \in \{0, \dots, n\}. \quad (2.26)$$

In case

$$A_{\nu} = d_{\nu} c_{\nu}, \quad B_{\nu} = e_{\nu} c_{\nu}$$

the positive integer c_{ν} would divide the l.h.s. of (2.26), hence also the r.h.s. The latter, however, is only possible for $c_{\nu} = 1$.

Example³⁰ $N = 899$, $L = 10$: If, for instance, the projective measurement gives $|267137\rangle_{2L}$ for the first $2L$ qubits, then we get³¹

$$\begin{aligned} \frac{c}{2^{2L}} &= [0, 3, 1, 12, 2, 1, 1, 1, 26, 1, 1, 22, 2] \\ &\stackrel{\text{def}}{=} 0 + \frac{1|}{|3} + \frac{1|}{|1} + \frac{1|}{|12} + \frac{1|}{|2} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|26} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|22} + \frac{1|}{|2} \end{aligned}$$

and succeed with $t = 7$:

$$[0, 3, 1, 12, 2, 1, 1, 1] = \frac{107}{420} = \frac{d}{r},$$

i.e. testing $r = 420$, we get³² the factors

$$\gcd(11^{210} + 1, 899) = 29, \quad \gcd(11^{210} - 1, 899) = 31 = \frac{899}{29}.$$

If, for instance, we unfortunately measure $c = 801411$ then we get

$$\frac{801411}{2^{20}} = [0, 1, 3, 4, 7, 1, 80, 1, 1, 7, 6]$$

with the subconvergent

$$[0, 3, 4, 7, 1] = \frac{107}{140} \left(= \frac{321}{420} \right).$$

In this case, although the condition

$$\left| \frac{c}{2^{2L}} - \frac{d}{r} \right| \leq \frac{1}{2r^2}$$

(but **not** $\gcd(d, r) = 1$) is fulfilled (with $d = 321$) $r = 420$ will presumably not be detected and the whole procedure will be repeated, maybe with a different random value for x .

³⁰Compare (Rosé et al., 2004, Section III).

³¹In Maple, after the command "with(numtheory);" this result will be produced by the command "convert(267137/2²⁰, cfrag);" and the *subconvergent* $[0, 3, 1, 12, 2, 1, 1, 1]$ can be evaluated by the command "nthconver([0, 3, 1, 12, 2, 1, 1, 1], 7);".

³²E.g., by the Maple commands "gcd(11²¹⁰, 899);" and "gcd(11²¹⁰, 899);".

Chapter 3

Physical Realizations of Quantum Gates¹

A set of necessary conditions to be fulfilled for the physical implementation of quantum computation is given by DIVINCENZO's *checklist* (DiVincenzo, 2000; Perez-Delgado and Kok, 2009):

1. Qubits have to be well characterized and *scalable*.²
2. The standard states $|0, \dots, 0\rangle$ must be preparable.³
3. The duration of a gate operation must be much smaller than the *decoherence time*.
4. A universal set of gates must be implementable.
5. The qubits must be *measurable* in order to be able to 'read out the result' of a quantum computation.

Remark: For quantum communication the following two requirements have to be added:

- It must be possible to convert static qubits into *flying qubits* (typically photons).
- It must be possible to protect flying qubits against decoherence.

3.1 Quantum Optical Implementations

Optical systems currently constitute the only realistic proposal for long-distance quantum communication and underly implementations of quantum cryptography.

(Knill et al., 2001)

DRAFT, June 26, 2009

¹See the special volume *Fortschr. Phys.* **48** (2000) No. 9–11.

²Thus, 1-photon realizations of n-qubit systems should be considered as *qudits* with $d = 2^n$ rather than n-qubit systems proper.

³This is still difficult for n -photon systems.

3.1.1 Photons

In the COULOMB *gauge* the free electromagnetic field $\mathbf{E}(\mathbf{x}, t)$, $\mathbf{B}(\mathbf{x}, t)$ is given in the form

$$\mathbf{B}(\mathbf{x}, t) = \text{curl } \mathbf{A}(\mathbf{x}, t), \quad \mathbf{E}(\mathbf{x}, t) = -\frac{\partial}{\partial t} \mathbf{A}(\mathbf{x}, t),$$

$$\mathbf{A}(\mathbf{x}, t) = \mathbf{A}^{(+)}(\mathbf{x}, t) + (\mathbf{A}^{(+)}(\mathbf{x}, t))^*$$

by some complex vector potential

$$\mathbf{A}^{(+)}(\mathbf{x}, t) = \int \left(\sum_{j=1}^2 \boldsymbol{\epsilon}_j(\mathbf{k}) \check{f}_j(\mathbf{k}) \right) e^{-i(c|\mathbf{k}|t - \mathbf{k} \cdot \mathbf{x})} \frac{d\mathbf{k}}{\sqrt{2|\mathbf{k}|}},$$

where, for every $\mathbf{k} \neq 0$, the vectors $\boldsymbol{\epsilon}_j(\mathbf{k})$ form a

$$\text{right handed orthonormal basis } \left\{ \boldsymbol{\epsilon}_1(\mathbf{k}), \boldsymbol{\epsilon}_2(\mathbf{k}), \frac{\mathbf{k}}{|\mathbf{k}|} \right\}$$

and thus guarantee $\text{div } \mathbf{A}^{(+)} = 0$.

Remark: We use SI conventions; see Appendix A.3.3 of (Lücke, edyn).

In the HEISENBERG picture of the quantized theory the classical fields $\mathbf{E}(\mathbf{x}, t)$ and $\mathbf{B}(\mathbf{x}, t)$ have to be replaced by corresponding observables on the state space $\mathcal{H}_{\text{field}}$, i.e. by operator-valued (generalized) functions $\hat{\mathbf{E}}(\mathbf{x}, t)$ and $\hat{\mathbf{B}}(\mathbf{x}, t)$ to be interpreted in the following way:

If $\Phi \in \mathcal{H}_{\text{field}}$ is a sufficiently well-behaved (and $\|\Phi\| = 1$) then

$$\langle \Phi | \hat{\mathbf{E}}(\mathbf{x}, t) \Phi \rangle \quad \text{resp.} \quad \langle \Phi | \hat{\mathbf{B}}(\mathbf{x}, t) \Phi \rangle$$

is the expectation value for $\mathbf{E}(\mathbf{x}, t)$ resp. $\mathbf{B}(\mathbf{x}, t)$ in the HEISENBERG state (corresponding to) Φ .

Up to unitary equivalence these observables are given by

$$\hat{\mathbf{B}}(\mathbf{x}, t) = \text{curl } \hat{\mathbf{A}}(\mathbf{x}, t), \quad \hat{\mathbf{E}}(\mathbf{x}, t) = -\frac{\partial}{\partial t} \hat{\mathbf{A}}(\mathbf{x}, t),$$

$$\hat{\mathbf{A}}(\mathbf{x}, t) = \hat{\mathbf{A}}^{(+)}(\mathbf{x}, t) + \left(\hat{\mathbf{A}}^{(+)}(\mathbf{x}, t) \right)^\dagger,$$

where⁴

$$\hat{\mathbf{A}}^{(+)}(\mathbf{x}, t) \stackrel{\text{def}}{=} (2\pi)^{-3/2} \sqrt{\mu_0 \hbar c} \int \left(\sum_{j=1}^2 \boldsymbol{\epsilon}_j(\mathbf{k}) \hat{a}_j(\mathbf{k}) \right) e^{-i(c|\mathbf{k}|t - \mathbf{k} \cdot \mathbf{x})} \frac{d\mathbf{k}}{\sqrt{2|\mathbf{k}|}} \quad (3.1)$$

and the $\hat{a}_j(\mathbf{k})$ are **annihilation operators**⁵ fulfilling the commutation relations⁶

$$[\hat{a}_j(\mathbf{k}), \hat{a}_{j'}(\mathbf{k}')]_- = 0, \quad [\hat{a}_j(\mathbf{k}), (\hat{a}_{j'}(\mathbf{k}'))^\dagger]_- = \delta_{jj'} \delta(\mathbf{k} - \mathbf{k}') \quad (3.2)$$

on a suitable dense subspace D_0 of the HILBERT space \mathcal{H} containing a cyclic normalized **vacuum** state vector Ω characterized (up to a constant phase factor) by

$$\hat{a}_j(\mathbf{k}) \Omega = 0 \quad (3.3)$$

(in the distributional sense). This also fixes the inner product on \mathcal{H} .

The operators \hat{a} of the form

$$\hat{a} = \sum_{j=1,2} \int \hat{a}_j(\mathbf{k}) (\check{f}_j(\mathbf{k}))^* d\mathbf{k}, \quad \check{f}_1, \check{f}_2 \in L^2(\mathbb{R}^3) \quad (3.4)$$

with⁷

$$[\hat{a}, \hat{a}^\dagger]_- = \hat{1} \quad (3.5)$$

characterize **modes** of the quantized electromagnetic field corresponding to the classical complex vector potentials

$$\begin{aligned} \mathbf{A}^{(+)}(\mathbf{x}, t) &= \left\langle \left(\hat{\mathbf{A}}^{(+)}(\mathbf{x}, t) \right)^\dagger \Omega \left| \hat{a}^\dagger \Omega \right\rangle \\ &= \left\langle \Omega \left| \left[\hat{\mathbf{A}}^{(+)}(\mathbf{x}, t), \hat{a}^\dagger \right]_- \Omega \right\rangle \\ &\stackrel{(3.4), (3.1), (3.2)}{=} (2\pi)^{-3/2} \sqrt{\mu_0 \hbar c} \int \left(\sum_{j=1}^2 \boldsymbol{\epsilon}_j(\mathbf{k}) \check{f}_j(\mathbf{k}) \right) e^{-i(c|\mathbf{k}|t - \mathbf{k} \cdot \mathbf{x})} \frac{d\mathbf{k}}{\sqrt{2|\mathbf{k}|}}. \end{aligned} \quad (3.6)$$

— DRAFT, June 26, 2009 —

⁴Thanks to the special choice of the factor in front of the integral we get the desired expression

$$\hat{H} = \frac{1}{2} \int \left(\epsilon_0 : \hat{\mathbf{E}}(\mathbf{x}, t) \cdot \hat{\mathbf{E}}(\mathbf{x}, t) : + \frac{1}{\mu_0} : \hat{\mathbf{B}}(\mathbf{x}, t) \cdot \hat{\mathbf{B}}(\mathbf{x}, t) : \right) d\mathbf{x}$$

for the HAMILTON operator, characterized (up to an additive constant) by

$$\frac{\partial}{\partial t} \hat{\mathbf{A}}^{(+)}(\mathbf{x}, t) = \frac{i}{\hbar} \left[\hat{H}, \hat{\mathbf{A}}^{(+)}(\mathbf{x}, t) \right]_-.$$

⁵See (Mizrahi and Dodonov, 2002), however.

⁶Of course, the notation \dagger includes the requirement

$$\langle \Phi | \hat{a}_j(\mathbf{k}) \Phi' \rangle = \left\langle \left(\hat{a}_j(\mathbf{k}) \right)^\dagger \Phi \left| \Phi' \right\rangle \right.$$

⁷Condition (3.5) is equivalent to $\|\hat{a}^\dagger \Omega\| = 1$.

With these modes the subspaces $\mathcal{H}^{(n)} \subset \mathcal{H}$ of n -**photon** state vectors may be defined recursively by

$$\mathcal{H}^{(0)} \stackrel{\text{def}}{=} \{\lambda \Omega : \lambda \in \mathbb{C}\}$$

and

$$\mathcal{H}^{(n+1)} \stackrel{\text{def}}{=} \{\hat{a}^\dagger \Phi^{(n)} : \Phi^{(n)} \in \mathcal{H}^{(n)}, \hat{a} \text{ mode}\} \quad \text{for } n = 0, 1, 2, \dots$$

Physical characterization of n -photon states: n (ideal) detectors but no more can be made fire by an incoming n -photon state.

Modes \hat{a}_ν, \hat{a}_μ are called **orthogonal**, iff the states $\hat{a}_\nu^\dagger \Omega, \hat{a}_\mu^\dagger \Omega$ are orthogonal, i.e. iff $[\hat{a}_\nu, \hat{a}_\mu]_- = 0$.

Fortunately, already classical electrodynamics tells us how photons are affected by passive linear optical components:

The change of the mode \hat{a} of a photon, caused by a passive linear optical component, is such that the corresponding complex vector potential changes as predicted by classical electrodynamics.

3.1.2 Photonic n -Qubit Systems

Single-Photon Realization

For every $n \in \mathbb{N}$, using sufficiently many beam splitters a single-photon state $\hat{a}^\dagger \Omega$ can be changed into a coherent superposition⁸

$$\sum_{\mathbf{b} \in \{0,1\}^n} \lambda_{\mathbf{b}} \hat{a}_{\mathbf{b}}^\dagger \Omega$$

of (essentially) orthogonal 1-photon states

$$|\mathbf{b}\rangle \stackrel{\text{def}}{=} \hat{a}_{\mathbf{b}}^\dagger \Omega$$

which may be chosen as elements of the computational basis of a (simulated) n -qubit system.

Remarks:

1. Since the single qubits of the 1-photon realization cannot exist independently from each other we should better call the system a qu2ⁿit system.

———— DRAFT, June 26, 2009 ————

⁸For the special case $n = 3$ an example is illustrated in Figure 3.1.

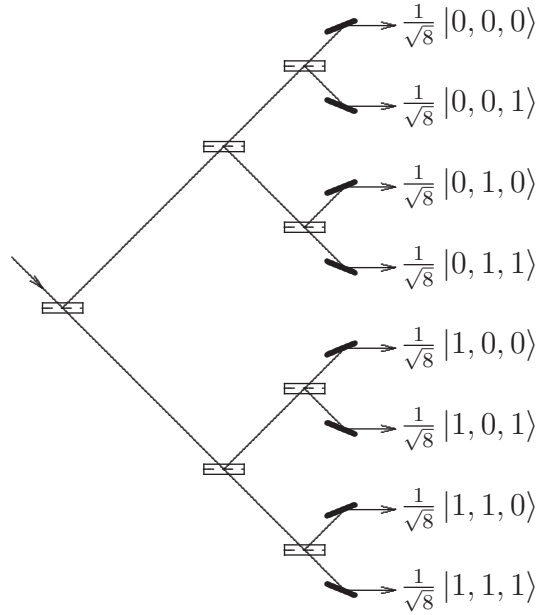


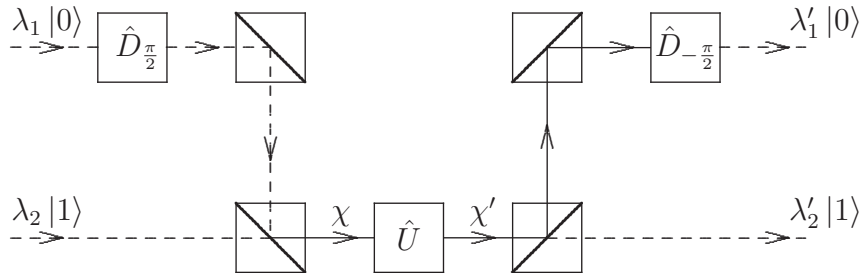
Figure 3.1: Preparation of $\Phi_0^{(3)}$ in a single-photon realization.

2. Cascades of beam splitters may also be used to implement approximate measurement of the number of photons:⁹

E.g., replace the single-photon input in Figure 3.1 by a 2-photon state and direct the output rays into separate ideal detectors. Then the probability that exactly two of these detectors ‘fire’ is $15/16$ ($\approx 94\%$).

For such a choice of computational bases all unitary transformations can be (essentially) effected by linear optical components. Thanks to Theorem 1.2.1 it is sufficient to show this for $n = 1$:

Assume, for instance, that that $|0\rangle$ and $|1\rangle$ describe horizontally polarized (almost monochromatic) photons. Then the 1-qubit gates may be implemented by linear optical elements corresponding to JONES matrices \hat{U} in the following way:



All unitary transformations of the polarization state of a photon (with almost sharp momentum) can be (almost accurately) performed by proper use of only $\lambda/2$ -blades

DRAFT, June 26, 2009

⁹See (Bartlett et al., 2002) for details. See also (Haderka et al., 2004; Waks et al., 2003).

and polarization-dependent phase shifters.

General remark: Instead of performing the n -qubit transformations $\hat{U}_{(n)}$ one may choose a fixed n -qubit transformation $\hat{V}_{(n)}$ perform the n -qubit transformations $\hat{U}_{(n)}\hat{V}_{(n)}$ and interpret the result w.r.t. the new computational bases $\{|\mathbf{b}'\rangle \stackrel{\text{def}}{=} \hat{V}_{(n)}|\mathbf{b}\rangle : \mathbf{b} \in \{0,1\}^n\}$. Usually, in practice, this freedom is tacitly made use of.

Exercise 13 Consider the single-photon realization of a 2-qubit system with:

$$\begin{aligned} \hat{a}_{I(0,0)} &\hat{=} \begin{cases} \text{upper path and} \\ \text{vertical polarization,} \end{cases} \\ \hat{a}_{I(0,1)} &\hat{=} \begin{cases} \text{upper path and} \\ \text{horizontal polarization,} \end{cases} \\ \hat{a}_{I(1,0)} &\hat{=} \begin{cases} \text{lower path and} \\ \text{vertical polarization,} \end{cases} \\ \hat{a}_{I(1,1)} &\hat{=} \begin{cases} \text{lower path and} \\ \text{horizontal polarization.} \end{cases} \end{aligned}$$

- a) Show that the CNOT gate may be implemented by placing a 90° polarization rotator into the lower path.
- b) Show that the TCNOT gate may be implemented by applying a polarization beam splitter — reflecting the vertically polarized components and transmitting the horizontally polarized components — in the following way:

$$\begin{array}{ccc} \alpha_{00}|0,0\rangle + \alpha_{01}|0,1\rangle \longrightarrow & \begin{array}{c} \text{---} \diagup \quad \diagdown \text{---} \\ \text{---} \diagdown \quad \diagup \text{---} \\ \text{---} \diagup \quad \diagdown \text{---} \\ \text{---} \diagdown \quad \diagup \text{---} \end{array} & \longrightarrow \alpha_{00}|0,0\rangle + \alpha_{11}|0,1\rangle \\ \alpha_{10}|1,0\rangle + \alpha_{11}|1,1\rangle \longrightarrow & & \longrightarrow \alpha_{10}|1,0\rangle + \alpha_{01}|1,1\rangle . \end{array}$$

The single-photon ‘realization’ has a serious disadvantage spoiling the eventual speed-up of quantum computation:

The number of optical devices required for the single-photon simulation of n -qubit systems grows exponentially with n (Cerf et al., 1998; Kwiat et al., 2000).

Therefore, we will consider only many-photon realizations in the following.

Multi-Photon Realization

For given $n \in \mathbb{N}$ we may choose a fixed¹⁰ set

$$\left\{ \hat{a}_{\nu,j} : \nu \in \{1, \dots, n\}, j \in \{0, 1\} \right\}$$

of 2^n pairwise orthogonal modes and consider the n -photon states

$$|\mathbf{b}\rangle \stackrel{\text{def}}{=} \hat{a}_{1,b_1}^\dagger \cdots \hat{a}_{n,b_n}^\dagger \Omega \quad \forall \mathbf{b} \in \{0, 1\}^n$$

as elements of the computational basis of a true n -qubit system.¹¹

Here, while the 1-qubit gates may still be easily implemented by linear optical components, the physical realization of universal 2-qubit gates is quite a technological challenge.¹²

FOCK Realization

Another possibility is to choose some fixed set $\{\hat{a}_1, \dots, \hat{a}_n\}$ of pairwise orthogonal modes and consider the states

$$|\mathbf{b}\rangle = |\mathbf{b}\rangle^{\text{F}} \quad \forall \mathbf{b} \in \{0, 1\}^n, \quad (3.7)$$

where

$$|\nu_1, \dots, \nu_n\rangle^{\text{F}} \stackrel{\text{def}}{=} \frac{1}{\sqrt{\nu_1! \cdots \nu_n!}} \left(\hat{a}_1^\dagger \right)^{\nu_1} \cdots \left(\hat{a}_n^\dagger \right)^{\nu_n} \Omega \quad \forall \nu_1, \dots, \nu_n \in \mathbb{Z}_+, \quad (3.8)$$

as elements of the computational basis of the n -qubit system.

The states $\hat{a}_{\mathbf{b}}^\dagger \Omega$ of the single-photon realization for n -qubit systems form the subset

$$\left\{ |\mathbf{b}\rangle^{\text{F}} : b_1 + \dots + b_n = 1 \right\}$$

of the computational basis of the FOCK realization for 2^n -qubit systems using the 2^n modes

$$\hat{a}_{I(\mathbf{b})+1} = \hat{a}_{\mathbf{b}}, \quad \mathbf{b} \in \{0, 1\}^n.$$

Obviously, for $n=1$ the FOCK realization does **not** coincide with the single-photon realization. Actually, 1-qubit gates like the HADAMARD gate cannot be implemented by linear optical components, since $|0\rangle^{\text{F}}$ represents the vacuum state. Nevertheless, the FOCK realization has certain advantages as, e.g., those to be discussed in 3.1.4.

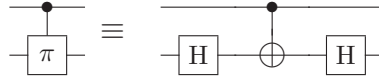
¹⁰Recall the above general remark, however.

¹¹Of course, for $n = 1$ the n -photon realization coincides with the single-photon realization.

¹²Concerning recent progress in detector technologies see (Rosenberg et al., 2005).

3.1.3 Nonlinear Optics Quantum Gates

For both the n -photon and the FOCK realization of n -qubit systems the (universal) CPHASE gate $\Lambda_1(\hat{S}_\pi)$



is *nonlinear* in the sense that — contrary to the action of linear optics components — the modes are not transformed independently of each other.

If a *non-linear sign gate* NS is available,¹³ i.e. an optical one-way gate acting according to¹⁴

$$(\alpha (\hat{a}^*)^0 + \beta (\hat{a}^*)^1 + \gamma (\hat{a}^*)^2) \Omega \rightarrow \boxed{\text{NS}} \rightarrow (\alpha (\hat{a}^*)^0 + \beta (\hat{a}^*)^1 - \gamma (\hat{a}^*)^2) \Omega$$

then the CPHASE gate can be easily implemented by proper use of linear optical components like the HADAMARD *beam splitters* (with deflecting mirrors) characterized in Figure 3.2.

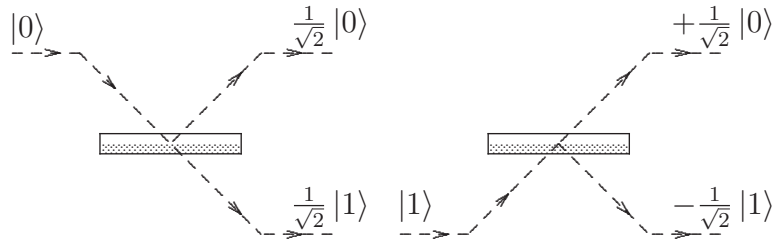


Figure 3.2: HADAMARD beam splitter.

One such implementation,¹⁵ suggested in (Ralph et al., 2002), is sketched in Figure 3.3. The essential idea is exploiting *two-photon interference* (see Section 5.2.3 of (Lücke, nlqo)) at two HADAMARD beam splitters forming a balanced MACH-ZEHNDER interferometer as sketched in Figure 3.4.

One would like to realize the necessary NS gates by means of optical nonlinearities. Unfortunately, sufficiently strong nonlinearities of crystals are accompanied by too strong absorption and therefore are not suitable. A way out may eventually be

DRAFT, June 26, 2009

¹³See (Sanaka et al., 2003) for an experimental realization.

¹⁴The gate is non-linear in the sense that its action cannot be reduced to a linear transformation of the modes \hat{a} .

¹⁵The modes $\hat{a}_{\nu,\mu}$ are assumed to differ only by vertical translation and to describe photons with (almost) sharp momenta.

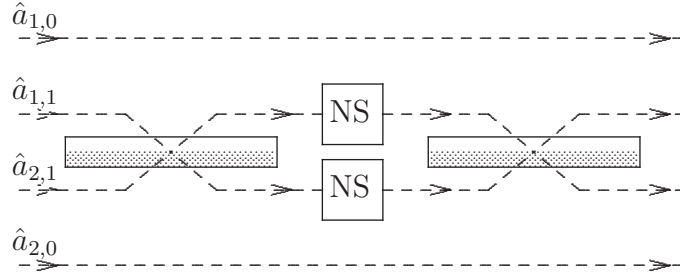


Figure 3.3: Optical implementation of a CPHASE gate.

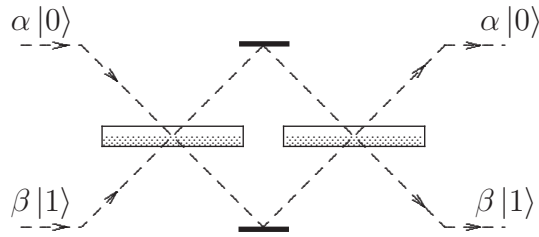
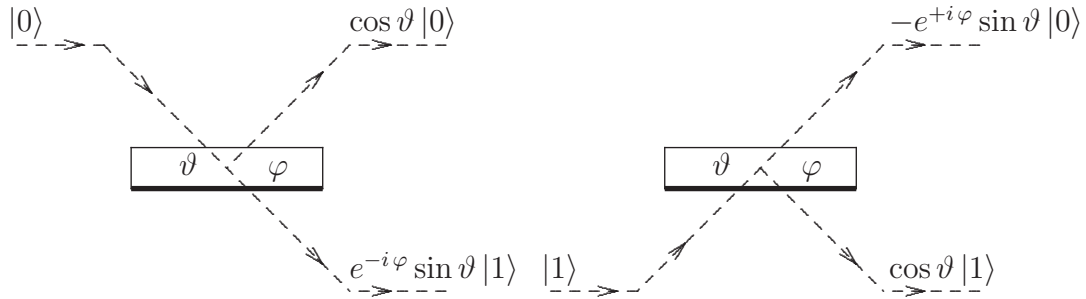


Figure 3.4: Action of a balanced MACH-ZEHNDER interferometer.

provided by electromagnetically induced transparency¹⁶ (EIT), discussed in Section 8.3.2 of (Lücke, nlqo).

Using beam splitters characterized by



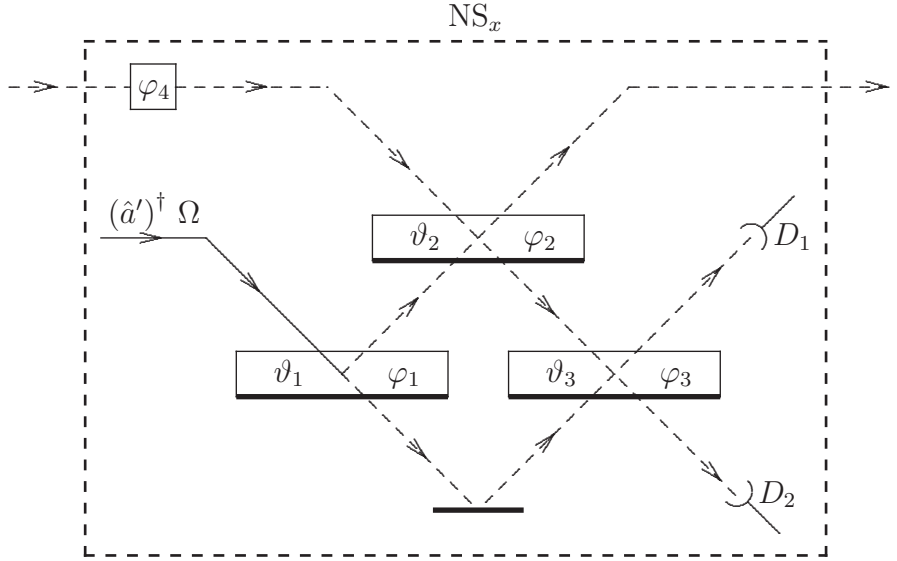
indeterministic¹⁷ NS_x-gates, i.e. gates acting according to

$$\left(\alpha \hat{1} + \beta \hat{a}^\dagger + \gamma (\hat{a}^\dagger)^2\right) \Omega \quad \mapsto \quad \left(\alpha \hat{1} + \beta \hat{a}^\dagger + x \gamma (\hat{a}^\dagger)^2\right) \Omega$$

DRAFT, June 26, 2009

¹⁶See (Ottaviani et al., 2006) and concluding discussion of (Munro et al., 2005a). See also (Munro et al., 2005b) concerning the use of ‘weak’ cross KERR nonlinearities.

¹⁷A gate is called *indeterministic* if it acts correctly with nonzero probability < 1 not depending on the input state and if, after its action, it is known whether the action was correct or not. An indeterministic gate is called *near-deterministic* if its probability of success is near to 1.

Figure 3.5: An indeterministic NS_x -gate

if successful, can be implemented¹⁸ as sketched in Figure 3.5. According to (Knill et al., 2001, Fig. 1) these gates act successfully iff a single-photon state is detected by D_1 and the vacuum state is detected by D_2 . For

$$\begin{pmatrix} \vartheta_1 \\ \vartheta_2 \\ \vartheta_3 \end{pmatrix} = \begin{pmatrix} +22.5^\circ \\ 65.5302^\circ \\ -22.5^\circ \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \varphi_3 \\ \varphi_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 180^\circ \end{pmatrix}$$

we have $\underline{x}=-1$ and the probability of success is 0.25. For

$$\begin{pmatrix} \vartheta_1 \\ \vartheta_2 \\ \vartheta_3 \end{pmatrix} = \begin{pmatrix} +36.53^\circ \\ 62.25^\circ \\ -36.53^\circ \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \varphi_3 \\ \varphi_4 \end{pmatrix} = \begin{pmatrix} 88, 24^\circ \\ -66, 52^\circ \\ -11, 25^\circ \\ 102, 24^\circ \end{pmatrix}$$

we have $\underline{x}=i$ and the probability of success is 0.18082.

3.1.4 Linear Optics Quantum Gates¹⁹

Indeterministic Gates

Fortunately, using photonic memory and quantum teleportation, (deterministic) CPHASE gates may be implemented using indeterministic ones:

— DRAFT, June 26, 2009 —

¹⁸See also (Rudolph and Pan, 2001; Ralph et al., 2002; Hofmann and Takeuchi, 2002) and especially (Gilchrist and Milburn, 2002) for other possibilities.

¹⁹See (Dowling et al., 2004).

The essential observation, due to (Gottesman and Chuang, 1999), is the equivalence

(3.9)

where

is the inverse of the BELL network and Φ_+ the state defined in 1.2.2. This equivalence is obvious from the discussion of quantum teleportation in 1.2.2 and, thanks to

implies the equivalence²⁰

Therefore:

If the auxiliary 4-qubit state

$$\Phi_B^{(4)} \stackrel{\text{def}}{=} (\hat{1} \otimes \text{CPHASE} \otimes \hat{1})(\Phi_+ \otimes \Phi_+)$$

is available then the (deterministic) CNOT gate can be replaced by appropriately modified double quantum teleportation.

DRAFT, June 26, 2009

²⁰See also (Brukner et al., 2003) in this connection.

If $\Phi_B^{(4)}$ can be stored for later use²¹ then it is sufficient to have a nondeterministic gate producing $\Phi_B^{(4)}$ with nonzero probability from standard input. One such possibility, obviously, is to replace the deterministic CNOT gates in the above characterization of $\Phi_B^{(4)}$ by nondeterministic ones, if the latter are available.

In principle (Kim et al., 2001), (deterministic) teleportation is possible by exploiting sum frequency generation of both type I and type II for a complete BELL measurement (see, e.g., Section [ref*nlqo-S-TWM](#) of (Lücke, nlqo) for the explanation of sum frequency generation). However, also indeterministic teleportation by only partial BELL measurement — as, e.g. sketched in Figure 3.6 and explained by Exercise 14 — may be useful for improving the probability of success, at least, of an indeterministic CPHASE gate.

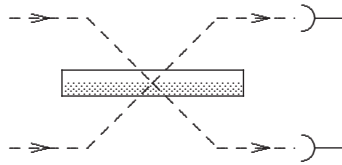


Figure 3.6: Partial BELL measurement.

Exercise 14 Consider a HADAMARD beam splitter for the orthogonal modes \hat{a}_1 \hat{a}_2 , i.a a beam splitter acting as

$$\hat{a}_1 \mapsto \frac{1}{\sqrt{2}} (\hat{a}_1 + \hat{a}_2) , \quad \hat{a}_2 \mapsto \frac{1}{\sqrt{2}} (\hat{a}_1 - \hat{a}_2) .$$

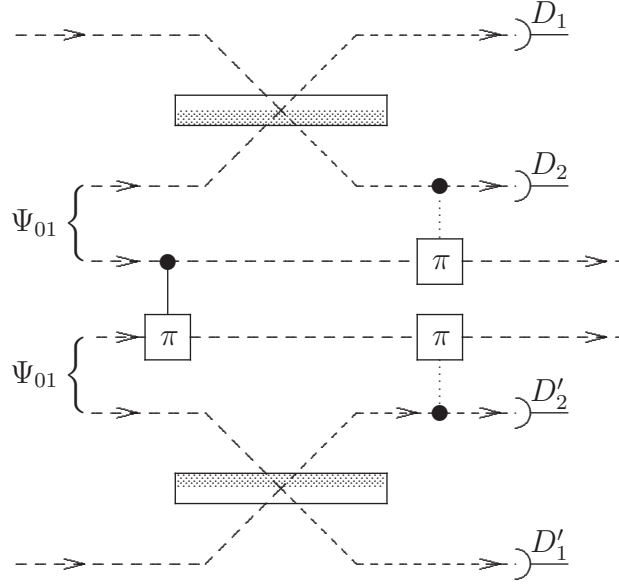
Show that the beam splitter, applied to the BELL states

$$\Phi_{\pm} = \frac{1}{\sqrt{2}} \left(\Omega \pm \hat{a}_1^{\dagger} \hat{a}_2^{\dagger} \Omega \right) , \quad \Psi^{\pm} = \frac{1}{\sqrt{2}} \left(\hat{a}_1^{\dagger} \pm \hat{a}_2^{\dagger} \right) \Omega$$

in the corresponding FOCK representation as sketched in Figure 3.6, acts as follows:

$$\begin{aligned} \Phi_{\pm} &\longmapsto \frac{1}{\sqrt{2}} \left(|0, 0\rangle^{\text{F}} \pm \frac{1}{2} \left(|2, 0\rangle^{\text{F}} - |0, 2\rangle^{\text{F}} \right) \right) , \\ \Psi_{01} = \Psi_{+} &\longmapsto |1, 0\rangle^{\text{F}} , \\ \Psi_{11} = \Psi_{-} &\longmapsto |0, 1\rangle^{\text{F}} . \end{aligned}$$

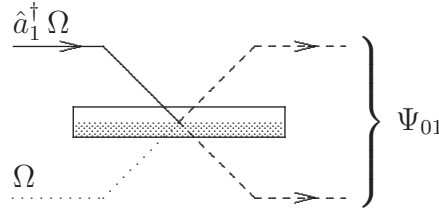
According to (3.9) and Exercise 14 a so-called $\text{CZ}_{\frac{1}{4}}$ gate, i.e. an indeterministic CPHASE gate working with probability of success $1/4$, can be implemented in the FOCK realization as sketched in Figure 3.7 This gate succeeds if the (photon number

Figure 3.7: Implementation of a $CZ_{\frac{1}{4}}$ gate

resolving) detectors D_1, \dots, D'_2 indicate that the common state of the first two qubits as well as that of the last two qubits is a single-photon state.²² The ancillary states

$$\Psi_{01} = \frac{|0, 1\rangle + |1, 0\rangle}{\sqrt{2}} = \frac{\hat{a}_1^\dagger + \hat{a}_2^\dagger}{\sqrt{2}} \Omega$$

may be easily prepared using a single-photon source and a HADAMARD beam splitter:²³



Near-Deterministic Quantum Gates

The construction sketched in Figure 3.7 can be generalized in the following way using $4n$ ancillary qubits²⁴ instead of only 4 (Knill et al., 2000; Knill et al., 2001):

— DRAFT, June 26, 2009 —

²¹See (Pittman and Franson, 2002) in this connection.

²²The dotted vertical lines indicate that the effect of the corresponding CPHASE gates on the output qubits can be achieved via LOCC (Local Operations and Classical Communication).

²³Note that the single-photon state Ψ_{01} is **entangled** when interpreted as FOCK realization of a 2-qubit state.

²⁴The case $n = 2$ is of special interest (Nielsen, 2004).

Let $\hat{a}_0, \dots, \hat{a}_{2n}$ be pairwise orthonormal modes describing photons with (almost) sharp momenta and prepare the first $2n$ ancillary qubits in the state

$$\Phi_{\text{tele}}^{(n)} \stackrel{\text{def}}{=} \frac{1}{\sqrt{n+1}} \sum_{j=0}^n \left(\prod_{\nu=1}^j \hat{a}_{\nu}^{\dagger} \right) \left(\prod_{\mu=n+j+1}^{2n} \hat{a}_{\mu}^{\dagger} \right) \Omega,$$

(instead of Ψ_{01}). Let $\hat{F}_{(n)}$ be the linear operator on $\mathcal{H}_{\hat{a}_0, \dots, \hat{a}_{2n}}$ characterized by $\hat{F}_{(n)} \Omega = \Omega$ and

$$\hat{F}_{(n)} \hat{a} \hat{F}_{(n)}^{-1} = \begin{cases} \hat{a} & \text{for } \hat{a} \perp \{\hat{a}_0, \dots, \hat{a}_n\}, \\ \frac{1}{\sqrt{n+1}} \sum_{j=0}^n e^{-ik \frac{2\pi}{n+1} j} \hat{a}_j & \text{for } \hat{a} = \hat{a}_k, k \in \{0, \dots, n\}, \end{cases} \quad (3.10)$$

where — as in Section 1.2.4 of (Lücke, nlqo) — we denote by $\mathcal{H}_{\hat{a}_0, \dots, \hat{a}_{2n}}$ the smallest closed subspace of $\mathcal{H}_{\text{field}}$ that contains Ω and is invariant under $\hat{a}_0^{\dagger}, \dots, \hat{a}_{2n}^{\dagger}$. Then, as explained in connection with the single-photon simulation of n -qubit systems, the transformation

$$\hat{a}_{\nu} \mapsto \hat{F}_{(n)} \hat{a}_{\nu} \hat{F}_{(n)}^{-1} \quad \forall \nu \in \{0, \dots, 2n\} \quad (3.11)$$

can be implemented using by linear optics.

Remark: For $n+1 = 2^m$ and²⁵

$$|k\rangle_m = \hat{a}_k^{\dagger} \Omega \quad \forall k \in \{0, \dots, 2^m - 1\}$$

the corresponding state transformation

$$|k\rangle_m \mapsto \hat{F}_{(n)} |k\rangle_m = \frac{1}{\sqrt{n+1}} \sum_{j=0}^n e^{+ik \frac{2\pi}{n+1} j} |j\rangle_m \quad \forall k \in \{0, \dots, 2^m - 1\}$$

simulates the m -qubit quantum FOURIER transform.

Exercise 15 Using the CAMPBELL-HAUSDORFF *formula*²⁶

$$e^{\hat{A}} \hat{B} e^{-\hat{A}} = \exp(\text{ad}_{\hat{A}}) \hat{B}, \quad (3.12)$$

where

$$\text{ad}_{\hat{A}} \hat{C} \stackrel{\text{def}}{=} [\hat{A}, \hat{C}]_{-},$$

show the following:

a)

$$e^{-i \hat{a}_j^{\dagger} \hat{a}_j \varphi} \hat{a}_k e^{+i \hat{a}_j^{\dagger} \hat{a}_j \varphi} = e^{+i \varphi \delta_{j,k}} \hat{a}_k \quad \forall j, j \in \{0, \dots, 2n\}, \varphi \in \mathbb{R}.$$

²⁵Recall (1.12).

²⁶Compare Footnote 50.

b)

$$\left. \begin{aligned} e^{-i(\hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1)\theta} \hat{a}_1 e^{+i(\hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1)\theta} &= \cos \theta \hat{a}_1 + i \sin \theta \hat{a}_2 \\ e^{-i(\hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1)\theta} \hat{a}_2 e^{+i(\hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1)\theta} &= i \sin \theta \hat{a}_1 + \cos \theta \hat{a}_2 \end{aligned} \right\} \forall \theta \in \mathbb{R}.$$

c) $\hat{F}_{(n)}$ is a unitary operator on $\mathcal{H}_{\hat{a}_0, \dots, \hat{a}_{2n}}$.

Since

$$\begin{aligned} \prod_{\nu=1}^j \left(\hat{F}_{(n)} \hat{a}_\nu \hat{F}_{(n)}^{-1} \right) &\stackrel{(3.10)}{=} \prod_{\nu=1}^j \left(\sum_{l_\nu=0}^n e^{+i\nu \frac{2\pi}{n+1} l_\nu} \hat{a}_{l_\nu}^\dagger \right) \\ &= \sum_{l_1, \dots, l_j=0}^n \prod_{\nu=1}^j \left(e^{+i\nu \frac{2\pi}{n+1} l_\nu} \hat{a}_{l_\nu}^\dagger \right) \quad \forall j \in \{1, \dots, n\} \end{aligned}$$

and

$$\begin{aligned} \prod_{\nu=0}^j \left(\hat{F}_{(n)} \hat{a}_\nu \hat{F}_{(n)}^{-1} \right) &= \sum_{l_0, \dots, l_j=0}^n \prod_{\nu=0}^j e^{+i\nu \frac{2\pi}{n+1} l_\nu} \hat{a}_{l_\nu}^\dagger \\ &= \sum_{l_1, \dots, l_{j+1}=0}^n \prod_{\nu=1}^{j+1} e^{-i \frac{2\pi}{n+1} l_\nu} e^{+i\nu \frac{2\pi}{n+1} l_\nu} \hat{a}_{l_\nu}^\dagger \quad \forall j \in \{0, \dots, n-1\} \\ &= \sum_{l'_0, \dots, l'_j=0}^n \prod_{\nu=1}^{j+1} e^{-i \frac{2\pi}{n+1} l'_\nu} e^{+i\nu \frac{2\pi}{n+1} l'_\nu} \hat{a}_{l'_\nu}^\dagger \quad \forall j \in \{0, \dots, n-1\}, \end{aligned}$$

we get

$$\begin{aligned} &\hat{F}_{(n)} \left(\alpha \hat{1} + \beta \hat{a}_0^\dagger \right) \Phi_{\text{tele}}^{(n)} \\ &= \frac{1}{\sqrt{n+1}} \left(\alpha \left(\prod_{\nu=n+1}^{2n} \hat{a}_\nu^\dagger \right) \Omega + \beta \hat{F}_{(n)} \left(\prod_{\nu=0}^n \hat{a}_\nu^\dagger \right) \Omega \right) \\ &+ \alpha \sum_{\substack{N_0, \dots, N_n=0 \\ 0 < N_0 + \dots + N_n \leq n}} \lambda_{N_0, \dots, N_n} \left(\prod_{j=0}^n \left(\hat{a}_j^\dagger \right)^{N_j} \right) \left(\prod_{\nu=n+1+N_0+\dots+N_n}^{2n} \hat{a}_\nu^\dagger \right) \Omega \\ &+ \beta \sum_{\substack{N_0, \dots, N_n=0 \\ 0 < N_0 + \dots + N_n \leq n}} \lambda_{N_0, \dots, N_n} \left(\prod_{j=0}^n \left(e^{-i \frac{2\pi}{n+1} j} \hat{a}_j^\dagger \right)^{N_j} \right) \left(\prod_{\nu=n+N_0+\dots+N_n}^{2n} \hat{a}_\nu^\dagger \right) \Omega \end{aligned} \quad (3.13)$$

with suitable $\lambda_{N_0, \dots, N_n} \in \mathbb{R}$, not depending on $\alpha, \beta \in \mathbb{C}$. Now, if the number N_ν of photons of mode \hat{a}_ν in the state $\hat{F}_{(n)} \left(\alpha \hat{1} + \beta \hat{a}_0^\dagger \right) F_{(n)} \Phi_{\text{tele}}^{(n)}$ is checked for all $\nu \in \{0, \dots, n\}$ by projective measurement then:

- If

$$0 < N_0 + \dots + N_n \leq n \quad (3.14)$$

then the state is projected onto

$$\hat{A}_{N_0, \dots, N_n} \left(\alpha \hat{1} + \beta \left(\prod_{j=1}^n e^{-i \frac{2\pi}{n+1} j N_j} \right) \hat{a}_{n+N_0+\dots+N_n}^\dagger \right) \hat{B}_{N_0, \dots, N_n} \Omega,$$

where

$$\begin{aligned} \hat{A}_{N_0, \dots, N_n} &\stackrel{\text{def}}{=} \lambda_{N_0, \dots, N_n} \prod_{\nu=0}^n (\hat{a}_\nu^\dagger)^{N_\nu}, \\ \hat{B}_{N_0, \dots, N_n} &\stackrel{\text{def}}{=} \prod_{\nu=n+1+N_0+\dots+N_n}^{2n} \hat{a}_\nu^\dagger. \end{aligned}$$

- The probability for (3.14) — thanks to unitarity of $\hat{F}_{(n)}$ — is $\frac{n}{n+1}$.

Since the phase factor $\prod_{j=1}^n e^{-i \frac{2\pi}{n+1} j N_j}$ is fixed by the measurement result, this shows:

With probability arbitrarily close to 1 the state $(\alpha \hat{1} + \beta \hat{a}_0^\dagger) \Omega$ with unknown $\alpha, \beta \in \mathbb{C}$ can be teleported²⁷ into $(\alpha \hat{1} + \beta \hat{a}_{n+N_0+\dots+N_n}^\dagger) \Omega$ with random N_0, \dots, N_n fulfilling (3.14) resulting from — typically destructive — measurement of the corresponding photon numbers in the state $\hat{F}_{(n)} (\alpha \hat{1} + \beta \hat{a}_0^\dagger) F_{(n)} \Phi_{\text{tele}}^{(n)}$.

In order to implement a $\text{CZ}_{n^2/(n+1)^2}$ gate, i.e. an indeterministic CPHASE gate working with probability of success $n^2/(n+1)^2$, $4n+2$ pairwise orthogonal modes $\hat{a}_0, \dots, \hat{a}_{2n}, \hat{b}_0, \dots, \hat{b}_{2n}$ are needed. \hat{a}_0 resp. \hat{b}_0 is used for the FOCK realization of the first resp. second input qubit of the gate. The ancillary FOCK qubits corresponding to the modes $\hat{a}_1, \dots, \hat{a}_{2n}, \hat{b}_1, \dots, \hat{b}_{2n}$ have to be prepared in the $4n$ -qubit state

$$\check{\Psi}_{\text{anc}}^{(n)} \stackrel{\text{def}}{=} \prod_{\nu, \mu=n+1}^{2n} \hat{S}_\pi^{(\nu, \mu)} \Phi_{\text{tele}}^{(n)} \otimes \Psi_{\text{tele}}^{(n)},$$

where $\Psi_{\text{tele}}^{(n)}$ is defined similarly to $\Phi_{\text{tele}}^{(n)}$ with modes \hat{a}_ν replaced by modes \hat{b}_ν and $\hat{S}_\pi^{(\nu, \mu)}$ means action of the CPHASE gate on the pair of FOCK qubits corresponding to the modes \hat{a}_ν, \hat{b}_μ . Defining $\hat{F}'_{(n)}$ resp. $\hat{A}'_{N_0, \dots, N_n}$ resp. $\hat{B}'_{N_0, \dots, N_n}$ similarly to $\hat{F}_{(n)}$ resp. $\hat{A}_{N_0, \dots, N_n}$ resp. $\hat{B}_{N_0, \dots, N_n}$ with \hat{a} -modes replaced by \hat{b} -modes and

$$\begin{aligned} \hat{t}_{\alpha, \beta}(\mathbf{N}) &\stackrel{\text{def}}{=} \left(\alpha \hat{1} + \beta \left(\prod_{j=1}^n e^{-i \frac{2\pi}{n+1} j N_j} \right) \hat{a}_{n+N_0+\dots+N_n}^\dagger \right), \\ \hat{t}'_{\alpha, \beta}(\mathbf{N}) &\stackrel{\text{def}}{=} \left(\alpha \hat{1} + \beta \left(\prod_{j=1}^n e^{-i \frac{2\pi}{n+1} j N_j} \right) \hat{b}_{n+N_0+\dots+N_n}^\dagger \right) \end{aligned} \quad (3.15)$$

²⁷See (Fattal et al., 2003) for an experimental demonstration of the basic version.

we get

$$\begin{aligned} & \hat{F}_{(n)} \hat{F}'_{(n)} \left((\alpha \hat{1} + \beta \hat{a}_0^\dagger) (\alpha' \hat{1} + \beta' \hat{b}_0^\dagger) \check{\Psi}_{\text{anc}}^{(n)} \right) \\ &= \prod_{\nu, \mu=n+1}^{2n} \hat{S}_\pi^{(\nu, \mu)} \left(\hat{F}_{(n)} (\alpha \hat{1} + \beta \hat{a}_0^\dagger) \Phi_{\text{tele}}^{(n)} \right) \otimes \left(\hat{F}'_{(n)} (\alpha' \hat{1} + \beta' \hat{b}_0^\dagger) \Psi_{\text{tele}}^{(n)} \right) \end{aligned}$$

and hence, by (3.13):

$$\begin{aligned} & \hat{F}_{(n)} \hat{F}'_{(n)} \left((\alpha \hat{1} + \beta \hat{a}_0^\dagger) (\alpha' \hat{1} + \beta' \hat{b}_0^\dagger) \check{\Psi}_{\text{anc}}^{(n)} \right) \\ &= \prod_{\nu, \mu=n+1}^{2n} \hat{S}_\pi^{(\nu, \mu)} \left(\left(\frac{\alpha}{\sqrt{n+1}} \left(\prod_{\nu=n+1}^{2n} \hat{a}_\nu^\dagger \right) \Omega + \frac{\beta}{\sqrt{n+1}} \hat{F}_{(n)} \left(\prod_{\nu=0}^n \hat{a}_\nu^\dagger \right) \Omega \right. \right. \\ & \quad \left. \left. + \sum_{\substack{N_0, \dots, N_n=0 \\ 0 < N_0 + \dots + N_n \leq n}}^n \lambda_{N_0, \dots, N_n} \hat{A}_{N_0, \dots, N_n} \hat{t}_{\alpha, \beta}(\mathbf{N}) \hat{B}_{N_0, \dots, N_n} \Omega \right) \right. \\ & \quad \left. \otimes \left(\frac{\alpha'}{\sqrt{n+1}} \left(\prod_{\nu=n+1}^{2n} \hat{b}_\nu^\dagger \right) \Omega + \frac{\beta'}{\sqrt{n+1}} \hat{F}'_{(n)} \left(\prod_{\nu=0}^n \hat{b}_\nu^\dagger \right) \Omega \right. \right. \\ & \quad \left. \left. + \sum_{\substack{N'_0, \dots, N'_n=0 \\ 0 < N'_0 + \dots + N'_n \leq n}}^n \lambda_{N'_0, \dots, N'_n} \hat{A}'_{N'_0, \dots, N'_n} \hat{t}'_{\alpha', \beta'}(\mathbf{N}') \hat{B}'_{N'_0, \dots, N'_n} \Omega \right) \right) \end{aligned}$$

Therefore, if the numbers $N_0, \dots, N_n, N'_0, \dots, N'_n$ of photons in the modes $\hat{a}_0, \dots, \hat{a}_n, \hat{b}_0, \dots, \hat{b}_n$ are checked for the state $\hat{F}_{(n)} \hat{F}'_{(n)} \left((\alpha \hat{1} + \beta \hat{a}_0^\dagger) (\alpha' \hat{1} + \beta' \hat{b}_0^\dagger) \check{\Psi}_{\text{anc}}^{(n)} \right)$ by projective measurement then:

- If

$$0 < N_0 + \dots + N_n \leq n \quad \text{and} \quad 0 < N'_0 + \dots + N'_n \leq n \quad (3.16)$$

then the state is projected onto a state with the factor

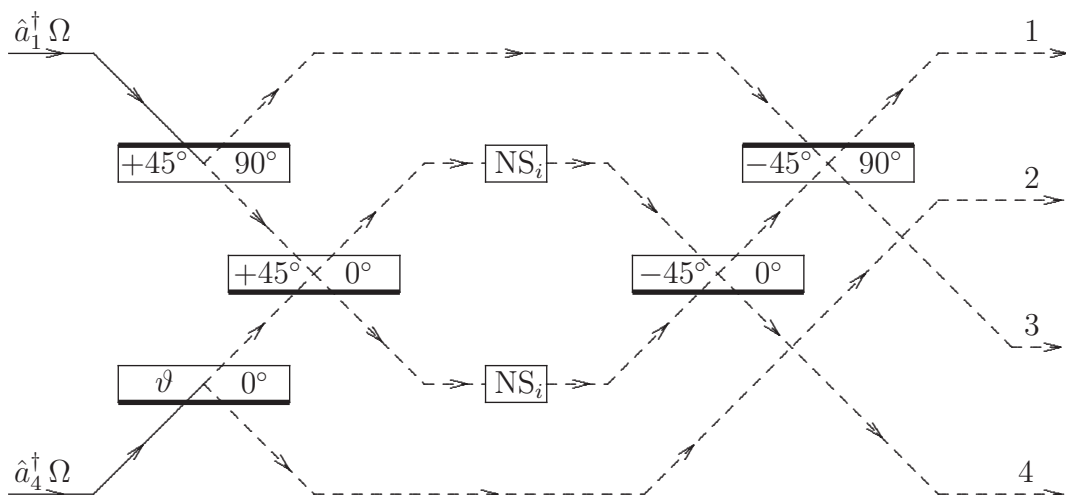
$$\begin{aligned} \Psi_{\text{out}} &\stackrel{\text{def}}{=} \prod_{\nu, \mu=n+1}^{2n} \hat{S}_\pi^{(\nu, \mu)} t_{\alpha, \beta}(\mathbf{N}) t'_{\alpha', \beta'}(\mathbf{N}') \Omega \\ &= \hat{S}_\pi^{(n+N_0+\dots+N_n, n+N'_0+\dots+N'_n)} t_{\alpha, \beta}(\mathbf{N}) t'_{\alpha', \beta'}(\mathbf{N}') \Omega \end{aligned}$$

which may be easily transformed, using only linear optical components, into the desired output

$$\hat{S}_\pi^{(0,0)} (\alpha \hat{1} + \beta \hat{a}^\dagger) (\alpha' \hat{1} + \beta' \hat{b}^\dagger) \Omega.$$

- The probability for (3.16) is $n^2 / (n+1)^2$.

Especially for $n = 2$, according to (Knill et al., 2001, Supplementary Information, Fig. 4), the ancillary state $\Phi_{\text{tele}}^{(n)}$ can be prepared (indeterministically) using only linear optics as sketched in Figure 3.8.

Figure 3.8: Preparation of $\Phi_{\text{tele}}^{(2)}$

3.2 Measurement-Based Schemes for Quantum Computation²⁸

The implementation of near deterministic CPHASE gates just described shows some interesting deviations from the conventional network model:

- Many ancillary qubits are used in addition to the input-qubits.
- The total state of all the qubits is suitably prepared using easily implementable deterministic gates and indeterministic gates, the latter acting only on the ancillary qubits.
- Then the desired output state can be transported onto the output-qubits using only (photon number) measurements and applying some easily performable final correction depending on the measurement results.

Meanwhile it turned out that for every n -qubit gate ($n \in \mathbb{N}$) and standard input state the corresponding output state can be efficiently produced,²⁹ e.g., as follows (Childs et al., 2005; Walther et al., 2005; Nielsen, 2005):

1. Prepare a $n \times m$ -qubit **cluster state**³⁰ with sufficiently large m in the following way:

———— DRAFT, June 26, 2009 ————

²⁸See also (Browne and Rudolph, 2005; Rudolph and Virmani, 2005; Varnava et al., 2006; Raussendorf, 2005) and (Lim et al., 2005).

²⁹Concerning the preparation of **explicitly** known states see (Kaye and Mosca, 2004).

³⁰We use the notion *cluster state* in a more general sense than originally introduced in (Raussendorf and Briegel, 2001; Raussendorf, 2003).

- (a) Prepare $n \times m$ qubits in the states

$$|+\rangle_{\nu\mu} \stackrel{\text{def}}{=} \frac{|0\rangle_{\nu\mu} + |1\rangle_{\nu\mu}}{\sqrt{2}}, \quad (\nu, \mu) \in \{1, \dots, n\} \times \{1, \dots, m\},$$

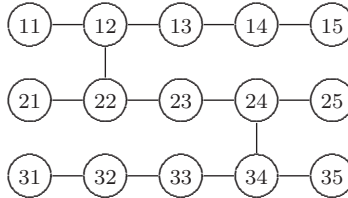
and imagine them arranged in a $n \times m$ -matrix scheme:

$$\begin{array}{cccc} |+\rangle_{11} & |+\rangle_{12} & \cdots & |+\rangle_{1m} \\ |+\rangle_{21} & |+\rangle_{22} & \cdots & |+\rangle_{2m} \\ \vdots & \vdots & \cdots & \vdots \\ |+\rangle_{n1} & |+\rangle_{n2} & \cdots & |+\rangle_{nm} \end{array}$$

- (b) Join all horizontally neighbouring qubit states and certain vertically neighbouring qubit states, depending on the effective network action desired, by lines respecting the rule that every state attached to a vertical line should have only one neighbour attached to a vertical line. Writing

$$\textcircled{\nu\mu} \quad \text{instead of} \quad |+\rangle_{\nu\mu}$$

we may get, e.g.



as an example for $n = 3$, $m = 5$.

- (c) For every (horizontal or vertical) line (bond) apply a CPHASE gate to the pair of qubits connected by the line.
2. Once the cluster state is prepared certain projective single qubit measurements are performed on the qubits corresponding to the first row (qubits $11, \dots, n1$).
 3. Once the qubits of the ν -th column have been tested certain projective single qubit measurements, depending on the outcome of the previous measurements³¹ (and the final output desired), are performed on the qubits corresponding to the $(\nu + 1)$ -th column.
 4. When the measurements on the $m - 1$ -th column are performed the n -qubit system corresponding to the m -th column is left in the desired output state up to known single-qubit transformations depending on the results of the previous measurements.
 5. The deviation from the desired output state may be either corrected or may be taken account of by appropriate change of the computational basis.

DRAFT, June 26, 2009

³¹Measurements the outcome of which determine the choice of subsequent measurements are called *feed-forwardable*.

A fascinating aspect of such measurement-based schemes for quantum computation is that the universal CPHASE gate is needed only for preparing the cluster state and for this purpose an indeterministic implementation of the phase gate is sufficient (Nielsen, 2004; Nielsen and Dawson, 2004; Chen et al., 2006).³²

Every cluster state can be prepared by successively applying single-bond and/or double-bond operations:

I. Single-bond operations: E.g. for the case sketched in Figure 3.9 the two teleportations (measurements of N_0, N_1, N_2 resp. N'_0, N'_1, N'_2) are attempted one after the other.

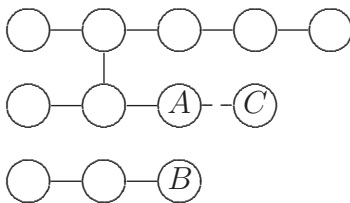


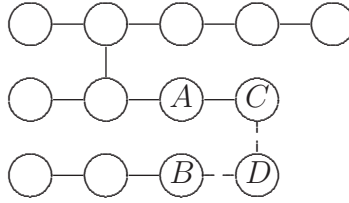
Figure 3.9: Trying to add qubit C with a single bond.

The teleportation that does not affect A is tried first. If it does not succeed one has to restart with a newly prepared qubit C . If it does succeed then the second teleportation is tried. If the latter also succeeds C is added with a bond to A . If it does not succeed then a projective single-qubit measurement w.r.t. the computational basis has been performed on A and this qubit has to be removed from the cluster and single-qubit correction have to be performed on the qubits connected to A (for the sketched special case only one) depending on the measurement result indicated by the corresponding detectors. As soon as the size of the cluster has been changed by this procedure we say that a **single-bond operation** has been performed. Thus:

A single-bond operation adds resp. removes a qubit with probability $2/3$ resp. $1/3$.

II. Double-bond operations: E.g. for the case sketched in Figure 3.10 one first try to connect D to C by a single-bond operation. If this adds D to the cluster we apply $CZ_4/9$ to the pair B, D . If the corresponding teleportation not affecting B fails then D has to be removed from the cluster and we have to restart with a newly prepared qubit D . If the first teleportation succeeds also the second teleportation is tried. If the

³²Moreover, such schemes circumvent the problem of programmable deterministic quantum gate arrays (Nielsen and Chuang, 1997).

Figure 3.10: Trying to add qubit D with two bonds.

latter succeeds D is connected to both C and B if not then B and D have to be removed from the cluster. As soon as either C or B has been removed or D has been connected to both C and D we say that a **double-bond operation** has been performed. Thus:

A double-bond operation adds resp. removes a qubit with probability $\frac{2}{3} \cdot \frac{2}{3}$ resp. $\frac{1}{3} + \frac{2}{3} \cdot \frac{1}{3}$.

In order to create the cluster, after every double-bond operation that removed a qubit a single-bond operation can be applied. Then:

On average, $2N$ successive operations add at least

$$\left\lfloor \left(\frac{2}{3} - \frac{1}{3} \right) N + \left(\frac{2}{3} \cdot \frac{2}{3} - \frac{2}{3} \cdot \frac{1}{3} \right) N \right\rfloor = \left\lfloor \frac{2N}{9} \right\rfloor$$

qubits to the cluster.

Easier implementable indeterministic CPHASE gates³³ with lower probabilities of success are sufficient if the cluster is built from microclusters in which a single qubits are connected to several dangling qubits in order to allow for multiple gluing attempts.³⁴

3.3 Cold Trapped Ions³⁵

Of all the proposed technologies for quantum information processing devices, arguably one of the most promising and certainly one of the most popular is trapped ions.

(James, 2000)

DRAFT, June 26, 2009

³³See, e.g., (Gasparoni et al., 2004; Zhao et al., 2005).

³⁴See end of (Nielsen, 2004).

³⁵See (Bužek and Šašura, 2002; Ghosh, 1995; Wunderlich and Balzer, 2003).

3.3.1 General Considerations

One of the earliest proposals to fulfill DiVINCENZO's requirements for quantum computation is the following:

1.
 - Qubits are identified with ions of some specified kind being in a superposition of two specified (at least) metastable energy eigenstates $|g\rangle$ resp. $|e\rangle$ representing the computational basis states $|0\rangle$ resp. $|1\rangle$. Typically, $|g\rangle$ is the ground state.
 - The ions are bound to specified places inside an ion trap and their collective oscillation is *cooled* to the quantum mechanical ground state.
2. The states $|g_1, \dots, g_n\rangle \equiv |0, \dots, 0\rangle$ may be prepared by applying Laser radiation tuned to the transition of $|e\rangle$ into a rapidly decaying higher energy eigenstate.
3. The decoherence time is of the order 10^{-1} seconds while the duration of gate operations is of the order 10^{-14} seconds.³⁶
4.
 - 1-qubit rotations are implemented by laser pulses — of appropriate duration and phase — tuned to the transition between $|g\rangle$ and $|e\rangle$.
 - The controlled sign gate $\Lambda_1(\hat{S}_\pi)$ is implemented by a suitable sequence of laser pulses exploiting one of the collective translational modes as *data bus* in the following way:

(i) A first pulse on the control qubit (Ion j_1) acts according to

$$\begin{aligned} |g_{j_1}\rangle|0\rangle_{\text{osc}} &\longmapsto |g_{j_1}\rangle|0\rangle_{\text{osc}} , \\ |e_{j_1}\rangle|0\rangle_{\text{osc}} &\longmapsto -i |g_{j_1}\rangle|1\rangle_{\text{osc}} . \end{aligned} \quad (3.17)$$

(ii) A second laser pulse on the target qubit (Ion j_2) — tuned to the transition of $|g\rangle$ into an excited energy eigenstate $|\tilde{e}\rangle$ different from $|e\rangle$ — acts for $b \in \{0, 1\}$ according to

$$\begin{aligned} |g_{j_2}\rangle|b\rangle_{\text{osc}} &\longmapsto (-1)^b |g_{j_2}\rangle|b\rangle_{\text{osc}} , \\ |e_{j_2}\rangle|b\rangle_{\text{osc}} &\longmapsto |e_{j_2}\rangle|b\rangle_{\text{osc}} . \end{aligned} \quad (3.18)$$

(iii) A third pulse of the same type as used in (i) acts according to

$$\begin{aligned} |g_{j_1}\rangle|0\rangle_{\text{osc}} &\longmapsto |g_{j_1}\rangle|0\rangle_{\text{osc}} , \\ |g_{j_1}\rangle|1\rangle_{\text{osc}} &\longmapsto -i |e_{j_1}\rangle|0\rangle_{\text{osc}} . \end{aligned} \quad (3.19)$$

These laser pulses have no effect if the control qubit (Ion j_1) is originally in the state $|g_{j_1}\rangle$. On the other hand, if the control qubit (Ion j_1) is originally in the state $|e_{j_1}\rangle$ then the action is as follows:

³⁶See, e.g. (Nielsen and Chuang, 2001, Fig. 7.1) for a comparison with other implementations.

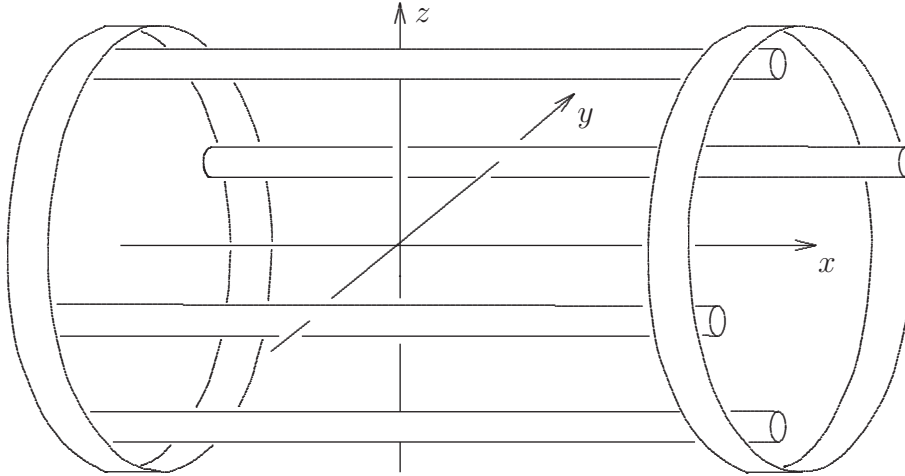


Figure 3.11: A linear PAUL trap

- The first pulse transfers this information into the data bus by exciting it to $|1\rangle_{\text{osc}}$ and applies $-i\hat{\sigma}_1$ to the control qubit.
- Then the second pulse multiplies the $|g_{j_2}\rangle$ -component of the target qubit's state by -1 .
- Finally, the third pulse returns the data bus into its ground state and acts on the $|g_{j_2}\rangle$ -component of the control qubit's state by $-i\hat{\sigma}_1$, once more.

Obviously, the resulting action is that of a $\Lambda_1(\hat{S}_\pi)$ gate.

5. Measurement of the final state of the computation may be done by irradiating by continuous laser radiation tuned to the transition of $|g\rangle$ into a rapidly decaying higher energy eigenstate. Then only those ions 'found' in the ground state show strong fluorescence.

All this will be explained in more detail — for the special case³⁷ of $^{40}\text{Ca}^+$ ions in a linear PAUL trap — in the subsequent sections.

3.3.2 Linear PAUL Trap

The linear PAUL trap used by the Innsbruck group is sketched in Figure 3.11.

———— DRAFT, June 26, 2009 ————

³⁷See <http://heart-c704.uibk.ac.at/quantumcomputation.html>

There are four rod electrodes, namely along

$$\begin{aligned}\mathcal{C}_1 &\stackrel{\text{def}}{=} \left\{ (x, y, z) \in \mathbb{R} : y = -r_0, z = 0, x \in \left\{ -\frac{x_0}{2}, +\frac{x_0}{2} \right\} \right\}, \\ \mathcal{C}_2 &\stackrel{\text{def}}{=} \left\{ (x, y, z) \in \mathbb{R} : z = +r_0, y = 0, x \in \left\{ -\frac{x_0}{2}, +\frac{x_0}{2} \right\} \right\}, \\ \mathcal{C}_3 &\stackrel{\text{def}}{=} \left\{ (x, y, z) \in \mathbb{R} : y = +r_0, z = 0, x \in \left\{ -\frac{x_0}{2}, +\frac{x_0}{2} \right\} \right\}, \\ \mathcal{C}_4 &\stackrel{\text{def}}{=} \left\{ (x, y, z) \in \mathbb{R} : z = -r_0, y = 0, x \in \left\{ -\frac{x_0}{2}, +\frac{x_0}{2} \right\} \right\},\end{aligned}$$

and two ring electrodes (end caps). The electric potential of the rod electrodes along \mathcal{C}_1 and \mathcal{C}_3 is³⁸ $\Phi(t)$ while the rod electrodes \mathcal{C}_2 and \mathcal{C}_4 are grounded. Both ring electrodes have the constant electric potential $\Phi_{\text{ring}} > 0$.

Trapping in Radial direction

If the rod electrodes were infinitely long and infinitely thin then they would contribute the electric potential

$$\Phi_{\text{ideal}}(x, y, z, t) = \frac{\Phi_0}{2} \left(1 + \frac{y^2 - z^2}{r_0^2} \right) \quad \text{if } \Phi(t) = \Phi_0 = \text{const}$$

since this fulfills the LAPLACE equation as well as the boundary conditions along the rods. If

$$\Phi(t) = \Phi_0 \cos(\Omega t), \quad \Omega \approx 16 - 18 \text{ MHz (radio frequency)},$$

then the quasi stationary approximation

$$\begin{aligned}\Phi_{\perp}(x, y, z, t) &\approx \frac{\Phi_0 \cos(\Omega t)}{2} \left(1 + \frac{y^2 - z^2}{r_0^2} \right) \\ &= \Phi_0 \cos(\Omega t) \frac{y^2 - z^2}{2r_0^2} + \frac{1}{2} \Phi_0 \cos(\Omega t)\end{aligned} \quad (3.20)$$

can be used near the center of the trap — also for finite rods, if sufficiently long.

The evolution equations of a particle of mass m and electric charge q in the electric potential (3.20) are³⁹

$$\ddot{y}(t) + \frac{q \Phi_0}{m r_0^2} \cos(\Omega t) y(t) = 0, \quad (3.21)$$

$$\ddot{z}(t) - \frac{q \Phi_0}{m r_0^2} \cos(\Omega t) z(t) = 0, \quad (3.22)$$

$$\ddot{x}(t) = 0.$$

³⁸Note that static electric potentials cannot have minima in regions free of electric charge.

³⁹In the Innsbruck experiment: $\Phi_0 \approx 300 - 800 \text{ V}$, $\frac{\Omega}{2\pi}$, $r_0 \approx 1.2 \text{ mm}$.

With

$$b \stackrel{\text{def}}{=} \frac{2q\Phi_0}{m r_0^2 \Omega^2}, \quad \zeta \stackrel{\text{def}}{=} \frac{\Omega t}{2} \quad (3.23)$$

equations (3.21) and (3.22) become equivalent to the special cases

$$\left(\frac{d}{d\zeta}\right)^2 y(\zeta) + 2b \cos(2\zeta) y(\zeta) = 0, \quad (3.24)$$

$$\left(\frac{d}{d\zeta}\right)^2 z(\zeta) - 2b \cos(2\zeta) z(\zeta) = 0 \quad (3.25)$$

of the MATHIEU *differential equation*

$$\left(\frac{d}{d\zeta}\right)^2 y(\zeta) + (a + 2b \cos(2\zeta)) y(\zeta) = 0. \quad (3.26)$$

The general solution of (3.26) is⁴⁰

$$y(\zeta) = \sum_{n \in \mathbb{Z}} C_{2n} (\lambda_+ e^{+\mu\zeta} e^{+2in\zeta} + \lambda_- e^{-\mu\zeta} e^{-2in\zeta}),$$

with general integration constants λ_{\pm} (to be adapted to the initial conditions) and certain constants C_{2n} and μ depending on a, b . We are interested in stable solutions, only, and therefore have to require

$$\mu = i\beta, \quad \beta \in \mathbb{R}.$$

Then

$$y(\zeta) = \sum_{n \in \mathbb{Z}} C_{2n} \left(\lambda_1 \cos((2n + \beta)\zeta) + \lambda_2 \sin((2n + \beta)\zeta) \right), \quad (3.27)$$

where

$$\lambda_1 \stackrel{\text{def}}{=} \lambda_+ + \lambda_-, \quad \lambda_2 = i(\lambda_+ - \lambda_-).$$

Inserting this into (3.26) gives the recursion formula

$$C_{2n+2} - \frac{a - (2n + \beta)}{b} C_{2n} + C_{2n-2} = 0. \quad (3.28)$$

Defining

$$G_{2n} \stackrel{\text{def}}{=} \frac{C_{2n}}{C_0}, \quad A \stackrel{\text{def}}{=} \lambda_1 C_0, \quad B \stackrel{\text{def}}{=} \lambda_2 C_0$$

and exploiting the well-known theorems for sin and cos we can rewrite (3.27) in the equivalent form

$$y(\zeta) = Y^+(\zeta) + \delta_y(\zeta),$$

⁴⁰See (Ghosh, 1995, Section 2.3).

where:

$$Y^\pm(\zeta) \stackrel{\text{def}}{=} A \cos(\beta \zeta) \pm B \sin(\beta \zeta),$$

$$\delta_y(\zeta) \stackrel{\text{def}}{=} \sum_{n=1}^{\infty} (Y^+(\zeta) (G_{2n} + G_{-2n}) \cos(2n\beta\zeta) - Y^-(\zeta) (G_{2n} - G_{-2n}) \sin(2n\beta\zeta)).$$

For sufficiently small⁴¹ $|b|$ one may show:

1. Solution of (3.28) gives a stable solution (3.27).
2. The *micromotion* $\delta_y(\zeta)$ is negligible.
3. The corresponding statements hold also for $z(\zeta)$.

In the following the micromotion will be neglected.

Trapping in Axial Direction

The positive potential of the ring electrodes in Figure 3.11 serves to confine positive ions also in axial direction. The additional (time-independent) electric potential contributed by these electrodes is

$$\Phi_{\parallel}(x, y, z) \approx \xi \Phi_{\text{ring}} \left(\frac{x}{x_0} \right)^2 \quad \text{for } x/x_0 \ll 1,$$

where ξ is some geometric factor of order 1 characterizing the contribution of Φ_{ring} on the center of the ring electrodes.

In the Innsbruck experiment we have

$$\Phi_{\text{ring}} \approx 2000 \text{ V}, \quad x_0 \approx 5 \text{ mm}$$

and

$$q \Phi_{\parallel}(x, y, z) \approx \frac{m}{2} \omega_x^2 x^2$$

with

$$\frac{\omega_x}{2\pi} \approx 500 - 700 \text{ kHz} \quad \text{for } {}^{40}\text{Ca}^+.$$

Since ω_x is definitely smaller than $\beta \zeta \approx 1,4 - 2$ MHz, in this experiment, it is sufficient — for what follows — to consider only the motion along the x -axis in the potential contributed by the ring electrodes and the repulsive Coulomb potential of the ions. The total mechanical potential for N identical ions then is (approximately)

$$\check{V}(x_1, \dots, x_N) = \frac{m}{2} \omega_x^2 \sum_{j=1}^N x_j^2 + \frac{q^2}{4\pi \epsilon_0} \sum_{\substack{j,k=1 \\ j < k}}^N \frac{1}{|x_j - x_k|}. \quad (3.29)$$

⁴¹Note that $b \sim q/m$.

Mean Values of the Ion Positions

For $j \in \{1, \dots, N\}$, let \check{x}_j be the mean value of the j -th ion's x -coordinate. Obviously, for

$$x \stackrel{\text{def}}{=} (x_1, \dots, x_N) = \check{x} \stackrel{\text{def}}{=} (\check{x}_1, \dots, \check{x}_N)$$

the potential of the N -ion system has to be minimal:

$$\left(\frac{\partial}{\partial x_j} \check{V}(x_1, \dots, x_N) \right)_{|x=\check{x}} = 0 \quad \forall j \in \{1, \dots, N\}. \quad (3.30)$$

Without loss of generality we may assume

$$\check{x}_1 < \check{x}_2 < \dots < \check{x}_N. \quad (3.31)$$

under this condition (3.30) is equivalent to

$$X_j - \sum_{\substack{k,j=1 \\ k < j}}^N \frac{1}{(X_k - X_j)^2} + \sum_{\substack{k,j=1 \\ k > j}}^N \frac{1}{(X_k - X_j)^2} = 0 \quad \forall j \in \{1, \dots, N\}, \quad (3.32)$$

where⁴²

$$X_j \stackrel{\text{def}}{=} \check{x}_j / \gamma, \quad \gamma \stackrel{\text{def}}{=} \left(\frac{q^2}{4\pi\epsilon_0 m \omega_x^2} \right)^{\frac{1}{3}}. \quad (3.33)$$

For $N \leq 3$ the solutions are easily determined:

$$N = 1: \quad X_1 = 0,$$

$$N = 2: \quad X_1 = -\sqrt[3]{\frac{1}{4}}, \quad X_2 = +\sqrt[3]{\frac{1}{4}},$$

$$N = 3: \quad X_1 = -\sqrt[3]{\frac{5}{4}}, \quad X_2 = 0, \quad X_3 = +\sqrt[3]{\frac{5}{4}}.$$

For $N > 3$ the X_j have to be determined numerically.

Of course, the distance between the ions is minimal at the center of the trap. Numerical calculations show that

$$\Delta\check{x}_{\min} \approx \frac{2.018}{N^{0.559}} \gamma$$

(James, 1998). Therefore, in the Innsbruck experiment, the overlap of the ions' wave functions is negligible⁴³ and the ions are individually addressable by laser beams.

———— DRAFT, June 26, 2009 ————

⁴²For $^{40}\text{Ca}^+$ and $\frac{\omega_x}{2\pi} \approx 700$ kHz: $\gamma \approx 4.85 \mu\text{m}$.

⁴³Recall Footnote 17 of Chapter 1.

Collective Oscillations

Near its minimum the potential (3.29) may be approximated as

$$\check{V}(x_1, \dots, x_N) \approx V(q_1, \dots, q_N) \stackrel{\text{def}}{=} \frac{m}{2} \omega_x^2 \sum_{j,k=1}^N V_{jk} q_j q_k,$$

where

$$\begin{aligned} q_j &\stackrel{\text{def}}{=} x_j - \check{x}_j \quad \forall j \in \{1, \dots, N\}, \\ V_{jk} &\stackrel{\text{def}}{=} \frac{1}{m \omega_x^2} \left(\frac{\partial}{\partial x_j} \frac{\partial}{\partial x_k} V(x_1, \dots, x_N) \right)_{|x=\check{x}} \quad \forall j, k \in \{1, \dots, N\}. \end{aligned} \quad (3.34)$$

Explicitly, by (3.29) and (3.33), we have

$$V_{jk} = V_{kj} = \begin{cases} 1 + \sum_{\substack{l=1 \\ l \neq j}}^N \frac{2}{|X_l - X_j|^3} & \text{for } j = k, \\ -\frac{2}{|X_k - X_j|^3} & \text{for } j \neq k. \end{cases} \quad (3.35)$$

The corresponding system of evolution equations is

$$\ddot{q}_j(t) + \omega_x^2 \sum_{k=1}^n V_{jk} q_k(t) = 0. \quad (3.36)$$

Since the matrix (V_{jk}) is positive and symmetric, there is an orthonormal system of eigenvectors

$$\mathbf{C}_l = \begin{pmatrix} C_{l1} \\ \vdots \\ C_{lN} \end{pmatrix}, \quad l \in \{1, \dots, N\},$$

of this matrix in \mathbb{R}^N with positive eigenvalues:

$$\begin{pmatrix} V_{11} & \dots & V_{1N} \\ \vdots & & \vdots \\ v_{N1} & \dots & V_{NN} \end{pmatrix} \begin{pmatrix} C_{l1} \\ \vdots \\ C_{lN} \end{pmatrix} = \left(\frac{\check{\omega}_l}{\omega_x} \right)^2 \begin{pmatrix} C_{l1} \\ \vdots \\ C_{lN} \end{pmatrix} \quad l \in \{1, \dots, N\}. \quad (3.37)$$

Hence, every solution of (3.36) is a superposition

$$q_j(t) = \sum_{l=1}^N \left(\lambda_l^+ q_j^{(+l)}(t) + \lambda_l^- q_j^{(-l)}(t) \right) \quad (3.38)$$

of the special collective motions (*eigenmodes*)

$$q_j^{(\pm l)}(t) \stackrel{\text{def}}{=} C_{lj} e^{\mp i \check{\omega}_l t}. \quad (3.39)$$

The first two eigenvectors may always be chosen as

$$\begin{aligned} \mathbf{C}_1 &= \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} && \text{with } \tilde{\omega}_1 = \omega_x, \\ \mathbf{C}_2 &= \frac{1}{\sqrt{X_1^2 + \dots + X_N^2}} \begin{pmatrix} X_1 \\ \vdots \\ X_N \end{pmatrix} && \text{with } \tilde{\omega}_2 = \sqrt{3}\omega_x. \end{aligned} \quad (3.40)$$

Proof: (3.35) directly implies $\sum_{k=1}^N V_{jk} = 1$ and, therefore, (3.37) for $l = 1$ with $\tilde{\omega}_1 = \omega_x$. On the other hand, we have

$$\begin{aligned} \sum_{k=1}^N V_{jk} X_k &\stackrel{(3.35)}{=} X_j + \sum_{j \neq l=1}^N \frac{2X_l}{|X_l - X_j|^3} - \sum_{j \neq l=1}^N \frac{2X_j}{|X_l - X_j|^3} \\ &= X_j + 2 \sum_{j \neq l=1}^N \frac{X_j - X_l}{|X_l - X_j|^3} \\ &\stackrel{(3.31)}{=} X_j + \sum_{\substack{l=1 \\ l < j}}^N \frac{2}{|X_l - X_j|^2} - \sum_{\substack{l=1 \\ l > j}}^N \frac{2}{|X_l - X_j|^2} \\ &\stackrel{(3.32)}{=} 3X_j. \end{aligned}$$

The latter implies (3.37) for $l = 2$ with $\tilde{\omega}_2 = \sqrt{3}\omega_x$. ■

Then $(q_1^{(1)}, \dots, q_N^{(1)})$ is called the *center of mass mode* and $(q_1^{(2)}, \dots, q_N^{(2)})$ the *breathing mode*.

3.3.3 Implementing Quantum Gates by Laser Pulses

Quantization of the Collective Oscillations

Using the generalized coordinates

$$Q_l(t) = \Re(\lambda_l^+ e^{-i\tilde{\omega}_l t} + \lambda_l^- e^{+i\tilde{\omega}_l t}) \quad (3.41)$$

we get

$$x_j(t) = \tilde{x}_j + \sum_{l=1}^N C_{lj} Q_l(t) \quad \forall j \in \{1, \dots, N\} \quad (3.42)$$

for the x -coordinates of the ions and

$$L = \frac{m}{2} \sum_{l=1}^N (\dot{Q}_l^2 - \tilde{\omega}_l^2 Q_l^2) \quad (3.43)$$

for the Lagrangian corresponding to (3.36). With the canonically conjugate momenta

$$P_j \stackrel{\text{def}}{=} \frac{\partial}{\partial \dot{Q}_j} L = m \dot{Q}_j$$

we get the Hamiltonian

$$H(Q, P, t) = \frac{1}{2m} \sum_{l=1}^N P_l^2 + \frac{m}{2} \sum_{l=1}^N \tilde{\omega}_l^2 Q_l^2$$

and standard quantization of the system amounts to selecting a (normalized) ground state (vector) $|0\rangle_{\text{osc}}$ and replacing the Q_l, P_l by operators

$$\begin{aligned} \hat{Q}_l &= \sqrt{\frac{\hbar}{2m\tilde{\omega}_l}} (\tilde{a}_l + \tilde{a}_l^\dagger), \\ \hat{P}_l &= -i\sqrt{\frac{\hbar m\tilde{\omega}_l}{2}} (\tilde{a}_l - \tilde{a}_l^\dagger), \end{aligned} \quad (3.44)$$

with *annihilation operators* \tilde{a}_l and *creation operators* \tilde{a}_l^\dagger obeying the *canonical commutation relations*⁴⁴

$$[\tilde{a}_l, \tilde{a}_k]_- = 0, \quad [\tilde{a}_l, \tilde{a}_k^\dagger]_- = \delta_{lk} \quad (3.45)$$

and the FOCK *condition*

$$\tilde{a}_l |0\rangle_{\text{osc}} = 0 \quad \forall l \in \{1, \dots, N\}. \quad (3.46)$$

The quantized Hamiltonian, then, is

$$\begin{aligned} \hat{H}_{\text{osc}} &= \frac{1}{2m} \sum_{l=1}^N \hat{P}_l^2 + \frac{m}{2} \sum_{l=1}^N \tilde{\omega}_l^2 \hat{Q}_l^2 \\ &= \sum_{l=1}^N \hbar \tilde{\omega}_l \left(\tilde{a}_l^\dagger \tilde{a}_l + \frac{1}{2} \right) \end{aligned} \quad (3.47)$$

and a maximal orthonormal system of the state space (for the quantized oscillatory motion) is given by the FOCK *states*

$$|n_1, \dots, n_N\rangle_{\text{osc}} \stackrel{\text{def}}{=} \frac{1}{\sqrt{n_1! \dots n_N!}} \prod_{l=1}^N (\tilde{a}_l^\dagger)^{n_l} |0\rangle_{\text{osc}}, \quad n_1, \dots, n_N \in \mathbb{Z}_+, \quad (3.48)$$

———— DRAFT, June 26, 2009 ————

⁴⁴These commutation relations are easily seen to be equivalent to

$$[\hat{Q}_l, \hat{Q}_k]_- = 0, \quad [\hat{P}_l, \hat{P}_k]_- = 0, \quad [\hat{Q}_l, \hat{P}_k]_- = i\hbar \delta_{lk}.$$

fulfilling

$$\tilde{a}_l^\dagger \tilde{a}_l |n_1, \dots, n_N\rangle_{\text{osc}} = n_l |n_1, \dots, n_N\rangle_{\text{osc}}. \quad (3.49)$$

The corresponding observables for the x -coordinates of the ions are

$$\begin{aligned} \hat{x}_j &\stackrel{(3.42)}{=} \tilde{x}_j \hat{1}_{\text{osc}} + \sum_{l=1}^N C_{lj} \hat{Q}_l(t) \\ &\stackrel{(3.44)}{=} \tilde{x}_j \hat{1}_{\text{osc}} + \sum_{l=1}^N \sqrt{\frac{\hbar}{2m\tilde{\omega}_l}} C_{lj} \left(\tilde{a}_l + \tilde{a}_l^\dagger \right). \end{aligned} \quad (3.50)$$

Of course, a more detailed description of the ions' motion would require inclusion of the modes describing radial oscillations.

Laser-Ion Interaction

In the following we assume that all the ions are $^{40}\text{Ca}^+$ ions. Moreover we select a special mode \tilde{a}_{l_0} (typically $l = 1$ or 2) as *data bus*. All other modes are assumed *cooled* into their ground state and will not be included in the description. The Hamiltonian describing the collective motion of all ions the the internal state of the j -th ion not interacting with an external electromagnetic field then is

$$\begin{aligned} \hbar \tilde{\omega}_{l_0} \left(\tilde{a}_{l_0}^\dagger \tilde{a}_{l_0} + \frac{1}{2} \right) + & \underbrace{E_{e_j} |e_j\rangle\langle e_j| + E_{g_j} |g_j\rangle\langle g_j|}_{= \hat{1}_{\text{int}}}, \\ & = \frac{E_{e_j} - E_{g_j}}{2} (|e_j\rangle\langle e_j| - |g_j\rangle\langle g_j|) + \frac{E_{e_j} + E_{g_j}}{2} \underbrace{(|e_j\rangle\langle e_j| + |g_j\rangle\langle g_j|)}_{= \hat{1}_{\text{int}}} \end{aligned}$$

where E_{e_j} resp. E_{g_j} is the energy level of the qubit state $|e_j\rangle$ resp. $|g_j\rangle$. This Hamiltonian describes the same time evolution as

$$\hat{H}_{0j} \stackrel{\text{def}}{=} -\frac{\hbar \omega_{0j}}{2} \hat{\sigma}_{3j} + \hbar \tilde{\omega}_{l_0} \tilde{a}_{l_0}^\dagger \tilde{a}_{l_0}, \quad (3.51)$$

where

$$\omega_{0j} \stackrel{\text{def}}{=} \frac{E_{e_j} - E_{g_j}}{2\hbar}, \quad \hat{\sigma}_{3j} \stackrel{\text{def}}{=} |g_j\rangle\langle g_j| - |e_j\rangle\langle e_j|. \quad (3.52)$$

(3.52) will be used in the following. We assume the laser radiation to be strong enough for the exterior field formalism to be adequate (see, e.g., Sections 7.1.1 and 7.2.1 of (Lücke, nlqo) in this connection). Interaction with the classical laser radiation will be described in the **dipole approximation**⁴⁵ by adding

$$\hat{V}_j \stackrel{\text{def}}{=} -q_{\text{el}} \hat{\mathbf{r}}_j \cdot \mathbf{E}(\hat{x}_j, 0, 0) t,$$

DRAFT, June 26, 2009

⁴⁵In the **quadrupole approximation** we would have to add

$$\hat{V}'_j \stackrel{\text{def}}{=} -q_{\text{el}} \hat{\mathbf{r}}_j \cdot \left((\hat{\mathbf{r}}_j \cdot \nabla_{\mathbf{r}'}) \mathbf{E}(\mathbf{x}', t) \right) \Big|_{\mathbf{r}'=(\hat{x}_j, 0, 0)}.$$

where

$$\begin{aligned} q_{\text{el}} &\stackrel{\text{def}}{=} \text{electric charge of the valence electron,} \\ \hat{\mathbf{r}}_j &\stackrel{\text{def}}{=} \begin{cases} \text{observable of the valence electron's} \\ \text{position relative to the center of the ion,} \end{cases} \\ \mathbf{E}(\mathbf{x}, t) &\stackrel{\text{def}}{=} \text{external electric field at position } \mathbf{x} \text{ and time } t. \end{aligned}$$

We assume that the exterior field is of the form

$$\mathbf{E}(\mathbf{x}, t) = \mathbf{E}_0 \left(e^{-i(\omega_L t - \mathbf{k}_L \cdot \mathbf{x} + \check{\phi})} + e^{+i(\omega_L t - \mathbf{k}_L \cdot \mathbf{x} + \check{\phi})} \right). \quad (3.53)$$

Replacing $\hat{\mathbf{r}}_j$ by

$$\begin{aligned} \hat{\mathbf{1}}_{\text{int}} \hat{\mathbf{r}}_j \hat{\mathbf{1}}_{\text{int}} &= (|g_j\rangle\langle g_j| + |e_j\rangle\langle e_j|) \hat{\mathbf{r}}_j (|g_j\rangle\langle g_j| + |e_j\rangle\langle e_j|) \\ &= \langle g_j | \hat{\mathbf{r}}_j | e_j \rangle \underbrace{|g_j\rangle\langle e_j|}_{\hat{\sigma}_j^- \stackrel{\text{def}}{=}} + \langle e_j | \hat{\mathbf{r}}_j | g_j \rangle \underbrace{|e_j\rangle\langle g_j|}_{\hat{\sigma}_j^+ \stackrel{\text{def}}{=}} \end{aligned}$$

we get

$$\hat{V}_j = -q_{\text{el}} \left(\mathbf{r}_{\text{eg},j} \hat{\sigma}_j^+ + (\mathbf{r}_{\text{eg},j})^\dagger \hat{\sigma}_j^- \right) \cdot \mathbf{E}_0 \left(e^{-i(\omega_L t - \eta_{0j}(\check{a}_{l_0} + \check{a}_{l_0}^\dagger) + \phi_j)} + e^{+i(\omega_L t - \eta_{0j}(\check{a}_{l_0} + \check{a}_{l_0}^\dagger) + \phi_j)} \right),$$

where

$$\eta_{0j} \stackrel{\text{def}}{=} k_L^1 \sqrt{\frac{\hbar}{2m\check{\omega}_{l_0}}}, \quad \phi_j \stackrel{\text{def}}{=} \check{\phi} - k_L^1 \check{x}_j.$$

In the interaction picture (see, e.g., Section 7.1.1 of (Lücke, nlqo)) the time evolution is determined by

$$\hat{V}_j^{\text{I}} = e^{+\frac{i}{\hbar} \hat{H}_{0j} t} \hat{V}_j e^{-\frac{i}{\hbar} \hat{H}_{0j} t}$$

instead of $\hat{H}_{0j} + \hat{V}_j$. Using the CAMPBELL-HAUSDORFF formula,⁴⁶ here in the form

$$e^{+\frac{i}{\hbar} \hat{H}_{0j} t} \hat{V}_j e^{-\frac{i}{\hbar} \hat{H}_{0j} t} = \exp \left(\text{ad}_{\frac{i}{\hbar} \hat{H}_{0j} t} \right) \hat{V}_j,$$

and

$$\begin{aligned} [\hat{H}_{0j}, \check{a}_{l_0}^\dagger]_- &= +\hbar \check{\omega}_{l_0} \check{a}_{l_0}^\dagger, \\ [\hat{H}_{0j}, \check{a}_{l_0}]_- &= -\hbar \check{\omega}_{l_0} \check{a}_{l_0}, \\ [\hat{H}_{0j}, \hat{\sigma}_j^\pm]_- &= \frac{\hbar \omega_{0j}}{2} [\hat{\sigma}_{3j}, \hat{\sigma}_j^\pm]_- \\ &= \pm \hbar \omega_{0j} \hat{\sigma}_j^\pm, \end{aligned}$$

we get⁴⁷

$$\hat{V}_j^{\text{I}} = -q_{\text{el}} \left(\mathbf{r}_{\text{eg},j} \cdot \mathbf{E}_0 \hat{\sigma}_j^+ e^{+i\omega_{0j} t} + \text{H.c.} \right) \left(e^{-i(\omega_L t - \eta_{0j}(\check{a}_{l_0} e^{-i\check{\omega}_{l_0} t} + \text{H.c.}) + \phi_j)} + \text{H.c.} \right).$$

⁴⁶Recall Exercise 15.

⁴⁷By ‘H.c.’ we denote the hermitian conjugate of the preceding term.

Hence in the **rotating wave approximation**,⁴⁸ i.e. if we neglect the contributions of the higher frequencies $\pm(\omega_L + \omega_{0j})$:

$$\hat{V}_j^I \approx \lambda_j \frac{\hbar}{2} \hat{\sigma}_j^+ e^{+i\eta_{0j}} (\check{a}_{l_0} e^{-i\check{\omega}_{l_0} t} + \text{H.c.}) e^{-i(\omega_L - \omega_{0j})t} + \text{H.c.},$$

where⁴⁹

$$\lambda_j \stackrel{\text{def}}{=} -\frac{2}{\hbar} q_{\text{el}} \mathbf{r}_{\text{eg},j} \cdot \mathbf{E}_0 e^{-i\phi_j}. \quad (3.54)$$

Using the BAKER-HAUSDORFF **formula**⁵⁰

$$\left[\hat{A}, [\hat{A}, \hat{B}]_- \right]_- = \left[\hat{B}, [\hat{A}, \hat{B}]_- \right]_- = 0 \implies e^{\hat{A} + \hat{B}} = e^{-\frac{1}{2}[\hat{A}, \hat{B}]_-} e^{\hat{A}} e^{\hat{B}} \quad (3.55)$$

and (3.45) we get

$$e^{+i\eta_{0j}} (\check{a}_{l_0} e^{-i\check{\omega}_{l_0} t} + \text{H.c.}) = e^{+i\eta_{0j}} \check{a}_{l_0}^\dagger e^{+i\check{\omega}_{l_0} t} e^{+i\eta_{0j}} \check{a}_{l_0} e^{-i\check{\omega}_{l_0} t} e^{-\frac{1}{2}\eta_{0j}^2}.$$

Therefore, if

$$\boxed{\omega_L - \omega_{0j} = k \check{\omega}_{l_0}, \quad k \in \mathbb{Z}}, \quad (3.56)$$

then the rotating wave approximation becomes

$$\hat{V}_j^I \approx \lambda_j \frac{\hbar}{2} \hat{\sigma}_j^+ e^{-\frac{1}{2}\eta_{0j}^2} \sum_{\mu, \nu=0}^{\infty} (i\eta_{0j})^{\mu+\nu} \frac{(\check{a}_{l_0}^\dagger)^\mu}{\mu!} \frac{(\check{a}_{l_0})^\nu}{\nu!} e^{+i(\mu-\nu-k)\omega_{0j}t} + \text{H.c.}$$

For sufficiently small λ_j non-resonant transitions and hence terms with $\mu - \nu - k \neq 0$ may be neglected. Then we may use

$$\hat{V}_j^I = \begin{cases} \lambda_j \frac{\hbar}{2} \hat{\sigma}_j^+ (\check{a}_{l_0}^\dagger)^{|k|} \check{F}_k(\check{a}_{l_0}^\dagger, \check{a}_{l_0}) + \text{H.c.} & \text{for } k \geq 0, \\ \lambda_j \frac{\hbar}{2} \hat{\sigma}_j^+ \check{F}_k(\check{a}_{l_0}^\dagger, \check{a}_{l_0}) (\check{a}_{l_0})^{|k|} + \text{H.c.} & \text{for } k \leq 0, \end{cases} \quad (3.57)$$

DRAFT, June 26, 2009

⁴⁸See (Aniello et al., 2003) for some criticism of this approximation.

⁴⁹In the quadrupole approximation (recall Footnote 45) we have to add

$$\lambda_j' \stackrel{\text{def}}{=} -\frac{2}{\hbar} q_{\text{el}} \left\langle \mathbf{e}_j \left| (\hat{r}_j \cdot \mathbf{E}_0) (\hat{r}_j \cdot \mathbf{k}_L) \mathbf{g}_j \right. \right\rangle.$$

⁵⁰For operators in **finite** dimensional vector spaces (3.55) may be proved as follows: Since $e^{\lambda \hat{A}} \hat{B} e^{-\lambda \hat{A}}$ and $\exp(\text{ad}_{\lambda \hat{A}}) \hat{B}$ fulfill the same first order differential equation and initial condition (for $\lambda = 0$), the CAMPBELL-HAUSDORFF formula (3.12) holds for arbitrary \hat{A} , \hat{B} . Therefore, also

$$f_1(\lambda) \stackrel{\text{def}}{=} e^{\lambda \hat{A}} e^{\lambda \hat{B}}$$

and

$$f_2(\lambda) \stackrel{\text{def}}{=} e^{\lambda(\hat{A} + \hat{B}) + \frac{\lambda^2}{2} [\hat{A}, \hat{B}]_-}$$

fulfill the same first order differential equation and initial condition (for $\lambda = 0$), **if** the l.h.s. of (3.55) holds, and hence $f_1 = f_2$.

where

$$\tilde{F}_k(\tilde{a}_{l_0}^\dagger \tilde{a}_{l_0}) \stackrel{\text{def}}{=} e^{-\frac{1}{2}\eta_{l_0j}^2} (i\eta_{l_0j})^{|k|} \sum_{\nu=0}^{\infty} (-\eta_{l_0j}^2)^\nu \frac{(\tilde{a}_{l_0}^\dagger)^\nu (\tilde{a}_{l_0})^\nu}{\nu! (\nu + |k|)!}. \quad (3.58)$$

Multiplying \hat{V}_j^I from the right with

$$\hat{\mathbf{1}}_{\text{osc}} = \sum_{n=0}^{\infty} |n\rangle_{\text{osc}} {}_{\text{osc}}\langle n|$$

and inserting

$$\hat{\sigma}_j^+ = |e_j\rangle\langle g_j|$$

finally yields

$$\hat{V}_j^I = \frac{\hbar}{2} \sum_{n=0}^{\infty} \left(\Omega_j^{n,k} \hat{A}_j^{n,k} + \left(\Omega_j^{n,k} \hat{A}_j^{n,k} \right)^\dagger \right), \quad (3.59)$$

with

$$\hat{A}_j^{n,k} \stackrel{\text{def}}{=} \begin{cases} |e_j\rangle\langle g_j| \otimes |n + |k|\rangle_{\text{osc}} {}_{\text{osc}}\langle n| & \text{for } k \geq 0, \\ |e_j\rangle\langle g_j| \otimes |n\rangle_{\text{osc}} {}_{\text{osc}}\langle n + |k|| & \text{for } k \leq 0, \end{cases} \quad (3.60)$$

and

$$\Omega_j^{n,k} \stackrel{\text{def}}{=} \lambda_j e^{-\frac{1}{2}\eta_{l_0j}^2} (i\eta_{l_0j})^{|k|} \sqrt{\frac{n!}{(n + |k|)!}} L_n^{|k|}(\eta_{l_0j}^2), \quad (3.61)$$

$$L_n^\alpha(x) \stackrel{\text{def}}{=} \sum_{\nu=0}^n \frac{(-x)^\nu}{\nu!} \binom{n + \alpha}{n - \nu} \quad (\textit{generalized LAGUERRE polynomials}).$$

Outline of proof for (3.61): We have to show

$$\sum_{\nu=0}^{\infty} (-x)^\nu \frac{(\tilde{a}_{l_0}^\dagger)^{\nu+|k|} (\tilde{a}_{l_0})^\nu}{\nu! (\nu + |k|)!} |n\rangle_{\text{osc}} {}_{\text{osc}}\langle n| = \sqrt{\frac{n!}{(n + |k|)!}} L_n^{|k|}(x) |n + |k|\rangle_{\text{osc}} {}_{\text{osc}}\langle n|$$

and

$$\sum_{\nu=0}^{\infty} (-c)^\nu \frac{(\tilde{a}_{l_0}^\dagger)^\nu (\tilde{a}_{l_0})^{\nu+|k|}}{\nu! (\nu + |k|)!} |n + |k|\rangle_{\text{osc}} {}_{\text{osc}}\langle n + |k|| = \sqrt{\frac{n!}{(n + |k|)!}} L_n^{|k|}(x) |n\rangle_{\text{osc}} {}_{\text{osc}}\langle n + |k||.$$

Since

$$(\tilde{a}_{l_0}^\dagger)^\nu (\tilde{a}_{l_0})^\nu = (\tilde{a}_{l_0}^\dagger \tilde{a}_{l_0}) (\tilde{a}_{l_0}^\dagger \tilde{a}_{l_0} - 1) \dots (\tilde{a}_{l_0}^\dagger \tilde{a}_{l_0} - (n - 1))$$

(see Equation 1.63 of (Lücke, nlqo)), the first of these equations follows from

$$\begin{aligned} (\tilde{a}_{l_0}^\dagger)^{\nu+|k|} (\tilde{a}_{l_0})^\nu |n\rangle_{\text{osc}} &= (\tilde{a}_{l_0}^\dagger)^{|k|} n(n-1) \dots (n - (\nu - 1)) |n\rangle_{\text{osc}} \\ &\stackrel{(3.48)}{=} n(n-1) \dots (n - (\nu - 1)) \sqrt{\frac{(n+|k|)!}{n!}} |n + |k|\rangle_{\text{osc}} \\ &= \begin{cases} \sqrt{\frac{n!}{(n + |k|)!}} \frac{(n + |k|)!}{(n - \nu)!} |n + |k|\rangle_{\text{osc}} & \text{for } n \geq \nu \\ 0 & \text{else,} \end{cases} \end{aligned}$$

the second from

$$\begin{aligned}
(\check{a}_{l_0}^\dagger)^\nu (\check{a}_{l_0})^{\nu+|k|} |n+|k\rangle_{\text{osc}} &= |n\rangle_{\text{osc}} \langle n| (\check{a}_{l_0}^\dagger)^\nu (\check{a}_{l_0})^{\nu+|k|} |n+|k\rangle_{\text{osc}} \\
&= \left({}_{\text{osc}} \langle n+|k| | (\check{a}_{l_0}^\dagger)^{\nu+|k|} (\check{a}_{l_0})^\nu | n \rangle_{\text{osc}} \right)^\dagger |n\rangle_{\text{osc}} \\
&= \begin{cases} \sqrt{\frac{n!}{(n+|k|)!}} \frac{(n+|k|)!}{(n-\nu)!} |n\rangle_{\text{osc}} & \text{for } n \geq \nu \\ 0 & \text{else.} \quad \blacksquare \end{cases}
\end{aligned}$$

The propagator in the interaction picture is the exponential⁵¹

$$\begin{aligned}
e^{-\frac{i}{\hbar} \hat{V}_j^1 t} &= \sum_{n=0}^{\infty} \left(\cos \left(\left| \Omega_j^{n,k} \right| \frac{t}{2} \right) \left(\hat{B}_j^{n,k} + \hat{C}_j^{n,k} \right) \right. \\
&\quad \left. - i \sin \left(\left| \Omega_j^{n,k} \right| \frac{t}{2} \right) \left(\hat{A}_j^{n,k} e^{-i\tilde{\Phi}_{k,j}} + \text{H.c.} \right) \right) + \hat{D}_j^{n,k}, \tag{3.62}
\end{aligned}$$

where

$$\tilde{\Phi}_{k,j} \stackrel{\text{def}}{=} \arg \left(\Omega_j^{n,k} \right) \stackrel{(3.61), (3.54)}{=} \phi_j - \frac{\pi}{2} |k| \tag{3.63}$$

and

$$\begin{aligned}
\hat{B}_j^{n,k} &\stackrel{\text{def}}{=} \begin{cases} |e_j\rangle \langle e_j| \otimes |n+|k\rangle_{\text{osc}} \langle n+|k| & \text{for } k \geq 0, \\ |e_j\rangle \langle e_j| \otimes |n\rangle_{\text{osc}} \langle n| & \text{for } k \leq 0, \end{cases} \\
\hat{C}_j^{n,k} &\stackrel{\text{def}}{=} \begin{cases} |g_j\rangle \langle g_j| \otimes |n\rangle_{\text{osc}} \langle n| & \text{for } k \geq 0, \\ |g_j\rangle \langle g_j| \otimes |n+|k\rangle_{\text{osc}} \langle n+|k| & \text{for } k \leq 0, \end{cases} \\
\hat{D}_j^{n,k} &\stackrel{\text{def}}{=} \begin{cases} \sum_{n=0}^{|k|-1} |e_j\rangle \langle e_j| \otimes |n\rangle_{\text{osc}} \langle n| & \text{for } k \geq 0, \\ \sum_{n=0}^{|k|-1} |g_j\rangle \langle g_j| \otimes |n\rangle_{\text{osc}} \langle n| & \text{for } k \leq 0. \end{cases}
\end{aligned}$$

Outline of proof for (3.62): By (3.60) we have

$$(\hat{A}_j^{n,k})^\dagger = \begin{cases} |g_j\rangle \langle e_j| \otimes |n\rangle_{\text{osc}} \langle n+|k| & \text{for } k \geq 0 \\ |g_j\rangle \langle e_j| \otimes |n+|k\rangle_{\text{osc}} \langle n| & \text{for } k \leq 0 \end{cases}$$

———— DRAFT, June 26, 2009 ————

⁵¹Usually $|\Omega_j^{n,k}|$ is called the RABI **frequency** for the transition

$$|g_j\rangle \otimes |n+|k\rangle_{\text{osc}} \Leftrightarrow |e_j\rangle \otimes |n\rangle_{\text{osc}} \quad \text{if } k \leq 0,$$

resp.

$$|g_j\rangle \otimes |n\rangle_{\text{osc}} \Leftrightarrow |e_j\rangle \otimes |n+|k\rangle_{\text{osc}} \quad \text{if } k \geq 0.$$

and therefore

$$\begin{aligned}\hat{A}_j^{n_1,k} \hat{A}_j^{n_2,k} &= 0, \\ \hat{A}_j^{n_1,k} \left(\hat{A}_j^{n_2,k}\right)^\dagger &= \delta_{n_1 n_2} \hat{B}_j^{n_1,k}, \\ \left(\hat{A}_j^{n_1,k}\right)^\dagger \hat{A}_j^{n_2,k} &= \delta_{n_1 n_2} \hat{C}_j^{n_1,k}\end{aligned}\quad (3.64)$$

for $k \geq 0$ as well as for $k \leq 0$. This implies, first of all,

$$e^{-\frac{i}{\hbar} \hat{V}_j^I t} = \prod_{n=0}^{\infty} \exp\left(-i \frac{t}{2} \left(\Omega_j^{n,k} \hat{A}_j^{n,k} + \text{H.c.}\right)\right). \quad (3.65)$$

Moreover, (3.64) implies

$$\begin{aligned}\left(\Omega_j^{n,k} \hat{A}_j^{n,k} + \text{H.c.}\right)^2 &= \left|\Omega_j^{n,k}\right|^2 \left(\hat{B}_j^{n,k} + \hat{C}_j^{n,k}\right), \\ \left(\Omega_j^{n,k} \hat{A}_j^{n,k} + \text{H.c.}\right)^{2\nu+1} &= \left|\Omega_j^{n,k}\right|^{2\nu+1} \left(\hat{A}_j^{n,k} e^{-i\tilde{\Phi}_{k,j}} + \text{H.c.}\right)\end{aligned}$$

and hence

$$\begin{aligned}\exp\left(-i \frac{t}{2} \left(\Omega_j^{n,k} \hat{A}_j^{n,k} + \text{H.c.}\right)\right) &= \hat{1} + \left(1 - \cos\left(\left|\Omega_j^{n,k}\right| \frac{t}{2}\right)\right) \left(\hat{B}_j^{n,k} + \hat{C}_j^{n,k}\right) \\ &\quad - i \sin\left(\left|\Omega_j^{n,k}\right| \frac{t}{2}\right) \left(\hat{A}_j^{n,k} e^{-i\tilde{\Phi}_{k,j}} + \text{H.c.}\right).\end{aligned}$$

Inserting this into (3.65) yields (3.62). ■

Especially, we have

$$\begin{aligned}e^{-\frac{i}{\hbar} \hat{V}_j^I t} &= \sum_{n=0}^{\infty} \left(\cos\left(\left|\Omega_j^{n,0}\right| \frac{t}{2}\right) \left(|e_j\rangle\langle e_j| \otimes |n\rangle_{\text{osc}} \langle n| + |g_j\rangle\langle g_j| \otimes |n\rangle_{\text{osc}} \langle n|\right) \right. \\ &\quad \left. - i \sin\left(\left|\Omega_j^{n,0}\right| \frac{t}{2}\right) \left(|e_j\rangle\langle g_j| \otimes |n\rangle_{\text{osc}} \langle n| e^{-i\phi_j} + \text{H.c.}\right) \right) \quad \underline{\underline{\text{for } k=0}}\end{aligned}\quad (3.66)$$

and

$$\begin{aligned}e^{-\frac{i}{\hbar} \hat{V}_j^I t} &= \sum_{n=0}^{\infty} \left(\cos\left(\left|\Omega_j^{n,1}\right| \frac{t}{2}\right) \left(|e_j\rangle\langle e_j| \otimes |n\rangle_{\text{osc}} \langle n| + |g_j\rangle\langle g_j| \otimes |n+1\rangle_{\text{osc}} \langle n+1|\right) \right. \\ &\quad \left. - i \sin\left(\left|\Omega_j^{n,1}\right| \frac{t}{2}\right) \left(|e_j\rangle\langle g_j| \otimes |n\rangle_{\text{osc}} \langle n+1| e^{-i(\phi_j - \pi/2)} + \text{H.c.}\right) \right) \\ &\quad + |g_j\rangle\langle g_j| \otimes |0\rangle_{\text{osc}} \langle 0| \quad \underline{\underline{\text{for } k=-1}}.\end{aligned}\quad (3.67)$$

Laser Pulses for Quantum Computation

An exterior electromagnetic field of the form⁵² (plane-wave), (3.56) acting on the j -th ion during the time interval

$$\Delta t = 2\varphi / \left| \Omega_j^{n,k} \right|$$

is called a φ -**pulse** for (n, k) . Examples for the action $\exp\left(-\frac{i}{\hbar} \hat{V}_j^I \Delta t\right)$ of these pulses are:

1. φ -pulse for $(0,0)$ with $\phi_j = \psi$:

$$\begin{aligned} \alpha |g_j\rangle \otimes |0\rangle_{\text{osc}} + \beta |e_j\rangle \otimes |0\rangle_{\text{osc}} \mapsto & (\alpha \cos \varphi - i e^{+i\psi} \beta \sin \varphi) |g_j\rangle \otimes |0\rangle_{\text{osc}} \\ & + (\beta \cos \varphi - i e^{-i\psi} \alpha \sin \varphi) |e_j\rangle \otimes |0\rangle_{\text{osc}} . \end{aligned}$$

2. $\frac{\pi}{2}$ -pulse for $(0,-1)$ with $\phi_j = \frac{\pi}{2}$:

$$\begin{aligned} |g_j\rangle \otimes |0\rangle_{\text{osc}} & \mapsto + |g_j\rangle \otimes |0\rangle_{\text{osc}} , \\ |e_j\rangle \otimes |0\rangle_{\text{osc}} & \mapsto -i |g_j\rangle \otimes |1\rangle_{\text{osc}} . \end{aligned}$$

3. π -pulse for $(0,-1)$ with $\phi_j = 0$:

$$\begin{aligned} |g_j\rangle \otimes |0\rangle_{\text{osc}} & \mapsto + |g_j\rangle \otimes |0\rangle_{\text{osc}} , \\ |g_j\rangle \otimes |1\rangle_{\text{osc}} & \mapsto - |g_j\rangle \otimes |1\rangle_{\text{osc}} , \\ |e_j\rangle \otimes |0\rangle_{\text{osc}} & \mapsto - |g_j\rangle \otimes |0\rangle_{\text{osc}} , \\ |e_j\rangle \otimes |1\rangle_{\text{osc}} & \mapsto + |g_j\rangle \otimes |1\rangle_{\text{osc}} . \end{aligned}$$

Obviously, the action of a φ -pulse is that of a **1-qubit rotation**, i.e. it is described by the matrix

$$\begin{pmatrix} \cos \varphi & -i e^{+i\psi} \sin \varphi \\ -i e^{-i\psi} \sin \varphi & \cos \varphi \end{pmatrix} \quad \text{w.r.t. } \left\{ |g_j\rangle \hat{=} |0\rangle , |e_j\rangle \hat{=} |1\rangle \right\} ,$$

as long as $n_{l_0} = 0$. Moreover, suitable laser pulses for implementing the CNOT gate as described in 3.3.1 are the following:

$$(3.17) : \quad \text{a } \frac{\pi}{2}\text{-pulse for } (0, -1) \text{ with } \phi_j = \frac{\pi}{2} \text{ on ion } j_1$$

$$(3.18) : \quad \text{a } \pi\text{-pulse for } (0, -1) \text{ with } \phi_{j_2} = 0 \text{ on ion } j_2 , \\ \text{tuned to a transition } |g_{j_2}\rangle \otimes |1\rangle_{\text{osc}} \rightleftharpoons |e'_{j_2}\rangle \otimes |0\rangle_{\text{osc}} \\ \text{with } |e'_{j_2}\rangle \text{ sufficiently different from } |e_{j_2}\rangle ,$$

$$(3.19) : \quad \text{a } \frac{\pi}{2}\text{-pulse for } (0, -1) \text{ with } \phi_j = \frac{\pi}{2} \text{ on ion } j_1 .$$

———— DRAFT, June 26, 2009 ————

⁵²Note that for electromagnetic radiation the electric field uniquely fixes the magnetic field and vice versa.

This shows that a sufficiently large class of quantum gates may be implemented, **provided** that the oscillatory modes can be cooled to their ground state.

Exercise 16 Show the following:

- a) The matrices $e^{i\hat{\sigma}_1\varphi}$ and $e^{i\hat{\sigma}_2\varphi}$ correspond to special 1-qubit rotations, for all $\varphi \in \mathbb{R}$.
- b) $e^{-i\hat{\sigma}_1\frac{\pi}{4}}\hat{\sigma}_2e^{+i\hat{\sigma}_1\frac{\pi}{4}} = \hat{\sigma}_3$.
- c) Every $\hat{U} \in \text{SU}(2)$ may be represented in the form⁵³

$$\hat{U} = e^{i\hat{\sigma}_2\frac{\psi}{2}} e^{i\hat{\sigma}_1\frac{\theta}{2}} e^{i\hat{\sigma}_2\frac{\phi}{2}}, \quad \psi, \theta, \phi \in \mathbb{R}.$$

3.3.4 Laser Cooling

See (Metcalf and van der Straten, 1999).

⁵³Recall the beginning of the proof of Lemma 1.2.2.

Part II

Fault Tolerant Quantum Information Processing

Chapter 4

General Aspects of Quantum Information

An open system is nothing more than one which has interactions with some other environment system, whose dynamics we wish to neglect, or average over.

(Nielsen and Chuang, 2001, p. 353)

4.1 Introduction

Quantum information theory deals with transmission and quantification of quantum information. Roughly speaking, **quantum information** is the information carried by n -qubit systems ($n \in \mathbb{N}$). Of the utmost importance for quantum information — as opposed to *classical information*,¹ — are:

1. The quantum mechanical **superposition principle**:

The pure states of a quantum system are in 1-1-correspondence with the 1-dimensional subspaces of a complex HILBERT space (unless there are superselection rules²).

2. The **no-cloning theorem** (Dieks, 1982; Wootters and Zurek, 1982; Peres, 2002):

There cannot exist any recipe for preparing any two or more systems such that each of them carries the same quantum information as a given quantum system — unless the state of the latter is completely known, of course.

DRAFT, June 26, 2009

¹See (Shannon, 1949) for the theory of classical information.

²See (Verstraete and Cirac, 2003; Bartlett and Wiseman, 2003) for the case with superselection rules.

Remark: There are several justifications for the no-cloning theorem,³ e.g.:

- Given $\Psi_0 \in \mathcal{H}$, there is no linear extension of the mapping

$$\mathcal{C}(\Psi \otimes \Psi_0) \stackrel{\text{def}}{=} \Psi \otimes \Psi \quad \text{for all **normalized** } \Psi \in \mathcal{H}$$

to all of $\mathcal{H} \otimes \mathcal{H}$.

- Cloning would allow measurement of incommensurable quantum observables — impossible according to quantum mechanics.
- Cloning would, by proper use of one of the available BELL sources, allow for superluminal communication⁴ — impossible according to special relativity.

While the superposition principle opens up the fascinating possibilities of quantum computation, the impossibility of cloning unknown quantum states strongly limits the amount of information that can be read out from quantum states.⁵ Thus, e.g., it is impossible to distinguish nonorthogonal states⁶ by a single measurement. Nevertheless, quantum information seems to offer a wealth of useful applications without any classical equivalent.

We say that quantum information is transmitted — to whatever degree intact — through a *quantum* (rather than *classical*) **channel** if the information is sent using systems whose quantum character cannot be neglected in this respect. In other words:

We identify *quantum channels* with **open**⁷ quantum systems, used for quantum communication.

For practical communication it is important that information can be transferred in a reversible way from one physical system to another. The no-cloning theorem implies that unknown quantum information cannot be transferred from quantum to purely classical systems in a reversible way. This is why quantum channels and entanglement-assisted classical channels are the main topic of these lectures.

In the following, unless stated otherwise, we will always work in the interaction picture and make extensive use of DIRAC's bra-ket notation.⁸ For simplicity, we **consider only finite-dimensional HILBERT spaces**. This is sufficient for clarifying the main points.

DRAFT, June 26, 2009

³See (Werner, 2001, Section 2.3) for a detailed discussion.

⁴See (Herbert, 1982). Similarly, joint measurability (without cloning) of non-commuting observables would enable superluminal communication.

⁵On the other hand, the non-cloning theorem constitutes the basis for secure quantum cryptography (see <http://www.idquantique.com>) and quantum passwords (Gu and Weedbrook, 2005).

⁶We tacitly identify states with their density matrices or wave functions (if pure).

⁷We have to consider open quantum systems since quantum information is prone to quantum noise caused by interaction with the environment.

⁸See, e.g., (Lücke, eine).

4.2 Quantum Channels

4.2.1 Open Quantum Systems and Quantum Operations

Let us consider two quantum systems \mathcal{S}_1 resp. \mathcal{S}_2 with (finite dimensional) state spaces \mathcal{H}_1 resp. \mathcal{H}_2 and consider \mathcal{S}_2 as the *environment* of \mathcal{S}_1 ; i.e. let us assume the bipartite system \mathcal{S} composed of \mathcal{S}_1 and \mathcal{S}_2 to be closed. Moreover, let us assume that \mathcal{S}_1 is prepared in a pure state⁹ $\hat{\rho}^{(1)} \in S(\mathcal{H}_1)$ at time 0. Then, at time 0 there are no correlations between \mathcal{S}_1 and \mathcal{S}_2 and the state of \mathcal{S} is of the form

$$\hat{\rho}_0 = \hat{\rho}^{(1)} \otimes \hat{\rho}^{(2)} \quad (4.1)$$

with $\hat{\rho}^{(2)} \in S(\mathcal{H}_2)$. At time t , then (see, e.g., Section 6.1.2 of (Lücke, nlqo)), the state of \mathcal{S} is

$$\hat{\rho}_t = \hat{U} \hat{\rho}^{(1)} \otimes \hat{\rho}^{(2)} \hat{U}^\dagger, \quad (4.2)$$

where the unitary operator \hat{U} on the state space $\mathcal{H}_1 \otimes \mathcal{H}_2$ of system \mathcal{S} is given by

$$\hat{U} \stackrel{\text{def}}{=} e^{+\frac{i}{\hbar} \hat{H}_0 t} e^{-\frac{i}{\hbar} \hat{H} t},$$

\hat{H} resp. $\hat{H}_0 = \hat{H}_0^{(1)} \otimes \hat{H}_0^{(2)}$ being the actual resp. *free* Hamiltonian of \mathcal{S} . The partial state of \mathcal{S}_1 at time t , therefore, is

$$\hat{\rho}_t^{(1)} = \mathfrak{C}(\hat{\rho}^{(1)}), \quad (4.3)$$

where¹⁰

$$\mathfrak{C}(\hat{\rho}') \stackrel{\text{def}}{=} \text{trace}_2 \left(\hat{U} (\hat{\rho}' \otimes \hat{\rho}^{(2)}) \hat{U}^\dagger \right) \quad \forall \hat{\rho}' \in S(\mathcal{H}_1). \quad (4.4)$$

Thanks to the spectral theorem, the initial state of the environment can be written in the form

$$\hat{\rho}^{(2)} = \sum_{\beta=1}^{n_2} \underbrace{\lambda_\beta}_{\geq 0} \left| \phi_\beta^{(2)} \right\rangle \left\langle \phi_\beta^{(2)} \right|, \quad \sum_{\beta=1}^{n_2} \lambda_\beta = 1 \quad (4.5)$$

with some orthonormal basis $\left\{ \phi_1^{(2)}, \dots, \phi_{n_2}^{(2)} \right\}$ of \mathcal{H}_2 . (4.4) and (4.5) imply¹¹

$$\begin{aligned} \mathfrak{C}(\hat{\rho}') &= \sum_{\alpha, \beta=1}^{n_2} \lambda_\beta \left\langle \psi_\alpha^{(2)} \right| \hat{U} \left(\hat{\rho}' \otimes \left| \phi_\beta^{(2)} \right\rangle \left\langle \phi_\beta^{(2)} \right| \right) \hat{U}^\dagger \left| \psi_\alpha^{(2)} \right\rangle \\ &= \sum_{\alpha, \beta=1}^{n_2} \hat{K}_{\alpha, \beta} \hat{\rho}' \hat{K}_{\alpha, \beta}^\dagger \quad \forall \hat{\rho}' \in S(\mathcal{H}_1) \end{aligned} \quad (4.6)$$

———— DRAFT, June 26, 2009 ————

⁹By $S(\mathcal{H})$ we denote the set of all *states*, i.e. of all positive operators $\hat{\rho}$ on the HILBERT space \mathcal{H} with $\text{trace}(\hat{\rho}) = 1$. $\mathcal{L}(\mathcal{H})$, as usual, denotes the set of all bounded linear operators on \mathcal{H} .

¹⁰Note that \mathfrak{C} depends not only on \hat{H} and \hat{H}_0 but also on the initial state of the environment!

¹¹We use the notation

$$\left\langle \phi^{(2)} \right| \left(\sum_{k=1}^N \hat{A}_k \otimes \hat{B}_k \right) \left| \psi^{(2)} \right\rangle \stackrel{\text{def}}{=} \sum_{k=1}^N \hat{A}_k \left\langle \phi^{(2)} \right| \hat{B}_k \left| \psi^{(2)} \right\rangle$$

for $\phi^{(2)}, \psi^{(2)} \in \mathcal{H}_2$, $\hat{A}_1, \dots, \hat{A}_N \in \mathcal{H}_1$, and $\hat{B}_1, \dots, \hat{B}_N \in \mathcal{H}_2$.

for every orthonormal basis $\{\psi_1^{(2)}, \dots, \psi_{n_2}^{(2)}\}$ of \mathcal{H}_2 , where

$$\hat{K}_{\alpha,\beta} \stackrel{\text{def}}{=} \sqrt{\lambda_\beta} \langle \psi_\alpha^{(2)} | \hat{U} | \phi_\beta^{(2)} \rangle \in \mathcal{L}(\mathcal{H}_1) \quad \forall \alpha, \beta \in \{1, \dots, n_2\}$$

and, therefore,

$$\begin{aligned} \sum_{\alpha,\beta=1}^{n_2} \hat{K}_{\alpha,\beta}^\dagger \hat{K}_{\alpha,\beta} &= \sum_{\alpha,\beta=1}^{n_2} \lambda_\beta \langle \phi_\beta^{(2)} | \hat{U}^\dagger | \phi_\alpha^{(2)} \rangle \langle \phi_\alpha^{(2)} | \hat{U} | \phi_\beta^{(2)} \rangle \\ &= \sum_{\beta=1}^{n_2} \lambda_\beta \underbrace{\langle \phi_\beta^{(2)} | \hat{U}^\dagger \hat{U} | \phi_\beta^{(2)} \rangle}_{=1} \\ &\stackrel{(4.5)}{=} 1. \end{aligned}$$

If, from an ensemble in the state (4.2), those individuals are selected (by projective measurement of the environment) for which \mathcal{S}_2 is in the partial state $|\psi_\alpha^{(2)}\rangle\langle\psi_\alpha^{(2)}|$ then (4.6) has to be replaced by¹²

$$\mathfrak{C}(\hat{\rho}') = \sum_{\beta=1}^{n_2} \hat{K}_{\alpha,\beta} \hat{\rho}' \hat{K}_{\alpha,\beta}^\dagger \quad \forall \hat{\rho}' \in S(\mathcal{H}_1)$$

and

$$\text{trace}(\mathfrak{C}(\hat{\rho})) \leq 1$$

is the relative number of individuals selected. In either case \mathcal{E} is just a special *quantum operation*:¹³

Definition 4.2.1 Let \mathcal{H} and \mathcal{H}' be HILBERT-spaces. Then by $\mathcal{Q}(\mathcal{H}, \mathcal{H}')$ we denote the set of all mappings \mathfrak{C} from $S(\mathcal{H})$ into $\mathcal{L}(\mathcal{H}')$ of the form

$$\mathfrak{C}(\hat{\rho}) = \sum_{k=1}^N \hat{K}_k \hat{\rho} \hat{K}_k^\dagger \quad \forall \hat{\rho} \in S(\mathcal{H}), \quad (4.7)$$

with suitable $N \in \mathbb{N}$ and $\hat{K}_k \in \mathcal{L}(\mathcal{H}, \mathcal{H}')$ fulfilling¹⁴

$$\sum_{k=1}^N \hat{K}_k^\dagger \hat{K}_k \leq \hat{1}. \quad (4.8)$$

———— DRAFT, June 26, 2009 ————

¹²For a corresponding representation of general linear maps see (Shabani and Lidar, 2006, Theorem1).

¹³ See (Buscemi et al., 2003) for efficient realizations and (Werner, 2001, Section 2.6.2) for the dual action of quantum operations on the observable algebras.

¹⁴Note that the adjoint \hat{K}^\dagger of a linear mapping $\hat{K} \in \mathcal{L}(\mathcal{H}, \mathcal{H}')$ is characterized by

$$\langle \psi' | \hat{K} \psi \rangle_{\mathcal{H}'} = \langle \hat{K}^\dagger \psi' | \psi \rangle_{\mathcal{H}} \quad \forall \psi \in \mathcal{H}, \psi' \in \mathcal{H}'.$$

Thus, e.g., $(|\psi'\rangle\langle\psi|)^\dagger = |\psi\rangle\langle\psi'|$.

The elements of $\mathcal{Q}(\mathcal{H}, \mathcal{H}')$ are called **quantum operations** and the \hat{K}_k in (4.7) are called **KRAUS operators for \mathfrak{C}** .

Remarks:

1. Note that¹⁵

$$0 \leq \underbrace{\text{trace}(\mathfrak{C}(\hat{\rho}))}_{\geq 0} \leq 1 \quad \forall \hat{\rho} \in S(\mathcal{H}_1)$$

and that

$$\sum_{k=1}^N \hat{K}_k^\dagger \hat{K}_k = \hat{1} \iff \text{trace}(\mathfrak{C}(\hat{\rho})) = 1 \quad \forall \hat{\rho} \in S(\mathcal{H}_1).$$

2. Obviously, we also have

$$\mathfrak{C}_1 \in \mathcal{Q}(\mathcal{H}_1, \mathcal{H}_2), \mathfrak{C}_2 \in \mathcal{Q}(\hat{\mathcal{H}}_2, \mathcal{H}_3) \implies \mathfrak{C}_2 \circ \mathfrak{C}_1 \in \mathcal{Q}(\mathcal{H}_1, \mathcal{H}_3).$$

3. But, given $\mathfrak{C}_1 \in \mathcal{Q}(\mathcal{H}_1, \mathcal{H}_2)$ and $\mathfrak{C}_3 \in \mathcal{Q}(\mathcal{H}_1, \mathcal{H}_3)$, this does **not** guarantee existence of an $\mathfrak{C}_2 \in \mathcal{Q}(\mathcal{H}_2, \mathcal{H}_3)$ with $\mathfrak{C}_3 = \mathfrak{C}_2 \circ \mathfrak{C}_1$.
4. Of course, nonexistence of such \mathfrak{C}_2 is only possible if \mathfrak{C}_1 is not invertible. The latter is obviously the case if, e.g., $\mathcal{H}_1 = \mathcal{H}_2$ and

$$\begin{aligned} \mathfrak{C}_1(\hat{\rho}) &= \frac{1}{4} \sum_{\nu=0}^3 \hat{\tau}^\nu \hat{\rho} \hat{\tau}^\nu \\ &= \frac{1}{2} \hat{1} \quad \forall \hat{\rho} \in S(\mathcal{H}). \end{aligned}$$

5. The linear extension

$$\bar{\mathfrak{C}}(\hat{A}) \stackrel{\text{def}}{=} \sum_{k=1}^N \hat{K}_k \hat{A} \hat{K}_k^\dagger \quad \forall \hat{A} \in \mathcal{L}(\mathcal{H}_1),$$

of \mathfrak{C} to all of $\mathcal{L}(\mathcal{H}_1)$ is **completely positive**,¹⁶ i.e.:

$$\hat{A}' \geq 0 \implies (\mathbf{1} \otimes \bar{\mathfrak{C}})(\hat{A}') \geq 0 \quad \forall \hat{A}' \in \underline{\mathbb{C}^n} \otimes \mathcal{H}_1, n \in \mathbb{N}.$$

DRAFT, June 26, 2009

¹⁵The possibility $\text{trace}(\underbrace{\mathfrak{C}(\hat{\rho})}_{\geq 0}) < 1$ is included to allow for absorption.

¹⁶Every trace preserving affine mapping of $S(\mathcal{H})$ into $S(\mathcal{H})$ can be represented as (the restriction of) a difference of two completely positive mappings (Kuah and Sudarshan, 2005).

Lemma 4.2.2 Let \mathcal{H}_1 and \mathcal{H}_2 be finite-dimensional HILBERT-spaces¹⁷ and let \mathfrak{C} be a mapping from $S(\mathcal{H}_1)$ into $\mathcal{L}(\mathcal{H}_2)$. Then \mathfrak{C} is a quantum operation, i.e. $\mathfrak{C} \in \mathcal{Q}(\mathcal{H}_1, \mathcal{H}_2)$, iff the following three conditions are fulfilled:

1.

$$\text{trace} \left(\mathfrak{C}(\hat{\rho}) \right) \leq 1 \quad \forall \hat{\rho} \in S(\mathcal{H}_1).$$

2.

$$\mathfrak{C} \left(\lambda \hat{\rho}_1 + (1 - \lambda) \hat{\rho}_2 \right) = \lambda \mathfrak{C}(\hat{\rho}_1) + (1 - \lambda) \mathfrak{C}(\hat{\rho}_2) \quad \forall \lambda \in [0, 1], \hat{\rho}_1, \hat{\rho}_2 \in S(\mathcal{H}_1).$$

3.

$$(\mathbf{1} \otimes \bar{\mathfrak{C}}) \left(|\Psi\rangle\langle\Psi| \right) \geq 0 \quad \forall \Psi \in \mathcal{H}_1 \otimes \mathcal{H}_1,$$

where $\bar{\mathfrak{C}}$ denotes the unique linear extension¹⁸ of \mathfrak{C} to all of $\mathcal{L}(\mathcal{H}_1)$.

Outline of proof: Assume that \mathfrak{C} fulfills the requirements 1–3. Choose an orthonormal basis $\{\phi_1^{(1)}, \dots, \phi_{n_1}^{(1)}\}$ of \mathcal{H}_1 and defining

$$\psi^* \stackrel{\text{def}}{=} \sum_{\nu=1}^{n_1} \langle \psi | \phi_{\nu}^{(1)} \rangle \phi_{\nu}^{(1)} \quad \forall \psi \in \mathcal{H}_1 \quad (4.9)$$

we get

$$\langle \psi^* | \phi_{\nu}^{(1)} \rangle = \langle \phi_{\nu}^{(1)} | \psi \rangle \quad \forall \psi \in \mathcal{H}_1, \nu \in \{1, \dots, n_1\}$$

and hence¹⁹

$$\begin{aligned} \mathfrak{C}(|\psi\rangle\langle\psi|) &\stackrel{2. \text{ req.}}{=} \sum_{\nu, \mu=1}^{n_1} \langle \phi_{\nu}^{(1)} | \psi \rangle \langle \psi | \phi_{\mu}^{(1)} \rangle \bar{\mathfrak{C}} \left(|\phi_{\nu}^{(1)}\rangle\langle\phi_{\mu}^{(1)}| \right) \\ &= \sum_{\nu, \mu=1}^{n_1} \langle \psi^* | \left(|\phi_{\nu}^{(1)}\rangle\langle\phi_{\mu}^{(1)}| \otimes \bar{\mathfrak{C}} \left(|\phi_{\nu}^{(1)}\rangle\langle\phi_{\mu}^{(1)}| \right) \right) | \psi^* \rangle \\ &= \langle \psi^* | \hat{A} | \psi^* \rangle \quad \forall \psi \in \mathcal{H}_1, \|\psi\| = 1, \end{aligned} \quad (4.10)$$

———— DRAFT, June 26, 2009 ————

¹⁷Since we agreed to consider only finite-dimensional HILBERT spaces, all operators on \mathcal{H}_1 resp. \mathcal{H}_2 are of trace class. For infinite-dimensional HILBERT spaces $\mathcal{H}_1 = \mathcal{H}_2$ see (Davies, 1976, Theorem 2.3 and notes on page 147).

¹⁸Existence of this extension, is guaranteed by the second condition. For self-adjoint \hat{A} it is given by

$$\bar{\mathfrak{C}}(\hat{A}) \stackrel{\text{def}}{=} \text{trace}(\hat{A}_+) \mathfrak{C} \left(\frac{\hat{A}_+}{(\text{trace } \hat{A}_+)} \right) + \text{trace}(\hat{A}_-) \mathfrak{C} \left(\frac{\hat{A}_-}{(\text{trace } \hat{A}_-)} \right),$$

where \hat{A}_+ resp. \hat{A}_- denotes the positive resp. negative part of \hat{A} :

$$\hat{A} = \hat{A}_+ + \hat{A}_- \quad \pm \hat{A}_{\pm} \geq 0, \quad \hat{A}_+ \hat{A}_- = \hat{0}.$$

Linear mappings from $\mathcal{L}(\mathcal{H}_1)$ into $\mathcal{L}(\mathcal{H}_2)$ are also called *superoperators*.

¹⁹We use the notation explained in Footnote 11, with the roles of the tensor factors $\mathcal{H}_1, \mathcal{H}_2$ interchanged.

where

$$\begin{aligned}\hat{A} &\stackrel{\text{def}}{=} \sum_{\nu,\mu=1}^{n_1} |\phi_\nu^{(1)}\rangle\langle\phi_\mu^{(1)}| \otimes \bar{\mathfrak{C}}(|\phi_\nu^{(1)}\rangle\langle\phi_\mu^{(1)}|) \\ &= (\mathbf{1} \otimes \bar{\mathfrak{C}}) \underbrace{\left(\sum_{\nu,\mu=1}^{n_1} |\phi_\nu^{(1)}\rangle\langle\phi_\mu^{(1)}| \otimes |\phi_\nu^{(1)}\rangle\langle\phi_\mu^{(1)}| \right)}_{=|\sum_{\nu=1}^{n_1} \phi_\nu^{(1)} \otimes \phi_\nu^{(1)}\rangle\langle\sum_{\nu=1}^{n_1} \phi_\nu^{(1)} \otimes \phi_\nu^{(1)}| \geq 0}\end{aligned}$$

and hence

$$0 \underset{3. \text{ req.}}{\leq} \hat{A} \in \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2).$$

This, together with the spectral theorem implies

$$\hat{A} = \sum_{k=1}^N |\Psi_k\rangle\langle\Psi_k| \quad \text{for suitable } \Psi_1, \dots, \Psi_N \in \mathcal{H}_1 \otimes \mathcal{H}_2.$$

The latter, together with (4.10) gives

$$\bar{\mathfrak{C}}(|\psi\rangle\langle\psi|) = \sum_{k=1}^N \langle\psi^*|\Psi_k\rangle\langle\Psi_k|\psi^*\rangle \quad \forall \psi \in \mathcal{H}_1.$$

Thus, defining the linear mappings²⁰

$$\hat{K}_k \psi \stackrel{\text{def}}{=} \langle\psi^*|\Psi_k\rangle \quad \forall \psi \in \mathcal{H}_1, k \in \{1, \dots, N\}$$

from \mathcal{H}_1 into \mathcal{H}_2 we get

$$\mathfrak{C}(|\psi\rangle\langle\psi|) = \sum_{k=1}^N \hat{K}_k |\psi\rangle\langle\psi| \hat{K}_k^\dagger \quad \forall \psi \in \mathcal{H}_1, \|\psi\| = 1.$$

By condition 2 this gives (4.7). The latter together with condition 1, finally, gives²¹ (4.8).

Conversely, conditions 1–3 are easily seen to be fulfilled for $\mathfrak{C} \in \mathcal{Q}(\mathcal{H}_1, \mathcal{H}_2)$. \blacksquare

Remark: At first glance one might consider conditions 1–3 of Lemma 4.2.2 as natural requirements on the action of quantum channels. Note, however, that the output state of a quantum channel need not even be determined by the input state in case of initial correlations with the environment.²²

———— DRAFT, June 26, 2009 ————

²⁰Here, we use the notation

$$\langle\psi| \left| \sum_{j=1}^{N'} \psi_j^{(1)} \otimes \psi_j^{(2)} \right\rangle \stackrel{\text{def}}{=} \sum_{j=1}^{N'} \langle\psi| \psi_j^{(1)} \rangle \psi_j^{(2)}$$

for $\psi, \psi_1^{(1)}, \dots, \psi_{N'}^{(1)} \in \mathcal{H}_1$ and $\psi_1^{(2)}, \dots, \psi_{N'}^{(2)} \in \mathcal{H}_2$.

²¹Violation of (4.8) would imply existence of a normalized eigenvector ψ_+ of $\sum_{k=1}^N \hat{K}_k^\dagger \hat{K}_k$ with eigenvalue greater than 1 and thus $\text{trace}(\mathfrak{C}(\hat{\rho})) > 1$ for $\hat{\rho} = |\psi_+\rangle\langle\psi_+|$.

²²Recall Footnote 10. See also (Kuah and Sudarshan, 2005), in this connection.

Definition 4.2.1 and Lemma 4.2.1 describe the most general quantum operations. Simple versions are, among others:

1. Unitary transformations

$$\hat{\rho}' \longmapsto \mathfrak{C}(\hat{\rho}') = \hat{V} \hat{\rho} \hat{V}^\dagger$$

given, e.g., by (4.4) for

$$\hat{U} = \hat{V} \times \hat{V}', \quad \hat{V} \text{ unitary.}$$

2. Complete projective measurement operations

$$\hat{\rho}' \longmapsto \mathfrak{C}(\hat{\rho}') = \sum_{j=1}^{n_1} \hat{P}_{\phi_j^{(1)}} \hat{\rho} \hat{P}_{\phi_j^{(1)}}, \quad \{\phi_1^{(1)}, \dots, \phi_{n_1}^{(1)}\} \text{ orthonormal basis of } \mathcal{H}_1,$$

given, e.g., by (4.4) if there are $\hat{\rho}_1^{(2)}, \dots, \hat{\rho}_{n_1}^{(2)} \in \mathcal{S}(\mathcal{H}_2)$ with pairwise orthogonal supports and such that²³

$$\hat{U} \hat{P}_{\phi_j^{(1)}} \otimes \hat{\rho}_j^{(2)} \hat{U}^\dagger = \hat{P}_{\phi_j^{(1)}} \otimes \hat{\rho}_j^{(2)} \quad \forall j \in \{1, \dots, n_1\}.$$

Example:²⁴

$$\begin{aligned} \hat{U} &= \text{action of CNOT,} \\ \mathcal{S}_1 &= \text{control qubit,} \\ \mathcal{S}_2 &= \text{target qubit,} \\ \hat{\rho}^{(2)} &= |0\rangle\langle 0| \text{ (or } |1\rangle\langle 1|). \end{aligned}$$

3. Cascaded complete projective measurement operations

$$\hat{\rho}' \longmapsto \mathfrak{C}(\hat{\rho}') = \sum_{j_1, \dots, j_r=1}^{n_1} \hat{K}_{(j_1, \dots, j_r)} \hat{\rho}' \hat{K}_{(j_1, \dots, j_r)}^\dagger,$$

where

$$\hat{K}_{(j_1, \dots, j_r)} = \hat{P}_{r, j_r} \cdots \hat{P}_{1, j_1} \quad \forall (j_1, \dots, j_r) \in \{1, \dots, n_1\}^r$$

with $\hat{P}_{k,1}, \dots, \hat{P}_{k,n_1}$ being the projectors of the k -th projective measurement.

Remark: Note that

$$\sum_{j_1, \dots, j_r=1}^{n_1} \hat{K}_{(j_1, \dots, j_r)}^\dagger \hat{K}_{(j_1, \dots, j_r)} = 1$$

but that, in general, the $\hat{K}_{(j_1, \dots, j_r)}$ are no longer projection operators.

DRAFT, June 26, 2009

²³In this case *nondemolition* measurements on \mathcal{S}_1 can be performed by corresponding (usually destructive) measurements on \mathcal{S}_2 . Note, however, that for the resulting partial state of \mathcal{S}_1 it does not matter whether the state of the environment, including the *measurement apparatus*, is checked or not (the possibility of *postselection* is sufficient).

²⁴Another example would be the STERN-GERLACH measurement if it really worked as usually described.

Theorem 4.2.3 *Let \mathcal{H}_1 and \mathcal{H}_2 be HILBERT-spaces and let $\hat{K}_1, \dots, \hat{K}_N, \hat{K}'_1, \dots, \hat{K}'_N \in \mathcal{L}(\mathcal{H}_1, \mathcal{H}_2)$. Then*

$$\sum_{k=1}^N \hat{K}_k \hat{\rho} (\hat{K}_k)^\dagger = \sum_{k=1}^N \hat{K}'_k \hat{\rho} (\hat{K}'_k)^\dagger \quad \forall \hat{\rho} \in \mathcal{S}(\mathcal{H}_1) \quad (4.11)$$

iff there is a unitary $N \times N$ -matrix (U^j_k) with

$$\hat{K}'_j = \sum_{k=1}^N U^j_k \hat{K}_k \quad \forall j \in \{1, \dots, N\}. \quad (4.12)$$

Outline of proof: Assume that (4.11) holds. Then, if we choose an orthonormal basis $\{\phi_1, \dots, \phi_n\}$ of \mathcal{H}_1 and define

$$\begin{aligned} \Psi_k &\stackrel{\text{def}}{=} \sum_{\nu=1}^n \phi_\nu \otimes (\hat{K}_k \phi_\nu), \\ \Psi'_k &\stackrel{\text{def}}{=} \sum_{\nu=1}^n \phi_\nu \otimes (\hat{K}'_k \phi_\nu) \end{aligned}$$

for $k \in \{1, \dots, N\}$, we get

$$\begin{aligned} \sum_{k=1}^N |\Psi_k\rangle\langle\Psi_k| &= \sum_{k=1}^N \sum_{\nu, \mu=1}^n (|\phi_\nu\rangle\langle\phi_\mu|) \otimes (\hat{K}_k |\phi_\nu\rangle\langle\phi_\mu| (\hat{K}_k)^\dagger) \\ &\stackrel{(4.11)}{=} \sum_{k=1}^N \sum_{\nu, \mu=1}^n (|\phi_\nu\rangle\langle\phi_\mu|) \otimes (\hat{K}'_k |\phi_\nu\rangle\langle\phi_\mu| (\hat{K}'_k)^\dagger) \\ &= \sum_{k=1}^N |\Psi'_k\rangle\langle\Psi'_k|. \end{aligned}$$

Therefore, by Corollary A.4.3, there is a unitary $N \times N$ -matrix (U^j_k) with

$$\Psi_k = \sum_{j=1}^N U_k^j \Psi'_j \quad \forall k \in \{1, \dots, N\},$$

i.e. with

$$\sum_{\nu=1}^n \phi_\nu \otimes (\hat{K}_k \phi_\nu) = \sum_{\nu=1}^n \phi_\nu \otimes \left(\sum_{j=1}^N U_k^j \hat{K}'_j \phi_\nu \right) \quad \forall k \in \{1, \dots, N\}.$$

This implies

$$\hat{K}_k \phi_\nu = \sum_{j=1}^N U_k^j \hat{K}'_j \phi_\nu \quad \forall \nu \in \{1, \dots, n\}, k \in \{1, \dots, N\}$$

and hence (4.12).

Conversely, it is obvious that (4.12) implies (4.11). \blacksquare

The standard example, in case $n_1 > 1$, for a mapping \mathfrak{C} of $S(\mathcal{H}_1)$ into $S(\mathcal{H}_1)$ fulfilling conditions 1 and 2, but **not** 3, of Lemma 4.2.2 is the **transposition**²⁵

$$\hat{\rho}' = \sum_{j,k=1}^{n_1} \rho_k^j \left| \phi_j^{(1)} \right\rangle \left\langle \phi_k^{(1)} \right| \longmapsto \mathfrak{C}(\hat{\rho}') = \mathfrak{T}(\hat{\rho}') \stackrel{\text{def}}{=} \sum_{j,k=1}^{n_1} \rho_k^j \left| \phi_k^{(1)} \right\rangle \left\langle \phi_j^{(1)} \right|. \quad (4.13)$$

depending on the basis $\left\{ \phi_1^{(1)}, \dots, \phi_{n_1}^{(1)} \right\}$ of \mathcal{H}_1 .

Proof of positivity: Thanks to the spectral theorem it is sufficient to show that $S_{\text{pure}}(\mathcal{H}_1)$ is left invariant under transposition. This, however follows from²⁶

$$\mathfrak{T}\left(|\phi\rangle\langle\psi| \right) = |\psi^*\rangle\langle\phi^*| \quad \forall \phi, \psi \in \mathcal{H}_1. \quad \blacksquare \quad (4.14)$$

Disproof of complete positivity: Obviously, it is sufficient to check the case $n_1 = 2$. Then, with

$$|jk\rangle \stackrel{\text{def}}{=} \phi_j^{(1)} \otimes \phi_k^{(1)} \quad \forall j, k \in \{1, 2\},$$

we have

$$\begin{aligned} (\mathbf{1} \otimes \bar{\mathfrak{T}})(\hat{W}_\lambda) &= \frac{1-\lambda}{4} \left(|0,0\rangle\langle 0,0| + |1,1\rangle\langle 1,1| \right) \\ &\quad + \frac{1+\lambda}{4} \left(|0,1\rangle\langle 0,1| + |1,0\rangle\langle 1,0| \right) \\ &\quad - \frac{\lambda}{2} \left(|1,1\rangle\langle 0,0| + |0,0\rangle\langle 1,1| \right) \end{aligned} \quad (4.15)$$

for the WERNER states²⁷

$$\hat{W}_\lambda \stackrel{\text{def}}{=} \frac{1-\lambda}{4} \hat{\mathbf{1}} \otimes \hat{\mathbf{1}} + \lambda |\Psi^-\rangle\langle\Psi^-|, \quad \lambda \in [0, 1].$$

But for $\lambda > 1/3$ (4.15) cannot be positive, since, e.g.

$$\left((\mathbf{1} \otimes \bar{\mathfrak{T}})(\hat{W}_\lambda) \right) \left(|0,0\rangle + |1,1\rangle \right) = \frac{1-3\lambda}{4} \left(|0,0\rangle + |1,1\rangle \right). \quad \blacksquare$$

———— DRAFT, June 26, 2009 ————

²⁵Note that, for $\hat{\rho}' \in S(\mathcal{H}_1)$, transposition is equivalent to complex conjugation

$$\hat{\rho}' = \sum_{j,k=1}^{n_1} \rho_k^j \left| \phi_j^{(1)} \right\rangle \left\langle \phi_k^{(1)} \right| \longmapsto \sum_{j,k=1}^{n_1} \left(\rho_k^j \right)^* \left| \phi_j^{(1)} \right\rangle \left\langle \phi_k^{(1)} \right|.$$

²⁶Recall (4.9).

²⁷These states are distinguished by their invariance property

$$\left(\hat{U} \otimes \hat{U} \right) \hat{W}_\lambda \left(\hat{U} \otimes \hat{U} \right)^\dagger = \hat{W}_\lambda \quad \text{for all unitary } \hat{U} \in \mathcal{L}(\mathcal{H})$$

(Werner, 1989, Section II). Note that the **flip operator**

$$|0,0\rangle\langle 0,0| + |1,0\rangle\langle 0,1| + |0,1\rangle\langle 1,0| + |1,1\rangle\langle 1,1|$$

coincides with $\hat{\mathbf{1}} \otimes \hat{\mathbf{1}} - 2 |\Psi^-\rangle\langle\Psi^-|$.

4.2.2 Quantum Noise and Error Correction

The action of noisy quantum channels corresponds to non-invertible quantum operations \mathfrak{C} . Nevertheless such an operation may become invertible by restriction to states with support on a suitable subspace \mathcal{C} of \mathcal{H} — and thus allow for *error correction* on the *code space* \mathcal{C} .

Theorem 4.2.4 *Let \mathcal{H} be HILBERT space, $\mathfrak{C} \in \mathcal{Q}(\mathcal{H}, \mathcal{H})$ and let \mathcal{C} be a linear subspace of \mathcal{H} . Then the following three statements are equivalent:*

1. *There are KRAUS operators $\hat{K}_1, \dots, \hat{K}_N$ for \mathfrak{C} and $a_1, \dots, a_N \geq 0$ with*

$$\hat{P}_{\mathcal{C}} \hat{K}_j^\dagger \hat{K}_k \hat{P}_{\mathcal{C}} = \delta_{jk} a_j \hat{P}_{\mathcal{C}} \quad \forall j, k \in \{1, \dots, N\}. \quad (4.16)$$

2. *There is a trace preserving quantum operation \mathfrak{R} with*

$$(\mathfrak{R} \circ \mathfrak{C})(|\psi\rangle\langle\psi|) \propto |\psi\rangle\langle\psi| \quad \forall \psi \in \mathcal{C} \quad \|\psi\| = 1. \quad (4.17)$$

3. *There are KRAUS operators $\hat{K}'_1, \dots, \hat{K}'_N$ for \mathfrak{C} with*

$$\hat{P}_{\mathcal{C}} \hat{K}'_j \hat{K}'_k \hat{P}_{\mathcal{C}} = a_{jk} \hat{P}_{\mathcal{C}} \quad \forall j, k \in \{1, \dots, N\} \quad (4.18)$$

for some self-adjoint matrix (a_{jk}) .

Outline of proof: Assume the first statement to be true. Then, using the polar decomposition

$$\begin{aligned} \hat{K}_j \hat{P}_{\mathcal{C}} &= \hat{U}_j \sqrt{\hat{P}_{\mathcal{C}} \hat{K}_j^\dagger \hat{K}_j \hat{P}_{\mathcal{C}}} \\ &= \sqrt{a_j} \hat{U}_j \hat{P}_{\mathcal{C}} \end{aligned} \quad (4.19)$$

(see, e.g., Lemma 7.3.20 of (Lücke, eine)) we have

$$\delta_{jk} \hat{P}_{\mathcal{C}} = \hat{P}_{\mathcal{C}} \hat{U}_j^\dagger \hat{U}_k \hat{P}_{\mathcal{C}} \quad (4.20)$$

and hence

$$\hat{P}_{\hat{U}_j \mathcal{C}} \hat{P}_{\hat{U}_k \mathcal{C}} = \delta_{jk} \hat{P}_{\hat{U}_j \mathcal{C}}. \quad (4.21)$$

For

$$\mathfrak{R}(\hat{\rho}) \stackrel{\text{def}}{=} \sum_{j=1}^N (\hat{U}_j^\dagger \hat{P}_{\hat{U}_j \mathcal{C}}) \hat{\rho} (\hat{U}_j \hat{P}_{\hat{U}_j \mathcal{C}})^\dagger + \hat{P}_0 \hat{\rho} \hat{P}_0 \quad \forall \hat{\rho} \in S(\mathcal{H}), \quad (4.22)$$

where

$$\hat{P}_0 \stackrel{\text{def}}{=} \hat{1} - \sum_{j=1}^N \hat{P}_{\hat{U}_j \mathcal{C}} \quad (4.23)$$

and thus

$$\begin{aligned} \hat{P}_0 \mathfrak{C}(\hat{P}_{\mathcal{C}} \hat{\rho} \hat{P}_{\mathcal{C}}) \hat{P}_0 &\stackrel{(4.19)}{=} \sum_{j=1}^N a_j \hat{P}_0 \hat{U}_j \hat{P}_{\mathcal{C}} \hat{\rho} \hat{P}_{\mathcal{C}} \hat{U}_j^\dagger \hat{P}_0 \\ &\stackrel{(4.21)}{=} 0 \quad \forall \hat{\rho} \in S(\mathcal{H}), \end{aligned}$$

this gives²⁸

$$\begin{aligned} (\mathfrak{R} \circ \mathfrak{C})(|\psi\rangle\langle\psi|) &= \sum_{j,k=1}^N \hat{P}_C \hat{U}_j^\dagger \hat{P}_{\hat{U}_j C} \underbrace{\hat{K}_k |\psi\rangle}_{\substack{= \\ (4.19) \\ \sqrt{a_k} \hat{U}_k |\psi\rangle}} \langle\psi| \hat{K}_k^\dagger \hat{P}_{\hat{U}_j C} \hat{U}_j \hat{P}_C \quad (4.24) \\ &\quad \underbrace{\hspace{10em}}_{\substack{= \\ (4.21) \\ \delta_{jk} \sqrt{a_k} \hat{U}_k |\psi\rangle}} \\ &\stackrel{(4.20)}{=} \sum_{j=1}^N a_j |\psi\rangle\langle\psi| \quad \forall \psi \in \mathcal{C}. \end{aligned}$$

Since

$$\sum_{j=1}^N \left(\hat{U}_j^\dagger \hat{P}_{\hat{U}_j C} \right)^\dagger \left(\hat{U}_j^\dagger \hat{P}_{\hat{U}_j C} \right) + \hat{P}_0^\dagger \hat{P}_0 \stackrel{(4.21)}{=} \hat{1},$$

this implies the second statement.²⁹ Now assume the second statement to be true. Then (4.17) holds and, of course,³⁰ $\text{trace} \left(\mathfrak{C}(|\psi\rangle\langle\psi|) \right)$ must be constant for normalized $\psi \in \mathcal{C}$. Therefore,

$$(\mathfrak{R} \circ \mathfrak{C}) \left(\hat{P}_C \hat{\rho} \hat{P}_C \right) = \gamma \hat{P}_C \hat{\rho} \hat{P}_C \quad \forall \hat{\rho} \in S(\mathcal{H}) \quad (4.25)$$

holds for some $\gamma \geq 0$. If $\hat{K}'_1, \dots, \hat{K}'_N$ are KRAUS operators for \mathfrak{C} and $\hat{R}_1, \dots, \hat{R}_N$ are KRAUS operators for \mathfrak{R} then (4.25) is equivalent to

$$\sum_{j,k=1}^N \hat{R}_j \hat{K}'_k \hat{P}_C \hat{\rho} \hat{P}_C \hat{K}'_k{}^\dagger \hat{R}_j^\dagger = \gamma \hat{P}_C \hat{\rho} \hat{P}_C \quad \forall \hat{\rho} \in S(\mathcal{H}).$$

Then,³¹ by Theorem 4.2.3, there are complex numbers λ_{jk} with

$$\hat{R}_j \hat{K}'_k \hat{P}_C = \lambda_{jk} \hat{P}_C \quad \forall j, k \in \{1, \dots, N\}$$

and hence

$$\hat{P}_C \hat{K}'_l{}^\dagger \hat{R}_j^\dagger \hat{R}_j \hat{K}'_k \hat{P}_C = \lambda_{jl}^* \lambda_{jk} \hat{P}_C \quad \forall j, k, l \in \{1, \dots, N\}.$$

Since \mathfrak{R} is trace preserving, this implies the third statement with

$$a_{lk} = \sum_{j=1}^N \lambda_{jl}^* \lambda_{jk} \quad \forall k, l \in \{1, \dots, N\}.$$

Finally, assume the third statement to be true. Then, by the spectral theorem, there are a unitary matrix (u_{jk}) and real numbers a_1, \dots, a_N with

$$\sum_{j',k'=1}^N u_{j'j}^* a_{j'k'} u_{k'k} = a_j \delta_{j,k} \quad \forall j, k \in \{1, \dots, N\}.$$

DRAFT, June 26, 2009

²⁸Note that $\hat{P}_C \hat{U}_j^\dagger \hat{P}_{\hat{U}_j C} = \hat{U}_j^\dagger \hat{P}_{\hat{U}_j C}$.

²⁹Recall Remark 1 to Definition 4.2.1.

³⁰Note that for $\hat{\rho}_1, \hat{\rho}_2 \in S(\mathcal{H})$ and $\lambda_1, \lambda_2 \in \mathbb{C}$ we have

$$\left. \begin{array}{l} \lambda_1 \hat{\rho}_1 + \lambda_2 \hat{\rho}_2 \propto \hat{\rho}_1 + \hat{\rho}_2 \\ \hat{\rho}_1 \neq \hat{\rho}_2 \end{array} \right\} \implies \lambda_1 = \lambda_2.$$

³¹We may add $N - 1$ zeros as KRAUS operators to $\sqrt{\gamma} \hat{P}_C$.

This, together with (4.18), implies the first statement with

$$\hat{K}_j = \sum_{k=1}^N u_{kj} \hat{K}'_k \quad \forall j \in \{1, \dots, N\} . \quad \blacksquare$$

Remark: (4.19), (4.21), and (4.22) show how errors produced by \mathfrak{C} can be corrected for the code \mathcal{C} :

Perform a projective measurement w.r.t. the orthogonal subspaces $\hat{U}_j \mathcal{C}$ and apply \hat{U}_j^\dagger according to the result of this ‘measurement’.

Corollary 4.2.5 *Let \mathcal{C} be a linear subspace of the HILBERT space \mathcal{H} and let $\hat{K}_1, \dots, \hat{K}_N$ resp. $\hat{K}'_1, \dots, \hat{K}'_N$ be KRAUS operators for $\mathfrak{C} \in \mathcal{Q}(\mathcal{H}, \mathcal{H})$ resp. $\mathfrak{C}' \in \mathcal{Q}(\mathcal{H}, \mathcal{H})$. If (4.16) holds and if the \hat{K}'_j are complex linear combinations of the \hat{K}_j then, with \mathfrak{R} as constructed in the proof of Theorem 4.2.4, (4.17) holds also for \mathfrak{C} replaced by \mathfrak{C}' .*

Outline of proof: Assume that

$$\hat{K}'_j = \sum_{k=1}^N \lambda_{jk} \hat{K}_k$$

and let \mathfrak{R} be defined as in the proof of Theorem 4.2.4. Then

$$\begin{aligned} & (\mathfrak{R} \circ \mathfrak{C}')(|\psi\rangle\langle\psi|) \\ & \stackrel{(4.24)}{=} \sum_{j,k,l,r=1}^N \left(\hat{P}_C \hat{U}_j^\dagger \hat{P}_{\hat{U}_j \mathcal{C}} \right) \lambda_{kl} \sqrt[4]{a_k} \hat{U}_l \hat{P}_C |\psi\rangle\langle\psi| \lambda_{kr}^* \sqrt[4]{a_r} \hat{P}_C \hat{U}_r^\dagger \left(\hat{P}_C \hat{U}_j^\dagger \hat{P}_{\hat{U}_j \mathcal{C}} \right)^\dagger \\ & \stackrel{(4.21)}{=} \sum_{j,k=1}^N a_j |\lambda_{kl}|^2 |\psi\rangle\langle\psi| \quad \forall \psi \in \mathcal{C} . \quad \blacksquare \end{aligned}$$

4.3 Error Correcting Codes

4.3.1 General Aspects

According to standard formulations (Lücke, 1996) the time evolution of **closed**³² quantum mechanical systems is unitary.

Let us consider the closed system of one qubit together with its environment. A unitary transformation of the corresponding state space maps separated pure states to **entangled** pure states:

$$\begin{aligned} |\chi\rangle &= \left(\alpha |0\rangle + \beta |1\rangle \right) \otimes |E\rangle \\ \longmapsto |\chi'\rangle &= \alpha \left(|0\rangle \otimes |E_{0,0}\rangle + |1\rangle \otimes |E_{0,1}\rangle \right) + \beta \left(|0\rangle \otimes |E_{1,0}\rangle + |1\rangle \otimes |E_{1,1}\rangle \right) \end{aligned} \quad (4.26)$$

DRAFT, June 26, 2009

³²For **open** quantum systems see (Alicki, 2003) and references given there.

($\forall \alpha, \beta \in \mathbb{C}$). This way the originally pure **partial** state³³

$$\langle \chi | \hat{A} \otimes \hat{I} | \chi \rangle = |\alpha|^2 \langle 0 | \hat{A} | 0 \rangle + |\beta|^2 \langle 1 | \hat{A} | 1 \rangle + 2 \Re(\bar{\alpha} \beta \langle 0 | \hat{A} | 1 \rangle) \quad \forall \hat{A} \in \mathcal{L}_{\text{sa}}(\mathbb{C}^2)$$

may become a mixture:³⁴

$$\langle \chi' | \hat{A} \otimes \hat{I} | \chi' \rangle = |\alpha|^2 \langle 0 | \hat{A} | 0 \rangle + |\beta|^2 \langle 1 | \hat{A} | 1 \rangle \quad \text{if}^{35} \quad \langle E_{j,k} | E_{lm} \rangle = \delta_{jl} \delta_{k0} \delta_{m0}.$$

In other words:

The environment may cause **decoherence**.

Therefore, we have to be able to undo unwanted changes caused by the environment.

Now, for arbitrary vectors $|E_r\rangle$ from the state space of the environment we have

$$\sum_{r=0}^3 (\hat{\sigma}_r |0\rangle) \otimes |E_r\rangle = |0\rangle \otimes (|E_0\rangle + |E_3\rangle) + |1\rangle \otimes (|E_1\rangle + i |E_2\rangle) \quad (4.27)$$

and

$$\sum_{r=0}^3 (\hat{\sigma}_r |1\rangle) \otimes |E_r\rangle = |0\rangle \otimes (|E_1\rangle - i |E_2\rangle) + |1\rangle \otimes (|E_0\rangle - |E_3\rangle), \quad (4.28)$$

where the $\hat{\sigma}_r$ correspond to the PAULI **matrices**.³⁶

$$\sigma_0 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 \stackrel{\text{def}}{=} \begin{pmatrix} 0 & -i \\ +i & 0 \end{pmatrix}, \quad \sigma_3 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (4.29)$$

Equations (4.26)–(4.28) imply

$$|\chi'\rangle = \sum_{r=0}^3 (\sigma_r (\alpha |0\rangle + \beta |1\rangle)) \otimes |E_r\rangle \quad (4.30)$$

if

$$\begin{aligned} |E_{0,0}\rangle &= |E_0\rangle + |E_3\rangle, & |E_{0,1}\rangle &= |E_1\rangle + i |E_2\rangle, \\ |E_{1,0}\rangle &= |E_1\rangle - i |E_2\rangle, & |E_{1,1}\rangle &= |E_0\rangle - |E_3\rangle, \end{aligned}$$

i.e. if

$$\begin{aligned} |E_0\rangle &= \frac{|E_{0,0}\rangle + |E_{1,1}\rangle}{2}, & |E_1\rangle &= \frac{|E_{0,1}\rangle + |E_{1,0}\rangle}{2}, \\ |E_2\rangle &= \frac{|E_{0,1}\rangle - |E_{1,0}\rangle}{2i}, & |E_3\rangle &= \frac{|E_{0,0}\rangle - |E_{1,1}\rangle}{2}. \end{aligned}$$

³³We assume that $|\alpha|^2 + |\beta|^2 = 1$ and $\langle E | E \rangle = 1$.

³⁴This is why *open* quantum mechanical systems (Davies, 1976) do **not** evolve unitarily.

³⁵Consider, e.g., the simple example $|E\rangle = |0\rangle$, $|\chi'\rangle = \text{CNOT} |\chi\rangle$.

³⁶Hence $\hat{\sigma}_0 = \hat{I}$, $\hat{\sigma}_1 = \hat{\sigma}_x$, $\hat{\sigma}_3 = \hat{S}_\pi$, $\hat{\sigma}_2 = i \hat{\sigma}_1 \hat{\sigma}_3$.

(4.30) tells us that there are only three types of errors to be corrected, corresponding to³⁷ $\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3$. In this sense the set of possible errors for single-qubit systems is discrete.

More generally, a unitary operation of the state space of an n -qubit system and its environment acts according to³⁸

$$\sum_{\mathbf{b} \in \{0,1\}^n} \lambda_{\mathbf{b}} |\mathbf{b}\rangle \otimes |E\rangle \mapsto \sum_{\mathbf{b} \in \{0,1\}^n} \lambda_{\mathbf{b}} \sum_{\mathbf{b}' \in \{0,1\}^n} |\mathbf{b}'\rangle \otimes |E_{\mathbf{b},\mathbf{b}'}\rangle, \quad (4.31)$$

where the $|E_{\mathbf{b},\mathbf{b}'}\rangle$ are suitable state vectors of the environment depending on $|E\rangle$ (and \mathbf{b}, \mathbf{b}' , of course), but not on the $\lambda_{\mathbf{b}}$. Now, from (4.27)/(4.28) we see that for arbitrary states $|E_{b,b'}\rangle$ of the environment there are vectors $|E_r\rangle$ with

$$\sum_{r=0}^3 (\hat{\sigma}_r |b\rangle) \otimes |E_r\rangle = \sum_{b' \in \{0,1\}} |b'\rangle \otimes |E_{b,b'}\rangle \quad \forall b \in \{0,1\}.$$

Straightforward induction shows that for arbitrary state vectors $|E_{\mathbf{b},\mathbf{b}'}\rangle$ there are corresponding state vectors $|E_{\mathbf{r}}(\mathbf{b})\rangle$; $\mathbf{r} \in \{0, \dots, 3\}^n$; with

$$\sum_{\mathbf{r} \in \{0,1,2,3\}^n} (\hat{\sigma}_{\mathbf{r}} |\mathbf{b}\rangle) \otimes |E_{\mathbf{r}}(\mathbf{b})\rangle = \sum_{\mathbf{b}' \in \{0,1\}^n} |\mathbf{b}'\rangle \otimes |E_{\mathbf{b},\mathbf{b}'}\rangle \quad \forall \mathbf{b} \in \{0,1\}^n,$$

where

$$\hat{\sigma}_{\mathbf{r}} \stackrel{\text{def}}{=} \hat{\sigma}_{r_1} \otimes \dots \otimes \hat{\sigma}_{r_n} \quad \forall \mathbf{r} \in \{0, \dots, 3\}^n.$$

Together with (4.31) this shows that every unitary action on an n -qubit system³⁹ and its environment is of the form

$$\sum_{\mathbf{b} \in \{0,1\}^n} \lambda_{\mathbf{b}} |\mathbf{b}\rangle \otimes |E\rangle \mapsto \sum_{\mathbf{b} \in \{0,1\}^n} \lambda_{\mathbf{b}} \sum_{\mathbf{r} \in \{0,1,2,3\}^n} (\hat{\sigma}_{\mathbf{r}} |\mathbf{b}\rangle) \otimes |E_{\mathbf{r}}(\mathbf{b})\rangle, \quad \forall \mathbf{b} \in \{0,1\}^n.$$

Usually, in the theory of quantum error correction, only the case

$$|E_{\mathbf{r}}(\mathbf{b})\rangle = |E_{\mathbf{r}}\rangle \quad \forall \mathbf{b} \in \{0,1\}^n, \quad \mathbf{r} \in \{0,1,2,3\}^n$$

DRAFT, June 26, 2009

³⁷Of course, the $\hat{\sigma}_\nu$ are not the only set of operators serving this purpose:

$$\begin{aligned} \hat{\sigma}'_r &\stackrel{\text{def}}{=} \sum_{s=0}^3 u_{rs} \hat{\sigma}_s, & |E'_r\rangle &\stackrel{\text{def}}{=} \sum_{s=0}^3 u_{rs}^* |E_s\rangle, & \sum_{q=0}^3 u_{rq} u_{qs}^* &= \delta_{rs} \\ \implies \sum_{r=0}^3 (\hat{\sigma}'_r |b\rangle) \otimes |E'_r\rangle &= \sum_{r=0}^3 (\hat{\sigma}_r |b\rangle) \otimes |E_r\rangle & \forall b \in \{0,1\}. \end{aligned}$$

³⁸This is a simple consequence of linearity and the fact that the $|\mathbf{b}\rangle$ form a basis of the n -qubit state space.

³⁹We assume that the qubits are not destroyed. For instance, if a qubit is identified with an atom in a superposition of its ground state and its first excited state, then exciting a higher level destroys this qubit.

is considered.⁴⁰ Then the error action is of the form

$$\boxed{\Psi \otimes |E\rangle \longmapsto \sum_{\mathbf{r} \in \{0,1,2,3\}^n} (\hat{\sigma}_{\mathbf{r}} \Psi) \otimes |E_{\mathbf{r}}\rangle, \quad \Psi = \sum_{\mathbf{b} \in \{0,1\}^n} \lambda_{\mathbf{b}} |\mathbf{b}\rangle,} \quad (4.32)$$

and error correction for such *quantum noise* should be possible along the lines indicated below.

Remark: Alternatively, (4.32) may be written in the form

$$\Psi \otimes |E\rangle \longmapsto \sum_{\mathbf{a}, \mathbf{b} \in \{0,1\}^n} (\hat{X}_{\mathbf{a}} \hat{Z}_{\mathbf{b}} \Psi) \otimes |E_{\mathbf{a}, \mathbf{b}}\rangle, \quad (4.33)$$

where:

$$\begin{aligned} \hat{X}_{\mathbf{b}} &\stackrel{\text{def}}{=} (\delta_{0b_1} + \delta_{1b_1} \hat{\sigma}_1) \otimes \dots \otimes (\delta_{0b_n} + \delta_{1b_n} \hat{\sigma}_1), \\ \hat{Z}_{\mathbf{b}} &\stackrel{\text{def}}{=} (\delta_{0b_1} + \delta_{1b_1} \hat{\sigma}_3) \otimes \dots \otimes (\delta_{0b_n} + \delta_{1b_n} \hat{\sigma}_3). \end{aligned} \quad (4.34)$$

To explain the essential idea of quantum error correction, let us assume that also for multi-qubits systems only one-qubit errors corresponding to $\hat{\sigma}_3$ (*phase errors*) occur. In order to conserve an unknown one-qubit state (disentangled from the environment) we first of all encode

$$\Psi = \alpha |0\rangle + \beta |1\rangle$$

for arbitrary $\alpha, \beta \in \mathbb{C}$ into the (pure) three-qubit state

$$\hat{\Psi} = \alpha |\hat{w}_0\rangle + \beta |\hat{w}_1\rangle,$$

where

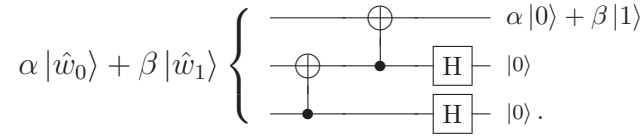
$$\begin{aligned} |\hat{w}_0\rangle &\stackrel{\text{def}}{=} \frac{1}{\sqrt{4}} (|0, 0, 0\rangle + |0, 1, 1\rangle + |1, 0, 1\rangle + |1, 1, 0\rangle) && (\text{even parity}) \\ |\hat{w}_1\rangle &\stackrel{\text{def}}{=} \frac{1}{\sqrt{4}} (|1, 1, 1\rangle + |1, 0, 0\rangle + |0, 1, 0\rangle + |0, 0, 1\rangle) && (\text{odd parity}). \end{aligned} \quad (4.35)$$

This may be done in the following way:

$$\left. \begin{array}{l} \alpha |0\rangle + \beta |1\rangle \text{---} \text{---} \text{---} \oplus \text{---} \text{---} \text{---} \\ |0\rangle \text{---} \text{---} \text{---} \text{H} \text{---} \text{---} \text{---} \bullet \text{---} \text{---} \text{---} \oplus \text{---} \text{---} \text{---} \\ |0\rangle \text{---} \text{---} \text{---} \text{H} \text{---} \text{---} \text{---} \bullet \text{---} \text{---} \text{---} \end{array} \right\} \alpha |\hat{w}_0\rangle + \beta |\hat{w}_1\rangle.$$

⁴⁰ For the general case see (Knill et al., 1999). The \mathbf{b} -independence of the $|E_{\mathbf{r}}(\Psi)\rangle$ is easily derived if every qubit interacts only with its own environment. Note, however, that the $|E_{\mathbf{r}}\rangle$ need neither be orthogonal nor normalized nor unique!

Decoding is not more difficult:



If the state vector of the total system (three-qubit system plus environment) is $\hat{\Psi} \otimes |\hat{E}\rangle$ then, according to our assumption, the interaction between both subsystems can cause only transitions of the form

$$\hat{\Psi} \otimes |\hat{E}\rangle \mapsto \sum_{\nu=0}^3 \left(\hat{\sigma}_3^{(\nu)} \hat{\Psi} \right) \otimes |\hat{E}_3^{(\nu)}\rangle$$

with suitable state vectors $|\hat{E}_3^{(\nu)}\rangle$ of the environment, where

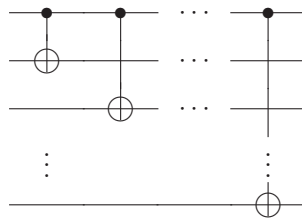
$$\hat{\sigma}_3^{(\nu)} |b_1, b_2, b_3\rangle \stackrel{\text{def}}{=} \begin{cases} |b_1, b_2, b_3\rangle & \text{if } \nu = 0 \\ (-1)^{b_\nu} |b_1, b_2, b_3\rangle & \text{else} \end{cases} \quad \forall \mathbf{b} \in \{0, 1\}^3.$$

The essential point is that the subspaces

$$\mathcal{H}_\nu \stackrel{\text{def}}{=} \hat{\sigma}_3^{(\nu)} \left\{ \hat{\alpha} |\hat{w}_0\rangle + \hat{\beta} |\hat{w}_1\rangle : \hat{\alpha}, \hat{\beta} \in \mathbb{C} \right\}$$

are pairwise orthogonal. Therefore, to restore the original encoded state vector $\alpha |0\rangle + \beta |1\rangle$, it suffices to perform an optimal test (*measurement of first kind*) to which of the four subspaces \mathcal{H}_ν this state vector belongs and apply $\hat{\sigma}_3^{(\nu)}$ according to the outcome.

Exercise 17 Show that the $(n + 1)$ -qubit network



transforms $(\lambda_0 |0\rangle + \lambda_1 |1\rangle) \otimes |0, \dots, 0\rangle$ into $\lambda_0 |0, \dots, 0\rangle + \lambda_1 |1, \dots, 1\rangle$ and discuss its possible use for error correction.

4.3.2 Classical Codes

The general idea of classical error correction (Hamming, 1950; Pless, 1989) is the following:

- Consider a channel transmitting n -bit *words* without changing more than m bits of any word.
- Then the original words can be uniquely reconstructed from the received ones if only special **code words** $\mathbf{w} = (w_1, \dots, w_n) \in \{0, 1\}^n$ are sent which are chosen such that the **HAMMING distance**

$$d(\mathbf{w}, \mathbf{w}') \stackrel{\text{def}}{=} \sum_{\nu=1}^n |w_\nu - w'_\nu| \quad \left(= \|\mathbf{w} - \mathbf{w}'\|^2 \right)$$

between any two code words \mathbf{w}, \mathbf{w}' is $> 2m$.

Obviously, 2^n must be larger than the number of code words (the more the larger m is) for error correction to work this way.⁴¹ Actually:

“Error-correcting coding is the art of adding redundancy efficiently so that most messages, if distorted, can be correctly decoded.”

(Pless, 1989, p. 2)

Especially convenient are the $[n, k]$ **linear** classical codes, for which a set $\mathcal{C} \subset \{0, 1\}^n$ of 2^k code words — the **code** — is selected by means of an $(n - k) \times n$ -matrix \hat{H} as⁴²

$$\mathcal{C} = \ker(\hat{H}) \stackrel{\text{def}}{=} \left\{ \mathbf{b} \in \{0, 1\}^n : \hat{H} \mathbf{b} = 0 \right\}.$$

Of course, the $n - k$ rows of the so-called **parity check**⁴³ **matrix** \hat{H} have to be independent in order to have

$$\dim(\ker(\hat{H})) = k.$$

Warning: The code \mathcal{C} may contain transposed row vectors of the parity check matrix \hat{H} .

Without restriction of generality the parity check matrix can be assumed to be of the form⁴⁴

$$\hat{H} = \left(\hat{A} \mathbb{1}_{n-k} \right),$$

———— DRAFT, June 26, 2009 ————

⁴¹Of course this reduces the capacity of the communication channel.

⁴²Here, we identify matrices with the corresponding linear maps. Note that the components of \hat{H} are in $\{0, 1\}$ and that all arithmetic is to be understood modulo 2. Hence, e.g., $\hat{H} \equiv -\hat{H}$.

⁴³Every row (h_1, \dots, h_n) gives rise to a parity check $\sum_{\nu=1}^n h_\nu b_\nu \stackrel{?}{=} 0$ on the substring of those bits of \mathbf{b} in places where the row has 1's.

⁴⁴This is easily seen using GAUSSIAN elimination. Eventually the bits have to be relabeled.

where \hat{A} is some $(n - k) \times k$ -matrix. In this form we easily see that

$$\hat{H}\hat{G} = 0$$

holds with the $n \times k$ -matrix

$$\hat{G} = \begin{pmatrix} \mathbb{1}_k \\ \hat{A} \end{pmatrix},$$

hence⁴⁵

$$\mathcal{C} = \left\{ \hat{G} \mathbf{a} : \mathbf{a} \in \{0, 1\}^k \right\}.$$

Remark: A possible coding would be

$$\{0, 1\}^k \ni \underbrace{\mathbf{a}}_{\text{word of message}} \longmapsto \underbrace{\hat{G} \mathbf{a}}_{\text{corresp. code word}} \in \{0, 1\}^n.$$

While \hat{G} may directly be used as a *generator* of the code, \hat{H} is more convenient for error detection:

Let $E \subset \{0, 1\}^n$ be the set of possible ‘errors’ and let $\hat{H} \wedge E$ be an injection. Then the distortion

$$\mathbf{w} \mapsto \mathbf{w}' = \mathbf{w} + \mathbf{e}$$

of a code word $\mathbf{w} \in \mathcal{C}$ by an error $\mathbf{e} \in E$ can be identified by checking the *error syndrome*

$$\hat{H} \mathbf{w}' = \hat{H} \mathbf{e}$$

and corrected by adding (=subtracting) \mathbf{e} .

Exercise 18 The rows of the $r \times (2^r - 1)$ parity check matrix characterizing the so-called *binary HAMMING code* $\text{Ham}[r, 2]$ are the nonzero elements of $\{0, 1\}^r$, ordered⁴⁶ according to the value of the corresponding binary numbers.⁴⁷

- Show for every $r \geq 2$ that $\text{Ham}[r, 2]$ is suitable for correcting errors on single bits.
- Discuss $\text{Ham}[2, 2]$ in detail.

Let \mathcal{C} be a $[n, k]$ linear classical code. Then

$$\mathcal{C}^\perp \stackrel{\text{def}}{=} \{\mathbf{b} \in \{0, 1\}^n : \mathbf{b} \cdot \mathbf{b}' = 0 \pmod{2} \forall \mathbf{b}' \in \mathcal{C}\}$$

is called its *dual code*.

⁴⁵Note that, thanks to $\mathbb{1}_k$, the rows of \hat{G} are all independent.

⁴⁶Actually, different orderings give rise to equivalent codes.

⁴⁷See (4.53) for $r = 3$.

Exercise 19 Let \mathcal{C} be a $[n, k]$ linear classical code with parity check matrix \hat{H} and generator \hat{G} . Show the following:⁴⁸

a) \mathcal{C}^\perp is a $[n - k, n]$ linear classical code with parity check matrix $\hat{H}^\perp = \hat{G}^T$ and generator $\hat{G}^\perp = \hat{H}^T$.

b)

$$(\mathcal{C}^\perp)^\perp = \mathcal{C}.$$

c)

$$\sum_{\mathbf{b}' \in \mathcal{C}} (-1)^{\mathbf{b} \cdot \mathbf{b}'} = \begin{cases} |\mathcal{C}| & \text{if } \mathbf{b} \in \mathcal{C}^\perp, \\ 0 & \text{if } \mathbf{b} \in \{0, 1\}^n \setminus \mathcal{C}^\perp. \end{cases}$$

4.3.3 Quantum Codes

In classical communication the received message may be inspected and corrected according to the error syndrome. In quantum communication, however, we should carefully avoid too detailed ‘measurement’ (associated with uncontrollable ‘collapse’) of the state before reconstruction. Therefore, in order to be able to correct all errors corresponding to error operations $\hat{\sigma} \in \mathfrak{E}$ we have to look for quantum codes⁴⁹ of the following form:

- The n -qubit state space \mathcal{H} containing the quantum code words is a direct sum of specified subspaces \mathcal{H}_d .
- Every $\hat{\sigma} \in \mathfrak{E}$ is of a definite *type* d , i.e. $\hat{\sigma} |\hat{w}\rangle \in \mathcal{H}_d$ holds for all quantum code words⁵⁰ $|\hat{w}\rangle$.
- If $\hat{\sigma}, \hat{\sigma}' \in \mathfrak{E}$ are of the same type d then $\hat{\sigma} |w\rangle \sim \hat{\sigma}' |w\rangle$ holds for all quantum code words $|w\rangle$ (but not necessarily for other state vectors).

Under these conditions — if only errors corresponding to operations $\hat{\sigma} \in \mathfrak{E}$ are superimposed⁵¹ — quantum error correction is possible as indicated in 4.3.1:

- The ‘received’ state is forced — via corresponding ‘measurement’ — to ‘collapse’ into a state described by an element of one of the subspaces \mathcal{H}_d .
- Since the ‘collapsed’ state is just the sent code word distorted by an error of type d we only have to apply the inverse of some unitary error operation of type d to reconstruct the correct code word.

DRAFT, June 26, 2009

⁴⁸As usual, we denote the number of elements of a finite set \mathcal{C} by $|\mathcal{C}|$.

⁴⁹By *n -qubit quantum code* we always mean the set of pairwise orthogonal n -qubit state vectors used as *quantum code words*. Note, however, that many authors mean by *quantum code* the complex linear span of quantum code words.

⁵⁰In 4.3.1 we already used linear superpositions $|\hat{w}_0\rangle, |\hat{w}_1\rangle$ of the computational base states as quantum code words, in order to indicate additional possibilities in quantum coding.

⁵¹Of course, \mathfrak{E} should include the trivial ‘error operation’ $\hat{\sigma} = \hat{1}$.

Exercise 20

a) Show that for SHOR's 9-qubit code words

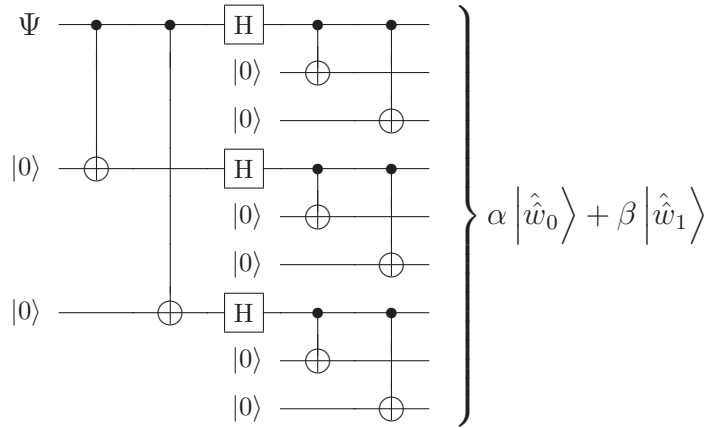
$$\begin{aligned} |\hat{w}_0\rangle &\stackrel{\text{def}}{=} 2^{-3/2} \left(|0, 0, 0\rangle + |1, 1, 1\rangle \right) \otimes \left(|0, 0, 0\rangle + |1, 1, 1\rangle \right) \otimes \left(|0, 0, 0\rangle + |1, 1, 1\rangle \right), \\ |\hat{w}_1\rangle &\stackrel{\text{def}}{=} 2^{-3/2} \left(|0, 0, 0\rangle - |1, 1, 1\rangle \right) \otimes \left(|0, 0, 0\rangle - |1, 1, 1\rangle \right) \otimes \left(|0, 0, 0\rangle - |1, 1, 1\rangle \right) \end{aligned}$$

every superposition of single-qubit errors, i.e. every distortion of the form

$$\begin{aligned} \left(\alpha |\hat{w}_0\rangle + \beta |\hat{w}_1\rangle \right) \otimes |E\rangle &\longmapsto \sum_{\mathbf{r} \in \mathcal{R}_9} \left(\alpha \hat{\sigma}_{\mathbf{r}} |\hat{w}_0\rangle + \beta \hat{\sigma}_{\mathbf{r}} |\hat{w}_1\rangle \right) \otimes |E_{\mathbf{r}}\rangle, \\ \mathcal{R}_9 &\stackrel{\text{def}}{=} \bigcup_{r=0}^3 \left\{ \text{permutations of } (r, 0, 0, 0, 0, 0, 0, 0, 0) \right\}, \end{aligned}$$

may be corrected as described above.

b) Show that encoding $\Psi = \alpha |0\rangle + \beta |1\rangle$ into $\alpha |\hat{w}_0\rangle + \beta |\hat{w}_1\rangle$ may be achieved as follows:



Recall that, according to (4.33), for every $n \in \mathbb{N}$ the possible error n -qubit error operations are elements of the PAULI *group*⁵²

$$\mathfrak{G}_n \stackrel{\text{def}}{=} \left\{ i^\nu \hat{X}_{\mathbf{b}_1} \hat{Z}_{\mathbf{b}_3} : \nu \in \{0, \dots, 3\}, \mathbf{b}_1, \mathbf{b}_3 \in \{0, 1\}^n \right\} \quad (4.36)$$

DRAFT, June 26, 2009

⁵²The $\hat{X}_{\mathbf{b}}$ and $\hat{Z}_{\mathbf{b}}$ were defined by (4.34) and (4.29).

That the latter is a group w.r.t. operator multiplication follows immediately from the algebra of PAULI matrices:

$$\begin{aligned}
\hat{\sigma}_\nu \hat{\sigma}_\nu &= \hat{1} & \forall \nu \in \{0, 1, 2, 3\}, \\
\hat{\sigma}_j \hat{\sigma}_k &= -\hat{\sigma}_k \hat{\sigma}_j & \forall j, k \in \{1, 2, 3\}, j \neq k, \\
\hat{\sigma}_1 \hat{\sigma}_2 &= i \hat{\sigma}_3, \\
\hat{\sigma}_2 \hat{\sigma}_3 &= i \hat{\sigma}_1, \\
\hat{\sigma}_3 \hat{\sigma}_1 &= i \hat{\sigma}_2.
\end{aligned} \tag{4.37}$$

The following statements also follow directly from these relations:

$$\hat{\sigma}_\nu = \hat{\sigma}_\nu^* = \hat{\sigma}_\nu^{-1} \quad \forall \nu \in \{0, 1, 2, 3\}, \tag{4.38}$$

$$\mathfrak{S}_n \supset \mathfrak{S}_n^0 \stackrel{\text{def}}{=} \left\{ \hat{\sigma}_{r_1} \otimes \cdots \otimes \hat{\sigma}_{r_n} : r_1, \dots, r_n \in \{0, \dots, 3\} \right\} \text{ is **not** a group,} \tag{4.39}$$

$$i^\nu \hat{X}_{\mathbf{b}_1} \hat{Z}_{\mathbf{b}_3} \in \mathfrak{S}_n^0 \iff i^\nu = i^{\mathbf{b}_1 \cdot \mathbf{b}_3} \quad \forall \nu \in \{0, 1, 2, 3\}, \mathbf{b}_1, \mathbf{b}_3 \in \{0, 1\}^n, \tag{4.40}$$

$$\hat{\sigma} \hat{\sigma}' \in \{+\hat{\sigma}'\hat{\sigma}, -\hat{\sigma}'\hat{\sigma}\} \quad \forall \hat{\sigma}, \hat{\sigma}' \in \mathfrak{S}_n. \tag{4.41}$$

Theorem 4.3.1 *Let $\mathcal{W} \subset \mathcal{H}$ be an n -qubit quantum code and let $\mathfrak{E} \subset \mathfrak{S}_n$ be a set of error operations including the trivial operation $\hat{1}$. Assume that the linear span $\mathcal{H}_{\mathcal{W}}$ of \mathcal{W} is **stabilized** by the subset $\mathfrak{S}_{\mathcal{W}}$ of \mathfrak{S}_n , i.e. that*

$$\mathcal{H}_{\mathcal{W}} = \left\{ \hat{\Psi} \in \mathcal{H} : \hat{g} \hat{\Psi} = \hat{\Psi} \quad \forall \hat{g} \in \mathfrak{S}_{\mathcal{W}} \right\}. \tag{4.42}$$

Moreover, assume

$$\hat{\sigma}^* \hat{\sigma}' \notin \mathfrak{N}(\mathfrak{S}_{\mathcal{W}}) \setminus \mathfrak{S}_{\mathcal{W}} \quad \forall \hat{\sigma}, \hat{\sigma}' \in \mathfrak{E}, \tag{4.43}$$

where $\mathfrak{N}(\mathfrak{S}_{\mathcal{W}})$ denotes the **normalizer** of $\mathfrak{S}_{\mathcal{W}}$:

$$\mathfrak{N}(\mathfrak{S}_{\mathcal{W}}) = \{ \hat{\sigma} \in \mathfrak{S}_n : \hat{\sigma} \hat{g} \hat{\sigma}^* = \hat{g} \quad \forall \hat{g} \in \mathfrak{S}_{\mathcal{W}} \}.$$

Then there is a unique mapping $d_{\hat{\sigma}}$ from $\mathfrak{S}_{\mathcal{W}}$ into $\{+1, -1\}$ such that:

$$\hat{g} \left(\hat{\sigma} \hat{\Psi} \right) = d_{\hat{\sigma}}(\hat{g}) \left(\hat{\sigma} \hat{\Psi} \right) \quad \forall \hat{g} \in \mathfrak{S}_{\mathcal{W}}, \hat{\sigma} \in \mathfrak{E}, \hat{\Psi} \in \mathcal{H}_{\mathcal{W}}, \tag{4.44}$$

$$\hat{\sigma} \mathcal{H}_{\mathcal{W}} \subset \mathcal{H}_{d_{\hat{\sigma}}} \stackrel{\text{def}}{=} \left\{ \hat{\Phi} \in \mathcal{H} : \hat{g} \hat{\Phi} = d_{\hat{\sigma}}(\hat{g}) \hat{\Phi} \right\} \quad \forall \hat{\sigma} \in \mathfrak{E}, \tag{4.45}$$

$$d_{\hat{\sigma}} \neq d_{\hat{\sigma}'} \implies \mathcal{H}_{d_{\hat{\sigma}}} \perp \mathcal{H}_{d_{\hat{\sigma}'}} \quad \forall \hat{\sigma}, \hat{\sigma}' \in \mathfrak{E}, \tag{4.46}$$

$$d_{\hat{\sigma}} = d_{\hat{\sigma}'} \implies \hat{\sigma} \hat{\Psi} = \hat{\sigma}' \hat{\Psi} \quad \forall \hat{\sigma}, \hat{\sigma}' \in \mathfrak{E}, \hat{\Psi} \in \mathcal{H}_{\mathcal{W}}. \tag{4.47}$$

Outline of proof: (4.44) is a direct consequence of (4.41) and (4.42). (4.44) directly implies (4.45). Since⁵³

$$\hat{g} = \hat{g}^* \quad \forall \hat{g} \in \mathfrak{S}_{\mathcal{W}} \tag{4.48}$$

⁵³This is because for all $\hat{\sigma} \in \mathfrak{S}_n$ we have $\hat{\sigma}^2 = \hat{1} \iff \hat{\sigma} = \hat{\sigma}^*$.

— and since eigenvectors corresponding to different eigenvalues of a self-adjoint operator are always orthogonal — (4.44) also implies (4.46). Finally, (4.44) and (4.41) imply

$$\hat{g} \hat{\sigma}^{(*)} = d_{\hat{\sigma}}(\hat{g}) \hat{\sigma}^{(*)} \hat{g} \quad \forall \hat{g} \in \mathfrak{S}_{\mathcal{W}}, \hat{\sigma} \in \mathfrak{E}$$

and hence

$$\begin{aligned} (\hat{\sigma}^* \hat{\sigma}') \hat{g} (\hat{\sigma}^* \hat{\sigma}')^* &= d_{\hat{\sigma}}(\hat{g}) d_{\hat{\sigma}'}(\hat{g}) \hat{g} (\hat{\sigma}^* \hat{\sigma}') (\hat{\sigma}^* \hat{\sigma}')^* \\ &\stackrel{(4.38)}{=} d_{\hat{\sigma}}(\hat{g}) d_{\hat{\sigma}'}(\hat{g}) \hat{g} \quad \forall \hat{g} \in \mathfrak{S}_{\mathcal{W}}, \hat{\sigma}, \hat{\sigma}' \in \mathfrak{E}. \end{aligned}$$

Therefore (4.47) follows according to

$$\begin{aligned} d_{\hat{\sigma}} = d_{\hat{\sigma}'} &\implies (\hat{\sigma}^* \hat{\sigma}') \hat{g} (\hat{\sigma}^* \hat{\sigma}')^* = \hat{g} \quad \forall \hat{g} \in \mathfrak{S}_{\mathcal{W}} \\ &\implies \hat{\sigma}^* \hat{\sigma}' \in \mathfrak{N}(\mathfrak{S}_{\mathcal{W}}) \\ &\stackrel{(4.43)}{\implies} \hat{\sigma}^* \hat{\sigma}' \in \mathfrak{S}_{\mathcal{W}} \\ &\stackrel{(4.42)}{\implies} \hat{\sigma}^* \hat{\sigma}' \hat{\Psi} = \hat{\Psi} \quad \forall \hat{\Psi} \in \mathcal{H}_{\mathcal{W}} \\ &\stackrel{(4.38)}{\implies} \hat{\sigma}' \hat{\Psi} = \hat{\sigma} \hat{\Psi} \quad \forall \hat{\Psi} \in \mathcal{H}_{\mathcal{W}}. \quad \blacksquare \end{aligned}$$

Remarks:

1. In view of (4.43), $\mathfrak{S}_{\mathcal{W}}$ should be chosen as large as possible.
2. The maximal $\mathfrak{S}_{\mathcal{W}}$ fulfilling the requirements of Theorem 4.3.1 for given $\mathcal{H}_{\mathcal{W}}$ is an abelian group called the *stabilizer* of $\mathcal{H}_{\mathcal{W}}$.
3. Quantum codes \mathcal{W} fulfilling the requirements of Theorem 4.3.1 are called *stabilizer codes*.
4. If there are $\hat{\sigma}, \hat{\sigma}' \in \mathfrak{E}$ and $|\hat{w}\rangle \in \mathcal{W}$ with

$$\hat{\sigma} |\hat{w}\rangle = \hat{\sigma}' |\hat{w}\rangle \quad \text{but} \quad \hat{\sigma} \neq \hat{\sigma}'$$

then the code is called *degenerate* w.r.t. \mathfrak{E} .

5. SHOR's 9-qubit code, described in Exercise 20, is degenerate w.r.t. the set of single qubit error operations. This can be easily seen by considering phase flip errors on different qubits.
6. A stabilizer code is nondegenerate w.r.t \mathfrak{E} iff

$$\hat{\sigma} \neq \hat{\sigma}' \implies \hat{\sigma}^* \hat{\sigma}' \notin \mathfrak{S}_{\mathcal{W}} \quad \forall \hat{\sigma}, \hat{\sigma}' \in \mathfrak{E}.$$

7. In classical coding there is no analog for degeneracy.

Lemma 4.3.2 For $j \in \{1, 2\}$, let the \mathcal{C}_j be a $[n, k_j]$ linear classical codes with $\mathcal{C}_2 \subset \mathcal{C}_1 \neq \mathcal{C}_2$, and define

$$\mathcal{W} = \text{CSS}(\mathcal{C}_1, \mathcal{C}_2) \stackrel{\text{def}}{=} \left\{ |\hat{w}_{\mathbf{b}}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\mathbf{b}' \in \mathcal{C}_2} |\mathbf{b} + \mathbf{b}'\rangle : \mathbf{b} \in \mathcal{C}_1 \right\}. \quad (4.49)$$

where \mathcal{H} denotes the n -qubit state space. Then (4.42) holds for

$$\mathfrak{S}_{\mathcal{W}} = \left\{ \hat{X}_{\mathbf{a}} \hat{Z}_{\mathbf{b}} : \mathbf{a} \in \mathcal{C}_2, \mathbf{b} \in \mathcal{C}_1^{\perp} \right\}. \quad (4.50)$$

Outline of proof: Let

$$\hat{\Psi} = \sum_{\mathbf{b} \in \{0,1\}^n} \lambda_{\mathbf{b}} |\mathbf{b}\rangle \in \left\{ \hat{\Psi} \in \mathcal{H} : \hat{g} \hat{\Psi} = \hat{\Psi} \quad \forall \hat{g} \in \mathfrak{S}_{\mathcal{W}} \right\}.$$

Then

$$\begin{aligned} \hat{\Psi} &\stackrel{(4.50)}{=} \frac{1}{|\mathcal{C}_1^{\perp}|} \sum_{\mathbf{b}' \in \mathcal{C}_1^{\perp}} \hat{Z}_{\mathbf{b}'} \sum_{\mathbf{b} \in \{0,1\}^n} \lambda_{\mathbf{b}} |\mathbf{b}\rangle \\ &= \sum_{\mathbf{b} \in \{0,1\}^n} \lambda_{\mathbf{b}} \frac{1}{|\mathcal{C}_1^{\perp}|} \sum_{\mathbf{b}' \in \mathcal{C}_1^{\perp}} (-1)^{\mathbf{b} \cdot \mathbf{b}'} |\mathbf{b}\rangle \\ &\stackrel{\text{Ex. 19}}{=} \sum_{\mathbf{b} \in \mathcal{C}_1} \lambda_{\mathbf{b}} |\mathbf{b}\rangle \\ &\stackrel{(4.50)}{=} \frac{1}{|\mathcal{C}_2|} \sum_{\mathbf{b}' \in \mathcal{C}_2} \hat{X}_{\mathbf{b}'} \sum_{\mathbf{b} \in \mathcal{C}_1} \lambda_{\mathbf{b}} |\mathbf{b}\rangle \\ &= \sum_{\mathbf{b} \in \mathcal{C}_1} \lambda_{\mathbf{b}} |\hat{w}_{\mathbf{b}}\rangle. \end{aligned}$$

Since, obviously,

$$\hat{X}_{\mathbf{a}} \hat{Z}_{\mathbf{b}'} |\hat{w}_{\mathbf{b}}\rangle = |\hat{w}_{\mathbf{b}}\rangle \quad \forall \mathbf{a} \in \mathcal{C}_2, \mathbf{b}' \in \mathcal{C}_1^{\perp}, \mathbf{b} \in \mathcal{C}_1$$

this proves the lemma. ■

Remarks:

1. The quantum codes $\text{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ described by Lemma 4.3.2 are called CALDERBANK-SHOR-STEANE *codes*.
2. The number of code words for these codes is

$$|\text{CSS}(\mathcal{C}_1, \mathcal{C}_2)| = \frac{|\mathcal{C}_1|}{|\mathcal{C}_2|} = 2^{k_1 - k_2}.$$

Lemma 4.3.3 Let \mathcal{C}_j , \mathcal{W} and $\mathfrak{S}_{\mathcal{W}}$ be given as in Lemma 4.3.2. If \mathcal{C}_1 as well as \mathcal{C}_2^{\perp} is suitable for correcting errors on up to t bits then

$$\hat{\sigma} \neq \hat{\sigma}' \implies \hat{\sigma}^* \hat{\sigma}' \notin \mathfrak{N}(\mathfrak{S}_{\mathcal{W}}) \quad \forall \hat{\sigma}, \hat{\sigma}' \in \mathfrak{E} \quad (4.51)$$

holds for

$$\mathfrak{E} = \left\{ \hat{X}_{\mathbf{e}_1} \hat{Z}_{\mathbf{e}_3} : \mathbf{e}_1, \mathbf{e}_3 \in \left\{ \mathbf{b} \in \{0,1\}^n : \sum_{\nu=1}^n |b^{\nu}| \leq t \right\} \right\}. \quad (4.52)$$

Outline of proof: Consider $\hat{\sigma}, \hat{\sigma}' \in \mathfrak{E}$ with $\hat{\sigma} \neq \hat{\sigma}'$. Then there are

$$\mathbf{e}_j, \mathbf{e}'_j \in \left\{ \mathbf{b} \in \{0, 1\}^n : \sum_{\nu=1}^n |b^\nu| \leq t \right\}$$

with⁵⁴

$$\{\mathbf{e}_1 + \mathbf{e}'_1, \mathbf{e}_3 + \mathbf{e}'_3\} \neq \{0\}$$

and

$$\begin{aligned} \hat{\sigma}^* \hat{\sigma}' &= \left(\hat{X}_{\mathbf{e}_1} \hat{Z}_{\mathbf{e}_3} \right)^* \hat{X}_{\mathbf{e}'_1} \hat{Z}_{\mathbf{e}'_3} \\ &= \hat{Z}_{\mathbf{e}_3} \hat{X}_{\mathbf{e}_1 + \mathbf{e}'_1} \hat{Z}_{\mathbf{e}'_3} \\ &= (-1)^{\mathbf{e}_3 \cdot (\mathbf{e}_1 + \mathbf{e}'_1)} \hat{X}_{\mathbf{e}_1 + \mathbf{e}'_1} \hat{Z}_{\mathbf{e}_3 + \mathbf{e}'_3} \end{aligned}$$

Hence

$$\begin{aligned} (\hat{\sigma}^* \hat{\sigma}') \hat{X}_{\mathbf{a}} \hat{Z}_{\mathbf{b}} (\hat{\sigma}^* \hat{\sigma}')^* &= \hat{X}_{\mathbf{e}_1 + \mathbf{e}'_1} \hat{Z}_{\mathbf{e}_3 + \mathbf{e}'_3} \hat{X}_{\mathbf{a}} \hat{Z}_{\mathbf{b}} \hat{Z}_{\mathbf{e}_3 + \mathbf{e}'_3} \hat{X}_{\mathbf{e}_1 + \mathbf{e}'_1} \\ &= i^{(\mathbf{e}_3 + \mathbf{e}'_3) \cdot \mathbf{a}} i^{\mathbf{b} \cdot (\mathbf{e}_1 + \mathbf{e}'_1)} \hat{X}_{\mathbf{a}} \hat{Z}_{\mathbf{b}} \quad \forall \mathbf{a}, \mathbf{b} \in \{0, 1\}^n. \end{aligned}$$

If $\mathbf{e}_3 + \mathbf{e}'_3 \neq 0$ then $(\mathbf{e}_3 + \mathbf{e}'_3) \cdot \mathbf{a} \neq 0 \pmod 2$ and, consequently,

$$(\hat{\sigma}^* \hat{\sigma}') \hat{X}_{\mathbf{a}} (\hat{\sigma}^* \hat{\sigma}')^* = -\hat{X}_{\mathbf{a}}$$

for some $\mathbf{a} \in \mathcal{C}_2$ since the generator of \mathcal{C}_2 is the parity check matrix of \mathcal{C}_2^\perp . On the other hand, if $\mathbf{e}_1 + \mathbf{e}'_1 \neq 0$ then $\mathbf{b} \cdot (\mathbf{e}_1 + \mathbf{e}'_1) \neq 0 \pmod 2$ and, consequently,

$$(\hat{\sigma}^* \hat{\sigma}') \hat{Z}_{\mathbf{b}} (\hat{\sigma}^* \hat{\sigma}')^* = -\hat{Z}_{\mathbf{b}}$$

for some $\mathbf{b} \in \mathcal{C}_1^\perp$. Thus $\hat{\sigma}^* \hat{\sigma}' \notin \mathfrak{N}(\mathfrak{S}_{\mathcal{W}})$. ■

Remark: Obviously, $\text{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ is nondegenerate w.r.t. \mathfrak{E} specified by Lemma 4.3.3.

In general, the number of operations⁵⁵ $\hat{\sigma}_{\mathbf{r}}$ affecting at most $t \in \{0, \dots, n\}$ qubits of an n -qubit system is⁵⁶ $\sum_{j=0}^t \binom{n}{j} 3^j$. Therefore, in order to correct all corresponding errors for a nondegenerate n -qubit code according to the scheme described above, that many subspaces \mathcal{H}_d are needed. Moreover, the dimension of each of these subspaces must not be smaller than the number of code words. Therefore:

Correction of all errors on at most t qubits of a **nondegenerate** n -qubit code spanned by 2^k orthogonal code words is not possible if the **quantum HAMMING bound**

$$\sum_{j=0}^t \binom{n}{j} 3^j 2^k \leq 2^n$$

is violated.

⁵⁴Recall Footnote 42.

⁵⁵Recall (4.32).

⁵⁶The index $j = 0$ corresponds to the trivial error operation (unit operator).

Note that for $k = t = 1$ the quantum HAMMING bound becomes $2 + 6n \leq 2^n$, hence $n \geq 5$.

For further details on quantum codes see (Preskill, 01, Chapter 7), and (Schlingemann and Werner, 2001; Keyl and Werner, 2002).

4.3.4 Reliable Quantum Computation

Let us discuss the implementation of error correction in more detail. For simplicity, we consider only the quantum code $\text{CSS}(\text{Ham}[3, 2], \text{Ham}[3, 2]^\perp)$, called the STEANE code. According to Exercise 18 a parity check matrix for $\text{Ham}[3, 2]$ is

$$\hat{H}_3 \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}. \quad (4.53)$$

Exercise 21

- a) Show that the code words corresponding to the parity check matrix \hat{H}_3 are the same as those corresponding to the parity check matrix

$$\hat{H}'_3 \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

- b) Show that⁵⁷

$$\hat{H}_4 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

is a parity matrix for $\text{Ham}[3, 2]^\perp$.

- c) Show that

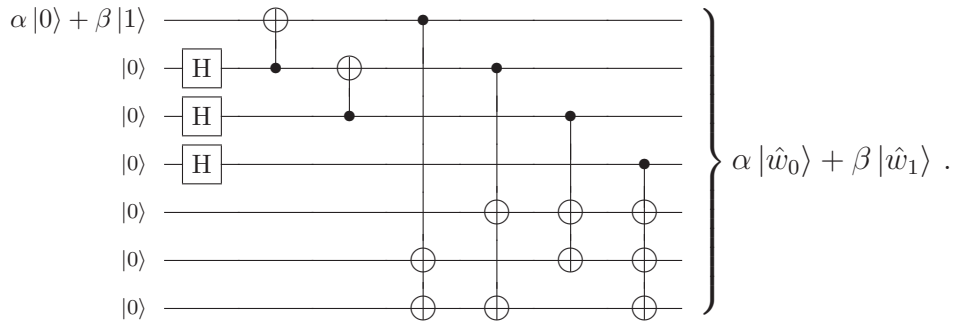
$$\text{Ham}[3, 2]^\perp = \left\{ \mathbf{b} \in \{0, 1\}^7 : \hat{H}_3 \mathbf{b} = 0, (-1)^{b_1 + \dots + b_7} = 1 \right\}.$$

According to Exercise 21, the quantum code words of the STEANE code are

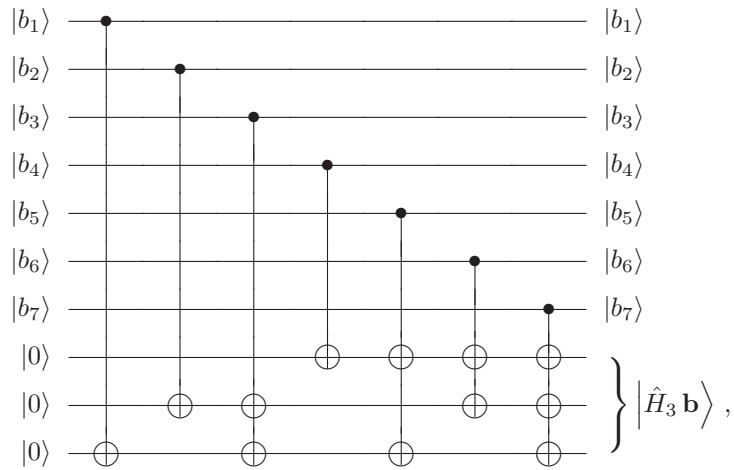
$$\begin{aligned} |\hat{w}_0\rangle &= \frac{1}{\sqrt{8}} \left(|0000000\rangle + |1101001\rangle + |1011010\rangle + |0111100\rangle \right. \\ &\quad \left. + |0110011\rangle + |1100110\rangle + |1010101\rangle + |0001111\rangle \right), \\ |\hat{w}_1\rangle &= \frac{1}{\sqrt{8}} \left(|1111111\rangle + |0010110\rangle + |0100101\rangle + |1000011\rangle \right. \\ &\quad \left. + |1001100\rangle + |0011001\rangle + |0101010\rangle + |1110000\rangle \right), \end{aligned} \quad (4.54)$$

⁵⁷Recall Exercise 19 a).

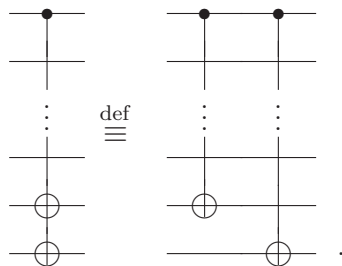
Exercise 22 Show for (4.54) that the following network acts as indicated:



Exercise 23 Show that the following 10-qubit network acts as indicated:



where, e.g.,



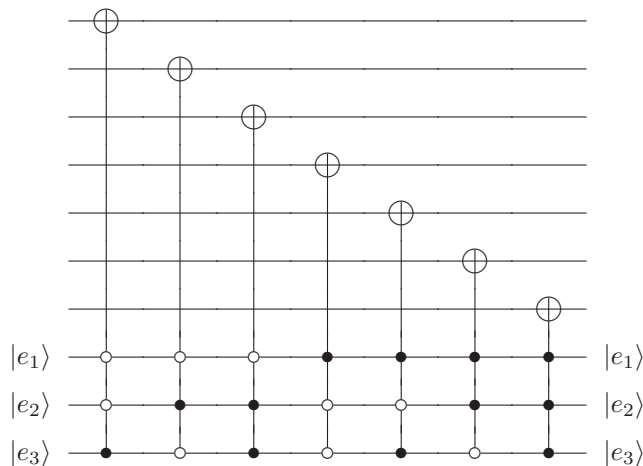
The network of Exercise 23 may be used to reduce single-qubit errors of type $\hat{\sigma}_1$ or/and $\hat{\sigma}_2$ to those of type $\hat{\sigma}_0$ or/and $\hat{\sigma}_3$:

An ideal test for the computational basis of the last 3 (ancillary) qubits causes the 10-qubit state to collapse into some state being the direct product of

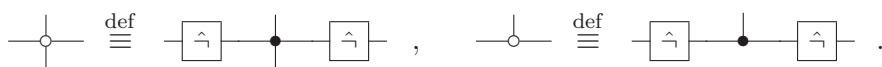
- a (possibly only partially coherent) superposition of distortions of the original code word by single-qubit errors, appearing in one and the same position if of type $\hat{\sigma}_1$ or $\hat{\sigma}_2$, and
- a base state of the ancillary 3-qubit system which corresponds either to $(0, 0, 0)$, if the collapsed 7-qubit state is a distortion of the original code word by single-qubit errors of only type $\hat{\sigma}_0$ or/and $\hat{\sigma}_3$, or else corresponds to the classical error syndrome of a bit-flip in the position, where the code word is distorted by an error of type $\hat{\sigma}_1$ or/and $\hat{\sigma}_2$.

If the collapsed state of the ancillary system does not correspond to $(0, 0, 0)$ then $\hat{\sigma}_1$ should be applied to the qubit in the position where the code word is distorted. In any case, then, the resulting 7-qubit state will be a (possibly only partially coherent) superposition of distortions of the original code word by single-qubit errors of type $\hat{\sigma}_0$ or/and $\hat{\sigma}_3$.

Exercise 24 Show that the following 10-qubit network flips the $\left(\sum_{j=1}^3 e_j 2^{3-j}\right)$ -th qubit for input of the specified type with $|e_1, e_2, e_3\rangle \neq |0, 0, 0\rangle$ and, therefore, may be used to avoid testing the error syndrome for single-qubit errors of type $\hat{\sigma}_1$ or/and $\hat{\sigma}_2$:



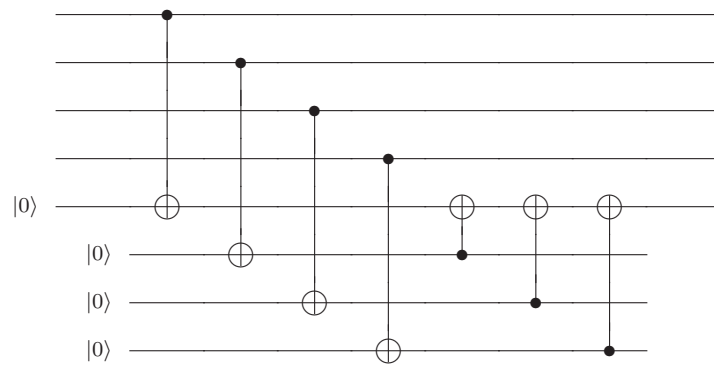
where



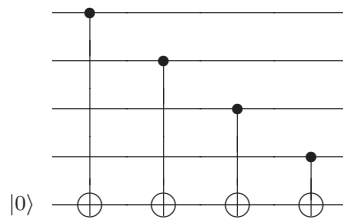
The eventually remaining single-qubit errors of only type $\hat{\sigma}_0$ or/and $\hat{\sigma}_3$. may be converted into errors of type $\hat{\sigma}_0$ or/and $\hat{\sigma}_1$ by applying $\hat{U}_H^{\otimes n}$. Correction these errors as just described and applying $\hat{U}_H^{\otimes n}$ once more restores the original message.

Up to now we tacitly assumed that all devices used for error correction work perfectly error free. Of course this is unrealistic and, actually, special care has to be taken to prevent these devices from making things worse.

For instance, if a phase error appears for the first ancillary qubit of the error syndrome network presented in Exercise 23 then according to Exercise this error may propagate into all of the last four data qubits. To prevent this one could use



instead of



and implement $\text{---} \text{---}$ in a suitable way.⁵⁸

While such precautions prohibit propagation of errors of the ancillary part of the network into the data part they do not guarantee a correct error syndrome. Therefore the ‘measurement’ of the error syndrome should be repeated and only used for error correction if confirmed.

In order to protect calculations against quantum noise they should be performed directly on the encoded data.

Of course, the encoded data should be error checked sufficiently often. Especially, the actual computation should not be started before the initial encoded state has been checked to be free of errors.

_____ DRAFT, June 26, 2009 _____

⁵⁸See (Möttönen and Vartiainen, 2005, Fig. 8), in this connection.

Altogether it seems possible to implement reliable quantum computation, if sufficient care is taken. For further details see (Preskill, 1998b; Preskill, 1998a; Leung, 2000).

4.4 Entanglement Assisted Channels⁵⁹

“Entanglement is monogamous — the more entangled Bob is with Alice, the less entangled he can be with anyone else.”

Charles Bennett⁶⁰

4.4.1 Quantum Dense Coding⁶¹

Let $\mathcal{S} = \mathcal{S}_1 \oplus \mathcal{S}_2$ be a bipartite⁶² 2-qubit system with state space $\mathcal{H} \otimes \mathcal{H}$ and computational basis $\left\{ |\nu, \mu\rangle \stackrel{\text{def}}{=} \phi_\nu \otimes \phi_\mu \right\}_{\nu, \mu \in \{0,1\}}$. Then the so-called BELL *states*

$$\begin{aligned}\Phi^+ &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|0,0\rangle + |1,1\rangle), \\ \Phi^- &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|0,0\rangle - |1,1\rangle), \\ \Psi^+ &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|0,1\rangle + |1,0\rangle), \\ \Psi^- &\stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|0,1\rangle - |1,0\rangle)\end{aligned}\tag{4.55}$$

form an orthonormal basis of $\mathcal{H} \otimes \mathcal{H}$ and may be **locally** transformed into each other.⁶³

$$\begin{aligned}\Phi^\mp &= (\hat{\sigma}_3 \otimes \hat{1}) \Phi^\pm, \\ \Psi^\mp &= (\hat{\sigma}_3 \otimes \hat{1}) \Psi^\pm, \\ \Psi^+ &= (\hat{\sigma}_1 \otimes \hat{1}) \Phi^+.\end{aligned}\tag{4.56}$$

Obviously, 2 classical bits of information may be encoded via the BELL states, e.g.:

$$(0,0) \hat{=} \Phi^+, \quad (0,1) \hat{=} \Phi^-, \quad (1,0) \hat{=} \Psi^+, \quad (1,1) \hat{=} \Psi^-.$$

———— DRAFT, June 26, 2009 ————

⁵⁹See Section 1.2.2 for the network models of dense coding, teleportation, and entanglement swapping. See also (Devetak and Winter, 2003; Devetak et al., 2004) for related protocols.

⁶⁰<http://qip-server.tcs.tifr.res.in/qpip/HTML/Courses/Bennett/TIFR2.pdf>

⁶¹See also (Mermin, 2002).

⁶²See Appendix A.4.3.

⁶³As usual, we denote by $\hat{\sigma}_1, \dots, \hat{\sigma}_3$ the PAULI operators, i.e. w.r.t. $(|0\rangle, |1\rangle)$:

$$\hat{\sigma}_1 \hat{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma}_2 \hat{=} \begin{pmatrix} 0 & -i \\ +i & 0 \end{pmatrix}, \quad \hat{\sigma}_3 \hat{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Thus, if Alice and Bob (situated arbitrarily far apart) initially share a pair of qubits forming $\mathcal{S}_1 \oplus \mathcal{S}_2$ in a BELL state,⁶⁴ say Ψ_- , then Alice may communicate 2 bits of information by sending Bob her single qubit (system \mathcal{S}_1) after acting on it in an appropriate way:

2-bit information	operation by Alice	new BELL state
(0,0)	$\hat{\sigma}_1 \hat{\sigma}_3$	Φ^+
(0,1)	$\hat{\sigma}_3 \hat{\sigma}_1 \hat{\sigma}_3$	Φ^-
(1,0)	$\hat{\sigma}_3$	Ψ^+
(1,1)	none	Ψ^-

After receiving Alice's qubit Bob just has to perform a projective measurement w.r.t. the BELL basis⁶⁵ $\{\Phi^+, \Phi^-, \Psi^+, \Psi^-\}$ in order to decode the 2-bit information.

Needless to say, without entanglement Alice would not have any chance to transmit more than a single bit by sending just a single qubit. Therefore, the described procedure to communicate 2 bits by sending just 1 qubit is called **quantum dense coding** (of classical information). Of course, the crucial point is that Alice has to be given one partner of an entangled pair of qubits first. Note, however, that Alice and Bob may store their qubits for some time in suitable quantum memory⁶⁶ before starting to communicate. Then the information carried by the sent qubit is of no use for any potential eavesdropper.

4.4.2 Quantum Teleportation

Consider, e.g., a 3-qubit system $\mathcal{S} = \mathcal{S}_1 \oplus \mathcal{S}_2 \oplus \mathcal{S}_3$ with state space $\mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}$ and computational basis $\left\{ |\alpha, \beta, \gamma\rangle \stackrel{\text{def}}{=} \phi_\alpha \otimes \phi_\beta \otimes \phi_\gamma \right\}_{\alpha, \beta, \gamma \in \{0,1\}}$ in the initial state⁶⁷

$$\Psi_0 = \psi \otimes \frac{1}{\sqrt{2}} (\phi_0 \otimes \phi_1 - \phi_1 \otimes \phi_0). \quad (4.57)$$

In order to determine the effect of a projective measurement on the subsystem $\mathcal{S}_1 \oplus \mathcal{S}_2$ w.r.t. its BELL basis we rewrite this state in the form

$$\Psi_0 = \Phi^+ \otimes \chi_0 + \Phi^- \otimes \chi_1 + \Psi^+ \otimes \chi_2 + \Psi^- \otimes \chi_3. \quad (4.58)$$

Writing

$$\psi = \alpha |0\rangle + \beta |1\rangle$$

———— DRAFT, June 26, 2009 ————

⁶⁴For the creation of photon pairs in BELL states via parametric down conversion see, e.g., (Gatti et al., 2003) and references given there.

⁶⁵For the implementation of such measurements see, e.g., (Paris et al., 2000; Tomita, 2000; Kim et al., 2001).

⁶⁶For the possibility of storing optical qubits see (Gingrich et al., 2003).

⁶⁷Obviously, then, the subsystem $\mathcal{S}_2 \oplus \mathcal{S}_3$ is in the BELL state corresponding to Ψ^- .

and comparing

$$\begin{aligned} & \sqrt{2} \psi \otimes \frac{1}{\sqrt{2}} (\phi_0 \otimes \phi_1 - \phi_1 \otimes \phi_0) \\ &= \alpha |0, 0, 1\rangle - \alpha |0, 1, 0\rangle - \beta |1, 1, 0\rangle + \beta |1, 0, 1\rangle \end{aligned}$$

with

$$\begin{aligned} & \sqrt{2} \Phi^+ \otimes \chi_0 + \Phi^- \otimes \chi_1 + \Psi^+ \otimes \chi_2 + \Psi^- \otimes \chi_3 \\ &= \frac{1}{2} \left(|0, 0\rangle \otimes \chi_0 + |1, 1\rangle \otimes \chi_0 + |0, 0\rangle \otimes \chi_1 - |1, 1\rangle \otimes \chi_1 \right. \\ & \quad \left. + |0, 1\rangle \otimes \chi_2 + |1, 0\rangle \otimes \chi_2 + |0, 1\rangle \otimes \chi_3 - |1, 0\rangle \otimes \chi_3 \right) \\ &= |0, 0\rangle \otimes \frac{\chi_0 + \chi_1}{2} + |0, 1\rangle \otimes \frac{\chi_2 + \chi_3}{2} + |1, 0\rangle \otimes \frac{\chi_2 - \chi_3}{2} + |1, 1\rangle \otimes \frac{\chi_0 - \chi_1}{2} \end{aligned}$$

we get

$$\begin{aligned} \chi_0 + \chi_1 &= +\alpha |1\rangle, \\ \chi_2 + \chi_3 &= -\alpha |0\rangle, \\ \chi_2 - \chi_3 &= +\beta |1\rangle, \\ \chi_0 - \chi_1 &= -\beta |0\rangle \end{aligned}$$

and hence

$$\begin{aligned} \chi_0 &= \alpha |1\rangle - \beta |0\rangle, \\ &= \hat{\sigma}_1 \hat{\sigma}_3 \psi \\ \chi_1 &= \alpha |1\rangle + \beta |0\rangle, \\ &= \hat{\sigma}_1 \psi \\ \chi_2 &= \beta |1\rangle - \alpha |0\rangle, \\ &= -\hat{\sigma}_3 \psi \\ \chi_3 &= -\alpha |0\rangle - \beta |1\rangle, \\ &= -\psi. \end{aligned} \tag{4.59}$$

(4.57)–(4.59) show the possibility of *quantum teleportation* (of quantum information).⁶⁸

If Alice and Bob (situated arbitrarily far apart) initially share a pair of qubits forming $\mathcal{S}_2 \oplus \mathcal{S}_3$ in the BELL state $\frac{1}{\sqrt{2}} (\phi_0 \otimes \phi_1 - \phi_1 \otimes \phi_0)$ then Alice may communicate to Bob the quantum information contained in the **unknown** state ψ in the following way:

Alice performs a projective measurement on $\mathcal{S}_1 \oplus \mathcal{S}_2$ w.r.t. the BELL basis $\{\Phi^+, \Phi^-, \Psi^+, \Psi^-\}$ and tells Bob her result via **classical** communication. Bob just has to perform one of the operations $\hat{\sigma}_1 \hat{\sigma}_3$, $\hat{\sigma}_1$, $\hat{\sigma}_3$ or none — according to the outcome of Alice’s measurement — on his

⁶⁸See (Sanctuary et al., 2003) for critical remarks on corresponding experiments.

qubit (system \mathcal{S}_3) in order to have the latter in the state $\pm\psi$:

result of Alice's measurement	Bob's operation
Φ^+	$\hat{\sigma}_3\hat{\sigma}_1 = (\hat{\sigma}_1\hat{\sigma}_3)^{-1}$
Φ^-	$\hat{\sigma}_1 = (\hat{\sigma}_1)^{-1}$
Ψ^+	$\hat{\sigma}_3 = (\hat{\sigma}_3)^{-1}$
Ψ^-	none

Note that the classical information sent by Alice would be of no use to an eavesdropper and that sending classical information avoids the decoherence problems connected with sending qubits.

4.4.3 Entanglement Swapping

Consider a 4-qubit system $\mathcal{S} = \mathcal{S}_0 \oplus \mathcal{S}_1 \oplus \mathcal{S}_2 \oplus \mathcal{S}_3$ in the initial state

$$\hat{\Psi}_0 = \Psi^- \otimes \Psi^-. \quad (4.60)$$

Then the calculations of Section 4.4.2 show that

$$\begin{aligned} \hat{\Psi}_0 = & (\hat{1} \otimes \hat{1} \otimes \hat{1} \otimes \hat{\sigma}_1\hat{\sigma}_3) \frac{1}{2} \left(|0\rangle \otimes \Phi^+ \otimes |1\rangle - |1\rangle \otimes \Phi^+ \otimes |0\rangle \right) \\ & (\hat{1} \otimes \hat{1} \otimes \hat{1} \otimes \hat{\sigma}_1) \frac{1}{2} \left(|0\rangle \otimes \Phi^- \otimes |1\rangle - |1\rangle \otimes \Phi^- \otimes |0\rangle \right) \\ & - (\hat{1} \otimes \hat{1} \otimes \hat{1} \otimes \hat{\sigma}_3) \frac{1}{2} \left(|0\rangle \otimes \Psi^+ \otimes |1\rangle - |1\rangle \otimes \Psi^+ \otimes |0\rangle \right) \\ & - \frac{1}{2} \left(|0\rangle \otimes \Psi^- \otimes |1\rangle - |1\rangle \otimes \Psi^- \otimes |0\rangle \right). \end{aligned} \quad (4.61)$$

Now assume that

- Victor has access to \mathcal{S}_0 ,
- Alice has access to $\mathcal{S}_1 \oplus \mathcal{S}_2$,
- Bob has access to \mathcal{S}_3 .

Then — even though Victor, Alice, and Bob may be arbitrarily far apart, the entanglement of the subsystem $\mathcal{S}_0 \oplus \mathcal{S}_1$ may be swapped to the subsystem $\mathcal{S}_0 \oplus \mathcal{S}_3$ in the following way:

Alice performs a projective measurement on $\mathcal{S}_1 \oplus \mathcal{S}_2$ w.r.t. the BELL basis $\{\Phi^+, \Phi^-, \Psi^+, \Psi^-\}$ and tells Bob her result via **classical** communication. Bob just has to perform one of the operations $\hat{\sigma}_1\hat{\sigma}_3$, $\hat{\sigma}_1$, $\hat{\sigma}_3$ or none — according to the outcome of Alice's measurement — on his qubit (system \mathcal{S}_3) in order to have the partial state of the subsystem $\mathcal{S}_0 \oplus \mathcal{S}_3$ in the state Ψ^- .

Thus Alice may act as an entanglement provider:

Alice prepares pairs of entangled qubits and distributes one partner of each pair to various customers including Victor and Bob. If Victor and Bob need to share an entangled pair they instruct Alice to perform a projective measurement on $\mathcal{S}_1 \oplus \mathcal{S}_2$ w.r.t. the BELL basis $\{\Phi^+, \Phi^-, \Psi^+, \Psi^-\}$ and communicate the result to either Victor and Bob who then knows the type of entanglement of the pair shared with Bob.

4.4.4 Quantum Cryptography⁶⁹

As explained in 2.2.1 the security of the RSA encryption scheme relies on the extreme difficulty to factorize large numbers n by classical means (and the possibility of authentication of submitted messages). Otherwise d could be determined from n and e . However, in view of SHOR's quantum factoring algorithm (Shor, 1994) and the possible implementation of quantum computers such classical cryptosystems as RSA may become insecure. Fortunately, quantum mechanics itself offers means for secure communication exploiting the VERNAM *cipher*⁷⁰ (also called *one time pad*):

Exploiting quantum mechanisms, Victor and Bob agree on a purely random secret key $\mathbf{c} = (c_1, \dots, c_n) \in \{0, 1\}^n$. Then, instead of sending Bob the pure the plaintext message $\mathbf{c} = (c_1, \dots, c_n) \in \{0, 1\}^n$ Victor sends him the encoded message⁷¹

$$\mathbf{e} = (b_1 \oplus c_1, \dots, b_n \oplus c_n)$$

(through some public channel) which Bob may decrypt as

$$\mathbf{b} = (e_1 \oplus c_1, \dots, e_n \oplus c_n)$$

but appears purely random to all eventual eavesdroppers.

As shown by Claude Shannon (Shannon, 1949a), this cryptosystem is absolutely secure if \mathbf{e} is kept secret and used only once.

If Victor and Bob share enough (nearly) maximally entangled pairs of qubits⁷² they may establish a secret key in the following way:

DRAFT, June 26, 2009

⁶⁹See (Bowmeester et al., 2000, Chapter 2) for a nice introduction and (Elliott et al., 2005) for actual implementation. A commercial quantum cryptosystem is offered at: www.idquantique.com

⁷⁰Developed by Gilbert Vernam at AT&T in 1917 (first published in 1926).

⁷¹Note that

$$b \oplus b' \stackrel{\text{def}}{=} b + b' \bmod 2 \quad \forall b, b' \in \{0, 1\} .$$

⁷²If the entanglement is not good enough even if it is fairly bad they may perform *entanglement distillation* resulting in a smaller number of nearly perfectly entangled pairs; see Section 6.2.3.

Via public communication they agree on an orthonormal basis $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ of \mathbb{R}^3 and on a series of joint measurements of the following type on definite pairs:

For every tested pair the momenta of the partners are directed parallel or antiparallel \mathbf{e}_2 and a check for linear polarization is performed, but Victor and Bob independently and randomly between two possibilities: Either they test whether the linear polarization of their photon is parallel or orthogonal to \mathbf{e}_1 or check whether the linear polarization is parallel or orthogonal to $\mathbf{e}'_1 = \frac{1}{\sqrt{2}}(\mathbf{e}_1 + \mathbf{e}_3)$.

As long as their choices are different their results for the corresponding pairs are completely uncorrelated. Whenever they choose the same type of measurement their results are (nearly) perfectly correlated. Thus they may agree via public communication on a random secret key in the following way:

- Alice and Bob identify those pairs for which, by chance, they had chosen the same type of measurement and discard those pairs of which at least one partner got lost and thus did not provide a definite result.
- The remaining pairs are split into two groups.
- Bob and Alice (publicly) compare their results for the first group in order to check perfect correlation.
- If the correlations turn out to be (nearly) perfect for the first group then Alice and Bob agree to use their results on the second group for a common key. Thank to the correlations they need not communicate the results concerning the second group. Therefore a possible eavesdropper has no access to the chosen key.
- Weak deviations from perfect correlation may be error corrected after communicating results of various parity checks⁷³ — of almost no use for any eavesdropper.

This cryptosystem can only be attacked by manipulating the entangled pairs before Victor's and Bob's measurements. But such attack will be detected by Victor and Bob, who can eventually discard the current key and create another one.

DRAFT, June 26, 2009

⁷³Alternatively, if the correlations are only marginally spoiled, one could apply standard classical error correction. to the appropriately encoded (and slightly disturbed) plaintext after use of the one time pad.

Chapter 5

Quantifying Quantum Information

In fact, the mathematical machinery we need to develop quantum information theory is very similar to SHANNON's mathematics (typical sequences, random coding, ...); so similar as to sometimes obscure that the conceptual context is really quite different.

(Preskill, 01, Section 5.2)

5.1 SHANNON Theory for Pedestrians

For simplicity, let us consider an information source (Z, p) of the following type:

1. **Letters** x are randomly drawn from a finite **alphabet** $Z = \{z_1, \dots, z_N\}$.
2. The probability for drawing the n -**letter word** $w = (z_{j_1}, \dots, z_{j_n})$ is¹

$$p(z_{j_1}, \dots, z_{j_n}) = \prod_{\nu=1}^n p(z_{j_\nu}) \quad \forall z_{j_1}, \dots, z_{j_n} \in Z,$$

where

$$p(z) = \text{probability for drawing } z \quad \forall z \in Z.$$

Consistency, of course requires

$$p(z_1) + \dots + p(z_N) = 1. \tag{5.1}$$

Then, for the corresponding SHANNON **entropy**

$$H(Z, p) \stackrel{\text{def}}{=} - \sum_{j=1}^N p(z_j) \log_2(p(z_j)) \tag{5.2}$$

one may prove²

DRAFT, June 26, 2009

¹Thus we assume that the probabilities for the successively drawn letters are independent.

²See (Shannon, 1949, Appendix 3).

SHANNON'S noiseless coding theorem:

For arbitrarily given $\delta > 0$, we may associate with every $n \in \mathbb{N}$ a set $W_{\delta,n}$ of *typical* n -letter words³ such that:

1.

$$|W_{\delta,n}| \leq 2^{n(H(Z,p)+\delta)} \quad \forall n \in \mathbb{N}.$$
2. The probability for a drawing a n -letter word $w \notin W_{\delta,n}$ tends to 0 for $n \rightarrow \infty$.

In other words:

Asymptotically, the relevant words can be indexed by $\lceil n(H(Z,p) + \delta) \rceil$ bits,⁴ for every fixed $\delta > 0$.

In this sense, the information gained by drawing the letter z is $-\log_2(p(z))$ bits. The average information gained by drawing a letter, correspondingly, is $H(Z,p)$ bits.

Remarks:

1. As to be expected, we have:

$$H(Z,p) = 0 \iff \exists z_0 \in Z : p(z_0) = 1. \quad (5.3)$$

2. Straightforward calculation shows that⁵

$$\begin{aligned} Z &= Z_1 \cup Z_2, \quad Z_1 \neq \emptyset = Z_1 \cap Z_2 \neq Z_2 \\ \implies H(Z,p) &= H(\{Z_1, Z_2\}, \bar{p}) + \bar{p}(Z_1) H(Z_1, p_1) + \bar{p}(Z_2) H(Z_2, p_2), \end{aligned} \quad (5.4)$$

where

$$\left. \begin{aligned} \bar{p}(Z_j) &\stackrel{\text{def}}{=} \sum_{z \in Z_j} p(z) \\ p_j(z) &\stackrel{\text{def}}{=} p(z)/\bar{p}(Z_j) \quad \forall z \in Z_j \end{aligned} \right\} \quad \forall j \in \{1, 2\}.$$

———— DRAFT, June 26, 2009 ————

³The *typical* words have to include essentially all those containing the letter x approximately $\lceil np(z) \rceil$ -times for every $z \in Z$. For large n the number of such words is of the order

$$\frac{n!}{\prod_z (np(z))!} \approx 2^{nH(Z,p)} \quad \left(\text{since } N! \underset{\text{STIRLING}}{\approx} e^{-N} N^N \text{ for large } N \right).$$

⁴Obviously, such coding can be used for data compression, if $H(Z,p) < \log_2(|Z|)$.

⁵(5.4) together with (5.5) and continuity in the $p(z)$ fixes H uniquely (Shannon, 1949, Theorem 2).

3. $H(Z, p)$ as a functional of p is maximal⁶ for constant p , i.e. for $p(z_1) = \dots = p(z_N) = 1/N$.

4.

$$p(z) = \frac{1}{|Z|} \quad \forall z \in Z \quad \implies \quad H(Z, p) = \log_2(|Z|). \quad (5.5)$$

5. Since

$$\log_2(|Z|) = N \quad \text{if } |Z| = 2^N,$$

compression is not possible for constant $p(z)$ (essentially all words are *typical*).

Now assume

$$Z = X \times Y$$

and define

$$p_1(x) \stackrel{\text{def}}{=} \sum_{y \in Y} p(x, y) \quad \forall x \in X, \quad (5.6)$$

$$p_2(y) \stackrel{\text{def}}{=} \sum_{x \in X} p(x, y) \quad \forall y \in Y, \quad (5.7)$$

$$p_1(x|y) \stackrel{\text{def}}{=} \begin{cases} p(x, y)/p_2(y) & \text{if } p_2(y) > 0 \\ 1/|X| & \text{else} \end{cases} \quad \forall (x, y) \in Z, \quad (5.8)$$

$$p_2(y|x) \stackrel{\text{def}}{=} \begin{cases} p(x, y)/p_1(x) & \text{if } p_1(x) > 0 \\ 1/|Y| & \text{else} \end{cases} \quad \forall (x, y) \in Z. \quad (5.9)$$

Remark: A possible application is the following:

- X = {elements drawn and sent via some *channel*} ,
- Y = {elements received through that channel} ,
- $p(x, y)$ = joint probability for sending x and receiving y ,
- $p_1(x)$ = probability for sending x ,
- $p_2(y)$ = probability for receiving y ,
- $p_2(y|x)$ = probability for receiving y when x is sent ,
- $p_1(x|y)$ = probability for x having been sent when y is received .

Then, thanks to⁷

$$\boxed{a \neq b \implies a(\ln a - \ln b) > a - b \quad \forall a, b > 0} \quad (5.10)$$

———— DRAFT, June 26, 2009 ————

⁶The simplest way to check this is by means of a LAGRANGE multiplier λ : Determine $\lambda \in \mathbb{R}$ and $p(z_1), \dots, p(z_N) \geq 0$ (not a priori postulating (5.1)) for which $H(Z, p) + \lambda(1 - \sum_{z \in Z} p(z))$ is maximal.

⁷Setting $x = b/a$, (5.10) follows from: $0 < x \neq 1 \implies \ln x < x - 1$.

we have⁸

$$H(X \times Y, p) \leq H(X, p_1) + H(Y, p_2) \quad (\text{subadditivity}) \quad (5.11)$$

and

$$\begin{aligned} H(X \times Y, p) &= H(X, p_1) + H(Y, p_2) \\ \implies p(x, y) &= p_1(x) p_2(y) \quad \forall (x, y) \in X \times Y. \end{aligned} \quad (5.12)$$

Outline of proof: Replacing b by bc in (5.10) and using

$$\log_2(x) = \frac{\ln(x)}{\ln(2)} \quad \forall x > 0,$$

we get

$$a \neq bc \implies a \left(\log_2(a) - \log_2(b) - \log_2(c) \right) > \frac{a - bc}{\ln(2)} \quad \forall a, b, c > 0$$

and hence

$$\begin{aligned} &H(X, p_1) + H(Y, p_2) - H(X \times Y, p) \\ &= - \sum_{x \in X} \left(\sum_{y \in Y} p(x, y) \right) \log_2(p_1(x)) - \sum_{y \in Y} \left(\sum_{x \in X} p(x, y) \right) \log_2(p_2(y)) \\ &\quad + \sum_{(x, y) \in X \times Y} p(x, y) \log_2(p(x, y)) \\ &= \sum_{(x, y) \in X \times Y} p(x, y) \left(\log_2(p(x, y)) - \log_2(p_1(x)) - \log_2(p_2(y)) \right) \\ &\geq \sum_{(x, y) \in X \times Y} \left(p(x, y) - p_1(x) p_2(y) \right) / \ln(2) \\ &\geq 0 \end{aligned}$$

with equality iff

$$p(x, y) = p_1(x) p_2(y) \quad \forall (x, y) \in X \times Y. \quad \blacksquare$$

Moreover, according to SHANNON's noiseless coding theorem, the **conditional entropy**⁹

$$H_1(X|Y) \stackrel{\text{def}}{=} \sum_{y \in Y} p_2(y) H(X, p_1(\cdot|y)) \quad (5.13)$$

is the average asymptotic amount of bits of information needed in addition per Y -part of the drawn $z \in Z$, if only these parts are known, in order to determine also the X -parts. Accordingly, we have

$$H(X \times Y, p) = H(Y, p_2) + H(X|Y). \quad (5.14)$$

⁸This corresponds to the fact that correlations between X and Y contain additional information.

⁹Its quantum analogue can be negative (Horodecki et al., 2005).

Outline of proof:

$$\begin{aligned}
 & H(X|Y) \\
 \stackrel{(5.13)}{=} & - \sum_{y \in Y} p_2(y) \sum_{x \in X} p_1(x|y) \log_2 \left(\underbrace{p_1(x|y)}_{=p(x,y)/p_2(y)} \right) \\
 = & - \sum_{(x,y) \in Z} \underbrace{p_2(y) p_1(x|y)}_{=p(x,y)} \log_2(p(x,y)) + \sum_{y \in Y} p_2(y) \underbrace{\sum_{x \in X} p_1(x|y)}_{=1} \log_2(p_2(y)). \quad \blacksquare
 \end{aligned}$$

Similarly we have

$$H(X \times Y, p) = H(X, p_1) + H(Y|X)$$

for

$$H_2(Y|X) \stackrel{\text{def}}{=} \sum_{x \in X} p_1(x) H(Y, p_2(\cdot|x)).$$

Thanks to subadditivity (5.11), the *mutual information*

$$I(X : Y) \stackrel{\text{def}}{=} H(X, p_1) + H(Y, p_2) - H(X \times Y, p) \quad (5.15)$$

is non-negative, as required by its interpretation as amount of information contained in the correlations between X and Y . Its relation to the conditional entropy is given by

$$\begin{aligned}
 I(X : Y) &= H(X, p_1) - H_1(X|Y) \\
 &= H(Y, p_2) - H_2(Y|X) \\
 &\geq 0.
 \end{aligned} \quad (5.16)$$

5.2 Adaption to Quantum Communication

5.2.1 VON NEUMANN Entropy¹⁰

The VON NEUMANN *entropy*¹¹

$$S_1(\hat{\rho}) \stackrel{\text{def}}{=} -\text{trace}(\hat{\rho} \log_2 \hat{\rho}) \quad \forall \hat{\rho} \in S(\mathcal{H}) \quad (5.17)$$

(von Neumann, 1927) can be considered as a generalization of the SHANNON entropy in the following sense:

———— DRAFT, June 26, 2009 ————

¹⁰See also (Wehrl, 1978; Ohya and Petz, 1993; Petz, 2001; Ruskai, 2002).

¹¹One can easily prove that, at least for the (normalized) statistical operator $\hat{\rho}$ of the micro-canonical or canonical ensemble, $k \ln(2) S_1(\hat{\rho})$ is the usual thermodynamic entropy; see, e.g., (Gardiner and Zoller, 2000, Section 2.4.1). Note, however, that the VON NEUMANN entropy — contrary to the thermodynamic entropy — is non-extensive (not additive) for homogeneous non-equilibrium systems. For generalizations of the VON NEUMANN entropy as a measure of ‘mixedness’ see (Berry and Sanders, 2003) and references given there.

If

$$\hat{\rho} = \sum_{\nu=1}^n \underbrace{\lambda_{\nu}}_{\geq 0} |\phi_{\nu}\rangle\langle\phi_{\nu}|, \quad \langle\phi_{\alpha} | \phi_{\beta}\rangle = \begin{cases} 1 & \text{for } \alpha = \beta, \\ 0 & \text{else,} \end{cases}$$

then

$$S_1(\hat{\rho}) = H(X, p_1) \quad (5.18)$$

holds for

$$X \stackrel{\text{def}}{=} \left\{ |\phi_1\rangle\langle\phi_1|, \dots, |\phi_n\rangle\langle\phi_n| \right\} \quad (5.19)$$

$$p_1(|\phi_{\nu}\rangle\langle\phi_{\nu}|) \stackrel{\text{def}}{=} \lambda_{\nu} \quad \forall \nu \in \{1, \dots, n\}. \quad (5.20)$$

Warning: If $\{\phi_1, \dots, \phi_n\}$ is not an orthonormal system then (5.19) and (5.20) do **not** imply (5.18) in general!

Theorem 5.2.1 (KLEIN'S INEQUALITY¹²) *For all $\hat{A}, \hat{B} \in \mathcal{L}(\mathcal{H})$ we have*

$$\begin{aligned} 0 \leq \hat{A} \neq \hat{B} \geq 0, \quad \ker(\hat{B}) \subset \ker(\hat{A}) \\ \implies \text{trace} \left(\hat{A} \left(\ln \hat{A} - \ln \hat{B} \right) \right) > \text{trace}(\hat{A} - \hat{B}). \end{aligned}$$

Outline of proof: Thanks to the spectral theorem there are orthonormal systems $\{\phi_1, \dots, \phi_n\}$ and $\{\phi'_1, \dots, \phi'_n\}$ of \mathcal{H} with

$$\hat{A} = \sum_{\nu=1}^n \underbrace{a_{\nu}}_{\geq 0} |\phi_{\nu}\rangle\langle\phi_{\nu}|, \quad \hat{B} = \sum_{\nu=1}^n \underbrace{b_{\nu}}_{\geq 0} |\phi'_{\nu}\rangle\langle\phi'_{\nu}|$$

for suitable a_1, \dots, b_n . Then

$$\text{trace}(\hat{A} \ln \hat{A}) = \sum_{\nu=1}^n a_{\nu} \ln a_{\nu}$$

and

$$\begin{aligned} \text{trace}(\hat{A} \ln \hat{B}) &= \sum_{\alpha=1}^n \left\langle \phi_{\alpha} \left| \sum_{\beta=1}^n a_{\beta} |\phi_{\beta}\rangle\langle\phi_{\beta}| \sum_{\gamma=1}^n \ln b_{\gamma} |\phi_{\gamma}\rangle\langle\phi_{\gamma}| \phi_{\alpha} \right. \right\rangle \\ &= \sum_{\alpha, \gamma=1}^n a_{\alpha} \ln(b_{\gamma}) |\langle\phi_{\alpha} | \phi'_{\gamma}\rangle|^2, \end{aligned}$$

hence

$$\text{trace}(\hat{A} \ln \hat{A}) - \text{trace}(\hat{A} \ln \hat{B}) = \sum_{\alpha=1}^n a_{\alpha} \left(\ln a_{\alpha} - \sum_{\gamma=1}^n \ln(b_{\gamma}) |\langle\phi_{\alpha} | \phi'_{\gamma}\rangle|^2 \right).$$

¹²See (Klein, 1931).

Since, for $x > 0$, $\ln(x)$ is a strictly concave function,¹³ the latter implies

$$\text{trace}(\hat{A} \ln \hat{A}) - \text{trace}(\hat{A} \ln \hat{B}) \quad (5.21)$$

$$\geq \sum_{\alpha=1}^n a_{\alpha} \left(\ln a_{\alpha} - \ln \left(\sum_{\gamma=1}^n b_{\gamma} |\langle \phi_{\alpha} | \phi'_{\gamma} \rangle|^2 \right) \right) \quad (5.22)$$

$$\begin{aligned} &\stackrel{(5.10)}{\geq} \sum_{\alpha=1}^n \left(a_{\alpha} - \sum_{\gamma=1}^n b_{\gamma} |\langle \phi_{\alpha} | \phi'_{\gamma} \rangle|^2 \right) \quad (5.23) \\ &= \sum_{\alpha=1}^n a_{\alpha} - \sum_{\gamma=1}^n b_{\gamma} \\ &= \text{trace}(\hat{A} - \hat{B}). \end{aligned}$$

In (5.22) equality holds only if, for every $\alpha \in \{1, \dots, n\}$, at most one of products $a_{\alpha} b_{\gamma} |\langle \phi_{\alpha} | \phi'_{\gamma} \rangle|^2$ is different from zero. Then, with suitable relabelling of the ϕ'_{γ} , we have $\sum_{\gamma=1}^n b_{\gamma} |\langle \phi_{\alpha} | \phi'_{\gamma} \rangle|^2 = b_{\alpha}$ and equality in (5.23) holds only if $a_{\alpha} = b_{\alpha}$ for all $\alpha \in \{1, \dots, n\}$, i.e. if $\hat{A} = \hat{B}$. ■

Remark: As an immediate consequence of Theorem 5.2.1 we have strict positivity of the *quantum relative entropy*

$$S(\hat{\rho} \parallel \hat{\rho}') \stackrel{\text{def}}{=} \text{trace} \left(\hat{\rho} (\ln \hat{\rho} - \ln \hat{\rho}') \right)$$

for all states $\hat{\rho}, \hat{\rho}' \in S(\mathcal{H})$ with $\ker(\hat{\rho}') \subset \ker(\hat{\rho})$ and $\hat{\rho} \neq \hat{\rho}'$.

Corollary 5.2.2 *Let $\mathcal{H}_1, \mathcal{H}_2$ be HILBERT spaces and $\hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$. Then*

$$S_1(\hat{\rho}) \leq S_1(\text{trace}_2(\hat{\rho})) + S_1(\text{trace}_1(\hat{\rho})) \quad (\text{subadditivity})$$

and

$$S_1(\hat{\rho}) = S_1(\text{trace}_2(\hat{\rho})) + S_1(\text{trace}_1(\hat{\rho})) \iff \hat{\rho} = \text{trace}_2(\hat{\rho}) \otimes \text{trace}_1(\hat{\rho}).$$

Outline of proof: Application of KLEIN's inequality to

$$\hat{A} = \hat{\rho}, \quad \hat{B} = \text{trace}_2(\hat{\rho}) \otimes \text{trace}_1(\hat{\rho})$$

gives

$$\begin{aligned} 0 &= \text{trace}(\hat{A} - \hat{B}) \\ &\leq -S_1(\hat{\rho}) - \text{trace}(\hat{A} \log_2 \hat{B}) \end{aligned}$$

———— DRAFT, June 26, 2009 ————

¹³Strictly concave functions f of $x > 0$ are those fulfilling

$$\lambda f(x_1) + (1 - \lambda) f(x_2) < f(\lambda x_1 + (1 - \lambda) x_2) \quad \forall \lambda \in (0, 1), x_1, x_2 > 0.$$

with equality only for $\hat{\rho} = \text{trace}_2(\hat{\rho}) \otimes \text{trace}_1(\hat{\rho})$. Since

$$\begin{aligned} & \text{trace}(\hat{A} \log \hat{B}) \\ &= \text{trace} \left(\hat{A} \left(\log_2(\text{trace}_2(\hat{\rho})) \otimes \hat{1} + \hat{1} \otimes \log_2(\text{trace}_1(\hat{\rho})) \right) \right) \\ &= \text{trace} \left(\text{trace}_2(\hat{\rho}) \log_2(\text{trace}_2(\hat{\rho})) \right) + \text{trace} \left(\text{trace}_1(\hat{\rho}) \log_2(\text{trace}_1(\hat{\rho})) \right) \\ &= -S_1(\text{trace}_2(\hat{\rho})) - S_1(\text{trace}_1(\hat{\rho})), \end{aligned}$$

this proves the corollary. ■

The VON NEUMANN entropy of a state ρ increases if the latter is changed by a complete projective measurement operation (ignoring the results):

Corollary 5.2.3 *Let \mathcal{H} be a HILBERT space, $\hat{\rho}_0 \in S(\mathcal{H})$, $\{\hat{P}_1, \dots, \hat{P}_l\}$ a set of pairwise orthogonal projection operators on \mathcal{H} with*

$$\hat{P}_1 + \dots + \hat{P}_l = \hat{1}$$

and define

$$\hat{\rho}'_0 \stackrel{\text{def}}{=} \sum_{k=1}^l \hat{P}_k \hat{\rho}_0 \hat{P}_k.$$

Then

$$\hat{\rho}_0 \neq \hat{\rho}'_0 \implies S_1(\hat{\rho}_0) < S_1(\hat{\rho}'_0).$$

Proof: Since

$$\begin{aligned} \text{trace}(\hat{\rho} \log_2 \hat{\rho}') &= \text{trace} \left(\underbrace{\sum_{k=1}^l \hat{P}_k \hat{P}_k}_{=\hat{1}} \hat{\rho} \log_2 \hat{\rho}' \right) \\ &= \text{trace} \left(\sum_{k=1}^l \hat{P}_k \hat{\rho} \log_2(\hat{\rho}') \hat{P}_k \right) \\ &\stackrel{[\hat{\rho}', \hat{P}_k]_{-}=0}{=} \text{trace} \left(\sum_{k=1}^l \hat{P}_k \hat{\rho} \hat{P}_k \log_2(\hat{\rho}') \right) \\ &= -S_1(\hat{\rho}'), \end{aligned}$$

The statement follows from KLEIN's inequality (Theorem 5.2.1) applied to $\hat{A} = \hat{\rho}$, $\hat{B} = \hat{\rho}'$. ■

Warning: In general, trace preserving quantum operations may **decrease** the VON NEUMANN entropy.¹⁴

———— DRAFT, June 26, 2009 ————

¹⁴E.g., if

$$\hat{K}_1 = |0\rangle\langle 0| \quad \hat{K}_2 = |0\rangle\langle 1|$$

5.2.2 Accessible Information

Assume that the ‘alphabet’ $X = \{\hat{\rho}_1, \dots, \hat{\rho}_{N_1}\}$ is a set of (pairwise different) states on \mathcal{H} . Then, by “drawing the ‘letter’ $\hat{\rho}$ from X ” we mean the random choice of an individual from an ensemble in the state $\hat{\rho}$. Again, for simplicity, we assume that for every letter $\hat{\rho}$ its probability $p_1(\hat{\rho})$ for being drawn is given, positive, and does not depend on which letters have been drawn before.

The best one can do, in order to acquire information about a drawn letter, is perform a POV measurement¹⁵ corresponding to some set $Y = \{\hat{E}_1, \dots, \hat{E}_{N_2}\}$ of *events* \hat{E} represented by positive bounded operators on \mathcal{H} with¹⁶

$$\hat{E}_1 + \dots + \hat{E}_{N_2} = \hat{1}.$$

According to quantum mechanical rules, the probability for \hat{E} is $\text{trace}(\hat{\rho} \hat{E})$, if $\hat{\rho}$ was drawn. Hence, the probability for $\hat{\rho}$ being drawn and \hat{E} being detected is¹⁷

$$p(\hat{\rho}, \hat{E}) \stackrel{\text{def}}{=} p_1(\hat{\rho}) \text{trace}(\hat{\rho} \hat{E}). \quad (5.24)$$

If the letter drawn is unknown, the probability for \hat{E} is

$$\begin{aligned} p_2(\hat{E}) & \stackrel{(5.7)}{=} \sum_{j=1}^{N_1} p(\hat{\rho}_j, \hat{E}) \\ & = \text{trace}(\hat{\rho}_0 \hat{E}), \end{aligned}$$

where

$$\hat{\rho}_0 \stackrel{\text{def}}{=} \sum_{j=1}^{N_1} p_1(\hat{\rho}_j) \hat{\rho}_j$$

is the state of the source providing the letters. Of course,¹⁸ $\hat{\rho}_0$ does not uniquely determine (X, p_1) . Nevertheless, the VON NEUMANN *entropy* fulfills the HOLEVO *bound*

$$I(X : Y) \leq S_1(\hat{\rho}_0) - \sum_{j=1}^{N_1} p_1(\hat{\rho}_j) S_1(\hat{\rho}_j) \quad (5.25)$$

———— DRAFT, June 26, 2009 ————

are the KRAUS operator of the quantum operation \mathfrak{C} acting on a qubit system we have $\mathfrak{C}(\hat{1}/2) = |0\rangle\langle 0|$ and hence

$$S_1(\hat{1}/2) > S_1(\mathfrak{C}(\hat{1}/2)) = 0.$$

¹⁵If the elements of X are linearly independent, then the best result can be achieved by projective measurement, i.e. with $\hat{E}_1, \dots, \hat{E}_{N_2}$ being projection operators (Eldar, 2003). For the importance of considering also linearly dependent \hat{E}_ν ’s see, e.g., (Kaszlikowski et al., 2003).

¹⁶Recall Corollary A.4.3, in this connection.

¹⁷Obviously, (5.24) is consistent with (5.6).

¹⁸Recall Corollary A.4.3.

(Nielsen and Chuang, 2001, Theorem 12.1) and the condition

$$\boxed{\begin{aligned} &\exists j_1, j_2 \in \{1, \dots, N_1\} : \text{trace}(\hat{\rho}_{j_1} \hat{\rho}_{j_2}) \neq 0, j_1 \neq j_2 \\ \implies &S_1(\hat{\rho}_0) < H(X, p_1) + \sum_{j=1}^{N_1} p_1(\hat{\rho}_j) S_1(\hat{\rho}_j) \end{aligned}} \quad (5.26)$$

(Nielsen and Chuang, 2001, Theorem 11.10). A direct consequence of (5.25) and (5.26) is the upper bound

$$\begin{aligned} &\exists j_1, j_2 \in \{1, \dots, N_1\} : \text{trace}(\hat{\rho}_{j_1} \hat{\rho}_{j_2}) \neq 0, j_1 \neq j_2 \\ \implies &A(X, p) < H(X, p_1) \end{aligned} \quad (5.27)$$

on the *accessible information*

$$A(X, p) \stackrel{\text{def}}{=} \max_{Y \equiv \text{POV}} I(X : Y). \quad (5.28)$$

Hence:

It is impossible to get full information on the letters actually drawn unless¹⁹

$$\hat{\rho} \neq \hat{\rho}' \implies \hat{\rho} \hat{\rho}' = \hat{0} \quad \forall \hat{\rho}, \hat{\rho}' \in X.$$

Remark: Note that, for arbitrary $\hat{\rho}, \hat{\rho}' \in S(\mathcal{H})$ we have²⁰

$$\begin{aligned} \hat{\rho} \hat{\rho}' = \hat{0} &\iff \text{trace}(\hat{\rho} \hat{\rho}') = 0 \\ &\iff \hat{\rho} \mathcal{H} \perp \hat{\rho}' \mathcal{H}. \end{aligned}$$

On the other hand, (5.27) (together with continuity of the entropies) implies the bound

$$A(X, p) \leq S_1(\hat{\rho}_0). \quad (5.29)$$

———— DRAFT, June 26, 2009 ————

¹⁹Otherwise, distinguishability of arbitrary states could be used for superluminal communication.

²⁰Here, positivity of the operators $\hat{\rho}, \hat{\rho}'$ is essential! For $\hat{A} = \hat{A}^\dagger \in \mathcal{L}(\mathcal{H})$ the range $\hat{A} \mathcal{H}$ of \hat{A} is also called the *support* of \hat{A} , since

$$\hat{A} \Psi \neq 0 \iff 0 \neq \Psi \in \hat{A} \mathcal{H}$$

for such \hat{A} .

5.2.3 Distance Measures for Quantum States²¹

A natural distance measure for quantum states $\hat{\rho}, \hat{\rho}'$ of a finite-dimensional²² quantum system is the **trace distance**²³

$$D(\hat{\rho}, \hat{\rho}') \stackrel{\text{def}}{=} \frac{1}{2} \|\hat{\rho} - \hat{\rho}'\|_1, \quad (5.30)$$

where $\|\cdot\|_1$ denotes the **trace norm**

$$\|A\|_1 \stackrel{\text{def}}{=} \text{trace} \left(\sqrt[+]{\hat{A}^\dagger \hat{A}} \right) \quad (5.31)$$

for trace class operators \hat{A} on a HILBERT space \mathcal{H} . Especially for qubits we have

$$\hat{\rho} = \frac{1}{2} (\hat{1} + \boldsymbol{\rho} \cdot \hat{\boldsymbol{\tau}}), \quad \hat{\rho}' = \frac{1}{2} (\hat{1} + \boldsymbol{\rho}' \cdot \hat{\boldsymbol{\tau}})$$

and hence²⁴

$$\begin{aligned} D(\hat{\rho}, \hat{\rho}') &= \frac{1}{4} \text{trace} \sqrt[+]{(\boldsymbol{\rho} \cdot \hat{\boldsymbol{\tau}} - \boldsymbol{\rho}' \cdot \hat{\boldsymbol{\tau}})^2} \\ &= \frac{1}{4} \text{trace} \left(|\boldsymbol{\rho} - \boldsymbol{\rho}'| \sqrt[+]{\hat{1}} \right) \\ &= \frac{1}{2} |\boldsymbol{\rho} - \boldsymbol{\rho}'|, \end{aligned}$$

i.e.:

For qubit states $\hat{\rho}, \hat{\rho}'$ the trace distance is half the EUCLIDEAN distance of the corresponding BLOCH vectors $\boldsymbol{\rho}, \boldsymbol{\rho}'$.

For general mixed states we have the following:

Lemma 5.2.4 *Let \mathcal{H} be a finite-dimensional HILBERT space and $\hat{\rho}, \hat{\rho}' \in S(\mathcal{H})$. Then²⁵*

$$D(\hat{\rho}, \hat{\rho}') = \max_{\hat{P} \in \mathcal{P}} \left(\text{trace}(\hat{P} \hat{\rho}) - \text{trace}(\hat{P} \hat{\rho}') \right), \quad (5.32)$$

where \mathcal{P} denotes the set of all projection operators on \mathcal{H} .

———— DRAFT, June 26, 2009 ————

²¹See also (Gilchrist et al., 2005).

²²For infinite-dimensional systems, however, the trace distance is not physically adequate (Streater, 2003).

²³Note that

$$\left. \begin{aligned} \hat{\rho} &= \sum_{\nu=1}^{\infty} p_{\nu} |\Phi_{\nu}\rangle \langle \Phi_{\nu}|, \\ \hat{\rho}' &= \sum_{\nu=1}^{\infty} p'_{\nu} |\Phi_{\nu}\rangle \langle \Phi_{\nu}| \end{aligned} \right\} \implies D(\hat{\rho}, \hat{\rho}') = \frac{1}{2} \sum_{\nu=1}^{\infty} |p_{\nu} - p'_{\nu}|$$

if $\{|\Phi_{\nu}\rangle\}_{\nu \in \mathbb{N}}$ is a MONS of \mathcal{H} .

²⁴Recall that

$$|\mathbf{e}| = 1 \implies (\mathbf{e} \cdot \hat{\boldsymbol{\tau}})^2 = \hat{1} \quad \forall \mathbf{e} \in \mathbb{R}^3.$$

²⁵This formula holds also with \mathcal{P} replaced by the set of all *events*; i.e. of all positive operators with trace ≤ 1 .

Outline of proof: The spectral theorem tells us that there are an orthonormal basis $\{\phi_\nu\}_{\nu \in \mathbb{N}}$ of \mathcal{H} and real numbers $\lambda_1, \dots, \lambda_n$ with

$$\hat{\rho} - \hat{\rho}' = \sum_{\nu=1}^n \lambda_\nu \phi_\nu \quad (5.33)$$

and

$$\sum_{\nu=1}^n \lambda_\nu = 0. \quad (5.34)$$

Then

$$\sqrt{\hat{\rho} - \hat{\rho}'} = \sum_{\nu=1}^n |\lambda_\nu| \phi_\nu$$

and, therefore,

$$\begin{aligned} D(\hat{\rho}, \hat{\rho}') &= \frac{1}{2} \sum_{\nu=1}^n |\lambda_\nu| \\ &\stackrel{(5.34)}{=} \sum_{\substack{\nu \in \{1, \dots, n\} \\ \lambda_\nu > 0}} \lambda_\nu \\ &= \text{trace} \left(\sum_{\substack{\nu \in \{1, \dots, n\} \\ \lambda_\nu > 0}} \lambda_\nu \phi_\nu \right) \\ &\geq \text{trace} \left(\hat{P} \sum_{\substack{\nu \in \{1, \dots, n\} \\ \lambda_\nu > 0}} \lambda_\nu \phi_\nu \right) + \text{trace} \left(\hat{P} \sum_{\substack{\nu \in \{1, \dots, n\} \\ \lambda_\nu \leq 0}} \lambda_\nu \phi_\nu \right) \quad \forall \hat{P} \in \mathcal{P} \end{aligned}$$

with equality for

$$\hat{P} = \sum_{\substack{\nu \in \{1, \dots, n\} \\ \lambda_\nu > 0}} |\phi_\nu\rangle\langle\phi_\nu|.$$

By (5.33) and linearity of the trace, this implies (5.32). ■

Now it is obvious that the **trace distance is a metric** on the set of states:²⁶

$$\begin{aligned} D(\hat{\rho}_1, \hat{\rho}_2) &\geq 0, \\ D(\hat{\rho}_1, \hat{\rho}_2) &= 0 \iff \hat{\rho}_1 = \hat{\rho}_2, \\ D(\hat{\rho}_1, \hat{\rho}_2) &= D(\hat{\rho}_2, \hat{\rho}_1), \\ D(\hat{\rho}_1, \hat{\rho}_3) &\leq D(\hat{\rho}_1, \hat{\rho}_2) + D(\hat{\rho}_2, \hat{\rho}_3). \end{aligned}$$

Corollary 5.2.5 *Let \mathcal{H}_1 and \mathcal{H}_2 be finite-dimensional HILBERT spaces and let $\mathfrak{C} \in \mathcal{Q}(\mathcal{H}_1, \mathcal{H}_1)$ be trace-preserving. Then $\mathcal{Q}(\mathcal{H}_1, \mathcal{H}_1)$ is **contractive** w.r.t. the trace distance, i.e.:*

$$D(\mathfrak{C}(\hat{\rho}), \mathfrak{C}(\hat{\rho}')) \leq D(\hat{\rho}, \hat{\rho}') \quad \forall \hat{\rho}, \hat{\rho}' \in S(\mathcal{H}_1).$$

———— DRAFT, June 26, 2009 ————

²⁶The inequality follows from (5.32) and

$$\text{trace}(\hat{\rho}_1) - \text{trace}(\hat{\rho}_3) = \left(\text{trace}(\hat{\rho}_1) - \text{trace}(\hat{\rho}_2) \right) + \left(\text{trace}(\hat{\rho}_2) - \text{trace}(\hat{\rho}_3) \right).$$

Outline of proof: With ϕ_1, \dots, ϕ_n and $\lambda_1, \dots, \lambda_n$ chosen as in the proof for (5.32), we have²⁷

$$\begin{aligned}
D(\hat{\rho}, \hat{\rho}') &= \text{trace} \left(\sum_{\substack{\nu \in \{1, \dots, n\} \\ \lambda_\nu > 0}} \lambda_\nu \phi_\nu \right) \\
&= \text{trace} \left(\bar{\mathfrak{C}} \left(\sum_{\substack{\nu \in \{1, \dots, n\} \\ \lambda_\nu > 0}} \lambda_\nu \phi_\nu \right) \right) \\
&\geq \text{trace} \left(\hat{P} \bar{\mathfrak{C}} \left(\sum_{\substack{\nu \in \{1, \dots, n\} \\ \lambda_\nu > 0}} \lambda_\nu \phi_\nu \right) \right) + \text{trace} \left(\hat{P} \bar{\mathfrak{C}} \left(\sum_{\substack{\nu \in \{1, \dots, n\} \\ \lambda_\nu \leq 0}} \lambda_\nu \phi_\nu \right) \right) \\
&= \text{trace} \left(\hat{P} (\mathfrak{C}(\hat{\rho}) - \hat{\mathfrak{c}}(\hat{\rho}')) \right) \quad \forall \hat{P} \in \mathcal{P}.
\end{aligned}$$

This, together with (5.32), proves the theorem. ■

Corollary 5.2.6 *Let \mathcal{H} be a HILBERT space and $N \in \mathbb{N}$. Moreover, consider $\hat{\rho}_1, \dots, \hat{\rho}'_N \in S(\mathcal{H})$ and $p_1, \dots, p'_N \geq 0$ with*

$$\sum_{\nu=1}^N p_\nu = 1 = \sum_{\nu=1}^N p'_\nu. \quad (5.35)$$

Then

$$D \left(\sum_{\nu=1}^N p_\nu \hat{\rho}_\nu, \sum_{\nu=1}^N p'_\nu \hat{\rho}'_\nu \right) \leq \frac{1}{2} \sum_{\nu=1}^N |p_\nu - p'_\nu| + \sum_{\nu=1}^N p_\nu D(\hat{\rho}_\nu, \hat{\rho}'_\nu). \quad (5.36)$$

Outline of proof: By Lemma 5.2.4 there is a $\hat{P} \in \mathcal{P}$ with

$$\begin{aligned}
D \left(\sum_{\nu=1}^N p_\nu \hat{\rho}_\nu, \sum_{\nu=1}^N p'_\nu \hat{\rho}'_\nu \right) &= \text{trace} \left(\hat{P} \sum_{\nu=1}^N p_\nu \hat{\rho}_\nu - \hat{P} \sum_{\nu=1}^N p'_\nu \hat{\rho}'_\nu \right) \\
&= \sum_{\nu=1}^N \left(p_\nu \underbrace{\text{trace} \left(\hat{P} \hat{\rho}_\nu - \hat{P} \hat{\rho}'_\nu \right)}_{\substack{\leq D(\hat{\rho}_\nu, \hat{\rho}'_\nu) \\ \text{L. 5.2.4}}} + (p_\nu - p'_\nu) \underbrace{\text{trace} \left(\hat{P} \hat{\rho}'_\nu \right)}_{\in [0,1]} \right) \\
&\leq \sum_{\nu=1}^N p_\nu D(\hat{\rho}_\nu, \hat{\rho}'_\nu) + \sum_{\substack{\nu \in \{1, \dots, N\} \\ p_\nu - p'_\nu > 0}} (p_\nu - p'_\nu).
\end{aligned}$$

Together with

$$\sum_{\substack{\nu \in \{1, \dots, N\} \\ p_\nu - p'_\nu > 0}} (p_\nu - p'_\nu) \stackrel{(5.35)}{=} \frac{1}{2} \sum_{\nu=1}^N |p_\nu - p'_\nu|$$

this implies (5.36). ■

A direct consequence of (5.36) is

$$D\left(\sum_{\nu=1}^N p_{\nu} \hat{\rho}_{\nu}, \sum_{\nu=1}^N p_{\nu} \hat{\rho}'_{\nu}\right) \leq \sum_{\nu=1}^N p_{\nu} D(\hat{\rho}_{\nu}, \hat{\rho}'_{\nu}). \quad (5.37)$$

Moreover, setting $\hat{\rho}'_{\nu} \equiv \hat{\rho}'$ in (5.37) and recalling (5.35), we get

$$D\left(\sum_{\nu=1}^N p_{\nu} \hat{\rho}_{\nu}, \hat{\rho}'\right) \leq \sum_{\nu=1}^N p_{\nu} D(\hat{\rho}_{\nu}, \hat{\rho}'). \quad (5.38)$$

Another important measure for the distance of states is the BURES *fidelity*.²⁸

$$F(\hat{\rho}, \hat{\rho}') \stackrel{\text{def}}{=} \left(\text{trace} \sqrt{\left(\sqrt{\hat{\rho}} \sqrt{\hat{\rho}'} \sqrt{\hat{\rho}} \right)^{\dagger} \left(\sqrt{\hat{\rho}} \sqrt{\hat{\rho}'} \sqrt{\hat{\rho}} \right)} \right)^2.$$

Since $\sqrt{|\psi\rangle\langle\psi|} = |\psi\rangle\langle\psi|$ and hence

$$\begin{aligned} \sqrt{\sqrt{|\psi\rangle\langle\psi|} \hat{\rho}' \sqrt{|\psi\rangle\langle\psi|}} &= \sqrt{|\psi\rangle\langle\psi| \hat{\rho}' |\psi\rangle\langle\psi|} \\ &= \sqrt{\langle\psi| \hat{\rho}' |\psi\rangle} |\psi\rangle\langle\psi| \end{aligned}$$

holds for all normalized $\psi \in \mathcal{H}$, we have:

$$\boxed{\hat{\rho} = |\psi\rangle\langle\psi| \implies F(\hat{\rho}, \hat{\rho}') = \langle\psi| \hat{\rho}' |\psi\rangle \quad \forall \hat{\rho}, \hat{\rho}' \in S(\mathcal{H}).} \quad (5.39)$$

Symmetry of the fidelity in general is not evident from its definition but follows directly from UHLMANN'S *theorem* (Uhlman, 1976):

Theorem 5.2.7 *Let \mathcal{H} be a HILBERT-space and $\hat{\rho}_1, \hat{\rho}_2 \in S(\mathcal{H})$. Then*

$$F(\hat{\rho}_1, \hat{\rho}_2) = \max_{\Psi_1 \in \mathcal{T}_{\hat{\rho}_1}, \Psi_2 \in \mathcal{T}_{\hat{\rho}_2}} |\langle\Psi_1 | \Psi_2\rangle|^2,$$

where²⁹

$$\mathcal{T}_{\hat{\rho}} \stackrel{\text{def}}{=} \left\{ \Psi \in \mathcal{H} \otimes \mathcal{H} : \hat{\rho} = \text{trace}_2(|\Psi\rangle\langle\Psi|) \right\} \quad \forall \hat{\rho} \in S(\mathcal{H}).$$

DRAFT, June 26, 2009

²⁸For commuting $\hat{\rho}, \hat{\rho}'$ the BURES fidelity has a simple geometrical interpretation, since

$$\left. \begin{aligned} \hat{\rho} &= \sum_{\nu} p_{\nu} |\phi_{\nu}\rangle\langle\phi_{\nu}|, \\ \hat{\rho}' &= \sum_{\nu} p'_{\nu} |\phi_{\nu}\rangle\langle\phi_{\nu}| \end{aligned} \right\} \implies F(\hat{\rho}, \hat{\rho}') = \left(\sum_{\nu} \sqrt{p_{\nu} p'_{\nu}} \right)^2.$$

See (Chen et al., 2002) for a geometrical interpretation of the BURES fidelity of general qubit states.

²⁹Note that $\mathcal{T}_{\hat{\rho}}$ is the set of all purifications of $\hat{\rho}$ as introduced in Lemma A.4.8.

Outline of proof: Let $j \in \{1, 2\}$ and $\Psi_j \in \mathcal{T}_{\hat{\rho}_j}$. By the spectral theorem, there is an orthonormal basis $\{\phi_1^{(j)}, \dots, \phi_n^{(j)}\}$ of \mathcal{H} , some $n' \in \{1, \dots, n\}$, and $s_1^{(j)}, \dots, s_{n'}^{(j)} > 0$ with

$$\hat{\rho}_j = \sum_{\nu=1}^{n'} \left(s_{\nu}^{(j)} \right)^2 \phi_{\nu}^{(j)}.$$

Therefore, the SCHMIDT-decomposition of Ψ_j has to be of the form

$$\begin{aligned} \Psi_j &= \sum_{\nu=1}^{n'} s_{\nu}^{(j)} \phi_{\nu}^{(j)} \otimes \psi_{\nu}^{(j)} \\ &= \sum_{\nu=1}^{n'} \left(\sqrt[3]{\hat{\rho}_j} \phi_{\nu}^{(j)} \right) \otimes \psi_{\nu}^{(j)} \end{aligned}$$

with some orthonormal basis $\{\psi_1^{(j)}, \dots, \psi_n^{(j)}\}$ of \mathcal{H} . Considering $j = 1$ and $j = 2$ together we thus get

$$\langle \Psi_2 | \Psi_1 \rangle = \sum_{\nu, \mu=1}^{n'} \left\langle \sqrt[3]{\hat{\rho}_2} \phi_{\nu}^{(2)} \mid \sqrt[3]{\hat{\rho}_1} \phi_{\mu}^{(1)} \right\rangle \left\langle \psi_{\nu}^{(2)} \mid \psi_{\mu}^{(1)} \right\rangle. \quad (5.40)$$

In order to rewrite the r.h.s. of (5.40) as a trace we use the unitary operators \hat{V} and \hat{V}' characterized by

$$\hat{V} \phi_{\mu}^{(2)} = \phi_{\mu}^{(1)} \quad \forall \mu \in \{1, \dots, n\}$$

and

$$\left\langle \phi_{\mu}^{(2)} \mid \hat{V}' \phi_{\nu}^{(2)} \right\rangle = \left\langle \psi_{\nu}^{(2)} \mid \psi_{\mu}^{(1)} \right\rangle \quad \forall \nu, \mu \in \{1, \dots, n\}.$$

Then

$$\begin{aligned} \langle \Psi_2 | \Psi_1 \rangle &\stackrel{(5.40)}{=} \sum_{\nu, \mu=1}^{n'} \left\langle \sqrt[3]{\hat{\rho}_2} \phi_{\nu}^{(2)} \mid \sqrt[3]{\hat{\rho}_1} \hat{V} \phi_{\mu}^{(2)} \right\rangle \left\langle \phi_{\mu}^{(2)} \mid \hat{V}' \phi_{\nu}^{(2)} \right\rangle \\ &= \sum_{\nu=1}^{n'} \left\langle \phi_{\nu}^{(2)} \mid \sqrt[3]{\hat{\rho}_2} \sqrt[3]{\hat{\rho}_1} \hat{V} \hat{V}' \phi_{\nu}^{(2)} \right\rangle \\ &= \text{trace} \left(\sqrt[3]{\hat{\rho}_2} \sqrt[3]{\hat{\rho}_1} \hat{V} \hat{V}' \right) \\ &= \text{trace} \left(\hat{V} \hat{V}' \sqrt[3]{\hat{\rho}_2} \sqrt[3]{\hat{\rho}_1} \right) \end{aligned}$$

Applying Lemma 5.2.8, below, to the polar decomposition

$$\hat{V} \hat{V}' \sqrt[3]{\hat{\rho}_2} \sqrt[3]{\hat{\rho}_1} = \hat{U} \sqrt[3]{\left(\sqrt[3]{\hat{\rho}_2} \sqrt[3]{\hat{\rho}_1} \right)^{\dagger} \left(\sqrt[3]{\hat{\rho}_2} \sqrt[3]{\hat{\rho}_1} \right)}, \quad \hat{U} \text{ unitary,}$$

(see, e.g., Lemma 7.3.20 of (Lücke, eine)) we always get

$$\begin{aligned} |\langle \Psi_1 | \Psi_2 \rangle|^2 &\leq \left(\text{trace} \sqrt[3]{\left(\sqrt[3]{\hat{\rho}_2} \sqrt[3]{\hat{\rho}_1} \right)^{\dagger} \left(\sqrt[3]{\hat{\rho}_2} \sqrt[3]{\hat{\rho}_1} \right)} \right)^2 \\ &= F(\hat{\rho}_1, \hat{\rho}_1). \end{aligned}$$

Obviously, by appropriate choice of the $\psi_{\nu}^{(j)}$ we get equality. ■

Lemma 5.2.8 *Let \mathcal{H} be a finite-dimensional³⁰ HILBERT space. Then*

$$\left| \text{trace}(\hat{B} \hat{\rho}) \right| \leq \left\| \hat{B} \right\| \quad \forall \hat{\rho} \in S(\mathcal{H}), \hat{B} \in \mathcal{L}(\mathcal{H}).$$

Outline of proof: By the spectral theorem, there are an orthonormal basis $\{\phi_1, \dots, \phi_n\}$ of \mathcal{H} and $p_1, \dots, p_n \geq 0$ with

$$\hat{\rho} = \sum_{\nu=1}^n p_{\nu} |\phi_{\nu}\rangle\langle\phi_{\nu}|, \quad \sum_{\nu=1}^n p_{\nu} = 1.$$

Then

$$\begin{aligned} \left| \text{trace}(\hat{B} \hat{\rho}) \right| &= \left| \sum_{\nu=1}^n p_{\nu} \text{trace}(\hat{B} |\phi_{\nu}\rangle\langle\phi_{\nu}|) \right| \\ &= \left| \sum_{\nu=1}^n p_{\nu} \langle\phi_{\nu} | \hat{B} \phi_{\nu}\rangle \right| \\ &\leq \sum_{\nu=1}^n p_{\nu} \underbrace{\left| \langle\phi_{\nu} | \hat{B} \phi_{\nu}\rangle \right|}_{\leq \|\hat{B}\|} \\ &\leq \left\| \hat{B} \right\|. \quad \blacksquare \end{aligned}$$

UHLMANN'S theorem and the definition of the BURES fidelity show:

$$F(\hat{\rho}_1, \hat{\rho}_2) = F(\hat{\rho}_2, \hat{\rho}_1), \quad (5.41)$$

$$F(\hat{\rho}_1, \hat{\rho}_2) \in [0, 1], \quad (5.42)$$

$$F(\hat{\rho}_1, \hat{\rho}_2) = \begin{cases} 1 & \text{iff } \hat{\rho}_1 = \hat{\rho}_2 \\ 0 & \text{iff } \hat{\rho}_1 \hat{\rho}_2 = 0. \end{cases} \quad (5.43)$$

Using UHLMANN'S theorem one may also show:³¹

$$A(\hat{\rho}_1, \hat{\rho}_2) \stackrel{\text{def}}{=} \arccos \sqrt{F(\hat{\rho}_1, \hat{\rho}_2)} \in [0, \pi/2] \quad \text{is a metric,} \quad (5.44)$$

$$F(\mathfrak{C}(\hat{\rho}_1), \mathfrak{C}(\hat{\rho}_2)) \geq F(\hat{\rho}_1, \hat{\rho}_2), \quad (5.45)$$

$$F\left(\sum_{\nu} p_{\nu} \hat{\rho}_{\nu}, \sum_{\nu} p'_{\nu} \hat{\rho}'_{\nu}\right) \geq \sum_{\nu} \sqrt{p_{\nu} p'_{\nu}} F(\hat{\rho}_{\nu}, \hat{\rho}'_{\nu}). \quad (5.46)$$

For pure states ϕ, ψ :

$$\begin{aligned} F(\hat{P}_{\phi}, \hat{P}_{\psi}) &= |\langle\phi | \psi\rangle| \\ &= \sqrt{1 - D(\hat{P}_{\phi}, \hat{P}_{\psi})^2}. \end{aligned}$$

_____ DRAFT, June 26, 2009 _____

³⁰The given may be directly extended to the infinite-dimensional case.

³¹Necessary and sufficient conditions for a given set of **pure** states to be transformable via a quantum operation into another given set of (not necessarily pure) states are given in (Chefles et al., 2003, Theorem 4).

For general states:

$$\boxed{1 - F(\hat{\rho}_1, \hat{\rho}_2) \leq D(\hat{\rho}_1, \hat{\rho}_2) \leq \sqrt{1 - F(\hat{\rho}_1, \hat{\rho}_2)^2}}.$$

Remark: In principle, fidelity and trace distance are of equal use to characterize the difference of states. However, usually, calculations are easier with fidelity. Therefore only the latter will be used in the following.

Relevant for transmission of (unknown) states:

$$\begin{aligned} F_{\min}(\mathfrak{C}) &\stackrel{\text{def}}{=} \min_{\hat{\rho}} F(\hat{\rho}, \mathfrak{C}(\hat{\rho})) \\ &\stackrel{(5.46)}{=} \min_{\psi} F(\hat{P}_{\psi}, \mathfrak{C}(\hat{P}_{\psi})). \end{aligned}$$

Relevant for the (approximate) realization of a gate \hat{U} as the quantum operation \mathfrak{C} is the **gate fidelity**

$$\begin{aligned} F(\hat{U}, \mathfrak{C}) &\stackrel{\text{def}}{=} \min_{\hat{\rho}} F(\hat{U}\hat{\rho}\hat{U}^{-1}, \mathfrak{C}(\hat{\rho})) \\ &= \min_{\psi} F(\hat{P}_{\hat{U}\psi}, \mathfrak{C}(\hat{P}_{\hat{U}\psi})) \end{aligned}$$

for which we have, e.g.,³²

$$\arccos \sqrt{F(\hat{U}_1\hat{U}_2, \mathfrak{C}_1 \circ \mathfrak{C}_2)} \leq \arccos \sqrt{F(\hat{U}_1, \mathfrak{C}_1)} + \arccos \sqrt{F(\hat{U}_2, \mathfrak{C}_2)}.$$

Relevant for quantum sources producing $\hat{\rho}_j$ with probability p_j and disturbed by \mathfrak{C} is the **ensemble average fidelity**

$$\bar{F} \stackrel{\text{def}}{=} \sum_j p_j F(\hat{\rho}_j, \mathfrak{C}(\hat{\rho}_j)).$$

5.2.4 SCHUMACHER Encoding

Lemma 5.2.9 *Let \mathcal{H} be a finite-dimensional HILBERT space, $\hat{\rho}_0 \in S(\mathcal{H})$, and $\delta > 0$. Then*

$$\lim_{n \rightarrow \infty} \text{trace} \left(\hat{\rho}_0^{\otimes n} \hat{\Lambda}_{\hat{\rho}_0, \delta}^{(n)} \right) = 1$$

and³³

$$2^{n(S_1(\hat{\rho}_0) + \delta)} \geq \dim \left(\hat{\Lambda}_{\hat{\rho}_0, \delta}^{(n)} \mathcal{H}^{\otimes n} \right) \geq 2^{n(S_1(\hat{\rho}_0) - \delta)} \quad \forall n \in \mathbb{N},$$

where, for $n \in \mathbb{N}$, $\hat{\Lambda}_{\hat{\rho}_0, \delta}^{(n)}$ denotes the projector onto the subspace of all eigenvectors of $\hat{\rho}_0^{\otimes n}$ with eigenvalues in $[2^{n(S_1(\hat{\rho}_0) - \delta)}, 2^{n(S_1(\hat{\rho}_0) + \delta)}]$.

³²Recall (5.44).

³³See (Mitchison and Jozsa, 2003) in this connection.

Lemma 5.2.10

Let \mathcal{H} be a HILBERT space and \hat{A} a self-adjoint operator on \mathcal{H} . Then for arbitrary $\psi_1, \dots, \psi_N \in \mathcal{H}$ and $p_1, \dots, p_N > 0$ we have

$$\sum_{\nu=1}^N p_{\nu} \left| \langle \psi_{\nu} | \hat{A} \psi_{\nu} \rangle \right|^2 \geq 2 \operatorname{trace} \left(\hat{A} \sum_{\nu=1}^N p_{\nu} |\psi_{\nu}\rangle \langle \psi_{\nu}| \right) - \sum_{\nu=1}^N p_{\nu}.$$

Outline of proof: Apply the inequality

$$x^2 \geq 2x - 1 \quad \forall x \in \mathbb{R}$$

to $x = \langle \psi_{\nu} | \hat{A} \psi_{\nu} \rangle$. ■

⋮

make a guess, FANO inequality

5.2.5 A la NIELSEN/CHUANG

Klein inequality (Nielsen and Chuang, 2001, Theorem 11.7):³⁴

$$\text{trace} \left(\hat{\rho} \log(\hat{\rho}) \right) \geq \text{trace} \left(\hat{\rho} \log(\hat{\rho}') \right) \quad \forall \hat{\rho}, \hat{\rho}' \in S(\mathcal{H}). \quad (5.47)$$

$$H_{\text{bin}}(p) \stackrel{\text{def}}{=} H(\{p, 1-p\}) \quad \forall p \in [0, 1].$$

⋮

PPT criterion

Cat states implemented for JOSEPHSON junctions or coherent states (entanglement laser)

5.2.6 Entropy³⁵

Classically, every message can be encoded in a string of bits. But can quantum information always be encoded in a string of qubits?!

³⁴The r.h.s of (5.47) may become $-\infty$. Equality holds iff $\hat{\rho} = \hat{\rho}'$.

³⁵See also (Ohya and Petz, 1993) and (Petz, 2001).

Chapter 6

Handling Entanglement¹

We have seen in 4.4 that perfect entanglement may be used for implementing noiseless quantum communication. Therefore, quantification and handling (e.g., distillation) of entanglement is important. Here, for simplicity, we consider only bipartite systems. One might expect, then, that separability is equivalent to the existence of corresponding (local) hidden variable models, hence to the validity of all (generalized) BELL inequalities.² However, as shown in (Werner, 1989), that this is **not** the case.

6.1 Detecting Entanglement

Detecting entanglement of pure states is very easy:

$$\hat{\rho} \in S_{\text{pure}}(\mathcal{H}_1 \otimes \mathcal{H}_2) \cup S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2) \quad \begin{array}{c} \Longleftrightarrow \\ \text{Lemma A.4.6} \\ \text{Theorem A.4.7} \end{array} \quad \left\{ \begin{array}{l} \hat{\rho} \in S_{\text{pure}}(\mathcal{H}_1 \otimes \mathcal{H}_2) \\ (\text{trace}_2(\hat{\rho}))^2 = \text{trace}_2(\hat{\rho}). \end{array} \right.$$

It is mixedness which can make detection of entanglement a very hard problem (Gurvits, 2002).

6.1.1 Entanglement Witnesses and Non-Completely Positive Mappings

Lemma 6.1.1 *A state $\hat{\rho}$ of the bipartite system \mathcal{S} with state space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is non-separable³ iff it possesses an **entanglement witness**, i.e. an operator $\hat{W} \in \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ fulfilling the following two properties:⁴*

———— DRAFT, June 26, 2009 ————

¹See also (Horodecki et al., 2001) and references given there.

²See (Werner and Wolf, 2001; Collins and Gisin, 2003) in this connection.

³Recall Definition A.4.4.

⁴The second property guarantees that \hat{W} is Hermitian — thanks to the **polarization identity**

$$h(\mathbf{x}_1, \mathbf{x}_1) = \frac{1}{4} \sum_{\alpha=0}^3 (-i)^\alpha |\mathbf{x}_1 + i^\alpha \mathbf{x}_2\rangle \langle \mathbf{x}_1 + i^\alpha \mathbf{x}_2|,$$

valid for every mapping h that is linear in the second and conjugate linear in the first argument; especially for $h(\phi, \psi) = |\phi\rangle\langle\psi|$.

1.

$$\text{trace}(\hat{\rho}\hat{W}) < 0.$$

2.

$$\hat{\rho}' \text{ separable} \implies \text{trace}(\hat{\rho}'\hat{W}) \geq 0 \quad \forall \hat{\rho}' \in S(\mathcal{H}_1 \otimes \mathcal{H}_2).$$

Outline of proof: The statement follows from the known fact⁵ that for every point X outside a convex set \mathcal{K} there is a hyperplane separating X from \mathcal{K} . ■

Lemma 6.1.2 (Jamiołkowski) For $j \in \{1, 2\}$, let $\{\phi_1^{(j)}, \dots, \phi_{n_j}^{(j)}\}$ be a MONS of the HILBERT space \mathcal{H}_j . Then for every $\hat{W} \in \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ there is a unique linear mapping $\mathfrak{L}_{\hat{W}} : \mathcal{L}(\mathcal{H}_1) \rightarrow \mathcal{L}(\mathcal{H}_2)$ with

$$\hat{W} = n_1 (\mathbf{1} \otimes \mathfrak{L}_{\hat{W}}) (\hat{P}_{\mathcal{H}_1}^+), \quad (6.1)$$

where

$$\hat{P}_{\mathcal{H}_1}^+ \stackrel{\text{def}}{=} \frac{1}{n_1} \left| \sum_{\nu=1}^{n_1} \phi_{\nu}^{(1)} \otimes \phi_{\nu}^{(1)} \right\rangle \left\langle \sum_{\mu=1}^{n_1} \phi_{\mu}^{(1)} \otimes \phi_{\mu}^{(1)} \right|. \quad (6.2)$$

$\mathfrak{L}_{\hat{W}}$ fulfills

$$\mathfrak{L}_{\hat{W}} \left(|\phi_{\nu_1}^{(1)}\rangle \langle \phi_{\mu_1}^{(1)}| \right) = \sum_{\nu_2, \mu_2=1}^{n_2} \left\langle \phi_{\nu_1}^{(1)} \otimes \phi_{\nu_2}^{(2)} \mid \hat{W} \left(\phi_{\mu_1}^{(1)} \otimes \phi_{\mu_2}^{(2)} \right) \right\rangle |\phi_{\nu_2}^{(2)}\rangle \langle \phi_{\mu_2}^{(2)}| \quad (6.3)$$

for all $\nu_1, \nu_2 \in \{1, \dots, n_1\}$ and:

$$\mathfrak{L}_{\hat{W}} \text{ positive} \iff \text{trace}(\hat{W}\hat{\rho}) \geq 0 \quad \forall \hat{\rho} \in S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2), \quad (6.4)$$

where⁶

$$S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2) \stackrel{\text{def}}{=} \{ \hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2) : \hat{\rho} \text{ separable} \}. \quad (6.5)$$

Outline of proof: Defining $\mathfrak{L}_{\hat{W}}$ by (6.3) plus linear continuation gives

$$\begin{aligned} \hat{W} &= \sum_{\nu_1, \mu_1=1}^{n_1} \sum_{\nu_2, \mu_2=1}^{n_2} \left\langle \phi_{\nu_1}^{(1)} \otimes \phi_{\nu_2}^{(2)} \mid \hat{W} \left(\phi_{\mu_1}^{(1)} \otimes \phi_{\mu_2}^{(2)} \right) \right\rangle |\phi_{\nu_1}^{(1)} \otimes \phi_{\nu_2}^{(2)}\rangle \langle \phi_{\mu_1}^{(1)} \otimes \phi_{\mu_2}^{(2)}| \\ &\stackrel{(6.3)}{=} \sum_{\nu_1, \mu_1=1}^{n_1} \left(|\phi_{\nu_1}^{(1)}\rangle \langle \phi_{\mu_1}^{(1)}| \right) \otimes \mathfrak{L}_{\hat{W}} \left(|\phi_{\nu_1}^{(1)}\rangle \langle \phi_{\mu_1}^{(1)}| \right) \\ &\stackrel{\text{lin. cont.}}{=} (\mathbf{1} \otimes \mathfrak{L}_{\hat{W}}) \left(\sum_{\nu_1, \mu_1=1}^{n_1} |\phi_{\nu_1}^{(1)} \otimes \phi_{\nu_1}^{(1)}\rangle \langle \phi_{\mu_1}^{(1)} \otimes \phi_{\mu_1}^{(1)}| \right) \end{aligned}$$

DRAFT, June 26, 2009

⁵See, e.g., (Neumark, 1959, §1, No. 9) and (Robertson and Robertson, 1967, Kap. 1, Satz 8).

⁶Note that

$$S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2) \stackrel{\text{Theorem A.4.5}}{=} S(\mathcal{H}_1) \otimes_{\text{alg}} S(\mathcal{H}_2).$$

and hence (6.1). Conversely, (6.1) gives

$$\begin{aligned}
\mathfrak{L}_{\hat{W}}\left(\left|\phi_{\nu_1}^{(1)}\right\rangle\left\langle\phi_{\mu_1}^{(1)}\right|\right) &= \left\langle\phi_{\nu_1}^{(1)}\left|\sum_{\nu_1, \mu_1=1}^{n_1}\left(\left|\phi_{\nu_1}^{(1)}\right\rangle\left\langle\phi_{\mu_1}^{(1)}\right|\right)\otimes\mathfrak{L}_{\hat{W}}\left(\left|\phi_{\nu_1}^{(1)}\right\rangle\left\langle\phi_{\mu_1}^{(1)}\right|\right)\right|\phi_{\mu_1}^{(1)}\right\rangle \\
&\stackrel{\text{lin.}}{=} \left\langle\phi_{\nu_1}^{(1)}\left|\dim(\mathcal{H}_1)\left(\mathbf{1}\otimes\mathfrak{L}_{\hat{W}}\right)\left(\hat{P}_{\mathcal{H}_1}^+\right)\right|\phi_{\mu_1}^{(1)}\right\rangle \\
&\stackrel{(6.1)}{=} \left\langle\phi_{\nu_1}^{(1)}\left|\hat{W}\right|\phi_{\mu_1}^{(1)}\right\rangle,
\end{aligned}$$

i.e. (6.3). Since

$$\text{trace}\left(\hat{W}\sum_{k=1}^N\hat{\rho}_k^{(1)}\otimes\hat{\rho}_k^{(2)}\right)\stackrel{\text{Jami}}{=} \dim(\mathcal{H}_1)\sum_{k=1}^N\text{trace}\left(\hat{\rho}_k^{(1)}\otimes\mathfrak{L}_{\hat{W}}\left(\hat{\rho}_k^{(2)}\right)\right),$$

positivity of $\mathfrak{L}_{\hat{W}}$ implies nonnegativity of $\text{trace}(\hat{W}\hat{\rho})$ for separable⁷ $\hat{\rho}$. Conversely the latter implies positivity of $\mathfrak{L}_{\hat{W}}$, since

$$\left\langle\phi^{(2)}\left|\mathfrak{L}_{\hat{W}}\left(\left|\phi^{(1)}\right\rangle\left\langle\phi^{(1)}\right|\right)\phi^{(2)}\right\rangle\stackrel{(6.3)}{=} \left\langle\Psi_{\phi^{(1)},\phi^{(2)}}\left|\hat{W}\Psi_{\phi^{(1)},\phi^{(2)}}\right\rangle\quad\forall\phi^{(1)}\in\mathcal{H}_1,\phi^{(2)}\in\mathcal{H}_2,$$

where

$$\Psi_{\phi^{(1)},\phi^{(2)}}\stackrel{\text{def}}{=} \left(\sum_{\nu_1=1}^{\dim(\mathcal{H}_1)}\left\langle\phi^{(1)}\left|\phi_{\nu_1}^{(1)}\right\rangle\phi_{\nu_1}^{(1)}\right)\otimes\phi^{(2)}. \quad \blacksquare$$

Corollary 6.1.3 For $j\in\{1,2\}$, let $\{\phi_1^{(j)},\dots,\phi_{n_j}^{(j)}\}$ be a MONS of the HILBERT space \mathcal{H}_j . Then for every $\hat{W}\in\mathcal{L}(\mathcal{H}_1\otimes\mathcal{H}_2)$ we have⁸

$$\text{trace}(\hat{\rho}\hat{W}) < 0 \implies \left(\mathbf{1}\otimes\mathfrak{L}_{\hat{W}}^\dagger\right)(\hat{\rho}) \not\geq 0 \quad \forall\hat{\rho}\in S(\mathcal{H}_1\otimes\mathcal{H}_2) \quad (6.6)$$

and

$$\text{trace}(\hat{\rho}\hat{W}) \geq 0 \quad \forall\hat{\rho}\in S_{\text{sep}}(\mathcal{H}_1\otimes\mathcal{H}_2) \iff \mathfrak{L}_{\hat{W}}^\dagger(\hat{\rho}_2) \geq 0 \quad \forall\hat{\rho}_2\in S(\mathcal{H}_2), \quad (6.7)$$

where $\mathfrak{L}_{\hat{W}}^\dagger$ denotes the HILBERT-SCHMIDT adjoint of the linear mapping $\mathfrak{L}_{\hat{W}}$ that is characterized by (6.3), i.e.:

$$\text{trace}\left(\mathfrak{L}_{\hat{W}}^\dagger(\hat{A}_2)\hat{A}_1\right) = \text{trace}\left(\hat{A}_2\mathfrak{L}_{\hat{W}}(\hat{A}_1)\right) \quad \forall\hat{A}_1\in\mathcal{L}(\mathcal{H}_1),\hat{A}_2\in\mathcal{L}(\mathcal{H}_2).$$

———— DRAFT, June 26, 2009 ————

⁷Recall Footnote 6.

⁸Positivity of $\hat{A}\in\mathcal{L}(\mathcal{H})$ is easily to checked:

$$\hat{A} \geq 0 \iff \det(\hat{A} - x\hat{1}) = \underbrace{c}_{\in\mathbb{R}} \sum_{\nu=1}^{\dim(\mathcal{H})} (-1)^\nu \underbrace{c_\nu}_{\geq 0} x^\nu.$$

Outline of proof: (6.6) follows from

$$\begin{aligned} \frac{1}{n_1} \text{trace}(\hat{\rho} \hat{W}) &\stackrel{(6.1)}{=} \text{trace}\left(\hat{\rho}(\mathbf{1} \otimes \mathfrak{L}_{\hat{W}})(\hat{P}_{\mathcal{H}_1}^+)\right) \\ &= \text{trace}\left(\left(\mathbf{1} \otimes \mathfrak{L}_{\hat{W}}^\dagger\right)(\hat{\rho}) \hat{P}_{\mathcal{H}_1}^+\right) \end{aligned}$$

and (6.7) from (6.4). ■

We may conclude:

1. If \hat{W} is an entanglement witness for $\hat{\rho}$ then $(\mathbf{1} \otimes \mathfrak{L}_{\hat{W}}^\dagger)(\hat{\rho}) \not\geq 0$ and, therefore, the positive map $\mathfrak{L}_{\hat{W}}^\dagger$ cannot be completely positive.
2. For every **positive** mapping $\mathfrak{L}' : \mathcal{H}_2 \longrightarrow \mathcal{H}_1$ we have:⁹

$$(\mathbf{1} \otimes \mathfrak{L}')(\hat{\rho}) \not\geq 0 \implies \hat{\rho} \notin S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2).$$
3. A state $\hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is separable if and only if $(\mathbf{1} \otimes \mathfrak{L}')(\hat{\rho})$ is positive for **all** positive mappings $\mathfrak{L}' : \mathcal{H}_2 \longrightarrow \mathcal{H}_1$.

Remark: In general, for detecting entanglement, $\mathfrak{L}_{\hat{W}}^\dagger$ is more useful than \hat{W} since

$$\mathfrak{L}_{\hat{W}}^\dagger(\hat{\rho}) \not\geq 0 \stackrel{\text{i.g.}}{\not\iff} \text{trace}(\hat{W} \hat{\rho}) < 0.$$

\hat{W} , on the other hand, allows to detect entanglement by local measurements (Gühne et al., 2002).

6.1.2 Examples

Lemma 6.1.4 The **flip operator** of the bipartite system \mathcal{S} with state space $\mathcal{H} \otimes \mathcal{H}$, i.e. the linear Operator \hat{F} on $\mathcal{H} \otimes \mathcal{H}$ characterized by

$$\hat{F}(\psi_1 \otimes \psi_2) \stackrel{\text{def}}{=} \psi_2 \otimes \psi_1 \quad \forall \psi_1, \psi_2 \in \mathcal{H}, \quad (6.8)$$

has the following properties:¹⁰

1.

$$\hat{F} = \hat{F}^\dagger, \quad \hat{F}^2 = \hat{1}.$$

⁹Of course this statement is relevant for non-completely positive \mathfrak{L}' , only.

¹⁰Recall Definition A.4.4.

2.

$$\hat{F} = \hat{P}_+ - \hat{P}_-,$$

where the

$$\hat{P}_\pm \stackrel{\text{def}}{=} \frac{1}{2} (\hat{1} \pm \hat{F})$$

are the projectors onto the symmetric resp. anti-symmetric pure states of \mathcal{S} :

$$\Psi \in \hat{P}_\pm(\mathcal{H} \otimes \mathcal{H}) \iff \hat{F} \Psi = \pm \hat{\Psi} \quad \forall \Psi \in \mathcal{H} \otimes \mathcal{H}.$$

3. For all $\beta \in \mathbb{R}$:

$$\hat{1} + \beta \hat{F} \geq 0 \iff \beta \in [-1, +1].$$

4.

$$\text{trace}(\hat{F}) = -\dim(\mathcal{H}).$$

5. For all $\hat{\rho} \in S(\mathcal{H} \otimes \mathcal{H})$:

$$\hat{\rho} \text{ separable} \implies \text{trace}(\hat{F} \hat{\rho}) \geq 0.$$

Outline of proof: The first four statements are more or less obvious and the last one follows from

$$\begin{aligned} \text{trace}\left(\hat{F}\left(|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2|\right)\right) &= \text{trace}\left(\hat{F}|\psi_1 \otimes \psi_2\rangle\langle\psi_1 \otimes \psi_2|\right) \\ &= \text{trace}\left(|\psi_2 \otimes \psi_1\rangle\langle\psi_1 \otimes \psi_2|\right) \\ &= \langle\psi_1 \otimes \psi_2 | \psi_2 \otimes \psi_1\rangle \\ &= |\langle\psi_1 | \psi_2\rangle|^2. \quad \blacksquare \end{aligned}$$

Consequence: The flip operator \hat{F} is an entanglement witness for the mixed WERNER *states*¹¹ $\hat{\rho}_W(\beta)$ with $\beta \in [-1, -1/\dim(\mathcal{H})]$, where

$$\hat{\rho}_W(\beta) \stackrel{\text{def}}{=} \frac{\hat{1} + \beta \hat{F}}{\text{trace}(\hat{1} + \beta \hat{F})} \quad \forall \beta \in [-1, +1]. \quad (6.9)$$

¹¹Compare Footnote 27 of Chapter 4.

For $\mathcal{H}_1 = \mathcal{H}_2 = \mathcal{H}$ the positive linear mapping (6.3) associated with the flip operator on $\mathcal{H} \otimes \mathcal{H}$ is the transposition¹² w.r.t. $\{\phi_1, \dots, \phi_n\} = \{\phi_1^{(1)}, \dots, \phi_{n_1}^{(1)}\}$:

$$\begin{aligned} \mathfrak{L}_{\hat{F}}(|\phi_{\nu_1}\rangle\langle\phi_{\nu_2}|) &= T(|\phi_{\nu_1}\rangle\langle\phi_{\nu_2}|) \\ &\stackrel{\text{def}}{=} |\phi_{\nu_2}\rangle\langle\phi_{\nu_1}| \\ &= \mathfrak{L}'_{\hat{F}}(|\phi_{\nu_1}\rangle\langle\phi_{\nu_2}|) \quad \forall \nu_1, \nu_2 \in \{1, \dots, n\}. \end{aligned} \quad (6.10)$$

While the flip operator cannot be an entanglement witness for, e.g., the \hat{F} -invariant pure states,¹³ a two-qubit state $\hat{\rho}$ is separable iff its partial transpose $(\mathbf{1} \otimes \mathfrak{T})(\hat{\rho})$ is positive. Slightly more generally we have:

Theorem 6.1.5 For $j \in \{1, 2\}$, let $\{\phi_1^{(j)}, \dots, \phi_{n_j}^{(j)}\}$ be a MONS of the HILBERT space \mathcal{H}_j . If $n_1 + n_2 \in \{4, 5\}$ then an arbitrarily given state

$$\hat{\rho} = \sum_{\nu_1, \mu=1}^{n_1} \sum_{\nu_2, \mu_2=1}^{n_2} \rho_{\nu_1 \nu_2, \mu_1 \mu_2} |\phi_{\nu_1}^{(1)} \otimes \phi_{\nu_2}^{(2)}\rangle\langle\phi_{\mu_1}^{(1)} \otimes \phi_{\mu_2}^{(2)}| \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$$

is separable iff it has a **positive partial transpose**.¹⁴

$$\sum_{\nu_1, \mu=1}^{n_1} \sum_{\nu_2, \mu_2=1}^{n_2} \rho_{\nu_1 \nu_2, \mu_1 \mu_2} |\phi_{\nu_1}^{(1)} \otimes \phi_{\nu_2}^{(2)}\rangle\langle\phi_{\mu_1}^{(1)} \otimes \phi_{\mu_2}^{(2)}| \geq 0.$$

Proof:¹⁵ See (Horodecki et al., 1996, Theorem 3). ■

Another example for $\mathcal{H}_1 = \mathcal{H}_2 = \mathcal{H}$ and $\{\phi_1, \dots, \phi_n\} = \{\phi_1^{(1)}, \dots, \phi_{n_1}^{(1)}\} = \{\phi_1^{(2)}, \dots, \phi_{n_1}^{(2)}\}$ is

$$\begin{aligned} \hat{W} &= \hat{\mathbf{1}}_{\mathcal{H} \otimes \mathcal{H}} - n \hat{P}_{\mathcal{H}}^+ \\ &= \sum_{\nu, \mu=1}^n (|\phi_{\nu}\rangle\langle\phi_{\mu}|) \otimes (\delta_{\nu\mu} \hat{\mathbf{1}} - |\phi_{\nu}\rangle\langle\phi_{\mu}|) \\ &= m (\mathbf{1} \otimes \mathfrak{L}_{\mathcal{H}}^D) (\hat{P}_{\mathcal{H}}^+), \end{aligned}$$

———— DRAFT, June 26, 2009 ————

¹²The transposition was considered at the end of 4.2.1.

¹³See, however, (Horodecki and Horodecki, 1996).

¹⁴Positivity of the partial transpose, contrary to the partial transpose itself, does not depend on the choice for the MONS $\{\phi_1^{(2)}, \dots, \phi_{n_2}^{(2)}\}$.

¹⁵The essential point is that — provided $n_1 + n_2 \in \{4, 5\}$ — every positive mapping $\mathfrak{L}' : \mathcal{L}(\mathcal{H}_2) \rightarrow \mathcal{L}(\mathcal{H}_1)$ is decomposable; see (Labuschagne et al., 2003) and references given there. For entangled PPT states in higher dimensions see (Ha et al., 2003).

where

$$\mathfrak{L}_{\hat{W}}(\hat{B}) \stackrel{(6.1)}{=} \mathfrak{L}_{\mathcal{H}}^{\text{D}}(\hat{B}) \quad (6.11)$$

$$\stackrel{\text{def}}{=} \text{trace}(\hat{B}) - \hat{B} \quad \forall \hat{B} \in \mathcal{L}(\mathcal{H}), \quad (6.12)$$

Obviously, $\mathfrak{L}_{\mathcal{H}}^{\text{D}}$ is positive and

$$(\mathbf{1} \otimes \mathfrak{L}_{\mathcal{H}}^{\text{D}})(\hat{\rho}) = \text{trace}_2(\hat{\rho}) \otimes \hat{\mathbf{1}} - \hat{\rho} \quad \forall \hat{\rho} \in \mathcal{L}(\mathcal{H}).$$

Therefore,¹⁶

$$\text{trace}_2(\hat{\rho}) \otimes \hat{\mathbf{1}} \not\geq \hat{\rho} \implies \hat{\rho} \notin S_{\text{sep}}(\mathcal{H} \otimes \mathcal{H}). \quad (6.13)$$

6.1.3 Other Criteria¹⁷

Up to now, in view of Corollary 6.1.3, we considered the entanglement criterion

$$\boxed{(\mathbf{1} \otimes \underbrace{\mathfrak{L}}_{\geq 0})(\hat{\rho}) \not\geq 0 \implies \hat{\rho} \notin S_s(\mathcal{H}_1 \otimes \mathcal{H}_1)}. \quad (6.14)$$

only for positive maps $\mathfrak{L} : \mathcal{L}(\mathcal{H}_2) \longrightarrow \mathcal{L}(\mathcal{H}_1)$. But, of course, (6.14) also holds for positive maps $\mathfrak{L} : \mathcal{L}(\mathcal{H}_2) \longrightarrow \mathcal{L}(\mathcal{H}_2)$. Typical examples are

1. $\mathfrak{L} = \mathfrak{T}$:

Every separable state $\hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is PPT, i.e. has a positive partial transpose $(\mathbf{1} \otimes \mathfrak{T})(\hat{\rho})$ — for every choice of MONS.

2. $\mathfrak{L} = \mathfrak{L}_{\mathcal{H}}^{\text{D}}$:

$$\hat{\rho} \in S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2) \implies \text{trace}_2(\hat{\rho}) \otimes \hat{\mathbf{1}} \geq \hat{\rho}. \quad (6.15)$$

Remarks:

1. Since¹⁸

$$\left((\mathbf{1} \otimes \mathfrak{T})(\hat{\rho}) \right)^\dagger = (\mathbf{1} \otimes \mathfrak{T})(\hat{\rho}) \quad \forall \hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$$

and

$$\text{trace} \left((\mathbf{1} \otimes \mathfrak{T})(\hat{\rho}) \right) = 1 \quad \forall \hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2),$$

———— DRAFT, June 26, 2009 ————

¹⁶See (Hiroshima, 2003) in this connection.

¹⁷See also (Doherty et al., 2003)

¹⁸Note that

$$(\mathbf{1} \otimes \mathfrak{T})(\hat{A}^\dagger) = \left((\mathbf{1} \otimes \mathfrak{T})(\hat{A}) \right)^\dagger \quad \forall \hat{A} \in \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2).$$

we have¹⁹

$$\boxed{(\mathbf{1} \otimes \mathfrak{T})(\hat{\rho}) \not\geq 0 \iff \|(\mathbf{1} \otimes \mathfrak{T})(\hat{\rho})\|_1 > 1 \quad \forall \hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2),}$$

as exploited in (Vidal and Werner, 2002).

2. Since²⁰

$$T(\hat{\tau}^\nu) = (-1)^{\delta_{\nu 2}} \hat{\tau}^\nu \quad \forall \nu \in \{0, \dots, 3\},$$

we have for two-qubit states $\hat{\rho}$:²¹

$$\boxed{(\mathbf{1} \otimes \mathfrak{T})(\hat{\rho}) = \hat{\rho} \iff \text{trace} \left((\hat{\tau}^\mu \otimes \hat{\tau}^2) \hat{\rho} \right) = 0 \quad \forall \mu \in \{0, \dots, 3\} .}$$

3. For all $\hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$:

$$\boxed{\begin{aligned} & (\mathbf{1} \otimes \mathfrak{T})(\hat{\rho}) \Psi = \underbrace{\lambda}_{<0} \Psi \neq 0 \\ \implies & \begin{cases} (\mathbf{1} \otimes \mathfrak{T})(|\Psi\rangle\langle\Psi|) \text{ entanglement witness for } \hat{\rho}, \\ \Psi \text{ non-separable.} \end{cases} \end{aligned}}$$

Let us list some other sufficient criteria for entanglement:

1. **Range criterion.**²²

$$\boxed{\begin{aligned} & \psi^{(1)} \otimes (\psi^{(2)})^* \notin \text{range} \left((\mathbf{1} \otimes \mathfrak{T})(\hat{\rho}) \right) \quad \forall \psi^{(1)} \otimes \psi^{(2)} \in \text{range}(\hat{\rho}) \\ \implies & \hat{\rho} \notin S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2), \end{aligned}} \quad (6.16)$$

where

$$(\psi^{(2)})^* \stackrel{(4.9)}{=} \sum_{\nu=1}^{n_2} \langle \psi^{(2)} | \phi_\nu^{(2)} \rangle \phi_\nu^{(2)}$$

depends on the MONS $\{\phi_1^{(2)}, \dots, \phi_{n_2}^{(2)}\}$ of \mathcal{H}_2 .

Outline of proof: By Theorem A.4.5 (and the spectral theorem), every $\hat{\rho} \in S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ can be written in the form

$$\hat{\rho} = \sum_{k=1}^N \left| \psi_k^{(1)} \otimes \psi_k^{(2)} \right\rangle \left\langle \psi_k^{(1)} \otimes \psi_k^{(2)} \right|.$$

———— DRAFT, June 26, 2009 ————

¹⁹Recall (5.31).

²⁰Recall (A.22)

²¹Compare (Altafini, 2003, Sect. II.B., Corollary 1).

²²This criterion especially implies that every state $\hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$ containing no product state in its range must be entangled. For a non-separable PPT state on $\mathbb{C}^2 \otimes \mathbb{C}^4$ containing product states in its range and fulfilling the range criterion see (Horodecki et al., 2001, Eqn. (27)).

Then Lemma A.4.2 implies

$$\psi_k^{(1)} \otimes \psi_k^{(2)} \in \text{range}(\hat{\rho}) \quad \forall k \in \{1, \dots, N\}$$

and, since²³

$$(\mathbf{1} \otimes \mathfrak{F})(\hat{\rho}) = \sum_{k=1}^N \left| \psi_k^{(1)} \otimes (\psi_k^{(2)})^* \right\rangle \left\langle \psi_k^{(1)} \otimes (\psi_k^{(2)})^* \right|,$$

also

$$\psi_k^{(1)} \otimes (\psi_k^{(2)})^* \in \text{range}\left((\mathbf{1} \otimes \mathfrak{F})(\hat{\rho})\right) \quad \forall k \in \{1, \dots, N\}. \quad \blacksquare$$

2. Entropic inequalities:²⁴

$$\boxed{\left. \begin{array}{l} \hat{\rho} \in S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2) \\ \alpha \in \{0, 1, 2, \infty\} \end{array} \right\} \implies S_\alpha(\text{trace}_j(\hat{\rho})) \leq S_\alpha(\hat{\rho}) \quad \forall j \in \{1, 2\},} \quad (6.17)$$

(more information for the total state than for the partial states), where²⁵

$$S_\alpha(\hat{\rho}) \stackrel{\text{def}}{=} \frac{\log_2(\text{trace}(\hat{\rho}^\alpha))}{1 - \alpha} \quad \forall \alpha \in (0, 1) \cup (1, \infty) \quad (6.18)$$

and²⁶

$$S_k(\hat{\rho}) \stackrel{\text{def}}{=} \lim_{\alpha \rightarrow k} S_\alpha(\hat{\rho}) \quad \forall k \in \{0, \infty\}.$$

3. Greatest cross norm criterion (Rudolph, 2000, Thm. 5):

$$\boxed{\hat{\rho} \in S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2) \iff \|\hat{\rho}\|_\gamma = 1,} \quad (6.19)$$

where

$$\|\hat{A}\|_\gamma \stackrel{\text{def}}{=} \inf \left\{ \sum_{k=1}^N \|\hat{A}_k^{(1)}\|_1 \|\hat{A}_k^{(2)}\|_1 : \sum_{k=1}^N \underbrace{\hat{A}_k^{(1)}}_{\in \mathcal{L}(\mathcal{H}_1)} \otimes \underbrace{\hat{A}_k^{(2)}}_{\in \mathcal{L}(\mathcal{H}_2)} = \hat{A}, N \in \mathbb{N} \right\} \quad (6.20)$$

for $\hat{A} \in \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$.

———— DRAFT, June 26, 2009 ————

²³Recall (4.14).

²⁴See (Vollbrecht and Wolf, 2002, Sect. III) and references given there.

²⁵The normalization factor $1/1 - \alpha$ guarantees

$$\max_{\hat{\rho} \in S(\mathcal{H})} S_\alpha(\hat{\rho}) = \log_2(\dim(\mathcal{H}))$$

for the so-called RENYI *quantum entropies* S_α ; see also (Lavenda and Dunning-Davies, 2003).

²⁶Note also that

$$S_1(\hat{\rho}) = \lim_{1 < \alpha \rightarrow 1} S_\alpha(\hat{\rho}).$$

4. **Computable cross norm criterion**²⁷ (Rudolph, 2002, Prop. 19):

$$\hat{\rho} \in S_{\text{sep}}(\mathcal{H} \otimes \mathcal{H}) \implies \|\mathfrak{A}(\hat{\rho})\| \leq 1, \quad (6.21)$$

where the linear mapping $\mathfrak{A} : \mathcal{L}(\mathcal{H} \otimes \mathcal{H}) \longrightarrow \mathcal{L}(\mathcal{L}(\mathcal{H}))$ is characterized by

$$\begin{aligned} & \mathfrak{A}\left(|\phi_{\nu_1} \otimes \phi_{\nu_2}\rangle\langle\phi_{\mu_1} \otimes \phi_{\mu_2}| \right) \hat{A} \\ & \stackrel{\text{def}}{=} \left\langle \phi_{\nu_2} \left| \hat{A} \phi_{\mu_2} \right\rangle |\phi_{\nu_1}\rangle\langle\phi_{\mu_1}| \quad \forall \nu_1, \nu_2, \mu_1, \mu_2 \in \{1, \dots, n\}, \hat{A} \in \mathcal{L}(\mathcal{H}) \end{aligned} \quad (6.22)$$

w.r.t. the *fundamental* MONS $\{\phi_1, \dots, \phi_n\}$ of \mathcal{H} .

5. **Reduction criterion**²⁸ (Horodecki and Horodecki, 1999):

$$\hat{\rho} \in S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2) \iff \begin{cases} \text{trace}_2(\hat{\rho}) \otimes \hat{1} - \hat{\rho} \geq 0, \\ \hat{1} \otimes \text{trace}_1(\hat{\rho}) - \hat{\rho} \geq 0. \end{cases} \quad (6.23)$$

6.2 Local Operations and Classical Communication (LOCC)

6.2.1 General Aspects

By *local operations and classical communication* (LOCC) state transformations of the form²⁹

$$\hat{\rho} \longmapsto \hat{\rho}' = \mathfrak{L}_{\text{LOCC}}(\hat{\rho}) = \sum_{k=1}^N p_k \left(\mathfrak{C}_k^{(1)} \otimes \mathfrak{C}_k^{(2)} \right) (\hat{\rho}) \quad (6.24)$$

can be implemented on a bipartite system with state space $\mathcal{H}_1 \otimes \mathcal{H}_2$, where

$$N \in \mathbb{N} \quad \sum_{j=1}^N \underbrace{p_k}_{>0} = 1$$

and the $\mathfrak{C}_k^{(1)}$ resp. $\mathfrak{C}_k^{(2)}$ are trace preserving elements of $\mathcal{Q}(\mathcal{H}_1, \mathcal{H}_1)$ resp. $\mathcal{Q}(\mathcal{H}_2, \mathcal{H}_2)$. Obviously,

$$\left. \begin{array}{l} \psi^{(1)} \in \mathcal{H}_1, \psi^{(2)} \in \mathcal{H}_2 \\ \|\psi^{(1)}\| = \|\psi^{(2)}\| = 1 \end{array} \right\} \implies S_{\text{LOCC}}(\psi^{(1)} \otimes \psi^{(2)}) = S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2), \quad (6.25)$$

DRAFT, June 26, 2009

²⁷Note that for $\dim(H) \geq \dim(H_1), \dim(H_2)$ there is a canonical mapping of $S(\mathcal{H}_1 \otimes \mathcal{H}_2)$ into $S(\mathcal{H} \otimes \mathcal{H})$ respecting separability. Therefore, it is sufficient to consider the case $\mathcal{H}_1 = \mathcal{H}_2$.

²⁸See (Hiroshima, 2003), in this connection.

²⁹Obviously, the LOCC quantum operations (6.24) form a group.

where

$$S_{\text{LOCC}}(\hat{\rho}) \stackrel{\text{def}}{=} \{\text{states } \hat{\rho}' \text{ of the form (6.24)}\} .$$

In order to characterize the possible transformations of pure states by LOCC we need the following definition:

Definition 6.2.1 *Let \hat{H}, \hat{H}' be Hermitian operators on the HILBERT space \mathcal{H} with spectral decompositions*

$$\hat{H} = \sum_{\nu=1}^n E_{\nu} |\psi_{\nu}\rangle\langle\psi_{\nu}| , \quad \hat{H}' = \sum_{\nu=1}^n E'_{\nu} |\psi'_{\nu}\rangle\langle\psi'_{\nu}| .$$

Then we write $\hat{H} \preceq \hat{H}'$ iff³⁰ there $p_1, \dots, p_n \geq 0$ and permutations $\pi_1, \dots, \pi_n \in S_n$ with

$$E_{\mu} = \sum_{\nu=1}^n p_{\nu} E'_{\pi_{\nu}(\mu)} \quad \forall \mu \in \{1, \dots, n\} , \quad \sum_{\nu=1}^n p_{\nu} = 1 .$$

Theorem 6.2.2 *Let \hat{H}, \hat{H}' be Hermitian operators on the HILBERT space \mathcal{H} . Then $\hat{H} \preceq \hat{H}'$ iff there are $p_1, \dots, p_n \geq 0$ and unitary Operators $\hat{U}_1, \dots, \hat{U}_n$ on \mathcal{H} with*

$$\hat{H} = \sum_{\nu=1}^n p_{\nu} \hat{U}_{\nu} \hat{H}' \hat{U}_{\nu}^{\dagger} , \quad \sum_{\nu=1}^n p_{\nu} = 1 .$$

Proof: See (Nielsen and Chuang, 2001, Theorem 12.13). ■

For pure states and $\mathcal{H}_1 = \mathcal{H}_2$, concerning LOCC, nothing is lost if the operations on one side are restricted to be unitary:

Lemma 6.2.3 *Let \mathcal{H} be a HILBERT space, $0 \neq \Psi \in \mathcal{H} \otimes \mathcal{H}$ and $\hat{M} \in \mathcal{L}(\mathcal{H})$. Then there are $\hat{N}, \hat{U} \in \mathcal{L}(\mathcal{H})$ with*

$$\left(\hat{1} \otimes \hat{M}\right) \Psi = \left(\hat{N} \otimes \hat{U}\right) \Psi , \quad \hat{U}^{\dagger} = \hat{U}^{-1} .$$

Outline of proof: According to Theorem A.4.7 there are non-negative numbers s_1, \dots, s_n and orthonormal bases $\{\phi_1^{(1)}, \dots, \phi_n^{(1)}\}$ and $\{\phi_1^{(2)}, \dots, \phi_n^{(2)}\}$ of \mathcal{H} with

$$\Psi = \sum_{\alpha=1}^n s_{\alpha} \phi_{\alpha}^{(1)} \otimes \phi_{\alpha}^{(2)} , \quad n \stackrel{\text{def}}{=} \dim(\mathcal{H}) .$$

³⁰Obviously, \preceq does not depend on the choice of orthonormal eigenbases for \hat{H}, \hat{H}' and gives a semi-ordering of $S(\mathcal{H})$.

Then, writing

$$\hat{M} = \sum_{\nu, \mu=1}^n M_{\nu\mu} \left| \phi_{\nu}^{(2)} \right\rangle \left\langle \phi_{\mu}^{(2)} \right|$$

and defining

$$\hat{N}' \stackrel{\text{def}}{=} \sum_{\nu, \mu=1}^n M_{\nu\mu} \left| \phi_{\nu}^{(1)} \right\rangle \left\langle \phi_{\mu}^{(1)} \right|$$

we get

$$\hat{S} \left(\hat{N}' \otimes \hat{1} \right) \Psi = \left(\hat{1} \otimes \hat{M} \right) \Psi,$$

where \hat{S} denotes the linear swap operator characterized by

$$\hat{S} \phi \otimes \psi \stackrel{\text{def}}{=} \psi \otimes \phi \quad \forall \phi, \psi \in \mathcal{H}.$$

Therefore $\left(\hat{N}' \otimes \hat{1} \right) \Psi$ and $\left(\hat{1} \otimes \hat{M} \right) \Psi$ have the same SCHMIDT coefficients, i.e. there are unitary $\hat{U}, \hat{V} \in \mathcal{L}(\mathcal{H})$ with

$$\left(\hat{1} \otimes \hat{M} \right) \Psi = \left(\hat{V} \otimes \hat{U} \right) \left(\hat{N}' \otimes \hat{1} \right) \Psi.$$

Defining $\hat{N} \stackrel{\text{def}}{=} \hat{V} \hat{N}'$ we get the statement of the lemma. \blacksquare

The state $\mathfrak{L}_{\text{LOCC}}(\hat{\rho})$ in (6.24) can be pure only if it coincides with $\left(\mathfrak{e}_k^{(1)} \otimes \mathfrak{e}_k^{(2)} \right) (\hat{\rho})$ for all $k \in \{1, \dots, N\}$ with $p_k \neq 0$. This, together with Theorem 6.2.2 allows us to prove the following:

Theorem 6.2.4 *Let \mathcal{H} be a HILBERT space. Then*

$$\hat{\rho}' \in S_{\text{LOCC}}(\hat{\rho}) \iff \text{trace}_2(\hat{\rho}) \preceq \text{trace}_2(\hat{\rho}') \quad \forall \hat{\rho}, \hat{\rho}' \in S_{\text{pure}}(\mathcal{H} \otimes \mathcal{H}).$$

Outline of proof: Assume that (6.24) holds. Then, by Lemma 6.2.3, $\mathfrak{L}_{\text{LOCC}}$ can be chosen such that

$$\hat{\rho}' = \sum_{j=1}^{N'} \underbrace{\left(\hat{M}_j \otimes \hat{U}_j \right) \hat{\rho} \left(\hat{M}_j^\dagger \otimes \hat{U}_j^\dagger \right)}_{\propto \hat{\rho}'}$$

holds with $N' \in \mathbb{N}$ and $\hat{M}_j, \hat{U}_j \in \mathcal{L}(\mathcal{H})$ fulfilling

$$\sum_{j=1}^{N'} \hat{M}_j^\dagger \hat{M}_j = \hat{1}, \quad \hat{U}_j = \hat{U}_j^\dagger \quad \forall j \in \{1, \dots, N'\}. \quad (6.26)$$

This implies

$$\hat{M}_j \text{trace}_2(\hat{\rho}) \hat{M}_j^\dagger = p'_j \text{trace}_2(\hat{\rho}') \quad \forall j \in \{1, \dots, N'\}, \quad (6.27)$$

where

$$p'_j \stackrel{\text{def}}{=} \text{trace} \left(\hat{M}_j \text{trace}_2(\hat{\rho}) \hat{M}_j^\dagger \right) \quad \forall j \in \{1, \dots, N'\}. \quad (6.28)$$

Using the polar decomposition

$$\begin{aligned}
\sqrt{\text{trace}_2(\hat{\rho})} \hat{M}_j^\dagger &= \hat{U}_j \sqrt{\left(\sqrt{\text{trace}_2(\hat{\rho})} \hat{M}_j^\dagger \right)^\dagger \sqrt{\text{trace}_2(\hat{\rho})} \hat{M}_j^\dagger} \\
&= \hat{U}_j \sqrt{\hat{M}_j \text{trace}_2(\hat{\rho}) \hat{M}_j^\dagger} \\
&\stackrel{(6.27)}{=} \hat{U}_j \sqrt{p'_j \text{trace}_2(\hat{\rho}')}
\end{aligned}$$

and multiplying from the right with its adjoint gives

$$\sqrt{\text{trace}_2(\hat{\rho})} \hat{M}_j^\dagger \hat{M}_j \sqrt{\text{trace}_2(\hat{\rho})} = p'_j \hat{U}_j \text{trace}_2(\hat{\rho}') \hat{U}_j^\dagger \quad \forall j \in \{1, \dots, N'\}.$$

Finally, summing over j gives

$$\text{trace}_2(\hat{\rho}) \stackrel{(6.26)}{=} \sum_{j=1}^{N'} p'_j \hat{U}_j \text{trace}_2(\hat{\rho}') \hat{U}_j^\dagger \quad (6.29)$$

and hence $\text{trace}_2(\hat{\rho}) \preceq \text{trace}_2(\hat{\rho}')$, by Theorem 6.2.2, since (6.26) and (6.28) imply

$$\sum_{j=1}^{N'} \underbrace{p'_j}_{\geq 0} = 1. \quad (6.30)$$

Conversely, if $\hat{\rho}_1 \preceq \hat{\rho}'_1$, where

$$\hat{\rho}_1 \stackrel{\text{def}}{=} \text{trace}_2(\hat{\rho}_1), \quad \hat{\rho}'_1 \stackrel{\text{def}}{=} \text{trace}_2(\hat{\rho}'_1),$$

then Theorem 6.2.2 implies (6.29) for suitable unitary $\hat{U}_1, \dots, \hat{U}_{N'} \in \mathcal{L}(\mathcal{H})$ and $p'_1, \dots, p'_{N'} > 0$ fulfilling (6.30). Then, if we define

$$\hat{M}_j \stackrel{\text{def}}{=} \sqrt{p'_j \hat{\rho}'_1} \hat{U}_j^\dagger \sqrt{(\hat{\rho}_1 \wedge \hat{\rho} \mathcal{H})^{-1}} \hat{P}_{\hat{\rho} \mathcal{H}} + \frac{\hat{1} - \hat{P}_{\hat{\rho} \mathcal{H}}}{\sqrt{p'_j}} \quad \forall j \in \{1, \dots, N'\}$$

(6.29) and (6.30) imply

$$\sum_{j=1}^{N'} \hat{M}_j^\dagger \hat{M}_j = \hat{1} \quad (6.31)$$

and

$$\text{trace}_2\left(\left(\hat{M}_j \otimes \hat{1}\right) \hat{\rho} \left(\hat{M}_j^\dagger \otimes \hat{1}\right)\right) = p'_j \text{trace}_2(\hat{\rho}') \quad \forall j \in \{1, \dots, N'\}, \quad (6.32)$$

Since

$$\left. \begin{array}{l} \text{trace}_2(\hat{\rho}'') = \text{trace}_2(\hat{\rho}') \\ \hat{\rho}', \hat{\rho}'' \in S_{\text{pure}}(\mathcal{H} \otimes \mathcal{H}) \end{array} \right\} \stackrel{\text{Theorem A.4.7}}{\implies} \left\{ \begin{array}{l} (\hat{1} \otimes \hat{U}) \hat{\rho}'' (\hat{1} \otimes \hat{U}^\dagger) = \hat{\rho}' \\ \text{for some unitary } \hat{U} \in \mathcal{L}(\mathcal{H}), \end{array} \right.$$

(6.32) shows that there are unitary $\hat{V}_1, \dots, \hat{V}_{N'} \in \mathcal{L}(\mathcal{H})$ with

$$\left(\hat{M}_j \otimes \hat{V}_j\right) \hat{\rho} \left(\hat{M}_j^\dagger \otimes \hat{V}_j^\dagger\right) = p'_j \hat{\rho}' \quad \forall j \in \{1, \dots, N'\}.$$

This, together with (6.30) and (6.31), shows that $\hat{\rho}$ can be transformed into $\hat{\rho}'$ by LOCC. \blacksquare

Lemma 6.2.5 *Let \hat{H}, \hat{H}' be Hermitian operators on the HILBERT space \mathcal{H} with spectral decompositions*

$$\hat{H} = \sum_{\nu=1}^n E_{\nu} |\psi_{\nu}\rangle\langle\psi_{\nu}|, \quad \hat{H}' = \sum_{\nu=1}^n E'_{\nu} |\psi'_{\nu}\rangle\langle\psi'_{\nu}|.$$

Then $\hat{H} \preceq \hat{H}'$ iff the conditions

$$\sum_{\nu=1}^n E_{\nu} = \sum_{\nu=1}^n E'_{\nu} \tag{6.33}$$

and

$$\max_{\pi \in S_n} \sum_{\nu=1}^{n'} E_{\pi(\nu)} \leq \max_{\pi \in S_n} \sum_{\nu=1}^{n'} E'_{\pi(\nu)} \quad \forall n' \in \{1, \dots, n-1\} \tag{6.34}$$

are fulfilled.

Proof: See (Nielsen and Chuang, 2001, Proposition 12.11). ■

Remarks:

1. Obviously,

$$\frac{1}{\dim \mathcal{H}} \hat{1} \preceq \hat{\rho}_1 \quad \forall \hat{\rho}_1 \in S(\mathcal{H}).$$

2. According to Theorem 6.2.4, therefore,³¹

$$S_{\text{pure}}(\mathcal{H} \otimes \mathcal{H}) \subset S_{\text{LOCC}}(\hat{P}_{\mathcal{H}}^+).$$

3. For qubit states $\hat{\rho}, \hat{\rho}'$ we always have either $\hat{\rho} \preceq \hat{\rho}'$ or $\hat{\rho}' \preceq \hat{\rho}$ or both.
4. However, for higher dimensional \mathcal{H} neither $\hat{\rho} \preceq \hat{\rho}'$ nor $\hat{\rho}' \preceq \hat{\rho}$ need be true for $\hat{\rho}, \hat{\rho}' \in S(\mathcal{H})$ as application of Lemma 6.2.5 to, e.g., the case

$$\hat{\rho} = \frac{1}{15} (7\phi_1 + 7\phi_2 + \phi_3), \quad \hat{\rho}' = \frac{1}{15} (11\phi_1 + 2\phi_2 + 2\phi_3)$$

shows if $\{\phi_1, \phi_2, \phi_3\}$ is a MONS of \mathcal{H} .

Note that LOCC would be much more powerful if intermediate use of nonlocally entangled ancillary pairs, restoring their original states, could be made:

³¹Recall (6.2).

For $j = 1$ resp. $j = 2$ let $\{\phi_1^{(j)}, \dots, \phi_{n_j}^{(j)}\}$ be a MONS of the HILBERT space \mathcal{H}_j , let

$$\Psi = \sum_{\nu, \mu=1}^{n_1} \lambda_{\nu\mu} \phi_\nu^{(1)} \otimes \phi_\mu^{(1)}, \quad \Psi' = \sum_{\nu, \mu_1}^{n_1} \lambda'_{\nu\mu} \phi_\nu^{(1)} \otimes \phi_{\mu_1}^{(1)}$$

be pure states of the bipartite system with state space $\mathcal{H}_1 \otimes \mathcal{H}_1$ and let

$$\begin{aligned} \Phi &= \sum_{\nu_1}^{n_1} \sum_{\alpha, \beta=1}^{n_2} \lambda_{\nu\mu} \lambda_{\alpha\beta}^{\text{anc}} (\phi_\nu^{(1)} \otimes \phi_\alpha^{(2)}) \otimes (\phi_\mu^{(1)} \otimes \phi_\beta^{(2)}), \\ \Phi' &= \sum_{\nu_1}^{n_1} \sum_{\alpha, \beta=1}^{n_2} \lambda'_{\nu\mu} \lambda_{\alpha\beta}^{\text{anc}} (\phi_\nu^{(1)} \otimes \phi_\alpha^{(2)}) \otimes (\phi_\mu^{(1)} \otimes \phi_\beta^{(2)}) \end{aligned}$$

be pure states of the bipartite system with state space $(\mathcal{H}_1 \otimes \mathcal{H}_2) \otimes (\mathcal{H}_1 \otimes \mathcal{H}_2)$. Then it may happen that³²

$$|\Psi\rangle \not\preceq |\Psi'\rangle \quad \text{but} \quad |\Phi\rangle \preceq |\Phi'\rangle$$

— an effect of the ancillary system in the state $\sum_{\alpha, \beta=1}^{n_2} \lambda_{\alpha\beta}^{\text{anc}} \phi_\alpha^{(2)} \otimes \phi_\beta^{(2)}$ that is called *entanglement catalysis*.

Finally, given $\hat{\rho}, \hat{\rho}' \in S_{\text{pure}}(\mathcal{H} \otimes \mathcal{H})$, let us note that $\hat{\rho}$ can be transformed into $\hat{\rho}'$ by local operations without communication iff

$$\text{trace}_2(\hat{\rho}') \propto \hat{K} \text{trace}_2(\hat{\rho}) \hat{K}^\dagger, \quad \hat{K}^\dagger \hat{K} \leq \hat{1} \quad (6.35)$$

holds for some $\hat{K} \in \mathcal{L}(\mathcal{H})$. Let

$$\text{trace}_2(\hat{\rho}) = \sum_{\nu=1}^n p_\nu |\psi_\nu\rangle\langle\psi_\nu|, \quad \text{trace}_2(\hat{\rho}') = \sum_{\nu=1}^n p'_\nu |\psi'_\nu\rangle\langle\psi'_\nu|$$

be spectral decompositions of $\hat{\rho}, \hat{\rho}'$. Then, exploiting unitary transformations and the polar decomposition of \hat{K} one can show that (6.35) is equivalent to existence of real numbers k_1, \dots, k_n and a permutation $\pi \in S_n$ with:

$$\sum_{\nu=1}^n (k_\nu)^2 \leq 1, \quad p'_\nu = (k_\nu)^2 p_{\pi(\nu)} \quad \forall \nu \in \{1, \dots, n\}.$$

DRAFT, June 26, 2009

³²See (Nielsen and Chuang, 2001, Exercise 12.21) for an explicit example with $(n_1, n_2) = (4, 2)$.

6.2.2 Entanglement Dilution

⋮

6.2.3 Entanglement Distillation

See, e.g., (Bowmeester et al., 2000, Section 8.4) and (Devetak and Winter, 2005).

6.3 Quantification of Entanglement³³

For pure states $|\Psi\rangle\langle\Psi|$ of a bipartite system \mathcal{S} with state space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ there is a generally accepted measure of entanglement, namely the *entropy of entanglement*³⁴

$$\begin{aligned} E_{\text{pure}}(|\Psi\rangle\langle\Psi|) &\stackrel{\text{def}}{=} S_1\left(\text{trace}_2(|\Psi\rangle\langle\Psi|)\right) \\ &\stackrel{\text{Th. A.4.7}}{=} S_1\left(\text{trace}_1(|\Psi\rangle\langle\Psi|)\right), \end{aligned} \quad (6.36)$$

i.e. the VON NEUMANN entropy of the partial states. Since

$$E_{\text{pure}}\left(\sum_{\nu=1}^{n'} \sqrt{p_\nu} \phi_\nu^{(1)} \otimes \phi_\nu^{(2)}\right) = - \sum_{\nu=1}^{n'} \underbrace{p_\nu}_{>0} \log_2(p_\nu)$$

holds for SCHMIDT decompositions, $E_{\text{pure}}(|\Psi\rangle\langle\Psi|)$ becomes maximal³⁵ for

$$n' = \min\left\{\dim(\mathcal{H}_1), \dim(\mathcal{H}_2)\right\}, \quad p_\nu = \frac{1}{n'} \quad \forall \nu \in \{1, \dots, n'\}.$$

Hence

$$\max_{\substack{\Psi \in \mathcal{H}_1 \otimes \mathcal{H}_2 \\ \|\Psi\|=1}} E(|\Psi\rangle\langle\Psi|) = \log_2\left(\min\left\{\dim(\mathcal{H}_1), \dim(\mathcal{H}_2)\right\}\right) \quad (6.37)$$

holds for $E = E_{\text{pure}}$.

Strict requirements for every entanglement measure E on $S(\mathcal{H}_1 \otimes \mathcal{H}_2)$:

1.

$$E(\hat{\rho}) \geq 0 \quad \forall \hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2).$$

———— DRAFT, June 26, 2009 ————

³³See also (Řeháček and Hradil, 2002).

³⁴The unit of entanglement is one *ebit*.

³⁵Recall Remark 3 in the beginning of Section 5.1.

2.

$$E(\hat{\rho}) = 0 \quad \forall \hat{\rho} \in S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2).$$

3.

$$E(\hat{\rho}) = 0 \implies \hat{\rho} \in S_{\text{sep}}(\mathcal{H}_1 \otimes \mathcal{H}_2) \quad \forall \hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$$

(could be relaxed by consideration of additional entanglement measures).

4.

$$\hat{\rho}' \in S_{\text{LOCC}}(\hat{\rho}) \implies E(\hat{\rho}') \leq E(\hat{\rho}) \quad \forall \hat{\rho}, \hat{\rho}' \in S(\mathcal{H}_1 \otimes \mathcal{H}_2).$$

5. For all pure states $|\Psi_1\rangle\langle\Psi_1|, |\Psi_2\rangle\langle\Psi_2| \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$:

$$E_{\text{pure}}(|\Psi_1\rangle\langle\Psi_1|) < E_{\text{pure}}(|\Psi_2\rangle\langle\Psi_2|) \implies E(|\Psi_1\rangle\langle\Psi_1|) < E(|\Psi_2\rangle\langle\Psi_2|).$$

Desirable for entanglement measures E on $S(\mathcal{H}_1 \otimes \mathcal{H}_2)$:

1.

$$E(\hat{\rho}) \geq E(\hat{\rho}') \implies \hat{\rho}' \in S_{\text{LOCC}}(\hat{\rho}) \quad \forall \hat{\rho}, \hat{\rho}' \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$$

(not possible).

2. **Continuity**3. **Additivity**4. **Subadditivity**5. **Convexity**Standard entanglement measures:³⁶1. **Entanglement of formation**³⁷ is the convex continuation

$$E_{\text{F}}(\hat{\rho}) \stackrel{\text{def}}{=} \inf_{\hat{\rho} = \sum_{\nu} \underbrace{p_{\nu}}_0 \underbrace{\hat{\rho}_{\nu}}_{\text{pure}}} \sum_{\nu} p_{\nu} S_1(\text{trace}_2(\hat{\rho}_{\nu}))$$

of the entropy of entanglement (6.36) to all of $S(\mathcal{H}_1 \otimes \mathcal{H}_2)$.

Additivity of the entanglement of formation is generally conjectured but not yet proved.

2.

DRAFT, June 26, 2009

³⁶There cannot be a unique entanglement measure (Morikoshi et al., 2003).³⁷For pairs of qubits the entanglement of formation coincides with the **concurrence** (Wootters, 2001, Section 3.1).

Squashed Entanglement (Christandl and Winter, 2004)

- In general, WERNER states are not maximally entangled, i.e. their entanglement of formation (tangle) is not maximal for given a fixed degree of mixedness (linear entropy) (White et al., 2001).
 - Compare with (Eckert et al., 2002). (see also quant-ph/0210107)
 - What about local superselection rules? (Verstraete and Cirac, 2003; Bartlett and Wiseman, 2003)
 - Exploit the notion of truncated expectation values. (Lee et al., 2003)
 - What is the generalization of the latter for mixed states?
 - Existiert ein Abstandsmaß a la (Lee et al., 2003)?
 - Warum verwendet man nicht den HILBERT-SCHMIDT-Abstand von Zuständen, der sich leicht mithilfe von Erwartungswerten von (Produkten von) PAULI-Operatoren ausdrücken läßt?
 - Besteht ein Zusammenhang mit (Lee et al., 2003)? Der Abstand zur Menge der separablen Zustände sollte doch ein Maß für Verschränktheit sein...

Remarks:

1. For $(\dim(\mathcal{H}_1), \dim(\mathcal{H}_2))$ either (2,2) or (3,2) PPT w.r.t. the second factor is necessary and sufficient for separability (Horodecki et al., 1996).
2. Otherwise states with ***bound entanglement***, i.e. entangled PPT states, exist (Horodecki et al., 1996, Appendix).
3. In the 2-qubit case every entangled mixed state can be represented as a convex combination of a separable (in general mixed) state with a pure entangled state (Lewenstein and Sanpera, 1998). The representation with minimal norm of the pure state is unique.
4. Also this shows that, for the 2-qubit case, separability is equivalent to PPT.

Appendix A

A.1 TURING'S Halting Problem

The *halting problem* is the following:

There is no algorithm by which one may decide for every program and every finite input to the program whether the program will halt or loop forever.

The proof given by TURING is essentially as follows:

Since every program may be encoded into a finite sequence (b_1, \dots, b_n) of bits the programs may be indexed by the corresponding numbers $\sum_{\nu=1}^n b_\nu 2^{n-\nu}$. The same holds for all finite inputs. Now assume that there is an algorithm telling us for all $(j, k) \in \mathbb{Z}_+^2$ whether program j will halt on input k . Then this algorithm may be used to write a program P with the following property:

For every $j \in \mathbb{Z}_+$, program P will hold on input j iff program j will not.

Obviously, program P is different from program j for every $j \in \mathbb{Z}_+$ — a contradiction.

A heuristic explanation is the following:

There are uncountably many possibilities for infinite loops which, therefore, cannot be checked in a systematic way. But we cannot be sure whether a given program will halt on a given input or not unless

- an infinite loop is found by chance or
- the program was actually tested on the input and found to halt.

Let us finally note that the halting problem is a solution to HILBERT'S 23rd problem (see <http://aleph0.clarku.edu/~djoyce/hilbert/>).

A.2 Some Remarks on Quantum Teleportation

Even though quantum teleportation, described in 1.2.2, seems to indicate some kind of quantum nonlocality, there is a naive ‘explanation’ relying on locality and some kind of realism:

There is a set of four compatible relations, corresponding to the BELL states, between a pair of qubits. These correlations are so strong that the state (predicting ensemble averages) of the second qubit is fixed by that of the first qubit and the BELL relation (considered as an *element of reality*). Therefore, Alice need only inform Bob about the BELL relation of qubit 1 to some qubit 2 with known BELL relation to Bob’s qubit 3 in order to enable Bob to transform qubit 3 into the unknown state of qubit 1. If qubits 1 and 2 are accessible to Alice and far apart from Bob, then Alice can access this information without influencing Bob’s qubit (thanks to locality) , although disturbing qubits 1 and 2 in an uncontrollable way.

Strictly speaking, of course, this picture is inconsistent:

Two qubits may be in a factorized 2-qubit state with factors meeting none of the BELL relations. Nevertheless we claim that one of the BELL relations is an element of reality which we find by measuring w.r.t. to the BELL basis.

This inconsistency, however, is typical for our talking about quantum systems:

Even when we know the state Φ of a system (since its preparation is well specified), we may ask for the probability $|\langle \Psi | \Phi \rangle|^2$ to find it in another state Ψ .

Concerning the BELL relation the situation is even less disturbing:

The 1-qubit states give no information about the actual relation between the partners of the individual pairs. Selection into subensembles corresponding to the 4 BELL relations has to be expected to change the partial 1-qubit states – even from a classical point of view.

In order to test for the BELL relations it seems necessary to get the qubits into contact — not necessarily into interaction (Resch et al., 2002; Hofmann and Takeuchi, 2002). This way they loose their identity – a natural reason for the change of the total (internal) state through measurement.

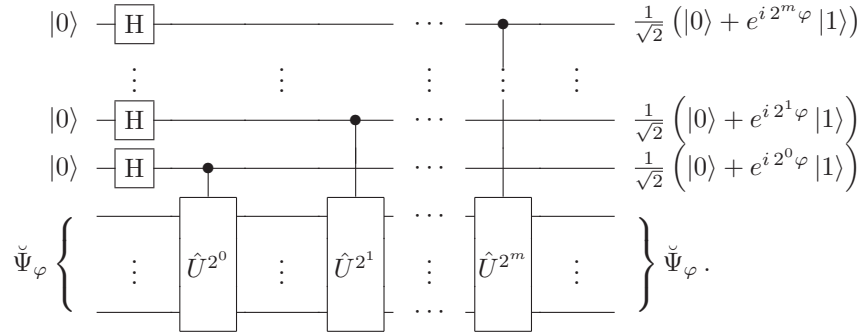
It seems that the BELL relations may be taken as elements of reality, but they can be applied to only one (freely chosen) set of 1-particle ‘properties’.¹

DRAFT, June 26, 2009

¹More generally, see (Griffiths, 2002).

A.3 Quantum Phase Estimation and Order Finding

Exercise 25 Show that the following quantum network acts as indicated if $\check{\Psi}_\varphi$ is a n -qubit eigenstate of the unitary Operator \hat{U} with eigenvalue $e^{i\varphi}$:



First, let us consider the case

$$\varphi = 2\pi \frac{I(\mathbf{b})}{2^{m+1}} \quad \text{for some } \mathbf{b} \in \{0, 1\}^{m+1} . \tag{A.1}$$

Since

$$(A.1) \implies e^{i2^{(m+1)-\nu}\varphi} = \exp\left(i2\pi \sum_{\mu=(m+1)-\nu+1}^{m+1} b_\mu 2^{(m+1)-\nu-\mu}\right) ,$$

(2.22) tells us that

$$(A.1) \implies |\mathbf{b}\rangle = \hat{F}^{-1} \left(2^{-\frac{m+1}{2}} \bigotimes_{\nu=1}^{m+1} (|0\rangle + e^{i2^{(m+1)-\nu}\varphi} |1\rangle) \right) . \tag{A.2}$$

Therefore, the phase φ considered in Exercise 25 can be determined by applying the inverse quantum Fourier transform to the state

$$\begin{aligned} \check{\Phi}_\varphi &\stackrel{\text{def}}{=} 2^{-\frac{m+1}{2}} \bigotimes_{\nu=1}^{m+1} (|0\rangle + e^{i2^{(m+1)-\nu}\varphi} |1\rangle) \\ &= 2^{-\frac{m+1}{2}} \sum_{j=0}^{2^{m+1}-1} e^{i\varphi j} |j\rangle_{m+1} \end{aligned} \tag{A.3}$$

of the first $m + 1$ qubits of the output produced by the described network and measuring the result — **if** (A.1) holds exactly and everything works perfectly.

If $\varphi \in [0, 2\pi)$ is not of the form (A.1), we have

$$\begin{aligned}
\hat{F}^{-1}\check{\Phi}_\varphi &\stackrel{(A.3),(2.18)}{=} \frac{1}{2^{m+1}} \sum_{j,k=0}^{2^{m+1}-1} e^{i\varphi j} e^{-ik \frac{2\pi}{2^{m+1}} j} |k\rangle_{m+1} \\
&= \frac{1}{2^{m+1}} \sum_{j,k=0}^{2^{m+1}-1} \left(e^{i2\pi \left(\frac{\varphi}{2\pi} - \frac{k}{2^{m+1}} \right) j} \right)^j |k\rangle_{m+1} \\
&= \frac{1}{2^{m+1}} \sum_{k=0}^{2^{m+1}-1} \frac{1 - e^{i2\pi \left(2^{m+1} \frac{\varphi}{2\pi} - k \right)}}{1 - e^{i2\pi \left(\frac{\varphi}{2\pi} - \frac{k}{2^{m+1}} \right)}} |k\rangle_{m+1} \\
&= \frac{1}{2^{m+1}} \sum_{k=0}^{2^{m+1}-1} \frac{1 - e^{i2^{m+1}\varphi}}{1 - e^{i2\pi \left(\frac{\varphi}{2\pi} - \frac{k}{2^{m+1}} \right)}} |k\rangle_{m+1}. \tag{A.4}
\end{aligned}$$

Then (A.4) implies that the probability $p(k)$ for finding $|k\rangle_{m+1}$ when testing $\hat{F}^{-1}\check{\Phi}_\varphi$ fulfills the inequality

$$p(k) \leq \frac{1}{2^{2m}} \left| 1 - e^{i2\pi \left(\frac{\varphi}{2\pi} - \frac{k}{2^{m+1}} \right)} \right|^{-2}. \tag{A.5}$$

Let us define

$$D(k) \stackrel{\text{def}}{=} \min_{\nu \in \mathbb{Z}} \left| 2^{m+1} \left(\frac{\varphi}{2\pi} - \nu \right) - k \right| \quad \forall k \in \mathbb{Z}.$$

Then, given $d \in \{3, \dots, 2^m - 1\}$, the probability p_d for getting any state $|k\rangle_{m+1}$ with $D(k) > d$ when testing $\hat{F}^{-1}\check{\Phi}_\varphi$ fulfills the inequality

$$p_d \leq \frac{1}{2(d-2)}. \tag{A.6}$$

Proof: Choosing $k_0 \in \{0, \dots, 2^{m+1} - 1\}$ such that

$$\Delta \stackrel{\text{def}}{=} 2^{m+1} \frac{\varphi}{2\pi} - k_0 \in (0, 1)$$

we get

$$\begin{aligned}
p_d &= \sum_{\substack{k \in \{0, \dots, 2^{m+1}-1\} \\ D(k) > d}} p(k) \\
&\stackrel{(A.5)}{\leq} \frac{1}{2^{2m}} \sum_{\substack{k \in \{0, \dots, 2^{m+1}-1\} \\ \min_{\nu \in \mathbb{Z}} |k_0 - k - \nu 2^{m+1}| \geq d}} \left| 1 - e^{i2\pi \frac{\Delta}{2^{m+1}}} e^{-i2\pi \frac{k-k_0}{2^{m+1}}} \right|^{-2} \\
&= \frac{1}{2^{2m}} \sum_{\substack{j \in \{-2^m+1, \dots, 2^m\} \\ \min_{\nu \in \mathbb{Z}} |j - \nu 2^{m+1}| \geq d}} \left| 1 - e^{i2\pi \frac{\Delta}{2^{m+1}}} e^{-i2\pi \frac{j}{2^{m+1}}} \right|^{-2} \\
&\leq \frac{1}{2^{2m}} \sum_{\substack{j \in \{-2^m+1, \dots, 2^m\} \\ j \notin \{-d+1, \dots, d-1\}}} \left| 1 - e^{i2\pi \frac{\Delta}{2^{m+1}}} e^{-i2\pi \frac{j}{2^{m+1}}} \right|^{-2}.
\end{aligned}$$

By (A.6), therefore²

$$\begin{aligned}
p_d &\leq \frac{1}{2^{2m}} \sum_{\substack{j \in \{-2^m+1, \dots, 2^m\} \\ j \notin \{-d+1, \dots, d-1\}}} \left| \frac{2}{\pi} 2\pi \frac{\Delta - j}{2^{m+1}} \right|^{-2} \\
&= \frac{1}{4} \left(\sum_{j=-2^m+1}^{-d} (\Delta - j)^{-2} + \sum_{j=d}^{2^m} (\Delta - j)^{-2} \right) \\
&\leq \frac{1}{4} \left(\sum_{j=-2^m+1}^{-d} j^{-2} + \sum_{j=d}^{2^m} (1 - j)^{-2} \right) \\
&\leq \frac{1}{2} \sum_{j=d-1}^{2^m-1} j^{-2} \\
&\leq \frac{1}{2} \int_{d-2}^{\infty} \frac{dx}{x^2} \\
&= \frac{1}{2(d-2)}. \quad \blacksquare
\end{aligned}$$

(A.6) tells us that, with probability $\geq 1 - (d-2)^{-1}/2$, testing $\hat{F}^{-1}\check{\Phi}_\varphi$ w.r.t. the computational $(m+1)$ -qubit base gives a state $|\mathbf{b}\rangle$ for which

$$\min_{\nu \in \mathbb{Z}} \left| \varphi - 2\pi\nu - 2\pi \frac{I(\mathbf{b})}{2^{m+1}} \right| \leq 2\pi \frac{d}{2^{m+1}}.$$

Now, let x and N be arbitrarily given **coprime** positive integers. Then the order finding problem is to determine

$$\boxed{r \stackrel{\text{def}}{=} \min \{r' \in \mathbb{N} : x^{r'} = 1 \pmod{N}\},}$$

the **order** of x modulo N .

Defining

$$L \stackrel{\text{def}}{=} \min \{l \in \mathbb{N} : N \leq 2^l\}$$

and

$$[j \bmod N] \stackrel{\text{def}}{=} \min \{k \in \mathbb{Z}_+ : k = j \bmod N\} \quad \forall j \in \mathbb{Z},$$

———— DRAFT, June 26, 2009 ————

²Note that

$$\frac{1}{2} |1 - e^{i\theta}| = \left| \sin \frac{\theta}{2} \right| \geq \frac{|\theta|}{2\sqrt{2}} \geq \frac{|\theta|}{\pi} \quad \forall \theta \in [-\pi, +\pi],$$

since

$$\frac{d}{d\theta} \left(\sin \frac{\theta}{2} - \frac{\theta}{2\sqrt{2}} \right) = \frac{1}{2} \cos \frac{\theta}{2} - \frac{1}{2\sqrt{2}} \geq 0 \quad \forall \theta \in [0, +\pi].$$

we have³

$$r = \left| \left\{ \left| [x^j \bmod N] \right\rangle_L : j \in \mathbb{N} \right\} \right|$$

and

$$\left\langle [x^j \bmod N] \left| [x^k \bmod N] \right\rangle_L = \delta_{jk} \quad \forall j, k \in \{0, 1, \dots, r-1\} .$$

Therefore the states

$$\Psi_s \stackrel{\text{def}}{=} \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-i2\pi \frac{s}{r} j} \left| [x^j \bmod N] \right\rangle_L \quad \forall s \in \{0, \dots, r-1\} \quad (\text{A.7})$$

are normalized and, thanks to (2.17), fulfill the equation

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{+i2\pi \frac{s}{r} j} \Psi_s = \left| [x^j \bmod N] \right\rangle_L \quad \forall j \in \{0, \dots, r-1\} .$$

Especially for $j = 0$ the latter gives

$$\left| 1 \right\rangle_L = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \Psi_s . \quad (\text{A.8})$$

We do not yet know the states Ψ_s explicitly since we do not yet know r . But we know that these states exist and have the nice property that they are eigenstates of the unitary⁴ L -qubit operator \hat{U} characterized by

$$\hat{U} \left| y \right\rangle_L \stackrel{\text{def}}{=} \begin{cases} \left| [x y \bmod N] \right\rangle_L & \text{if } y \in \{0, \dots, N-1\} \\ \left| y \right\rangle & \text{else} \end{cases} \quad \forall y \in \{0, \dots, 2^L-1\} .$$

More precisely, we have

$$\hat{U} \Psi_s = e^{i2\pi \frac{s}{r}} \Psi_s \quad \forall s \in \{0, \dots, r-1\} .$$

Therefore, replacing n by L and $\check{\Psi}_\varphi$ by $\left| 1 \right\rangle_L$, in Exercise 25 we get the total output state⁵

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \check{\Phi}_{2\pi \frac{s}{r}} \otimes \Psi_s .$$

Since the Ψ_s form an orthonormal subset of the L -qubit state space, we may assume that the **partial** state of the system of the first $m+1$ qubits is one of the vector states $\check{\Phi}_{2\pi \frac{s}{r}}$ with equal probability and the results concerning phase estimation show:

———— DRAFT, June 26, 2009 ————

³Recall (1.12).

⁴Note that, because $\gcd(x, N) = 1$,

$$y_1 \neq y_2 \bmod N \implies x y_1 \neq x y_2 \bmod N .$$

⁵Recall (A.3).

When $\hat{F}^{-1} \check{\Phi}_{2\pi \frac{s}{r}}$ is tested w.r.t. the computational $(m+1)$ -qubit basis the probability for getting a state $|k\rangle_{m+1}$ with

$$\left| \frac{s}{r} - \frac{k}{2^{m+1}} \right| \leq \frac{d}{2^{m+1}},$$

for $d \geq 3$, is not less than $1 - \frac{1}{2(d-2)}$.

Choosing d and $2^{m+1}/d$ sufficiently large we obtain, this way, an excellent approximation $k/2^{m+1}$ of s/r for some random $s \in \{0, \dots, r-1\}$.

A.4 Finite-Dimensional Quantum Kinematics

A.4.1 General Description

- The **state space** of a finite-dimensional quantum system is a finite-dimensional complex EUCLIDEAN space \mathcal{H} the inner product of which we denote by $\langle \cdot | \cdot \rangle$.
- The vectors $\psi \in \mathcal{H}$ with norm 1 correspond to **pure states**.⁶
- In the **interaction picture**, used here, the state vectors ψ do not depend on time as long as the states are not disturbed by additional interaction (e.g. with some ‘measurement’ apparatus).
- The state vectors label equivalence classes of preparation procedures for **ensembles** of individual systems of the considered type.
- Preparation procedures are called **equivalent** if the ensembles they provide cannot be distinguished by the statistical outcome of measurements.
- Important measurements performable (in principle) on individual elements of an ensemble are **projective measurements**:

The individual drawn from an ensemble with state vector

$$\psi = \sum_{\nu=1}^n \langle \phi_{\nu} | \psi \rangle \phi_{\nu}$$

will be forced to a transition (if necessary) into one of the ϕ_{ν} -ensembles.⁷ According to the rules of quantum theory we have⁸

$$\boxed{|\langle \phi_{\nu} | \psi \rangle|^2 = \text{probability for the transition } \psi \mapsto \phi_{\nu}} \quad (\text{A.9})$$

for all $\nu \in \{1, \dots, n\}$.

⁶We assume that there are no superselection rules.

⁷I.e., an ensemble formed by a (sufficiently) large number of individuals for which ϕ_{ν} is ‘measured’ actually corresponds (sufficiently well) to ϕ_{ν} , unless additional perturbations have appeared.

⁸Therefore, $\langle \phi_{\nu} | \psi \rangle$ is called **probability amplitude** for the transition $\psi \mapsto \phi_{\nu}$.

- **Observables** are operators $\hat{A} \in \mathcal{L}(\mathcal{H})$ of the form

$$\hat{A} = \sum_{\nu=1}^n \underbrace{a_\nu}_{\in \mathbb{R}} |\phi_\nu\rangle\langle\phi_\nu|, \quad \{\phi_1, \dots, \phi_n\} \text{ an orthonormal basis of } \mathcal{H}, \quad (\text{A.10})$$

with the following interpretation:

In a state with state vector ϕ_ν the physical entity A (corresponding to \hat{A}) has the definite value a_ν .

This together with (A.9) implies:⁹

$$\text{trace}(|\psi\rangle\langle\psi| \hat{A}) = \begin{cases} \text{expectation value for } A \\ \text{in a state with state vector } \psi. \end{cases} \quad (\text{A.11})$$

- Individuals which are only known to be members of an ensemble with state vector ψ_j with probability λ_j for $j \in \{1, \dots, N\}$, $\sum_{j=1}^N \lambda_j = 1$, form an ensemble to be described by the **density matrix**¹⁰

$$\hat{\rho} = \sum_{j=1}^N \underbrace{\lambda_j}_{\geq 0} \underbrace{|\psi_j\rangle\langle\psi_j|}_{\text{normalized}}, \quad \text{trace}(\hat{\rho}) = 1, \quad (\text{A.12})$$

in the sense that

$$\text{trace}(\hat{\rho} \hat{A}) = \text{expectation value for } \hat{A}. \quad (\text{A.13})$$

- In this sense, the set of **all** states corresponds to

$$S(\mathcal{H}) \stackrel{\text{def}}{=} \left\{ \hat{A} \in \mathcal{L}(\mathcal{H}) : \hat{A} \geq 0, \text{trace}(\hat{A}) = 1 \right\}.$$

States¹¹ with $\hat{\rho}^2 \neq \hat{\rho}$ are called **mixed**.

———— DRAFT, June 26, 2009 ————

⁹Note that

$$\text{trace}(|\psi\rangle\langle\psi| \hat{A}) = \sum_{\nu=1}^n a_\nu |\langle\phi_\nu | \psi\rangle|^2 = \langle\psi | \hat{A} \psi\rangle.$$

¹⁰Such ensembles arise, e.g., from projective measurements on pure states if the individuals are not selected according to the ‘measurement’ results.

¹¹From now on we identify states with their density matrices. Note that

$$\hat{\rho} = |\psi\rangle\langle\psi| \quad \text{for some } \psi \in \mathcal{H} \quad \iff \quad \hat{\rho}^2 = \hat{\rho}.$$

Lemma A.4.1 *Let $\hat{\rho}_1, \hat{\rho}_2 \in S(\mathcal{H})$. Then*

$$0 \leq \text{trace}(\hat{\rho}_1 \hat{\rho}_2) \leq 1$$

and

$$\text{trace}(\hat{\rho}_1 \hat{\rho}_2) = 1 \iff \exists \psi \in \mathcal{H} : \hat{\rho}_1 = \hat{\rho}_2 = |\psi\rangle\langle\psi|.$$

Outline of proof: Thanks to the spectral theorem there are an orthonormal basis $\{\phi_1, \dots, \phi_n\}$ of \mathcal{H} and $\lambda_1, \dots, \lambda_n \geq 0$ with

$$\hat{\rho}_1 = \sum_{\nu=1}^n \lambda_\nu |\phi_\nu\rangle\langle\phi_\nu|$$

and hence

$$\begin{aligned} \text{trace}(\hat{\rho}_1 \hat{\rho}_2) &= \sum_{\nu, \mu=1}^n \lambda_\nu \langle\phi_\nu | \phi_\mu\rangle \langle\phi_\nu | \hat{\rho}_2 \phi_\mu\rangle \\ &= \sum_{\nu=1}^n \lambda_\nu \langle\phi_\nu | \hat{\rho}_2 \phi_\nu\rangle. \end{aligned}$$

Therefore, $0 \leq \text{trace}(\hat{\rho}_1 \hat{\rho}_2) \leq 1$ and

$$\begin{aligned} \text{trace}(\hat{\rho}_1 \hat{\rho}_2) = 1 &\iff (0 < \lambda_\nu < 1 \implies \langle\phi_\nu | \hat{\rho}_2 \phi_\nu\rangle = 1) \quad \forall \mu \in \{1, \dots, n\} \\ &\iff \exists \nu_0 \in \{1, \dots, n\} : \hat{\rho}_1 = \hat{\rho}_2 = |\phi_{\nu_0}\rangle\langle\phi_{\nu_0}|. \quad \blacksquare \end{aligned}$$

Lemma A.4.2 *Let¹² $\psi_1, \dots, \psi_N \in \mathcal{H}$. Then*

$$\left(\sum_{k=1}^N |\psi_k\rangle\langle\psi_k| \right) \mathcal{H} = \text{span} \left(\bigcup_{k=1}^N \{\psi_k\} \right). \quad (\text{A.14})$$

Outline of proof: Thanks to the spectral theorem there is an ONS $\{\phi_1, \dots, \phi_{n'}\} \subset \mathcal{H}$ with

$$\sum_{k=1}^N |\psi_k\rangle\langle\psi_k| = \sum_{\nu=1}^{n'} \lambda_\nu |\phi_\nu\rangle\langle\phi_\nu| \quad (\text{A.15})$$

for suitable $\lambda_1, \dots, \lambda_{n'} > 0$ and, consequently,

$$\left(\sum_{k=1}^N |\psi_k\rangle\langle\psi_k| \right) \mathcal{H} = \text{span} \left(\bigcup_{k=1}^N \{\phi_k\} \right). \quad (\text{A.16})$$

Then

$$\begin{aligned} \sum_{k=1}^N |\langle\chi | \psi_k\rangle|^2 &= \sum_{k=1}^N \langle\chi | \psi_k\rangle\langle\psi_k | \chi\rangle \\ &\stackrel{(\text{A.15})}{=} \sum_{\nu=1}^{n'} \lambda_\nu \langle\chi | \phi_\nu\rangle\langle\phi_\nu | \chi\rangle \\ &= \sum_{\nu=1}^{n'} \lambda_\nu |\langle\chi | \phi_\nu\rangle|^2 \quad \forall \chi \in \mathcal{H} \end{aligned}$$

———— DRAFT, June 26, 2009 ————

¹²If not stated otherwise, by $\mathcal{H}, \mathcal{H}_1, \mathcal{H}_2$ we denote arbitrarily given finite-dimensional complex EUCLIDEAN vector spaces.

and, consequently,

$$\chi \perp \psi_k \quad \forall k \in \{1, \dots, N\} \quad \iff \quad \chi \perp \phi_\nu \quad \forall \nu \in \{1, \dots, n\},$$

i.e.

$$\text{span} \left(\bigcup_{k=1}^N \{\psi_k\} \right) = \text{span} \left(\bigcup_{\nu=1}^{n'} \{\phi_\nu\} \right).$$

The latter together with (A.16) implies (A.14). ■

Corollary A.4.3 *Let $\psi_1, \dots, \psi_N, \psi'_1, \dots, \psi'_N \in \mathcal{H}$. Then*

$$\sum_{k=1}^N |\psi_k\rangle\langle\psi_k| = \sum_{k=1}^N |\psi'_k\rangle\langle\psi'_k|. \quad (\text{A.17})$$

holds iff there is a unitary $N \times N$ -matrix (U_j^k) with¹³

$$\psi_k = \sum_{j=1}^N U_k^j \psi'_j \quad \forall k \in \{1, \dots, N\}. \quad (\text{A.18})$$

Proof: Assume that (A.17) holds and, as in the proof of Lemma A.4.2, let us choose an orthonormal basis $\{\phi_1, \dots, \phi_n\} \subset \mathcal{H}$ and $\lambda_1, \dots, \lambda_{n'} > 0$ for which (A.15) holds. Then Lemma A.4.2 implies

$$\text{span} \left(\bigcup_{k=1}^N \{\psi_k\} \right) = \text{span} \left(\bigcup_{\nu=1}^{n'} \{\phi_\nu\} \right).$$

Especially, the ψ_k 's can be written as linear combinations

$$\psi_k = \sum_{\nu=1}^{n'} c_k^\nu \sqrt{\lambda_\nu} \phi_\nu$$

of ϕ_ν 's. Then we have

$$\sum_{\nu=1}^{n'} \lambda_\nu |\phi_\nu\rangle\langle\phi_\nu| \stackrel{(\text{A.15})}{=} \sum_{k=1}^N \sum_{\nu, \mu=1}^{n'} (c_k^\mu)^* c_k^\nu \lambda_\nu |\phi_\nu\rangle\langle\phi_\mu|.$$

Since the $|\phi_\nu\rangle\langle\phi_\mu|$ form an ONS w.r.t. the HILBERT-SCHMIDT *scalar product*

$$\langle \hat{A} | \hat{B} \rangle \stackrel{\text{def}}{=} \text{trace}(\hat{A}^\dagger \hat{B}) \quad \forall \hat{A}, \hat{B} \in S(\mathcal{H}), \quad (\text{A.19})$$

this implies

$$\sum_{k=1}^N (c_k^\nu)^* c_k^\mu = \delta_{\nu\mu} \quad \forall \mu, \nu \in \{1, \dots, n'\},$$

¹³In general, of course, the (U_j^k) are not fixed by (A.18)

i.e. the

$$\mathbf{c}_\nu = \begin{pmatrix} c_1^\nu \\ \vdots \\ c_N^\nu \end{pmatrix}, \quad \nu \in \{1, \dots, n'\},$$

form an orthonormal system in \mathbb{C}^N . Extending this to an orthonormal basis of \mathbb{C}^N we get a unitary $N \times N$ -matrix (c_k^ν) with

$$\psi_k = \sum_{\nu=1}^N c_k^\nu \sqrt[3]{\lambda_\nu} \phi_\nu \quad \forall k \in \{1, \dots, N\}, \quad (\text{A.20})$$

where

$$\lambda_\nu \stackrel{\text{def}}{=} 0 \quad \text{for } \nu > n'.$$

Similarly, we get a unitary $N \times N$ -matrix $(c'_k{}^\nu)$ with

$$\psi'_k = \sum_{\nu=1}^N c'_k{}^\nu \sqrt[3]{\lambda_\nu} \phi_\nu \quad \forall k \in \{1, \dots, N\}$$

and hence

$$\sqrt[3]{\lambda_\nu} \phi_\nu = \sum_{l=1}^N (c'_l{}^\nu)^* \psi'_l \quad \forall \nu \in \{1, \dots, N\}. \quad (\text{A.21})$$

Combining (A.20) with (A.21) we get (A.18) for the unitary matrix with components

$$U_k{}^l \stackrel{\text{def}}{=} \sum_{\nu=1}^N c_k^\nu (c'_l{}^\nu)^* \quad \forall k, l \in \{1, \dots, N\}.$$

Conversely, (A.17) follows from (A.18) by straightforward calculation. ■

A.4.2 Qubits

Qubits are 2-dimensional quantum systems for which some orthonormal **computational basis** $\{|0\rangle, |1\rangle\}$ of their state space \mathcal{H} is chosen. According to the standard convention

$$\left. \begin{aligned} \psi &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad \text{w.r.t. } (|0\rangle, |1\rangle) \\ \stackrel{\text{def}}{\iff} \psi &= \alpha |0\rangle + \beta |1\rangle \end{aligned} \right\} \quad \forall \alpha, \beta \in \mathbb{C}$$

we have

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

All $\hat{A} \in \mathcal{L}(\mathcal{H})$ may be identified with their matrix $\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ w.r.t. the computational basis:

$$\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \implies \hat{A}\psi = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad \text{w.r.t. } (|0\rangle, |1\rangle).$$

Here an orthonormal basis w.r.t. the scalar product (A.19) is $\{\hat{\tau}^0/\sqrt{2}, \dots, \hat{\tau}^3/\sqrt{2}\}$, where

$$\hat{\tau}^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \hat{\tau}^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \hat{\tau}^2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \hat{\tau}^3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (\text{A.22})$$

are the well-known PAULI *matrices*. Therefore we have

$$\hat{A} = \frac{1}{2} \sum_{\nu=0}^3 \text{trace}(\hat{A}\hat{\tau}^\nu) \hat{\tau}^\nu \quad \forall \hat{A} \in \mathcal{L}(\mathcal{H}),$$

especially

$$\hat{\rho} = \frac{1}{2} (\hat{1} + \boldsymbol{\rho} \cdot \hat{\boldsymbol{\tau}}) \quad \forall \hat{\rho} \in S(\mathcal{H}),$$

where the vector¹⁴

$$\boldsymbol{\rho} \stackrel{\text{def}}{=} \text{trace}(\hat{\rho} \hat{\boldsymbol{\tau}})$$

fulfills¹⁵

$$|\boldsymbol{\rho}| \leq 1, \quad \hat{\rho}^2 = \hat{\rho} \iff |\boldsymbol{\rho}| = 1.$$

Note that the components of $\boldsymbol{\rho}$ are just expectation values of observables which are sufficient for *quantum state tomography*.

Remark: Since

$$(\mathbf{e}_{\vartheta, \varphi} \cdot \hat{\boldsymbol{\tau}}) \chi_{\vartheta, \varphi} = \chi_{\vartheta, \varphi}$$

holds for

$$\mathbf{e}_{\vartheta, \varphi} \stackrel{\text{def}}{=} \begin{pmatrix} \sin \vartheta \cos \varphi \\ \sin \vartheta \sin \varphi \\ \cos \vartheta \end{pmatrix}, \quad \chi_{\vartheta, \varphi} \stackrel{\text{def}}{=} \begin{pmatrix} e^{-i \frac{\varphi}{2}} \cos \frac{\vartheta}{2} \\ e^{+i \frac{\varphi}{2}} \sin \frac{\vartheta}{2} \end{pmatrix},$$

every pure state corresponds to a definite spin orientation in the spin- $\frac{1}{2}$ case — where $\frac{\hbar}{2} \hat{\boldsymbol{\tau}}$ is the spin vector observable.

A.4.3 Bipartite Systems

For $j = 1, 2$ let $\{\phi_1^{(j)}, \dots, \phi_{n_j}^{(j)}\}$ be an orthonormal basis of the state space \mathcal{H}_j of a quantum mechanical system \mathcal{S}_j . If \mathcal{S}_1 and \mathcal{S}_2 are **distinguishable** then the **bipartite system** \mathcal{S} composed of these two has the state space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ with orthonormal basis

$$\left\{ \phi_\nu^{(1)} \otimes \phi_\mu^{(2)} : \nu \in \{1, \dots, n_1\}, \mu \in \{1, \dots, n_2\} \right\}.$$

———— DRAFT, June 26, 2009 ————

¹⁴Usually, the **vector of coherence** $\boldsymbol{\rho}$ is called BLOCH **vector** when associated with electron spin and STOKES **vector** when associated with photon polarization. More generally see (Altafini, 2003).

¹⁵Note that

$$1 = \text{trace}(\hat{\rho}) \geq \text{trace}(\hat{\rho}^2) = \frac{1}{2} (1 + |\boldsymbol{\rho}|^2).$$

Extending \otimes to a bilinear mapping of $\mathcal{H}_1 \times \mathcal{H}_2$ into $\mathcal{H}_1 \otimes \mathcal{H}_2$ we get

$$\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2) = \text{span} \left(\hat{A}_1 \otimes \hat{A}_2 : \hat{A}_1 \in \mathcal{L}(\mathcal{H}_1), \hat{A}_2 \in \mathcal{L}(\mathcal{H}_2) \right),$$

where the linear operators $\hat{A}_1 \otimes \hat{A}_2$ are fixed by

$$\left(\hat{A}_1 \otimes \hat{A}_2 \right) (\psi^{(1)} \otimes \psi^{(2)}) \stackrel{\text{def}}{=} \left(\hat{A}_1 \psi^{(1)} \right) \otimes \left(\hat{A}_2 \psi^{(2)} \right) \quad \forall (\psi^{(1)}, \psi^{(2)}) \in \mathcal{H}_1 \otimes \mathcal{H}_2. \quad (\text{A.23})$$

If \hat{A}_1 resp. \hat{A}_2 is the observable of \mathcal{S}_1 resp. \mathcal{S}_2 corresponding to the physical entity A_1 resp A_2 then $\hat{A}_1 \otimes \hat{A}_2$ is the observable corresponding to the physical entity $A_1 A_2$.

If one is only interested in the subsystem \mathcal{S}_1 of the total system \mathcal{S} in state $\hat{\rho}$ then it is sufficient to know its **partial state**¹⁶

$$\hat{\rho}_1 \stackrel{\text{def}}{=} \text{trace}_2(\hat{\rho}) \stackrel{\text{def}}{=} \sum_{\mu=1}^{n_2} \langle \phi_\mu^{(2)} | \hat{\rho} | \phi_\mu^{(2)} \rangle, \quad (\text{A.24})$$

since:

$$\text{trace} \left(\hat{\rho} \left(\hat{A}_1 \otimes \hat{1} \right) \right) = \text{trace} (\hat{\rho}_1 \hat{A}_1) \quad \forall \hat{A}_1 \in \mathcal{L}(\mathcal{H}_1).$$

Note that

$$\hat{\rho} \text{ pure} \not\stackrel{\text{i.g.}}{\iff} \hat{\rho}_1 \text{ pure}.$$

Example: If \mathcal{S}_1 and \mathcal{S}_2 are qubit systems then for the the BELL state

$$\Psi^- \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$$

we have

$$\text{trace}_2 \left(|\Psi^-\rangle \langle \Psi^-| \right) = \frac{1}{2} \hat{1},$$

i.e. the partial states give no information at all:

$$\text{trace} \left(|\Psi^-\rangle \langle \Psi^-| \left(|\psi\rangle \langle \psi| \right) \otimes \hat{1} \right) = \frac{1}{2} \|\psi\|^2 \quad \forall \psi \in \mathbb{C}^2.$$

But there are strong (non-classical) correlations between the subsystems, since

$$\Psi^- = \frac{1}{\sqrt{2}} (\psi \otimes \psi_\perp - \psi_\perp \otimes \psi)$$

———— DRAFT, June 26, 2009 ————

¹⁶The so-called **partial trace** trace_2 w.r.t. the second factor is the linear mapping of $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ into $\mathcal{L}(\mathcal{H}_1)$ characterized by

$$\begin{aligned} \text{trace}_2 \left(|\psi_1 \otimes \psi_2\rangle \langle \psi'_1 \otimes \psi'_2| \right) &= \underbrace{\langle \psi'_2 | \psi_2 \rangle}_{=\text{trace} \left(|\psi_2\rangle \langle \psi'_2| \right)} |\psi_1\rangle \langle \psi'_1| \quad \forall \psi_1, \psi'_1 \in \mathcal{H}_1, \psi_2, \psi'_2 \in \mathcal{H}_2. \end{aligned}$$

The partial trace w.r.t. the first factor, written trace_1 , is defined similarly.

for all normalized $\psi \in \mathbb{C}^2$, where

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}_{\perp} \stackrel{\text{def}}{=} \begin{pmatrix} -\beta^* \\ \alpha^* \end{pmatrix} \quad \text{for all } \alpha, \beta \in \mathbb{C},$$

and hence

$$\text{trace} \left(|\Psi^-\rangle \langle \Psi^-| \left(|\psi\rangle \langle \psi| \right) \otimes \left(|\phi\rangle \langle \phi| \right) \right) = \frac{1}{2} |\langle \phi | \psi_{\perp} \rangle|^2$$

holds for all normalized $\psi, \phi \in \mathbb{C}^2$.

Definition A.4.4 A state $\hat{\rho}$ of the bipartite system \mathcal{S} with state space $\mathcal{H}_1 \otimes \mathcal{H}_2$ is called **separable** iff there is a sequence $\{\hat{\rho}_N\}_{N \in \mathbb{N}}$ of states of the form

$$\hat{\rho}_N = \sum_{\nu=1}^N \underbrace{\lambda_{\nu}}_{\geq 0} \underbrace{\hat{\rho}_{\nu}^{(1)}}_{\in S(\mathcal{H}_1)} \otimes \underbrace{\hat{\rho}_{\nu}^{(2)}}_{\in S(\mathcal{H}_2)} \quad (\text{A.25})$$

with¹⁷

$$\lim_{N \rightarrow \infty} \|\hat{\rho} - \hat{\rho}_N\|_1 = 0.$$

Theorem A.4.5 (Horodecki) Let \mathcal{S} be a bipartite system with state space $\mathcal{H}_1 \otimes \mathcal{H}_2$. Then the separable states of \mathcal{S} are exactly those of the form (A.25) with

$$N \leq (\dim(\mathcal{H}_1 \otimes \mathcal{H}_2))^2.$$

Proof: See (Horodecki, 1997). ■

Lemma A.4.6 Let Ψ be a normalized vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$. Then $\hat{\rho} = |\Psi\rangle \langle \Psi|$ is separable iff

$$\Psi = \phi^{(1)} \otimes \phi^{(2)} \quad (\text{A.26})$$

holds for some normed $\phi^{(1)} \in \mathcal{H}_1$ and $\phi^{(2)} \in \mathcal{H}_2$.

Outline of proof: Let $\hat{\rho} = \hat{\rho}^2$ be separable, hence of the form

$$\hat{\rho} = \sum_{\nu=1}^N \underbrace{\lambda_{\nu}}_{>0} \underbrace{\hat{\rho}_{\nu}^{(1)}}_{\in S(\mathcal{H})} \otimes \underbrace{\hat{\rho}_{\nu}^{(2)}}_{\in S(\mathcal{H})}, \quad \sum_{\nu=1}^N \lambda_{\nu} = 1.$$

¹⁷Recall (5.31) and Footnote 22 of Chapter 5.

Then, by Lemma A.4.1,

$$\begin{aligned} 1 &= \text{trace}(\hat{\rho}^2) \\ &= \sum_{\nu, \mu=1}^N \lambda_\nu \lambda_\mu \underbrace{\text{trace}_{\mathcal{H}_1}(\hat{\rho}_\nu^{(1)} \hat{\rho}_\mu^{(1)})}_{\in[0,1]} \underbrace{\text{trace}_{\mathcal{H}_2}(\hat{\rho}_\nu^{(2)} \hat{\rho}_\mu^{(2)})}_{\in[0,1]} \end{aligned}$$

and, therefore,

$$\text{trace}_{\mathcal{H}_1}(\hat{\rho}_\nu^{(1)} \hat{\rho}_\mu^{(1)}) = \text{trace}_{\mathcal{H}_2}(\hat{\rho}_\nu^{(2)} \hat{\rho}_\mu^{(2)}) = 1 \quad \forall \nu, \mu \in \{1, \dots, N\}.$$

By Lemma A.4.1, again, the latter is equivalent to the existence of normed $\phi^{(1)} \in \mathcal{H}_1$ and $\phi^{(2)} \in \mathcal{H}_2$ with

$$\hat{\rho}_\nu^{(j)} = \left| \phi^{(j)} \right\rangle \left\langle \phi^{(j)} \right| \quad \forall \nu \in \{1, \dots, N\}, j \in \{1, 2\}$$

and hence (A.26).

Conversely, (A.26) together with

$$\hat{\rho}^{(j)} \stackrel{\text{def}}{=} \left| \phi^{(j)} \right\rangle \left\langle \phi^{(j)} \right| \quad \forall j \in \{1, 2\}$$

implies

$$|\Psi\rangle\langle\Psi| = \hat{\rho}^{(1)} \otimes \hat{\rho}^{(2)}$$

and hence separability of $|\Psi\rangle\langle\Psi|$. ■

Theorem A.4.7 *Every vector state on $\mathcal{H}_1 \otimes \mathcal{H}_2$ allows a SCHMIDT **decomposition**,¹⁸ i.e. for every $\Psi \in \mathcal{H}_1 \otimes \mathcal{H}_2$ there are a unique SCHMIDT **number** $n' \in \mathbb{N}$ and orthonormal subsets $\{\phi_1^{(1)}, \dots, \phi_{n'}^{(1)}\}$ resp. $\{\phi_1^{(2)}, \dots, \phi_{n'}^{(2)}\}$ of \mathcal{H}_1 resp. \mathcal{H}_2 with*

$$\Psi = \sum_{\nu=1}^{n'} \underbrace{s_\nu}_{>0} \phi_\nu^{(1)} \otimes \phi_\nu^{(2)} \quad (\text{A.27})$$

for suitable SCHMIDT **coefficients** $s_1, \dots, s_{n'}$. If the eigenvalues of the partial state $\text{trace}_2(|\Psi\rangle\langle\Psi|)$ are non-degenerated then the SCHMIDT decomposition of Ψ is unique.

Outline of proof: Consider any $\Psi \in \mathcal{H}_1 \otimes \mathcal{H}_2$. Thanks to the spectral theorem there are an orthonormal basis $\{\phi_1^{(1)}, \dots, \phi_{n_1}^{(1)}\}$ of \mathcal{H}_1 , a positive integer $n' \leq n_1$, and $s_1, \dots, s_{n'} > 0$ with

$$\text{trace}_2(|\Psi\rangle\langle\Psi|) = \sum_{\nu=1}^{n_1} (s_\nu)^2 \left| \phi_\nu^{(1)} \right\rangle \left\langle \phi_\nu^{(1)} \right|, \quad s_\nu \stackrel{\text{def}}{=} 0 \quad \forall \nu > n'. \quad (\text{A.28})$$

Then there are $\psi_1, \dots, \psi_{n_1} \in \mathcal{H}_2$ with

$$\Psi = \sum_{\nu=1}^{n_1} \phi_\nu^{(1)} \otimes \psi_\nu \quad (\text{A.29})$$

¹⁸For the generalization to n -partite systems see (Carteret et al., 2000)

and, therefore,

$$\text{trace}_2(|\Psi\rangle\langle\Psi|) = \sum_{\nu,\mu=1}^{n_1} \langle\psi_\mu | \psi_\nu\rangle \left| \phi_\nu^{(1)} \right\rangle \left\langle \phi_\mu^{(1)} \right|.$$

The latter together with (A.28) implies

$$\langle\psi_\mu | \psi_\nu\rangle = (s_\nu)^2 \delta_{\nu\mu} \quad \forall \nu, \mu \in \{1, \dots, n_1\}.$$

Thus, with

$$\phi_\nu^{(2)} \stackrel{\text{def}}{=} \frac{\psi_\nu}{s_\nu} \quad \forall \nu \in \{1, \dots, n'\},$$

(A.29) becomes equivalent to (A.27). Since, conversely, (A.27) implies (A.28) the stated uniqueness properties are obvious. ■

Remarks:

1. Note that the BELL states (4.55) have SCHMIDT number 2 and hence, by Lemma A.4.6, be separable.
2. The vector state

$$\frac{1}{2} \left(|0, 0\rangle + |0, 1\rangle + |1, 0\rangle + |1, 1\rangle \right),$$

however, is separable since equal to $(\hat{H} |0\rangle) \otimes (\hat{H} |0\rangle)$, where

$$\hat{H} |0\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle), \quad \hat{H} |1\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

characterizes the unitary HADAMARD *operator*, strongly used in quantum computing.

3. For mixed states $\hat{\rho} \in S(\mathcal{H}_1 \otimes \mathcal{H}_2)$ there is a SCHMIDT-like decomposition of the Form

$$\hat{\rho} = \sum_{\nu=1}^{n'} \underbrace{s_\nu}_{>0} \hat{A}_\nu^{(1)} \otimes \hat{A}_\nu^{(2)}$$

with $n' \leq (\dim \mathcal{H}_1)^2, (\dim \mathcal{H}_2)^2$. According to (Herbut, 2002, Corollary 1) the operators $\hat{A}_\nu^{(j)}$ may be chosen Hermitian and such that

$$\nu \neq \mu \implies \text{trace} \left(\hat{A}_\nu^{(j)} \hat{A}_\mu^{(j)} \right) = 0.$$

However, in general, they cannot be positive.

Pure states are non-separable iff their partial states are mixed.¹⁹ Therefore, the correlations in non-separable pure states are non-classical.²⁰ Obviously, the *partial transpose*

$$\begin{aligned} & (\mathbf{1} \otimes \tilde{\mathfrak{T}}) \left(\sum_{\nu_1, \mu_1=1}^{n_1} \sum_{\nu_2, \mu_2=1}^{n_2} \lambda_{\nu_1 \mu_1 \nu_2 \mu_2} |\phi_{\nu_1}^{(1)} \otimes \phi_{\nu_2}^{(2)}\rangle \langle \phi_{\mu_1}^{(1)} \otimes \phi_{\mu_2}^{(2)}| \right) \\ & \stackrel{(4.13)}{=} \sum_{\nu_2, \mu_2=1}^{n_2} \lambda_{\nu_1 \mu_1 \nu_2 \mu_2} |\phi_{\nu_1}^{(1)} \otimes \phi_{\mu_2}^{(2)}\rangle \langle \phi_{\mu_1}^{(1)} \otimes \phi_{\nu_2}^{(2)}| \end{aligned}$$

w.r.t. the orthonormal basis $\{\phi_1^{(2)}, \dots, \phi_{n_2}^{(2)}\}$ of \mathcal{H}_2 must be positive for separable states:

$$(\mathbf{1} \otimes \mathfrak{T}) \left(\sum_{\nu=1}^N \lambda_{\nu} \hat{\rho}_{\nu}^{(1)} \otimes \hat{\rho}_{\nu}^{(2)} \right)^{T_2} = \sum_{\nu=1}^N \lambda_{\nu} \hat{\rho}_{\nu}^{(1)} \otimes \mathfrak{T}(\hat{\rho}_{\nu}^{(2)}) \geq 0.$$

Therefore, the mixed WERNER states \hat{W}_{λ} with $\lambda > 1/3$, considered at the end of Section 4.2.1, are non-separable.²¹

Lemma A.4.8 *For every state $\hat{\rho} \in \mathcal{H}$ there is a **purification** in $\mathcal{H} \otimes \mathcal{H}$, i.e. a normalized vector $\Psi \in \mathcal{H} \otimes \mathcal{H}$ with*

$$\hat{\rho} = \text{trace}_2(|\Psi\rangle\langle\Psi|). \quad (\text{A.30})$$

Outline of proof: Thanks to the spectral theorem there are an orthonormal basis $\{\phi_1^{(1)}, \dots, \phi_n^{(1)}\}$ of \mathcal{H} and $\lambda_1, \dots, \lambda_n \geq 0$ with

$$\hat{\rho} = \sum_{\nu=1}^n \lambda_{\nu} |\phi_{\nu}^{(1)}\rangle \langle \phi_{\nu}^{(1)}|, \quad \sum_{\nu=1}^n \lambda_{\nu} = 1. \quad (\text{A.31})$$

For the normalized vector²²

$$\Psi \stackrel{\text{def}}{=} \sum_{\nu=1}^n \sqrt{\lambda_{\nu}} \phi_{\nu}^{(1)} \otimes \phi_{\nu}^{(1)}$$

then, we get (A.30). ■

¹⁹Usually, non-separable states are called *entangled*; see (Verstraete and Cirac, 2003), however.

²⁰In a way, also the mixed non-separable states are non-classically correlated (Werner, 1989).

²¹A decomposition of the 2-qubit WERNER states, taking the form (A.25) for $\lambda \leq 1/3$, is presented on page 6 of: <http://www.physik.uni-augsburg.de/weh-school/bruss.pdf>

²²For the set of all suitable Ψ see (Kuah and Sudarshan, 2003, Lemma 1).

Bibliography

- Aaronson, S. and Gottesman, D. (2004). Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70:052328. [quant-ph/0406196](#). 36
- Aho, A. V. and Svore, K. M. (2003). Compiling quantum circuits using the Palindrome transform. [quant-ph/0311008](#), (1–17). 32
- Alber, G., Beth, T., Horodecki, M., Horodecki, P., Horodecki, R., Rötteler, M., Weinfurter, H., Werner, R., and Zeilinger, A. (2001). *Quantum Information*, volume 173 of *Springer Tracts in Modern Physics*. Springer. An Introduction to Basic Theoretical Concepts and Experiments. 3
- Alicki, R. (2003). Controlled quantum open systems. *Lecture Notes in Physics*, 622:121–139. [quant-ph/0302132](#). 105
- Altafini, C. (2003). Tensor of coherences parameterization of multiqubit density operators for entanglement characterization. *Phys. Rev. A*, 69:012311. [quant-ph/0308019](#). 156, 178
- Ambainis, A. (2005). Quantum search algorithms. [quant-ph/0504012](#), pages 1–12. 39
- Aniello, P., Man'ko, V., Marmo, G., A., Porzio, , and Zaccaria, S. S. F. (2003). Trapped ions interacting with laser fields: a perturbative analysis without rotating wave approximation. [quant-ph/0301138](#), pages 1–26. 85
- Audretsch, J., editor (2002). *Verschränkte Welt*. WILEY-VCH, Weinheim. Faszination der Quanten. 3
- Baladi, V. and Vallery, B. (2003). Euclidean algorithms are Gaussian. [mp-arc/03-474](#), pages 1–45. 49
- Barenco, A., Bennet, C., Cleve, R., DiVincenzo, D., Margolus, N., Shor, P., Sleator, T., Smolin, J., and Weinfurter, H. (1995). Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467. [quant-ph/9503016](#). 29
- Bartlett, S. D., Diamanti, E., Sanders, B. C., and Yamamoto, Y. (2002). Photon counting schemes and performance of non-deterministic nonlinear gates in linear optics. [quant-ph/0204073](#), pages 1–9. 19, 57

- Bartlett, S. D. and Wiseman, H. M. (2003). Entanglement in the presence of superselection rules. *Phys. Rev. Lett.*, 91:097903. [quant-ph/0303140](#). 93, 166
- Bennet, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899. 26
- Berry, D. W. and Sanders, B. C. (2003). Bounds on general entropy measures. *J. Phys. A*, 36:12255. [quant-ph/0305059](#). 133
- Bertlmann, R. A. and Zeilinger, A., editors (2002). *Quantum [Un]speakables*. Springer. From Bell to Quantum Information. 3
- Bettelli, S., Serafini, L., and Calarco, T. (2001). Toward an architecture for quantum programming. *cs.PL/0103009*, pages 1–23. 20
- Bowmeester, D., Ekert, A., and Zeilinger, A., editors (2000). *The Physics of Quantum Information*. Springer-Verlag. 3, 27, 126, 164
- Boyer, M., Brassard, G., Høyer, P., and Tapp, A. (1998). Tight bounds on quantum searching. *Fortschr. Phys.*, 46(493–506). [quant-ph/9605034](#). 38, 39
- Braunstein, S. L. and van Loock, P. (2005). Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513. [quant-ph/0410100](#).
- Brezinski, C. (1991). *History of Continued Fractions and Padé Approximants*, volume 12 of *Springer Series in Computational Mathematics*. Springer-Verlag. 49
- Brigham, E. O. (1974). *The Fast Fourier Transform*. Prentice-Hall, Inc., Englewood Cliffs, NJ. 46
- Browne, D. E. and Rudolph, T. (2005). Resource-efficient linear optical quantum computation. *Phys. Rev. Lett.*, 95:010501. [quant-ph/0405157](#). 70
- Brukner, C., Pan, J.-W., Simon, C., Weihs, G., and Zeilinger, A. (2003). Probabilistic instantaneous quantum computation. *Phys. Rev. A*, 67:034304. [quant-ph/0109022](#). 20, 63
- Brukner, C., Zukowski, M., and Zeilinger, A. (2001). The essence of entanglement. [quant-ph/0106119](#), pages 1–10. 25
- Bruß, D. (2003). *Quanteninformation*. Fischer Taschenbuch Verlag. 3
- Bub, J. (2001). Maxwell’s demon and the thermodynamics of computation. *Studies in History and Philosophy of Modern Physics*, 32:569–579. [quant-ph/0203017](#). 15

- Buscemi, F., D'Ariano, G. M., and Sacchi, M. F. (2003). Physical realizations of quantum operations. *Phys. Rev. A*, 68:042113. [quant-ph/0305180](#). 96
- Bužek, V. and Šašura, M. (2002). Cold trapped ions as quantum information processors. *J. Mod. Opt.*, 49:1593–1647. [quant-ph/0112041](#). 73
- Carteret, H. A., Higuchi, A., and Sudbery, A. (2000). Multipartite generalisation of the Schmidt decomposition. *J. Mathem. Phys.*, 41:7932–7939. [quant-ph/0006125](#). 181
- Cerf, N. J., Adami, C., and Kwiat, P. G. (1998). Optical simulation of quantum logic. *Phys. Rev. A*, 57:R1477–R1480. [quant-ph/9706022](#). 58
- Chefles, A., Jozsa, R., and Winter, A. (2003). On the existence of physical transformations between sets of quantum states. [quant-ph/0307227](#), pages 1–8. 144
- Chen, J.-L., Fu, L., Ungar, A. A., and Zhao, X.-G. (2002). Geometric observation for the Bures fidelity between two states of a qubit. *Phys. Rev. A*, 65:024303. [quant-ph/0112169](#). 142
- Chen, Q., Cheng, J., Wang, K.-L., and Du, J. (2006). Efficient construction of 2-D cluster states with probabilistic quantum gates. *Phy. Rev. A*, 73:012303. [quant-ph/0507066](#). 72
- Cheng, K.-W. and Tseng, C.-C. (2002). Quantum plain and carry look-ahead adders. [quant-ph/0206028](#), pages 1–16. 16
- Childs, A. M., Leung, D. W., and Nielsen, M. A. (2005). Unified derivations of measurement-based schemes for quantum computation. *Phys. Rev. A*, 71:032318. [quant-ph/0404132](#). 70
- Christandl, M. and Winter, A. (2004). “Squashed entanglement”- An additive entanglement measure. *J. Mathem. Phys.*, 45:829–840. [quant-ph/0308088](#). 166
- Cleve, R., Ekert, A., Macchiavello, C., and Mosca, M. (1998). Quantum algorithms revisited. *Proc. R. Soc. Lond. A*, 454:339–354. [quant-ph/9708016](#). 23
- Collins, D. and Gisin, N. (2003). A relevant two qubit Bell inequality inequivalent to the CHSH inequality. [quant-ph/0306129](#), pages 1–3. 149
- Coppersmith, D. (1994). An approximate Fourier transform useful in quantum factoring. [quant-ph/0201067](#), pages 1–8. IBM Research RC 19642. 47
- Cover, T. M. and Thomas, J. A. (1991). *Elements of Information Theory*. Wiley Series in Telecommunications. Joh Wiley & Sons, Inc.
- D'Alessandro, D. (2001). Optimal evaluation of generalized Euler angles with applications to classical and quantum control. [quant-ph/0110120](#), pages 1–13. 30

- Davies, E. B. (1976). *Quantum Theory of Open Systems*. Academic Press. 98, 106
- Deutsch, D. and Ekert, A. (1998). Quantum computation. *Physics World*, 11:47–52. 39
- Devetak, I., Harrow, A. W., and Winter, A. (2004). A family of quantum protocols. *Phys. Rev. Lett.*, 93:230504. [quant-ph/0308044](#). 122
- Devetak, I. and Winter, A. (2003). Distilling common randomness from bipartite quantum states. [quant-ph/0304196](#), pages 1–22. 122
- Devetak, I. and Winter, A. (2005). Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A*, 461:207–235. [quant-ph/0306078](#). 164
- Díaz-Caro, A. (2005). On the teleportation of n -qubit states. [quant-ph/0505009](#), pages 1–5. 26
- Dieks, D. (1982). Communication by EPR devices. *Physics Letters A*, pages 271–272. 93
- Diță, P. (2001). Factorization of unitary matrices. [math-ph/0103005](#), pages 1–12. 28
- DiVincenzo, D. P. (2000). The physical implementation of quantum computation. *Fortschr. Phys.*, 48:771–783. [quant-ph/9705009](#). 53
- Doherty, A. C., Parrilo, P. A., and Spedalieri, F. M. (2003). A complete family of separability criteria. *Phys. Rev. A*, 69:022308. [quant-ph/0308032](#). 155
- Dong, D.-Y., Chen, C.-L., Zhang, C.-B., and Chen, Z.-H. (2006). Quantum robot: Structure, algorithms and applications. *Robotica*, 24:513–521. [quant-ph/0506155](#). 39
- Dowling, J. P., Franson, J. D., Lee, H., and Milburn, G. J. (2004). Towards linear optical quantum computers. [quant-ph/0402090](#), pages 1–9. 62
- Draper, T. G. (2000). Addition on a quantum computer. [quant-ph/0008033](#), pages 1–8. 16
- Eckert, K., Schliemann, J., Bruß, D., and Lewenstein, M. (2002). Quantum correlations in systems of indistinguishable particles. *Annals of Physics*, 299:88–127. [quant-ph/0203060](#). 19, 166
- Ekert, A., Hayden, P., and Inamori, H. (2000). Basic concepts in quantum computation. [quant-ph/0011013](#), pages 1–37. Lectures given at les Houches Summer School on "Coherent Matter Waves", July-August 1999. 3
- Eldar, Y. C. (2003). Von Neumann measurement is optimal for detecting linearly independent mixed quantum states. [quant-ph/0304077](#), pages 1–4. 137

- Elliott, C., Colvin, A., Pearson, D., Pikal, O., Schlafer, J., and Yeh, H. (2005). Current status of the DARPA quantum network. *quant-ph/0503058*, pages 1–12. [126](#)
- Fattal, D., Diamanti, E., Inoue, K., and Yamamoto, Y. (2003). Quantum teleportation with a quantum dot single photon source. *quant-ph/0307105*, pages 1–4. [68](#)
- Feynman, R. P. (1982). Simulating physics with computers. *Int. J. Theoret. Phys.*, 21:467–488.
- Feynman, R. P. (1985). Quantum mechanical computers. *Optics News*, February:11–20.
- Galindo, A. and Martín-Delgado, M. A. (2002). Information and computation: Classical and quantum aspects. *Rev. Mod. Phys.*, 74:347–423. [quant-ph/0112105](#).
- Gardiner, C. W. and Zoller, P. (2000). *Quantum Noise*, volume 56 of *Springer Series in Synergetics*. Springer, 2. edition. A Handbook of Markovian and Non-Markovian Quantum Stochastic Methods with Applications to Quantum Optics. [133](#)
- Gasparoni, S., Pan, J.-W., Walther, P., Rudolph, T., and Zeilinger, A. (2004). Realization of a photonic CNOT gate sufficient for quantum computation. *Phys. Rev. Lett.*, 93:020504. [quant-ph/0404107](#). [73](#)
- Gatti, A., Zambrini, R., Miguel, M. S., and Lugiato, L. A. (2003). Multi-photon, multi-mode polarization entanglement in parametric down-conversion. *quant-ph/0306133*, pages 1–22. [123](#)
- Ghosh, P. K. (1995). *Ion Traps*. Clarendon Press, Oxford. [73](#), [77](#)
- Giacomini, S., Sciarrino, F., Lombardi, E., and Martini, F. D. (2002). “Active” teleportation of a quantum bit. *Phys. Rev. A*, 66:030302. [quant-ph/0204158](#). [26](#)
- Gilchrist, A., Langford, N. K., and Nielsen, M. A. (2005). Distance measures to compare real and ideal quantum processes. *Phys. Rev. A*, 71:062310. [quant-ph/0408063](#). [139](#)
- Gilchrist, A. and Milburn, G. J. (2002). Conditional phase shifts using trapped atoms. *quant-ph/0208157*, pages 1–6. [62](#)
- Gingrich, R. M., Ko, P., Lee, H., Vatan, F., and Dowling, J. P. (2003). An all linear optical quantum memory based on quantum error correction. *Phys. Rev. Lett.*, 91:217901. [quant-ph/0306098](#). [123](#)
- Gisin, N. and Gisin, B. (2002). A local variable model for entanglement swapping exploiting the detection loophole. *quant-ph/0201077*, pages 1–5. [27](#)

- Gottesman, D. and Chuang, I. L. (1999). Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402:390–393. [quant-ph/9908010](#). 63
- Griffiths, R. B. (2002). The nature and location of quantum information. *Phys. Rev. A*, 66:012311. [quant-ph/0203058](#). 168
- Groisman, B. (2008). Is teleportation a (quantum) mystery? *arXiv: 0806.1679 [quant-ph]*, pages 1–10. 26
- Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, Philadelphia (1996)*, pages 212–219. 36
- Grover, L. K. and Radhakrishnan, J. (2004). Is partial quantum search of a database any easier? [quant-ph/0407122](#), pages 1–9. 38
- Gruska, J. (1999). *Quantum Computing*. Advanced Topics in Computer Science Series. McGraw-Hill.
- Gu, M. and Weedbrook, C. (2005). Quantum passwords. [quant-ph/0506255](#), pages 1–5. 94
- Gu, M., Weedbrook, C., Menicucci, N. C., and Timothy C. Ralph, P. v. L. (2009). Quantum computing with continuous-variable clusters. *arXiv:0903.3233 [quant-ph]*, pages 1–17.
- Gühne, O., Hyllus, P., Bruß, D., Ekert, A., Lewenstein, M., Macchiavello, C., and Sanpera, A. (2002). Detection of entanglement with few local measurements. *Phys. Rev. A*, 66:062305. [quant-ph/0205089](#). 152
- Gulde, S., Riebe, M., Lancaster, G. P. T., Becher, C., Eschner, J., Häffner, H., Schmidt-Kaler, F., Chuang, I. L., and Blatt, R. (2003). Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer. *Nature*, 421:48–50. 23
- Gurvits, L. (2002). Quantum matching theory (with new complexity theoretic, combinatorial and topological insights on the nature of the quantum entanglement). [quant-ph/0201022](#), pages 1–10. 149
- Ha, K.-C., Kye, S.-H., and Park, Y. S. (2003). Entangled states with positive partial transpose arising from indecomposable positive linear maps. *Phys. Lett. A*, 313:163–174. [quant-ph/0305005](#). 154
- Haderka, O., Hamar, M., and Perina, J. (2004). Experimental multi-photon-resolving detector using a single avalanche photodiode. *Eur. Phys. J. D*, 28:149. [quant-ph/0302154](#). 57

- Hamming, R. W. (1950). Error detecting and error correcting codes. *The Bell System Technical Journal*, 26:147–160. <http://www.engelschall.com/u/sb/hamming/>. 110
- Hayden, P., Jozsa, R., Petz, D., and Winter, A. (2004). Structure of states which satisfy strong subadditivity of quantum entropy with equality. *Commun. Math. Phys.*, 246(2):359–374. [quant-ph/0304007](#).
- Heiss, D., editor (2001). *Fundamentals of Quantum Information*. Springer. Quantum Computation, Communication, Decoherence and All That.
- Herbert, N. (1982). FLASH—A superluminal communicator based upon a new kind of quantum measurement. *Foundations of Physics*, 12:1171–1181. 94
- Herbut, F. (2002). Hermitian Schmidt decomposition and twin observables of bipartite mixed states. *J. Phys. A*, 35:1691–1708. [quant-ph/0305181](#). 182
- Hiroshima, T. (2003). Majorization criterion for distillability of a bipartite quantum state. *Phys. Rev. Lett.*, 91:057902. [quant-ph/0303057](#). 155, 158
- Hirvensalo, M. (2001). *Quantum Computing*. Natural Computing Series. Springer-Verlag.
- Hofmann, H. F. and Takeuchi, S. (2002). Quantum phase gate for photonic qubits using only beam splitters and post-selection. *Phys. Rev. A*, 66:024308. [quant-ph/0204045](#). 62, 168
- Horodecki, M. and Horodecki, P. (1999). Reduction criterion of separability and limits for a class of protocols of entanglement distillation. *Phys. Rev. A*, 59:4206–4216. [quant-ph/9708015](#). 158
- Horodecki, M., Horodecki, P., and Horodecki, R. (1996). Separability of mixed states: Necessary and sufficient conditions. *Phys. Lett. A*, 223:1–8. [quant-ph/9605038](#). 154, 166
- Horodecki, M., Horodecki, P., and Horodecki, R. (2001). Mixed-state entanglement and quantum communication. *Springer Tracts in Modern Physics*, 173:151–195. [quant-ph/0109124](#). 149, 156
- Horodecki, M., Oppenheim, J., and Winter, A. (2005). Quantum information can be negative. *Nature*, 436:673–676. [quant-ph/0505062](#). 132
- Horodecki, P. (1997). Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A*, 232:333–339. [quant-ph/9703004](#). 180
- Horodecki, R. and Horodecki, M. (1996). Information-theoretic aspects of quantum inseparability of mixed states. *Phys. Rev. A*, 54:1838–1843. [quant-ph/9607007](#). 154

- James, D. F. V. (1998). Quantum dynamics of cold trapped ions with application to quantum computation. *App. Phys. B*, 66:181. [79](#)
- James, D. F. V. (2000). Quantum computation with hot and cold ions: An assessment of proposed schemes. *Fortschritte der Physik*, 48:811–821. [quant-ph/0003122](#). [73](#)
- Kahn, D. (1967). *The Codebreakers: The Story of Secret Writing*. Macmillan, New York. [40](#)
- Kaszlikowski, D., Gopinathan, A., Liang, Y. C., Kwek, L. C., and Englert, B.-G. (2003). How well can you know the edge of a quantum pyramid? [quant-ph/0307086](#), pages 1–3. [137](#)
- Kaye, P. and Mosca, M. (2004). Quantum networks for generating arbitrary quantum states. [quant-ph/0407102](#), pages 1–3. [70](#)
- Keyl, M. and Werner, R. F. (2002). How to correct small quantum errors. *Lecture Notes in Physics*, 611:263. [quant-ph/0206086](#). [118](#)
- Kim, Y.-H., Kulik, S. P., and Shih, Y. (2001). Quantum teleportation with a complete Bell state measurement. *Phys. Rev. Lett.*, 86:1370. [quant-ph/0010046](#). [64](#), [123](#)
- Klein, O. (1931). Zur Quantenmechanischen Begründung des zweiten Hauptsatzes der Wärmelehre. *Z. Physik*, 72:767–775. [134](#)
- Knill, E., Laflamme, R., and Milburn, G. (2000). Efficient linear optics quantum computation. *Nature*, 409:46. [quant-ph/0006088](#). [65](#)
- Knill, E., Laflamme, R., and Milburn, G. J. (2001). A scheme for efficient quantum computation with linear optics. *Nature*, 409:46–52. [53](#), [62](#), [65](#), [69](#)
- Knill, E., Laflamme, R., and Viola, L. (1999). Theory of quantum error correction for general noise. [quant-ph/9908066](#), pages 1–6. [108](#)
- Korepin, V. E. and Grover, L. K. (2006). Simple algorithm for partial quantum search. *Quantum Information Processing*, 5:5–10. [quant-ph/0504157](#). [39](#)
- Kuah, A. and Sudarshan, E. (2003). Manifold of density matrices. [quant-ph/0307218](#), pages 1–5. [183](#)
- Kuah, A. and Sudarshan, E. C. G. (2005). Extension maps. [quant-ph/0503119](#), pages 1–6. [97](#), [99](#)
- Kwiat, P. G., Mitchell, J. R., Schwindt, P. D. D., and White, A. G. (2000). Grover’s search algorithm: An optical approach. *J.Mod.Opt.*, 47:257–266. [quant-ph/9905086](#). [58](#)

- Labuschagne, L. E., Majewski, W. A., and Marciniak, M. (2003). On k -decomposability of positive maps. *math-ph/0306017*, pages 1–23. 154
- Landauer, R. (1961). Irreversibility and heat generation in the computing process. *IBM J. Res. Dev.*, 5:183–191. 15
- Landauer, R. (1998). Energy needed to send a bit. *Proc. R. Soc. Lond. A*, 454:305–311. 15
- Lavenda, B. H. and Dunning-Davies, J. (2003). Additive entropies of degree- q and the Tsallis entropy. *physics/0310117*, pages 1–13. 157
- Lee, H., Oh, S. D., and Ahn, D. (2003). Entanglement measure for any quantum states. *quant-ph/0306127*, pages 1–6. 166
- Lee, J.-S., Chung, Y., Kim, J., and Lee, S. (1999). A practical method of constructing quantum combinational logic circuits. *quant-ph/9911053*, pages 1–6. 14
- Leung, D. (2000). *Towards robust quantum computation*. PhD thesis, Stanford University. cs.CC/0012017. 122
- Lewenstein, M. and Sanpera, A. (1998). Separability and entanglement of composite quantum systems. *Phys. Rev. Lett.*, 80:2261–2264. *quant-ph/9707043*. 166
- Lim, Y. L., Beige, A., and Kwek, L. C. (2005). Repeat-until-success quantum computing. *Phys. Rev. Lett.*, 95:030505. *quant-ph/0408043*. 70
- Lindner, H., Brayer, H., and Lehmann, C. (1999). *Taschenbuch der Elektrotechnik und Elektronik*. Fachbuchverlag Leipzig im Carl Hanser Verlag. 14
- Long, G.-L. and Sun, Y. (2001). Efficient scheme for initializing a quantum register with an arbitrary superposed state. *Phys. Rev. A*, 64:014303. *quant-ph/0104030*. 18
- Lücke, W. (1996). Axiomatic quantum theory. *Acta Phys. Pol.*, 27:2357–2385. 105
- Lücke, W. (edyn). Elektrodynamik .
<http://www.wolfgang-luecke.de/skripten/edyn.pdf>. 54
- Lücke, W. (eine). Ergänzungen zu “Mathematische Methoden der Physik”.
<http://www.wolfgang-luecke.de/skripten/eine.pdf>. 29, 94, 103, 143
- Lücke, W. (mech). Klassische Mechanik .
<http://www.wolfgang-luecke.de/skripten/mech.pdf>. 30
- Lücke, W. (musi). Theorie zur Physik der Musikinstrumente.
<http://www.wolfgang-luecke.de/skripten/musi.html>. 43

- Lücke, W. (nlqo). Introduction to photonics.
<http://www.wolfgang-luecke.de/skripten/nlqo.pdf>. 19, 60, 61, 64, 66, 83, 84, 86, 95
- Lücke, W. (qft). Particles and fields.
<http://www.wolfgang-luecke.de/skripten/qft.pdf>. 20
- Lücke, W. (tdst). Thermodynamik und Statistik
<http://www.wolfgang-luecke.de/skripten/tdst.pdf>. 20
- MacWilliams, F. J. and Sloane, N. J. A. (1998). *The theory of error-correcting codes*. North-Holland, New York.
- Mahler, G. and Weberruß, V. A. (1995). *Quantum Networks*. Springer-Verlag. Dynamics of Open Nanostructures.
- Mermin, N. D. (2002). Deconstructing dense coding. *Phys. Rev. A*, 66:032308. [quant-ph/0204107](https://arxiv.org/abs/quant-ph/0204107). 24, 25, 122
- Mermin, N. D. (2004). Copenhagen computation: How I learned to stop worrying and love Bohr. *IBM Journal of Research and Development*, 48:53–62. [quant-ph/0305088](https://arxiv.org/abs/quant-ph/0305088).
- Mershin, A., Nanopoulos, D. V., and Skoulakis, E. M. C. (2000). Quantum brain? *PROC. ACAD. ATHENS*, 74 A. [quant-ph/0007088](https://arxiv.org/abs/quant-ph/0007088).
- Mertens, S. (2002). Computational complexity for physicists. *Computing in Science & Engineering*, 4:31–41. [cond-mat/0012185](https://arxiv.org/abs/cond-mat/0012185). 32
- Metcalf, H. J. and van der Straten, P. (1999). *Laser Cooling and Trapping*. Springer-Verlag. 90
- Milburn, G. J. (1996). *Quantum Technology*. Frontiers of science. Allen & Unwin.
- Mitchison, G. and Jozsa, R. (2001). Counterfactual computation. *Proc. Roy. Soc. Lond.*, A457:1175–1194. [quant-ph/9907007](https://arxiv.org/abs/quant-ph/9907007). 20
- Mitchison, G. and Jozsa, R. (2003). Towards a geometrical interpretation of quantum information compression. [quant-ph/0309177](https://arxiv.org/abs/quant-ph/0309177), pages 1–11. 145
- Mizrahi, S. S. and Dodonov, V. V. (2002). Creating quanta with ‘annihilation’ operator. [quant-ph/0207035](https://arxiv.org/abs/quant-ph/0207035), pages 1–8. 55
- Morikoshi, F., Santos, M. F., and Vedral, V. (2003). Accessibility of physical states and non-uniqueness of entanglement measure. *J. Phys. A*, 37:5887. [quant-ph/0306032](https://arxiv.org/abs/quant-ph/0306032). 165
- Möttönen, M. and Vartiainen, J. J. (2005). Decompositions of general quantum gates. [quant-ph/0504100](https://arxiv.org/abs/quant-ph/0504100), pages 1–25. 121

- Munro, W., Nemoto, K., Spiller, T., Barrett, S., Kok, P., and Beausoleil, R. (2005a). Efficient optical quantum information processing. *J. Opt. B: Quantum Semi-class. Opt.*, 7:S135. [quant-ph/0506116](#). 61
- Munro, W. J., Nemoto, K., and Spiller, T. P. (2005b). Weak nonlinearities: A new route to optical quantum computation. *New J. Phys.*, 7:137. [quant-ph/0507084](#). 61
- Neumark, M. A. (1959). *Normierte Algebren*. VEB Deutscher Verlag der Wissenschaften, Berlin. 150
- Nielsen, M. A. (2004). Optical quantum computation using cluster states. *Phys. Rev. Lett.*, 93:040503. [quant-ph/0402005](#). 65, 72, 73
- Nielsen, M. A. (2005). Cluster-state quantum computation. [quant-ph/0504097](#), pages 1–15. 70
- Nielsen, M. A. and Chuang, I. L. (1997). Programmable quantum gate arrays. *Phys. Rev. Lett.*, 79:321–324. [quant-ph/9703032](#). 72
- Nielsen, M. A. and Chuang, I. L. (2001). *Quantum Computation and Quantum Information*. Cambridge University Press. 3, 41, 42, 49, 74, 93, 138, 147, 159, 162, 163
- Nielsen, M. A. and Dawson, C. M. (2004). Fault-tolerant quantum computation with cluster states. [quant-ph/0405134](#), pages 1–31. 72
- Nussbaumer, H. J. (1982). *Fast Fourier Transform and Convolution Algorithms*, volume 2 of *Springer Series in Information Sciences*. Springer-Verlag. 46
- Ohya, M. and Petz, D. (1993). *Quantum Entropy and Its Use*. Springer-Verlag. 133, 147
- Ottaviani, C., Rebic, S., Vitali, D., and Tombesi, P. (2006). Quantum phase gate operation based on nonlinear optics: Full quantum analysis. *Phys. Rev. A*, 73:010301(R). [quant-ph/0507137](#). 61
- Paris, M., Plenio, M., Jonathan, D., Bose, S., and D’Ariano, G. (2000). Optical Bell measurement by Fock filtering. *Physics Letters A*, 273:153–158. [quant-ph/9911036](#). 123
- Parker, M. C. and Walker, S. D. (2003). Information transfer and Landauer’s principle. [physics/0310116](#), pages 1–5. 15
- Patel, A. (2001). Quantum algorithms and the genetic code. *Pramana*, 56:367–381. [quant-ph/0002037](#).
- Peres, A. (2002). How the no-cloning theorem got its name. [quant-ph/0205076](#), pages 1–4. 18, 93

- Perez-Delgado, C. A. and Kok, P. (2009). What is a quantum computer, and how do we build one? *arXiv:0906.4344 [quant-ph]*, pages 1–15. [53](#)
- Perron, O. (1954). *Die Lehre von den Kettenbrüchen*, volume I: Elementare Kettenbrüche. B.G. Teubner Verlagsgesellschaft, Stuttgart. [49](#)
- Perron, O. (1957). *Die Lehre von den Kettenbrüchen*, volume I: Analytisch-funktionentheoretische Elementare Kettenbrüche. B.G. Teubner Verlagsgesellschaft, Stuttgart. [49](#)
- Petz, D. (2001). Entropy, von Neumann and the von Neumann entropy. *math-ph/0102013*, pages 1–10. [133](#), [147](#)
- Pittman, T. B. and Franson, J. D. (2002). Cyclical quantum memory for photonic qubits. *Phys. Rev. A*, 66:062302. [65](#)
- Plenio, M. B. and Vitelli, V. (2001). The physics of forgetting: Landauer’s erasure principle and information theory. *Contemporary Physics*, 42:25–60. [quant-ph/0103108](#). [15](#)
- Pless, V. (1989). *Introduction to the Theory of Error-Correcting Codes*. John Wiley & Sons. [110](#)
- Preskill, J. (1998a). Fault-tolerant quantum computation. In Lo, H.-K., Popescu, S., and Spiller, T. P., editors, *Introduction to Quantum Computation and Information*, pages 213–269. World Scientific. ISBN 981-02-339-X. [quant-ph/9712048](#). [122](#)
- Preskill, J. (1998b). Reliable quantum computers. *Proc. R. Soc. Lond. A*, 454:385–410. [quant-ph/9705031](#). [122](#)
- Preskill, J. (2000–01). Physics 219/Computer Science 219 Quantum Computation (Formerly Physics 229). (<http://theory.caltech.edu/~preskill/ph229/#lecture>). [3](#), [118](#), [129](#)
- Pütz, J., editor (1971). *Einführung in die Elektronik*. Bücher des Wissens. Fischer Taschenbuch Verlag GmbH, Frankfurt am Main. [11](#)
- Ralph, T. C., White, A. G., Munro, W. J., and Milburn, G. J. (2002). Simple scheme for efficient linear optics quantum gates. *Phys. Rev. A*, 65:012314. [quant-ph/0108049](#). [19](#), [60](#), [62](#)
- Raussendorf, R. (2003). *Measurement-based quantum computation with cluster states*. Dissertation, Ludwig-Maximilians Universität, München. [70](#)
- Raussendorf, R. (2005). Quantum computation via translation-invariant operations on a chain of qubits. *Phys. Rev. A*, 72:052301. [quant-ph/0505122](#). [70](#)

- Raussendorf, R. and Briegel, H. J. (2001). A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191. [quant-ph/0010033](#). 70
- Raussendorf, R., Browne, D. E., and Briegel, H. J. (2002). The one-way quantum computer - a non-network model of quantum computation. *J. Mod. Opt.*, 49:1299–1306. [quant-ph/0108118](#). 19
- Reck, M., Zeilinger, A., Bernstein, H. J., and Bertani, P. (1994). Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61. 28
- Řeháček, J. and Hradil, Z. (2002). Quantification of entanglement by means of convergent iterations. *Phys. Rev. Lett.*, 90:127904. [quant-ph/0205071](#). 164
- Resch, K. J., Lundeen, J. S., and Steinberg, A. M. (2002). Practical creation and detection of polarization Bell states using parametric down-conversion. [quant-ph/0204034](#), (1–13). 168
- Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126. <http://theory.lcs.mit.edu/~cis/pubs/rivest/rsapaper.ps>. 40
- Robertson, A. and Robertson, W. (1967). *Topologische Vektorräume*, volume 164/164a. Bibliographisches Institut · Mannheim. 150
- Rosé, H., Aßelmeyer-Maluga, T., Kolbe, M., Niehörster, F., and Schramm, A. (2004). The Fraunhofer quantum computing portal - www.qc.fraunhofer.de - A web-based simulator of quantum computing processes. [quant-ph/0406089](#), pages 1–7. 51
- Rosenberg, D., Lita, A. E., Miller, A. J., and Nam, S. W. (2005). Noise-free high-efficiency photon-number-resolving detectors. *Phys. Rev. A*, 71:061803. [quant-ph/0506175](#). 59
- Rudolph, O. (2000). A separability criterion for density operators. *J. Phys. A*, 33:3951–3955. [quant-ph/0002026](#). 157
- Rudolph, O. (2002). Further results on the cross norm criterion for separability. [quant-ph/0202121](#), pages 1–19. 158
- Rudolph, T. and Pan, J.-W. (2001). A simple gate for linear optics quantum computing. [quant-ph/0108056](#), pages 1–1. 62
- Rudolph, T. and Virmani, S. S. (2005). A relational quantum computer using only two-qubit total spin measurement and an initial supply of highly mixed single qubit states. [quant-ph/0503151](#), pages 1–5. 70
- Ruskai, M. B. (2002). Inequalities for quantum entropy: A review with conditions for equality. *J. Math. Phys.*, 43:4358–4375. [quant-ph/0205064](#). 133

- Sanaka, K., Jennewein, T., Pan, J.-W., Resch, K., and Zeilinger, A. (2003). Experimental nonlinear sign shift for linear optics quantum computation. *Phys. Rev. Lett.*, 92:017902. [quant-ph/0308134](#). 60
- Sanctuary, B. C., Presse, S., Lazzara, T. D., Henderson, E. J., and Hourani, R. F. (2003). Interpretation of “non-local” experiments using disentanglement. [quant-ph/0308026](#), pages 1–14. 124
- Schlingemann, D. (2001). Stabilizer codes can be realized as graph codes. [quant-ph/0111080](#), (1–7). 118
- Schlingemann, D. and Werner, R. F. (2000). Quantum error-correcting codes associated with graphs. *Phys. Rev. A*, 65:012308. [quant-ph/0012111](#). 118
- Schneier, B. (1996). *Applied Cryptography*. John Wiley & Sons, Inc. 40
- Schroeder, M. R. (1997). *Number Theory in Science and Communication*, volume 7 of *Springer Series in Information Sciences*. Springer-Verlag. 41
- Shabani, A. and Lidar, D. A. (2006). Quantum error correction beyond completely positive maps. [quant-ph/0610028](#), pages 1–5. 96
- Shannon, C. (1949a). Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28:656–715. 126
- Shannon, C. E. (1949b). *The mathematical theory of communication*. University of Illinois Press. 3, 11, 93, 129, 130
- Shende, V. V., Bullock, S. S., and Markov, I. L. (2006). Synthesis of quantum logic circuits. *IEEE Trans. on Computer-Aided Design*, 25, no. 6:1000–1010. [quant-ph/0406176](#). 15
- Shende, V. V., Markov, I. L., and Bullock, S. S. (2004). On universal gate libraries and generic minimal two-qubit quantum circuits. *Phys. Rev. A*, 69:062321. [quant-ph/0308033](#). 32
- Shende, V. V., Prasad, A. K., Markov, I. L., and Hayes, J. P. (2003). Reversible logic circuit synthesis. *IEEE Trans. on CAD*, 22:710–722. [quant-ph/0207001](#). 14, 15
- Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 Nov. 1994*, pages 124–134. IEEE Comput. Soc. Press. 42, 126
- Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Sci. Statist. Comput.*, 26:1484–1509. [quant-ph/9508027](#). 48

- Shor, P. W. (2000). Introduction to quantum algorithms. [quant-ph/0005003](#). Course at the January 2000 AMS meeting. 35
- Singh, S. (2002). *Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Random House Children's Publishing. 40
- Sleator, T. and Weinfurter, H. (1994). Realizable universal quantum logic gates. *Phys. Rev. Lett.*, 74:4087–4090. 31
- Streater, R. F. (2003). Duality in quantum information geometry. [math-ph/0308037](#), pages 1–7. 139
- Tarasov, V. E. (2002). Quantum computations by quantum operations on mixed states. [quant-ph/0201033](#), pages 1–11. 19
- Toffoli, T. (1980a). Reversible computing. In Goos, G. and Hartmanis, J., editors, *Automata, Languages and Programming*, pages 632–644. Springer-Verlag. 15
- Toffoli, T. (1980b). Reversible computing. Technical Memo MIT/LCS/TM-151, MIT Lab. for Comp. Sci. (<http://pm1.bu.edu/~tt/publ.html>). 16
- Tomita, A. (2000). Complete Bell state measurement with controlled photon absorption and quantum interference. [quant-ph/0006093](#), pages 1–4. 123
- Tsai, I. M. and Kuo, S. Y. (2001). A systematic algorithm for quantum boolean circuits construction. [quant-ph/0104037](#), pages 1–12. 15, 16
- Tucci, R. R. (2004). QC Paulinesia. [quant-ph/0407215](#), pages 1–45. See also: <http://www.ar-tiste.com/PaulinesiaVer1.pdf>. 13
- Tulsi, T., Grover, L., and Patel, A. (2005). A new algorithm for directed quantum search. [quant-ph/0505007](#), pages 1–12. 39
- Uhlman, A. (1976). The ‘transition probability’ in the state space of a *-algebra. *Rep. Math. Phys.*, 9:273–279. 142
- Varnava, M., Browne, D. E., and Rudolph, T. (2006). Loss tolerance in one-way quantum computation via counterfactual error correction. *Phys. Rev. Lett.*, 97:120501. [quant-ph/0507036](#). 70
- Vatan, F. and Williams, C. (2004). Optimal quantum circuits for general two-qubit gates. *Phys. Rev. A*, 69:032315. [quant-ph/0308006](#). 32
- Vedral, V., Barenco, A., and Ekert, A. (1996). Quantum networks for elementary arithmetic operations. *Phys. Rev. A*, 54:147–153. [quant-ph/9511018](#). 16, 43
- Verstraete, F. and Cirac, J. (2003). Quantum nonlocality in the presence of superselection rules and some applications. *Phys. Rev. Lett.*, 91:10404. [quant-ph/0302039](#). 93, 166, 183

- Vidal, G. and Werner, R. F. (2002). A computable measure of entanglement. *Phys. Rev. A*, 65:032314. [quant-ph/0102117](#). 156
- Vollbrecht, K. G. H. and Wolf, M. M. (2002). Conditional entropies and their relation to entanglement criteria. *J. Mathem. Phys.*, 43:4299. [quant-ph/0202058](#). 157
- von Neumann, J. (1927). Thermodynamik quantenmechanischer Gesamtheiten. *Nachr. der Gesellschaft der Wiss. Gött.*, pages 273–291. 133
- Waks, E., Inoue, K., Diamanti, E., and Yamamoto, Y. (2003). High efficiency photon number detection for quantum information processing. [quant-ph/0308054](#), pages 1–10. 57
- Walther, P., Resch, K., Rudolph, T., Schenck, E., Weinfurter, H., Vedral, V., Aspelmeyer, M., and Zeilinger, A. (2005). Experimental one-way quantum computing. *Nature*, 434:169–176. [quant-ph/0503126](#). 39, 70
- Wehrl, A. (1978). General properties of entropy. *Rev. Modern Phys.*, 50:221–260. 133
- Werner, R. (2001). Quantum information theory — an invitation. *Springer Tracts in Modern Physics*, 173:14–57. [quant-ph/0101061](#). 18, 94, 96
- Werner, R. F. (1989). Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281. 102, 149, 183
- Werner, R. F. and Wolf, M. M. (201). All multipartite Bell correlation inequalities for two dichotomic observables per site. [quant-ph/0102024](#), pages 1–11. 149
- White, A. G., James, D. F. V., Munro, W. J., and Kwiat, P. G. (2001). Exploring Hilbert space: accurate characterisation of quantum information. *Phys. Rev. A*, 64:R030302. [quant-ph/0108088](#). 166
- Wootters, W. K. (2001). Entanglement of formation and concurrence. *Quantum Information and Computation*, 1:27–44. 165
- Wootters, W. K. and Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299:802–803. 18, 93
- Wunderlich, C. and Balzer, C. (2003). Quantum measurements and new concepts for experiments with trapped ions. *Advances in Atomic, Molecular, and Optical Physics*, 49:295–376. [quant-ph/0305129](#). 73
- Younes, A. and Miller, J. (2004). Automated method for building CNOT based quantum circuits for Boolean functions. *Proceeding of ICENCO2004*, pages 562–565. [quant-ph/0304099](#). 15

- Zhao, Z., Zhang, A.-N., Chen, Y.-A., Zhang, H., Du, J.-F., Yang, T., and Pan, J.-W. (2005). Experimental demonstration of a non-destructive controlled-NOT quantum gate for two independent photon-qubits. *Phys. Rev. Lett.*, 94:030501. [quant-ph/0404129](#). 73

Index

- adder, 16
- balanced, 22
- BELL
 - measurement, 25, 26
 - network, 24, 26
 - states, 24
- BERNSTEIN-VAZIRANI
 - oracle, 24
- binary digit, 11
- bit, 11
 - qu-, 19
- BLOCH
 - vector, 178
- CAMPBELL-HAUSDORFF formula, 66
- circuit
 - classical logic, 12, 15
 - computational, 11
 - equivalent, 11
 - graph, 12
 - logic, 14
- classical
 - computation, 15, 17, 22
 - network, 18
 - logic circuit, 12, 15
 - reversible computation, 15, 16
 - reversible network, 15
- closed quantum system, 105
- code
 - CALDERBANK-SHOR-STEANE, 116
 - linear classical
 - dual, 111
 - quantum, 112
 - words, 112
 - stabilizer, 115
 - STEANE, 118
 - word, 110
- coding
 - quantum dense, 24
- coherence
 - vector of, 178
- coherent superposition, 18, 23
- complexity
 - computational, 32
- computation
 - al basis, 18–20
 - classical, 15, 17, 22
 - reversible, 15, 16
 - complexity, 32
- concurrence, 165
- CSS codes, 116
- decoherence, 106
- dense coding, 24
- DEUTSCH-JOZSA
 - oracle, 22, 23
 - problem, 22
- dual code, 111
- e-bit, 164
- entangled, 24
 - pure state, 24, 26, 105
- entanglemen
 - catalysis, 163
- entanglement
 - of formation, 165
 - swapping, 27
 - witness, 149, 153
- entropic inequalities, 157
- entropy
 - REN'YI, 157
- equivalent
 - classical network, 11

- preparation procedures, 173
 - quantum network, 22
- error correction, 18
- EULER angles, 30
- fast FOURIER, 46
- flip
 - operator, 102
- FOURIER transform
 - fast, 46
- FREDKIN gate, 13
- function
 - balanced, 22
 - decision, 14
- gate, 11
 - FREDKIN, 13
 - non-deterministic, 19
 - quantum, 19, 20
 - universal, 27
 - reversible, 13
 - TOFFOLI, 13
 - universal, 15, 16
- graph, 12
- halting problem, 11, 167
- HAMMING
 - distance, 110
- interaction picture, 173
- LOCC, 158
- logic circuit, 14
- measurement, 18, 19
 - BELL, 25, 26
 - projective, 173
- mixture, 106
- network
 - adder, 16
 - BELL, 24, 26
 - classical
 - 2-bit, 17
 - computational, 18
 - reversible, 15
- optimization, 15
- quantum
 - equivalent, 22
 - quantum computational, 18
 - reversible, 15
 - teleportation, 25
- open quantum system, 106
- operator
 - positive
 - support, 138
- oracle
 - BERNSTEIN-VAZIRANI, 24
 - DEUTSCH-JOZSA, 22, 23
- order
 - of an integer modulo N , 171
- Partial transpose, 154
- PAULI
 - group, 113
- PAULI matrices, 106
- polarization identity, 149
- post selection, 26
- problem
 - DEUTSCH-JOZSA, 22
 - halting, 167
- projective measurement, 173
- quantum
 - closed system, 105
 - code, 112
 - code words, 112
 - computation
 - network, 18
 - result, 19
 - dense coding, 24
 - gate, 19, 20
 - measurement, 18
 - network
 - equivalent, 22
 - open system, 106
 - parallelism, 18
 - state
 - entangled, 24, 26, 105
 - tomography, 178

- state collapse, 18
- teleportation, 25, 26
- wire, 19
- qubit, 19
- Range criterion, 156
- register, 11
 - n -qubit, 19
 - state space, 18
- RENÒI entropies, 157
- result
 - of a quantum computation, 19
- reversible
 - classical network, 15
- SLEATOR-WEINFURTER construction, 32
- stabilizer, 115
 - codes, 115
- state
 - BELL, 24
 - mixed, 106
 - pure, 173
 - quantum
 - entangled, 24, 26, 105
 - separable, 153, 180
 - WERNER, 153
- state space, 173
- STEANE code, 118
- STOKES
 - vector, 178
- superoperator, 98
- superposition
 - coherent, 23
- teleportation, 26
 - network, 25
 - of entanglement, 27
- tensor product
 - formalism of quantum mechanics, 19
- TOFFOLI gate, 13
- tomography
 - quantum state, 178
- trace
 - norm, 139
 - partial, 179
- transposition, 102, 154
 - partial, 154
- universal
 - gate, 15, 16
 - quantum gate, 27
- WERNER states, 153
- wire, 15
 - quantum, 19