Lecture Notes

Introduction to Quantum Information Theory

by
Prof. Daniel Braun
Version 18

University of Tübingen

Contents

& Chuang, 2010

1 Definition and Motivation

1.1 Definition: Quantum Information Processing

Definition 1
Quantum information processing = Processing of information by leveraging quantum effects, particularly including

- *Quantum interference*
- *Quantum entanglement*
- *Quantum non-locality*
- *Quantum uncertainty.*

1.2 Motivation and (Promised) Potential

- Algorithms with a fundamentally higher efficiency: Challenging the classical hierarchy of complexity classes, e.g. ($b := \log_2 \{N\}$)

Algorithm	Complexity		By
	Classic	Quantum	
Factorisation: $N = p_1 p_2$, $p_1 \simeq p_2$	$\exp\left\{b^{\frac{1}{3}} \log^{\frac{2}{3}} b\right\}$	b^3	Shor 1995
Searching an unsorted list of N elements	N	$\sqrt{N}$	Grover 1996

  and many others, including the hidden subgroup problem, solving systems of linear equations.

- Simulating the quantum behaviour in many body systems: The dimension of the Hilbert space $\mathcal{H}$ increases exponentially with the number of particles n, e.g. to determine the structure and spectrum of a molecule consisting of n atoms and m energy levels per atom, the dimension of Hilbert space is $\dim \mathcal{H} = m^n$. Let e.g. be $m = 10, n = 100$, then

$\dim \mathcal{H} = 10^{100} \ggg 10^{80} \simeq$ estimated number of atoms in the universe.

We also encounter the same problem when we try to probabilistically describe classical systems: Let

$$P(\boldsymbol{p_1}, \ldots, \boldsymbol{p_n}, \boldsymbol{q_1}, \ldots, \boldsymbol{q_n}) \mathrm{d}^3 p_1 \ldots \mathrm{d}^3 q_n \tag{1.1}$$

be the probability to find particle i at $(\boldsymbol{p_i}, \boldsymbol{q_i})$, where $i = 1, \ldots, n$. If the components p_{ik}, q_{ik} ($k = 1, 2, 3$ for directions x, y, z in a Cartesian coordinate system) are discretised with m possible values, then $P \in \mathbb{R}_+^d$, i.e. a $d = m^{6n}$ dimensional real vector is just as difficult (arguably up to a factor 2) to specify as $\psi \in \mathbb{C}^d$, i.e. a number of probabilities that grows exponentially fast with n would be needed to specify the state of the many-particle system. We can, however, successfully describe the dynamics of the classical problem using the trajectory within the $6n$ dimensional phase space. But $\nexists$ *hidden variables* which allow a correct and local description of a q-system[1]. To solve this problem, Feynmann proposed in 1982 the use of q-computers to simulate q-systems [20]

- q-communication: All known classical encryption technologies are problematic:
  - RSA: Based on the hope that nobody knows an efficient, classical algorithm to factorise numbers
  - The enigma machine: Development of decryption methods by profiting from human error, repetitive messages, and reused keys.
  - One-time-pad: Do you trust the messenger of the random key?

  q-communication is the first technology which allows for a intrinsically safe data transfer based on certifiable limits for the maximal allowed data loss (information loss) during establishment of a shared secret key.
- New insights into physics:
  - measurements: the ultimate limit for the accuracy of measurements and how to realise measurements with such accuracy (*q-enhanced measurements*)
  - more generalized measurements compared to von-Neumann projections
  - locality vs. q-non-locality and *true randomness*; with applications in safe and device-independent communication channels

[1] The guiding field in the *de-Broglie-Bohm pilot wave theory* is already non-local for a single particle.

  - q-thermodynamics: single shot entropy and quantum heat engines
  - black hole physics: quantum gravity, the *holographic principle* and the absorption of information, yes or no?

1.3 Literature

- M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, ISBN: 0-521-63503-9.
- John Preskill's course, `http://www.theory.caltech.edu/people/preskill/ph219/`.
- David Mermin, *Quantum Computer Science. An Introduction*, ISBN: 9780521876582

2 Physics of Information

2.1 R. Landauer: "Information is physical"

- Storage of information in physical devices: e.g. in capacitors (DRAM), magnetization (hard disk, MRAM)), charges on gate electrodes (Flash drives) or even in the qm state of an atom?
- Manipulation through physical devices
- Physical properties of these devices determine their performance, laws of physics set fundamental limits on our abilities to manipulate information. Examples for these limits are
  - speed of light limits speed of communication
  - tunnelling rates through gate oxide limits speed of flash memory
  - thermal activation limits retention time of information on hard drives.

2.2 Landauer's Principle (1961)

Erasure of information is a dissipative process. What is the minimum energy dissipation during the erasure process?

The arguably simplest version of a classical bit consists of a particle, such as a molecule or a single electron, in a box. Depending on whether it is in one or the

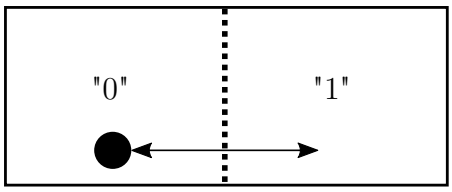


Figure 2.1: Representation of one bit using a single molecule in a box. Depending on the molecule's position, the bit stored is either 0 (molecule in the left half of the box) or 1 (molecule in the right half of the box).

other half of the box, the particle codes a classical state 0 or 1. In the simple case of Figure 2.1, in order to erase the state of the bit, the molecule is put to the left side, irrespective of whether it was on the right or left side before. Do it e.g. by removing the partition wall, then compress the "gas" with a piston until the molecule is on the left. In any case, the entropy of the system is reduced by

$$\Delta S = k_{\mathrm{B}} \ln 2 \tag{2.1}$$

This needs a minimum amount of heat $\Delta Q = T\Delta S$ (asusming an isothermal change at temperature T) to be dissipated to erase 1 bit of information! The order of magnitude is about

$$\Delta Q \sim 10^{-23}\,\mathrm{J} \cdot 10^{2} \simeq 10^{-21}\,\mathrm{J} \tag{2.2}$$

Compared to modern DRAM: A bit stored with charge of order 10^4e using 90 nm technology and the voltage of the capacitor at $\sim 0.1\,\mathrm{V}$ requires around $\Delta Q = qU \simeq 10^{-16}\,\mathrm{J}$, which is still a factor 10^5 away. About $500 k_{\mathrm{B}} T \ln 2$ are dissipated in an elementary logical operation with today's technology, and heat production has become one of the major technical problems in modern CPUs. Very recently a new proposal for "sub-Landauer thermodynamic efficiency" came up, where the information is stored in momentum states [34]. However, long before that, it was realized that the energy dissipation in computation can be reduced in principle to arbitrarily low levels by making the computation reversible.

2.3 Reversible Computation

Classical logical gates are typically irreversible, e.g. merge 2 input bits to 1 output bit. This means information loss and thus dissipation in each application of such an (irreversible) gate.

See e.g. the *NAND*gate where the truth table is shown in Table 2.1.

a	b	$c = \neg(a \wedge b)$
0	0	1
0	1	1
1	0	1
1	1	0

Table 2.1: Truth table for the *NAND*gate. The two input bits a, b are merged into a target bit c and there is no way to go back.

Theorem 1 (C. Bennett 1973)
Any computation can be performed using only reversible gates.

The trick is to keep all the input information when applying the gates. See e.g. the reversible version of the *NAND*gate called the *Toffoli gate* (Table 2.2).

a	b	c	a	b	$c \oplus (a \wedge b)$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Table 2.2: Truth table of the Toffoli gate.

$\oplus$ represents the *exclusive or XOR*, equivalent to the addition of the two bits (mod 2). Obviously the value of the last bit changes depending on c. The gate is a $NAND(a, b)$ gate for $c = 1$ but an $AND(a, b)$ for $c = 0$.

This way, the information is only reshuffled (indeed only the last two of the three-bit words are exchanged), and no reduction of entropy occurs. This implies that there is also no need to dissipate energy.

But can we simply replace all *NAND*gates by Toffoli gates to make an algorithm reversible? The answer is "no"! Rather, one needs a lot of storage space for all intermediate results which are necessary to revert the computation.

Suppose for example, we want to apply a gate twice on bits in different order, or on other bits. We can't just overwrite (neither input nor output), we need to store them. So we get a lot of extra junk. The next question to raise is: Don't we just have to pay the energy bill at the end of the computation, since then we surely will throw away all the intemediate results? Bennett's answer: No, we just have to pay the bill for printing the results. After that, we run the computation backwards and erase all the information reversibly.

Reversible classical computation has become a research field of its own, see [21] for an overview. The fact that computations can be done reversibly was a crucial

insight for the development of quantum computing: first quantum gates were based on a quantum generalization of the Toffoli gate, as you will learn in the next section.

3 Universal Quantum Computer

3.1 The Quantum Bit and Quantum Byte

A classical bit is a system with two defined states: It is either in a state "0" or in a state "1". A quantum bit, or "qubit" for short, however, is a quantum mechanical 2-state system with two orthonormal basis states $\{|0\rangle, |1\rangle\}$ called the *computational basis*. Physically, we can think of it as a spin-1/2 system, where the two computational basis states could be identified with e.g. spin-up and spin-down in a preferred direction, i.e. $|0\rangle = |\uparrow\rangle$, $|1\rangle = |\downarrow\rangle$. In Chapter 6 we will examine possible physical realizations in more detail. A general pure state can be written in the computational basis as

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{3.1}$$

where $|a|^2 + |b|^2 = 1$, $a, b \in \mathbb{C}$. A measurement that projects $|\psi\rangle$ on $|0\rangle$ or on $|1\rangle$, i.e. a measurement diagonal in these basis states such as $\sigma_z = \mathrm{diag}\,(1, -1)$, finds $|0\rangle$ with a probability $|a|^2$ and $|1\rangle$ with a probability $|b|^2$.

More generally, for N qubits, a general state can be expanded as

$$|\psi\rangle = \sum_{x=0}^{2^N-1} a_x\,|x\rangle\ , \tag{3.2}$$

where $|x\rangle = |x_n\rangle\,|x_{n-1}\rangle \ldots |x_0\rangle$, $x_i = 0, 1$ and $a_x \in \mathbb{C}, \sum_{x=0}^{2^N-1} |a_x|^2 = 1$.

While this looks trivial, it is in fact hard to write down $|\psi\rangle$ for even a modest number of qubits. For e.g. $N = 100$ qubits, this requires $2^N \simeq 10^{30}$ complex coefficients. For $N = 1000$, we require $2^N \simeq 10^{300}$ coefficients, which is by very far a number much greater than the estimated number of elementary particles in the universe, $N_p \simeq 10^{80}$! It is therefore impossible to store this information on a classical computer! But Nature somehow seems to keep track of it.

The "*computational basis*" for N qubits is the basis $\left\{|0\rangle, \ldots |2^N - 1\rangle\right\}$, where a state $|x\rangle$ is understood as the binary representation in terms of single-qubit states, e.g. $|5\rangle = |1\rangle\,|0\rangle\,|1\rangle \equiv |101\rangle$.

3.2 Quantum Algorithms

Feynmann suggested 1982: A quantum computer might be able to perform computations that a classical computer can't! Only three years later, David Deutsch came up with the decomposition of an arbitrary unitary transformation into elementary quantum gates — the quantum circuit model of a quantum algorithm was born [14].

A *q-algorithm* can be represented very generally as a unitary transformation that propagates the input of the algorithm in the form of a quantum state $|\psi\rangle$ to its output, another quantum state $|\psi'\rangle$:

$$|\psi'\rangle = U\,|\psi\rangle \tag{3.3}$$

with a well-defined initial state $|\psi\rangle$, typically (but not necessarily) $|0\rangle \ldots |0\rangle$.

The algorithm is *encoded* into the unitary transformation U. Since U has an inverse, $U^{-1} = U^\dagger$, it is clear that a quantum algorithm is a *reversible* algorithm. Later we will see how decoherence issues modify this ideal picture to some extent. The more urging challenge is, however, to generate an appropriate transformation U using physical manipulations of single or multiple qubits. We will see that a small number of single- and two-qubit gates, when applied sequentially on all qubits, allows one to generate an arbitrary unitary transformation on the full, huge Hilbert space. The q-algorithm can then be represented as a so-called *quantum-circuit*. A quantum-computer that is able to perform arbitrary unitary transformations on the full Hilbert space is called a "universal quantum-computer": it can be programmed to run any possible quantum-algorithm, just as a classical universal computer can be programmed to run any possible classical algorithm.

There exists, however, one fundamental dilemma: Accessing the q-computer for controlling the gates and, at the latest, reading out the result of the calculation, introduces decoherence, hence destroying the system's capability of quantum mechanical interference. Balancing the need to access with the need to preserve quantum coherence is the biggest challenge in building a functioning quantum-computer.

The state $|\psi'\rangle$ encodes the result of the algorithm. At the end of the algorithm, all qubits are measured (typically using σ_z), i.e. they are projected to either $|0\rangle$ or $|1\rangle$, such that the result 0 or 1 for each qubit is found with the corresponding probabilities. In general, quantum algorithms are therefore stochastic algorithms.

If the initial state of N qubits is chosen as $|\psi\rangle = |+\rangle^{\otimes N}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, then

$$|\psi'\rangle = U|\psi\rangle = U\frac{1}{2^{N/2}}\sum_{s=0}^{2^N-1}|s\rangle = \frac{1}{2^{N/2}}\sum_{s=0}^{2^N-1}U|s\rangle \ , \tag{3.4}$$

i.e. due to the linearity of the quantum mechanical propagation, all initial states $|s\rangle$ with $s = 0, 1, \ldots, 2^{N-1}$ are propagated in parallel. However, while this effect is often quoted as the source of the power of a quantum computer, the resulting parallelism is so far without consequences. If in the end one measures the states of the qubits, these will collapse to some value, and with them the superposition of all results, i.e. one does not get $U|s\rangle$ for all initiatl s. In fact, one would typically not even know to which input the output belongs. A similar parallelism appears, in fact, also in classical computing, when one considers the propgation of an ensemble of input states described according to a probability distribution over all input states. Making use of the quantum-parallelism is therefore much more subtle, and typically exploits the possibility of quantum mechanical interference between different paths in the algorithm — a feast that as far as we know is impossible classically in a sufficiently large Hilbert space.

We will later show that we can deconstruct any arbitrary U into an ensemble of universal q-gates.

3.3 Geometrical Representation of Qubits on the Bloch Sphere

3.3.1 Bloch vector

An arbitrary, possibly mixed state, i.e. a density matrix ρ of a qubit may be written as

$$\rho = \frac{1}{2}(\mathbb{1}_2 + \boldsymbol{r}\cdot\boldsymbol{\sigma}) = \sum_i p_i |i\rangle\langle i| \tag{3.5}$$

where $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ are the Pauli matrices, and $\boldsymbol{r} \in \mathbb{R}^3, |\boldsymbol{r}| \leq 1$. The Pauli matrices are given explicitly as

$$\sigma_x \equiv \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.6}$$

$$\sigma_y \equiv \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{3.7}$$

$$\sigma_z \equiv \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} . \tag{3.8}$$

If not otherwise specified, the basis in which they are written is the computational basis $\{|0\rangle, |1\rangle\}$, with the basis vectors arranged in this order. The density matrix has the following properties:

- $\operatorname{tr}\rho = 1/2 \operatorname{tr}\mathbb{1}_2 = 1$
- $\rho = \rho^\dagger$, since $\sigma_i = \sigma_i^\dagger$
- $\operatorname{tr}\rho^2 \leq 1$.

The last property, valid for any density matrix, is the one equivalent to $\boldsymbol{r}^2 \leq 1$:

$$\operatorname{tr}\rho^2 = \frac{1}{4}\operatorname{tr}\left(\mathbb{1}_2 + \boldsymbol{r}\cdot\boldsymbol{\sigma}\right)\left(\mathbb{1}_2 + \boldsymbol{r}\cdot\boldsymbol{\sigma}\right) \tag{3.9}$$

$$= \frac{1}{4}\operatorname{tr}\mathbb{1}_2 + 2\boldsymbol{r}\cdot\boldsymbol{\sigma} + \left(\boldsymbol{r}\cdot\boldsymbol{\sigma}\right)\left(\boldsymbol{r}\cdot\boldsymbol{\sigma}\right) \tag{3.10}$$

$$\overset{(*)}{=} \frac{1}{4}\operatorname{tr}\left(1 + \boldsymbol{r}^2\right)\mathbb{1}_2 \tag{3.11}$$

$$= \frac{1}{2}\left(1 + \boldsymbol{r^2}\right) \leq 1 \Leftrightarrow \boldsymbol{r}^2 \leq 1\,. \tag{3.12}$$

For $(*)$ we used the following relationship:

$$\left(\boldsymbol{r}\cdot\boldsymbol{\sigma}\right)^2 = \sum_{i,j} r_i\sigma_i r_j\sigma_j \tag{3.13}$$

$$= \sum_i r_i^2\sigma_i^2 + \sum_{i\neq j} r_i r_j \sigma_i\sigma_j \tag{3.14}$$

$$= \sum_i r_i^2\sigma_i^2 = \sum_i r_i^2\mathbb{1}_2 = \boldsymbol{r}^2\mathbb{1}_2\,, \tag{3.15}$$

where the last term in (3.14) vanishes, as it is a contraction of a symmetric and an anti-symmetric tensor of rank 2: The Pauli matrices anticommute, i.e. for $i \neq j$: $\sigma_i\sigma_j + \sigma_j\sigma_i = 0$. More precisely, $\sigma_i\sigma_j = \mathbb{1}\delta_{ij} + i\epsilon_{ijk}\sigma_k$ (using Einstein summation convention and the totally antisymmetric Levi-Civita tensor with $\epsilon_{123} = 1$). In addition, $\operatorname{tr}\sigma_i = 0\,\forall i$.

A pure state is very generally defined as a rank-1 projector, i.e. $\rho = |\psi\rangle\langle\psi|$, and has therefore $\operatorname{tr}\rho^2 = \operatorname{tr}\left(|\psi\rangle\langle\psi|\right)^2 = \operatorname{tr}|\psi\rangle\langle\psi| = \langle\psi|\psi\rangle = 1$, which implies $|\boldsymbol{r}| = 1$. All pure states are therefore located on the Bloch sphere. They correspond to a 3D unit-vector, which we may also write using a spherical coordinate system: (r, ϑ, φ), where hence $r = 1$ for pure states. In return we can for any state calculate $\boldsymbol{r}$ by

projecting ρ onto σ_i in the sense of the operator scalar-product, $(A, B) \equiv \operatorname{tr} A^\dagger B$, i.e. tracing over $\sigma_i \rho$:

$$r_i = \operatorname{tr} \sigma_i \rho \,. \tag{3.16}$$

With the above relation for $\sigma_i \sigma_j$, we have indeed

$$\operatorname{tr} \sigma_i \rho = \frac{1}{2} \operatorname{tr} \mathbb{1}_2 \sigma_i + r_j \sigma_i \sigma_j = r_j \delta_{ij} = r_i \,. \tag{3.17}$$

Example 1

- $\boldsymbol{r} = \mathbf{0}$*:* $\rho = \frac{1}{2}\mathbb{1}_2 = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)$ *(completely mixed state)*

- $\boldsymbol{r} = +\hat{e}_z = +\begin{pmatrix}0\\0\\1\end{pmatrix}$*:* $\rho = \frac{1}{2}\left(\mathbb{1}_2 + \sigma_z\right) = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} = |0\rangle\langle 0|$

- $\boldsymbol{r} = -\hat{e}_z = -\begin{pmatrix}0\\0\\1\end{pmatrix}$*:* $\rho = \frac{1}{2}\left(\mathbb{1}_2 - \sigma_z\right) = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix} = |1\rangle\langle 1|$

- $\boldsymbol{r} = \pm\hat{e}_x = \pm\begin{pmatrix}1\\0\\0\end{pmatrix}$*:* $\rho = \frac{1}{2}\left(\mathbb{1}_2 \pm \sigma_x\right) = \begin{pmatrix}1 & \pm 1\\\pm 1 & 1\end{pmatrix} = |\pm\rangle\langle\pm|$

- $\boldsymbol{r} = \pm\hat{e}_y = \pm\begin{pmatrix}0\\1\\0\end{pmatrix}$*:* $\rho = \frac{1}{2}\left(\mathbb{1}_2 \pm \sigma_y\right) = \begin{pmatrix}1 & \mp i\\\pm i & 1\end{pmatrix} = |\tilde{\pm}\rangle\langle\tilde{\pm}|$

where in the last two examples we used

$$|\pm\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right) \tag{3.18}$$

$$|\tilde{\pm}\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle \pm i\,|1\rangle\right) \tag{3.19}$$

Let in general be

$$|\psi\rangle = \cos\frac{\vartheta}{2}\,|0\rangle + \exp\{i\varphi\}\sin\frac{\vartheta}{2}\,|1\rangle \;. \tag{3.20}$$

The corresponding density matrix reads

$$\rho = |\psi\rangle\langle\psi| \tag{3.21}$$

$$= \cos^2\frac{\vartheta}{2}|0\rangle\langle 0| + \sin^2\frac{\vartheta}{2}|1\rangle\langle 1| + \cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}\left(\exp\{i\varphi\}|1\rangle\langle 0| + \exp\{-i\varphi\}|0\rangle\langle 1|\right) \tag{3.22}$$

$$= \cos^2\frac{\vartheta}{2}\frac{\mathbb{1}+\sigma_z}{2} + \sin^2\frac{\vartheta}{2}\frac{\mathbb{1}-\sigma_z}{2} + \cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}\left(\cos\varphi\cdot\sigma_x + i\sin\varphi\cdot\frac{\sigma_y}{i}\right) \tag{3.23}$$

$$= \frac{1}{2}\left(\mathbb{1}_2 + \sin\vartheta\cos\varphi\cdot\sigma_x + \sin\vartheta\sin\varphi\cdot\sigma_y + \cos\vartheta\cdot\sigma_z\right) \tag{3.24}$$

$$\equiv \frac{1}{2}\left(\mathbb{1}_2 + \boldsymbol{r}\cdot\boldsymbol{\sigma}\right) \tag{3.25}$$

from which we read off the Bloch vector $\boldsymbol{r}$,

$$\boldsymbol{r} = \begin{pmatrix}\sin\vartheta\cos\varphi\\ \sin\vartheta\sin\varphi\\ \cos\vartheta\end{pmatrix}. \tag{3.26}$$

This means that the parametrisation in (3.20) directly yields the Bloch vector in spherical coordinates.

This may appear puzzling: A general $U(2)$ transformation is parametrized by four real parameters. How is it then possible to create an arbitrary pure state of a qubit by applying a $U(2)$ matrix to an initial reference state $|0\rangle$ if $|\psi\rangle$ depends only on two real parameters? The answer is that *i.)* we did not specify any global phase of $|\psi\rangle$, and that *ii.)* to fully specify U we need its action on two base vectors, not only one.

3.3.2 Mixing of states

Let

$$\rho = (1-p)\frac{\mathbb{1}_2}{2} + p|\psi\rangle\langle\psi| \tag{3.27}$$

where $|\psi\rangle$ is associated with the Bloch vector $\boldsymbol{r}$ and $0 \leq p \leq 1$ is a mixing probability, i.e. ρ can describe a mixed state, where one prepares with probability p the pure state $|\psi\rangle$, and with probability $1-p$ the fully mixed state $\frac{\mathbb{1}_2}{2}$. If $p = 0$, then $\rho = \mathbb{1}/2$ and if $p = 1$, then ρ is pure. What is then for general p the Bloch vector $\boldsymbol{s}$ of ρ?
We have

$$\rho = \left(\frac{1}{2} - \frac{p}{2} + \frac{p}{2}\right)\mathbb{1}_2 + \frac{p}{2}\boldsymbol{r}\cdot\boldsymbol{\sigma} = \frac{\mathbb{1}_2 + p\boldsymbol{r}\cdot\boldsymbol{\sigma}}{2}. \tag{3.28}$$

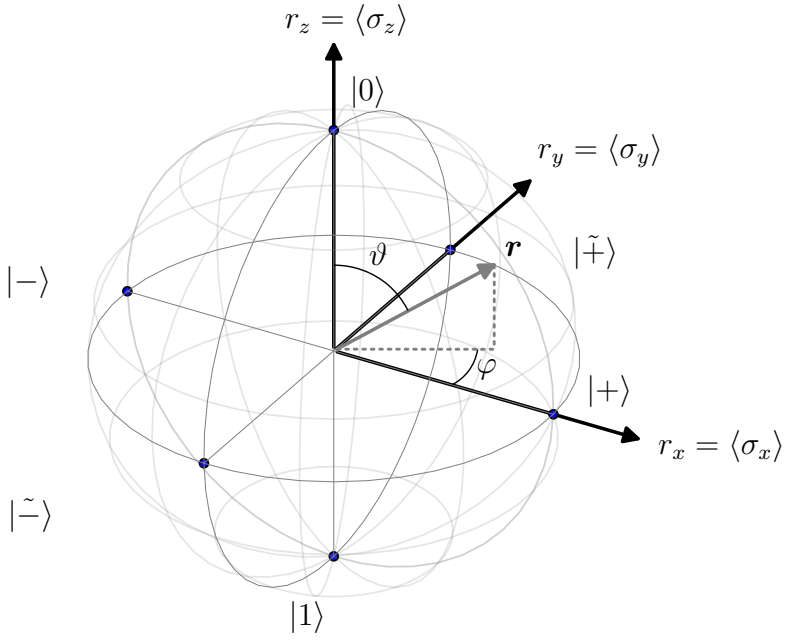


Figure 3.1: Representation of $\boldsymbol{r}$ on the Bloch sphere. $\boldsymbol{r}$ can be specified using spherical coordinates r, ϑ, φ. For pure states, $r = 1$.

So the length of the Bloch vector is reduced by a factor p, $\boldsymbol{s} = p\boldsymbol{r}$, by mixing the state with the probability $1 - p$ with the fully mixed state.

The geometric interpretation can be displayed on the Bloch sphere (Figure 3.1). We see that all mixed states are in the convex hull of the pure states located on the surface of the Bloch sphere. The set of all states of a qubit, mixed or pure, is said to form the "Bloch ball".

3.4 Single-qubit Quantum Gates

Single-qubit q-gates are unitary transformations on a single qubit.

Important examples of such unitary transforms are

- the Pauli matrices $X \equiv \sigma_x \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y \equiv \sigma_y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z \equiv \sigma_z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- the S or phase gate $S := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, where $S|0\rangle = |0\rangle, S|1\rangle = i|1\rangle$
- the T or $\frac{\pi}{8}$- gate $T := \begin{pmatrix} 1 & 0 \\ 0 & \exp\left\{i\frac{\pi}{4}\right\} \end{pmatrix}$ where $S = T^2$
- the Hadamard gate $H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(X + Z)$.

The Hadamard gate is an elementary gate for preparing superpositions, i.e. allowing for quantum interference, in the standard basis (computational basis $\{|0\rangle, |1\rangle\}$)). It acts as follows:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \tag{3.29}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle \ . \tag{3.30}$$

When applying an Hgate to each qubit of an n-qubit state (dimension of Hilbert space $d \equiv 2^n$) in an initial state $|00\ldots0\rangle$, we obtain

$$H^{\otimes n}|00\ldots0\rangle = H|0\rangle \otimes H|0\rangle \otimes \ldots \otimes H|0\rangle = \frac{1}{\sqrt{d}}(|0\rangle + |1\rangle)^{\otimes n} \tag{3.31}$$

$$= \frac{1}{\sqrt{d}}(|00\ldots0\rangle + |00\ldots1\rangle + \ldots + |11\ldots1\rangle) \tag{3.32}$$

$$= \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle \ . \tag{3.33}$$

This is used as a first step in almost all quantum algorithms!

The Xgate results in a qubit flip:

$$X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle \ . \tag{3.34}$$

This can be visualized on the Bloch sphere as a rotation by an angle π about the x-axis. The $|\pm\rangle$ states are eigenstates of X, and are therefore unaffected (up to a global phase factor (-1) in the case of $|-\rangle$). The states $|0\rangle, |1\rangle$, however, are located on the z-axis and are exchanged by X. X has the same effect, except for a global phase $\pm i$, on the $|\tilde{\pm}\rangle$ states located on the y-axis:

$$X|\tilde{\pm}\rangle = X(|0\rangle \pm i|1\rangle) = |1\rangle \pm i|0\rangle = \pm i(|0\rangle \mp i|1\rangle) = \pm i|\tilde{\mp}\rangle \ . \tag{3.35}$$

Z results in a phase flip

$$Z\left(a\left|0\right\rangle + b\left|1\right\rangle\right) = a\left|0\right\rangle - b\left|1\right\rangle \tag{3.36}$$

This is equivalent to a change of the phase $\varphi \to \varphi + \pi$, i.e. a rotation by angle π about the z-axis.

In general we have:

Theorem 2
An arbitrary unitary single qubit transform may be expressed as

$$U = \exp\left\{i\alpha\right\} R_{\hat{n}}(\theta) \tag{3.37}$$

where

$$R_{\hat{n}}(\theta) = \exp\left\{-i\theta\hat{n}\cdot\boldsymbol{\sigma}/2\right\} \tag{3.38}$$

represents the rotation operator by angle θ about the axis in direction of unit vector $\hat{n}$ (i.e. $\hat{n}^2 = 1$).

Proof.

See exercises. □

Quantum algorithms are often represented graphically as a so-called "quantum circuit". Usually, a set of qubits in their initial states is shown on the very left, but sometimes the initial states are also emitted. In the latter case, the quantum circuit represents just the unitary transformation, regardless of the initial state (see e.g. Fig.3.9), and hence, strictly speaking, not the entire quantum algorithm. The quantum gates are represented by boxes in which the kind of operation is written. The quantum circuit corresponding to the simple single-qubit circuit X acting on an initial state $|t\rangle$ is shown in Fig.3.2. We will find more complex quantum circuits in the following sections.

3.5 Controlled gates

Controlled gates are the quantum mechanical generalisation of an "if-then", but as reversible unitary gates. The simplest and also most important example is given by the *CNOT* gate (controlled *NOT*) that flips the value of the second bit if the value of the first bit is equal to 1. The first bit (number 1 in the standard verion)

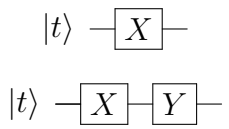


Figure 3.2: *Top:* Representation of the single-qubit X-gate as a quantum circuit, acting on state $|t\rangle$. *Bottom:* Quantum circuit representation of $YX\,|t\rangle$

$\|c\rangle$	$\|t\rangle$	$\|c\rangle$	$\|t \oplus c\rangle$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Table 3.1: Truth table for the *CNOT* gate, where a control bit conditions the bit flip of a target bit. An entry "0" means that the corresponding state is $|0\rangle$, and similarly for "1".

is called the *control bit*, which is always left unchanged. The second bit (number 2) is called the *target bit*:

$$|c\rangle\,|t\rangle \mapsto |c\rangle\,|t \oplus c\rangle \tag{3.39}$$

The truth table of the *CNOT* gate is given in Table 3.1. Due to the linearity of quantum mechanics, it is enough to specify the action on computational basis states, in which the *CNOT* has the matrix representation

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{3.40}$$

which is a manifestly unitary operation, $U_{CNOT}^2 = \mathbb{1}$, and thus reversible.

Its q-circuit representation is shown in Figure 3.3. The single dot in the first line represents a control that activates the gate on the target qubit iff the control qubit is $|1\rangle$. The vertical line indicates the direction of control, from control to target. The plus sign in the open circle on the last line is the standard notation used for the action of the X gate on the target in the CNOT gate.

More generally, a controlled single-qubit unitary is represented by a q-circuit as in Figure 3.4, and has a matrix representation in the computational basis

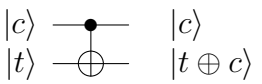


Figure 3.3: q-circuit representation of the controlled NOT gate, i.e. $CNOT$ gate.

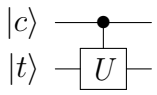


Figure 3.4: General q-circuit of a controlled unitary operation U, i.e. cUgate.

$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

$$U_{cU} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & & \\ 0 & 0 & & U \end{pmatrix}, \tag{3.41}$$

where U is a 2×2 block. E.g. for a CNOT, $U = X$. One step further into the more general direction, one can imagine multiply controlled gates acting on several other gates, e.g. with control bits $|c_1\rangle, \ldots, |c_4\rangle$ and target bits $|t_1\rangle, \ldots, |t_3\rangle$ (Figure 3.5):

Example 2 (Toffoli gate)
An important example is the Toffoli gate, a doubly controlled NOT, which flips the target bit if $|c_1\rangle = |c_2\rangle = |1\rangle$*, see Figure 3.6 and the corresponding truth table.*

The truth table is exactly the one from the classical Toffoli gate which we have seen as a reversible version of the NAND gate, but now the truth table is to be understood as a 8×8 matrix representing a unitary transformation that acts on vectors in the Hilbert space of three qubits. The truth table in Fig.3.6 is abbreviated, only c_1, c_2 and t_{out} are shown, while $t_{\text{in}} \in \{0, 1\}$ is kept as a free variable.

Example 3
Another example is a NOT gate controlled by two control bits, where the target bit is flipped if one control bit is zero and the second control bit is one, i.e. $|c_1\rangle = 0$ *and* $|c_2\rangle = 1$*, the corresponding q-circuit and the truth table are shown in Figure 3.7. A control needing a* $|0\rangle$ *for activation is denoted by a small open circle.*

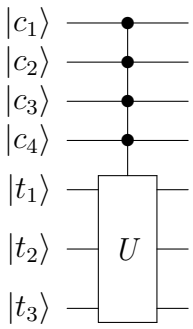
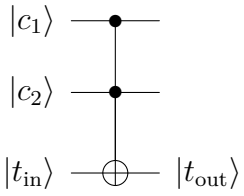


Figure 3.5: q-circuit representation of a multiply controlled gate acting on multiple bits, 4 control bits and 3 target bits.



$\lvert c_1\rangle$	$\lvert c_2\rangle$	$\lvert t_{\text{out}}\rangle$
0	0	$\lvert t_{\text{in}}\rangle$
0	1	$\lvert t_{\text{in}}\rangle$
1	0	$\lvert t_{\text{in}}\rangle$
1	1	$\lvert 1 \oplus t_{\text{in}}\rangle$

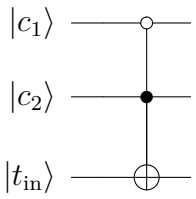
Figure 3.6: The q-circuit and truth table of the Toffoli gate.

3.6 Concatenation of gates: q-circuits

A concatenation of gates is a sequence of unitaries acting on the selected qubits, e.g. the quantum circuit in (Figure 3.8) means applying the Hadamard gate on qubit 1, followed by the U_{CNOT} on qubits 1 and 2, i.e.

$$U_{CNOT}(1,2)U_H(1) \tag{3.42}$$

where qubit 1 is the control bit and qubit 2 the target of the unitary. Propagation of the state in time from one quantum gate to the next, i.e. without changing the state, is represented by straight lines ("quantum wires"). Time runs from left to right, such that the order of matrices in the matrix-product representing the q-circuit is flipped compared to the order in the quantum circuit itself. In other words, when translating the quantum circuit into an equation, the operators or matrices representing the quantum gates are written in the opposite order in which they appear in the graphical representation of the quantum circuit, with the initial quantum state on which they act on the right, as usual. E.g. the second quantum circuit in Fig.3.2 gives an output state $|\psi'\rangle = YX\,|t\rangle$.



$\|c_1\rangle$	$\|c_2\rangle$	$\|t_{\text{out}}\rangle$
0	0	$\|t_{\text{in}}\rangle$
0	1	$\|1 \oplus t_{\text{in}}\rangle$
1	0	$\|t_{\text{in}}\rangle$
1	1	$\|t_{\text{in}}\rangle$

Figure 3.7: The q-circuit and truth table of a *NOT* gate on one target bit controlled by two control bits, where $|c_1\rangle$ has to be zero and $|c_2\rangle$ has to be one.

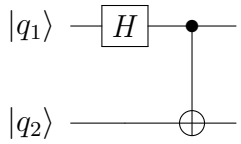


Figure 3.8: Example of a simple q-circuit. Time runs from left to right.

Example 4
Using H gates, on can invert the control and the target bit of the CNOT, see Fig.3.9.

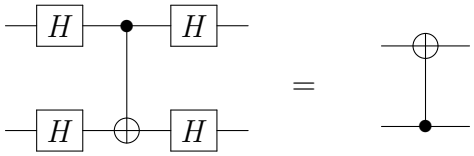


Figure 3.9: Swapping of the control and the target bit of a *CNOT* gate using multiple Hgates. Both q-circuits are identical.

Proof.

We can show this by calculating the action of both q-circuits on all four possible

combinations of the computational basis states for the two qubits involved:

$$|00\rangle \xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \xrightarrow{CNOT} \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \xrightarrow{H} |00\rangle \tag{3.43}$$

$$|01\rangle \xrightarrow{H} \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \xrightarrow{CNOT} \frac{1}{2}(|00\rangle - |01\rangle + |11\rangle - |10\rangle) \xrightarrow{H} |11\rangle \tag{3.44}$$

$$|10\rangle \xrightarrow{H} \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle + |1\rangle) \xrightarrow{CNOT} \frac{1}{2}(|00\rangle - |11\rangle + |01\rangle - |10\rangle) \xrightarrow{H} |10\rangle \tag{3.45}$$

$$|11\rangle \xrightarrow{H} \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \xrightarrow{CNOT} \frac{1}{2}(|00\rangle - |01\rangle - |11\rangle + |10\rangle) \xrightarrow{H} |01\rangle \tag{3.46}$$

This behaviour is exactly the definition of the *CNOT* gate with an exchanged control and target bit, i.e. qubit 1 is now the target qubit and qubit 2 the control qubit. □

3.7 Universal gate sets

A small set of classical gates (e.g. $\wedge$, $\vee$, $\neg$) can be used to construct any classical logical function on a arbitrary number of (classical) bits. Is there something similar for q-computing? The answer is: Yes! This is made more precise by the following theorem that we are going to prove:

Theorem 3 (Universal set)
Any unitary operation can be expressed exactly using single qubit unitaries and CNOT gates.

Proof.

For this proof, we need to make use of two additional lemmas.

Lemma 1
2-level unitaries are universal.

Proof (Lemma 1).

2-level unitaries are unitaries that act only on two states (*levels*) at the same time.

This is demonstrated with the help of a 3×3 unitary

$$U = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix} \tag{3.47}$$

We will show that $\exists\ U_1, U_2, U_3$ so that $U_3 U_2 U_1 U = \mathbb{1}$, which implies $U = U_1^\dagger U_2^\dagger U_3^\dagger$, where U_i are all 2-level unitaries, which implies that $U_i^\dagger$ is also a 2-level unitary.

The three U_i are constructed in the following manner

- if $b = 0$, then choose $U_1 = \mathbb{1}$
- if $b \neq 0$, then choose

$$U_1 = \frac{1}{\sqrt{|a|^2 + |b|^2}} \begin{pmatrix} a^* & b^* & 0 \\ b & -a & 0 \\ 0 & 0 & \sqrt{|a|^2 + |b|^2} \end{pmatrix}, \tag{3.48}$$

where U_1 is obviously a 2-level unitary, i.e. acting non-trivially only on levels one and two. Multiplying U_1 with U yields

$$U_1 U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix} \tag{3.49}$$

where we created the 0 in the first column through our construction. We continue in the same manner for U_2, i.e.

- if $c' = 0$, then choose $U_2 = \mathrm{diag}\,(a'^*, 1, 1)$
- if $c' \neq 0$, then choose

$$U_2 = \frac{1}{\sqrt{|a'|^2 + |c'|^2}} \begin{pmatrix} a'^* & 0 & c'^* \\ 0 & \sqrt{|a'|^2 + |c'|^2} & 0 \\ c' & 0 & -a' \end{pmatrix}, \tag{3.50}$$

where again U_2 is obviously a 2-level unitary, this time only acting non-trivially on levels one and three. The product of the matrices U, U_1, U_2 yields

$$U_2 U_1 U = \begin{pmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix}. \tag{3.51}$$

Since U, U_1, U_2 are unitary, $U_2 U_1 U$ is also unitary and hence $d'' = g'' = 0$, as the norm of the first row must be equal to 1.

Now choose U_3 as

$$U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{pmatrix} \tag{3.52}$$

i.e. as the hermitian conjugate and hence the inverse of the block matrix in the lower right corner of $U_2 U_1 U$.

This results in $U_3 U_2 U_1 U = \mathbb{1}$ and therefore $U = U_1^\dagger U_2^\dagger U_3^\dagger$ as claimed.

Now suppose we have a $d \times d$ unitary. Then one can find $U_1, \ldots, U_{d-1}$, such that $U_{d-1} U_{d-2} \ldots U_1 U$ has a 1 in the top left corner and otherwise zeros in the first row and first column. Continue then with the $(d-1) \times (d-1)$ lower right block in the same way, and so on. This way, we get in the end $U = V_1 \cdot \ldots \cdot V_k$ where V_i are unitaries and $k \leq (d-1) + (d-2) + \ldots + 1$, i.e. $k \leq d/2(d-1)$ 2-level unitaries. □

Lemma 2 (Implementation via the universal set)
An arbitrary 2-level unitary can be implemented using single qubit gates and CNOT gates.

Proof (Lemma 2).

Suppose we want to implement the two-level unitary $\tilde{U}$ between basis states s and t, with binary adresses $(s_{n-1}, \ldots, s_0)$, $(t_{n-1}, \ldots, t_0)$ where $s_i, t_i \in \{0, 1\}$. The idea is to swap basis states until these 2 addresses differ only in one bit, then perform the unitary on that bit conditioned on the values of all the other bits. Take as an example $s = 000, t = 111$. We swap basis states until we have for example mapped $s \to 011$, and then apply $\tilde{U}$ on the first qubit, conditioned on the value 11 of qubits 2,3. Swapping the basis states can be done by flipping one bit at a time, conditioned on the values of the other bits[1]. This defines a series of so called *Gray codes*. So in the example we follow the Gray codes $(ABC) = 000 \to 001 \to 011$; this can be achieved using the q-circuit in Figure 3.10. It is reminded, that empty circles are controls that activate iff the qubit is in the state $|0\rangle$ and filled circles are controls that activate iff the qubit is in the state $|1\rangle$. But a multiply controlled $\tilde{U}$ with some controls activated by $|0\rangle$ can always be reduced to a multiply controlled $\tilde{U}$ with standard control bits conditioned on the state $|1\rangle$, simply by flipping the control qubit before the controlled $\tilde{U}$ and flipping it back again afterwards, see e.g. Figure 3.11.

[1] Note that these are classical labels of computational basis states, not the basis states themselves, so they are known.

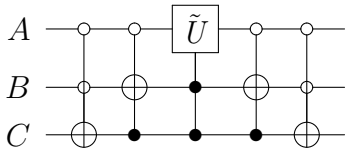


Figure 3.10: Example for the q-circuit implementation of Gray codes from $000 \rightarrow 011$, then applying $\tilde{U}$ controlled with the rest of the qubits and then following the Gray codes again in reverse order to restore the original ordering of the state, i.e. $\tilde{U}$ is applied between $|000\rangle$ and $|111\rangle$.

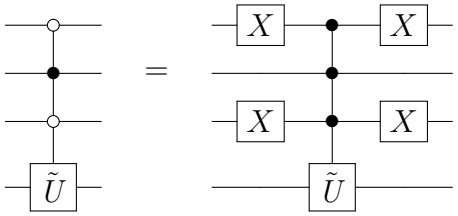


Figure 3.11: Conversion of a multiply controlled $\tilde{U}$ gate with control bits conditioned on the states $|0\rangle$ and $|1\rangle$ to a standard multiply controlled gate using only control bits conditioned on $|1\rangle$.

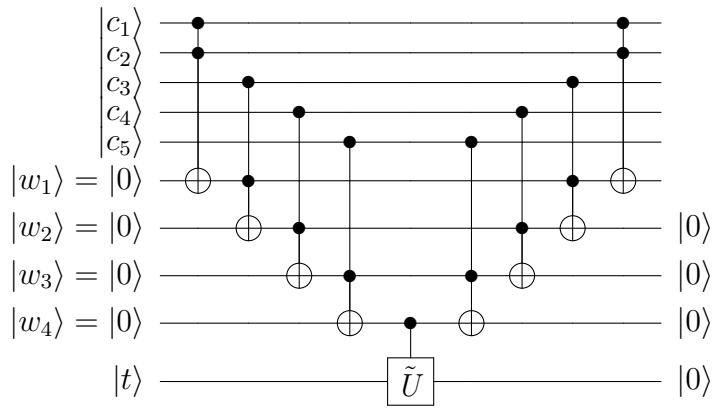


Figure 3.12: Conversion of a standard multiply controlled $\tilde{U}$ gate to a simply controlled gate using only control bits conditioned on $|1\rangle$.

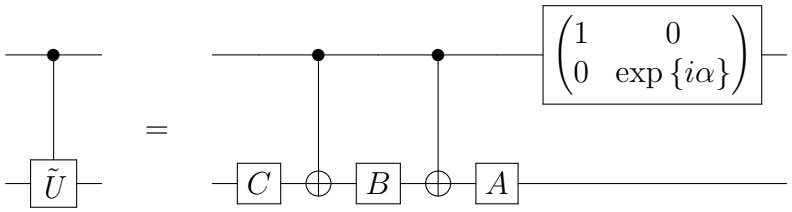


Figure 3.13: q-circuit representation of the controlled-$\tilde{U}$ gate using A, B, C and a controlled phase shift gate, i.e. only $CNOT$ gates and single qubit unitaries.

A standard multiply controlled $\tilde{U}$ (with m control bits conditioned on $|1\rangle$) can be constructed from $2(m-1)$ Toffoli gates using $m-1$ work qubits initialised in $|0\rangle \ldots |0\rangle$ and returned in $|0\rangle \ldots |0\rangle$ after the calculation, and an additional single-qubit-controlled $\tilde{U}$, see Figure 3.12. To achieve this, the first gate inscribes $c_1 \cdot c_2$ into $|w_1\rangle$. The second gate then takes $c_1 \cdot c_2$ and c_3 and inscribes $c_1 \cdot c_2 \cdot c_3$ into $|w_2\rangle$ and so on. In the end $\tilde{U}$ is controlled by $c_1 c_2 c_3 c_4 c_5$.

So now we are down to Toffoli gates and only single-qubit-controlled $\tilde{U}$. The latter can be implemented as shown in Figure 3.13, where $\tilde{U} = \exp\{i\alpha\} AXBXC$, $ABC = \mathbb{1}$. Such a decomposition for $\tilde{U}$ is always possible.

Proof (Decomposition of the controlled $\tilde{U}$).

One first shows that $\tilde{U} = \exp\{i\alpha\} R_z(\beta)R_y(\gamma)R_z(\delta)$ (Euler angle decomposition). Straight forward multiplication gives

$$\tilde{U} = \begin{pmatrix} \exp\{i(\alpha-\beta/2-\delta/2)\}\cos\left(\frac{\gamma}{2}\right) & -\exp\{i(\alpha-\beta/2+\delta/2)\}\sin\left(\frac{\gamma}{2}\right) \\ \exp\{i(\alpha+\beta/2-\delta/2)\}\sin\left(\frac{\gamma}{2}\right) & \exp\{i(\alpha+\beta/2+\delta/2)\}\cos\left(\frac{\gamma}{2}\right) \end{pmatrix} \tag{3.53}$$

which is the most general representation of a 2×2 unitary. We now set

$$A = R_z(\beta) R_y\left(\frac{\gamma}{2}\right) \tag{3.54}$$

$$B = R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta+\beta}{2}\right) \tag{3.55}$$

$$C = R_z\left(\frac{(\delta-\beta)}{2}\right) \tag{3.56}$$

$$ABC = R_z(\beta) \underbrace{R_y\left(\frac{\gamma}{2}\right) R_y\left(-\frac{\gamma}{2}\right)}_{=\mathbb{1}} \underbrace{R_z\left(-\frac{\delta+\beta}{2}\right) R_z\left(\frac{\delta-\beta}{2}\right)}_{=R_z(-\beta)} = \mathbb{1} \tag{3.57}$$

Also one finds by calculation

$$-Y = XYX \tag{3.58}$$

$$Y^2 = (XYX)(XYX) \tag{3.59}$$

$$\Rightarrow (-Y)^n = XY^nX \tag{3.60}$$

$$\Rightarrow XR_y(\theta)X = \sum_{n=0}^{\infty} \frac{1}{n!} X \left(iY\frac{\theta}{2}\right)^n X = R_y(-\theta) \tag{3.61}$$

and in the same manner

$$XR_z(\theta)X = R_z(-\theta), \tag{3.62}$$

resulting in

$$AXBXC = R_z(\beta) R_y\left(\frac{\gamma}{2}\right) XR_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta+\beta}{2}\right) XR_z\left(\frac{\delta-\beta}{2}\right) \tag{3.63}$$

$$= R_z(\beta) R_y\left(\frac{\gamma}{2}\right) XR_y\left(-\frac{\gamma}{2}\right) X\,X\, R_z\left(-\frac{\delta+\beta}{2}\right) XR_z\left(\frac{\delta-\beta}{2}\right) \tag{3.64}$$

$$= R_z(\beta)R_y(\gamma)R_z(\delta). \tag{3.65}$$

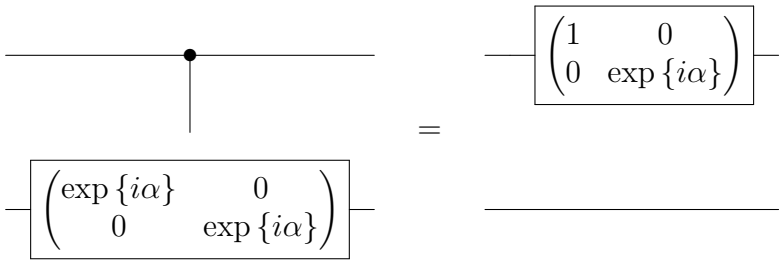


Figure 3.14: Equivalent q-circuit for a controlled phase gate and the alternative 2×2 unitary.

This yields

$$\tilde{U} = \exp\{i\alpha\} AXBXC\,. \tag{3.66}$$

Here, (3.65) is obtained from (3.63) by inserting $\mathbf{1} = X^2$ after $R_y(-\gamma/2)$ and using (3.61), and (3.62) for the following $R_z(-\frac{\delta+\beta}{2})$.

As a last gate, the decomposition of the controlled $\tilde{U}$ requires the controlled phase shift, which is equal to the gate operation in Figure 3.14, as can be seen by looking how it affects different states (truth table): $|00\rangle \to |00\rangle$, $|01\rangle \to |01\rangle$, $|10\rangle \to \exp\{i\alpha\}|10\rangle$ and $|11\rangle \to \exp\{i\alpha\}|11\rangle$. In Fig.3.13, the controlled phase shift was replaced already correspondingly by the single-qubit gate acting on the control qubit.

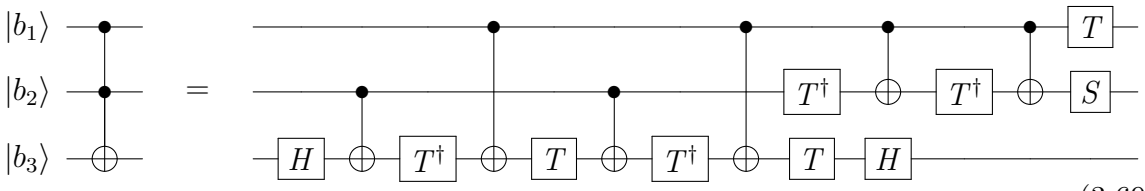
(End of the proof "Decomposition of the controlled $\tilde{U}$") □

Continuing the breaking down of multiply controlled unitaries, we note that the Toffoli gate (Figure 3.10) can itself be broken down into $\left\{H,\, T,\, T^\dagger,\, S,\, CNOT\right\}$, as shown in Figure 3.15.

Recall that the S and T gates can be represented in the computational basis by matrices

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \exp\{i\pi/4\} \end{pmatrix} \tag{3.67}$$

$$S = T^2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\,. \tag{3.68}$$



(3.69)

Figure 3.15: Decomposition of the Toffoli gate into *CNOT* gates and single qubit gates.

Proof (Decomposition Toffoli gate).

The validity of the decomposition can be shown through explicit calculation, where

$$|b_1\rangle \to T\,|b_1\rangle \tag{3.70}$$

gives

$$|0\rangle \to T\,|0\rangle = |0\rangle \tag{3.71}$$
$$|1\rangle \to T\,|1\rangle = \exp\{i\pi/4\}\,|1\rangle\,. \tag{3.72}$$

This result has to be combined with the (controlled) operations on $|b_2\rangle$ and $|b_3\rangle$

$$|0\rangle\,|b_2\rangle \to |0\rangle\,S\left(T^\dagger\right)^2|b_2\rangle = |0\rangle\,|b_2\rangle \tag{3.73}$$
$$|1\rangle\,|b_2\rangle \to \exp\{i\pi/4\}\,|1\rangle\,SXT^\dagger XT^\dagger\,|b_2\rangle = |1\rangle\,S\,|b_2\rangle \tag{3.74}$$
$$= |1\rangle \begin{pmatrix} 1 & 0 \\ 0 & \exp\{i\pi/2\} \end{pmatrix} |b_2\rangle \tag{3.75}$$

where we made use of the relation

$$XT^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \exp\{-i\pi/4\} \end{pmatrix} = \begin{pmatrix} 0 & \exp\{-i\pi/4\} \\ 1 & 0 \end{pmatrix} \tag{3.76}$$
$$\Rightarrow \left(XT^\dagger\right)^2 = \exp\{-i\pi/4\}\,\mathbb{1}. \tag{3.77}$$

Finally this result also has to be combined with the (controlled) operations on $|b_3\rangle$:

$$|0\rangle\,|0\rangle\,|b_3\rangle \to |0\rangle\,|0\rangle\,|b_3\rangle \tag{3.78}$$
$$|0\rangle\,|1\rangle\,|b_3\rangle \to |0\rangle\,|1\rangle\,HTT^\dagger XTT^\dagger XH\,|b_3\rangle = |0\rangle\,|1\rangle\,|b_3\rangle \tag{3.79}$$
$$|1\rangle\,|0\rangle\,|b_3\rangle \to |1\rangle\,\underbrace{S\,|0\rangle}_{=|0\rangle}\,\underbrace{HTXT^\dagger TXT^\dagger H}_{=\mathbb{1}}\,|b_3\rangle = |1\rangle\,|0\rangle\,|b_3\rangle \tag{3.80}$$
$$|1\rangle\,|1\rangle\,|b_3\rangle \to \exp\{i\pi/2\}\,|1\rangle\,|1\rangle\,\underbrace{HTXT^\dagger XTXT^\dagger XH}_{=\exp\{-i\pi/2\}X}\,|b_3\rangle = |1\rangle\,|1\rangle\,X\,|b_3\rangle \tag{3.81}$$

(3.82)

The last relation(s) were obtained by direct multiplication. As we can see, the substitute q-circuit exhibits the same effects on the qubits as the Toffoli gate. Because of the linearity of the operation(s), it is sufficient to show the effects of the operations on all computational basis states to also proof the equivalence of the substitute circuit for an arbitrary superposition of computational basis states and hence any state in the full Hilbert space of three qubits.

(End of decomposition of Toffoli gate proof)

□

This way, U is implemented *exactly* as a sequence of single qubit unitaries and $CNOT$ gates.

(End of decomposition of 2-level unitaries proof) □

(End of universal set proof) □

To summarise, for N qubits we start with

- a unitary operation $U\left(2^N \times 2^N\right)$, which undergoes
- decomposition into 2-level unitaries $\tilde{U}$. These can be implemented as
- multiply-controlled single qubit gates by using sequences of Gray codes for bringing the two levels between which one wants to implement the 2-level unitary next to each other in the sequence of binary labels so that they differ only by one bit. This re-ordering can itself be done by multiply-controlled single-qubit-NOT gates. Any of these multiply-controlled single-qubit gates is then substituted by
- Toffoli gates and single-qubit-controlled $\tilde{U}$ gates, i.e. $c\tilde{U}$ gates. For these we find equivalent q-circuits
- using $\left\{CNOT, T, T^\dagger, S, H\right\}$ for the Toffoli gate, and $\{CNOT, A, B, C\}$ for the single-qubit-controlled $c\tilde{U}$.

The number of gates required is estimated as follows:

- $\mathcal{O}\left(2^{2n}\right)$ 2-level unitaries (or $\mathcal{O}\left(d^2\right)$ where $d = 2^n$)

- $\mathcal{O}(n)$ Gray-code swaps for each 2-level unitary. A Gray-code swap is a multiply-controlled NOT. With $n-1$ controls, each Gray-code swap needs $\mathcal{O}(n)$ Toffoli gates, and thus we need $\mathcal{O}(n^2)$ $CNOT$ gates and single qubits gates for each 2-level unitary.

Hence, with such a universal decomposition, altogether $\sim \mathcal{O}(n^2 4^n)$ gates are required. So, in general, this is not very efficient. The art of quantum programming consists in finding a quantum algorithm in the form of a unitary U that does the job and requires a much smaller number of elementary gates.

Note

A, B, C need a continuous family of single qubit unitaries. An approximate representation of an arbitrary U can be found from the discrete set of gates $\{H, S, CNOT, T\}$. The *Solovay-Kitaev theorem* implies that a q-circuit consisting of m $CNOT$ gates and single qubit gates can be approximated to an accuracy ε using $\mathcal{O}(m \log^c(m/\varepsilon))$ gates from the discrete set, with $c \simeq 2$. The accuracy ε is defined through

$$E(U,V) = \max_{|\psi\rangle} || (U-V)|\psi\rangle || < \varepsilon \,. \tag{3.83}$$

The first universal set of quantum gates was discovered by Deutsch [14] in 1985 based on Toffoli gates and single-qubit unitaries. DiVincenzo [16] and Barenco et al. [1, 2] provided a universal set with $CNOT$gates and single qubit unitaries in 1995.

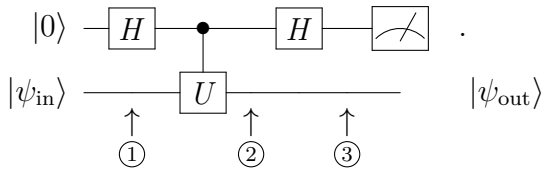
3.8 Measurements

A q-circuit ends with a projective measurement, indicated by the symbol

(3.84)

supposed to symbolize a good old-fashioned measurement device with pointer and scale. *Projective* refers to a projective measurement of the qubit in the computational basis, i.e. a measurement which gives different results for $|0\rangle$ and $|1\rangle$ and which projects on these state. In general, $\sigma_z = Z$ is used yielding $+1$ or -1 for $|0\rangle$ or $|1\rangle$, respectively.

Measurements in a basis different from the computational basis can always be realised using a preceding unitary transformation. Let e.g. U be a unitary transformation that is also hermitian, i.e. $U^\dagger = U, U^\dagger U = \mathbb{1}$ (as for Pauli matrices). Then U can be used as a unitary transformation or as an observable with eigenvalues $\lambda_i = \pm 1$. Measuring U can be done using an additional qubit starting in state $|0\rangle$, which is then measured in the computational basis using the following q-circuit:



(3.85)

Proof.

Starting with

$$|\psi_{\text{in}}\rangle = a\,|0\rangle + b\,|1\rangle \tag{3.86}$$

the states after each operation are:

$$|\psi_{①}\rangle = H\,|0\rangle\,|\psi_{\text{in}}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|\psi_{\text{in}}\rangle \tag{3.87}$$

$$|\psi_{②}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle\,|\psi_{\text{in}}\rangle + |1\rangle\;U\,|\psi_{\text{in}}\rangle\right) \tag{3.88}$$

$$|\psi_{③}\rangle = \frac{1}{2}\left(\left(|0\rangle + |1\rangle\right)|\psi_{\text{in}}\rangle + \left(|0\rangle - |1\rangle\right)U\,|\psi_{\text{in}}\rangle\right) \tag{3.89}$$

$$= \frac{1}{2}\left(|0\rangle\left(\mathbb{1} + U\right)|\psi_{\text{in}}\rangle + |1\rangle\left(\mathbb{1} - U\right)|\psi_{\text{in}}\rangle\right). \tag{3.90}$$

With the spectral decomposition of U

$$U = (+1)\cdot|u_+\rangle\langle u_+| + (-1)\cdot|u_-\rangle\langle u_-| \tag{3.91}$$

and expressing $|\psi_{\text{in}}\rangle$ in the basis of the eigenvectors of U

$$|\psi_{\text{in}}\rangle = \psi_+\,|u_+\rangle + \psi_-\,|u_-\rangle \tag{3.92}$$

the following holds:

$$U\,|\psi_{\text{in}}\rangle = \psi_+\,|u_+\rangle - \psi_-\,|u_-\rangle\,. \tag{3.93}$$

Using

$$\mathbb{1} = |u_+\rangle\langle u_+| + |u_-\rangle\langle u_-| \tag{3.94}$$

$$\Rightarrow \mathbb{1} + U = 2\,|u_+\rangle\langle u_+| \tag{3.95}$$

$$\mathbb{1} - U = 2\,|u_-\rangle\langle u_-|\,, \tag{3.96}$$

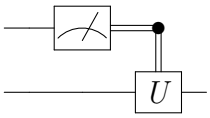
So we can evaluate (3.90) to

$$|\psi_{③}\rangle = \psi_+ |0\rangle |u_+\rangle + \psi_- |1\rangle |u_-\rangle \tag{3.97}$$

If we measure 0 in the first qubit, then the state collapses to $|0\rangle |u_+\rangle$, and analogously, if we measure 1 in the first qubit, then the state collapses to $|1\rangle |u_-\rangle$.

The probability of measuring 0 or 1 is given by the squared overlap of the original state with the collapsed state, i.e. $|\psi_+|^2$ or $|\psi_-|^2$ as desired. □

Results from measurements can be used to affect the course of a q-circuit. We use the notation = for classical information in a q-circuit, as shown in the following example

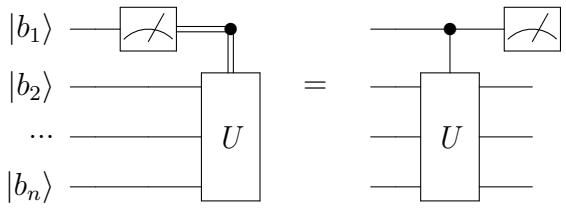


(3.98)

where we apply U to the second qubit if the measurement of the first qubit resulted in 1.

3.8.1 Principle of Deferred Measurements

Measurements can always be moved towards the end of a q-algorithm. If measurement results are used within the algorithm (classical information as input), it is sufficient to substitute any logical controlled operation which uses classical information by its quantum counterpart. For example



(3.99)

To proof this principle, we have to show that

- both q-circuits yield the same statistics for their measurement results, and
- both q-circuits yield the same state at the end of the circuit.

Proof.

We start with the arbitrary state $|\psi\rangle$.

left hand-side:
$|\psi\rangle$ evaluates as

$$|\psi\rangle = (P_0 + P_1)\,|\psi\rangle \tag{3.100}$$

where $P_i, i = 1, 2$ are the projectors onto the subspaces for $b_1 = 0 (i = 0)$ or $b_1 = 1 (i = 1)$. The density matrix of the system after the measurement is given by

$$W = p_0 P_0\,|\psi\rangle\langle\psi|\,P_0 + p_1 P_1\,|\psi\rangle\langle\psi|\,P_1 \tag{3.101}$$

where p_i denote the probabilities $p_i = \|P_i\,|\psi\rangle\|^2$ for $i = 1, 2$. After applying U on $|b_2\rangle, \ldots, |b_n\rangle$ (iff $b_1 = 1$), the density matrix is

$$W' = p_0 P_0\,|\psi\rangle\langle\psi|\,P_0 + p_1 \left(\mathbb{1}_2 \otimes U\right) P_1\,|\psi\rangle\langle\psi|\,P_1 \left(\mathbb{1}_2 \otimes U^\dagger\right) \tag{3.102}$$

where the $\mathbb{1}_2$ operator is a 2×2 matrix, operating only on first qubit and U operates on all the other qubits, i.e. is a $2^{n-1} \times 2^{n-1}$ matrix.

right hand-side:
The state of the system after applying cU is given by

$$|\psi'\rangle = cU\,|\psi\rangle \tag{3.103}$$

and we claim: $cU = P_0 + P_1\,(\mathbb{1}_2 \otimes U)\,P_1$. Indeed, we can always decompose cU as

$$\begin{aligned} cU &= (P_0 + P_1)\,cU\,(P_0 + P_1) && (3.104)\\ &= P_0 cU P_0 + P_1 cU P_1 + P_0 cU P_1 + P_1 cU P_0 && (3.105)\\ &= \underbrace{P_0 \mathbb{1}_{2^n} P_0}_{=P_0^2 = P_0} + P_1 \mathbb{1}_2 \otimes U P_1 + \underbrace{P_1 \mathbb{1}_{2^n} P_0 + P_0 \mathbb{1}_2 \otimes U P_1}_{=0} && (3.106) \end{aligned}$$

where the second two terms vanish, as neither $\mathbb{1}$ nor $\mathbb{1}_2 \otimes U$ connect different subspaces, i.e. $\mathbb{1}_2 \otimes U P_1$, is still an operator in the subspace onto which P_1 projects such that $P_0 \mathbb{1}_2 \otimes U P_1 = 0$, and correspondingly for $P_1 \mathbb{1}_{2^n} P_0$. Hence

$$cU = P_0 + P_1(\mathbb{1}_2 \otimes U)P_1 \tag{3.107}$$

as claimed. This results in a state for the whole system of

$$|\psi'\rangle = \left(P_0 + P_1 \mathbb{1}_2 \otimes U P_1\right)|\psi\rangle\,. \tag{3.108}$$

Since the probability to find $i = 0, 1$ in a measurement of the first qubit is $\tilde{p_0} = \|P_0 |\psi\rangle\|^2$, $\tilde{p_1} = \|P_1(\mathbb{1} \otimes U)P_1 |\psi\rangle\|^2$, we find:

$$\tilde{p_0} = \langle\psi|P_0|\psi\rangle = p_0 \tag{3.109}$$

$$\tilde{p_1} = \langle\psi|P_1 \left(\mathbb{1}_2 \otimes U^\dagger\right) P_1 P_1 \left(\mathbb{1}_2 \otimes U\right) P_1|\psi\rangle \tag{3.110}$$

$$= \langle\psi|P_1 \left(\mathbb{1} \otimes U^\dagger\right) P_1 \left(\mathbb{1}_2 \otimes U\right) P_1|\psi\rangle \tag{3.111}$$

$$= \langle\psi|P_1 \underbrace{\left(\mathbb{1}_2 \otimes U^\dagger\right)\left(\mathbb{1}_2 \otimes U\right)}_{=\mathbb{1}} P_1|\psi\rangle \tag{3.112}$$

$$= \langle\psi|P_1^2|\psi\rangle = \langle\psi|P_1|\psi\rangle = p_1. \tag{3.113}$$

In (3.111) we used the fact that $(\mathbb{1}_2 \otimes U)P_1 |\psi\rangle)$ is still in the subspace onto which P_1 projects, so that $P_1(\mathbb{1} \otimes U)P_1 |\psi\rangle = (\mathbb{1} \otimes U)P_1 |\psi\rangle$. (3.109) and (3.113) show that the measurement statistics of both q-circuits are the same.

This leaves us with proofing the equality of states after the measurement(s), which are

$$\tilde{W'} = p_0 P_0 |\psi'\rangle \langle\psi'| P_0 + p_1 P_1 |\psi'\rangle \langle\psi'| P_1 \tag{3.114}$$

$$= p_0 P_0 |\psi\rangle \langle\psi| P_0 + p_1 \underbrace{P_1 \left(\mathbb{1} \otimes U\right) P_1 |\psi\rangle}_{=(\mathbb{1}\otimes U)P_1|\psi\rangle} \langle\psi| P_1 \left(\mathbb{1} \otimes U^\dagger\right) P_1 \tag{3.115}$$

$$= W' \tag{3.116}$$

which is the same state as in eq.(3.102).

□

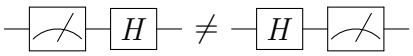
Note

U must operate on unmeasured (uncollapsed) qubits only; otherwise the proof and the principle do not hold.

Example 5

To illustrate the Note consider the two q-circuits in (Figure 3.16). They are not *equivalent, as one quickly realizes when propagating a single basis state, say* $|0\rangle$. *On the left-hand side we have*

$$|0\rangle \xrightarrow{\boxed{}} \{|0\rangle, p_0 = 1\} \xrightarrow{\boxed{H}} (|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}, \tag{3.118}$$



(3.117)

Figure 3.16: Two q-circuits for which the principle of deferred measurement does not hold, i.e. these q-circuits are not equal.

whereas on the right-hand side the created superposition results in a different distribution of probabilities

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \xrightarrow{} \left\{\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)\frac{1}{2}, p_0 = \frac{1}{2}\right\} \tag{3.119}$$

3.8.2 Principle of Implicit Measurements

Without loss of generality any open quantum wire at the end of a q-circuit can be treated as being measured.

Proof.

Any open threaded qubit can be measured after the measurement of any explicitly measured qubit. Because the measurement happens after the explicit measurements, it is unable to influence the results of the former measurements (the already collapsed states). □

Note

Measuring two qubits sequentially is in general not equivalent to a joint measurement of both of them. E.g. an observable $Z_1 Z_2 \equiv Z_1 \otimes Z_2$ is not the same as the set of observables $\{Z_1, Z_2\} \equiv \{Z_1 \otimes \mathbf{1}_2, \mathbf{1}_2 \otimes Z_2\}$. This will become important when we talk about quantum error correction.

4 Quantum Algorithms

4.1 Evaluating a Function in Parallel

Let $f(x)$ be a function $x \mapsto f(x) \in \{0,1\}$ where $x \in \{0,1\}^n$ for an integer number n. We look for a unitary transformation U_f that acts accordingly on states $|x,y\rangle := |x\rangle\,|y\rangle$, where $|x\rangle$ is a state of a register of n qubits and $|y\rangle$ the state of a single qubit. After the action of U_f, we want the value $f(x)$ stored in the y-qubit. To make the transformation reversible, we can achieve this via a unitary transformation that acts as

$$|x,y\rangle \mapsto U_f\,|x,y\rangle = |x, y \oplus f(x)\rangle = |x, (y + f(x)) \text{mod } 2\rangle \tag{4.1}$$

where the $XOR\ \oplus$ is equivalent to binary addition modulo 2.

Example 6

$$|0,0\rangle \mapsto |0, f(0)\rangle \tag{4.2}$$
$$|0,1\rangle \mapsto |0, (1 + f(0)) \text{mod } 2\rangle \tag{4.3}$$
$$|1,0\rangle \mapsto |1, f(1)\rangle \tag{4.4}$$
$$|1,1\rangle \mapsto |1, (1 + f(1)) \text{mod } 2\rangle\ . \tag{4.5}$$

One checks that independently of the values of $f(0)$ and $f(1)$, U_f acts as a permutation of all computational basis states and is hence indeed a unitary transformation, and in particular reversible. In addition, with U_f being linear, we also have

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|0\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0, f(0)\rangle + |1, f(1)\rangle\right). \tag{4.6}$$

The last result reflects the superposition of the two possible results, $f(0)$ and $f(1)$, which was evaluated in parallel. More generally for n qubits as input x,

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, 0\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle\,. \tag{4.7}$$

This demonstrates the " quantum parallelism " of the computation: the function f is evaluated for all possible input states in parallel. However, as such this is not useful yet, as we do not know how to extract all the results from the final state. Measuring the $|x\rangle$ register results in a collapse of the state on some random $|x\rangle |f(x)\rangle$, i.e. we only get one result at a time. Measuring the $|f(x)\rangle$ register collapses the state on $\sum_{x,f(x)=0} |x\rangle |0\rangle$ or $\sum_{x,f(x)=1} |x\rangle |1\rangle$, which is not useful either. Useful q-algorithms are much more subtle: they use quantum interference in the high-dimensional Hilbert space to engineer the flow of probability such that some " global property " of a function, like its periodicity can be extracted. We will now look how this works, starting with one of the first quantum algorithms discovered that gives an advantage over the best possible classical algorithm.

4.2 Deutsch-Josza Algorithm

Let $x = 0 \dots 2^n - 1, f(x) \in \{0, 1\}$ and be $f(x)$ either a constant or a balanced function, i.e. $f(x) = 0$ for half of the cases for x and $f(x) = 1$ for the other half of the cases for x. The goal of the algorithm is to reliably determine whether $f(x)$ is constant or balanced.

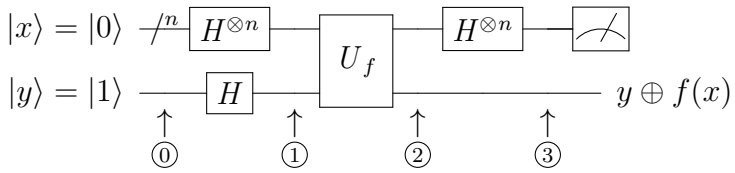
4.2.1 Classical Solution

The classical solution requires the evaluation of $f(x)$ at most $2^n/2 + 1$ times and at least twice:

- Twice if the two evaluations yield different results $f(x_1) \neq f(x_2)$, because then $f(x)$ cannot be constant and so has to be balanced.
- $2^n/2+1$ times if the first $2^n/2$ evaluations yield the same results, because then one additional evaluation determines if the function is constant or balanced.

4.2.2 Quantum solution

The q-algorithm given by the q-circuit in Figure 4.1 requires exactly one evaluation.



(4.8)

Figure 4.1: Deutsch-Josza algorithm as a q-circuit to determine a global property of a function (balanced or constant).

The states in the q-circuit are

$$|\psi_{⓪}\rangle = |0\rangle^{\otimes n} |1\rangle \tag{4.9}$$

$$|\psi_{①}\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \cdot \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \tag{4.10}$$

Then U_f evaluates f in parallel:

$$|x, y\rangle \to |x, y \oplus f(x)\rangle \tag{4.11}$$

Following the truth table we have

y	$f(x)$	$y \oplus f(x)$	
0	0	0	i.e. $\|x\rangle \|0 \oplus f(x)\rangle = \|x, f(x)\rangle$
0	1	1	
1	0	1	i.e. $\|x\rangle \|1 \oplus f(x)\rangle = \|x, 1 - f(x)\rangle$
1	1	0	

$$U_f |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} |x\rangle (|f(x)\rangle - |1 - f(x)\rangle) \tag{4.12}$$

$$= \frac{1}{\sqrt{2}} |x\rangle \cdot \begin{cases} |0\rangle - |1\rangle & \text{for } f(x) = 0 \\ |1\rangle - |0\rangle & \text{for } f(x) = 1 \end{cases} \tag{4.13}$$

giving us

$$|\psi_{②}\rangle = \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \tag{4.14}$$

where $f(x)$ is now encoded as phase factors in the sate. This is the decisive magic step that enables one to profit from quantum interference in Hilbert space! Given a single qubit $|x\rangle$, the last Hadamard results in

$$H|x\rangle = \sum_z (-1)^{xz} \frac{|z\rangle}{\sqrt{2}} \tag{4.15}$$

$$\Big[|0\rangle \overset{H}{\mapsto} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \tag{4.16}$$

$$|1\rangle \overset{H}{\mapsto} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \Big] \tag{4.17}$$

which for multiple qubits means

$$H^{\otimes^n} |x_1, \ldots, x_n\rangle = \sum_{z_1,\ldots,z_n \in \{0,1\}} \frac{(-1)^{x_1 z_1} \cdot \ldots \cdot (-1)^{x_n z_n}}{\sqrt{2^n}} |z_1, \ldots, z_n\rangle \tag{4.18}$$

$$= \sum_{\boldsymbol{z}} \frac{(-1)^{\boldsymbol{x}\cdot\boldsymbol{z}}}{\sqrt{2^n}} |z_1, \ldots, z_n\rangle \,, \tag{4.19}$$

and where $\boldsymbol{x} \cdot \boldsymbol{z}$ denotes the scalar product bit by bit where $\boldsymbol{x} = (x_1, \cdots, x_n)$ is the binary decomposition of $x \in \{0, 1, \cdots, 2^n - 1\}$ and correspondingly for $\boldsymbol{z}$. From (4.14) and (4.19) we obtain

$$|\psi_{③}\rangle = \sum_z \sum_x \frac{(-1)^{\boldsymbol{x}\cdot\boldsymbol{z} + f(x)} |z\rangle}{2^n} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{4.20}$$

Measuring the first register, the amplitude of the state $|0\rangle^{\otimes^n}$ is

$$\sum_{x=0}^{2^n-1} \frac{(-1)^{f(x)}}{2^n}. \tag{4.21}$$

Hence, if $f(x) =$ constant this amplitude is either $+1$ or -1 and so with probability 1, the measurement outcome is $\boldsymbol{x} = 0 \ldots 0$. On the other hand, if $f(x)$ is balanced then the amplitude is zero, and hence $\boldsymbol{x} = 0 \ldots 0$ is never observed. As a result, if we measure the first register and the outcome is $x = 0$, we know that $f(x)$ is constant, whereas if the outcome is not $x = 0$, $f(x)$ is balanced. Hence with a single quantum evaluation of $f(x)$ on a superposition we can obtain the desired information about $f(x)$. Compared to the classical case this looks like an exponential advantage. However, in the classical case we considered the worst case. With random sampling of x, one gets the desired information in a a time logarithmic in n if $f(x)$ is balanced, but it is clear that the g-algorithm provides an advantage of at least a factor 2 in the number of evaluations of $f(x)$.

4.3 The Quantum Fourier Transform

The classical discrete Fourier transform of a sequence

$$x_0, \ldots, x_{N-1}, \quad x_i \in \mathbb{C} \to y_0, \ldots, y_{N-1}, \quad y_i \in \mathbb{C} \tag{4.22}$$

is defined as

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \exp\{i2\pi jk/N\} \tag{4.23}$$

The q-Fourier transform is the same thing, but for a sequence of basis states:

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\{i2\pi jk/N\} |k\rangle \equiv U|j\rangle \tag{4.24}$$

$$\Rightarrow \sum_{j=0}^{N-1} x_i |j\rangle \mapsto \sum_{k=0}^{N-1} y_k |k\rangle = \frac{1}{\sqrt{N}} \sum_{j,k} x_j \exp\{i2\pi jk/N\} |k\rangle \tag{4.25}$$

Is the transform unitary? Yes, as a simple calculation shows:

$$\langle k|U|j\rangle = \frac{1}{\sqrt{N}} \exp\{i2\pi jk/N\} =: U_{jk} \tag{4.26}$$

$$\sum_k U_{jk} \underbrace{U^*_{lk}}_{=\left(U^\dagger\right)_{kl}} = \frac{1}{N} \sum_{k=0}^{N-1} \exp\{i2\pi\,(jk/N - lk/N)\} \tag{4.27}$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} \exp\{i2\pi(j-l)\,k/N\} \tag{4.28}$$

$$= \begin{cases} 1 & j = l \\ \frac{1}{N} \frac{1-\exp\{i2\pi(j-l)N/N\}}{1-\exp\{i2\pi(j-l)/N\}} = 0 & \text{else} \end{cases} \tag{4.29}$$

$$= \delta_{jl} \tag{4.30}$$

Now specialize to n qubits, and use the binary representation of integer numbers and binary fractions.

Definition 2 (Binary representation)
$j = j_1 j_2 \ldots j_n$ *meaning*

$$j = j_1 \cdot 2^{n-1} + j_2 \cdot 2^{n-2} + \ldots + j_n \cdot 2^0 = \sum_{k=1}^{n} j_k 2^{n-k} \tag{4.31}$$

Definition 3 (Binary fraction)

$$0.j_l j_{l+1} \dots j_m := \frac{j_l}{2} + \frac{j_{l+1}}{4} + \frac{j_m}{2^{m-l+1}} = \sum_{n=l}^{m} \frac{j_n}{2^{n-l+1}} \tag{4.32}$$

From the definition of the q-FT eq.(4.25) we get with $N := 2^n$ and the binary representation of $k = \sum_{l=1}^{n} k_l 2^{n-l}$:

$$|j\rangle \mapsto \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \exp\left\{ i2\pi j \left(\sum_{l=1}^{n} k_l 2^{-l} \right) \right\} |k_1 \dots k_n\rangle \ , \tag{4.33}$$

which factors as:

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} \exp\left\{ i2\pi j k_l 2^{-l} \right\} |k_l\rangle \tag{4.34}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left(\sum_{k_l=0}^{1} \exp\left\{ i2\pi j k_l 2^{-l} \right\} |k_l\rangle \right) \tag{4.35}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left(|0\rangle + \exp\left\{ i2\pi j 2^{-l} \right\} |1\rangle \right) . \tag{4.36}$$

Here j is an integer number, $j = \sum_{k=1}^{n} j_k 2^{n-k}$ and $j \cdot 2^{-l} = \sum_{k=1}^{n} j_k \cdot 2^{n-k-l}$. The integer part does not contribute as it only multiplies factors with $\exp\{i2\pi\} = 1$. So what is the fraction part of this? For $n - k - l < 0 \Rightarrow k > n - l$, therefore

$$l = 1 : \qquad k = n \tag{4.37}$$

$$l = 2 : \qquad k = n, n-1 \tag{4.38}$$

$$\dots \tag{4.39}$$

$$l = n : \qquad k = n, n-1, \dots, 1 \tag{4.40}$$

So

$$l = 1 : \qquad \frac{j}{2} \text{ has a fraction part of } j_n \cdot 2^{-1} = 0.j_n \tag{4.41}$$

$$j = 2 : \qquad \frac{j}{4} \text{ has a fraction part of } j_n 2^{-2} + j_{n-1} 2^{-1} = 0.j_{n-1} j_n \tag{4.42}$$

$$\dots \tag{4.43}$$

$$l = n : \qquad \frac{j}{2^n} \text{ has a fraction part of } j_n 2^{-n} + j_1 2^{-1} = 0.j_1 \dots j_n. \tag{4.44}$$

Using these fraction parts, the product representation in eq.(4.36) takes on the form

$$|j\rangle \mapsto \frac{1}{2^{n/2}} \left(|0\rangle + \exp\left\{i2\pi 0.j_n\right\}|1\rangle\right)\left(|0\rangle + \exp\left\{i2\pi 0.j_{n-1}j_n\right\}|1\rangle\right) \\ \cdot \ldots \cdot \left(|0\rangle + \exp\left\{i2\pi 0.j_1 j_2 \ldots j_n\right\}|1\rangle\right). \tag{4.45}$$

The product representation gives rise to a q-circuit representation. Define

$$R_k := \begin{pmatrix} 1 & 0 \\ 0 & \exp\left\{i2\pi/2^k\right\} \end{pmatrix} \tag{4.46}$$

so that

$$R_k|0\rangle = |0\rangle \tag{4.47}$$

$$R_k|1\rangle = \exp\left\{i2\pi/2^k\right\}|1\rangle \tag{4.48}$$

The Hadamard gate can be represented similarly with a binary fraction depending on the basis state on which it acts:

$$H|j_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left\{i2\pi 0.j_1\right\}|1\rangle\right) \tag{4.49}$$

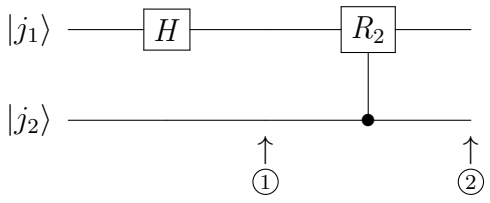
as

$$i2\pi 0.j_1 = \begin{cases} i\pi & \text{for } j_1 = 1 \\ 0 & \text{for } j_1 = 0 \end{cases} \Rightarrow \begin{cases} \exp\left\{i2\pi 0.j_1\right\} = -1 \\ \exp\left\{i2\pi 0.j_1\right\} = +1. \end{cases} \tag{4.50}$$

We also define a controlled R_k by the following map of computational basis states:

$\lvert j_1 j_2\rangle$	$cR_k\lvert j_1 j_2\rangle$
$\lvert 00\rangle$	$\lvert 00\rangle$
$\lvert 01\rangle$	$\lvert 01\rangle$
$\lvert 10\rangle$	$\lvert 10\rangle$
$\lvert 11\rangle$	$\exp\{2\pi i/2^k\}\lvert 11\rangle$.

It can be written as $|j_1 j_2\rangle \mapsto |j_1\rangle \exp\{2\pi i \frac{j_1 j_2}{2^k}\}|j_2\rangle$, where $j_1, j_2 \in \{0,1\}$ are the labels of control and target basis states. Note that R_k is symmetric under exchange of control and target, as the phase-factor is symmetric and multiplies the full state, so it could be attributed to the control or the target. Now consider the q-circuit



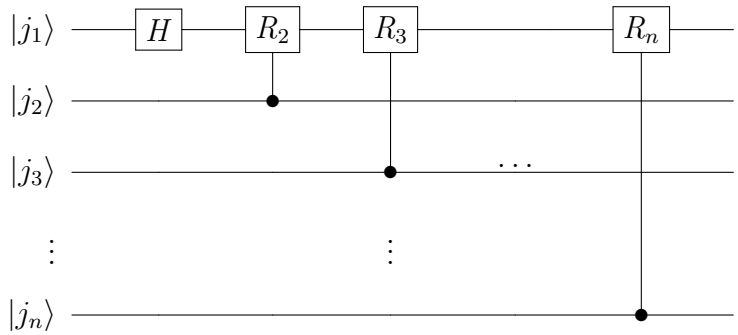
(4.51)

where

$$|\psi_{①}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left\{i2\pi 0.j_1\right\}|1\rangle\right)|j_2\rangle \tag{4.52}$$

$$|\psi_{②}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left\{i2\pi 0.j_1 j_2\right\}|1\rangle\right)|j_2\rangle\,. \tag{4.53}$$

The phase factor in (4.53) can be understood as $0.j_1 + 0.0(j1 \cdot j2)|_{j_1=1} = 0.j_1 + 0.0j_2 = 0.j_1 j_2$, where the $j_1 = 1$ arrives from the fact that the state is $|1\rangle|j_2\rangle$. Continue this way with all the other qubits as control (Figure 4.2). This results for the first



(4.54)

Figure 4.2: Controlled R_k gates on the first qubit, controlled by all other $n-1$ qubits, one after the other.

qubit $|j_1\rangle$ in the state

$$\frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left\{i2\pi 0.j_1 j_2 \ldots j_n\right\}|1\rangle\right). \tag{4.55}$$

Similarly with the second qubit: start with the Hadamard gate and then apply the controlled $R_2, \ldots, R_{n-1}$ with control by qubits $|j_3\rangle, \ldots, |j_n\rangle$, but do not touch the qubit $|j_1\rangle$ any more. This yields

$$|j_2\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left\{i2\pi 0.j_2 j_3 \ldots j_n\right\}|1\rangle\right)\,. \tag{4.56}$$

Continue like this for all other qubits. $|j_n\rangle$ just gets the Hadamard gate applied to it:

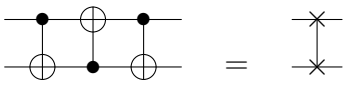
$$|j_n\rangle \mapsto \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left\{i2\pi 0.j_n\right\}|1\rangle\right). \tag{4.57}$$

This way, we get the product state

$$\frac{1}{2^{n/2}}\left(|0\rangle + \exp\left\{i2\pi 0.j_1 j_2 \ldots j_n\right\}|1\rangle\right)\left(|0\rangle + \exp\left\{i2\pi 0.j_2 \ldots j_n\right\}|1\rangle\right) \tag{4.58}$$

$$\cdot \ldots \cdot \left(|0\rangle + \exp\left\{i2\pi 0.j_n\right\}|1\rangle\right). \tag{4.59}$$

Compare this to eq.(4.45) to find that this is the QFT up to the different ordering of the qubits in the output state. So we have to swap the qubits, i.e. reverse their order. This is achieved by the *SWAP* gate, which exchanges two qubits, $|a, b\rangle \mapsto |b, a\rangle \; \forall a, b \in \{0, 1\}$ (Figure 4.3). The q-circuit in Figure 4.3 accomplishes this:



(4.60)

Figure 4.3: Representation of the q-circuit which implements the *SWAP* gate between two qubits.

$$|a, b\rangle \mapsto |a, a \oplus b\rangle \tag{4.61}$$
$$\mapsto |a \oplus (a \oplus b)\,, a \oplus b\rangle = |b, a \oplus b\rangle \tag{4.62}$$
$$\mapsto |b, b \oplus (a \oplus b)\rangle = |b, a\rangle \tag{4.63}$$

Swapping the qubits after applying the controlled R_k gates as $n \leftrightarrow 1, n-1 \leftrightarrow 2, \ldots$ (which are at most $n/2$ swaps) gives then indeed the product representation of the q-FT, eq.(4.45).

The complete number of gates required is shown in (Table 4.1). So overall $\mathcal{O}\left(n^2\right)$

	number of gates
H $+(n-1)$ R_k gates on 1st qubit	n
H $+(n-2)$ R_k gates on 2nd qubit	$n-1$
...	...
H on last qubit	1
	$\sum = \frac{n}{2}(n+1)$
$+\frac{n}{2}$ *SWAP* gates	$\frac{n}{2}$
	$\frac{n}{2}(n+2)$

Table 4.1: Total number of gates required for the implementation of the q-FT.

gates are required, Figure 4.4 shows the total q-circuit of the q-FT.

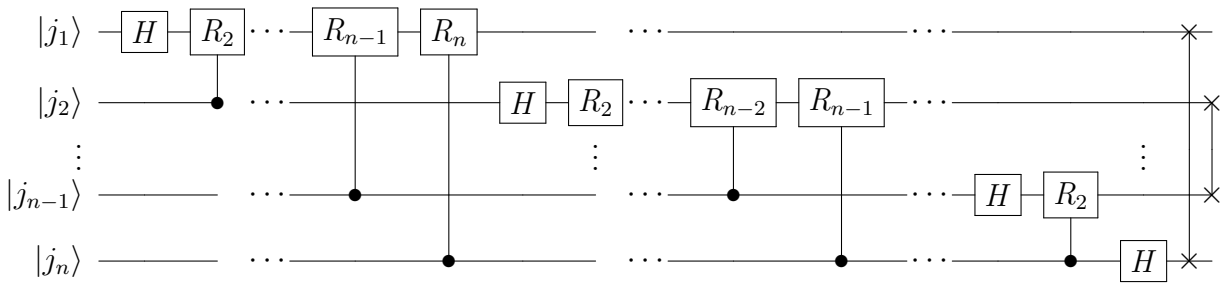


Figure 4.4: Total q-circuit of the q-FT. The R_2 gate acting on $|j_2\rangle$ is controlled by $|j_3\rangle$ (not shown), and only the first two of the final swap gates are shown.

Comparing this to the best classical discrete FT, the *Fast Fourier Transform*, which needs $\mathcal{O}(N \log N) = \mathcal{O}(2^n \cdot n)$ operations raises questions:

- Is the q-FT useful like this?
  No, not directly! What we would like, is to get all the y_k values for a given set of values (the x_k values are the $x_k = f(k)$, the function we want to Fourier transform). From the given x_k values, we would need to prepare the initial state $\sum x_j |j\rangle$ which can already require an exponential effort. Then we do the transform, get $\sum y_k |k\rangle$, and then would like to get all the y_k values. But if we measure the register, we only get some random $|k_i\rangle$, but no information at all on the y_k. To get all y_k, we have to repeat all steps many times, to get some statistics and hence at least the $|y_k|^2$.

  Note

  The useful applications of the q-FT are much more subtle!

- Do we need exponential precision for $\exp\left\{i2\pi/2^k\right\}$?
  Suppose we achieve R_k only with polynomial precision, $E(R_k) = 1/p(n)$, where $E(R_k) \equiv \max_{|\psi\rangle} \| \left(R_k - R_k^{\text{ideal}}\right) |\psi\rangle \|$, and $p(n)$ is a polynomial in n. Then one can show that the error $E(U,V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$ is polynomial in n, too ($\mathcal{O}(n^2/p(n))$). Here U is the ideal q-FT and V is the disturbed q-FT if errors in R_k occur. Hence, exponential precision of the R_k is not required if we can live with polynomial precision of the entire QFT.

4.4 Quantum Phase Estimation

Suppose some unitary U has an eigenvector $|u\rangle$ with the eigenvalue $\exp\{i2\pi\varphi\}$, where φ is unknown:[1]

$$U|u\rangle = \exp\{i2\pi\varphi\}|u\rangle \ . \tag{4.64}$$

We want to estimate the phase φ in a way that is independent of the specific q-circuit that generates U. This can be donoe with the q-circuit for quantum phase estimation shown in Fig. 4.6. A black box computes $U^{(2^j)}$ for us for integer j, see Figure 4.5.

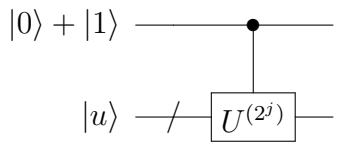


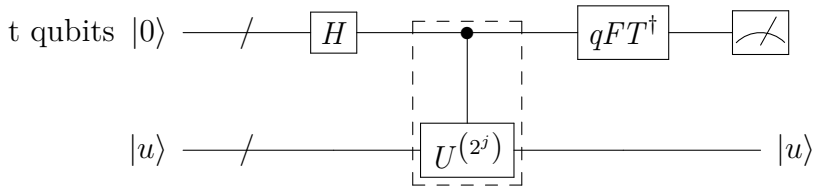
Figure 4.5: Controlled U operation with control qubit in superposition

Consider the action of a single controlled U^{2^j} after the control has been put into a superposition of $|0\rangle$ and $|1\rangle$ by a Hadamard gate (we skip the normalization $1/\sqrt{2}$ for the moment):

$$(|0\rangle + |1\rangle)|u\rangle \xrightarrow{U^{(2^j)}} |0\rangle|u\rangle + \exp\{2\pi i 2^j\varphi\}|1\rangle|u\rangle = \Big(|0\rangle + \exp\{2\pi i 2^j\varphi\}|1\rangle\Big)|u\rangle \ .$$

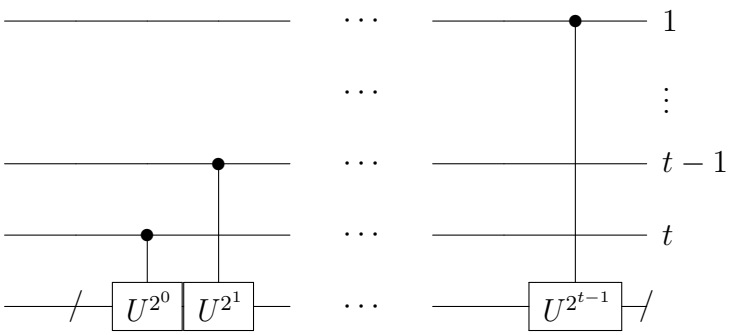
So the phase is now in the control qubit !

[1] This is important not only for quantum computation but also for q-metrology: One application is the estimation of phase shifts in interferometers



(4.65)

with the dashed box acting on the t qubits as:



(4.66)

Figure 4.6: Representation of the q-circuit for the phase estimation of an arbitrary operation U.

So after the H gates and the U^j gates, we have the state

$$|\psi\rangle = \frac{1}{2^{t/2}} \left(|0\rangle + \exp\left\{i2\pi 2^{t-1}\varphi\right\}|1\rangle\right)\left(|0\rangle + \exp\left\{i2\pi 2^{t-2}\varphi\right\}|1\rangle\right) \cdot \ldots \cdot \left(|0\rangle + \exp\left\{i2\pi 2^{0}\varphi\right\}|1\rangle\right)|u\rangle \ . \tag{4.67}$$

$$\tag{4.68}$$

Now suppose $\varphi = 0.\varphi_1\varphi_2\ldots\varphi_t \in [0,1]$ in units of 2π (finite binary representation). Then the exponential terms read

$$\exp\left\{i2\pi 2^{0}\varphi\right\} = \exp\left\{i2\pi 0.\varphi_1\varphi_2\ldots\varphi_t\right\} \tag{4.69}$$

$$\exp\left\{i2\pi 2^{1}\varphi\right\} = \exp\left\{i2\pi\, \varphi_1.\varphi_2\ldots\varphi_t\right\} = \exp\left\{i2\pi 0.\varphi_2\ldots\varphi_t\right\} \tag{4.70}$$

$$\vdots \quad = \quad \vdots \tag{4.71}$$

$$\exp\left\{i2\pi 2^{t-1}\varphi\right\} = \exp\left\{i2\pi\varphi\ldots\varphi_{t-i}.\varphi_t\right\} = \exp\left\{i2\pi 0.\varphi_t\right\} \ . \tag{4.72}$$

So the state in (4.67) is

$$|\psi\rangle = \frac{1}{2^{t/2}} \left(|0\rangle + \exp\left\{i2\pi 0.\varphi_t\right\}|1\rangle\right)\left(|0\rangle + \exp\left\{i2\pi 0.\varphi_{t-1}\varphi_t\right\}|1\rangle\right) \tag{4.73}$$

$$\cdot \ldots \cdot \left(|0\rangle + \exp\left\{i2\pi 0.\varphi_1\varphi_2\ldots\varphi_t\right\}|1\rangle\right)|u\rangle \ . \tag{4.74}$$

which is exactly the q-FT image of $|\varphi_1\ldots\varphi_t\rangle$ (see eq.(4.45)).

Hence, the inverse q-FT will give just this state $|\varphi_1\ldots\varphi_t\rangle$ with probability 1!

So

$$|\psi\rangle \xrightarrow{qFT^\dagger} |\varphi\rangle\,|u\rangle \tag{4.75}$$

where $|\varphi\rangle$ is only a single computational basis state. Measuring the first register gives us the value of $\varphi = 0.\varphi_1, \cdots \varphi_t$ digitally in the first register *if* φ has this *finite* binary representation.

4.4.1 Probability of Success and Precision

Until now we have presumed that there exists an exact representation of φ using a t-bit binary representation. We will now show, that even if φ can not be exactly represented in such a way, we can get a good approximation of φ. The approximation will have a precision of 2^{-n} and a probability of success $1-\varepsilon$, if we use at least

$$t = n + \left\lceil \log_2\left(2 + \frac{1}{2\varepsilon}\right)\right\rceil \tag{4.76}$$

qubits for the first register (which contains $\simeq \varphi$ at the end of the phase estimation algorithm).

Proof.

Let $\varphi = 0.\varphi_1\varphi_2\varphi_3\ldots$ and $b \in [0,\ldots,2^t-1]$, where b is exactly the integer number that can be represented using t bits such that $b/2^t = 0.b_1b_2b_3\ldots b_t = 0.\varphi_1\ldots\varphi_t$, i.e. b provides the best approximation of φ smaller than φ using t bits. The difference

$$\delta := \varphi - \frac{b}{2^t} = 0.0\ldots0_t\varphi_{t+1}\ldots \tag{4.77}$$

then also obviously satisfies (by definition) $0 \leq \delta \leq 2^{-t}$.

Applying the inverse q-FT to eq.(4.75) (which is the state in the first register after the q-FT) results in

$$\frac{1}{2^t}\sum_{k,l=0}^{2^t-1}\exp\left\{-i2\pi kl/2^t\right\}\exp\left\{i2\pi\varphi k\right\}|l\rangle\ . \tag{4.78}$$

Let α_l be the amplitude of the state $|(b+l)\,(\mathrm{mod}\ 2^t)\rangle$:

$$\alpha_l = \frac{1}{2^t}\sum_{k=0}^{2^t-1}\left(\exp\left\{i2\pi\left(\varphi-(b+l)/2^t\right)\right\}\right)^k. \tag{4.79}$$

Summing the geometric series, we get

$$= \frac{1}{2^t}\cdot\frac{1-\exp\left\{i2\pi\left(2^t\varphi-(b+l)\right)\right\}}{1-\exp\left\{i2\pi\left(\varphi-(b+l)/2^t\right)\right\}} \tag{4.80}$$

$$= \frac{1}{2^t}\cdot\frac{1-\exp\left\{i2\pi\left(2^t\delta-l\right)\right\}}{1-\exp\left\{i2\pi\left(\delta-l/2^t\right)\right\}}\,. \tag{4.81}$$

Let m now be the result of the measurement of the first register, i.e. the measurement of the t qubits after the q-FT. We will now calculate a lower bound for the probability to measure a value m that deviates more than e from the true value b, i.e. $|m-b| > e$. The probability is given by

$$p\left(|m-b|>e\right) = \sum_{|l|>e}|\alpha_l|^2 \tag{4.82}$$

$$= \left(\sum_{-2^{t-1}<l\leq-(e+1)} + \sum_{e+1\leq l\leq 2^{t-1}}\right)|\alpha_l|^2\,. \tag{4.83}$$

Note that $l = 0, \ldots, 2^t - 1$ implies $-2^{t-1} < l \leq 2^{t-1} \pmod{2^t}$. The numerator is bound by $|1 - \exp\{i2\pi\,(2^t\delta - 2)\}| \leq 2$, so that

$$|\alpha_l| \leq \frac{2}{2^t\,|1 - \exp\{i2\pi\,(\delta - l/2^t)\}|} \tag{4.84}$$

Using $\delta \in [0, \ldots, 2^{-t}]$ and $-2^{t-1} < l \leq 2^{t-1}$ we get

$$-\pi \leq 2\pi\left(\delta - \frac{l}{2^t}\right) \leq \pi \tag{4.85}$$

since the minimum of $\delta - l/2^t = -1/2$ for $\delta = 0, l = 2^{t-1}$ and the maximum is $+1/2$ for $\delta = 2^{-t}, l = -2^{t-1} + 1$. Within this interval, we have $|1 - \exp\{i\vartheta\}| \geq 2|\vartheta|/\pi = 4\,(\delta - l/2^t)$ (where $\vartheta = 2\pi\,(\delta - l/2^t)$), such that

$$|\alpha_l| \leq \frac{1}{2^{t+1}\left(\delta - \frac{l}{2^t}\right)}\,. \tag{4.86}$$

This leads to a bound for the probability of

$$p\,(|m - b| > e) \leq \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{\left(l - \underbrace{2^t\delta}_{\geq 0}\right)^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{\left(l - \underbrace{2^t\delta}_{\leq 1}\right)^2}\right] \tag{4.87}$$

$$\leq \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{l^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l-1)^2}\right] \tag{4.88}$$

$$\leq \frac{1}{4}\left(\sum_{l=e+1}^{2^{t-1}-1} \frac{1}{l^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l-1)^2}\right) \tag{4.89}$$

$$\leq \frac{1}{4}\left(\sum_{l=e+1}^{2^{t-1}-1} \frac{1}{l^2} + \sum_{l=e}^{2^{t-1}-1} \frac{1}{l^2}\right) \tag{4.90}$$

$$\leq \frac{1}{2}\sum_{l=e}^{2^{t-1}-1} \frac{1}{l^2} \tag{4.91}$$

$$\leq \frac{1}{2}\int_{e-1}^{2^{t-1}-1} \frac{1}{l^2}\,\mathrm{d}l \tag{4.92}$$

$$\leq \frac{1}{2\,(e-1)} \tag{4.93}$$

From (4.91) to (4.92) we used that $1/l^2$ is strictly monotonously decreasing, and hence upper bounds the integrand in each integer interval by its value at the lower edge of the interval.

If we want to extract φ with an accuracy of n bits, i.e. $e = 2^{t-n} - 1$ with $b \sim 2^t$ and a relative error of $\sim 2^{-n}$ meaning n bit accuracy, then we can use $t = n + p$ qubits to do so. Using such t qubits, we get $e = 2^{+p} - 1$ with an error probability of

$$p\left(|m - b| > e\right) \leq \frac{1}{2\left(2^p - 2\right)} \overset{!}{<} \varepsilon \tag{4.94}$$

or alternatively the probability of success

$$1 - \frac{1}{2\left(2^p - 2\right)}\,. \tag{4.95}$$

If the error probability is required to be below ε, then we need $p \geq \log_2\left(2 + 1/2\varepsilon\right)$, i.e. one has to use

$$t = n + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil \tag{4.96}$$

qubits. □

This means, that there is only a mild logarithmic increase in the number of qubits above n depending on the acceptable error probability ε.

We assumed that the second register contains an eigenstate of U, $|u\rangle$. In many cases however, no eigenstate is known. If $|\psi\rangle = \sum_u c_u |u\rangle$ is prepared with eigenvalues $\exp\{i2\pi\varphi_u\}$ for the eigenvector $|u\rangle$, then the q-algorithm results in $\sum_u c_u |\tilde{\varphi_u}\rangle |u\rangle$ where $|\tilde{\varphi_u}\rangle$ is an approximation of the true $|\varphi_u\rangle$ in the way explained above. Measuring the first register in this cases yields φ_u with a probability of $|c_u|^2$. Repeated measurements quickly allow one to find all φ_u of all the dominant eigenstates participating in the sum.

Phase estimation is an essential subroutine of important q-algorithms and in particular of the order-finding and factoring algorithms: It solves the key problem of transfering a quantum mechanical phase digitally into a quantum register.

4.5 Modular Arithmetic: Basics of Number Theory required by the Shor Algorithm

In this section I introduce the basics of number theory on which Shor's factoring algorithm is based upon. As this lies a bit outside of quantum information processing itself, the reader not interested in number theory can skip ahead to the next sections, where the corresponding quantum algorithms are developed. The main object is the order of an integer modulo N, the definition of which is given in

the present section (see Definition 7), but reviewed once more at the beginning of section 4.6.

In the following, we will operate on the integer numbers $\mathbb{Z}$. With $d \in \mathbb{Z}, n \in \mathbb{Z}$ we say that d *divides* n if there exists $k \in \mathbb{Z}$ so that $n = dk$ holds. In short we write $d|n$ or, if such a k does not exist, i.e. d does not divide n, $d \nmid n$.

- $a|b \wedge b|c \Rightarrow a|c$ (transitivity).
  Proof: $b = ka, c = lb \Rightarrow c = lka \iff a|c$.
- $d|a \wedge d|b \Rightarrow d|\,(xa + yb)$ (d also divides linear combinations where $x, y \in \mathbb{Z}$).
  Proof: $a = kd, b = ld \Rightarrow xa + yb = (xk + yl)\, d \Rightarrow d|\,(xa + yb)$.
- $a, b \in \mathbb{Z}^+, a|b \Rightarrow a \leq b$.
  Proof: $b = ka, k \geq 1 \Rightarrow b \geq a$, since $a, b \geq 0$.
- By these relations, it also follows: $a|b \wedge b|a \Rightarrow (a \leq b) \wedge (b \leq a) \iff a = b$.

Theorem 4 (Fundamental theorem of algebra)
$\forall a \in \mathbb{Z}, a > 1$ *there exists a unique prime factorisation* $a = p_1^{a_1} p_2^{a_2} \cdot \ldots \cdot p_n^{a_n}$ *(where* p_i *are prime and* $a_i \in \mathbb{Z}^+$*).*

Until now, no efficient classical algorithm for prime factorisation is known.

Definition 4 (Modular arithmetic)

$$x = r\,(mod\ n) \iff \exists k \in \mathbb{Z}^+ \mid x = kn + r. \tag{4.97}$$

We sometimes also write $x\,(mod\ n) = r$ *which indicates the remainder of the division of* x *by* n*.*

Definition 5 (Greatest common divisor)
The greatest common divisor $\gcd(a, b) = t$ *is the largest number* $t \in \mathbb{Z}$ *where* $t|a$ *and* $t|b$*. The greatest common divisor may be efficiently calculated using Euclid's algorithm.*

We first start of with how the greatest common divisor may be represented:

Theorem 5 (Representation of the greatest common divisor)
The $\gcd(a, b)$*,* $a, b \in \mathbb{Z}$ *is the smallest integer number* $t > 0 \mid t = ax + by$ *for* $x, y \in \mathbb{Z}$*.*

Proof.

Let $s = ax + by$ be the smallest number $\in \mathbb{Z}^+$ where $x, y \in \mathbb{Z}$. Then $\gcd(a,b) \,|s$ since the greatest common divisor divides by definition a and b, and s is a linear combination of a and b. Therefore $\gcd(a,b) \leq s$.

However, $s|a$ and $s|b$ also holds, which can be shown by contradiction: Let $s \nmid a$, then $a = ks + r$ where $1 \leq r \leq s-1$ (by definition). Since $s = ax + by$, we find $r = a(1 - kx) + b(-ky)$ as a linear combination of a, b, $r \in \mathbb{Z}^+$. But also $r < s$ which contradicts the definition of s as the smallest possible linear combination of a, b in $\mathbb{Z}^+$.

It therefore follows $s|a$ and with the same argument $s|b$. Since s divides a and b, it is a common divisor of a, b and hence, $s \leq \gcd(a,b)$. As we found before, also $s \geq \gcd(a,b)$, therefore $s = \gcd(a,b)$. □

Corollary 1

$$c|a \wedge c|b \Rightarrow c|\gcd(a,b) \tag{4.98}$$

Proof.

$\gcd(a,b) = xa + yb$ is a linear combination of a, b where $x, y \in \mathbb{Z}$. Therefore $c|\gcd(a,b)$. □

Corollary 2
Let $1 < n \in \mathbb{Z}^+$. Then there exists a multiplicative inverse to a (mod n), i.e. $\exists a^{-1}$ where $aa^{-1} = 1$ (mod n), if and only if a and n are co-prime ($\gcd(a,n) = 1$).

Proof.

" $\Rightarrow$"

1. Suppose there exists a multiplicate inverse of a (mod n). We denote this inverse as a^{-1}, i.e. $aa^{-1} = 1 + kn$ where $k \in \mathbb{Z}$, then $aa^{-1} + (-k)n = 1$. This obviously denotes the smallest positive integer number that is a linear combination of a and n, meaning $\gcd(a,n) = 1$.

" $\Leftarrow$ "

2. Let $\gcd(a,n) = 1$, it follows that there exist integer numbers a^{-1} and b such that $aa^{-1} + bn = 1 \Rightarrow aa^{-1} = 1 (\text{mod } n)$.

□

Euclid's algorithm allows for an efficient determination of the $\gcd(\cdot,\cdot)$. Calculating the $\gcd(\cdot,\cdot)$ by comparing the prime factorisation is highly inefficient, since there is no efficient classical algorithm known for the factorisation into primes.

Theorem 6
$a, b \in \mathbb{Z}$, r denotes the remainder if we divide a by b. If $r \neq 0$, then $\gcd(a,b) = \gcd(b,r)$.

Proof.

1. $\gcd(a,b) \,|\, \gcd(b,r)$, since $r = a - kb$ where $k \in \mathbb{Z}$. Since $\gcd(a,b)$ divides a and b and therefore also linear combination of a and b, it also divides r, $\gcd(a,b) \,|r$. Therefore $\gcd(a,b)$ also divides b and r and therefore also $\gcd(b,r)$.
2. $\gcd(b,r) \,|\, \gcd(a,b)$, since $\gcd(b,r) \,|b, r$, and since $a = r + kb$ is a linear combination of r and b, we get $\gcd(b,r) \,|a \Rightarrow \gcd(b,r) \,|a, b$ and therefore $\gcd(b,r) \,|\, \gcd(a,b)$. Then, from 1., 2. follows $\gcd(a,b) = \gcd(b,r)$.

□

This allows for setting up a fast converging algorithm:

1. Arrange a, b that $a > b$.
2. Divide a by b with the remainder r_1: $a = k_1 b + r_1$.
   Then $\gcd(a,b) = \gcd(b,r_1)$.
3. Divide b by r_1 with the remainder r_2: $b = k_2 r_1 + r_2$.
   Then $\gcd(b,r_1) = \gcd(r_1,r_2)$.
4. Divide r_1 by r_2 with the remainder r_3: $r_1 = k_3 r_2 + r_3$.
   Then $\gcd(r_1,r_2) = \gcd(r_2,r_3)$.
5. Continue until the remainder $r_{m+2} = 0$, so that $r_m = k_{m+2} r_{m+1}$

The $\gcd(a,b)$ is then given by $\gcd(r_m, r_{m+1}) = r_{m+1} = \gcd(r_{m-1}, r_m) = \ldots = \gcd(a,b)$.

Example 7 ($\gcd(18,243)$)

$$243 = 13 \cdot 18 + 9 \tag{4.99}$$
$$18 = 2 \cdot 9 \tag{4.100}$$
$$\Rightarrow \gcd(18,243) = 9 \tag{4.101}$$

Example 8 ($\gcd(6825, 1430)$)

$$6825 = 4 \cdot 1430 + 1105 \tag{4.102}$$
$$1430 = 1 \cdot 1105 + 325 \tag{4.103}$$
$$1105 = 3 \cdot 325 + 130 \tag{4.104}$$
$$325 = 2 \cdot 130 + 65 \tag{4.105}$$
$$130 = 2 \cdot 65 \tag{4.106}$$
$$\Rightarrow \gcd(6825, 1430) = 65 \tag{4.107}$$

The algorithm can be extended to also determine the linear combination which represents $\gcd(a, b)$ as a linear combination of a and b. To achieve this, the steps of the algorithm are simply followed backwards:

Example 9 ($\gcd(6825, 1430)$)

$$65 = 325 - 2 \cdot 130; \qquad 130 = 1105 - 3 \cdot 325 \tag{4.108}$$
$$= 325 - 2 \cdot (1105 - 3 \cdot 325) \tag{4.109}$$
$$= -2 \cdot 1105 + 7 \cdot 325 \tag{4.110}$$
$$= -2 \cdot 1105 + 7 \cdot (1430 - 1 \cdot 1105) \tag{4.111}$$
$$= 7 \cdot 1430 - 9 \cdot 1105 \tag{4.112}$$
$$= 7 \cdot 1430 - 9\,(6825 - 4 \cdot 1430) \tag{4.113}$$
$$= -9 \cdot 6825 + 43 \cdot 1430 \tag{4.114}$$

The algorithm requires $\sim 2\lceil \log a \rceil = \mathcal{O}(L)$ divisional operations (where L is the number of bits required to represent the number a). Every divisional operation requires $\sim L^2$ elemental operations, i.e. the effort for the algorithm is $\sim \mathcal{O}(L^3)$.

Euclid's algorithm can also be used to efficiently determine the modular inverse a^{-1}:
Let $\gcd(a, n) = 1$ a, n be co-prime. We use Euclid's algorithm to efficiently determine x, y where $ax + ny = 1$. Then $ax = (1 - ny) = 1 \pmod{n}$, then $x = a^{-1} \pmod{n}$.

This way, we can also solve linear equations $\pmod{n}$,

$$ax + b = c \pmod{n} \text{ where } \gcd(a, n) = 1 : \tag{4.115}$$

a^{-1} determines the $x = a^{-1}(c - b) \pmod{n}$ that solves the equation. This technique can be extended to general systems of linear equations:

Theorem 7 (Chinese remainder theorem)
Let $m_1, \ldots, m_n \in \mathbb{Z}^+$ where all pairs m_i, m_j are co-prime ($\gcd(m_i, m_j) = 1, \forall i \neq j$), and $a_i \in \mathbb{Z}$. Then there exists a solution for the following system of equations

$$x = a_1 \,(mod\ m_1) \tag{4.116}$$
$$x = a_2 \,(mod\ m_2) \tag{4.117}$$
$$\vdots \tag{4.118}$$
$$x = a_n \,(mod\ m_n) \tag{4.119}$$

Different solutions for the system are equal $(mod\ M)$ with $M = m_1 m_2 \cdot \ldots \cdot m_n$.

Proof.

Define $M_i := M/m_i$, then M_i and m_i are co-prime $\Rightarrow \exists M_i^{-1} \,(\text{mod } m_i) =: N_i$. The system of equations is solved by

$$x = \sum_i a_i M_i N_i \tag{4.120}$$

because $M_i N_i \equiv 1 \,(\text{mod } m_i)$ (by definition of N_i), while $M_i N_i = 0 \,(\text{mod } m_j)$ for $j \neq i$, since M_i contains all $m_j, j \neq i$. This is equivalent to $M_i N_i = \delta_{il} \,(\text{mod } m_l)$.

Then $x = \sum_i a_i M_i N_i = \sum_i a_i \delta_{il} \,(\text{mod } m_l) = a_l \,(\text{mod } m_l)\ \forall l$ proves the existence of a solution.

Let now be x, x' be two solutions, then $(x - x') = 0 \,(\text{mod } m_i)\, \forall i$. Hence $m_i | \,(x - x')\, \forall i$. Since all pairs of $m_i, m_j, i \neq j$ are co-prime: $M = \prod m_i | \,(x - x')$, which implies $(x - x') \,(\text{mod } M) = 0$ leading to the claim $x = x' \,(\text{mod } M)$. □

Corollary 3
There exists a bijective mapping between pairs of (x_a, x_b), where $1 \leq x_a < a, 1 \leq x_b < b$ such that $\gcd(x_a, a) = \gcd(x_b, b) = \gcd(a, b) = 1$, and integer numbers x, where $1 \leq x < ab$ is also co-prime to the product of a, b: $\gcd(x, ab) = 1$.

Proof.

We apply the Chinese remainder theorem, where $m_1 := a, m_2 := b$ and $a_1 = x_a, a_2 = x_b$, leading to the system of equations

$$x = x_a \,(\text{mod } a) \tag{4.121}$$
$$x = x_b \,(\text{mod } b) \tag{4.122}$$

which has a unique solution x where $1 \leq x < ab$. This means, that (x_a, x_b) determine x unambiguously. In reverse, (x_a, x_b) are also determined unambiguously

by x through $x = x_a \,(\text{mod } a)$ and $x = x_b \,(\text{mod } b)$ as the remainders of x divided by a and b respectively. □

Lemma 3
Let p be a prime and $k \in \mathbb{Z}$ where $1 \leq k \leq p-1$. Then

$$p| \binom{p}{k} \tag{4.123}$$

Proof.

$$\binom{p}{k} = \frac{p!}{(p-k)!k!} = \frac{1}{k!} p\,(p-1) \cdot \ldots \cdot (p-k+1) \tag{4.124}$$

$$\iff p\,(p-1) \cdot \ldots \cdot (p-k+1) = \binom{p}{k} k\,(k-1) \cdot \ldots \cdot 1 \tag{4.125}$$

The left hand side can be divided by p and therefore also the ride hand side. Since $k \leq p-1$, p can not divide $k\,(k-1) \cdot \ldots \cdot 1$, because all factors in this product are smaller than or equal to k and $p \geq k+1$. By this we conclude that the binomial coefficient must be dividable by p:

$$p| \binom{p}{k} \tag{4.126}$$

□

Theorem 8 (Fermat's little theorem)
Let p be prime and $a \in \mathbb{Z}$. Then

$$a^p = a \,(mod\ p) \tag{4.127}$$

and if $p \nmid a$, then

$$a^{p-1} = 1 \,(mod\ p) \tag{4.128}$$

Proof.

The later part can be directly derived from the first part, since, if $p \nmid a$, then $\gcd(a, p) = 1$ and there exists $a^{-1} \,(\text{mod } p)$ such as $a^{p-1} = a^{-1}a^p = a^{-1}a \,(\text{mod } p) = 1 \,(\text{mod } p)$.

Now we are left with showing the first part, where $a > 0$, which we proof by induction in a. For $\underline{a = 1}$:

$$a^p = 1 = 1 \,(\text{mod } p) \tag{4.129}$$

is valid. Now we assume the theorem holds for an arbitrary a and show that it also holds for $\underline{a+1}$:

$$(1+a)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \tag{4.130}$$

Following the previously proven Lemma $\binom{p}{k} = 0 \,(\mathrm{mod}\ p)$ for $k = 1, \ldots, p-1$, since $p | \binom{p}{k}$, we can finish the induction step through

$$(1+a)^p = (1+a^p) \,(\mathrm{mod}\ p) = (1+a) \,(\mathrm{mod}\ p) \tag{4.131}$$

which concludes the induction and thus proofs the theorem. □

There exists a generalisation by Euler, but first we have to introduce an auxiliary function:

Definition 6 (Euler's φ function)
Euler's φ function $\varphi(n)$ is defined as the number of positive integer numbers $m < n$ where $\gcd(m,n) = 1$, i.e. m, n are co-prime.

For an arbitrary prime number p, the function is obviously $\varphi(p) = p - 1$. For p^α, the only numbers which are not co-prime to p^α while also being between 1 and $p^\alpha - 1$ are the multiples of p, i.e. $p, 2p, 3p, 4p, \ldots, p^\alpha - p = (p^{\alpha-1} - 1)\, p$. These are exactly $p^{\alpha-1} - 1$ numbers, i.e.

$$\varphi(p^\alpha) = p^\alpha - 1 - \left(p^{\alpha-1} - 1\right) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)\,. \tag{4.132}$$

Lemma 4
If a and b are co-prime, $\gcd(a,b) = 1$, then:

$$\varphi(ab) = \varphi(a)\varphi(b)\,. \tag{4.133}$$

Proof.

Choose x_a, x_b to have $1 \leq x_a < a$ and $1 \leq x_b < b$, where each pair (x_a, a) and (x_b, b) is co-prime, $\gcd(x_a, a) = 1 = \gcd(x_b, b)$. Obviously there are $\varphi(a)\varphi(b)$ many such pairs (x_a, x_b). Now consider the system of equations

$$x = x_a \,(\mathrm{mod}\ a) \tag{4.134}$$
$$x = x_b \,(\mathrm{mod}\ b)\,. \tag{4.135}$$

The Chinese remainder theorem implies the existence of exactly one solution x where $1 \leq x < ab$ ($M = ab$ defines a period for the solutions of the Chinese

remainder theorem, where all solutions are unique (mod M), i.e. there is exactly one solution located in the interval $1 \leq x < ab$). On the other hand, there exist a multiplicate inverse (mod a) for x_a and one (mod b) for x_b, i.e. $\exists x_a^{-1}$ such that $x_a x_a^{-1} = 1 \,(\text{mod } a)$.

$$\overset{(4.134)}{\Rightarrow} x x_a^{-1} \,(\text{mod } a) = x_a x_a^{-1} \,(\text{mod } a) = 1 \,(\text{mod } a) \tag{4.136}$$

So there also exists a multiplicative inverse for x (mod a), hence $\gcd(x, a) = 1$, and correspondingly $\gcd(x, b) = 1$, and thus $\gcd(x, ab) = 1$.

By definition, there exist $\varphi(ab)$ many such x, and due to the bijective mapping between pairs (x_a, x_b) $(1 \leq x_a < a, \gcd(a, x_a) = 1$ and $1 \leq x_b < b, \gcd(b, x_b) = 1)$ and x $(1 \leq x < ab, \gcd(x, ab) = 1)$ we have

$$\varphi(ab) = \varphi(a)\varphi(b) \tag{4.137}$$

if a, b are co-prime, $\gcd(a, b) = 1$, as required by the Chinese remainder theorem. □

Theorem 9 (Generalisation of Fermat's little theorem by Euler)
Let $\gcd(a, n) = 1$*, then*

$$a^{\varphi(n)} = 1 \,(mod\ n)\ . \tag{4.138}$$

Proof.

First we will show using induction in a, that for p prime:

$$a^{\varphi(p^\alpha)} = 1 \,(\text{mod } p) \tag{4.139}$$

For the start of the induction choose $\alpha = 1$. Then, since $\varphi(p) = p - 1$, (4.138) yields

$$a^{p-1} = 1 \,(\text{mod } p)\ , \tag{4.140}$$

which is exactly Fermat's little theorem and therefore true.

Now assume the claim to be true for an arbitrary integer number $\alpha \geq 1$, $k \in \mathbb{Z}$

$$a^{\varphi(p^\alpha)} = 1 + kp^\alpha \tag{4.141}$$

$$\Rightarrow a^{\varphi\left(p^{\alpha+1}\right)} = a^{p^\alpha (p-1)} = a^{p\varphi(p^\alpha)} \tag{4.142}$$

$$= (1 + kp^\alpha)^p \tag{4.143}$$

$$= 1 + \sum_{j=1}^{p} \binom{p}{j} k^j p^{j\alpha} \tag{4.144}$$

In (4.142) we have used (4.132). p^α divides every single term of the sum, $p^\alpha | p^{j\alpha}$ and $p | \binom{p}{j}$. It therefore follows

$$p^{\alpha+1} | \sum_{j=1}^{p} \binom{p}{j} k^j p^{j\alpha} \tag{4.145}$$

and

$$a^{\varphi\left(p^{\alpha+1}\right)} = 1 \left(\mathrm{mod}\ p^{\alpha+1}\right) , \tag{4.146}$$

which proves the induction step.

For an arbitrary $n = p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m}$, $a^{\varphi(n)} = 1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right) \forall j$, since $\varphi(n)$ is a multiple of $\varphi\left(p_j^{\alpha_j}\right)$: In general we have for $b = lk + 1 = 1 \,(\mathrm{mod}\ k)$ also $b^n = 1 \,(\mathrm{mod}\ k)$, because $b^n = (lk+1)^n = 1 + mk = 1 \,(\mathrm{mod}\ k)$, $m \in \mathbb{Z}$. Then we can write

$$\begin{aligned} a^{\varphi(n)} =& a^{\prod_j \varphi\left(p_j^{\alpha_j}\right)} && (4.147)\\ =& \left(a^{\varphi\left(p_j^{\alpha_j}\right)}\right)^{\prod_{k\neq j} \varphi\left(p_k^{\alpha_k}\right)} && (4.148)\\ =& 1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right) \forall j \,. && (4.149) \end{aligned}$$

The Chinese remainder theorem dictates that the solution of $x = 1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$ $\forall j$ satisfies $x = 1 \,(\mathrm{mod}\ n)$ ($(\mathrm{mod}\ n)$ for different solutions), thus $x = a^{\varphi(n)} = 1 \,(\mathrm{mod}\ n)$. □

Definition 7 (Order)
The order r of $x \,(mod\ N)$, $1 \leq x < N$ is defined as the smallest number $r \in \mathbb{Z}^+$, which satisfies

$$x^r = 1 \,(mod\ N) \tag{4.150}$$

There exists an efficient q-algorithm for determining r, however no classical one is known. Knowing the order of a random number $x \,(\mathrm{mod}\ N)$ makes the factorisation of the number N easy.

Theorem 10
Let $x^r = 1 \,(mod\ N)$, $1 \leq x < N$ where r is the order of $x \,(mod\ N)$. If r is an even number and

$$x^{r/2} \neq \pm 1 \,(mod\ N) \tag{4.151}$$

then at least one of the greatest common divisors $\gcd\left(x^{r/2} - 1, N\right)$ or $\gcd\left(x^{r/2} + 1, N\right)$ is a non-trivial factor of N (non-trivial meaning $\neq 1, N$). This factor can be found using $\mathcal{O}\left(\lceil \log_2 N \rceil^3\right)$ operations.

Proof.

From $x^r = 1 \,(\text{mod } N)$ we have $x^r - 1 = kN, k \in \mathbb{Z}$ by definition. If r is even, then

$$\left(x^{r/2} - 1\right)\left(x^{r/2} + 1\right) = kN \tag{4.152}$$

$$\iff \frac{\left(x^{r/2} - 1\right)\left(x^{r/2} + 1\right)}{N} = k \tag{4.153}$$

where N then has to have a factor in common with the first or the second bracket, $x^{r/2} - 1$ or $x^{r/2} + 1$, since N divides the product of both. Since we require $x^{r/2} \neq \pm 1 \,(\text{mod } N)$ as a prerequisite, we have guaranteed that neither of the factors $x^{r/2} \pm 1$ is a multiple of N; otherwise we could find $x^{r/2} \pm 1 = 0 \,(\text{mod } N)$. Since neither factor is a multiple of N, the common factor can not be N. Calculating the two gcd $\left(x^{r/2} \pm 1, N\right)$ thus yields at least one non-trivial factor of N. □

Determining a factor of N this way is not yet efficient, as $x^{r/2} \pm 1$ is much (exponentially) larger than x. However if we take into account the fact that if a, N have a common, non-trivial divisor, then so does $a \,(\text{mod } N) = a - lN, l \in \mathbb{Z}$, $0 \leq a - lN < N$, because common divisors of a and N also divide lN. This leads us to the realisation that also the two numbers

$$\gcd\left(\left(x^{r/2} - 1\right) (\text{mod } N), N\right) \textit{ and } \gcd\left(\left(x^{r/2} + 1\right) (\text{mod } N), N\right) \tag{4.154}$$

yield a non-trivial factor of N. Euclid's algorithm requires $\mathcal{O}\left(L^3\right)$ elementary steps to find the common factor(s), since $a \,(\text{mod } N) < N$.

We are now left to show, that the prerequisites of the theorem, r even and $x^{r/2} \neq \pm 1 \,(\text{mod } N)$ are satisfied with a high probability. The case $x^{r/2} = +1 \,(\text{mod } N)$ is already ruled out by the definition of the order of $x \,(\text{mod } N)$. It is therefore sufficient to show that the case r odd *or* $x^{r/2} = -1 \,(\text{mod } N)$ are unlikely to occur. To prove this, we need more number theory. The reader not interested in the details may skip ahead to

To show this, take Z_n^* defined as the set of all elements which have an inverse $(\text{mod } n)$ in $\mathbb{Z}_n := \{1, 2, 3, \ldots, n\}$, i.e. do not share a common divisor with n.

Theorem 11
If p is an odd prime, $\alpha \in \mathbb{Z}^+$, then $Z_{p^\alpha}^*$ forms a cyclic group, i.e. there exists $g \in Z_{p^\alpha}^*$ such that $\forall x \in Z_{p^\alpha}^* \mid \exists l, 1 \leq l \leq \varphi\left(p^\alpha\right)$ with $g^l = x$. We call g the generator of the cyclic group and l the order of x.

Proof.

See [26] $p.16 - 23$. □

We do not reproduce the proof of theorem 11 here, but rather just illustrate it with an example.

Example 10
We choose $p = 5, \alpha = 1 \Rightarrow Z_5^* = \{1, 2, 3, 4\}$,

$$2^1 = 2\,(mod\ 5) \tag{4.155}$$
$$2^2 = 4\,(mod\ 5) \tag{4.156}$$
$$2^3 = 3\,(mod\ 5) \tag{4.157}$$
$$2^4 = 1\,(mod\ 5) \tag{4.158}$$

and obtain

x	1	2	3	4
l	4	1	3	2

So indeed all elements of Z_5^* can be obtained using the generator $g = 2$.

Lemma 5
Let p *be an odd prime and* 2^d *the largest power of* 2 *which divides* $\varphi(p^\alpha), \alpha \in \mathbb{Z}^+$.

Then 2^d *will, with a probability of* $1/2$ *also divide the order* $r\,(mod\ p^\alpha)$ *of a randomly and uniformly chosen element from* $Z_{p^\alpha}^*$.

Proof.

$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ is even, thus $d \geq 1$. $Z_{p^\alpha}^*$ is a cyclic group, thus there exists a generator g for the group which allows for the representation of any element in $Z_{p^\alpha}^*$ as $g^k \,(\text{mod}\ p^\alpha)$ where k is $1 \leq k \leq \varphi(p^\alpha)$. Let r be the order of $g^k \,(\text{mod}\ p^\alpha)$.

1. If k is odd and $g^{kr} = 1 \,(\text{mod}\ p^\alpha)$ by the definition of the order r, then kr has to be a multiple of $\varphi(p^\alpha)$ to allow for the generation of any of the $\varphi(p^\alpha)$ elements of the group, i.e. $\varphi(p^\alpha) \,|kr$. Because $\varphi(p^\alpha)$ is even and k is odd. The power of 2 contained in $\varphi(p^\alpha)$ must be able to divide r: $2^d|r$.

2. If k is even, then

$$g^{k\varphi(p^\alpha)/2} = \left(g^{\varphi(p^\alpha)}\right)^{k/2} \tag{4.159}$$

$$= 1^{k/2} \,(\mathrm{mod}\; p^\alpha) = 1 \,(\mathrm{mod}\; p^\alpha) \tag{4.160}$$

where we made use of Euler's generalisation $a^{\varphi(n)} = 1 \,(\mathrm{mod}\; n)$ with $n = p^\alpha$ and $a = g$. By definition of the order $g^{kr} \equiv 1 \,(\mathrm{mod}\; p^\alpha)$ where r is the smallest such integer number, and thus $r|\varphi\left(p^\alpha\right)/2$. However this means, that the power of 2 contained in r must be smaller or equal to $\varphi\left(p^\alpha\right)/2$, i.e. smaller or equal to $\leq 2^{d-1}$. In return this means that $2^d \not| r$.

This results in the splitting of $Z^*_{p^\alpha}$ into two equally large parts, $x = g^k$ where k is either even or odd. For the first case (k odd) we found $2^d|r$, where $r =$ order of $g^k \,(\mathrm{mod}\; \varphi(p^\alpha))$ for the second case (k even) we found $2^d \not| r$. This result implies, that a randomly chosen (equally distributed) number from $Z^*_{p^\alpha}$ has the property that 2^d divides its order $(\mathrm{mod}\; p^\alpha)$ with probability $1/2$. □

Example 11
Take again our previous example $p = 5, \alpha = 1$. This group has $\varphi(p) = 4$ and thus the highest power of two $d = 2$.

- *$k = 1, 3$ odd selects the elements $x = 2, 3$, respectively, yielding for the two orders*

$$2^4 = 16 = 1 \,(mod\; 5) \tag{4.161}$$

$$3^4 = 81 = 1 \,(mod\; 5) \tag{4.162}$$

i.e. $r = 4, 4$ each.

- *$k = 2, 4$ even select the elements $x = 4, 1$, respectively, yielding*

$$4^2 = 16 = 1 \,(mod\; 5) \tag{4.163}$$

$$1^1 = 1 = 1 \,(mod\; 5) \tag{4.164}$$

i.e. $r = 2, 1$ as the orders each.

This demonstrates that in 2 out of 4 cases (probability $1/2$) the order r is divided by $2^d = 2^2 = 4$.

Theorem 12
Let $N = p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m}$ be the prime factorisation of an arbitrary odd integer number. Let x be chosen randomly and uniformly distributed from $\mathbb{Z}^*_N$ (i.e. all numbers in $\{1, 2, \ldots, N-1\}$ having $\gcd(x, N) = 1$). Let also be r the order of $x \,(mod\; N)$. Then the probability

$$p\left(r \;\; odd \;\; \vee x^{r/2} = -1 \,(mod\; N)\right) \leq \frac{1}{2^m} \tag{4.165}$$

Proof.

Due to the Chinese remainder theorem, randomly choosing a uniformly distributed numbers $x \in \mathbb{Z}_N^*$ is equivalent to randomly choosing an equally distributed number $x_j \in \mathbb{Z}^*_{p_j^{\alpha_j}}$ where $x = x_j \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$. Let r_j be the order of $x_j \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$, 2^{f_j} the highest power of 2 that divides r_j, and 2^f the highest power of 2 that divides r.

First, we note that $r_j | r\ \forall j$. To see this, observe that

$$x_j^{r_j} = 1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right) \qquad \text{and} \qquad x^r = 1 \,(\mathrm{mod}\ N) \tag{4.166}$$

From the second equation, we can write

$$x^r - 1 = kN = k \prod_j p_j^{\alpha_j}, k \in \mathbb{Z}, \tag{4.167}$$

from which we can see that $\forall j$

$$p_j^{\alpha_j} | \,(x^r - 1) \Rightarrow x^r = 1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right). \tag{4.168}$$

So we have both

$$x^r = 1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right) \text{ and } x_j^r = 1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right). \tag{4.169}$$

Because r_j is the smallest of such r_j where $x_j^{r_j} = 1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$ holds, r has to be a multiple of r_j, i.e. $r_j | r$.

We distinguish two cases

1. r is odd. Then r_j also has to be odd to be able to fulfill $r_j | r$. Then the highest power of 2 is equal for all j, $f_j = 0 = f\ \forall j = 1, \ldots, m$.
2. r is even and $x^{r/2} = -1 \,(\mathrm{mod}\ N)$. By definition of r, $x^r = 1 \,(\mathrm{mod}\ N) \Rightarrow x^{r/2} = \pm 1 \,(\mathrm{mod}\ N)$ (because $\left(x^{r/2} - 1\right)\left(x^{r/2} + 1\right) = 0 \,(\mathrm{mod}\ N)$). The case $x^{r/2} = 1 \,(\mathrm{mod}\ N)$ is excluded by definition (since r is the order of x and not $r/2$). We therefore find $x^{r/2} = -1 \,(\mathrm{mod}\ N)$ which is equivalent to the existence of k such that $\left(x^{r/2} + 1\right) = kN = k \prod_j p_j^{\alpha_j}$. Then $p_j^{\alpha_j} | \left(x^{r/2} + 1\right)$ and hence $x^{r/2} = -1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$.

   If $r_j | r/2$ was true, then $x^{r/2} = x^{l r_j} = x_j^{l r_j} \left(\mathrm{mod}\ p_j^{\alpha_j}\right) = 1^l = 1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$, where in the second equality the Chinese remainder theorem was used, $x = x_j \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$. However, we have $x^{r/2} = -1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$ and thus $r_j \not| r/2$. Simultaneously $r_j | r$, implying that r_j must contain as many powers of 2 as r,

i.e. $2^{f_j} = 2^f \iff f_j = f$, i.e. also in case 2. all f_j, are identical. Thus r_j has the prime decomposition

$$r_j = 2^{f_j} \prod_{p_l > 2} p_l^{\rho_j^{(l)}} \tag{4.170}$$

with some powers $\rho_j^{(l)}$ and $f_j = f \forall j$. Let

$$\varphi\left(p_j^{\alpha_j}\right) = 2^{d_j} \prod_{p_l > 2} p_l^{\phi_j^{(l)}} \ . \tag{4.171}$$

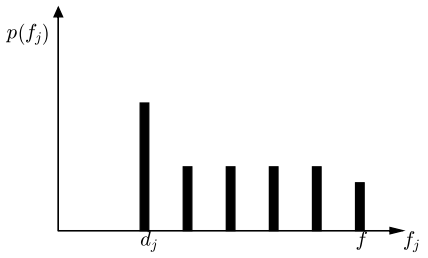
We upper bound now the probability that for randomly chosen $x \in Z_N^*$ (or equivalently randomly chosen $x_j \in Z^*_{p_j^{\alpha_j}}$ with $x = x_j \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$) and r_j the order of $x_j \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$ indeed all f_j are equal. For this we use lemma 5 for $p = p_j$ and $x = x_j$, i.e. we have that $2^{d_j} | r_j$ with a probability of $1/2$, where r_j is the order of random $x_j \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$, i.e. $x_j^{r_j} = 1 \left(\mathrm{mod}\ p_j^{\alpha_j}\right)$ and r_j is the smallest of such numbers. In other words $f_j \geq d_j$ with a probability of $p = 1/2$ and equally $p\left(f_j < d_j\right) = 1/2$.

Now, for all j it follows from $r_j | r$: $f_j \leq f$. For $d = \sum_j d_j$ obviously $d_j \leq d$. Then

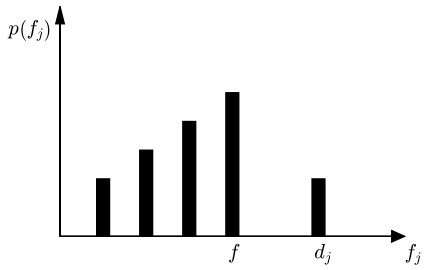
$$\left.\begin{array}{l} x^r = 1 \left(\mathrm{mod}\ N\right) \\ x^{\varphi(N)} = 1 \left(\mathrm{mod}\ N\right) \end{array}\right\} \Rightarrow r | \varphi(N) \Rightarrow f \leq d. \tag{4.172}$$

We can distinguish two cases for a given j:

1. $f \geq d_j \Rightarrow p\left(f_j = f\right) \leq p\left(f_j \geq d_j\right) = 1/2$.



2. $f < d_j \Rightarrow p\left(f_j = f\right) \leq p\left(f_j < d_j\right) = 1/2$.



This also means that the probability for all f_j to be the same for all j is

$$p\left(f_j = f \forall j\right)_{j=1,\ldots,m} \leq \left(\frac{1}{2}\right)^m \tag{4.173}$$

Since we have shown that for the two cases in (4.165) all $f_j = f$, theorem 12 follows. □

In summary, we found that if we can determine the order r of a $x \,(\text{mod } N)$, $1 \leq x < N$ with $\gcd(x, N) = 1$ efficiently, then we can also efficiently factorise N. The next section shows how the order of a $x \,(\text{mod } N)$ can be found efficiently with a quantum algorithm, which makes quantum order finding the key subroutine of Shor's factoring algorithm.

4.6 (Quantum) Order Finding

We defined the order of $x \,(\text{mod } N)$ as the least positive $r \in \mathbb{N}$ which satisfies $x^r = 1 \,(\text{mod } N)$ for $x, N \in \mathbb{N}$, $x < N$ and x, N are co-prime ($\gcd(x, N) = 1$).

Example 12
Let $x = 2, N = 3$, then we find the order of $x \,(mod\ N)$ by trial:

$$r = 1 : 2^1 \,(mod\ 3) = 2 \tag{4.174}$$
$$r = 2 : 2^2 \,(mod\ 3) = 1 \tag{4.175}$$

showing that the order of $2 \,(mod\ 3)$ is $r = 2$.

There is no classical algorithm known for order finding that is polynomial in L (the number of bits needed to specify the problem):

$$L := \lceil \log_2 \{N\} \rceil \,. \tag{4.176}$$

But there is a q-algorithm for order finding: It is simply phase estimation applied to a unitary operation $U(x, N)$ defined through

$$U(x, N) |y\rangle := |xy \,(\mathrm{mod}\ N)\rangle \tag{4.177}$$

for $y \in \{0,1\}^L$, i.e. the action of $U(x, N)$ on $|y\rangle$ is the multiplication of y with $x \,(\mathrm{mod}\ N)$. By convention we set $xy \,(\mathrm{mod}\ N) = y$ if $N \leq y \leq 2^L - 1$, i.e. $U(x, N)$ acts as the identity operation in that range of states $|y\rangle$, and non-trivially only for $0 \leq y \leq N - 1$.

To see this, note that the states

$$|u_s\rangle := \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\{-i2\pi sk/r\} \, |x^k \,(\mathrm{mod}\ N)\rangle \,, \qquad 0 \leq s \leq r-1, s \in \mathbb{N} \tag{4.178}$$

are eigenstates of $U(x, N)$ for integer s with $0 \leq s \leq r-1$ to an eigenvalue that contains information about r. This is shown by a simple calculation:

$$\begin{aligned} U(x, N) |u_s\rangle =& \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\{-i2\pi sk/r\} \, |x^{k+1} \,(\mathrm{mod}\ N)\rangle & (4.179)\\ =& \frac{1}{\sqrt{r}} \sum_{k'=1}^{r} \exp\{-i2\pi s(k'-1)/r\} \, |x^{k'} \,(\mathrm{mod}\ N)\rangle & (4.180)\\ =& 2^{i2\pi s/r} \frac{1}{\sqrt{r}} \sum_{k=1}^{r} \exp\{-i2\pi sk/r\} \, |x^k \,(\mathrm{mod}\ N)\rangle \,, & (4.181)\\ =& \exp\{i2\pi s/r\} \, |u_s\rangle \,. & (4.182) \end{aligned}$$

We substituted $k' = k + 1$ and used $x^r \,(\mathrm{mod}\ N) = 1$, i.e. the term $k = r$ can be replaced with $k = 0$. So we can use the phase estimation algorithm to find s/r. Below we will see that r can be extracted from s/r efficiently classically by a continued-fraction expansion.

The implementation of the algorithm requires an efficient calculation of $U^{2^j}(x, N)$ and an efficient preparation of the eigenstates $|u_s\rangle$ or at least a superposition of the eigenstates.

As a reminder, x, N, are classical information. In Shor's factoring algorithm, if N is the number to be factorised, then x is a random number $1 < x \leq N$ with $\gcd(x, N) = 1$. U^{2^j} comes up, because

$$|z\rangle |y\rangle \xrightarrow{U^z} |z\rangle |x^z y \,(\text{mod } N)\rangle = |z\rangle |x^{z_t 2^{t-1}} \cdot \ldots \cdot x^{z_1 2^0} y \,(\text{mod } N)\rangle \tag{4.183}$$

$$= |z\rangle \, U^{z_t 2^{t-1}} \cdot \ldots \cdot U^{z_1 2^0} |y\rangle \ , \tag{4.184}$$

where the application of U^{2^j} is conditioned by $z_j = 1$ for $j = 0, \ldots, t-1$. The calculation (mod N) is contained in the definition of U.

As we can see, the controlled application of U^{2^j}, conditioned by z_j, is equivalent to multiplying y with $x^z \,(\text{mod } N)$. One calculates $x^z \,(\text{mod } N)$ reversibly in an additional, third register and then multiplies it reversibly with y. Calculation of the operators U^{2^j}, required by $x^z \,(\text{mod } N)$, is achieved by iteratively squaring U:

$$U \cdot U = U^{2^0} \cdot U^{2^0} = U^{2 \cdot 2^0} = U^{2^1} \tag{4.185}$$

$$U^{2^1} \cdot U^{2^1} = U^{2 \cdot 2^1} = U^{2^2} \tag{4.186}$$

$$\vdots \tag{4.187}$$

$$U^{2^n} \cdot U^{2^n} = U^{2^{n+1}} \tag{4.188}$$

Any U^{2^j}, $j = 0, \ldots, t-1$ can hence be obtained by $t-1$ squaring operations starting with U. Squaring is multiplication, i.e. requires of $\mathcal{O}(L^2)$ operations . Recall that for successful phase estimation, we need $t = n + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil = \mathcal{O}(L)$ qubits for an estimate of φ accurate to n-bits. Since $\varphi = s/r$ and r, s can both be up to L bits long, we require φ to precision $> 2L$ bits and we hence set $n = 2L + 1$, leading to the requirement of

$$t = 2L + 1 + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil = \mathcal{O}(L) \tag{4.189}$$

qubits in the first register. We then multiply with y, which also costs $\mathcal{O}(L^2)$ elementary operations. In total we require $\mathcal{O}(L) \cdot \mathcal{O}(L^2) = \mathcal{O}(L^3)$ operations.

As for the preparation of the system in an eigenstate $|u_s\rangle$ of $U(x, N)$ it is clear that $|u_s\rangle$ cannot be prepared since it would require us to know r beforehand (in which case obviously we would not need to perform the algorithm). However, one easily shows that

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \ . \tag{4.190}$$

One can therefore simply start the algorithm with the second register in the state $|1\rangle$ and then one gains an estimation of the phase at the end of the algorithm, $\varphi \simeq s/r$ with s randomly and evenly distributed from $s \in \{0, \ldots, r-1\}$, accuracy of $2L+1$ bits, and a success probability of at least $(1-\varepsilon)/r$.

After obtaining φ, we can use continued fractions to efficiently determine numbers s, r which fulfil $s/r \simeq \varphi$.

Definition 8 (Continued fraction)
Continued fractions allow us to describe real numbers using only integer numbers.

A finite continued fraction is defined by

$$[a_0, a_1, \ldots, a_M] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + a_{M-1} + \cfrac{1}{a_M}}}} \tag{4.191}$$

If $M \to \infty$ then we can also describe irrational numbers, e.g.

$$s = \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ldots}}} \tag{4.192}$$

where

$$s = \frac{1}{2+s} \tag{4.193}$$

is the representation of $s = \sqrt{2} - 1$.

We use the term "m-th convergent" for $[a_0, \ldots, a_m]$ with $0 \leq m \leq M$.

Example 13

The continued fraction of $31/13$ *is*

$$\frac{31}{13} = \underbrace{2}_{\textit{integer part}} + \underbrace{5/13}_{\textit{fractional part}} \tag{4.194}$$

$$\underset{\textit{invert}}{=} 2 + \frac{1}{\frac{13}{5}} \qquad \underset{\textit{split}}{=} 2 + \frac{1}{2 + \frac{3}{5}} \qquad \underset{\textit{invert}}{=} 2 + \frac{1}{2 + 1/\left(\frac{5}{3}\right)} \qquad \underset{\textit{split}}{=} 2 + \frac{1}{2 + \frac{1}{1 + \frac{2}{3}}} \tag{4.195}$$

$$\underset{\textit{invert}}{=} 2 + \frac{1}{2 + \frac{1}{1 + 1/\left(\frac{3}{2}\right)}} \qquad \underset{\textit{split}}{=} 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}} \tag{4.196}$$

$$= [2, 2, 1, 1, 2] \tag{4.197}$$

The continued fraction converges for any rational number in a finite number of steps, as the numerators are strictly decreasing (i.e. 31, 13, 5, 3, 2, 1) and the algorithm stops when after a split the last denominator is an integer (i.e. 2 in the above example), corresponding to a_M. For s, r L-bit integers, we need $\mathcal{O}(L)$ *split* and *invert* steps, each using $\mathcal{O}(L^2)$ gates for the required elementary arithmetic, resulting in a runtime of order $\mathcal{O}(L^3)$.

Finding r from the phase φ returned by the quantum phase estimation algorithm applied to $U(x, N)$ is then based on the following theorem which we state without proof (see e.g. Appendix 4 of [31] for a proof):

Theorem 13
Let s/r *be a rational number such that*

$$\left|\frac{s}{r} - \varphi\right| \leq \frac{1}{2r^2}. \tag{4.198}$$

Then s/r *is a "convergent" of the continued fraction of* φ*and can be calculated in* $\mathcal{O}(L^3)$ *elementary operations.*

Hence, from a sufficiently good approximation of the exact s/r via a t-bit approximation of the phase φ returned from the phase estimation algorithm, the continued fraction algorithm will deliver a convergent of s/r that contains the sought order r of x (modulo N), and the entire quantum algorithm, including the classical post-processing via continued fractions, will need a runtime of order $\mathcal{O}(L^3)$ in the number L of bits.

4.6.1 Summary Order Finding

Input:

1. *Black box* $U(x, N)$, transforming the state $|j\rangle |k\rangle \xrightarrow{U(x,N)} |j\rangle |x^j k \pmod N\rangle$ where $\gcd(x, N) = 1$
2. t qubits prepared in the state $|0\rangle$, where $t = 2L + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right)\right\rceil$
3. L qubits prepared in the state $|1\rangle$.

Output: Order r of $x \pmod N$.

Runtime: $\mathcal{O}(L^3)$.

Probability of success: $\sim \mathcal{O}(1)$.

Algorithm:

1. Start with the initial state
$$|0\rangle^{\otimes t} |1\rangle \ . \tag{4.199}$$
2. Apply $H^{\otimes t}$ to create the superposition
$$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle |1\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle \ . \tag{4.200}$$
3. Apply the black box $U(x, N)$ on the superposition, giving
$$\frac{1}{\sqrt{r \cdot 2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} \exp\{i2\pi sj/r\} |j\rangle |u_s\rangle \ . \tag{4.201}$$
4. Apply the inverse q-FT, $qFT^\dagger$ to the first register, giving
$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\left(\widetilde{s/r}\right) \cdot 2^t\rangle |u_s\rangle \ . \tag{4.202}$$
where $\widetilde{s/r}$ is an L-bit approximation of s/r
5. Measure the first register to obtain $\widetilde{s/r}$ in the form of
$$\widetilde{s/r} \cdot 2^t \, . \tag{4.203}$$
6. Apply the continued fraction algorithm to obtain r.

4.7 Factorisation

The core of Shor's quantum algorithm [37] for the factorisation of an integer number N consists in finding the order of a random number x modulo N, which is a problem of which we have seen above how it can be solved using the phase estimation q-algorithm. The fact that factorisation can be reduced to order finding rests on theorems 10 and 12 that were proven in section 4.5.

Input: $N \in \mathbb{Z}^+$.

Output: At least one non-trivial integer factor of N.

Runtime: $\mathcal{O}\left(\log\left(N\right)^3\right)$ operations.

Probability of success: $\mathcal{O}\left(1\right)$.

Algorithm: 1. If N is even, return the factor 2.

2. Use an efficient classical algorithm to determine if $N = a^b$ where $a \geq 1, b \geq 2$. If the algorithm is successful, then we have obtained the factor a.

3. If the classical algorithm is not successful choose a random $x, 1 < x \leq N - 1$. If $\gcd\left(x, N\right) > 1$, then return $\gcd\left(x, N\right)$ as the factor.

4. Use the q-algorithm for order finding to obtain the order r of $x \left(\mathrm{mod}\ N\right)$.

5. If r is even and $x^{r/2} \neq -1 \left(\mathrm{mod}\ N\right)$ calculate the two numbers $\gcd\left(x^{r/2} \pm 1, N\right)$. Check which one of the two numbers is a non-trivial factor of N. Return the respective factor. If r is odd or $x^{r/2} = -1 \left(\mathrm{mod}\ N\right)$, the algorithm has failed (however, see above for the probability of success of the algorithm). Go back to step 3.

4.8 Further Applications of the Quantum Fourier Transform

4.8.1 Determining a Function's Period

We already used this algorithm for the order finding q-algorithm, in which case the order r was the period of the function $f_x(k) = x^k \pmod N$:

$$\begin{aligned} f_x(k+r) =& x^{r+k} \pmod N && (4.204)\\ =& \underbrace{\left[x^r \pmod N\right]}_{=1} \left[x^k \pmod N\right] && (4.205)\\ =& f_x(k), && (4.206) \end{aligned}$$

i.e. $f_x(k+r) = f_x(k)$ where r is the period of the function. This approach can be used for any general function f with a period r, $f(x+r) = f(x)$. The calculation is done reversibly using U, $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$. There exists a q-algorithm, where applying U once is sufficient for determining the period r.

Input:

- A black box which implements U
- A q-register consisting of t q-bits for evaluating $y \oplus f(x)$, prepared in the state $|0\rangle$
- A q-register consisting of $t = \mathcal{O}(L + \log 1/\varepsilon)$ qubits prepared in the state $|0\rangle$, where L is determined by the magnitude of the period r, $0 < r < 2^L$

Output: The period r of the function $f(x)$, i.e. the smallest number r to fulfil $f(x+r) = f(x)$.

Runtime: The time required for a single application of U and additionally $\mathcal{O}(L^2)$ operations.

Probability of success: $\simeq \mathcal{O}(1)$.

Algorithm: 1. Starting state

$$|0\rangle|0\rangle \qquad (4.207)$$

2. Superposition

$$\xrightarrow{H^{\otimes t}} \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle \qquad (4.208)$$

3. Application of the black box on the superposition

$$\xrightarrow{U} \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle |f(x)\rangle \simeq \frac{1}{\sqrt{r\,2^t}} \sum_{l=0}^{r-1} \sum_{x=0}^{2^t-1} \exp\{i2\pi lx/r\} |x\rangle |\tilde{f}(l)\rangle \quad (4.209)$$

where

$$|\tilde{f}(l)\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} \exp\{-i2\pi lx/r\} |f(x)\rangle \quad (4.210)$$

is the q-Fourier Transform of $|f(x)\rangle$.
We use the $\simeq$ to indicate that the equation is based on $\sum_{l=0}^{r-1} \exp\{i2\pi l(x-y)/r\} \simeq r\delta_{x-y,kr}$ with $k \in \mathbb{Z}$. More precisely, this equation is exact for $x-y=kr$, whereas otherwise the value zero is found only approximatively. This is the same discussion as for phase estimation with a value of φ that is only approximated with t binary digits, and the approximation is therefore also covered by the error estimate of the phase estimation algorithm.

4. Inverse q-FT of the first register, $qFT^\dagger$ to obtain

$$\xrightarrow{FT^\dagger} \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |\widetilde{l/r}\rangle |\tilde{f}(l)\rangle \quad (4.211)$$

5. Measure the first register to obtain $\widetilde{l/r}$.

6. Apply the continued fraction algorithm to obtain r

4.8.2 Others

The q-FT can further be used to calculate discrete logarithms and in general solve the hidden subgroup problem.

4.9 Quantum Search Algorithm: Grover's Algorithm

Consider the following problem: We are searching for a single or multiple (M) objects with a certain property in a set of N objects. The property in question can be defined using a function f

$$f : x \to \{0,1\}, x \in \{0,\ldots,N-1\} \quad (4.212)$$

where the value of the function indicates the presence (absence) of the said property

$$f(x) = \begin{cases} 1 & \text{if the property is present} \\ 0 & \text{else, if the property is absent}\,. \end{cases} \tag{4.213}$$

In the absence of any relevant information regarding the structure of the database, any classical algorithm has to test $\mathcal{O}(N)$ objects to find one object with the desired property.

Example 14
Find the entry regarding the person Markus Jäger in a list of data sets.

⇒ *If the list of names is unsorted, then all entries in the collection have to be searched. On average, this requires $N/2$ trials.*

⇒ *If the list of names is sorted in alphabetical order (e.g. phone book), then only $\sim \ln N$ trials are required. However, to sort a collection of items requires $\sim N \ln N$ steps (classical algorithm: quick sort) beforehand.*

Grover's algorithm [24] is able to achieve the same result on an unsorted collection of items in $\mathcal{O}\left(\sqrt{N}\right)$ steps.

4.9.1 Oracle O

The oracle is the quantum version of the function $f(x)$, using an *oracle qubit* $|q\rangle$

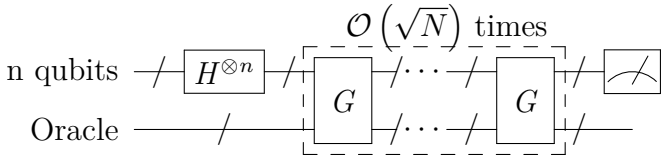
$$|x\rangle\,|q\rangle \xrightarrow{O} |x\rangle\,|q \oplus f(x)\rangle \tag{4.214}$$

$|q\rangle$ is to be prepared in the initial state $(|0\rangle - |1\rangle)/\sqrt{2}$. Using the oracle, the result of the function is then encoded as a phase information (like with the *Deutsch-Josza algorithm*):

$$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{O} (-1)^{f(x)}\,|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{4.215}$$

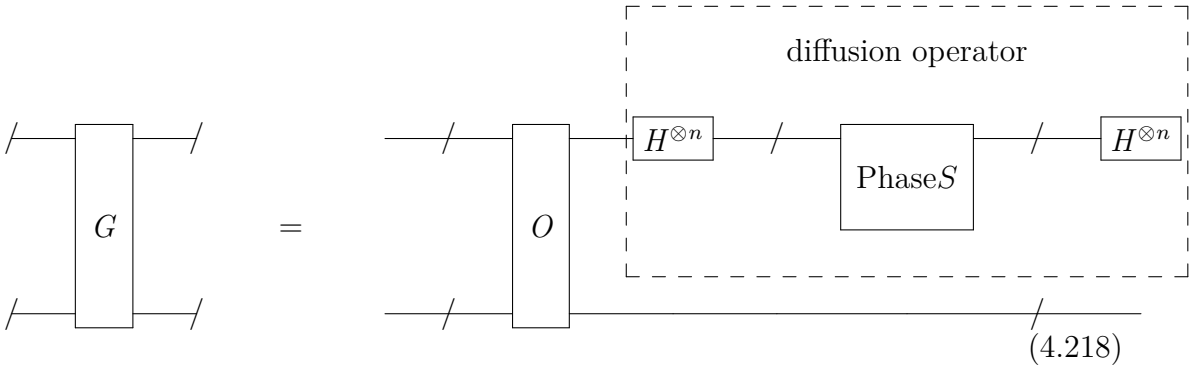
At this point, we may abstract from $|q\rangle$ and simply define the oracle by its effect on the working qubit as a phase shift by π if the state $|x\rangle$ exhibits the property in question:

$$|x\rangle \xrightarrow{O} (-1)^{f(x)}\,|x\rangle \tag{4.216}$$



(4.217)

Figure 4.7: Grover's algorithm using $\mathcal{O}\left(\sqrt{N}\right)$ Grover iterators G.



(4.218)

Figure 4.8: Grover iterator used by Grover's search algorithm, where the oracle O encodes the function evaluation $f(x)$ as a phase $(-1)^{f(x)}$ and the phase gate S maps $|0\rangle \mapsto |0\rangle$ and $|x\rangle \mapsto -|x\rangle$ for $x > 0$.

4.9.2 Grover's Algorithm

The q-circuit of the Grover's algorithm is shown in Figure 4.7 and requires, besides the n qubits to encode the data set, another register for the oracle to work on. This *working memory* is not relevant for the search algorithm itself, but required by the oracle to evaluate $f(x)$.

The Grover iterator G consists of the oracle and the so called *(Grover) diffusion operator*, see Figure 4.8. Every single of these steps can be executed efficiently using a q-computer (efficiently referring to using only a polynomial number of gates, poly(n) where $n = \log_2\{N\}$): The required $2n$ H gates and also the conditional phase shift require only $\sim \mathcal{O}(n)$ gates. The effort required to implement and execute the oracle depends on the function $f(x)$; however in this context only the number of calls of the oracle is relevant and considered.

Grover's iterator is defined as

$$G = H^{\otimes n} S H^{\otimes n} O \tag{4.219}$$

where the phase gate is given by

$$S = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & \ddots & \\ & & & -1 \end{pmatrix} = 2\left|0\right\rangle\left\langle 0\right| - \mathbb{1}\,. \tag{4.220}$$

With

$$\left|\psi\right\rangle \equiv \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \left|x\right\rangle, \tag{4.221}$$

where $N = 2^n$, we have $H^{\otimes n}\left|0\right\rangle = \left|\psi\right\rangle$ and hence

$$G = \underbrace{\left(2\left|\psi\right\rangle\left\langle\psi\right| - \mathbb{1}\right)}_{:=D} O\,. \tag{4.222}$$

The effect of $D = \left(2\left|\psi\right\rangle\left\langle\psi\right| - \mathbb{1}\right)$ on an arbitrary state $\left|\phi\right\rangle = \sum_{k=0}^{N-1} \alpha_k \left|k\right\rangle$ is

$$D \sum_{k=0}^{N-1} \alpha_k \left|k\right\rangle = \sum_k \alpha_k \left(2 \underbrace{\left|\psi\right\rangle}_{=1/\sqrt{N}\sum_l \left|l\right\rangle} \underbrace{\left\langle\psi|k\right\rangle}_{=1/\sqrt{N}} - \left|k\right\rangle \right) \tag{4.223}$$

$$= \sum_k \alpha_k \left(2\frac{1}{N} \sum_l \left|l\right\rangle - 1 \right) \left|k\right\rangle \tag{4.224}$$

$$= \sum_l 2\langle\alpha\rangle \left|l\right\rangle - \sum_k \alpha_k \left|k\right\rangle \tag{4.225}$$

$$= \sum_k \left(-\alpha_k + 2\langle\alpha\rangle\right) \left|k\right\rangle \tag{4.226}$$

where $\langle\alpha\rangle := 1/N \sum_k \alpha_k$. Thus D is an *inversion about the mean* of the vector $(\alpha_1, \ldots, \alpha_k)$.

Another way of seeing the action of D is found by decomposing $\left|\phi\right\rangle$ into components parallel and perpendicular to $\left|\psi\right\rangle$, $\left|\phi\right\rangle = \left|\phi_{||}\right\rangle + \left|\phi_{\perp}\right\rangle$, where comparing with $\left|\phi\right\rangle = \left|\psi\right\rangle\left\langle\psi|\phi\right\rangle + \left(\mathbb{1} - \left\langle\psi\right\rangle\right)\left|\phi\right\rangle$ allows us to identify $\left|\phi_{||}\right\rangle = \left|\psi\right\rangle\left\langle\psi|\phi\right\rangle$. This gives

$$\begin{aligned} D\left|\phi\right\rangle &= 2\left|\psi\right\rangle\left\langle\psi|\phi\right\rangle - \left|\phi\right\rangle \\ &= 2\left|\psi\right\rangle\left\langle\psi|\phi_{||}\right\rangle - \left(\left|\phi_{||}\right\rangle + \left|\phi_{\perp}\right\rangle\right) \\ &= \left|\phi_{||}\right\rangle - \left|\phi_{\perp}\right\rangle\,. \end{aligned} \tag{4.227}$$

Hence, D preserves the component of $\left|\phi\right\rangle$ parallel to $\left|\psi\right\rangle$ and flips the sign of the perpendicular component. We say that $\left|\phi\right\rangle$ is reflected on $\left|\psi\right\rangle$.

4.9.3 Geometrical Visualisation of the Grover's Iterator G

Consider the two dimensional subspace of Hilbert space $\mathcal{H}$ that is spanned by the vectors

$$|\alpha\rangle := \frac{1}{\sqrt{N-M}} \sum_x{}'' |x\rangle \tag{4.228}$$

where $\sum_x{}'' = \sum_{x|f(x)=0}$ is the sum of all objects not having the property in question, and

$$|\beta\rangle := \frac{1}{\sqrt{M}} \sum_x{}' |x\rangle \tag{4.229}$$

where $\sum_x{}' = \sum_{x|f(x)=1}$ is the sum of all solution vectors. The vector $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$, produced by the initial $H^{\otimes n}$ and fed into G^k, can be expressed as

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle \tag{4.230}$$

$$=: \cos\frac{\Theta}{2} |\alpha\rangle + \sin\frac{\Theta}{2} |\beta\rangle \tag{4.231}$$

where we defined $\cos\Theta/2 := \sqrt{(N-M)/N}$ and $\sin\Theta/2 := \sqrt{M/N}$. For obvious reasons $\langle\alpha|\beta\rangle = 0$, i.e. $|\alpha\rangle$ and $|\beta\rangle$ are two orthogonal basis vectors of the mentioned subspace.

The oracle produces a reflection on $|\alpha\rangle$ within the plane of $|\alpha\rangle$ and $|\beta\rangle$. Originally $|\psi\rangle$ is located between $|\alpha\rangle, |\beta\rangle$ since both square-roots in (4.230) are positive. Now,

$$O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle, \tag{4.232}$$

because the solution states get a phase factor of (-1). This holds $\forall a, b$, i.e. for all states in the plane spanned by $|\alpha\rangle$ and $|\beta\rangle$.

As shown above, the inversion about the mean, $D = (2|\psi\rangle\langle\psi| - \mathbb{1})$, creates a reflection on $|\psi\rangle$ in the plane of $|\alpha\rangle, |\beta\rangle$. The effects of oracle and inversion on $|\psi\rangle$ are shown for the first step (where the input state is also $|\psi\rangle$) in Figure 4.9 .

We deduce from the figure that G increases the initial angle $\Theta/2$ by Θ, i.e.

$$G|\psi\rangle = \cos\frac{3\Theta}{2} |\alpha\rangle + \sin\frac{3\Theta}{2} |\beta\rangle. \tag{4.233}$$

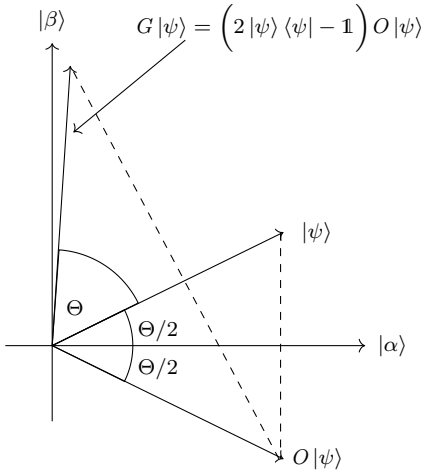


Figure 4.9: The Grover iterator G results in an increase of the angle Θ_0 between α and an input state $|\phi\rangle$ by Θ, where Θ is defined via $\cos\Theta/2 = \sqrt{(N-M)/N}$. $N = 2^n$ is the dimension of the Hilbert space (=maximum size of the database), and M the number of items with the searched property. In the first iteration, $\Theta_0 = \Theta/2$.

Note that with $M = \mathcal{O}(1), \Theta$ is is initially very small, $\mathcal{O}(1/\sqrt{N})$, but was drawn larger for illustration. In the next iteration $G|\psi\rangle$ replaces $|\psi\rangle$ as input state. The oracle still reflects $G|\psi\rangle$ about $|\alpha\rangle$, and the inversion about the mean still increases the angle between $|\alpha\rangle$ and $G|\psi\rangle$ by the same amount Θ, with Θ defined in eq. (4.230). In fact, the increase by the same angle Θ in one iteration of G holds for any input state in the plane spanned by $|\alpha\rangle$ and $|\beta\rangle$, as one can easily show with direct calculation. It is also clear that this must be the case, however, since G is a fixed quantum circuit that is independent of the input state. Hence, whatever the input state in the plane spanned by $|\alpha\rangle$ and $|\beta\rangle$, it always acts as the same rotation with the same rotation angle Θ. After k iterations we have

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\Theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\Theta\right)|\beta\rangle\,. \tag{4.234}$$

Alternatively in matrix representation

$$G = \begin{pmatrix} \cos\Theta & -\sin\Theta \\ \sin\Theta & \cos\Theta \end{pmatrix} \tag{4.235}$$

in the basis $\{|\alpha\rangle, |\beta\rangle\}$, where

$$\sin\Theta = 2\sin\frac{\Theta}{2}\cos\frac{\Theta}{2} \tag{4.236}$$

$$= 2\sqrt{\frac{N-M}{N}}\sqrt{\frac{M}{N}} = 2\frac{\sqrt{M\,(N-M)}}{N} \tag{4.237}$$

4.9.4 Number of Iterations

Since the starting state is

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle = \cos\frac{\Theta}{2}\,|\alpha\rangle + \sin\frac{\Theta}{2}\,|\beta\rangle \tag{4.238}$$

we have to rotate the state by an angle $\pi/2 - \Theta/2 = \pi/2 - \arcsin\sqrt{M/N} = \arccos\sqrt{M/N}$ in order to reach $|\beta\rangle$. Applying G once on the state results in a rotation by Θ, thus one has to apply G

$$R = \mathrm{CI}\left(\frac{\arccos\sqrt{M/N}}{\Theta}\right) \tag{4.239}$$

times ($\mathrm{CI}(\ldots)$ indicates the closest integer number).

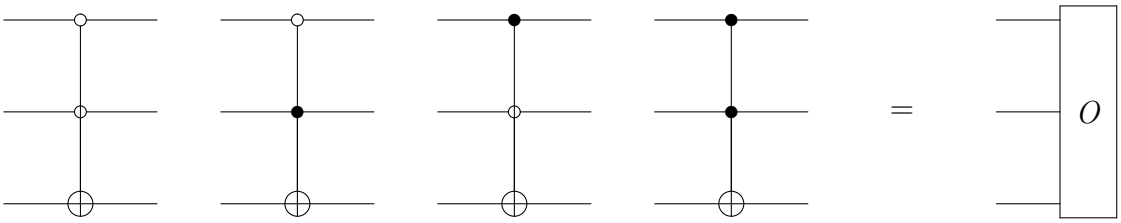
If $M \ll N$, then $\Theta \simeq \sin\Theta \simeq 2\sqrt{M/N}$. The error introduced to the final angle due to rounding is at most $\Theta/2 \simeq \sqrt{M/N}$ and thus the error probability is $\sim M/N$. If we know M, then we can apply G R times. One then obtains from (4.239) an upper bound of R by $\arccos \leq \pi/2$:

$$R \leq \left\lceil \frac{\pi}{2\Theta} \right\rceil$$

$\Big($where $\lceil x \rceil$ is the smallest integer number larger than x $\Big)$,
and because $\Theta/2 \geq \sin\Theta/2 = \sqrt{M/N}$

$$R \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil . \tag{4.240}$$

We can see that in any case $\mathcal{O}\left(\sqrt{N/M}\right)$ iterations suffice. At the end of the R iterations one gains a state close to $|\beta\rangle$, which is a superposition of all vectors which are solutions to the problem. By measuring the register, one obtains one of these solutions randomly.



(4.241)

Figure 4.10: Example for possible gates acting as oracle to encode $f(x)$. Since $|q\rangle = |-\rangle$ after the first Hadamard gate in Fig.4.11, activation of the X depending on the state of the first two qubits leads to a sign flip.

Example 15
Let $N = 4$, then we require 2 qubits and one additional working qubit. $f(x)$ encodes the property using one of the gates in Figure 4.10.

The complete algorithm is portrayed in Figure 4.11. One iteration of the circuit is sufficient:

$$R = \left\lceil \frac{\arccos 1/2}{2 \arcsin 1/2} \right\rceil = \left\lceil \frac{\pi/3}{\pi/3} \right\rceil = 1 \tag{4.242}$$

We check the phase shift, $|00\rangle \mapsto -|00\rangle, |x\rangle \mapsto |x\rangle \, \forall \, x > 0$ inside the diffusion operator D (dashed box in Fig.4.11):

$$|00\rangle \to X^2 |0\rangle \, XHXHX \, |0\rangle = -|00\rangle \tag{4.243}$$
$$|01\rangle \to X^2 |0\rangle \, XHXHX \, |1\rangle = |01\rangle \tag{4.244}$$
$$|10\rangle \to X^2 |1\rangle \underbrace{XHHX}_{=\mathbb{1}} |0\rangle = |10\rangle \tag{4.245}$$
$$|11\rangle \to X^2 |1\rangle \underbrace{XHHX}_{=\mathbb{1}} |1\rangle = |11\rangle \tag{4.246}$$

Thus for all cases we may write

$$|x\rangle \to (-1)^{\delta_{x,00}} |x\rangle = -\left(2 |0\rangle \langle 0| - \mathbb{1}\right) |x\rangle , \tag{4.247}$$

as required.

4.9.5 Conclusion

Grover's search algorithm can be summarized as follows.

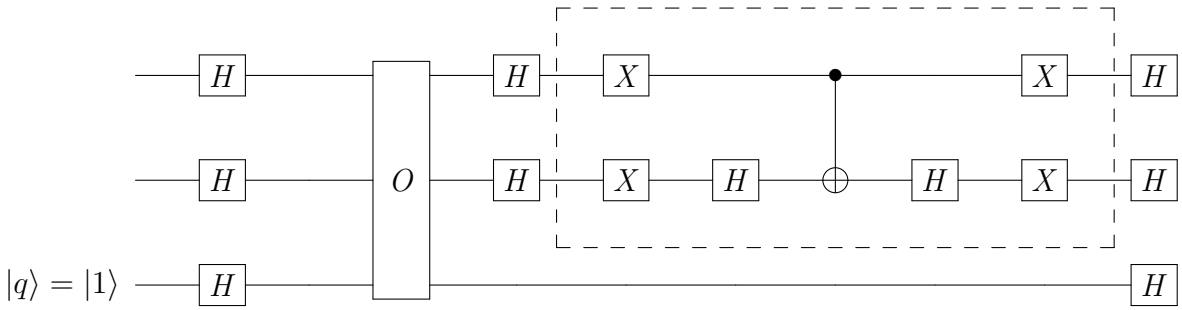


Figure 4.11: Representation as q-circuit of the complete Grover's algorithm for $N = 4$ and one oracle qubit. After the first Hadamard, the oracle qubit is in the state $|0\rangle - |1\rangle/\sqrt{2}$. The dashed box creates the phase shift $|00\rangle \mapsto -|00\rangle, |x\rangle \mapsto |x\rangle$ for $x > 0$, which is, up to a total phase, equivalent to $|x\rangle \mapsto -|x\rangle \, \forall \, x > 0$ and $|00\rangle \mapsto |00\rangle$.

Input: 1. *"Black box"* oracle O, which encodes the property $O|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ using the function $f(x) = 0 \forall 0 \leq x < 2^n$, except for M searched objects, for which $f(x_i) = 1$

2. $n + 1$ qubits initialised in $|0 \ldots 0\rangle|1\rangle$.

Output: x_0, i.e. one of the objects x_i for which $f(x_i) = 1$ in the first n qubits

Runtime: $R = \mathcal{O}\left(\sqrt{N}\right)$ applications of the iterator G, including one call to the oracle each.

Probability of success: $\mathcal{O}(1 - M/N)$

Algorithm: 1. Initialise the qubits to $|0\rangle^{\otimes n}|1\rangle$.

2. Apply the H gates on all qubits and in addition an X gate on the last (working) qubit. This gives the state

$$|\psi_l\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \tag{4.248}$$

3. Apply Grover's iterator G R times. If $m = 1$ and the sought object is x_0

$$G^R(|\psi_1\rangle) \simeq |x_0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{4.249}$$

4. Randomly obtain one x_i from the M eligible objects by measurement of the first register.

5 Quantum Communication

5.1 No-Cloning Theorem

In our classical world, we and the tele-communication servers around the globe work with copy-paste all the time: Classical information is being copied billions of time every day. Surprisingly, this is not possible in quantum mechanics, as was realized in the 1980s, see [15, 41]. The reason is that quantum information is encoded in quantum mechanical states. As the propagation of states in quantum mechanics is linear, a quantum copying machine should therefore be a linear transformation M affecting pure states in the following manner

$$M\left|\psi\right\rangle\left|0\right\rangle = \left|\psi\right\rangle\left|\psi\right\rangle \qquad \forall\left|\psi\right\rangle, \tag{5.1}$$

where the first $\left|\psi\right\rangle$ is the state to be copied and the second ket on the left-hand-side ($\left|0\right\rangle$) is a *reference state* to receive the state from the first system, corresponding to the empty sheet of paper in a classical copying machine.

Let us assume for the moment that such a machine exists. In the case of two input states, $\{\left|0\right\rangle, \left|1\right\rangle\}$, the machine should then act as:

$$\begin{aligned} M\left|0\right\rangle\left|0\right\rangle &= \left|0\right\rangle\left|0\right\rangle && (5.2)\\ M\left|1\right\rangle\left|0\right\rangle &= \left|1\right\rangle\left|1\right\rangle && (5.3)\\ M\left(a\left|0\right\rangle + b\left|1\right\rangle\right)\left|0\right\rangle &= \left(a\left|0\right\rangle + b\left|1\right\rangle\right)\left(a\left|0\right\rangle + b\left|1\right\rangle\right) && (5.4)\\ &= a^2\left|0\right\rangle\left|0\right\rangle + ab\left(\left|0\right\rangle\left|1\right\rangle + \left|1\right\rangle\left|0\right\rangle\right) + b^2\left|1\right\rangle\left|1\right\rangle\ . && (5.5) \end{aligned}$$

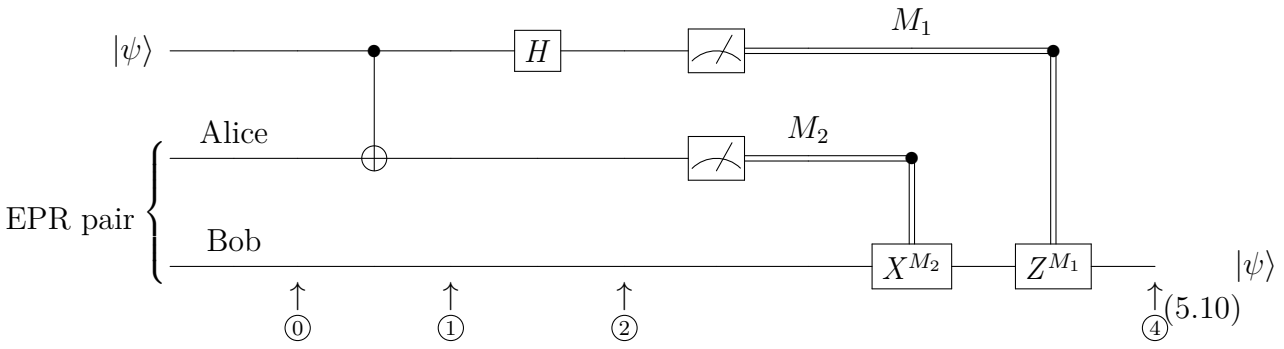
However, this behaviour would contradict the fact that M has to be linear, which implies for the last case

$$\begin{aligned} M\left(a\left|0\right\rangle + b\left|1\right\rangle\right)\left|0\right\rangle &= aM\left|0\right\rangle\left|0\right\rangle + bM\left|1\right\rangle\left|0\right\rangle && (5.6)\\ &= a\left|0\right\rangle\left|0\right\rangle + b\left|1\right\rangle\left|1\right\rangle. && (5.7) \end{aligned}$$

We see that this is only possible if $a^2 = a, ab = 0, b^2 = b$. The only solutions are $a = 1, b = 0$ or $a = 0, b = 1$, i.e. we can only create perfect copies of basis states that are orthogonal to each other. This is achieved by the $CNOT$gate for two qubits. Protocols for q-key distribution use non-orthogonal basis states because one does not want then to be perfectly copyable.

In	Out	
00	00	$\|0\rangle\|0\rangle \mapsto \|0\rangle\|0\rangle$
01	01	
10	11	$\|1\rangle\|0\rangle \mapsto \|1\rangle\|1\rangle$
11	10	

Table 5.1: $CNOT$ as perfect copying machine of orthogonal basis states $|0\rangle, |1\rangle$.



(5.10)

Figure 5.1: Using an EPR pair for q-teleportation.

5.2 Quantum Teleportation

It is nevertheless possible to perfectly transmit quantum states. One could send, of course, just a physical system, such as a photon, that was prepared in a certain state (e.g. the photon in a superposition of two polarzation states). A more elegant way that exploits entanglement (i.e. quantum correlations, see later) and classical communication is "quantum teleportation". Let

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad \alpha, \beta \in \mathbb{C} \tag{5.8}$$

be a single qubit state that Alice wants to teleport to Bob. She herself does not know the state. Let Alice be able to control also a second qubit that is initially entangled with a qubit of Bob prepared in the state

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{5.9}$$

This state is sometimes called EPR state (for Einstein-Podolsky-Rosen), Bell-state, or maximally entangled state. Consider the q-circuit in Figure 5.1.

$$|\psi_{⓪}\rangle = |\psi\rangle \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \tag{5.11}$$

$$= \frac{1}{\sqrt{2}} [\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle)] \tag{5.12}$$

$$|\psi_{①}\rangle = \frac{1}{\sqrt{2}} [\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|10\rangle + |01\rangle)] \tag{5.13}$$

$$|\psi_{②}\rangle = \frac{1}{2} [\alpha (|0\rangle + |1\rangle) (|00\rangle + |11\rangle) + \beta (|0\rangle - |1\rangle) (|10\rangle + |01\rangle)] \tag{5.14}$$

$$= \frac{1}{2} \Big[|00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) \tag{5.15}$$

$$+ |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle) \Big] \tag{5.16}$$

Alice then measures her two qubits and obtains the results (M_1, M_2). Depending on what she measures, the global state of the three qubits collapses onto different subspaces (Table 5.2). She communicates the measurement result to Bob, who

(M_1, M_2)	$\lvert\psi_{③}\rangle$	action
$(0,0)$	$\alpha \lvert0\rangle + \beta \lvert1\rangle$	$\lvert\psi\rangle = \lvert\psi_{④}\rangle$, no action required
$(0,1)$	$\alpha \lvert1\rangle + \beta \lvert0\rangle$	Alice tells Bob to apply X.
$(1,0)$	$\alpha \lvert0\rangle - \beta \lvert1\rangle$	Alice tells Bob to apply Z.
$(1,1)$	$\alpha \lvert1\rangle - \beta \lvert0\rangle$	Alice tells Bob to apply ZX.

Table 5.2: Possible results obtained by Alice through measurement, the resulting states, and the action of Bob needed to restore Alice's original state.

can apply a corrective action depending on the 4 possible outcomes. All of these different actions lead to $|\psi_{④}\rangle = |\psi\rangle$.

At the same time, Alice loses the q-state because of the measurement, such that there is no contradiction to the no-cloning theorem.

5.3 Quantum Key Distribution

To obtain a 100% secure encryption method, one can use the *Vernam cipher* (*1-time pad*). It works as follows:

Alice uses a string consisting of randomly chosen, uncorrelated zeros and ones and adds this string bitwise (mod 2)to her message to obtain the encrypted message.

Alice then transmits the encrypted message to Bob, who uses the same key to decrypt the encoded message by adding it again bitwise (mod 2). By this he obtains the original unencrypted message from Alice. Since the transmitted message is encrypted with a random key (which is used only once), the signal Eve could intercept during the transmission is purely random and thus contains no information for Eve.

An example is shown in Table 5.3.

Original message (Alice)	01110101
1-time pad (random string)	10010110
Bitwise sum (mod 2)(encrypted message)	11100011
Sum = Message transmitted to Bob	
Message received (Bob)	11100011
1-time pad (same random string)	10010110
Bitwise sum (mod 2)(decrypted message)	01110101

Table 5.3

The security of this method can be proven, given that the used 1-time pad consists of randomly chosen, uncorrelated bits and is used for encryption and decryption exactly once (and is then discarded). Until the invention of public key cryptography (*RSA*) in the 1970s, this method was the predominant method in cryptography.

The method has one important problem, however: how to transfer the key between the two communicating parties? Messengers were used as persons of trust, secret meetings were organized and private communication channels used; but none of these methods is really secure.

At this point q-key distribution comes into play. It allows Alice and Bob to create a pair of random private keys using q-communication, a method known as q-key distribution. The security of this method can be proven assuming the correctness of quantum mechanics: Based on the measurable (de-)correlation of a subset (e.g. 10%) of the common, randomly created bits, we can give an upper bound on how much information an eavesdropper Eve may obtain about the key. This is made possible by using non-orthogonal q-states:

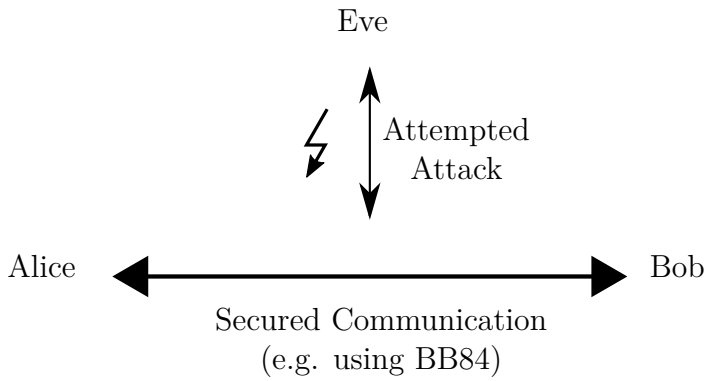


Figure 5.2: Attack situation, against which e.g. BB84 can protect: Alice and Bob want to communicate in a secured manner, while Eve is attempting an attack.

Theorem 14
In any attempt to distinguish between two non-orthogonal quantum states, information about them may only be obtained by perturbation of at least one of the two states.

Proof.

Let $|\psi\rangle, |\phi\rangle$ be two non-orthogonal states, $\langle\psi|\phi\rangle \neq 0$. Eve wants to distinguish these states. The most general method Eve can use to gain information about $|\psi\rangle$, $|\phi\rangle$ is to introduce an auxiliary system (*ancilla*) to the original system, to unitarily propagate them together, and then to measure. If we assume that the auxiliary system was in the state $|u\rangle$ in the beginning and that the original system has not been perturbed, she hence propagates

$$|\psi\rangle |u\rangle \overset{U}{\mapsto} |\psi\rangle |v\rangle \tag{5.17}$$

$$|\phi\rangle |u\rangle \overset{U}{\mapsto} |\phi\rangle |v'\rangle \ . \tag{5.18}$$

We require $|v\rangle \neq |v'\rangle$ in order for Eve to be able to learn something about the state of the original system. But because of the unitary transform, both scalar products have to be identical before and after the propagation:

$$(\langle\psi| \langle u|) (|\phi\rangle |u\rangle) = \langle\psi|\phi\rangle \langle u|u\rangle \overset{!}{=} \langle\psi|\phi\rangle \langle v|v'\rangle \tag{5.19}$$

$$\iff \langle v|v'\rangle = \langle u|u\rangle = 1 \iff |v\rangle = |v'\rangle \text{ in contradiction to the assumption} \tag{5.20}$$

Hence, it is impossible that Eve obtains any information about the two states and leaves both of them unperturbed. Note that from (5.19) to (5.20) we used the non-orthogonality of the two states, $\langle\psi|\phi\rangle \neq 0$. □

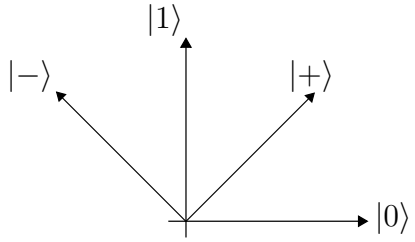


Figure 5.3: Pairs of basis states used in BB84 protocol. The basis states of two different pairs are explicitly non-orthogonal.

This feature is used by different protocols. In the following we consider the protocols *BB84* and *EPR*.

5.3.1 The BB84 Protocol

This protocol was developed for the situation in Figure 5.2 by [3] and works as follows:

1. Alice creates two random, classical strings a and b consisting of $\{0, 1\}$. The strings contain $(4 + \delta)\, n$ bits each (δ will be specified below).

2. Alice now creates a quantum state consisting of $(4 + \delta)\, n$ qubits, where the state of each qubit encodes one bit from a and b simultaneously. For this we use two pairs of basis states which are not all orthogonal to each other (Figure 5.3):

$$|\psi\rangle = \bigotimes_{k=1}^{(4+\delta)n} |\psi_{a_k,b_k}\rangle \tag{5.21}$$

$$\tag{5.22}$$

   where a_k, b_k are the value of the kth bit in each string a, b. b_k determines the basis used, while a_k determines the state used:

$$|\psi_{00}\rangle = |0\rangle \tag{5.23}$$

$$|\psi_{10}\rangle = |1\rangle \tag{5.24}$$

$$|\psi_{01}\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{5.25}$$

$$|\psi_{11}\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}\,. \tag{5.26}$$

3. Alice now sends all qubits (which are physical systems, such as photons in corresponding polarization states or time bins) to Bob using a public q-communication channel $\mathcal{E}$. Bob receives the (in general: mixed) state

$$\rho_{\text{Bob}} = \mathcal{E}\left(|\psi\rangle\langle\psi|\right) . \tag{5.27}$$

   $\mathcal{E}$ contains all influences on the qubits by the environment, such as decoherence, but also all actions (and perturbations) by Eve.

4. Bob measures the state for each qubit in a randomly chosen basis, $b'_k = 0, 1$ (i.e. measuring Zor X), based on a classical string b' of $(4+\delta)\,n$ bits which he generated randomly. His measurement provides him with the results a', a classical string of $(4+\delta)\,n$ bits.

5. Alice now releases b to the public, i.e. the basis states in which she prepared the transmitted quantum states. Alternatively, Bob can publicly release his classical string b'.

6. Both Alice and Bob disregard any bit in a, a' respectively, for which $b_k \neq b'_K$, i.e. they only keep the bits a_k, a'_k for which $b_k = b'_k$. All remaining bits should fulfill $a_k = a'_k$, since all of these states were diagonal states in the basis they were prepared and measured. On average, this should leave us with half of the bits in a, a' being equal, since half of the b_k, b'_k should be equal on average. By choosing δ sufficiently large, one can assert with a high probability, that $2n$-bits are left after this process. If Eve tried to tap the transmission between Alice and Bob, then she also destroyed at least part of the correlation $a_k = a'_k$ for these remaining bits in a.

7. Alice now randomly chooses a subset of n *check-bits* and publicly announces this subset to Bob as well as the corresponding values a_k in which she prepared these qubits. This action is to test for perturbations by signal tapping of Eve.

8. Alice and Bob communicate publicly and compare the values of the n check-bits. If too many of the check-bits deviate, communication is stopped (and the leakage / perturbation must be searched).

Example 16
Alice prepared the state $|0\rangle$ *and Bob expects the state* $|0\rangle$ *after confirming that for that qubit they worked in the same basis. However Eve tried to extract information by measuring in the basis* $\{|+\rangle, |-\rangle\}$ *and by doing so projected the state randomly onto either* $|+\rangle$ *or* $|-\rangle$*. Then Bob will receive* 1 *in half of the cases instead of* 0*. By using* n *check-bits the probability of not detecting Eve this way falls below* $1/2^n$*.*

9. If only an acceptably low number of check-bits deviate (such as might be expected from regular and characterized decoherence in the quantum channel), then the remaining n bits are accepted and are used as the common secret random key.

Remaining problems and their solutions (not detailed here):

- Non-identical keys.
  $\rightarrow$ Information reconciliation IR [4]: Due to unavoidable errors, in general the keys retained by Alice and Bob will not agree perfectly. IR is a classical error correction algorithm using a public channel and parity checks of sub-sets. The two initially strongly correlated strings x, y retained by Alice and Bob can with this be transformed into one identical string w that, however, may still be partially correlated with a string z which was captured by Eve's wiretapping.

- Remaining correlations between Alice, Bob and Eve
  $\rightarrow$ Privacy amplification PA [5]: Using a randomly and publicly chosen hash function
  $$\{0,1\}^n \mapsto \{0,1\}^{n-l-s}; \qquad x \mapsto h(x) \tag{5.28}$$
  reduces the expected amount of (Shannon) information Eve has about $h(x)$ to $\leq 2^{-s}/\ln 2$ (per bit), if Eve originally possessed l deterministic bits (e.g. parity check bits). s defines a security parameter. An example would be calculating the parity of $n-l-s$ randomly chosen subsets from the original set of n bits, which then are the basis for the (new) secret key.

- How to distinguish Eve from regular decoherence and errors (e.g. photodetectors click wrongly, rotation of polarization in optical fibers if the polarization degree is used, timing problems etc.)?
  $\rightarrow$ Definition of upper bounds for a maximum of information "lost" (gone) to the outside.

- It is hard to create single-photon pulses. It might happen that instead of $|\psi\rangle_{\updownarrow}$, e.g. $|2\rangle_{\updownarrow} = |1\rangle_{\updownarrow}|1\rangle_{\updownarrow}$, is emitted which contains a classical correlation that can be used by Eve.
  $\rightarrow$ Use of very weak coherent states, where the probability to have two photons is very small; development of better single photon sources; continuous-variable q-key distribution that uses non-orthogonal coherent states.

Example 17 (Key distribution using BB84)
Consider the two sets of basis states encoded by b_k

$$b_k = 0 \qquad \textit{bases} \qquad \{\leftrightarrow, \updownarrow\} \tag{5.29}$$
$$b_k = 1 \qquad \textit{bases} \qquad \{\nwarrow\!\!\searrow, \swarrow\!\!\nearrow\}, \tag{5.30}$$

and the respective key values encoded by a_k

$$a_k = 0 :\leftrightarrow \text{ or } \nwarrow\searrow \tag{5.31}$$
$$a_k = 1 :\updownarrow \text{ or } \swarrow\nearrow . \tag{5.32}$$

Now take the (randomly generated) bit strings

$$b = \{0110110100111\} \tag{5.33}$$
$$a = \{1001110001000\} . \tag{5.34}$$

In this case, Alice will transmit the following states

$$\updownarrow \nwarrow\searrow \updownarrow \swarrow\nearrow \leftrightarrow \nwarrow\searrow \leftrightarrow\updownarrow \nwarrow\searrow\nwarrow\searrow \tag{5.35}$$

Bob now randomly decides on b'_k *defining the base in which he will measure the received states*

$$b' = \{1011010110011\} . \tag{5.36}$$

Based on this string, he will measure a'

$$a' = \{01\underline{0}01\underline{10}0\underline{1}0 \cdot \underline{0}\} \tag{5.37}$$

The dot $\cdot$ *represents a non-transmitted qubit, such as a lost photon (i.e. missing from the transmission).* Underlined *values represent measurements which were conducted in the same basis as Alice prepared them, all other measured values are values which randomly collapsed to their respective value. Alice now releases* b *and Bob releases* b'*. The bits where* $b_k = b'_k$ *now provide both with the raw key*

$$\{010010\} . \tag{5.38}$$

In an ideal case, the raw key should be identical for both parties, i.e. $a_k = a'_k$*. Comparing a subset of the bits from the raw key allows for detection of Eve with a high certainty.*

5.3.2 EPR (E91) protocol

This protocol was developed by Artur Ekert in 1991 [19].

We assume that Alice and Bob both own n entangled qubits, initialised to the Bell state $|00\rangle + |11\rangle / \sqrt{2}$ (EPR pair). One way, e.g. would be to have Alice create these states and then have her send one qubit per pair to Bob. Another way would be to have a central source to create these states and then send them

to Alice and Bob. They both then publicly choose a subset of qubits and check if they sufficiently violate Bell's inequality (see later). If so then the state is adequately pure and entangled, and thus unperturbed. Alice and Bob then measure the qubits in randomly chosen basis (like in the BB84 protocol) and generate correlated, classical bits which in the end provide both sides with the secret key.

Proofing the security of these protocols goes beyond the scope of this lecture.

6 Physical Realisations

6.1 Five Basic Requirements

In order to physically build a quantum computer, one needs to satisfy at least the following five requirements. These where formulated by David DiVincenco [17], with a revised version in [18].

1. A scalable physical system with well characterised qubits:

   - qubits allow for coherent superpositions of the states $|0\rangle$ and $|1\rangle$;
   - *well characterised*: physical parameters of qubits must be known, including its internal Hamiltonian (eigenstates), the presence of and coupling to other qubits and the coupling to external fields. If the qubit has further states, the transition probability to them should be small;
   - *scalable* means that we can build and individually control many (N) qubits and put and keep them in arbitrary q-states $|\psi\rangle = \sum_{k=0}^{2^N-1} c_k |k\rangle$.

   Beware of superselection rules! E.g. we cannot superpose states involving different numbers of massive particles. For example, in two quantum dots with basis states $|0\rangle, |1\rangle$ for an electron absent or present we can make the superposition $\alpha|01\rangle + \beta|10\rangle$ with the same total particle number, where $|01\rangle$ means an electron in the second quantum dot but not in the first, and the other way round for $|10\rangle$. But we cannot create $\alpha|00\rangle + \beta|11\rangle$ (different number of particles in the two components to be superposed).

2. Ability to initialise the qubits to a simple fiducial state, e.g. $|000\ldots\rangle$. This is due to

   - computational requirements (start of the q-algorithm)
   - the need of continuous input of fresh low-entropy states for q-error correction; the cooling time is critical here.

   Resetting a qubit can be achieved by cooling or measuring in the computational basis. If $|1\rangle$ is found the qubit can be flipped to $|0\rangle$ with an X-gate. Both techniques are often quite similar and also used across different platforms, e.g. based on fluorescence techniques. Time scales can be a problem for

"natural" cooling, as $\tau_{\text{dissipation}} > \tau_{\text{decoherence}}$ (dissipation vs. decoherence) typically, and we want $\tau_{\text{decoherence}}$ to be large (see below). Ground-state cooling is particularly difficult for NMR q-computing with qubits based on nuclear spins due to their small energy gaps that lead to highly mixed thermal states and very slow relaxation. Due to these problems (and others, e.g. "spectral crowding"), NMR q-computing is not considered to be scalable.

3. Long relevant decoherence times

$$\tau_{\text{dec}} \gg \tau_{\text{gate}} \,. \tag{6.1}$$

Decoherence happens due to interaction with the environment and our ignorance of the state of the environment. It will be treated in much more detail in Sec.**??**, but to get the idea, consider the state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. Its corresponding density matrix is a projector,

$$\rho = |\psi\rangle\langle\psi| = |a|^2\,|0\rangle\langle 0| + |b|^2\,|1\rangle\langle 1| + ab^*\,|0\rangle\langle 1| + a^*b\,|1\rangle\langle 0| \,. \tag{6.2}$$

Under decoherence that destroys the fixed phase relation between $|0\rangle$ and $|1\rangle$ (e.g. due to a fluctuating magnetic field in the case that $|0\rangle$ and $|1\rangle$ are nuclear or electronic spin states), the state evolves to

$$\rho = |a|^2\,|0\rangle\langle 0| + |b|^2\,|1\rangle\langle 1| \,, \tag{6.3}$$

i.e. a classical mixture of the states $|0\rangle$ and $|1\rangle$ where all the possibilities of quantum interference are gone!

In general there are many couplings to the environment that lead to different decoherence processes with their own time scales, dependencies on parameters etc. For simplicity, suppose here that τ_{dec} is the shortest *relevant* decoherence time scale for a *single* qubit. Then we need

$$\tau_{\text{dec}} \simeq (10^4 \text{ to } 10^5) \cdot \tau_{\text{gate}} \tag{6.4}$$

where τ_{gate} is the time needed for a basic gate operation.

What about scaling (behaviour of the decoherence) with the number of qubits? Typically, for n qubits

$$\tau_{\text{dec}}^{(n)} \sim \frac{1}{n^p}\tau_{\text{dec}}^{(1)} \tag{6.5}$$

where $\tau_{\text{dec}}^{(1)}$ is the decoherence time for a single qubit. In general, p depends on the initial state and decoherence mechanism, but in any case, normally $p \geq 1$.

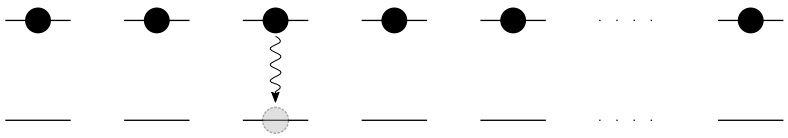


Figure 6.1: Decoherence time for spontaneous emission scales with the reciprocal of the number of atoms involved, $\tau_{\text{dec}}^{(n)} = \tau_{\text{dec}}^{(1)}/n$.

An example is spontaneous emission (Figure 6.1), where $p = 1$ for independent emission, but $p = 2$ for superradiant emission, relevant when the atoms get much closer than the wavelength of the emitted photons.

Does this destroy all hopes (for q-computing)? No, q-error correction allows scalable q-computers if the ratio between gate operation times and decoherence time in Equation 6.4 is met for each single qubit and uncorrelated errors. The total error in gate fidelity, including systematic errors, must be not larger than a certain threshold for being able to correct errors by stacking layers of error correction. Fortunately, the overhead grows only poly-logarithmically with the error. This is made more precise by the so-called

Theorem 15 (Threshold theorem for quantum computation:)
A quantum circuit containing $p(n)$ gates on n qubits maybe simulated with probability of error at most ϵ using

$$O(poly(\log p(n)/\epsilon)p(n)) \tag{6.6}$$

gates on hardware whose components fail with probability at most P, if $P < P_{th}$ and certain reasonable assumptions about the noise are made, such as uncorrelated errors.

Depending on the architecture of the quantum computer, in particular whether direct qubit-qubit interactions between all qubits are possible or only near-neighbors, the threshold P_{th} is situated around 10^{-6} to 10^{-3} per gate operation. This is very stringent, in particular for two-qubit gates, and must be achieved for possibly thousands or millions of physical qubits. At least five qubits are required for a first layer of error correction (see later). Hardware for superconducting "transmon" qubits, such as the publically available IBM machine "IBM Q 5 Yorktown" with just five qubits had single qubit errors of order 10^{-3}, and two-qubit errors and read-out errors of order 10^{-2} in 2018 (see e.g. here.) Single-qubit gates have sinced improved to about 10^{-4}, but two-qubit gates still have comparable values (see e.g. here).

4. A minimal set of gates.
   We need arbitrary single qubit transformations $U(2)$ and transformations acting on at least 2 qubits, like $CNOT$. In principle, $U_i = \exp\{-i/\hbar \cdot H_i t\}$, so we can just turn on the Hamilton H_i for the time t and then turn it off again. However, it is not so simple in practice:

   - interactions may be fixed, e.g. in NMR, and and need to be undone by special *refocusing* pulses
   - typically only nearest neighbour interactions are possible on a 2D grid of qubits, e.g. $\sum_{<i,j>} \boldsymbol{S}_i \boldsymbol{S}_j$. Interactions over large distances, can be created e.g. by a *bus qubit* such as phonons in an ion chain, or photons in a resonator with which all qubits can interact. However, parallel implementation of gates on many qubits, e.g. for q-error correction, may render such approaches impossible. In addition, a quantum bus may also introduce additional decoherence. As a result, in the most modern implementations based on superconducting qubits, one has gone back to direct interactions that can be switched on and off by tuning the qubits in and out off resonance which each other. But then one then needs to channel the quantum information through a sequence of gates, increasing the comlexity of the alrogithm. Quantum compilers exist already that take hardware speficities into account for optimally translating a q-circuit to actual pulses, adapted to the hardware and its errors.
   - abrupt switching on H strongly perturbs the system and leads to excitations to other levels or cross-talk. Hence, more gentle, possibly adiabatic switching on and off might be necessary, which however can increase the required decoherence time. On the theoretical side it means that one needs to calculate the unitary transformations using $T \exp\left(-i/\hbar \int_0^t H(t')dt'\right)$ instead of $e^{-i/\hbar Ht}$, where T is the time order operator;
   - parallel implementation of gates on many qubits, e.g. for q-error correction, may make the *bus qubit* approach impossible.

5. A qubit-specific measurement capability. We need to

   - address separate qubits separately for read-out;
   - solve problems of quantum efficiency. E.g. suppose we want to measure 0 with probability p_0 and 1 with probability p_1 if the q-bit's reduced density matrix ρ is $p_0 |0\rangle\langle 0| + p_1 |1\rangle\langle 1| + \alpha |0\rangle\langle 1| + \beta |1\rangle\langle 0|$. If the quantum efficiency is smaller than a desired level, say 90% instead of

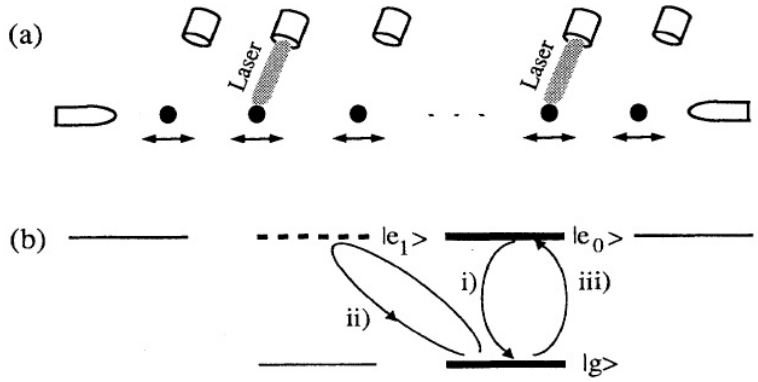


Figure 6.2: Setup of the Cirac-Zoller proposal of an ion-trap q-computer (from [13]). Ions are trapped in a linear Paul trap, cooled close to the ground state, and addressed with laser beams. The center-of-mass motion of the ions is used as a quantum bus. The qubit consists of states $|g\rangle$ and $|e_0\rangle$, whereas state $|e_1\rangle$ is used to temporarily "hide" an ion. In the experimental realization [7] fine-structure levels $S_{1/2}, D_{5/2}$ with dipole-forbidden transition in Ba^+ ion(s) where used for these states.

99%, then it can help to *copy* the result qubits to additional qubits, initialised in $|0\rangle$, and measure them all. This is done with $CNOT$gates:

$$(\alpha\,|0\rangle + \beta\,|1\rangle)\,|0\rangle \xrightarrow{CNOT} \alpha\,|00\rangle + \beta\,|11\rangle\,. \tag{6.7}$$

Recall that orthogonal states *can* be cloned, without contradiction to the no-cloning theorm. This approach should lead to the same measurement results for all measurements. If the error probability is ε for one measurement, then it is ε^n in total for a wrong result in all measurements. This way we can get very good quantum efficiency if we have enough auxiliary qubits and good $CNOT$gate implementations available.

We now consider some proposals in more detail that are relevant for the currently most advanced realizations of quantum computers, namely those based on ion-traps or superconducting qubits.

6.2 The Cirac-Zoller Proposal

This proposal was one of the first realistic and detailed proposals for the implementation of 2-qubit and 1-qubit gates in a physical system, see [13,30,35].

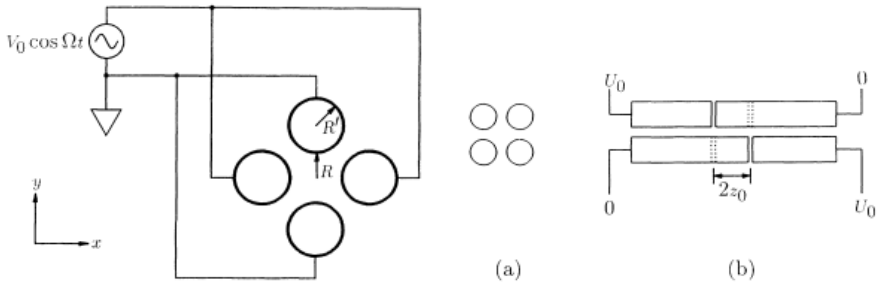


Figure 6.3: Cross-section and longitudinal view of a linear ion trap. From [33]

- The n qubits are realized by two internal states each of n ions in a linear (Paul) ion trap. The trap is realized with alternating potentials

$$\Phi_{\mathrm{RF}} = \frac{1}{2}\left(V_0 \cos \omega_r t + U_r\right)\left(1 + \frac{y^2 - z^2}{R^2}\right) \tag{6.8}$$

$$\Phi_{\mathrm{DC}} = \kappa U_0 \left[x^2 - \left(y^2 + z^2\right)\right] \qquad \text{(confinement along } x\text{)} \tag{6.9}$$

  with a setup shown schematically in (Figure 6.2). As Earnshaw's theorem states, a charge can not be confined in three dimensions by static potentials, but an effectively confining (time-averaged) potential in three dimensions is possible and realized in the linear ion trap, a schematic view of which is shown in Fig.6.3.

- The vibrational modes of the ions are cooled to the the ground-state by laser cooling. The hamiltonian for the motion of ions, with a mass M and charge e each for each ion, positions $\boldsymbol{r}_i = (x_i, y_i, z_i)$, and momenta $\boldsymbol{p}_i$ reads

$$H_{\mathrm{com}} = \sum_{i=1}^{n}\left(\frac{M}{2}\left(\omega_x^2 x_i^2 + \omega_y y_i^2 + \omega_z^2 z_i^2\right) + \frac{\boldsymbol{p_i}^2}{2M}\right) + \sum_{i=1}^{n}\sum_{j>i}\frac{e^2}{4\pi\varepsilon_0\left|\boldsymbol{r_i} - \boldsymbol{r_j}\right|}, \tag{6.10}$$

  where $\omega_x, \omega_y, \omega_z$ etc. are the trap frequencies in directions x, y, z, and the last term is due to the Coulomb interaction between the ions. Expanding the potential energy about the equilibrium position of the ions up to quadratic order in their displacements leads to canonical modes. The lowest frequency mode is the collective oscillation in x-direction with a frequency $\nu_x \equiv \omega_x/(2\pi)$, as no interaction effects are felt in that mode ("center-of-mass mode" or c.o.m. mode for short). The next frequency is $\sqrt{3}\nu$. All other modes have higher frequencies.

- Cooling of all modes to vibrational ground-state is achieved via

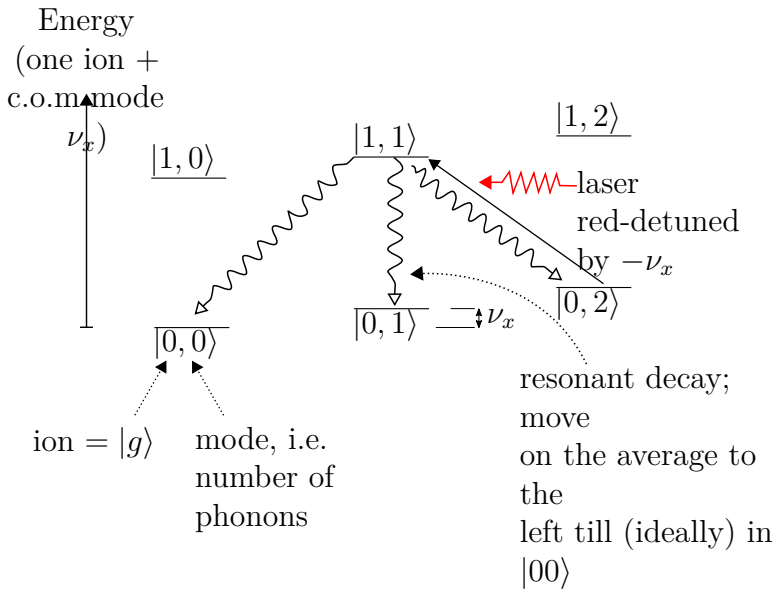


Figure 6.4: Schematic for the mechanism behind sideband cooling. The states form two ladders, $\{0, n\}$ and $\{1, n\}$ where n is the number of phonons in the center-of-mass (c.o.m.) vibration mode of the ion crystal (i.e. a collective slothing back and forth of all ions in the trap).

– Doppler cooling: Red detuned laser beams from $\pm(x, y, z)$ directions are used to cool the ions to $k_{\mathrm{B}}T \simeq \hbar\Gamma/2$, where Γ represents the natural linewidth of the transition;

– Sideband cooling: The scheme for sideband cooling is shown in Figure 6.4. Due to the resonant decay, the occupied energy level moves on average to the left, until (in an ideal case) the state $|0, 0\rangle$ is reached. A necessary condition for sideband cooling is the *Lamb-Dicke criterion*

$$\eta = \frac{2\pi x_0}{\lambda} \ll 1 \tag{6.11}$$

where x_0 is the width of the ion oscillation, i.e. the width of the oscillator wave function of the c.o.m. mode in the ground-state:

$$x_0 = \sqrt{\frac{\hbar}{2nM\omega_x}}. \tag{6.12}$$

nM is the total mass in the c.o.m. mode and thus defines the oscillator length.

The criterion can thus be interpreted as

$$\eta = \sqrt{\frac{\hbar k^2}{2nM\omega_x}} = \sqrt{\frac{\hbar^2 k^2}{2nM\hbar\omega_x}} \tag{6.13}$$

$$= \sqrt{\frac{\text{recoil energy}}{\text{phonon energy}}} \tag{6.14}$$

($\hbar k$ is the recoil from an emitted photon and $\hbar^2 k^2/2nM$ the corresponding energy of the entire chain). The Lamb-Dicke criterion thus guarantees that no excitations of c.o.m. phonons through the recoil of an emitted photon are possible (c.f. *Mössbauer effect*).

Sideband cooling allows for cooling down to temperatures as low as $k_\mathrm{B}T/\hbar\omega_x \ll 1$, in fact mean phonon numbers $\langle n\rangle \simeq (\Gamma/\omega_0)^2$ can be reached. It is assumed that cooling close to the ground state has been achieved before the quantum computation starts.

- The relevant internal states of an ion are denoted as $|\sigma\rangle$ with $\sigma \in\equiv \{g, e_0, e_1\}$, where $\{0,1\} \equiv \{g, e_0\}$ are the qubit states. $|e_0\rangle$ and $|e_1\rangle$ are connected to the ground state $|g\rangle$ via electric dipole transitions with different polarizations, $q = 0, 1$. $|e_1\rangle$ is only used for realizing certain quantum gates (auxiliary quantum state). The combined states of a single ion and the vibrational c.o.m. mode are denoted as $|\sigma, l\rangle$ with $l \in \mathbb{N}$. If several ions are involved in a gate, we write only the relevant parts involved, e.g. $|g\rangle_m |g\rangle_n |1\rangle$ is a (part of a) state in which ion m and ion n are in the ground state, and the vibrational mode has a single-phonon excitation.

- For the controlled phase gate:

  - Turning the laser on on ion n with a frequency red-shifted by $\delta_n = -\nu_x$ (i.e. the trap's frequency) and a phase Φ of the laser for the time $t = k\pi/\Omega\eta$ results in a $k\pi$-pulse ($k \in \mathbb{N}$):

$$H_{n,q} = \eta\frac{\hbar\Omega}{2}\left[|e_q\rangle_n \langle g| a \exp\{-i\Phi\} + |g\rangle_n \langle e_q| a^\dagger \exp\{i\Phi\}\right] \tag{6.15}$$

    where η is the LD parameter containing the mass Mn and the Rabi frequency Ω. The first term in brackets takes phonons out of the vibrational c.o.m. mode and excites atom n. The other modes are unaffected as they are off-resonant. The parameter q takes on values $q = 0, 1$ depending on the polarisation of the light. We get

$$U_n^{k,q}(\Phi) = \exp\left\{-ik\frac{\pi}{2}\left(|e_q\rangle_n \langle g| a \exp\{-i\Phi\} + h.c.\right)\right\} \tag{6.16}$$

We can show that

$$|g\rangle_n |1\rangle \xmapsto{U_n^{k,q}(\Phi)} \cos\left(\frac{k\pi}{2}\right) |g\rangle_n |1\rangle - i \exp\{i\Phi\} \sin\left(\frac{k\pi}{2}\right) |e_q\rangle_n |0\rangle \tag{6.17}$$

$$|e_q\rangle_n |0\rangle \xmapsto{U_n^{k,q}(\Phi)} \cos\left(\frac{k\pi}{2}\right) |e_q\rangle_n |0\rangle - i \exp\{-i\Phi\} \sin\left(\frac{k\pi}{2}\right) |g\rangle_n |1\rangle , \tag{6.18}$$

i.e. for $k = 1$:

$$|e_q\rangle_n |0\rangle \mapsto -ie^{-i\phi} |g\rangle_n |1\rangle \tag{6.19}$$

$$|g\rangle_n |1\rangle \mapsto -ie^{i\phi} |e_q\rangle_n |0\rangle \tag{6.20}$$

and if $k = 2$:

$$|\psi\rangle \mapsto -|\psi\rangle \tag{6.21}$$

in the subspace spanned by $|e_q\rangle_n |0\rangle$ and $|g\rangle_n |1\rangle$. Outside that subspace the effect is a simple $\mathbb{1}$-operation.

(6.22)

– A three pulse sequence is required for the controlled phase gate between n, m:

$$U_{m,n} = U_m^{1,0}(0) U_n^{2,1}(0) U_m^{1,0}(0) \tag{6.23}$$

One can show that this brings back $|0\rangle_{\text{phonon}} \mapsto |0\rangle_{\text{phonon}}$ and (for $\Phi = 0$)

$$|g\rangle_m |g\rangle_n |0\rangle \xmapsto{U_m^{1,0}} |g\rangle_m |g\rangle_n |0\rangle \xmapsto{U_n^{2,1}} |g\rangle_m |g\rangle_n |0\rangle \xmapsto{U_m^{1,0}} |g\rangle_m |g\rangle_n |0\rangle \tag{6.24}$$

$$|g\rangle_m |e_0\rangle_n |0\rangle \xmapsto{U_m^{1,0}} |g\rangle_m |e_0\rangle_n |0\rangle \xmapsto{U_n^{2,1}} |g\rangle_m |e_0\rangle_n |0\rangle \xmapsto{U_m^{1,0}} |g\rangle_m |e_0\rangle_n |0\rangle \tag{6.25}$$

$$|e_0\rangle_m |g\rangle_n |0\rangle \xmapsto{U_m^{1,0}} -i |g\rangle_m |g\rangle_n |1\rangle \xmapsto{U_n^{2,1}} i |g\rangle_m |g\rangle_n |1\rangle \xmapsto{U_m^{1,0}} |e_0\rangle_m |g\rangle_n |0\rangle \tag{6.26}$$

$$|e_0\rangle_m |e_0\rangle_n |0\rangle \xmapsto{U_m^{1,0}} -i |g\rangle_m |e_0\rangle_n |1\rangle \xmapsto{U_n^{2,1}} -i |g\rangle_m |e_0\rangle_n |1\rangle \xmapsto{U_m^{1,0}} -|e_0\rangle_m |e_0\rangle_n |0\rangle \tag{6.27}$$

In (6.26), $U_n^{2,1}$ flips the sign of $|g\rangle_n |1\rangle$, whereas in (6.27) the state $|e_0\rangle_n$ is insensitive to $U_n^{2,1}$ and thus unchanged, as it is "parked" outside the $|g\rangle_n |e_1\rangle$ subspace on which $U_n^{2,1}$ acts.

This provides us with a controlled phase gate in the atomic states $|gg\rangle, |ge_0\rangle, |e_0g\rangle, |e_0e_0\rangle$.

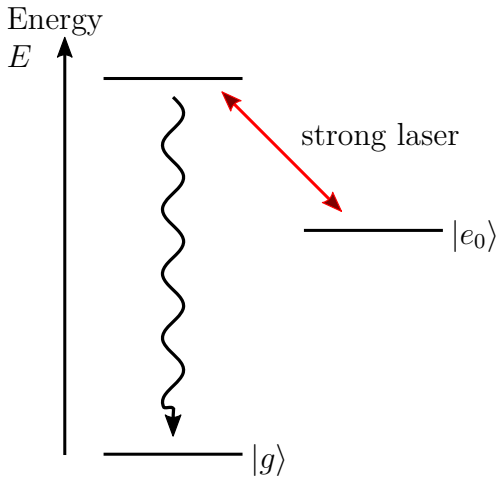


Figure 6.5: Schematic for measuring the state of qubits in the Cirac-Zoller proposal using fluorescence techniques. A strong laser excites the $|e_0\rangle$ state leading to fluorescence only when the qubit is in the selected state, here in $|e_0\rangle$; no fluorescence can be observed from $|g\rangle$.

- Single qubit rotations of ion n are realised by $\delta_n = 0$, i.e. in resonance with the transition. For $q = 0$:

$$H_n = \frac{\hbar\Omega}{2}\left(|e_0\rangle_n \langle g| e^{-i\Phi} + |g\rangle_n \langle e_0| e^{i\Phi}\right), \tag{6.28}$$

  which with an interaction time of $t = k\pi/\Omega$ gives

$$V_n^k = \exp\{-iH_n t\} = \exp\left\{-ik\pi/2\left(|e_0\rangle_n \langle g| e^{-i\Phi} + h.c.\right)\right\}. \tag{6.29}$$

  The combination with the controlled phase gate results in a $CNOT$gate.

- For read out, fluorescence techniques are used, see Figure 6.5.

A further development of the *Cirac-Zoller gate* is the *Mølmer-Sørensen gate* [38]. It also works if thermal phonons are left in the ion-chain. A major part of the initial work on ion-trap quantum computers was developped in the group of Rainer Blatt in Innsbruck and David Wineland at NIST in Boulder. This approach is not considered really scalable, however, due the problem of spectral crowding (i.e. with increasing number of ions it becomes difficult to spectrally select transitions, as there are more and more resonances in a given frequency interval), and simple pragmatic problems, like having enough optical accesses to the vacuum chamber for all the laser beams needed. Modern versions have gone in the direction of miniaturization, shuffling ions in and out of interaction zones, and modularization, allowing one to build and connect standardized parts of the quantum computer with a relatively small number of ions each, and then connecting those.

6.3 Quantum processor with superconducting qubits

The system is analogous to a atoms in a resonator, with the following substitutions:

- An *atom* is an "artificial" atom, i.e. a superconducting qubit. Characteristic for this system is the lack of any resistance R and a non-linear inductance, leading to an inharmonicity in the system which allows us to address two energy levels with a narrow-band pulse.
- The *resonator* is a microwave resonator, realised using a few cm long wire integrated in a chip.

Advantages of the system are

- an extremely high dipole moment ($\sim 10^4 e a_0$);
- an extremely low volume in which modes are localised; a photon in the modes is thus strongly coupled with the system;
- scalability in the fabrication of the system;
- no trapping and cooling of single ions or atoms required.

But the system also has the disadvantages of a highly complex environment created by the solid state material, in which the qubit is embedded. This environment has many uncontrolled degrees of freedom and requires extensive research into the used materials. E.g. *two-level fluctuators in oxide layers* were plagueing this field for many years.

6.3.1 The superconducting qubit

Superconducting qubits are in general variations of the *Cooper-pair box* shown in Figure 6.6a.

For temperatures T below the critical temperature T_c of the superconductors, $T \ll T_c$, we can use a macroscopic wavefunction to describe the system. The phase φ of the macroscopic wave function is given by a dynamical variable which itself is governed by the laws of quantum mechanics (possibility of coherent superposition [8])! Let

$$\psi_j = \sqrt{n_s} \exp\{i\varphi_j\} \tag{6.30}$$

with $j = 1, 2$ be the macroscopic wavefunctions of the superconducting electrons in the two superconductors. Here, n_s denotes the particle density of the superconducting electrons. Assuming a constant phase on each superconducting

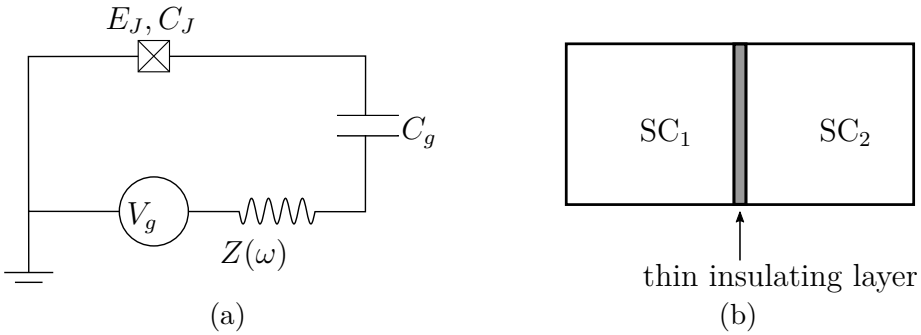


Figure 6.6: (a) Circuit diagram of the *Cooper-pair box* and (b) schematic of a *SIS Josephson junction* consisting of a thin insulating layer separating two superconducting electrodes. E_J = Josephson energy, C_J = capacity of the junction. The junction is biased via another capacitor C_g and impedance $Z(\omega)$ of the circuit.

island, $\varphi = \varphi_1 - \varphi_2$ is the phase difference between the two superconductors of the junction. The junction's behavior can be described using the Josephson relations:

1. Josephson DC relation
$$I(t) = I_c \sin \varphi(t) \tag{6.31}$$
I_c is the critical (maximum) current $I(t)$ through the junction.

2. Josephson AC relation
$$U(t) = \frac{\hbar}{2e} \frac{\partial \varphi}{\partial t}, \tag{6.32}$$
with $U(t)$ the voltage across the junction.

Assuming a phase difference at $t = 0$ of $\varphi(t = 0) = 0$ and after t a phase difference of $\varphi(t) = \varphi$, the work performed by the system is given by the integral

$$W = \int_0^t P\left(t'\right) \, \mathrm{d}t' = \int_0^t U\left(t'\right) I\left(t'\right) \, \mathrm{d}t' \tag{6.33}$$

$$= \frac{\hbar I_c}{2e} \int_0^t \sin \varphi\left(t'\right) \underbrace{\dot{\varphi}\left(t'\right) \mathrm{d}t'}_{\mathrm{d}\varphi} \tag{6.34}$$

$$= -\frac{\hbar I_c}{2e} \left[\cos \varphi'\right]_{\varphi'=0}^{\varphi} \tag{6.35}$$

$$= \frac{\hbar I_c}{2e} \left(1 - \cos \varphi\right) \tag{6.36}$$

We thus found the Hamiltonian of the system,

$$H = -E_J \cos\varphi \tag{6.37}$$

up to an irrelevant additive constant, where $E_J = \Phi_0 I_c/2\pi$ and $\Phi_0 := h/2e \simeq 2.067 \cdot 10^{-15}$ Weber is the magnetic flux quantum. The energy of the system is contained in the kinetic energy (i.e. in quantum mechanics the phase difference) of the tunnelling Cooper-pairs along the junction. This part of the system may also be interpreted as a non-linear inductance of the junction. However, the junction also has a capacity leading to a Coulomb energy of $4E_c\,(n - n_g)^2$, where $n \in \mathbb{N}_0$ denotes the number of Cooper-pairs located on the "box" (the small metallic island formed by the right half of the SIS junction in Fig.6.6a), insulated from the left half with the insulating layer of the junction, typically a thin oxide layer, and on the other side by the dielectric of the capacitor C_g. The parameter $n_g \in \mathbb{R}$ is a continuous "offset-charge", a parameter representing the shift of the minimal energy (ground state) induced by applying V_g and any other electrical fields. Remarkably φ and n can be re-quantized and turn out to be complementary variables, equivalent to a $1D$ particle on a ring. Their quantum mechanical state is described by a wavefunction $\psi(\varphi)$ with periodic boundary conditions, $\psi(\varphi) = \psi(\varphi + 2\pi)$, whose dynamics is governed by the Cooper pair box Hamiltonian

$$H = 4E_c\,(\hat{n} - n_g)^2 - E_J \cos\hat{\varphi}. \tag{6.38}$$

where $\hat{n} \to -i\partial/\partial\varphi$ in "φ-representation". Switching into the basis of charge states, we may write the Hamiltonian as

$$H = 4E_c \sum_n (n - n_g)^2 \,|n\rangle\langle n| - \frac{E_J}{2} \sum_n \left(|n+1\rangle\langle n| + |n\rangle\langle n+1|\right). \tag{6.39}$$

This notation places an emphasis on E_J as a tunnelling energy.

$|n+1\rangle\langle n| + |n\rangle\langle n+1|$ corresponds to a one-dimensional tight-binding model and brings us back to the energy band $\propto \cos\varphi$ via the complementary variable φ.

Real implementations usually use two Josephson junctions connected in parallel. This way, the effective Josephson energy can be regulated using an external flux Φ_{ext} (Figure 6.7):

$$E_J \propto \left|\cos\left(\frac{\pi\Phi_{\text{ext}}}{\Phi_0}\right)\right|. \tag{6.40}$$

The energy levels of the system as function of φ and n_g are sketched in Figure 6.8 and Figure 6.9.

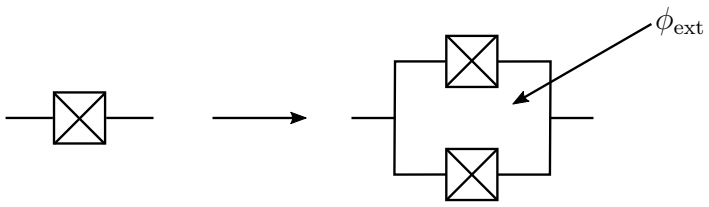


Figure 6.7: Instead of a single Josephson junction, two junctions in a parallel circuit are commonly used in applications. The effective Josephson energy can be adjusted with the external flux ϕ_{ext}.

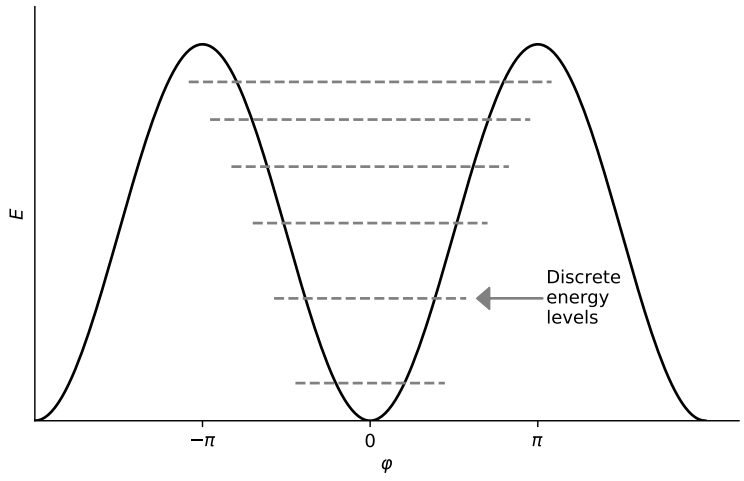
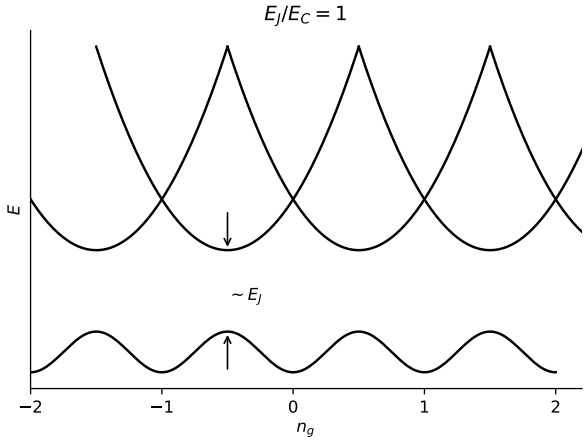
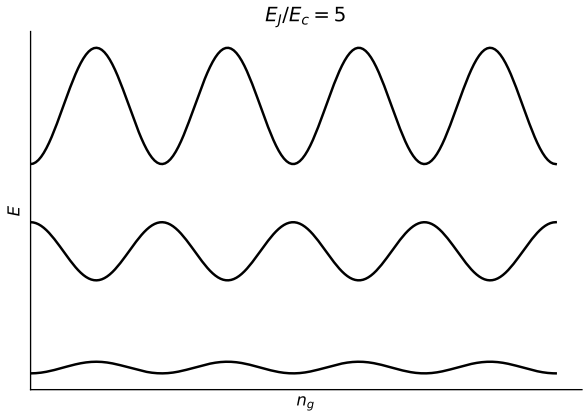


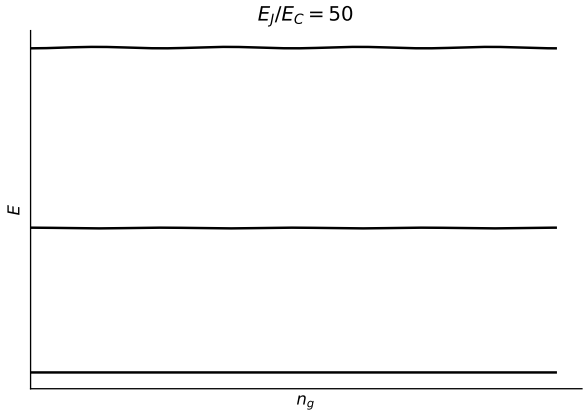
Figure 6.8: The discrete energy levels of the system in the $\cos\varphi$ potential.



(a)



(b)



(c)

Figure 6.9: The different energy bands of the system as function of the gate charge n_g for different ratios of E_J/E_C.

If d is the distance between the two superconducting islands of the qubit, one finds for the dipole moment

$$\boldsymbol{p_j} \sim 2ed \langle \psi_j | \hat{n} | \psi_j \rangle \,. \tag{6.41}$$

A stray electrical field $\boldsymbol{\epsilon}$ results in a shift of the energy states and therefore a change of the excitation energy ω_{01} given in first order perturbation theory by

$$\delta\omega_{01} = \frac{1}{\hbar} \boldsymbol{\epsilon} \cdot (\boldsymbol{p_1} - \boldsymbol{p_0}) \,. \tag{6.42}$$

The dephasing rate of a q-superposition due to $1/f$ charge noise is

$$T_\varphi^{-1} = \frac{1}{2} \left[\frac{\boldsymbol{p_1} - \boldsymbol{p_0}}{\hbar} \right]^2 S_{\epsilon\epsilon} \,, \tag{6.43}$$

where $S_{\epsilon\epsilon}$ denotes the spectral density of the electrical field at the corresponding transition frequency. Including fluctuations at low temperatures, the overall decoherence rate is given by

$$\frac{1}{T_2^*} = \frac{1}{2T_1} + \frac{1}{T_\varphi} \,, \tag{6.44}$$

where T_1 is the energy relaxation rate.

The second important energy scale in the system is the charging energy $E_C = (2e)^2/(2(C_g{+}C_J))$ of a single Cooper pair on the super-conducting island. Depending on the ratio E_J/E_c and the operating point, one distinguishes different variants of superconducting qubits. For the *Quantronium* qubit [40] the authors selected $E_J \simeq E_C$, and the bias point $n_g = 1/2$. In this case neither phase nor charge are good quantum numbers. The energy bands at this point are locally flat, i.e. fluctuations of n_g lead to

$$\delta\omega_{01} = \left. \frac{\partial\omega_{01}}{\partial n_g} \right|_{n_g=\frac{1}{2}} \left(n_g - \frac{1}{2} \right) + \frac{1}{2} \left. \frac{\partial^2\omega_{01}}{\partial n_g^2} \right|_{n_g=\frac{1}{2}} \left(n_g - \frac{1}{2} \right)^2 \tag{6.45}$$

The first (linear) term vanishes, such that fluctuations of n_g contribute only at second order. This lead to an increase of T_2^* by around three orders of magnitude compared to a simple Cooper pair box to $\sim 500\,\mathrm{ns}$.

The *Transmon* qubit [27] is another variant of the Cooper pair box operating in the limit of large E_J/E_C. The energy bands in this limit become extremely flat, with a width

$$\epsilon \sim \exp\left\{ -\sqrt{8E_J/E_c} \right\} \tag{6.46}$$

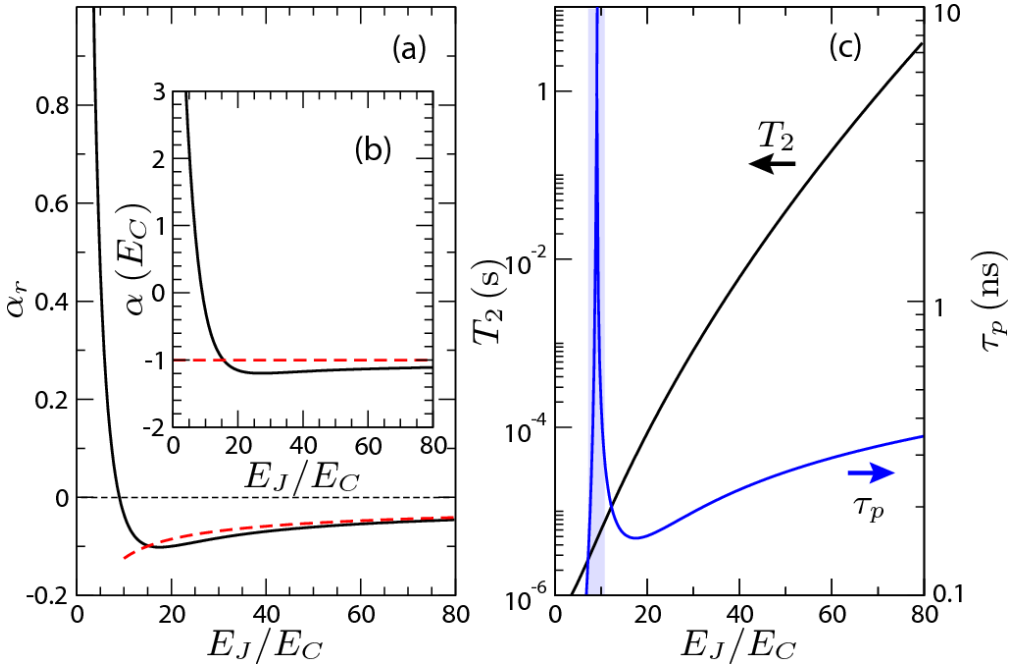


Figure 6.10: Left figures show the (a) relative and (b) absolute anharmonicity of the system, where the solid curves are exact results and the dashed curves indicate perturbative results. On the right (c) shows the effect of E_J/E_c on the decoherence times of the system [27].

This leads to a system which is highly insensitive to fluctuation of the electric field. This design also has a downside: The anharmonicity of the system decreases in this limit leading to energy levels which are nearly equidistant at the lower end of the spectrum, and the energy levels get closer and closer together with an increasing ratio of E_J/E_c. We define the anharmonicity of the system as

$$\alpha := \omega_{12} - \omega_{01} \tag{6.47}$$

and the relative anharmonicity

$$\alpha_r := \frac{\alpha}{\omega_{01}}\,, \tag{6.48}$$

where $\omega_{nm} \equiv (E_m - E_n)/\hbar$ is the transition frequency between energy eigenstates n and m, shown as function of E_J/E_C in Figure 6.10.

In the limit of $E_J/E_c \to \infty$ the system behaves as

$$\alpha \to -\frac{E_c}{\hbar} \qquad \text{energy of the charges} \tag{6.49}$$

$$\omega_{01} \to \Omega_{\text{plasma}} = \sqrt{8E_J E_c} \qquad \text{Josephson plasma frequency} \tag{6.50}$$

$$\alpha_r \sim -\sqrt{\frac{E_c}{8E_J}} \to 0 \tag{6.51}$$

In this regime, an incident pulse with a pulse duration of τ_p does no longer excite a single energy level, but also higher levels. A quick estimate gives the condition,

$$\tau_p \geq \frac{1}{\omega_{01}\alpha_r} \tag{6.52}$$

to avoid this. But what counts in the end is the ratio T_2/τ_p, the number of single gate operations that can be implemented before the system loses coherence. In practice the ratio E_J/E_c is chosen between

$$20 \lesssim \frac{E_J}{E_c} \ll 5 \cdot 10^4 \,. \tag{6.53}$$

E_c is reduced by artificially increasing the capacitance of the junction: A capacitor C_b with high capacitance is shunted parallel to the qubit. The system can be described using a so called *lumped circuit* (Figure 6.11), i.e. an equivalent electrical circuit with inductances, capacitances etc., where only near-fields are considered and the propagation via emission is irrelevant.

An implementation of this system yielded $T_2^* \simeq 3\,\mu$s, $T_\varphi \geq 35\,\mu$s (T_2^* is the "bare" dephasing time, without any additional refocusing techniques for decoherence suppression) [25].

6.3.2 Resonator

The resonator simply consists of a "strip-line", meaning a stretch of length L of a wire (or two parallel wires) evaporated on the surface of the chip. In the GHz regime it is typically a few cm long and curled up to fit on the chip. It can be modelled as in classical electrodynamics as a transmission line with a Lagrange function $\mathcal{L} = \int_{-L/2}^{L/2} dx \left(\frac{\ell}{2} j^2 - \frac{1}{2c} q^2\right)$ with $j(x,t), q(x,t)$ current density and charge density, c, l = inductance and capacitance per unit length. Define $\theta(x,t) \equiv \int_{-L/2}^{x} dx' q(x',t)$ with boundary conditions $\theta(-L/2,t) = \theta(L/2,t) = 0$,

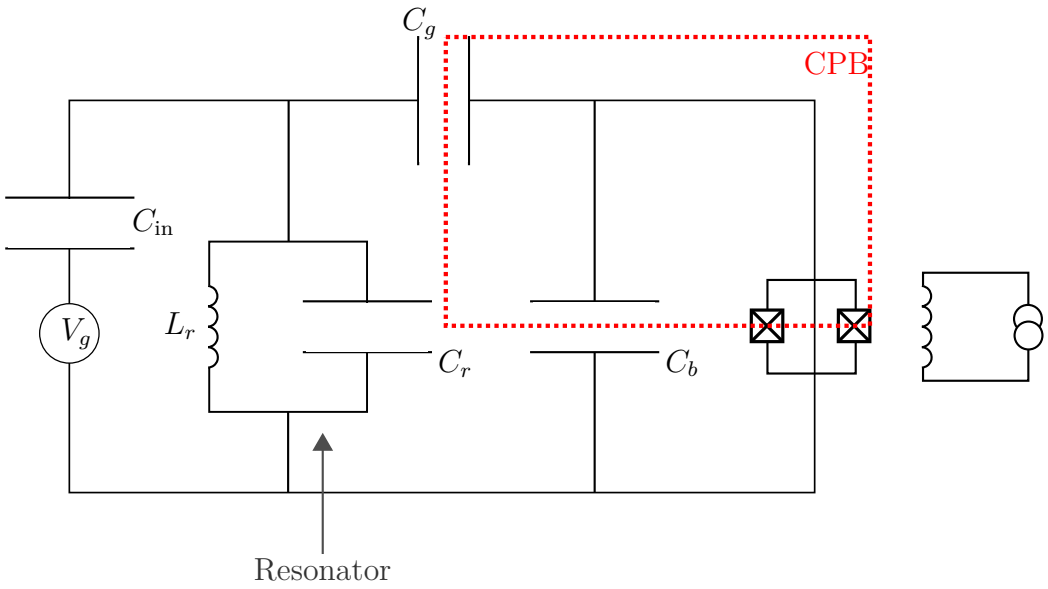


Figure 6.11: Lumped circuit model of the *Quantronium* qubit.

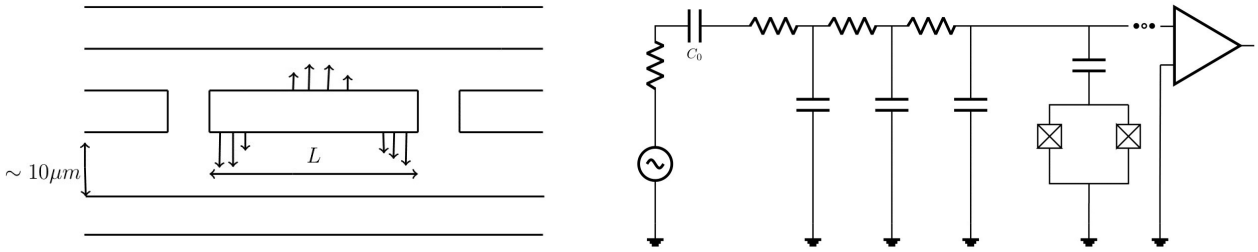


Figure 6.12: Strip line resonator and equivalent lumped circuit including a superconducting qubit based on two Josephson junctions.

where the latter quantity is the total electric charge on the transmission line, taken as uncharged.

$$\Rightarrow \mathcal{L} = \int_{-L/2}^{L/2} dx \left(\frac{\ell}{2}\dot{\theta}^2 - \frac{1}{2c}(\nabla\theta)^2 \right) \tag{6.54}$$

A mode expansion in odd and even modes gives

$$\theta(x,t) = \sqrt{\frac{2}{L}}\left(\sum_{k_0=1}^{k_{o,max}} \phi_{k_o}(t)\cos\frac{k_o\pi x}{L} + \sum_{k_e=2}^{k_{e,max}} \phi_{k_e}(t)\sin\frac{k_e\pi x}{L}\right) \tag{6.55}$$

$$\Rightarrow \mathcal{L} = \sum_k \left(\frac{\ell}{2}\dot{\phi_k}^2 - \frac{1}{2c}\left(\frac{k\pi}{L}\right)^2\phi_k^2\right) \tag{6.56}$$

$\rightarrow$ Quantization: $\phi_k \rightarrow \hat{\phi}_k, \quad l\dot{\hat{\phi}}_k = \hat{\Pi}_k \rightarrow a_k, a_k^\dagger$ as usual,

$$\hat{\phi}_k(t) = \sqrt{\frac{\hbar\omega_k c}{2}}\frac{L}{k\pi}\left(a_k(t) + a_k^\dagger(t)\right), \qquad \omega_k = k\pi\frac{v}{L}, \quad v = \frac{1}{\sqrt{\ell c}}$$

$$\hat{\Pi}_k(t) = -i\sqrt{\frac{\hbar\omega_k\ell}{2}}\left(a_k(t) - a_k^\dagger(t)\right), \qquad [a_k, a_{k'}^\dagger] = \delta_{kk'}\,.$$

The voltage is found from ($U = Q/C$ gives locally $\rightarrow \frac{q}{c} = \frac{1}{c}\frac{\partial\theta}{\partial x}$, with q = charge per unit length)

$$\begin{aligned} V(x,t) &= \frac{1}{c}\frac{\partial\theta}{\partial x} \\ &= -\sum_{k_o=1}^{k_{o,max}} \sqrt{\frac{\hbar\omega_{k_o}}{Lc}}\sin\left(\frac{k_o\pi x}{L}\right)\left(a_{k_o}(t) + a_{k_o}^\dagger(t)\right) \\ &+ \sum_{k_e=2}^{k_{e,max}} \sqrt{\frac{\hbar\omega_{k_e}}{Lc}}\cos\left(\frac{k_e\pi x}{L}\right)\left(a_{k_e}(t) + a_{k_e}^\dagger(t)\right)\,. \end{aligned}$$

Normally, there is only one mode excited, $k = 2$, and the qubit placed at the maximum of the electric-field amplitude close to the middle of the stip line. This gives an amplitude of the voltage $\sqrt{\frac{\hbar\omega_2}{Lc}}$ $\left[SIunits: \frac{Jm}{m\cdot F} = \frac{C.V}{C/V} = V^2\checkmark\right]$
Depending on form and material of the resonators, quality factors $\sim 10^2 - 10^5$ can be reached, see e.g. [23]. Typical frequencies are in the range of about 10 GHz.

6.3.3 Coupling

The full system can be described in good approximation by the Jaynes-Cummings Hamiltonian,

$$H = \hbar \underset{\substack{\uparrow \\ Resonator}}{\omega_r}\left(a^\dagger a + \frac{1}{2}\right) + \frac{\hbar\omega_{01}}{2}\underset{\substack{\uparrow \\ qubit}}{\sigma_z} + \hbar g\left(a^\dagger\sigma^- + \sigma^+ a\right) + H_{\text{drive}} + H_{\text{damping}}$$

in rotating-wave approximation (RWA). Typical couplings are $g \simeq 100\,\mathrm{MHz}$, such that $g/\omega_r \sim 5 \cdot 10^{-3}$ can be reached. The coupling g can be measured as vacuum Rabi splitting, i.e. a splitting $2g$ of the energy eigenstates $|01\rangle$ and $|10\rangle$, where the first number is the label of the computational states of the qubit, and the second the occupation of the resonator. In resonance, i.e. $\omega_r = \omega_{01}$, and for $g = 0$, these two states would be degenerate in energy, but the degeneracy is lifted for $g > 0$. In the dispersive regime characterized by $|\omega_{01} - \omega_r| \gg g$, i.e. strong detuning, one finds in second order in g the coupling $V = \hbar\frac{g^2}{\Delta}\left(a^\dagger a + \frac{1}{2}\right)\sigma_z$ which commutes with $H_r = \hbar\omega_r\left(a^\dagger a + \frac{1}{2}\right)$ and $H_q = \frac{\hbar\omega_{01}}{2}\sigma_z$.
The coupling V leads to a shift of the cavity resonance frequency depending on the state, or equivalently an AC-Stark shift of the qubit resonance. The "pulling" of the cavity resonance frequency allows a read-out of the qubit based on the transmission of a micro-wave pulse that is sent through the cavity, which in fact constitutes a so-called "quantum non-demolition measurement" (QND) of the qubit in the σ_z basis. These are measurements where the time-evolution of the system itself does not increase the uncertainty of the post-measurement state, a situation that is achieved if the interaction hamiltonian of the measurement apparatus with the system commutes with the system's own hamiltonian, i.e. in the present case $[H_0, V] = 0$ with $H_0 = H_r + H_q$. This allows continuous measurements, here of the qubit in the σ_z basis (computational basis), and could be used in principle to make several measurements for increasing the certainty of the read-out. Note, however, that QND does not mean that the state does not collapse in the measurement!

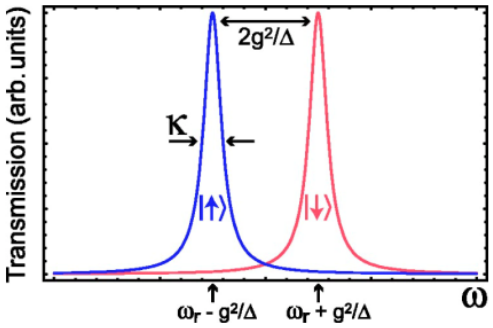


Figure 6.13: Shift of cavity resonance frequency depending on the state of the qubit. Sufficiently strong coupling g must be achieved in order to cleanly separate the two transmission lines, $2g^2/\Delta \gg \kappa$, where κ is the damping rate of the resonator. From [6].

6.3.4 Quantum gates

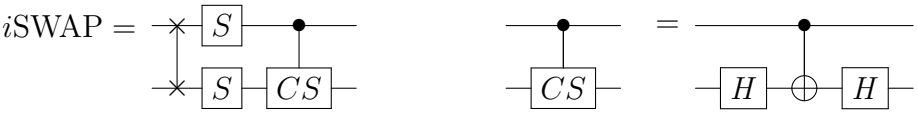
- Single-qubit gates can be realized using resonant pulses if the qubits have different resonance frequencies.
- The qubits can be coupled via photon exchange through the resonator. One brings the two qubits in resonance with each other, but detuned by Δ with respect to the resonator, such that the latter can only be virtually excited. This gives a hamiltonian

$$\Rightarrow H \simeq \hbar\left(\omega_r + \frac{g^2}{\Delta}(\sigma_i^z + \sigma_j^z)\right) a^\dagger a + \frac{\hbar}{2}\left(\omega_{01} + \frac{g^2}{\Delta}\right)(\sigma_i^z + \sigma_j^z) + \hbar\frac{g^2}{\Delta}(\sigma_i^+\sigma_j^- + \sigma_i^-\sigma_j^+).$$

In the frame rotating with frequency ω_{01} this leads to a unitary transformation [6]

$$\rightarrow U(t) = \exp\left[-i\frac{g^2}{\Delta}t(a^\dagger a + \frac{1}{2})(\sigma_i^z + \sigma_j^z)\right] \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\left(\frac{g^2}{\Delta}t\right) & i\sin\left(\frac{g^2}{\Delta}t\right) & 0 \\ 0 & i\sin\left(\frac{g^2}{\Delta}t\right) & \cos\left(\frac{g^2}{\Delta}t\right) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \otimes \mathbb{1}_r\,,$$

where the last equation is written in the computational basis of the two qubits i, j involved, and $\mathbb{1}_r$ is the identity operation on the resonator. For $t = \pi\frac{\Delta}{4g^2} \quad \sim 50\,\text{ns}$ $\Rightarrow U(t) = e^{i\alpha}\sqrt{i\text{SWAP}}$, with some irrelevant global phase α, which is equivalent to a CNOT up to local unitaries:



If the two qubits are not in resonance with each other, the coupling is effectively switched off.

Given that the resonator induces itself a certain amount of decoherence, state-of-the-art designs avoid it and rather use a direct inductive coupling by branching-off part of the current [11, 22], see Fig.6.14. Higher gate fidelities can herewith be reached, and the coupling can be tuned via the external flux ϕ_{ext} that modifies the inductance L_T.

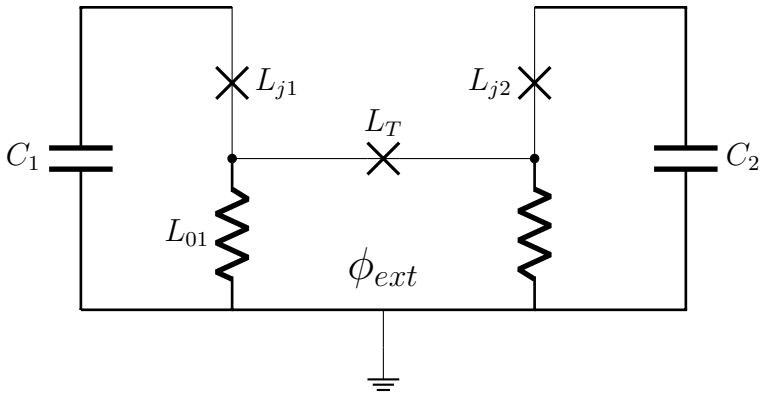


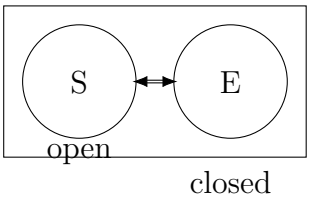
Figure 6.14: Inductive coupling of two superconducting qubits. The coupling can be controled via the external flux ϕ_{ext} that modifies the effective inductance L_T.

7 Open Quantum Systems, Decoherence and Quantum Channels

7.1 Open quantum systems

In standard non-relativistic quantum mechanics, the state vector $|\psi(t)\rangle$ evolves acccording to the Schrödinger equation. This is relevant for a system that is *closed*, meaning that the system does not interact with another quantum system with which it could exchange energy, particles, or information. If the hamiltonian depends on time, that time-dependence is supposed to arrive from a classical control system that dictates the time-dependence without back-action. This is an idealization, of course, as any system is fundamentally quantum, as far as we know. If $H(t) = H$ is independent of t, the system is also called isolated.
Systems that are not closed are called open, and this is the far more common situation. In principle, every system with arguably the exception of the entire universe is open, as there is at least the gravitational interaction with the rest of the universe. The issue of sufficiently isolating a system for independent, reproducible study exists already in classical mechanics, but is more severe in QM: There is the new effect of loss of coherence, absent in classical mechanics, besides the loss of energy/particles already present in classical mechanics. Loss of coherence is *the* main difficulty in building a quantum-computer, and so we need to understand how it comes about, how to describe and study it, and ultimately how to remedy it.

Hamiltonian embedding Idea: System S + Environment + Interaction $\Rightarrow$ closed total system.



$$H = H_s + H_e + H_{int}$$

Example:

$$\begin{aligned} H_s &= \frac{\hbar\omega_1}{2}\sigma_z^{(1)} \qquad \text{(a single spin } -\frac{1}{2}\text{)} \\ H_e &= \frac{\hbar\omega_2}{2}\sigma_z^{(2)} \qquad \text{(a second spin } -\frac{1}{2}\text{)} \\ H_{int} &= g\sigma_z^{(1)}\sigma_z^{(2)} \qquad \text{(an Ising interaction)} \end{aligned}$$

$\Rightarrow$ *Composite quantum system*

$\Rightarrow$ Description:

1. tensor products
2. density matrices.

In general, the environment can contain many degrees of freedom, and truly irreversible behavior arises when the number of degrees of freedom of the environment goes towards ∞ (e.g. continuum of harmonic oscillators). This has its counterpart in classical mechanics where the Poincaré-recurrence time approaches ∞ when the dimensions of phase space approaches ∞.

An important operation for composite systems is the *partial trace:* Let C be an operator on $\mathcal{H} = \underbrace{\mathcal{H}_1}_{S} \otimes \underbrace{\mathcal{H}_2}_{E}$ (with dimensions d_i, $i = 1, 2$). Then

$$\mathrm{tr}_2 C \equiv \sum_{i=1}^{d_2} \langle i|C|i\rangle \,,$$

where $\{|i\rangle\}_{i=1,\ldots,d_2}$ is an orthonormal basis of $\mathcal{H}_2$. So $\mathrm{tr}_2 C$ is still an operator on $\mathcal{H}_1$. In terms of matrix elements:

$$(\mathrm{tr}_2 C)_{mn} = \sum_{i=1}^{d_2} C_{mi,ni}, \qquad\qquad m, n = 1, \ldots, d_1$$

The partial trace over the first subsystem is defined correspondingly as

$$\mathrm{tr}_1 C = \sum_{i=1}^{d_1} \langle i|C|i\rangle \,,$$

where now $\{|i\rangle\}_{i=1,\ldots,d_1}$ is an orthonormal basis of $\mathcal{H}_1$. In terms of matrix elements:

$$(\mathrm{tr}_1 C)_{ij} = \sum_{m=1}^{d_1} C_{mi,mj}, \qquad\qquad i, j = 1, \ldots, d_2$$

Note that while $\mathrm{tr}(A \cdot B) = \mathrm{tr}(B \cdot A)$, in general $\mathrm{tr}_2(A \cdot B) \neq \mathrm{tr}_2(B \cdot A)$ (and similarly for tr_1).

Suppose a composite system is in pure state $|\Psi\rangle$, and we measure observable A of the first system. The expectation value is given by

$$\begin{aligned}
\langle A\rangle &= \langle\Psi|A\otimes\mathbb{1}|\Psi\rangle \\
\Rightarrow \langle A\rangle &= \mathrm{tr}\left(A\otimes\mathbb{1}\,|\Psi\rangle\langle\Psi|\right) = \sum_{n,i}\langle n,i|\,A\otimes\mathbb{1}\,|\Psi\rangle\langle\Psi|n,i\rangle \\
&= \sum_{\substack{n,m\\i,j}} \underbrace{\langle n,i|A\otimes\mathbb{1}|m,j\rangle}_{=A_{nm}\,\underbrace{\mathbb{1}_{ij}}_{=\delta_{ij}}}\langle m,j|\Psi\rangle\langle\Psi|n,i\rangle \\
\langle A\rangle &= \sum_{\substack{n,m\\i}} A_{nm}\langle m,i|\Psi\rangle\langle\Psi|n,i\rangle = \sum_{nm} A_{nm}\underbrace{\left(\mathrm{tr}_2\,|\Psi\rangle\langle\Psi|\right)_{mn}}_{\left(\rho_r^{(1)}\right)_{mn}} \\
&= \sum_{n,m} A_{nm}\left(\rho_r^{(1)}\right)_{mn} = \mathrm{tr}(A\rho_r^{(1)})\,.
\end{aligned}$$

So the expectation value of $\langle A\rangle$ can be calculated when knowing the *reduced-density matrix* $\rho_r^{(1)} \equiv \mathrm{tr}_2\,|\Psi\rangle\langle\Psi|$, obtained by tracing out the second subsystem with a partial trace. This generalizes to the case where also the total system is in a mixed state with density matrix W: Simply replace in the derivation $|\Psi\rangle\langle\Psi| \to \sum_n p_n\,|\Psi_n\rangle\langle\Psi_n| \equiv W$. Then $\boxed{\rho_r^{(1)} = \mathrm{tr}_2 W}$.

Clearly $W = |\Psi\rangle\langle\Psi|$ is a special case (pure state). It is a rank-1 projector, and thus $\mathrm{tr}W^2 = 1 \Leftrightarrow W = |\Psi\rangle\langle\Psi|$ pure state.

As the *total system is closed*, its time evolution for any initial state $|\Psi_n\rangle$ is given by the SE, and thus, for initially fixed p_n, $W(0) = \sum_n p_n\,|\Psi_n(0)\rangle\langle\Psi_n(0)|$

$$\begin{aligned}
W(t) &= U(t)W(0)U^\dagger(t) \\
i\hbar\dot{W}(t) &= [H(t), W(t)]
\end{aligned}$$

(note the opposite sign compared to the Heisenberg equation for an operator A).

The unitary *time evolution* of $W(t)$ of the density matrix of the full system entails an evolution *of the reduced density matrix* that is, in general, *not unitary* anymore.

$$\rho_r^{(1)}(t) = \mathrm{tr}_2\left(U(t)W(0)U^\dagger(t)\right)\,. \tag{7.1}$$

This is the origin of decoherence and dissipation. In the next section we will look at the description of open quantum systems on a more abstract level and introduce tools that allow one to study them independently of particular physical models of environments and interactions with environments. Only the most fundamental insight of this section, namely that the most general quantum evolution is obtained by coupling the system to another quantum system called "environment", "bath" or "ancilla", propagating them together and then tracing out the environment will be retained as guiding principle.

7.2 Quantum operations

A quantum operation or " quantum channel " is very generally a mapping of the density matrix ρ of a system

$$\rho' = \mathcal{E}(\rho). \tag{7.2}$$

We can think of ρ as the reduced density matrix, after tracing out an environment, but we will keep writing ρ instead of ρ_r, and think of ρ as *the* state of the system.

Reminder (properties of the density matrix):
In general, ρ describes a " mixed quantum state ", i.e. an ensemble of states $|\psi_i\rangle$ where each state is prepared with probability p_i. Mathematically, ρ is a linear operator on the Hilbert space $\mathcal{H}$ of the system. If $N = \dim \mathcal{H}$ is finite, ρ can be represented by a complex $N \times N$-matrix, $\rho \in \mathcal{M}_{\mathcal{N}}(\mathbb{C})$ with the following properties:

- $\rho = \rho^\dagger$
- $\operatorname{tr} \rho = 1$
- $\rho \geq 0$ (i.e. ρ is a positive matrix, $\langle\psi| \rho |\psi\rangle \geq \forall\, |\psi\rangle \in \mathcal{H}$)
- Decomposition $\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$, $0 < p_i \leq 1$, $\sum_i p_i = 1$ and $|\psi_i\rangle$ are arbitrary and arbitrarily many states, not necessarily orthonormal.
- The decomposition is not unique but it can be uniquely diagonalised:

$$\rho = \sum_{i=1}^{N} p_i |\varphi_i\rangle \langle\varphi_i|, \langle\varphi_i|\varphi_j\rangle = \delta_{ij} \tag{7.3}$$

where N is the dimension of Hilbert space $\mathcal{H}$.

Example 18

Unitary propagation of an isolated system,

$$\rho' = U\rho U^\dagger,\, U^\dagger U = \mathbb{1} = UU^\dagger\,. \tag{7.4}$$

Here we have $\mathrm{tr}\,\rho' = 1, \rho' \geq 0$ *if the same holds true for* ρ*. The propagation is given by* $U = U(t) = \exp(-iHt/\hbar)$ *according to the laws of quantum mechanics, where* H *is the hamiltonian of the system.*

Example 19
von-Neumann measurement (projective measurement)

$$\rho' = \mathrm{P}\,\rho\,\mathrm{P}, \mathrm{P}^2 = \mathrm{P}\ . \tag{7.5}$$

Here, P *is the projector onto the eigenvector corresponding to the eigenvalue of the observable that was found in the measurement. From this example we see that we can have* $\mathrm{tr}\,\rho' \leq \mathrm{tr}\,\rho$ *after a quantum operation. But post-selection of the measurement result leads to a rescaling,*

$$\rho' = \frac{\mathrm{P}\,\rho\,\mathrm{P}}{\mathrm{tr}\,\mathrm{P}\,\rho\,\mathrm{P}}\,, \tag{7.6}$$

such that the trace of the density matrix is again $\mathrm{tr}\,\rho' = 1$*. Post-selection means that from an initial ensemble of quantum systems in state* ρ*, we keep only the quantum systems for which we found the measurement result correponding to* P*. Classically, it amounts to going over to conditional probabilities. In order to have them normalized again, one has to divide with the probability of finding that measurement result. This operation makes the full map non-linear in* ρ*, however.*

We will now deduce a description for general quantum operations, which is valid for unitary, dissipative and decoherent dynamics or measurement processes. Let S be a system interacting with its environment, a thermal reservoir or "bath"B like for example phonons in a lattice, photons, or one or multiple other q-bits. We assume an initial state that can be factorised; this is in principle always possible by shifting the initial time t_0 to $t_0 \to -\infty$ where it is assumed that there was no interaction yet. The combined system $S + B$ is a closed system. Hence, the time evolution of both systems combined can be described using an unitary time evolution:

$$W(0) = \rho(0) \otimes \rho_B(0) \overset{U}{\mapsto} W(t) = UW(0)U^\dagger. \tag{7.7}$$

(a) (b)

Figure 7.1: Unitary time evolution of an isolated system in (b) vs. a general quantum channel for a system interacting with a heat bath in (a).

To describe the system S alone, one has to calculate the reduced density matrix

$$\rho(t) = \mathrm{tr}_B\, W(t) \tag{7.8}$$

where tr_B is the trace over the bath, i.e. $\mathrm{tr}_B(\cdots) = \sum_k {}_B\langle e_k| \cdots |e_k\rangle$ where $\{|e_k\rangle\}_k$ is an orthonormal basis of the Hilbert space $\mathcal{H}_B$ of the bath.
In general a quantum operation can hence be represented as

$$\rho' = \mathcal{E}(\rho) = \mathrm{tr}_B\, U\rho \otimes |e_0\rangle\langle e_0|\, U^\dagger \tag{7.9}$$

with the initial state $|e_0\rangle$ of B. It is sufficient to consider a fixed pure state $|e_0\rangle$ for the environment. The preparation of any other initial state can absorbed in U.

Let $\{|e_k\rangle\}$ be a complete orthonormal basis for B, then

$$\mathcal{E}(\rho) = \sum_k \langle e_k| U\rho \otimes |e_0\rangle\langle e_0| U^\dagger |e_k\rangle \tag{7.10}$$

$$\equiv \sum_k E_k \rho E_k^\dagger \tag{7.11}$$

where the $E_k := \langle e_k| U|e_0\rangle$ are still operators on the system Hilbert space $\mathcal{H}_S$. This decomposition (Equation 7.11) is called "Kraus representation" [**?**] or sometimes "operator-sum representation" [31].

We can obtain a matrix representation of E_k within the Hilbert space $\mathcal{H}_S$ by sandwiching in between the basis states $\{|\nu\rangle\}$ of $\mathcal{H}_S$,

$$\langle\nu|E_k|\mu\rangle = \langle\nu|\langle e_k| U|\mu\rangle|e_0\rangle\,, \tag{7.12}$$

where U now operates as it should on states of the combined Hilbert space $\mathcal{H}$. Thus the elements of the matrix associated with E_k and therefore E_k itself are

well-defined. The operators E_k are usually called "*Kraus operators*" or *"operation elements"*.

For q-operations which preserve the trace of a system's density matrix, i.e. $\operatorname{tr}\rho' = \operatorname{tr}\rho$, one finds

$$1 = \operatorname{tr}\mathcal{E}(\rho) = \operatorname{tr}\sum_k E_k \rho E_k^\dagger \tag{7.13}$$

$$= \operatorname{tr}\sum_k E_k^\dagger E_k \rho = \operatorname{tr}\rho \qquad \forall\rho \tag{7.14}$$

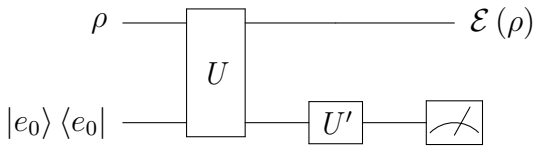
$$\iff \sum_k E_k^\dagger E_k = \mathbb{1}_S\,. \tag{7.15}$$

We can now consider Equation 7.11 as a definition for a q-operation which is specified by an ensemble of $\{E_k\}$. The operators E_k are in general neither hermitian nor unitary. Additionally, the representation in Equation 7.11 is not unique. This property is easily understood, considering that the index k also included states from $\mathcal{H}_B$ where the dimension $\dim\mathcal{H}_B$ can be arbitrarily large. At the same time, $E_k \in M_d(\mathbb{C})$ is a $d \times d$ matrix with complex elements, of which there exist at most d^2 linearly independent ones.

Hence, d^2 *Kraus operators suffice to describe any q-operation on a system* S *of dimension* $\dim\mathcal{H}_S = d$. This greatly simplifies the theory of open q-systems: Two q-processes are equivalent if they can be described with the same Kraus representation, regardless of the precise environments and interactions with the environment.

7.2.1 Freedom of Choice

The freedom of choosing different ensembles $\{E_k\}$ for one and the same quantum channel has a clear physical origin. It is based on the option of applying an additional unitary transformation on the system B alone after its interaction with S: This subsequent transformation leads us to Kraus operators F_k and their matrix



(7.16)

Figure 7.2: Physical basis for the freedom to choose different ensembles of $\{E_k\}$ for the same quantum channel: A unitary transformation that acts on the bath system B after its interaction with the system S cannot influence the final state of the system S.

elements

$$\langle\mu|F_k|\nu\rangle = \langle\mu|\langle e_k|\left(I\otimes U'\right)U|\nu\rangle|e_0\rangle \tag{7.17}$$

$$= \sum_{j,\lambda} \underbrace{\langle\mu|\langle e_k|\left(I\otimes U'\right)|\lambda e_j\rangle}_{=I_{\mu\lambda}U'_{kj}=\delta_{\mu\lambda}U'_{kj}} \langle\lambda e_j|U|\nu\rangle|e_0\rangle \tag{7.18}$$

$$= \sum_j U'_{kj}\langle\mu|\langle e_j|U|\nu\rangle|e_0\rangle \tag{7.19}$$

$$= \langle\mu|\left[\sum_j U'_{kj}\underbrace{\langle e_j|U|e_0\rangle}_{=E_j}\right]|\nu\rangle \tag{7.20}$$

$$\Rightarrow F_k = \sum_j U'_{kj}E_j \tag{7.21}$$

Theorem 16
Let $\{E_1,\ldots,E_m\}$ and $\{F_1,\ldots,F_n\}$ be two ensembles of Kraus operators describing q-operations $\mathcal{E}$ and $\mathcal{F}$, and $n \le m$. By appending 0-operators to the shorter list of Kraus operators, $n = m$ can be accomplished.

Then $\mathcal{E} = \mathcal{F}$ if and only if there exist some complex numbers u_{ij} such that

$$E_i = \sum u_{ij}F_j \tag{7.22}$$

where the u_{ij} form a unitary $m \times m$ matrix.

Proof.

We first show a little lemma.

Lemma 6
Two ensembles of states and corresponding probabilities $\{p_i, |\psi_i\rangle\}$ *und* $\{q_j, |\varphi_j\rangle\}$ *describe the same state* $\rho = \sum p_i |\psi_i\rangle \langle\psi_i| = \sum q_j |\varphi_j\rangle \langle\varphi_j|$ *if and only if*

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\varphi}_j\rangle ,$$

where

$$|\tilde{\psi}_i\rangle = \sqrt{p_i} |\psi_i\rangle , \quad |\tilde{\varphi}_j\rangle = \sqrt{q_j} |\varphi_j\rangle ,$$

where the u_{ij} *are complex numbers that combine to a unitary matrix, and the shorter of the two lists is padded with zero-vectors up to the length of the longer one.*

Proof.

(of lemma)

$$\begin{aligned}
\textit{Let} \quad |\tilde{\psi}_i\rangle &= \sum_j u_{ij} |\tilde{\varphi}_j\rangle \\
\Rightarrow \sum_i |\tilde{\psi}_i\rangle \langle\tilde{\psi}_i| &= \sum_{ijk} u_{ij} u_{ik}^* |\tilde{\varphi}_j\rangle \langle\tilde{\varphi}_j| = \sum_{jk} \sum_i (u^\dagger)_{ki} u_{ij} |\tilde{\varphi}_j\rangle \langle\tilde{\varphi}_j| \\
&= \sum_{jk} \delta_{kj} |\tilde{\varphi}_j\rangle \langle\tilde{\varphi}_k| = \sum_j |\tilde{\varphi}_j\rangle \langle\tilde{\varphi}_j| \\
\Rightarrow \rho &= \sum p_i |\psi_i\rangle \langle\psi_i| = \sum_j q_j |\varphi_j\rangle \langle\varphi_j|
\end{aligned}$$

Conversely, let $A = \sum_i |\tilde{\psi}_i\rangle \langle\tilde{\psi}_i| = \sum_j |\tilde{\varphi}_j\rangle \langle\tilde{\varphi}_j| .$ Diagaonalization $\Rightarrow A \geq 0, A = A^\dagger$

$$\begin{aligned}
\Rightarrow A &= \sum \lambda_k |k\rangle \langle k| \quad , \quad \lambda_k > 0, \quad \langle k|j\rangle = \delta_{kj}. \\
&= \sum_k |\tilde{k}\rangle \langle\tilde{k}| , \quad |\tilde{k}\rangle = \sqrt{\lambda_k} |k\rangle .
\end{aligned}$$

This means that all $|\tilde{\psi}_i\rangle$ must be linear combinations of the $|\tilde{k}\rangle$, $|\tilde{\psi}_i\rangle = \sum c_{ik} |\tilde{k}\rangle$, as otherwise A would have a component outside of the subspace spanned by the $|\tilde{k}\rangle$.

$$\Rightarrow \sum_k |\tilde{k}\rangle \langle\tilde{k}| = \sum_{kl} \left(\sum c_{ik} c_{il}^* \right) |\tilde{k}\rangle \langle\tilde{l}| .$$

The $|\tilde{k}\rangle \langle\tilde{l}|$ are linearly independent operators (canonical basis of matrices) and hence we must have $\sum_i c_{ik} c_{il}^* = \delta_{kl}$. Therefore, in the subspace spanned by the $|\tilde{k}\rangle$, the matrix c with matrix elements c_{ij} is already unitary. Outside that subspace we can add columns to c to create a unitary matrix v on the full Hilbert space such

that $|\tilde{\psi}_i\rangle = \sum_k v_{ik} |\tilde{k}\rangle$ (where zero-vectors are added also to the list of the $|\tilde{k}\rangle$ as needed). Correspondingly, we have for the $|\tilde{\varphi}_j\rangle$, $|\tilde{\varphi}_j\rangle = \sum w_{jk} |\tilde{k}\rangle$
$\Rightarrow |\tilde{\psi}_i\rangle = \sum u_{ij} |\tilde{\varphi}_j\rangle$, $\quad u = vw^\dagger$ unitary. □

Proof of Theorem:
Let $\{E_i\}$ and $\{F_j\}$ be two sets of Kraus operators that create the same quantum channel,

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger = \sum_j F_j \rho F_j^\dagger \qquad \forall \rho$$

$$\text{Define} \quad |e_i\rangle_{BS} \equiv \sum_k |k\rangle_B (E_i |k\rangle_S), \text{ which are not necessarily normalized}$$

$$|f_j\rangle = \sum_k |k\rangle_B (F_j |k\rangle_S) \quad (S\text{= system, } B = \text{bath.})$$

$$\text{Let} \quad |\alpha\rangle = \sum_i |i\rangle_B |i\rangle_S \quad \text{, a maximally entangled state of } S, B, \text{ and}$$

$$\sigma = \Big(I_B \otimes \mathcal{E}\Big) (|\alpha\rangle \langle\alpha|) \quad \text{the full state generated by application of } \mathcal{E} \text{ on } |\alpha\rangle.$$

$$\Rightarrow \sum_i |e_i\rangle_{BS} \langle e_i| = \sum_{i,k,k'} |k\rangle_B \langle k'| \otimes E_i |k\rangle_S \langle k'| E_i^\dagger = \sum_{k,k'} \Big(I_B \otimes \mathcal{E}\Big) |k\rangle_B |k\rangle_S \, {}_B\langle k'| \, {}_S\langle k'|$$

$$= \Big(I_B \otimes \mathcal{E}\Big) (|\alpha\rangle \langle\alpha|) = \sigma$$

Completely analogously, we also have $\quad \sum_j |f_j\rangle \langle f_j| = \sigma$.
Hence, from the Lemma, $\Rightarrow \quad \exists\, u_{ij}$ unitary such that $|e_i\rangle_{BS} = \sum u_{ij} |f_j\rangle_{BS}$.
Let now $|\psi\rangle_S = \sum_j \psi_j |j\rangle_S$ be an arbitrary state of the system. Define a corresponding state $|\tilde{\psi}\rangle$ of the bath,

$$|\tilde{\psi}\rangle_B \equiv \sum_j \psi_j^* |j\rangle_B .$$

$$\Rightarrow \; {}_B\langle\tilde{\psi}|\sigma|\tilde{\psi}\rangle_B = \langle\tilde{\psi}| \left(\sum_{i,j} |i\rangle_B \langle j| \otimes \mathcal{E} (|i\rangle_S \langle j|) \right) |\tilde{\psi}\rangle$$

$$= \sum_{i,j} \psi_i \psi_j^* \mathcal{E} (|i\rangle_S \langle j|) = \mathcal{E} (|\psi\rangle_S \langle\psi|) \; .$$

We can represent the action of the E_i on an arbitrary state $|\psi\rangle_S$ $E_i |\psi\rangle_S = \langle\tilde{\psi}|e_i\rangle_{BS}$,

as with this

$$\sum_i E_i \left|\psi\right\rangle_S \left\langle\psi\right| E_i^\dagger = \sum_i {}_B\left\langle\tilde{\psi}|e_i\right\rangle_{BS} \left\langle e_i|\tilde{\psi}\right\rangle_B = \langle\tilde{\psi}|\sigma|\tilde{\psi}\rangle = \mathcal{E}\left(\left|\psi\right\rangle_S \left\langle\psi\right|\right)$$

So now we have

$$E_i \left|\psi\right\rangle_S = \langle\tilde{\psi}|e_i\rangle = \sum_j u_{ij} \langle\tilde{\psi}|f_j\rangle = \sum_j u_{ij} F_j \left|\psi\right\rangle_S, \text{where we use}$$

$$F_j \left|\psi\right\rangle_S = \langle\tilde{\psi}|f_j\rangle \quad \text{completely analogously.}$$

Since $\left|\psi\right\rangle_S$ is arbitrary, it follows that $E_i = \sum_j u_{ij} F_j \quad \checkmark$.
Conversely, if $E_i = \sum_j u_{ij} F_j$ it follows by direct insertion and unitary of U that

$$\sum E_i \rho E_i^\dagger = \sum_j F_j \rho F_j^\dagger.$$

□

Central in the above proof is th surprising fact that the quantum channel $\mathcal{E}$ is uniquely determined by the state $\sigma = (I_B \otimes \mathcal{E})(|\alpha\rangle \langle\alpha|)$ with $\left|\alpha\right\rangle_{SB} = \sum_i \left|i\right\rangle_S \left|i\right\rangle_B$. This is the so-called Jamiełokowski isomorphism, and σ the Choi matrix. Another equivalent way of introducing the Choi matrix can be found in the next section.

7.3 Canonical Form

Given that two different sets of Kraus operators can describe the same quantum channel, the question arises how to determine in practice whether two given channels are the same or not. Of course, one could use theorem 16 and try to find a unitary that links the Kraus operators. There is a simpler way, however, which moreover gives additional insight into the set of all possible quantum channels. It works by constructing a unique canonical form of a given channel, such that comparison of the two channels can be based on that canonical form. The construction procedes in several steps:

1. Introduction of the *Choi* matrix [12].
   The propagation of the density matrix

$$\rho' = \mathcal{E}(\rho) \tag{7.23}$$

is written in the computational basis:

$$\rho'_{m\mu} = \sum_{n,\nu} P_{\substack{m\mu \\ n\nu}} \rho_{n\nu} \tag{7.24}$$

where P denotes the propagator with the elements $P_{\substack{m\mu \\ n\nu}}$ and the indices $M := (m, \mu)$ and $N := (n, \nu)$ (e.g. via $M = d\,(m-1) + \mu$ and $N = d\,(n-1) + \nu$). P is in general not hermitian . However, one can create a hermitian matrix D, the so-called Choi matrix, by reshuffling of the indices of P: *Choi matrix*:

$$D_{\substack{mn \\ \mu\nu}} := P_{\substack{m\mu \\ n\nu}}\,, \tag{7.25}$$

i.e. the first index of D is (m, n) (e.g. via $M = d(m-1)+n$), the second one (μ, ν) (e.g. via $N = d(\mu - 1) + \nu$).

$$D_{MN} := D_{\substack{mn \\ \mu\nu}} = {D^*}_{NM}\,. \tag{7.26}$$

We first show that D is indeed hermitian:

Proof.

$$\rho_{m\mu} = P_{\substack{m\mu \\ n\nu}} \rho_{n\nu} = \rho^*_{\mu m} \tag{7.27}$$

$$\rho^*_{\mu m} = {P^*}_{\substack{\mu m \\ n\nu}} \rho^*_{n\nu} = {P^*}_{\substack{\mu m \\ \nu n}} \rho^*_{\nu n} \tag{7.28}$$

$$= {P^*}_{\substack{\mu m \\ \nu n}} \rho_{n\nu} \qquad \forall \rho_{n\nu} \tag{7.29}$$

comparing with (7.27) gives

$$P_{\substack{m\mu \\ n\nu}} = {P^*}_{\substack{\mu m \\ \nu n}} \tag{7.30}$$

$$\Rightarrow D_{\substack{mn \\ \mu\nu}} = {D^*}_{\substack{\mu\nu \\ mn}} \iff D_{MN} = D^*_{NM} \tag{7.31}$$

thus

$$\Rightarrow D = D^\dagger \tag{7.32}$$

□

is a $d^2 \times d^2$ hermitian matrix.

2. Diagonalisation of matrix D leads to eigenvalues $d_i \geq 0$ (the positivity is linked to the "complete positivity" of any quantum channel, see below), and eigenstates $|\chi_i\rangle$. D can hence be represented as

$$D = \sum_{i=1}^{r} d_i \, |\chi_i\rangle \langle\chi_i| \, , \tag{7.33}$$

where the Kraus rank r is the number of strictly positive eigenvalues, $d_i > 0$. This gives the matrix representation

$$D_{\substack{mn \\ \mu\nu}} = \sum_{i=1}^{r} d_i \, (\chi_i)_{mn} \, (\chi_i^*)_{\mu\nu} \, , \tag{7.34}$$

where $\langle mn|\chi_i\rangle =: (\chi_i)_{mn}$: Since the eigenstates have dimensions d^2, they can be reshuffled into matrices, which are then $d \times d$, just as the original density matrix.

The Kraus operators are then given by $E_i = \sqrt{d_i}\chi_i$. Since the diagonalization of the Choi matrix is unique, we have found a canonical representation of the quantum channel:

$$\rho' = \sum_{i=1}^{r} E_i \rho E_i^\dagger = \sum_{i=1}^{r} d_i \chi_i \rho \chi_i^\dagger \tag{7.35}$$

Eq.(7.35) is best verified in the computational basis:

Proof.

$$\rho'_{m\mu} = P_{\substack{m\mu \\ n\nu}} \rho_{n\nu} = D_{\substack{mn \\ \mu\nu}} \rho_{n\nu} \tag{7.36}$$

$$= \sum_{i=1}^{r} d_i \, (\chi_i)_{mn} \, \rho_{n\nu} \underbrace{(\chi_i)^*_{\mu\nu}}_{(\chi_i)^\dagger_{\nu\mu}}, \tag{7.37}$$

and we see that only the $d_i > 0$ contribute.

□

Note that $\langle\chi_i|\chi_j\rangle = \delta_{ij}$ corresponds to $\operatorname{tr} E_i^\dagger E_j = d_i \delta_{ij}$:

$$\operatorname{tr} E_i^\dagger E_j = \sqrt{d_i d_j} \operatorname{tr} \chi_i^\dagger \chi_j \tag{7.38}$$

$$= \sqrt{d_i d_j} \, (\chi_i)^*_{nm} \, (\chi_j)_{nm} \tag{7.39}$$

$$= \sqrt{d_i d_j} \, \langle\chi_i|\chi_j\rangle = d_i \delta_{ij} \tag{7.40}$$

Example 20 (Unitary transformation)

$$\rho' = U\rho U^\dagger \Rightarrow r = 1, A_1 = U \tag{7.41}$$

Example 21 (Excitation and de-excitation)
Consider a channel with Kraus operators proportional to $\sigma_-, \sigma_+, \mathbb{1}$, defined by their action on the computational basis states $|0\rangle, |1\rangle$ as

$$\sigma_- = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \Rightarrow \sigma_- \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0 = \sigma_- |0\rangle, \;\; \sigma_- |1\rangle = \sigma_- \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$
$$\sigma_+ = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$
$$\sigma_-\sigma_+ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}(\mathbb{1} + \sigma_z)$$

Take $E_1' = \sqrt{p}\sigma_+ \quad , \quad E_2' = \sqrt{p}\sigma_- \quad , \quad E_3' = \sqrt{1-p}\,\mathbb{1}$, *i.e.*

$$\rho' = p\left(\sigma_+\rho\sigma_- + \sigma_-\rho\sigma_+\right) + (1-p)\,\rho\,.$$

Physically this channel excites and de-excites the system with equal probability p, while with probability $1-p$ it does nothing. Not surprisingly, it leads to a fully mixed stationary state, $\rho = \frac{1}{2}\mathbb{1}$, as one checks easily by propagating that state:

$$\Rightarrow \rho' = \frac{p}{2} \underbrace{\left[\sigma_+\sigma_- + \sigma_-\sigma_+\right]}_{\substack{= \frac{1}{2}(\mathbb{1}-\sigma_z)+\frac{1}{2}(\mathbb{1}+\sigma_z) \\ = \mathbb{1}}} + (1-p)\frac{\mathbb{1}}{2} = \frac{p}{2}\mathbb{1} + (1-p)\frac{\mathbb{1}}{2} = \frac{\mathbb{1}}{2} = \rho\,.$$

So we can think of the channel as describing relaxation at infinite temperature, leading to a thermal state of infinite temperature.

$$\rho'_{m\mu} = p\left((\sigma_+)_{mn}\rho_{n\nu}(\sigma_-)_{\nu\mu} + (\sigma_-)_{mn}\rho_{n\nu}(\sigma_+)_{\nu\mu}\right) + (1-p)\rho_{n\nu}\delta_{mn}\delta_{\nu\mu}$$
$$(\sigma_+)_{mn} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}_{mn} = \delta_{m1}\delta_{n0} \quad , (\sigma_-)_{\nu\mu} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}_{\nu\mu} = \delta_{\nu 0}\delta_{\mu 1}$$
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_\nu \to |1\rangle$$
$$\rho' = p\left[\sigma_+\rho\sigma_- + \sigma_-\rho\sigma_+\right] + (1-p)\rho$$

$$\Rightarrow \rho'_{m\mu} = \left(p\left(\delta_{m1}\delta_{n0}\delta_{\nu 0}\delta_{\mu 1} + \delta_{m0}\delta_{n1}\delta_{\nu 1}\delta_{\mu 0}\right) + (1-p)\delta_{mn}\delta_{\nu\mu}\right)\rho_{n\nu}$$
$$= \underset{n\nu}{P_{m\mu}}\rho_{n\nu}$$
$$\Rightarrow \underset{n\nu}{P_{m\mu}} = \underset{\mu\nu}{D_{mn}} = \left(p\left(\delta_{m1}\delta_{n0}\delta_{\nu 0}\delta_{\mu 1} + \delta_{m0}\delta_{n1}\delta_{\nu 1}\delta_{\mu 0}\right) + (1-p)\delta_{mn}\delta_{\nu\mu}\right)\,.$$

Each Kronecker-delta results in a non-zero entry in the matrix D, which can hence be represented as

mn \ $\mu\nu$	*00*	*01*	*10*	*11*
00	*1-p*			*1-p*
01		*p*		
10			*p*	
11	*1-p*			*1-p*

We read off the eigenvectors $|01\rangle, |10\rangle, (|00\rangle + |11\rangle)/\sqrt{2}, (|00\rangle - |11\rangle)/\sqrt{2}$ *and corresponding eigenvalues* $p, p, 2(1-p), 0$. *Reshuffling of the eigenvectors leads to*

$$\chi_1 = |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \Rightarrow \hat{\chi_1} = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix} = \sigma_-$$

$$\chi_2 = |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \Rightarrow \hat{\chi_2} = \begin{pmatrix}0 & 0\\1 & 0\end{pmatrix} = \sigma_+$$

$$\chi_3 = (|00\rangle + |11\rangle)/\sqrt{2} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} \Rightarrow \hat{\chi_3} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = \frac{\mathbb{1}}{\underset{\substack{\uparrow\\ \text{compensated}\\ \text{by } 2 \text{ in } d_3=2(1-p)}}{\sqrt{2}}}$$

$$\rightarrow \rho' = p\,(\sigma_-\rho\sigma_+ + \sigma_+\rho\sigma_-) + (1-p)\rho\,.$$

$\Rightarrow$ *So the original form was already the canonical form.*

Another important application of the Choi matrix is to check whether a given map of the density matrix is "completely positive". This concept is explained in the following two definitions.

Definition 9 (Positivity of a map)
$\mathcal{E}(\rho)$ *is called positive if* $\mathcal{E}(\rho) \geq 0 \quad \forall\, \rho \geq 0$.

Positivity is, of course, a necessary requirement for any quantum channel: the object returned by the map must qualify as a density matrix, hence be positive if its pre-image was a density matrix, hence positive. However, positivity of a map is

not sufficient for a quantum channel. We must require in addition that if we add whatever ancilla system and do nothing with it, the resulting state should *still* be positive:

Definition 10 (Complete Positivity)
A map $\mathcal{E}(\rho)$ is called completely positive if $\mathcal{E} \otimes \mathbb{1}_B$ is a positive map where $\mathbb{1}_B$ is the identity operation on an arbitrarily large ancilla Hilbert space.

Theorem 17 (Choi's theorem)
A linear map $\rho' = \mathcal{E}(\rho)$ is completely positive iff $D \geq 0$.

This implies the positivity of the eigenvalues of the Choi matrix, used in the construction of the canonical form of a quantum channel.

7.4 POVM Measurements

7.4.1 von-Neumann Measurements: Projective Measurements

Measurements in quantum mechanics are traditionally based on the standard axioms of projective measurements: Any possible result of the measurements of an observable A is given through the eigenvalues of its respective hermitian operator $\hat{A}$. Born's rule states that if $\hat{A}$ has the spectral decomposition $\hat{A} = \sum_i a_i |i\rangle \langle i|$, $\langle i|j\rangle = \delta_{ij}, \sum_i |i\rangle \langle i| = \mathbb{1}$, then the probability of finding the result a_i given the state $|\psi\rangle$ may be calculated by $p_i = |\langle i|\psi\rangle|^2$. After the measurement, the system is in the state $|i\rangle$ (respectively $\mathrm{P}_i |\psi\rangle / |\mathrm{P}_i |\psi\rangle|^2$, if a_i is a degenerate eigenvalue. P_i then denotes the projection to the respective subspace). Repeating the measurement many times results in an ensemble of states described the density matrix

$$\rho = \sum p_i |i\rangle \langle i| \,, \sum_i p_i = 1. \tag{7.42}$$

By using the von Neumann model for measurement processes, one may also obtain the same behaviour without postulating it:

Assume that a strong interaction $\mathrm{H}_{\mathrm{int}}$ between the system and the measuring apparatus completely dominates the dynamics of the system.

$$\mathrm{H}_{\mathrm{int}} = \sum_n |n\rangle_s \langle n| \otimes \hat{A}_n, \tag{7.43}$$

where $\hat{A}_n$ are operators of the measurement apparatus that can distinguish different states $|n\rangle$ of the system. Then an initial state $|n\rangle |\Phi_0\rangle$ propagates during the measurement process to

$$|n\rangle |\Phi_0\rangle \xmapsto{\text{Prop. in } t} |n\rangle e^{-i\hat{A}_n t/\hbar} |\Phi_0\rangle \equiv c_n |n\rangle |\Phi_n(t)\rangle \ . \tag{7.44}$$

The linearity of Schrödinger's equation implies

$$\Rightarrow \sum_n c_n |n\rangle |\Phi_0\rangle \xmapsto{\text{Prop. in } t} \sum_n c_n |n\rangle |\Phi_n(t)\rangle \, . \tag{7.45}$$

Hence the reduced density matrix of the system evolves as

$$\rho(0) = \sum c_m^* c_n |n\rangle \langle m| \longrightarrow \sum c_m^* c_n \langle \Phi_m(t)|\Phi_n(t)\rangle |n\rangle \langle m| = \rho(t) \, , \tag{7.46}$$

i.e. the coherences of the system are suppressed by the factor $\langle \Phi_m(t)|\Phi_n(t)\rangle$. For the measuring apparatus to be able to differentiate between the states $|n\rangle , |m\rangle$, $|\Phi_m(t)\rangle$ and $|\Phi_n(t)\rangle$ have to be different. An interaction with a macroscopic measuring apparatus (with very high dimensional Hilbert space) leads to $\langle \Phi_m(t)|\Phi_n(t)\rangle \to 0$ very rapidly, for $n \neq m$, i.e. $|\langle \Phi_n(t)|\Phi_m(t)\rangle| \to \delta_{nm}$. The density matrix then becomes very rapidly diagonal in the basis $\{|n\rangle\}$. We see that this basis is selected by the interaction $\mathrm{H}_{\mathrm{int}}$ with the measurement apparatus. It is also called " pointer basis " for that reason, where " pointer " refers to the pointer of the measurement apparatus.

$$\rho(t) \to \sum |c_m|^2 |n\rangle \langle n| = \sum_n p_n |n\rangle \langle n| \tag{7.47}$$

But what happens if we do not assume a macroscopic measuring apparatus?

7.4.2 POVM and Quantum Probes

Example 22
Measurement of σ_z of a spin-1/2 with a Stern-Gerlach apparatus. Using the magnetic field B in z direction one should be able to measure σ_z with one of two results, $S_z = \pm 1/2$ (in units of $\hbar$). However, in a real experiment, one finds a result resembling Figure 7.3.

Where do the results $S \neq \pm 1/2$ originate from ?

The study of open q-systems and emergence of q-information theory have lead to an increased understanding of the measurement process in quantum mechanics during the last ~ 20 years. We nowadays model a measuring apparatus as a more

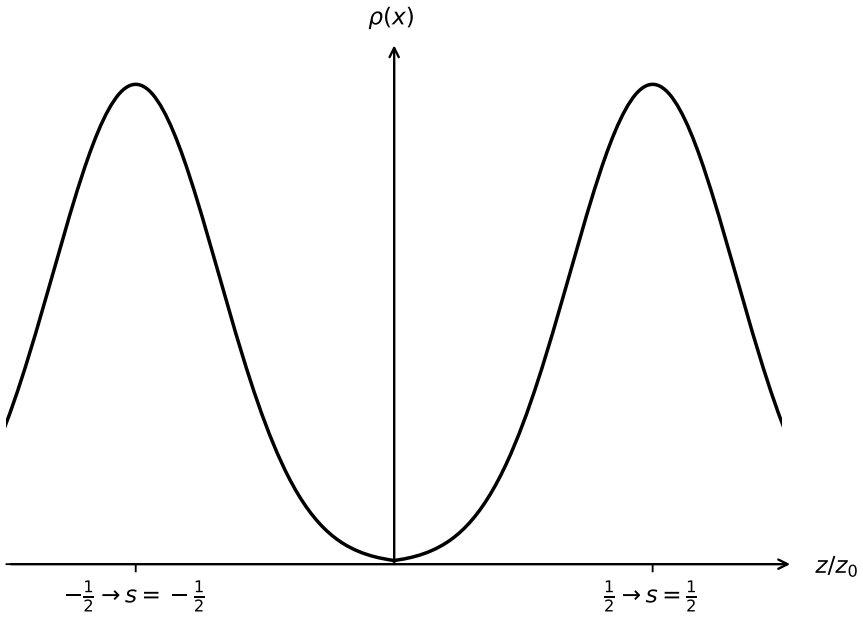


Figure 7.3: Qualitative results of measuring a spin-1/2. z is the position at which an atom arrives on the screen.

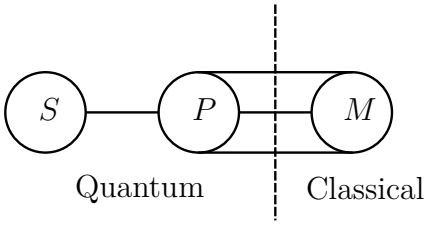


Figure 7.4: Schematic for modelling a measurement of a quantum system S using a q-probe P as an intermediate system between the actual system and the macroscopic measuring apparatus M. P interacts weakly with S but strongly with M and is hence subjected to a projective measurement by M.

or less realistic q-probe, and in general it is the latter, not the q-system itself, that is subjected to a strong projective measurement by the macroscopic measuring apparatus (from which we can then read out the value of the measurement). A schematic of this idea is shown in Figure 7.4. Sticking to this schematic we obviously stay within the framework of general q-operations (Figure 7.5a) and extend the old framework in (Figure 7.5b) considerably.

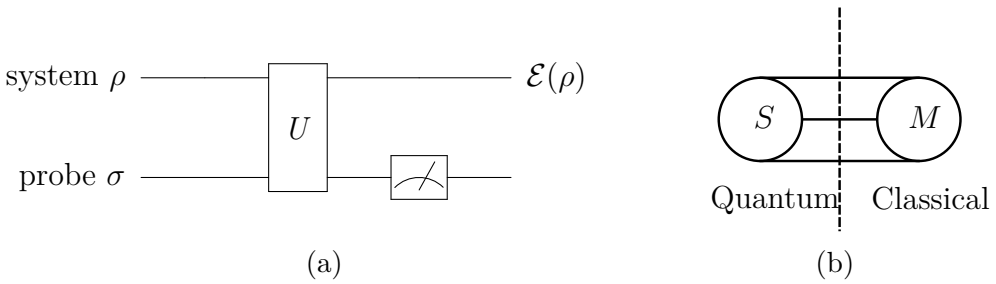


Figure 7.5: (a) Framework for quantum measurements and (b) previously considered framework for measurements.

The given example of the Stern-Gerlach experiment is representative: The gradient of the B-field entangles σ_z and z due to the interaction $\mathrm{H}_{\mathrm{int}} = \gamma\sigma_z \otimes z$ with $\gamma = -\mu\frac{\partial B_z}{\partial z}$, transforming the position of the particle into a q-probe. Here, μ is the magnetic moment of the atom, and the field $B_z(z)$ was linearized about $z = 0$, $B_z(z) \simeq \partial_z B_z(z)|_{z=0} z$ for $B(0) = 0$. Through this entangling process, the initial wave function $\psi(z)$ of the particle position is introduced into the measuring process. The uncertainty of the particle's position results in a smeared out probability distribution on the screen. The screen acts as the (macroscopic) measuring apparatus for z, not directly for σ_z!

Let the initial state $S-P$ of the system S and the probe P be

$$W_{\mathrm{SP}}(0) = \rho_S \otimes |\Phi\rangle_P \langle\Phi| , \tag{7.48}$$

where $|\Phi\rangle$ is a pure state of the probe P. The combined unitary evolution in time is given by

$$W_{\mathrm{SP}}(t) = U(t)\rho_S \otimes |\Phi\rangle_P \langle\Phi| \, U^\dagger(t). \tag{7.49}$$

We now measure the probe through the interaction with the actual, macroscopic apparatus. This apparatus performs an projective measurement of the observable $\hat{A} = \sum_i a_i |a_i\rangle \langle a_i|$ on P. We can then find the result a_i with the probability p_i that describes the distribution of the atoms' positions z on the screen.

$$p_i = \mathrm{tr}_{S,P}\left\{\mathbb{1}_S \otimes |a_i\rangle_P \langle a_i| \, W_{SP}(t)\right\} = \mathrm{tr}_{S,P}\left\{\hat{P}_i W_{SP}(t)\right\} \tag{7.50}$$

where $\hat{P}_i = \mathbb{1}_S \otimes |a_i\rangle_P \langle a_i|$:

$$p_i = \mathrm{tr}_{S,P}\left\{\mathbb{1}_S \otimes |a_i\rangle \langle a_i| \; U(t)\left(\rho \otimes |\Phi\rangle \langle \Phi|\right) U(t)^\dagger\right\} \tag{7.51}$$

$$= \mathrm{tr}_{S,P}\left\{\rho \otimes |\Phi\rangle \langle \Phi| \; U(t)^\dagger \mathbb{1}_S \otimes |a_i\rangle \langle a_i| \; U(t)\right\} \tag{7.52}$$

$$= \mathrm{tr}_S\left\{\rho \, \mathrm{tr}_P\left\{\otimes |\Phi\rangle \langle \Phi| \; U(t)^\dagger \otimes |a_i\rangle \langle a_i| \; U(t)\right\}\right\} \tag{7.53}$$

$$\equiv \mathrm{tr}_S\left\{\rho E_i\right\} \tag{7.54}$$

where from (7.51) to (7.52) we used the cyclic invariance of the trace, and in (7.54) we introduced

$$E_i := \mathrm{tr}_P\left\{\langle \Phi| U(t)^\dagger |a_i\rangle \langle a_i| U(t)|\Phi\rangle\right\} \equiv A_i^\dagger A_i \tag{7.55}$$

$$A_i := \langle a_i| U(t)|\Phi\rangle \; , \tag{7.56}$$

where we supressed the time-argument of E_i and A_i. The operators E_i are called *POVM elements* (engl. *positive operator valued measure*) [32]. The POVM elements constitute an ensemble, called POVM $\{E_i\}$. This ensemble is sufficient to calculate the probability a_i for all possible results a_i. Using $\sum_i |a_i\rangle \langle a_i| = \mathbb{1}_S$ we have

$$\sum_i E_i = \sum_i \langle \Phi| U(t)^\dagger |a_i\rangle \langle a_i| U(t)|\Phi\rangle = \mathbb{1}_S. \tag{7.57}$$

Because $E_i = A_i^\dagger A_i$, the elements POVM satisfy $E_i \geq 0$ (semi-positive definite operators, or "positive operator" for short). These properities motivate the name POVM: The ensemble $\{E_i\}$ can be compared to a classical measure $\mu(i)$ on a set of possible outcomes $\{\mathrm{i}\}$. The E_i sum to $\mathbb{1}_B$, are positive and operator-valued. It is also obvious, that $E_i = E_i^\dagger$. As we can see, all possible results of a measurement are determined by the probe and the measurement of the probe, but not as in a projective von-Neumann measurement by a hermitian operator of the system itself. The state of S at time $t+\epsilon$ right after the measurement with outcome i reads

$$\rho_S{}'^{(i)} = \mathrm{tr}_P\left\{W_{SP}(t+\epsilon)\right\} = \mathrm{tr}_P\left\{\frac{\hat{\mathrm{P}}_i W_{SP}(t) \hat{\mathrm{P}}_i}{p_i}\right\} \tag{7.58}$$

where p_i denotes the probability $p_i \equiv \mathrm{tr}_S\left\{\rho E_i\right\}$.

$$\rho_S{}'^{(i)} = \frac{1}{p_i} \sum_k \langle e_k| \, \mathrm{P}_i \; U(t)\left(\rho_s \otimes |\Phi\rangle \langle \Phi|\right) U(t)^\dagger \, \mathrm{P}_i \, |e_k\rangle \tag{7.59}$$

$$= \frac{1}{p_i} \sum_k \langle e_k| \, \mathrm{P}_i \; U(t)|\Phi\rangle \, \rho_s \, \langle \Phi| U(t)^\dagger \, \mathrm{P}_i \, |e_k\rangle \tag{7.60}$$

We introduce a new definition at this point using the same A_i as defined before (Equation 7.56):

$$\rho_S{}'^{(i)} \equiv \sum_k B_k^{(i)} \rho_s \left(B_k^{(i)}\right)^\dagger \tag{7.61}$$

$$B_k^{(i)} := \frac{1}{\sqrt{p_i}} \langle e_k | a_i \rangle A_i \,. \tag{7.62}$$

This way, the process of measuring now *formally looks like* a general quantum operation represented by Kraus operators. This however only holds formally, since the p_i depend on ρ through the renormalisation to $\operatorname{tr} S\rho_S = 1$ as the wave function collapses and implies a non-linear map of ρ. Also $\sum_k B_k^\dagger B_k = \mathbb{1}_S$ is not fulfilled. Rather we need in addition to insert the p_i,

$$\sum_{i,k} p_i B_k^{(i)\dagger} B_k^{(i)} = \sum_{k,i} \langle a_i \underbrace{|e_k\rangle\langle e_k|}_{\sum_k \Rightarrow \mathbb{1}_P} a_i \rangle A_i^\dagger A_i \tag{7.63}$$

$$= \sum_i A_i^\dagger A_i \tag{7.64}$$

$$= \sum_i E_i = \mathbb{1}_S \tag{7.65}$$

But without the postselection, i.e. when keeping the whole ensemble of post-measurement states, ($\rho'_s = \sum p_i \rho_i$) the operation is also formally a quantum operation:

$$\rho'_S = \sum_i p_i \rho_S^{'(i)} = \sum_{k,i} \langle e_k | a_i \rangle A_i \rho_s A_i^\dagger \langle a_i | e_k \rangle = \sum_i A_i \rho_s A_i^\dagger, \text{ and } \sum_i A_i^\dagger A_i = \sum_i E_i = \mathbb{1}_S. \tag{7.66}$$

Until now we assumed the initial state of the quantum probe P to be a pure state $|\Phi\rangle$. We now generalize to a mixed initial state ρ_P. For the POVM elements the formalism easily yields

$$E_i = \operatorname{tr}_P \left\{ \rho_P U(t)^\dagger |a_i\rangle \langle a_i| U(t) \right\}. \tag{7.67}$$

We do, however, loose the representation (7.55) in terms of A_i in this case. By writing ρ_P as $\rho_P = \sum_l q_l |l\rangle \langle l|$ we can at least get a similar form

$$E_i = \sum_l A_{il}^\dagger A_{il}, \qquad A_{il} = \langle a_i | U(t) | l \rangle \sqrt{q_l}. \tag{7.68}$$

If $q_l = \delta_{l,0}$ this gives back (7.55), and (7.56) .

For a mixed state we also get a more complicated update rule for the system state after the measurement:

$$\rho_S' = \sum_{k,l} B_{kl}^{(i)} \rho_S B_{kl}^{(i)\dagger} \tag{7.69}$$

$$B_{kl}^{(i)} = \frac{1}{\sqrt{p_i}} \langle e_k | a_i \rangle A_{il} \tag{7.70}$$

7.5 Axiomatic Approach to Quantum operations

Following the previous sections, we can now define q-operations axiomatically.

Definition 11 (Quantum operation)
A quantum operation $\mathcal{E}$ is a map of the set of density operators of the input Hilbert space $\mathcal{H}$ to the set of density operators on the output Hilbert space $\mathcal{H}'$ with the following properties:

- *(A1)* $\operatorname{tr} \mathcal{E}(\rho)$ *represents the probability of the process, being represented by* $\mathcal{E}$ *to take place if* ρ *is the initial state. Thus,* $0 \leq \operatorname{tr} \mathcal{E}(\rho) \leq 1 \forall \rho$.

- *(A2)* $\mathcal{E}$ *is a linear convex map, i.e. for arbitrary probabilities* $\{p_i\}$, $0 \leq p_i \leq 1, \sum_i p_i = 1$ *the relation*

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i) \tag{7.71}$$

  holds.

- *(A3)* $\mathcal{E}$ *is a completely positive map, i.e.* $\mathcal{E}(A) \geq 0 \; \forall A \geq 0$, *but also* $(\mathbb{1}_R \otimes \mathcal{E})(A) \geq 0 \; \forall A \geq 0$. *In the latter case* A *denotes a positive operator of an arbitrary composite system* $R + Q$ *where* $\mathbb{1}_R$ *is the identity operation on the Hilbert space of* R, *and* Q *the actual q-system.*

Axiom (A1) is with the possibility of a measurement as a quantum operation in mind, in which case $\mathcal{E}(\rho) = E_i \rho E_i^\dagger$ is a single quantum operation that leads to measurement outcome i, and $\operatorname{tr} \mathcal{E}(\rho) \leq 1$ in general. For a deterministic quantum operation such as a unitary transformation, the probability for the process to take place is equal to 1, which is reflected by the preservation of the trace of ρ in that case.

Theorem 18
A map $\rho' = \mathcal{E}(\rho)$ is a q-operation if and only if

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \tag{7.72}$$

for a set $\{E_i\}$ of operations mapping the input Hilbert space $\mathcal{H}$to the output Hilbert space $\mathcal{H}'$, where the E_i satisfy

$$\sum_i E_i^\dagger E_i \leq \mathbb{1} \tag{7.73}$$

Proof (Theorem 18).

"$\Leftarrow$":

- (A1) Because $\sum_i E_i^\dagger E_i \leq \mathbb{1}$, we have

$$0 \leq \operatorname{tr} \mathcal{E}(\rho) = \sum_i \operatorname{tr} E_i \rho E_i^\dagger = \operatorname{tr} \sum_i E_i^\dagger E_i \rho \leq \operatorname{tr} \rho = 1\,. \tag{7.74}$$

- (A2) Since $\mathcal{E}(\rho)$ is linear, it is also convex linear.
- (A3) What is left to show is that $\mathcal{E}(\rho)$ in eq.(7.72) is completely positive:

  Let $A \geq 0$ be a positive operator operating on the Hilbert space of a joined system RQ and let $|\psi\rangle$ be a state of this Hilbert space RQ. Define $|\varphi_i\rangle := \left(I_R \otimes E_i^\dagger\right)|\psi\rangle$ from which follows

$$\langle\psi| \left(I_R \otimes E_i\right) A \left(I_R \otimes E_i^\dagger\right) |\psi\rangle = \langle\varphi_i|A|\varphi_i\rangle \geq 0 \tag{7.75}$$

  because $A \geq 0$ is a positive operator of the joined system. By summing over i yields

$$\langle\psi|\Big(\mathcal{I} \otimes \mathcal{E}(A)\Big)|\psi\rangle = \langle\psi| \sum_i \left(I_R \otimes E_i\right) A \left(I_R \otimes E_i^\dagger\right) |\psi\rangle \tag{7.76}$$

$$= \sum_i \langle\varphi_i|A|\varphi_i\rangle \geq 0 \tag{7.77}$$

  for any positive operator A. This proves that $\rho \mapsto \mathcal{E}(\rho)$ is a completely positive map.

"⇒": let $\rho \mapsto \mathcal{E}(\rho)$ satisfy (A1), (A2), (A3).
We introduce an auxiliary system R which has the same dimension as the original system Q. Let $\left\{ |i\rangle_R \right\}, \left\{ |i\rangle_Q \right\}$ be two orthonormal bases of the two Hilbert spaces $\mathcal{H}_R$ and $\mathcal{H}_Q$. Define

$$|\alpha\rangle := \sum_i |i\rangle_R |i\rangle_Q \tag{7.78}$$

which is the maximally entangled state (unnormalised), and

$$\sigma := \Big(I \otimes \mathcal{E} \Big) \left(|\alpha\rangle \langle\alpha| \right) \tag{7.79}$$

generally a mixed state.

It can be shown, that the state σ uniquely identifies the q-operation $\rho \mapsto \mathcal{E}(\rho)$, which is the so called *Choi-Jamiełokowski-isomorphism*:
Let $|\psi\rangle = \sum \psi_j |j\rangle_Q$ be an arbitrary state of the system Q. We now define the corresponding state $|\tilde{\psi}\rangle$ of the system R, where

$$|\tilde{\psi}\rangle := \sum_j \psi_j^* |j\rangle_R \tag{7.80}$$

i.e. as the complex conjugate of the state, in the Hilbert space $\mathcal{H}_R$ instead of $\mathcal{H}_Q$ and in the basis $|j\rangle_R$. It follows from this definition, that

$$\langle\tilde{\psi}|\sigma|\tilde{\psi}\rangle = \langle\tilde{\psi}| \sum_{i,j} |i\rangle_R \langle j| \otimes \mathcal{E}\left(|i\rangle_Q \langle j| \right) |\tilde{\psi}\rangle \tag{7.81}$$

$$= \sum \psi_i \psi_j^* \mathcal{E}\left(|i\rangle_Q \langle j| \right) \tag{7.82}$$

$$= \mathcal{E}\left(|\psi\rangle \langle\psi| \right) . \tag{7.83}$$

This means that we can generate the q-channel simply by sandwiching the complex conjugate of the state to be mapped around the special state σ encoding $\mathcal{E}$. This is the Choi-Jamiełokowski isomorphism (Table 7.1)

$\mathcal{E}(\rho)$	$\Leftrightarrow$	σ on $\mathcal{H}_{QR}$
$\dim \mathcal{H}_Q = d$		$\dim \mathcal{H}_{QR} = d^2$

Table 7.1: Correspondences in the Choi-Jamiełokowski isomorphism for the q-channel $\mathcal{E}$ acting on the density operator ρ on $\mathcal{H}_Q$

We can diagonalise $\sigma \Rightarrow \sigma = \sum_i |s_i\rangle \langle s_i|$, where $|s_i\rangle$ are states of the joined Hilbert space $\mathcal{H}_{QR}$ but not normalised (the states contain the $\sqrt{\text{eigenvalue}_i}$). Then we

define the map $E_i(|\psi\rangle) := \langle\tilde{\psi}|s_i\rangle$ which still yields a state in the Hilbert space Q. The map is linear: Using $|\psi\rangle = \sum_j \psi_j |j\rangle_Q$, we have:

$$E_i(|\psi\rangle) = E_i\left(\sum \psi_j |j\rangle_Q\right) \tag{7.84}$$

$$= {}_Q\langle\tilde{\psi}|s_i\rangle \tag{7.85}$$

$$= \sum_j \psi_j \; {}_R\langle j|s_i\rangle \tag{7.86}$$

$$= \sum_j \psi_j E_i\left(|j\rangle_Q\right) . \tag{7.87}$$

This shows that E_i defines a linear operator on $\mathcal{H}_Q$. Summing over i we get

$$\sum_i E_i |\psi\rangle\langle\psi| E_i^\dagger = \sum_i \langle\tilde{\psi}|s_i\rangle\langle s_i|\tilde{\psi}\rangle \tag{7.88}$$

$$= \langle\tilde{\psi}|\sigma|\tilde{\psi}\rangle \tag{7.89}$$

$$= \mathcal{E}(|\psi\rangle\langle\psi|) . \tag{7.90}$$

Since the map is linear convex (A2), we can also directly derive the decomposition for mixed states:

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger, \tag{7.91}$$

i.e. we have found a Kraus representation of $\mathcal{E}$. The requirement $\sum_i E_i^\dagger E_i \leq \mathbb{1}$ is directly fulfilled due to the first axiom (A1), which identifies $\operatorname{tr}\mathcal{E}(\rho)$ with a probability. □

It can be shown that $\langle ij|\sigma|kl\rangle = D_{jilk}$, the Choi matrix from eq.(7.25).

7.5.1 Examples: Simple Quantum Operations

Trace

The q-operation is given by

$$\mathcal{E}(\rho) = (\operatorname{tr}\rho)|0\rangle\langle 0| \tag{7.92}$$

where $|0\rangle\langle 0|$ is a fixed state of reference. This operation is a q-operation, because one may write it using the Kraus operators

$$E_i = |0\rangle\langle i| , \qquad i = 1, \ldots, d \tag{7.93}$$

Interpretation: all of the basis states $|i\rangle$ of $\mathcal{H}_Q$ are mapped to $|0\rangle$. Thus, indeed,

$$\sum_{i=1}^{d} E_i \rho E_i^\dagger = \sum_{i=1}^{d} |0\rangle \langle i|\rho|i\rangle \langle 0| \tag{7.94}$$

$$= (\operatorname{tr}\rho)\,|0\rangle\langle 0| = \mathcal{E}(\rho)\ . \tag{7.95}$$

One may also define a q-operation

$$\mathcal{E}(\rho) = \operatorname{tr}\rho P/p\,, \tag{7.96}$$

where P represents an arbitrary general projector, $P^2 = P$ into a sub-space of dimensions p. This is achieved by defining additional Kraus operators:

$$E_{ji} := |j\rangle\langle i|/\sqrt{p}, \qquad i = 1,\ldots,d; j = 1,\ldots,p \tag{7.97}$$

which operate on ρ as

$$\sum_{i,j} E_{ji}\rho E_{ji}^\dagger = \frac{1}{p}\sum_{j=1}^{p}\sum_{i=1}^{d} |j\rangle\langle i|\rho|i\rangle\langle j| \tag{7.98}$$

$$= \frac{1}{p}\sum_{j=1}^{p} |j\rangle\langle j|\operatorname{tr}\rho. \tag{7.99}$$

In particular, for $p = d$ this becomes $\mathcal{E}(\rho) = (\operatorname{tr}\rho)\mathbb{1}$, and one checks that $\sum_{i,j} E_{ji}^\dagger E_{ji} = \mathbb{1}$.

Bit Flip and Phase Flip

The following effects represent the bit and phase flip operations:

bit flip

$$E_0 = \sqrt{p}\mathbb{1} = \sqrt{p}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \tag{7.100}$$

$$E_1 = \sqrt{1-p}X = \sqrt{1-p}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \tag{7.101}$$

phase flip:

$$E_0 = \sqrt{p}\mathbb{1} \tag{7.102}$$

$$E_1 = \sqrt{1-p}Z = \sqrt{1-p}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \tag{7.103}$$

which can be understood by observing the effects on the density matrix

$$\rho' = \mathcal{E}(\rho) = \begin{cases} p\rho + (1-p)\, X\rho X & \text{bit flip} \\ p\rho + (1-p)\, Z\rho Z & \text{phase flip.} \end{cases} \tag{7.104}$$

With a probability of p nothing happens. With a probability of $1-p$ the qubit (or its phase) is flipped [1]. A geometric representation can be given using a mapping of the Bloch sphere: Let

$$\rho = \frac{\mathbb{1} + \boldsymbol{r}\cdot\boldsymbol{\sigma}}{2} \tag{7.105}$$

where $\boldsymbol{r} \in \mathbb{R}^3, |\boldsymbol{r}| \leq 1$ denotes the Bloch vector ($|\boldsymbol{r}| = 1$ for pure states). ρ is mapped onto the following components

$$\rho = \frac{1}{2}\begin{pmatrix} 1+r_z & r_x - ir_y \\ r_x + ir_y & 1-r_z \end{pmatrix}. \tag{7.106}$$

We may write this map as a linear map of $\boldsymbol{r}$, since q-operations are also linear maps and ρ is linear in $\boldsymbol{r}$. This defines an affine map of the Bloch sphere onto itself:

$$\boldsymbol{r} \overset{\mathcal{E}}{\mapsto} \boldsymbol{r'} = M\boldsymbol{r} + \boldsymbol{c}. \tag{7.107}$$

$M \in \mathbb{M}^3(\mathbb{R})$ denotes a real 3×3 matrix (which does not necessarily have to be symmetric).

We can check this claim representing also the E_i in a basis of Pauli matrices:

$$E_i = \alpha_i \mathbb{1} + \sum a_{ik}\sigma_k, \tag{7.108}$$

where $\alpha_i, a_{ik} \in \mathbb{C}$. Then (proof see Exercises)

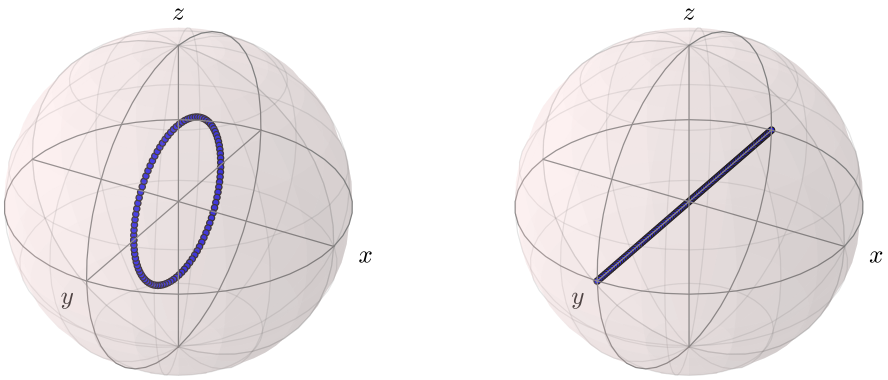
$$M_{jk} = \sum_l a_{lj}a^*_{lk} + a^*_{lj}a_{lk} + \left(|\alpha_l|^2 - \sum a_{lp}a^*_{lp}\right)\delta_{jk} + i\sum_p \left(\alpha_l a^*_{lp} - \alpha^*_l a_{lp}\right)\epsilon_{jkp} \tag{7.109}$$

$$c_k = 2i\sum_l \sum_{ip} \mathcal{E}_{jpk} a_{lj} a^*_{lp}\,, \tag{7.110}$$

where ϵ_{jkp} is the completly anti-symmetric (Levi-Civita) tensor, and δ_{jk} the Kronecker-delta.

We see that $\mathcal{E}(\rho)$ can move and deform the Bloch sphere. We call q-operations which leave the identity matrix invariant *unital* (not to be confused with "unitary":

[1] Sometimes p is defined as the probability for flipping.



(a) (b)

Figure 7.6: Mapping of the Bloch sphere under the bit-flip channel, where the blue dots represent the new y- and z- axis obtained by rescaling. (a) $p = 3/4$ and (b) $p = 1/2$.

unitary $\Rightarrow$ unital, however unitary $\not\Leftarrow$ unital.) Since $\rho = \mathbb{1}/2$ implies $\boldsymbol{r} = 0$, $\mathcal{E}(\rho)$ unital is equivilant to $\boldsymbol{c} = 0$.

In the basis consisting of the Pauli matrices the representation of ρ allows us to easily understand the effect of $\mathcal{E}(\rho)$.

E.g. for the bit flip:

$$\mathcal{E}(X) = pX + (1-p)\,XXX = X \tag{7.111}$$

i.e. the Bloch sphere stays invariant in x direction.

$$\mathcal{E}(Y) = pY + (1-p)\,XYX = (-1+2p)\,Y \tag{7.112}$$
$$\mathcal{E}(Z) = pZ + (1-p)\,XZX = (-1+2p)\,Z. \tag{7.113}$$

For the last two cases we used $XY = iZ$, $XZ =$ -iY. As we can see, the y and z axis both shrink by a factor of $(-1+2p)$, where $p \in [1/4, 1]$ suffices; if $p \in [0, 1/2]$, then the Bloch sphere is additionally turned over. If $p = 1/2$, then the Bloch sphere shrinks down to a simple line in x direction (see Figure 7.6)

A corresponding statement holds for the phase flip: The z axis is left invariant, while the x and y axis shrink by a factor of $(-1+2p)$. A special case for this

q-operation is a measurement in the computational basis. Without post-selection, such a measurement produces

$$\rho \mapsto \mathcal{E}(\rho) = P_0 \rho P_0 + P_1 \rho P_1. \tag{7.114}$$

P_i denote the projectors onto $|i\rangle, i \in \{0,1\}$. In case of post-selection the state of the system collapses onto either $|0\rangle\langle 0|$ or $|1\rangle\langle 1|$. The x and y components of $\boldsymbol{r}$ are completely lost due to the projection, i.e. we are left with

$$\boldsymbol{r'} = (0, 0, r_z) \tag{7.115}$$

which is exactly the phase flip with $p = 1/2$.

The combination of bit and phase flip yields the bit-phase-flip operation with the Kraus operators

$$E_0 = \sqrt{p}\mathbb{1} \tag{7.116}$$
$$E_1 = \sqrt{1-p}\, Y\,. \tag{7.117}$$

We could also define $E_1 := \sqrt{1-p}ZX$, since $ZX = +i\,Y$, where $+i$ would cancel the $-i$ of $E_1^\dagger = -i\,Y$ such that the sequence ZX is equivalent to applying Y. The same obviously holds for XZ.

7.5.2 Depolarising channel

This channel substitutes with probability p the state with the normalized identity $\mathbb{1}/2$, i.e. with the completely mixed state:

$$\mathcal{E}(\rho) = p\mathbb{1}/2 + (1-p)\,\rho = \frac{\mathbb{1} + (1-p)\,\boldsymbol{r}\cdot\boldsymbol{\sigma}}{2}\,. \tag{7.118}$$

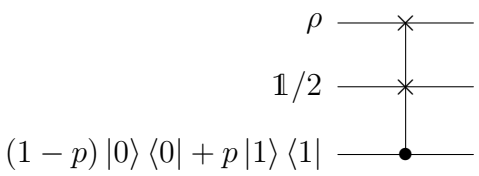
Through this q-operation the Bloch sphere shrinks isotropically ($\boldsymbol{r} \to \boldsymbol{r'} = (1-p)\,\boldsymbol{r}$). We can find an Kraus representation via

$$\frac{\mathbb{1}}{2} = \frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{4} \tag{7.119}$$

for all 2×2 density matrices. This gives

$$\mathcal{E}(\rho) = \left(1 - \frac{3p}{4}\right)\rho + \frac{\rho}{4}\left(X\rho X + Y\rho Y + Z\rho Z\right)\,. \tag{7.120}$$

Using a controlled $SWAP$gate one can obtain a simple representation of the operation as a q-circuit, where the $SWAP$gate exchanges q-bits 1 and 2 if the control



(7.121)

Figure 7.7: Depolarisation channel as q-circuit.

qubit is in state $|1\rangle$, which is the case with probability p for the chosen initial state; otherwise, nothing is done (compare Figure 7.7)

For qudits (i.e. generalizations of the qubit to a system with a Hilbert space $\mathcal{H}$ of dimension $\dim \mathcal{H} = d$), one defines the depolarzing channel accordingly as

$$\mathcal{E}(\rho) = \frac{p\mathbb{1}}{d} + (1-p)\,\rho\,. \tag{7.122}$$

7.6 Master Equations

For given open quantum mechanical system one normally obtains the time-dependent state $\rho(t)$ by e.g. solving a master equation given an initial state (density operator) $\rho(0)$. The most general Markovian, time-homogeneous (also called *convolution-less*) master equation that preserves the periodicity and trace of ρ has the form [28, 29]

$$\dot{\rho}(t) = -\frac{i}{\hbar}\left[H, \rho(t)\right] + \sum_{i=1}^{N^2-1} \gamma_i \left(A_i \rho A_i^\dagger - \frac{1}{2}\rho A_i^\dagger A_i - \frac{1}{2} A_i^\dagger A_i \rho \right), \tag{7.123}$$

where $\gamma_i \geq 0$ and $N = \dim \mathcal{H}$ is the dimension of the Hilbert space that ρ is operating on (i.e. ρ is represented as a $N \times N$ matrix). H is a hermitian matrix consisting of the Hamiltonian of the system and the Lamb-shift caused by the interaction with the system's environment. The dissipative part can also be written as

$$\frac{1}{2}\sum \gamma_i \left(\left[A_i, \rho A_i^\dagger\right] + \text{h.c.} \right). \tag{7.124}$$

The Lindblad operators A_i can be derived from models representing the system and its environment, i.e. $H = H_{\text{sys}} + H_{\text{env}} + H_{\text{int}}$ by assuming [9]

1. an initial state that factorises between system and environment
2. weak coupling

3. Born-Markov approximation

4. rotating wave approximation.

The operators A_i are in general closely related to the system operators in H_{int}.

Example 23 (Spontaneous emission from a two level system)
We take as an example a two level system (atom) with $|0\rangle$ the excited state. It is described by:

$$H_{\text{sys}} = \frac{\hbar\omega}{2}\sigma_z \tag{7.125}$$

$$H_{\text{env}} = \sum_k \frac{\hbar\omega_k}{2} a_k^\dagger a_k \tag{7.126}$$

$$H_{\text{int}}^{(RWA)} = \sum_k \gamma_k \left(\sigma_- a_k^\dagger + \sigma_+ a_k\right) \tag{7.127}$$

The environment consists of a set of harmonic oscillators, where each oscillator represents a mode k of the electromagnetic field, given e.g. by a wave vector $\boldsymbol{k}$ and a polarization. Following the above approximations, one then finds a master equation of the form

$$\dot{\rho}(t) = -\frac{i}{\hbar}\left[H'_{\text{sys}}, \rho\right] + \gamma\left(2\sigma_-\rho\sigma_+ - \sigma_+\sigma_-\rho - \rho\sigma_+\sigma_-\right), \tag{7.128}$$

where H'_{sys} is a modified system hamiltonian, containing the so-called Lamb-shift, which however is often negligible and will be neglected here as well, i.e. we set $H'_{\text{sys}} = H_{\text{sys}}$. Switching to the interaction picture with respect to H'_{sys} (and setting $\hbar = 1$), we obtain

$$\tilde{\rho}(t) \equiv \exp\{iH_{\text{sys}}t\}\,\rho(t)\exp\{-iH_{\text{sys}}t\} \tag{7.129}$$

$$\Rightarrow \dot{\tilde{\rho}} = i\left[H_{\text{sys}}, \tilde{\rho}\right] + \exp\{-iH_{\text{sys}}t\}\,\dot{\rho}\exp\{iH_{\text{sys}}t\} \tag{7.130}$$

$$= i\left[H_{\text{sys}}, \tilde{\rho}\right] - i\left[H_{\text{sys}}, \tilde{\rho}\right] + \gamma\exp\{iH_{\text{sys}}t\}\left(2\sigma_-\rho\sigma_+ - \sigma_+\sigma_- - \rho\sigma_+\sigma_-\right)\exp\{iH_{\text{sys}}t\} \tag{7.131}$$

$$= \gamma\left(2\tilde{\sigma}_-\tilde{\rho}\tilde{\sigma}_+ - \tilde{\sigma}_+\tilde{\sigma}_-\tilde{\rho} - \tilde{\rho}\tilde{\sigma}_+\tilde{\sigma}_-\right). \tag{7.132}$$

We transform all operators by injecting $\mathbb{1} = \exp\{-iH_{\text{sys}}t\}\exp\{iH_{\text{sys}}t\}$ between

any two operators. This gives

$$\tilde{\sigma}_\pm = \exp\{iH_{\rm sys}t\}\,\sigma_\pm \exp\{-iH_{\rm sys}t\} \tag{7.133}$$
$$= \exp\{i\omega t Z/2\}\,\frac{X \pm iY}{2}\exp\{-i\omega t Z/2\} \tag{7.134}$$
$$= \cos\omega t X - \sin\omega t\, Y \pm i\,(\cos\omega t\, Y + \sin\omega t X) \tag{7.135}$$
$$= \frac{1}{2}\left(\exp\{\pm i\omega t\}\,X \pm i\exp\{\pm i\omega t\}\;Y\right) \tag{7.136}$$
$$= \exp\{\pm i\omega t\}\,\sigma_\pm\,, \tag{7.137}$$

all in all resulting in

$$\dot{\tilde{\rho}} = \gamma\left(2\sigma_-\tilde{\rho}\sigma_+ - \sigma_+\sigma_-\tilde{\rho} - \tilde{\rho}\sigma_+\sigma_-\right)\,. \tag{7.138}$$

By representing ρ with the Bloch vector $\boldsymbol{r}$,

$$\tilde{\rho} = \frac{\mathbb{1} + \boldsymbol{r}\cdot\boldsymbol{\sigma}}{2}\,, \tag{7.139}$$

we obtain the following differential equations for $\boldsymbol{r}$:

$$\dot{r}_\pm = -\gamma r_\pm \tag{7.140}$$
$$\dot{r}_z = -2\gamma\,(r_z + 1)\,, \tag{7.141}$$

where $r_\pm = r_x \pm i r_y$. The solution is easily found,

$$r_x(t) = r_x(0)\exp\{-\gamma t\} \tag{7.142}$$
$$r_y(t) = r_y(0)\exp\{-\gamma t\} \tag{7.143}$$
$$r_z(t) = r_z(0)\exp\{-2\gamma t\} - 1 + \exp\{-2\gamma t\}\,. \tag{7.144}$$

By defining $\sqrt{1-\lambda} := \exp\{-\gamma t\} \Rightarrow 1-\lambda = \pm\exp\{-2\gamma t\}$ we get

$$\boldsymbol{r'} = \begin{pmatrix}\sqrt{1-\lambda}\,r_x\\ \sqrt{1-\lambda}\,r_y\\ (1-\lambda)r_z\end{pmatrix} + \begin{pmatrix}0\\0\\-\lambda\end{pmatrix}\,. \tag{7.145}$$

This is a realization of an "amplitude damping channel". The Bloch sphere shrinks non-uniformly (more in the $z-$direction), and moves towards the south pole $|1\rangle$. Hence, this is a non-unital channel. By exchanging $|0\rangle \leftrightarrow |1\rangle$ (making $|0\rangle$ the groundstate) the Kraus operators are given by

$$E_0(t) = \begin{pmatrix}\sqrt{1-\lambda} & 0\\ 0 & 1\end{pmatrix} \tag{7.146}$$
$$E_1(t) = \begin{pmatrix}0 & 0\\ \sqrt{\lambda} & 0\end{pmatrix}\,, \tag{7.147}$$

where we must remember the time-dependence of λ. More generally, as the propagation by a Lindblad master equation is a valid quantum process, it is clear that the state $\rho(t)$ at any time can be represented in Kraus form,

$$\rho(t) = \sum_k E_k(t)\rho(0)E_k^\dagger(t)\,, \tag{7.148}$$

where, however, the Kraus operators typically depend on time and can be found only after solving the master equation.

8 Quantum Error Correction

How many degrees of freedom does a qubit represent? 2 analogue degrees of freedom? This question is decisive, since error correction is hard to implement for analogue systems.

We will find that it is sufficient to correct "digital" errors, leading to powerful error correction similar to that of classical digital information processing systems. Nevertheless, the required generalization of classical error correction is very non trivial: Phase, no-cloning theorem, and the collapse of the wave function have to be taken into account.

8.1 Classical Error Correction

The central idea is to use redundancy

$$0 \to 000 \tag{8.1}$$
$$1 \to 111. \tag{8.2}$$

Let p be the probability of a single bit flip. The probabilities of transition between different bit values is then given by a so called *binary symmetrical channel* (Figure 8.1):

If we encode the information in three bits instead of one and use a majority vote (the information represented by the bits is the information stored in 2 of the 3 bits),

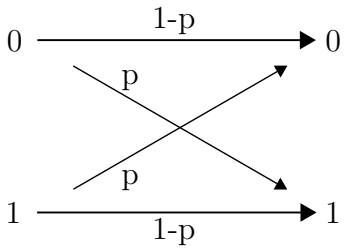


Figure 8.1: Binary symmetrical channel for one bit and a bit flip probability of p.

then we can not detect an error if at least 2 of the 3 bits undergo a bit flip. The probability of this process is

$$\underbrace{3}_{=\binom{3}{2}} \cdot \underbrace{p^2\,(1-p)}_{\text{exactly 2 flips}} + \underbrace{p^3}_{\text{3 bit flips}} = 3p^2 - 2p^3 \tag{8.3}$$

The probability of this process is smaller then p if the single bit flip probability is $p < 1/2$. The error probability is thus reduced for small p from p to $\sim p^2$. This code is called *repetition code* (dt. *Wiederholungscode*).

8.2 Three qubit bit-flip code

A direct transfer of this approach to qubits like

$$|\psi\rangle \to |\psi\rangle\,|\psi\rangle\,|\psi\rangle \tag{8.4}$$

is not possible due to the no-cloning restriction.

We can, however, clone computational basis states

$$\underbrace{|0\rangle}_{\text{logical qubits}} \to \underbrace{|0\rangle\,|0\rangle\,|0\rangle}_{\text{physical qubits}} \equiv |0\rangle_L \quad \text{and} \quad |1\rangle \to |1\rangle\,|1\rangle\,|1\rangle \equiv |1\rangle_L\,. \tag{8.5}$$

This cloning of the computational basis states can be achieved by the q-circuit in Figure 8.2 :

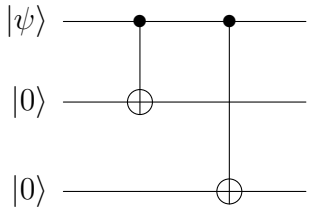


Figure 8.2

There exists a second problem not present in the classical case: *How to determine if a bit flip has taken place without collapsing the state of the system?*

Let $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. The 3-qubit flip code introduced above transforms $|\psi\rangle$ into

$$|\psi\rangle \mapsto a\,|000\rangle + b\,|111\rangle \tag{8.6}$$

As an example, this can become $a\,|100\rangle + b\,|011\rangle$ by a bit flip on the first qubit. We can not simply measure the first qubit (using $\sigma_z^{(1)}$) and determine if the qubit was flipped at a certain point in time. Measuring the qubit would collapse the state to $|000\rangle$ or $|111\rangle$ and lead to a loss of the phase and amplitude information contained in the state.

A solution to this problem exists in the form of global measurements and subsequent corrections. The solution allows to detect single qubit flips, to localise them and completely repair them. Consider the following four projectors

$$P_0 := |000\rangle\langle 000| + |111\rangle\langle 111| \tag{8.7}$$
$$P_1 := |100\rangle\langle 100| + |011\rangle\langle 011| \tag{8.8}$$
$$P_2 := |010\rangle\langle 010| + |101\rangle\langle 101| \tag{8.9}$$
$$P_3 := |001\rangle\langle 001| + |110\rangle\langle 110| \ . \tag{8.10}$$

These projectors are projections into orthogonal two dimensional subspaces, i.e. $P_i P_j = \delta_{ij} P_i$. For example

$$P_0^2 = |000\rangle\langle 000| + \underbrace{|000\rangle\langle 000|111\rangle\langle 111| + |111\rangle\langle 111|000\rangle\langle 000|}_{=0} + |111\rangle\langle 111| = P_0 \tag{8.11}$$

In the original state $|\psi\rangle$ we find

$$\langle\psi|P_0|\psi\rangle = |a|^2 + |b|^2 = 1 \tag{8.12}$$

whereas

$$\langle\psi|P_i|\psi\rangle = 0 \qquad i = 1, 2, 3. \tag{8.13}$$

On the other hand, in case of a bit flip, the projector yielding a non-zero result is the projector corresponding to the flipped qubit, while all the remaining projectors again yield zero as a result. Measuring all four projectors thus tells us, if a bit flip has happened and if so which qubit was flipped. If none of the four projectors triggers, then two qubits must have flipped. In case of three qubit flips the result obtained from the projectors is again $\langle P_0\rangle = 1$ and $\langle P_i\rangle = 0, i = 1, 2, 3$. Obviously we require again that the probability p of a bit flip to be small.

The step of measuring the different projectors P_i is called *error detection* or *syndrom diagnosis*. The result of these measurements is called *error syndrome*.

We can also see that a state for which at maximum one bit was flipped stays unchanged. This fact is obvious for the "right" P_i (i.e. the one yielding a positive result "1"), e.g.

$$P_0\,|\psi\rangle = (|000\rangle\langle 000| + |111\rangle\langle 111|)\,(a\,|000\rangle + b\,|111\rangle) = |\psi\rangle \tag{8.14}$$

If the projector yields a negative result ("0") the state is projected into an orthogonal subspace, i.e. $\mathbb{1} - \mathrm{P}_j$. This subspace completely contains $|\psi\rangle$ (per definition of the result "0") and thus the state is left unaffected. No information is obtained regarding a or b, meaning the q-information is left untouched.

The error syndrome tells us, which qubit was flipped. The error now has to be corrected, we can flip the affected qubit back independently from the other qubits by applying $X = \sigma_x$. The complete approach is thus as follows:

$$P_i = 1 \rightarrow \begin{cases} \text{do nothing} & i = 0 \\ \text{apply } X_i & i \in \{1, 2, 3\} \end{cases} \tag{8.15}$$

This solves the problem of a bit flip. The analysis for the probability of success is the same as in the classical case, i.e. this error correction code improves the success probability in case for qubit flip probabilities $p < 1/2$.

An equivalent measurement is achieved by measuring $Z_1 Z_2$ and $Z_2 Z_3$ which compares two qubits (qubit 1 and 2 or qubit 2 and 3): If $q_1 = q_2$, where $q_i \in \{0, 1\}$ represents the state of the qubit i, then $Z_1 Z_2$ yields 1, otherwise it yields -1. The same holds for $Z_2 Z_3$, the possible combinations and error syndromes are shown in Table 8.1.

Note

Measuring the error syndrome $Z_1 Z_2$ is a *global* measurement, not a measurement of Z_1 and then Z_2. The latter measurements would destroy the state, as we have seen! Indeed, $Z_1 Z_2$ is a *single* measurement, namely of the hermitian operator $Z \otimes Z \otimes \mathbb{1}_2$. The possible outcomes are ± 1, each one corresponding to a 4D degenerate subspace with either both first two qubits in the same state (outcome +1), or in the opposite state (outcome -1).

8.3 Three qubit phase flip code

Until now we have been able to protect the qubits against bit flips occurring with a small probability of error p_F, reducing the probability of an undetected error from $\mathcal{O}(p_F)$ to $\mathcal{O}(p_F^2)$. As we will see later, it is possible to reduce p_F to an arbitrarily small value by concatenation at the cost of a *polylogarithmical overhead* (as long as the initial $p_F < p_c \sim 10^{-2}$ to 10^{-4}, depending on the physical architecture).

Z_1Z_2	Z_2Z_3	error syndrome
1	1	no flips
1	-1	qubit 3 flipped
-1	1	qubit 1 flipped
-1	-1	qubit 2 flipped

Table 8.1: Possible error syndromes of a three qubit logical qubit when measuring Z_iZ_j and assuming one simultaneous flip at maximum.

Bit-flips, however, are only one type of possible errors. How do we cope with errors involving a phase flip? That is with a probability of p,

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \mapsto\ |\psi'\rangle = a\,|0\rangle - b\,|1\rangle\,. \tag{8.16}$$

We reduce the phase flip error to a bit flip error by changing the basis states to

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \tag{8.17}$$

or inversely

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \tag{8.18}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}. \tag{8.19}$$

The initial state $|\psi\rangle$ can be written as

$$|\psi\rangle = \frac{a+b}{\sqrt{2}}\,|+\rangle + \frac{a-b}{\sqrt{2}}\,|-\rangle \tag{8.20}$$

which changes after the phase flip (in the old basis) to (in the new basis)

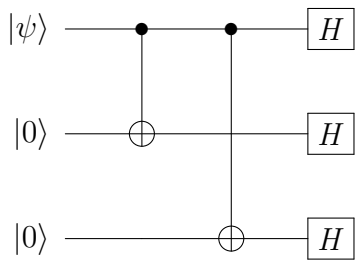
$$|\psi'\rangle = \frac{a-b}{\sqrt{2}}\,|+\rangle + \frac{a+b}{\sqrt{2}}\,|-\rangle \tag{8.21}$$

i.e. the phase flip results in a swap of $|+\rangle \leftrightarrow |-\rangle$.

(8.22)

Coding the state in the 3 qubit phase flip code leads to

$$|\psi\rangle \mapsto a\,|+++\rangle + b\,|---\rangle\ . \tag{8.23}$$



(8.24)

Figure 8.3: Encoding of a logical qubit as three physical qubits to protect against phase flips.

This allows us to use everything we have learned so far about bit flips for correcting phase flips. We only have to change to the basis $|\pm\rangle$. Encoding the logical qubits thus requires some additional Hadamard gates (Figure 8.3): The error syndrome is then determined in the $|\pm\rangle$ basis by measuring Z_1Z_2 and Z_2Z_3 conjugated with Hadamard gates:

$$H^{\otimes 3} Z_1 Z_2 H^{\otimes 3} = X_1 X_2 \tag{8.25}$$
$$H^{\otimes 3} Z_2 Z_3 H^{\otimes 3} = X_2 X_3. \tag{8.26}$$

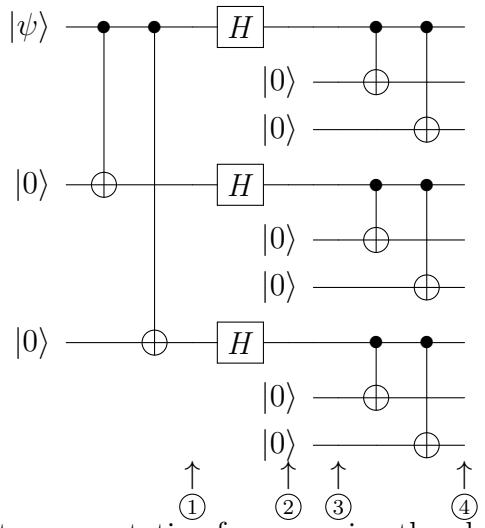
Indeed, since $X|\pm\rangle = \pm|\pm\rangle$, X plays exactly the same role in the $|\pm\rangle$ basis as Z in the computational basis. If a phase flip in the computational basis happens in say the 1st qubit, the coded state from eq.(8.23) is mapped to

$$a|-++\rangle + b|+--\rangle \ . \tag{8.27}$$

The error can be detected by measuring X_1X_2 and X_2X_3 as described and corrected by applying X_1 in the $|\pm\rangle$ basis (equivalently applying Z_1 in the computational basis). This completes the actions required to protect against phase flips. But what about protection against simultaneous phase and bit flips or any other arbitrary error?

8.4 Shor Code

The *Shor code* [36] is a concatenation of the phase flip code followed by the bit flip code. Logical qubits are thus represented by the following physical



(8.30)

Figure 8.4: Circuit representation for preparing the physical qubits required by a logical qubit in the Shor code.

qubits

$$|0\rangle \mapsto |0\rangle_L \equiv \frac{1}{2\sqrt{2}} \left(|000\rangle + |111\rangle\right) \left(|000\rangle + |111\rangle\right) \left(|000\rangle + |111\rangle\right) \tag{8.28}$$

$$|1\rangle \mapsto |1\rangle_L \equiv \frac{1}{2\sqrt{2}} \left(|000\rangle - |111\rangle\right) \left(|000\rangle - |111\rangle\right) \left(|000\rangle - |111\rangle\right) \tag{8.29}$$

The preparation of such states can be achieved by the q-circuit in Figure 8.4. Starting with

$$|\psi\rangle = |0\rangle \tag{8.31}$$

the circuit produces

$$|\psi_{①}\rangle = |000\rangle \tag{8.32}$$

$$|\psi_{②}\rangle = |+++\rangle = \frac{1}{2\sqrt{2}} \left(|0\rangle + |1\rangle\right)^{\otimes 3} \tag{8.33}$$

$$|\psi_{③}\rangle = \left(|+\rangle\,|00\rangle\right)^{\otimes 3} \tag{8.34}$$

$$|\psi_{④}\rangle = \left[\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right]^{\otimes 3} \tag{8.35}$$

similarly the circuit yields for $|\psi\rangle = |1\rangle$:

$$|\psi_{④}\rangle = \left[\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right]^{\otimes 3} \tag{8.36}$$

8.4.1 Protection against Bit Flips

Detection is achieved in a similar manner to the approach from before by measurement of

$$Z_1 Z_2 \text{ and } Z_2 Z_3 \quad \text{for detection of bit flips in the first 3 qubits} \tag{8.37}$$
$$Z_4 Z_5 \text{ and } Z_5 Z_6 \quad \text{for detection of bit flips in the second 3 qubits} \tag{8.38}$$
$$Z_7 Z_8 \text{ and } Z_8 Z_9 \quad \text{for detection of bit flips in the third 3 qubits} \tag{8.39}$$

8.4.2 Protection against Phase Flips

If a phase flip happens on one of the first three qubits (i.e. $|1\rangle \to -|1\rangle$), the phase flip leads to

$$|000\rangle + |111\rangle \to |000\rangle - |111\rangle \,. \tag{8.40}$$

So a phase flip in one of the first three qubits is also a phase flip in the first logical qubit of the 3-qubit bit flip code, $(|0\rangle_L, |1\rangle_L) \equiv (|000\rangle, |111\rangle)$. Detection of the phase flip is possible by comparing the sign of the first and the second two blocks, which is realised by measuring

$$\bigotimes_{i=1}^{6} X_i \qquad \text{and} \qquad \bigotimes_{i=4}^{9} X_i. \tag{8.41}$$

The operator $\otimes_{i=1}^{3} X_i$ has the eigenvalues ± 1 and eigenstates for the subspace associated with the eigenvalue $+1$ are

$$|+\rangle^{\otimes 3} = |+\rangle\,|+\rangle\,|+\rangle \propto (|000\rangle + |111\rangle + \ldots)\,, \tag{8.42}$$

and for the subspace associated with eigenvalue -1:

$$|-\rangle\,|+\rangle\,|+\rangle \propto (|000\rangle - |111\rangle \pm \ldots) \tag{8.43}$$
$$|+\rangle\,|-\rangle\,|+\rangle \propto (|000\rangle - |111\rangle \pm \ldots) \tag{8.44}$$
$$|+\rangle\,|+\rangle\,|-\rangle \propto (|000\rangle - |111\rangle \pm \ldots) \tag{8.45}$$

as well as others representing more than one phase flip. Based on this, the operator $\otimes_{i=1}^{6} X_i$ also has eigenvalues ± 1. An eigenstate for the $+1$ subspace is

$$|+\rangle^{\otimes 3}\,|+\rangle^{\otimes 3} \propto (|000\rangle + |111\rangle + \ldots)\,(|000\rangle + |111\rangle + \ldots)\,, \tag{8.46}$$

and for the -1 eigenvalue subspace

$$(|-\rangle |+\rangle |+\rangle) |+\rangle^{\otimes 3} \propto (|000\rangle - |111\rangle + \ldots) (|000\rangle + |111\rangle + \ldots) \tag{8.47}$$

$$\ldots \text{ (and 5 more combinations containing } |-\rangle) \tag{8.48}$$

All non-listed states have at least 2 or more phase flips and are thus neglected.

If the measurement of $\otimes_{i=1}^{6} X_i$ yields $+1$, then no (or at least 2) phase flips happened on the first 6 qubits.
If the measurement yields -1, then a phase flip happened in one of the first two blocks of three qubits. An analogous conclusion holds for $\otimes_{i=4}^{9} X_i$, providing us in combination with the information, in which of the three blocks the phase flip has happened.

For correction of the phase flip: If the phase flip was detected to have happened in the first block, then apply one of the gates Z_1, Z_2, Z_3 swapping the states

$$(|000\rangle + |111\rangle) \leftrightarrow (|000\rangle - |111\rangle) . \tag{8.49}$$

An analogous approach can be used for correcting phase flips in any of the other two blocks.

8.4.3 Simultaneous Bit and Phase Flips

If a bit and phase flip happen simultaneously on the first qubit, e.g. $Z_1 X_1$ on the state $|\psi\rangle$, we are left with the state

$$a (|100\rangle - |011\rangle) (|000\rangle + |111\rangle)^{\otimes 2} + b (|100\rangle + |011\rangle) (|000\rangle - |111\rangle)^{\otimes 2} . \tag{8.50}$$

The measurement of the bit flip error syndrome first detects the bit flip on the first qubit and allows for correction. This reduces the problem to a phase flip problem in the first block. This type of problem can easily be detected, localised and corrected with the described phase-flip error correction procedure.

8.4.4 Protection against Any Single Quantum Bit Error

The Shor code even protects against *any* single qubit error. Single qubit errors can be for example small unitary rotations or even the substitution of a qubit by a fully mixed qubit, i.e. a qubit in state $\mathbb{1}_2/2$.

Consider a q-channel for the jth qubit, $j = 1, \ldots, 9$:

$$\mathcal{E}^{(j)} (|\psi\rangle \langle\psi|) = \sum_i E_i^{(j)} |\psi\rangle \langle\psi| E_i^{(j)\dagger} . \tag{8.51}$$

We can represent each $E_i^{(j)}$ in the Pauli basis as

$$E_i^{(j)} = e_{i0}^{(j)} \mathbb{1}^{(j)} + e_{i1}^{(j)} X^{(j)} + e_{i2}^{(j)} Y^{(j)} + e_{i3}^{(j)} Z^{(j)}. \tag{8.52}$$

However, we also remember $Y^{(j)} = +iX^{(j)}Z^{(j)}$. This means that any perturbed state is a mixture of states with different single qubit errors. (To be precise: In order to obtain that mixture one also has to diagonalise again, but this is done in the subspaces of these 1-error states, so that in these subspaces there is still a maximum of only one error, and the eigenstates are superpositions of these *single qubit error states*). Each of these eigenstates exists with a certain probability. Measuring the error syndromes of a superposition projects the state into a subspace in which it exhibits the corresponding error. This error can then be corrected. In a certain way the measurement thus amplifies (or concentrates) the error but also leads to a new pure state which can then be transferred back into its original state.

8.5 General Theory of Quantum Error Correction

While the Shor code does its job, it requires 9 qubits to code 1 logical qubit, which is a lot. Is there a more efficient q-error correction? Can the full syndrome-measurement & correction procedure be simplified?

To be able to answer these questions, we need a general theory.

Definition 12
We introduce the following definitions:

- *The subspace $\mathcal{C}$ of Hilbert space $\mathcal{H}$in which the states to be protected are coded is called the (quantum) code $\mathcal{C}$.*
- *The projector P projects onto this code $\mathcal{C}$. E.g. for the 3-qubit bit flip code, $P = |000\rangle\langle 000| + |111\rangle\langle 111|$. In general $P = \sum_i |i\rangle_L \langle i|$, where $|i\rangle_L$ denotes the logical (multiple physical qubits) states.*
- *Interaction with the environment (noise) is given by a q-operation $\mathcal{E}$. This q-operation is completely positive, but not necessarily trace preserving (like e.g. a measurement with post-selection but without renormalization of the state).*
- *The error correction or correction procedure is another q-operation $\mathcal{R}$ which is completely positive and trace preserving, i.e. one should always be able to apply the correction procedure. The correction procedure combines the*

previously separate syndrome measurement and error correction into a single operation.

- *For a q-error correction to be successful, we require*

$$(\mathcal{R} \circ \mathcal{E})(\rho) \propto \rho \qquad \forall \rho \in \mathcal{C}, \tag{8.53}$$

where we only require "$\propto$" instead of "$=$" since $\mathcal{E}$ is not necessarily trace preserving.

Theorem 19 (Conditions for Quantum Error Correction)
Let $\mathcal{C}$ be a code and P the projector onto $\mathcal{C}$. Let $\mathcal{E}$ be a q-operation with Kraus operators $\{E_i\}$.

There exists a q-error correction $\mathcal{R}$, correcting $\mathcal{E}$ to $\mathcal{C}$, if and only if

$$P E_i^\dagger E_j P = \alpha_{ij} P \tag{8.54}$$

where α_{ij} represents a set of complex numbers constituting a hermitian matrix.

We call the operators E_i errors; if $\mathcal{R}$ exists, we call them " correctable errors ".

For proofing this theorem we first need to introduce the polar decomposition.

Theorem 20 (Polar Decomposition)
Let A be a linear operator on a vector space V. There exist unitary operators U and positive operators J, K so that

$$A = UJ = KU, \tag{8.55}$$

where J and K are uniquely defined through $J := \sqrt{A^\dagger A}$ and $K := \sqrt{AA^\dagger}$.

If A is invertible, then U is unique.

Proof.

$J := \sqrt{A^\dagger A}$ defines a positive hermitian operator, since

$$A^\dagger A \geq 0 \tag{8.56}$$

and

$$A^\dagger A = \left(A^\dagger A\right)^\dagger \tag{8.57}$$

thus

$$A^\dagger A = \sum_i \lambda_i^2 \left|i\right\rangle \left\langle i\right| \qquad \lambda_i^2 \geq 0 \tag{8.58}$$

which means for the square root

$$J = \sqrt{A^\dagger A} = \sum_i \lambda_i \left|i\right\rangle \left\langle i\right| \qquad \lambda_i \geq 0. \tag{8.59}$$

Now define

$$\left|\psi_i\right\rangle := A \left|i\right\rangle \tag{8.60}$$

such that

$$\langle\psi_i|\psi_i\rangle = \langle i|A^\dagger A|i\rangle = \lambda_i^2 \tag{8.61}$$

For $\lambda_i \neq 0$ define

$$\left|e_i\right\rangle := \frac{\left|\psi_i\right\rangle}{\lambda_i} \tag{8.62}$$

such that

$$\langle e_i|e_i\rangle = 1 \tag{8.63}$$

and

$$\langle e_i|e_j\rangle = 0 \,\forall\, i \neq j \tag{8.64}$$

as

$$\langle e_i|e_j\rangle = \frac{1}{\lambda_i\lambda_j} \langle i|A^\dagger A|j\rangle = \delta_{ij}. \tag{8.65}$$

For $\lambda_i = 0$ use the Gram-Schmidt method to extend the set $\{|e_i\rangle\}_{i,\lambda_i\neq 0}$ to obtain a full normalised orthogonal system of $\{e_i\}_i$.

Now define $U := \sum_i \left|e_i\right\rangle \left\langle i\right|$. For $\lambda_i \neq 0$ this leads to

$$UJ \left|i\right\rangle = U\lambda_i \left|i\right\rangle \tag{8.66}$$

$$= \lambda_i \left|e_i\right\rangle = \left|\psi_i\right\rangle = A \left|i\right\rangle . \tag{8.67}$$

But also for $\lambda_i = 0$

$$UJ \left|i\right\rangle = U\lambda_i \left|i\right\rangle \tag{8.68}$$

$$\Rightarrow = 0 = A \left|i\right\rangle . \tag{8.69}$$

Therefore

$$A \left|i\right\rangle = UJ \left|i\right\rangle \qquad \forall i, \tag{8.70}$$

$$A = UJ. \tag{8.71}$$

Since $A^\dagger A \geq 0$, we have that $J = \sqrt{A^\dagger A}$ is unique. If A is invertible, then $\forall\, |y\rangle \in V\ \exists\ |x\rangle$ so that

$$A\,|x\rangle = |y\rangle\,. \tag{8.72}$$

Then $\langle y| = \langle x|\, A^\dagger$. Therefore there exists a $\langle x|$ for all $\langle y|$ so that $\langle y| = \langle x|\, A^\dagger$. This means a $\left(A^\dagger\right)^{-1}$ exists and also

$$\left(A^\dagger A\right)^{-1} = A^{-1}\left(A^\dagger\right)^{-1} \tag{8.73}$$

so $A^\dagger A$ is invertible and therefore $\lambda_i \neq 0\ \forall\ i$, implying in fact $J > 0$ (i.e. J is strictly positive definite in this case). Then J^{-1} exists and U is determined uniquely from $U \equiv AJ^{-1}$.

The right polar decomposition is obtained from

$$A = UJ = UJU^\dagger U = KU \tag{8.74}$$

where

$$K = UJU^\dagger \geq 0 \tag{8.75}$$

as $J \geq 0$. From this we obtain the decomposition

$$AA^\dagger = KUU^\dagger K = K^2 \Rightarrow K = \sqrt{AA^\dagger}. \tag{8.76}$$

□

Proof (Conditions for Quantum Error Correction).

⇒:

We explicitly construct a q-error correction consisting of the syndrome measurement and the correction procedure.

Let $\{E_i\}$ be Kraus operators satisfying Equation (8.54), $\alpha = \{a_{ij}\}$ a hermitian matrix. Let U diagonalize α, i.e. $d = U^\dagger \alpha U$, where $U^\dagger U = \mathbb{1}$ is unitary and d is diagonal and real. Define

$$F_k := \sum_i U_{ik} E_i. \tag{8.77}$$

Then the $\{F_k\}$ define the same q-operation as the $\{E_k\}$ (see theorem 16), i.e.

$$\mathcal{E}(\rho) = \sum_k F_k \rho F_k^\dagger \tag{8.78}$$

$$PF_k^\dagger F_l P = \sum_{i,j} U_{ki}^\dagger U_{jl} P E_i^\dagger E_j P \tag{8.79}$$

$$\overset{(8.54)}{=} \sum_{i,j} U_{ki}^\dagger \alpha_{ij} U_{jl} P \tag{8.80}$$

$$= d_{kl} P = \delta_{kl} d_{kk} P\,. \tag{8.81}$$

This is a simplified version of the condition (8.54) and differentiates errors by different orthogonal vectors.

Polar decomposition of $F_k P$ yields

$$F_k P = U_k \sqrt{P F_k^\dagger F_k P} = \sqrt{d_{kk}} U_k P, \tag{8.82}$$

where $U_k^\dagger U_k = \mathbb{1}$ is unitary. This decomposition can be interpreted such that the operators F_k rotate the code $\mathcal{C}$ onto a new subspace defined by the projector

$$P_k := U_k P U_k^\dagger = \frac{F_k P U_k^\dagger}{\sqrt{d_{kk}}} \tag{8.83}$$

Following the condition in (8.81) these subspaces are orthogonal:

$$P_l P_k = P_l^\dagger P_k \tag{8.84}$$

$$= \frac{U_l P F_l^\dagger F_k P U_k^\dagger}{\sqrt{d_{ll} d_{kk}}} = \delta_{lk} \frac{d_{kk}}{\sqrt{d_{ll} d_{kk}}} U_k P U_k^\dagger \tag{8.85}$$

$$= \delta_{lk} P_k. \tag{8.86}$$

We now define the syndrome measurement as a projective measurement using the P_k and - if needed - complemented by additional orthogonal projectors in order to fulfil the completeness relation $\sum_k P_k = \mathbb{1}$.

The correction itself is achieved by applying $U_k^\dagger$, i.e. if projector P_k - triggered by rotating back the subspaces. The full procedure (detection and correction) thus reads

$$\mathcal{R}(\sigma) = \sum_k U_k^\dagger P_k \sigma P_k U_k. \tag{8.87}$$

For all $\rho \in \mathcal{C}$ the following holds:

$$U_k^\dagger P_k F_l \sqrt{\rho} = U_k^\dagger P_k^\dagger F_l P \sqrt{\rho} \tag{8.88}$$

where we use $P\sqrt{\rho} = \sqrt{\rho}$, which is true because ρ is in $\mathcal{C}$ and thus also $\sqrt{\rho} \in \mathcal{C}$. Substituting $P_k^\dagger = P_k$ results in

$$\overset{(8.83)}{=} U_k^\dagger \frac{\overbrace{U_k P F_k^\dagger}^{=P_k^\dagger}}{\sqrt{d_{kk}}} F_l P\sqrt{\rho} \tag{8.89}$$

$$= \mathbb{1} \cdot P \frac{d_{kl}\delta_{kl}}{\sqrt{d_{kk}}} P\sqrt{\rho} \tag{8.90}$$

$$= \delta_{kl}\sqrt{d_{kk}} P\sqrt{\rho} \tag{8.91}$$

The correction procedure hence performs as

$$\mathcal{R}\left(\mathcal{E}(\rho)\right) \overset{(8.78\,,\,8.87)}{=} \sum_{kl} U_k^\dagger P_k F_l \rho F_l^\dagger P_k U_k \tag{8.92}$$

$$\overset{(8.91)}{=} \sum_{kl} \delta_{kl} d_{kk} \underbrace{P\rho P}_{=\rho} \tag{8.93}$$

$$= \sum_{kl} \delta_{kl} d_{kk} \rho \tag{8.94}$$

$$= \left(\sum_k d_{kk}\right) \rho \quad \propto \ \rho \tag{8.95}$$

⇐:

Now we assume that we can fully correct the errors $\{E_i\}$ using the recovery q-operation $\mathcal{R}$ with operator elements $\{R_j\}$. We define

$$\mathcal{E}_c\left(\rho\right) := \mathcal{E}\left(P\rho P\right). \tag{8.96}$$

Since $P\rho P \in \mathcal{C}\,\forall\,\rho$, the recovered result is proportional to the argument of the noise q-channel, $\mathcal{R}\left(\mathcal{E}_c\left(\rho\right)\right) \propto P\rho P$, as $\mathcal{R}$ also must be able to correct $\mathcal{E}_c(\rho)\forall\rho$. The constant of proportionality must be independent of ρ due to linearity of the q-channels. Therefore

$$\mathcal{R}\left(\mathcal{E}_c\left(\rho\right)\right) = \sum_{i,j} R_j E_i P \rho P E_i^\dagger R_j^\dagger \tag{8.97}$$

$$= cP\rho P \qquad \forall\rho \tag{8.98}$$

because of the projection onto $\mathcal{C}$ from the right and the left. As we can see, we can reduce the q-operations involving the operator elements $\{R_j E_i P\}$ to a single q-operation involving a single operator element, namely $\sqrt{c}P$. The freedom of unitary in the operator elements implies

$$R_k E_i P = c_{ki} P \tag{8.99}$$

where $c_{ki} \in \mathbb{C}$ (or to be more precise: k, i denote doubled indices, i.e. $c_{ki} \equiv c_{ki,1}$). Taking the hermitian conjugate we find

$$PE_i^\dagger R_k^\dagger = c_{ki}^* P \tag{8.100}$$

$$\Rightarrow PE_i^\dagger R_k^\dagger R_k E_j P = c_{ki}^* c_{kj} P \tag{8.101}$$

Since $\mathcal{R}$ is trace preserving, $\sum_i R_i^\dagger R_i = \mathbb{1}$. Hence,

$$\sum_k PE_i^\dagger R_k^\dagger R_k E_j P = PE_i^\dagger E_j P = \alpha_{ij} P \tag{8.102}$$

where

$$\alpha_{ij} = \sum_k c_{ki}^* c_{kj} = \alpha_{ji}^*. \tag{8.103}$$

□

Theorem 21 (Discretisation of errors)
Let $\mathcal{C}$ be a q-code and $\mathcal{R}$ be the q-error correction procedure from the proof of Theorem 1 for errors given by operator elements $\{E_i\}$. Let $\mathcal{F}$ be a q-operation with errors $\{F_j\}$, which are linear combinations of the mentioned errors E_i, i.e.

$$F_j = \sum_i m_{ji} E_i \qquad , m_{ji} \in \mathbb{C}. \tag{8.104}$$

Then $\mathcal{R}$ also corrects errors from $\mathcal{F}$.

Proof.

The set of errors $\{E_i\}$ must fulfil the q-error correction condition, i.e.

$$PE_i E_j^\dagger \mathrm{P} = \alpha_{ij} P \tag{8.105}$$

As shown in the previous proof (eq. (8.81)), we can choose $\alpha_{ij} = d_{ij} = \delta_{ij} d_{ii}$ diagonal. $\mathcal{R}$ is represented by the operator elements $U_k^\dagger P_k$, where for all $\rho \in \mathcal{C}$ the following is valid

$$U_k^\dagger P_k E_i \sqrt{\rho} = \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho}. \tag{8.106}$$

From

$$F_j = \sum_i m_{ji} E_i \tag{8.107}$$

follows

$$U_k^\dagger P_k F_j \sqrt{\rho} = \sum_i m_{ji} \delta_{ki} \sqrt{d_{kk}} \sqrt{\rho} \tag{8.108}$$

$$= m_{jk} \sqrt{d_{kk}} \sqrt{\rho}\,. \tag{8.109}$$

The error correction applied to the q-operation $\mathcal{F}$ thus evaluates to

$$\mathcal{R}\left(\mathcal{F}\left(\rho\right)\right) = \sum U_k^\dagger P_k F_j \rho F_j^\dagger P_k U_k \tag{8.110}$$

$$= \sum_{jk} \left|m_{jk}\right|^2 d_{kk} \rho \qquad \propto \rho \tag{8.111}$$

Therefore, $\mathcal{R}$ also corrects errors from $\mathcal{F}$.

(8.112)

□

As we can see it is sufficient to to be able to correct a set of discrete errors $\{E_i\}$ to be able to correct any linear combination of these errors. In particular it follows that if we can protect a qubit against X, Y and Z errors, then we can protect it using the same code against any other arbitrary error!

8.6 Quantum Hamming Bound

In Shor's code we needed 9 qubits to encode 1 qubit, which seems relatively expensive. Does a cheaper solution with less qubits exist?

Generally speaking, the problem reads as follows: Encode k logical qubits into n physical qubits in a such way which allows the code to recover from errors on any subset of t or less qubits. We assume the code to be a non-degenerate code, i.e. different errors result in different states. (An example for a degenerate code would be Shor's code, where e.g. Z_1 and Z_2 errors would result in the same states: $|000\rangle + |111\rangle \xmapsto{Z_1 \text{or} Z_2} |000\rangle - |111\rangle$ of the first block). There exist $\binom{n}{j}$ combinations on how to distribute exactly j errors onto n qubits. Every error on a qubit can either be a X, Y or Z error. In total the number of possible errors on t or less qubits is therefore

$$n_F = \sum_{j=0}^{t} \binom{n}{j} 3^j \tag{8.113}$$

The case of $j = 0$, which represents "no error", also somehow has to be encoded and is therefore included. Every error has to correspond to it's own 2^k dimensional orthogonal subspace, in order to be able to code all k logical qubits in a non-degenerate way. All of these orthogonal subspaces have to fit into the 2^n dimensional space representing the n physical qubits, i.e.

$$2^k \cdot \sum_{j=0}^{t} \binom{n}{j} 3^j \leq 2^n \tag{8.114}$$

This relation is called the *quantum Hamming bound*. This bound may be improved by using degenerate codes, for which

$$n \leq 4t + k \tag{8.115}$$

the so called *quantum singelton bound* is relevant.

Example 24
1 logical qubit encoded as n physical qubits in a way which allows for correction from one error, i.e. $k = 1$, $t = 1$. *The q-Hamming bound becomes*

$$2\,(1 + 3n) \leq 2^n \tag{8.116}$$

We therefore need a minimum of $n = 5$ *(check:* $2 \cdot (1 + 15) = 2^5 = 32$*) qubits. If we were to use a degenerate code, i.e. the q-singelton bound would apply, then we would nevertheless obtain* $n = 5$.

8.7 Construction of Quantum Codes

Extensive knowledge regarding classical codes exists. As we will see, this knowledge will help us to construct q-codes, especially *CSS* (Calderbank-Shor-Steane) codes.

8.7.1 Classical Linear Codes

A classical code is a set of n-bit physical code words $\in \mathbb{Z}_2^n$, which ideally are in a one-to-one relation with the k-bit logical code words to be coded, where $n \geq k$. A simple way of achieving such a correspondence is to use a linear map generated by a generator matrix G. If code words y are $\in \mathbb{Z}_2^n$ and the unencoded words x are $\in \mathbb{Z}_2^k$ (where $\mathbb{Z}_2 = \{0, 1\}$), then G represents a $n \times k$ matrix with entries $G_{ij} \in \mathbb{Z}_2 = \{0, 1\}\ \forall i, j$. Then $y = Gx$ and all arithmetical operations are considered (mod 2). To guarantee the uniqueness of the mapping $x \to y$, the columns of G are chosen to be linearly independent.

Example 25 *1.* $n = 1, k = 1$ *then* $G = \begin{pmatrix} 1 \end{pmatrix}$ *and* $y = x$ *is the only possibility, but that's not really "encoding".*

2. $n = 2, k = 1$

a)

$$G = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{8.117}$$

with the encoding

$$x = 0 \mapsto y = \begin{pmatrix} 0 \\ 0 \end{pmatrix} := 00 \tag{8.118}$$

$$x = 1 \mapsto y = \begin{pmatrix} 0 \\ 1 \end{pmatrix} := 01, \tag{8.119}$$

b)

$$G = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{8.120}$$

with the encoding

$$x = 0 \mapsto y = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 00 \tag{8.121}$$

$$x = 1 \mapsto y = \begin{pmatrix} 1 \\ 0 \end{pmatrix} := 10, \tag{8.122}$$

$$i.e. \quad 0 \mapsto 00, \quad 1 \mapsto 10 \tag{8.123}$$

c)

$$G = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{8.124}$$

with the encoding

$$0 \mapsto 00, \quad 1 \mapsto 11 \tag{8.125}$$

3. The three bit repetition code already considered is a linear code with

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \tag{8.126}$$

which encodes

$$0 \mapsto 000 \qquad and \qquad 1 \mapsto 111 \tag{8.127}$$

Definition 13
A code encoding k logical bits into n physical bits is called $[n, k]$ code. Such codes use, if they are linear, a $n \times k$ generator matrix G.

Example 26
A linear $[6, 2]$ code is for example specified by the generator matrix

$$G = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \tag{8.128}$$

with the encoding

$$00 \to 000000 \tag{8.129}$$
$$01 \to 000111 \tag{8.130}$$
$$10 \to 111000 \tag{8.131}$$
$$11 \to 111111. \tag{8.132}$$

If we input an even number of bits and act on subsequent pairs of bits, this is identical to a 3-bit repetition code where $G = (111)^T$ acting on one bit at a time.

A repetition code encoding k bits with r repetitions for each bit is in general given by the $rk \times k$ generator matrix

$$G = \begin{pmatrix} 1 & 0 & & \\ \vdots & \vdots & & \\ 1 & 0 & & \\ 0 & 1 & & \\ \vdots & \vdots & & \\ 0 & 1 & \ddots & \\ & & & 1 \\ & 0 & & \vdots \\ & & & 1 \end{pmatrix} = \mathbb{1}_k \otimes \begin{pmatrix} 1 \\ \vdots \\ 1_r \end{pmatrix}. \tag{8.133}$$

Repetition codes are as expected from the dimensions of the matrix $[rk, k]$ linear codes. Because the repetition happens for each bit separately, we can generate the

same code simply using the generator matrix

$$G = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \tag{8.134}$$

and apply it instead to each bit separately.

In general one can see that we can obtain any code word $y \in \mathcal{C}$ by forming linear combinations of the columns of G:

$$\mathcal{C} = \left\{ y \mid y = Gx, x \in \mathbb{Z}_2^k \right\} \tag{8.135}$$

so

$$\mathcal{C} = \left\{ \sum_{j=1}^{k} g_j x_j \right\}_{x \in \{0,1\}^k} \tag{8.136}$$

where g_j denotes the jth column of the generator matrix G and x_j the jth bit of the logical code-word $x \in \mathbb{Z}_2^k$. Adding a column j from G to another column j_0 also changes the mapping $x \mapsto y$, of course. However, the code $\mathcal{C} = \{y \mid y = Gx\}$ remains unaffected. Only the words of the code undergo a permutation:

$$\tilde{g}_j = g_j + \delta_{jj_0} g_{j_1} \tag{8.137}$$

i.e.

$$\tilde{g}_{j_0} = g_{j_0} + g_{j_1} \tag{8.138}$$

and all the other columns stay unchanged. Then

$$\tilde{y} = \sum_j x_j \tilde{g}_j \tag{8.139}$$

$$= \sum_{j \neq j_0} x_j g_j + x_{j_0} \left(g_{j_0} + g_{j_1} \right) \tag{8.140}$$

$$= \sum_{j \neq j_1} x_j g_j + \underbrace{\left(x_{j_1} + x_{j_0} \right)}_{= \tilde{x}_{j_1}} g_{j_1} \tag{8.141}$$

$$= \sum_j \tilde{x}_j g_j \,. \tag{8.142}$$

Since this is a 1-to-1 mapping and the columns of G remain lineraly independent,

$$\tilde{x}_j = \begin{cases} x_j & j \neq j_1 \\ x_j + x_{j_0} & j = j_1 \,. \end{cases} \tag{8.143}$$

We see that now $x \to \tilde{y} \neq y$ in general, but $\tilde{y}$ is the code word that would have been obtained from the original G from a code word $\tilde{x}$ obtained by replacing $x_{j_1} \mapsto \tilde{x}_{j_1} = (x_{j_1} + x_{j_0}) \,(\mathrm{mod}\, 2) = x_{j_1} \oplus x_{j_0}$. The code words in the subset with $x_{j_0} = 1$ are permuted (and otherwise unchanged), but the set of code words and thus the code $\mathcal{C}$ are still the same.

Using the generator matrix G the code words are easily generated. The generator matrix is therefore a compact way to specify $\mathcal{C}$. The alternative would be to specify and store all n bits for each code word $y = Gx$ for every unencoded word x (which are 2^k many). This approach would involve $n \cdot 2^k$ "1"s or "0"s, i.e. $n \cdot 2^k$ bits, compared to $n \cdot k$ many if we use the generator matrix G. This is an exponential saving of storage space at the expense of only $\mathcal{O}(nk)$ elementary multiplications and summations $(\mathrm{mod}\, 2)$ for each x.

The easiest form of error correction operation for linear codes is via the so-called *parity check matrix*. This matrix leads to an equivalent formulation of linear codes: Here we define a linear code $\mathcal{C}$as the set of all vectors $x \in \mathbb{Z}_2^{\otimes n}$ such that

$$Hx = 0. \tag{8.144}$$

This means that $\mathcal{C}$ is the kernel of H (to be precise: of the linear mapping specified by H). H is a $(n-k) \times n$ matrix with entries $H_{ij} \in \{0, 1\}$. A code encoding k bits uniquely has to have 2^k code words and therefore has to have an associated H with a k dimensional kernel: For every vector $y \in \ker(H)$ there exists then the possibility to multiply the vector with either 0 or 1 and to create a linear combination of the basis vectors. Since the second dimension n is determined by the number of bits of each code word, the matrix H has to have indeed $(n-k)$ linearly independent rows in order to arrive at a $n-(n-k) = k$-dimensional kernel. Using a $(n-k) \times n$ matrix is therefore also the most compact way to represent H, compared to more (linear dependent) rows. Adding one row of H to another also leaves $\ker(H)$ unaffected and therefore also the code $\mathcal{C}$. By Gaussian elimination we can always bring H into the standard form $[A \mid \mathbb{1}_{n-k}]$, where A is a $(n-k) \times k$ matrix and $\mathbb{1}_{n-k}$ the identity matrix in $(n-k)$ dimensions.

We can generate H from G and vice versa:

$H \to G$

Choose k linearly independent vectors $y_1, \ldots, y_k$ which span the kernel of H ($y_i \in \mathbb{Z}_2^{\otimes n}$). Use these vectors as columns of G. Then obviously the following holds:

$$Hy = 0 \;\forall\; y = Gx \tag{8.145}$$

where $x \in \mathbb{Z}_2^{\otimes k}$, because the y are all linear combinations of the columns of G, i.e. the elements from the kernel $\ker(H)$.

$G \to H$

Choose $n-k$ linearly independent vectors $y_1, \ldots, y_{n-k}$ perpendicular to all the columns of G, $y_i \in \mathbb{Z}_2^{\otimes n}$. Perpendicular means a scalar product equal $0 \,(\mathrm{mod}\, 2)$. Use these vectors as rows for H. Thus, for any linear combination y of the columns of G, $Hy = 0$ as desired.

Example 27

Here are the parity check matrices for the examples above:

1. $n = 1, k = 1, G = \begin{pmatrix}1\end{pmatrix}$. *In this case H is not defined, because H needs $n-k$ rows, where $n-k=0$ in this case. This also means, that there is no error correction possible with this code, as expected.*

2. $n = 2, k = 1$ *and* $G = \begin{pmatrix}0 & 1\end{pmatrix}^T$. *To construct H, we need a vector perpendicular to* $\begin{pmatrix}0 & 1\end{pmatrix}^T$, *e.g.* $\begin{pmatrix}1 & 0\end{pmatrix}^T$. *Then* $H = \begin{pmatrix}1 & 0\end{pmatrix}$ *(without the transpose!) and*

$$C = \ker(H) = \left\{ \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\} \iff \mathcal{C} = \{00, 01\} \tag{8.146}$$

3. *For*

$$G = \begin{pmatrix}1\\1\\1\end{pmatrix} \tag{8.147}$$

we need two vectors perpendicular to G, e.g.

$$\begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix} \qquad (or \ \begin{pmatrix}0\\1\\1\end{pmatrix}) \tag{8.148}$$

Then the parity check matrix is

$$H = \begin{pmatrix}1 & 1 & 0\\1 & 0 & 1\end{pmatrix} \tag{8.149}$$

or any other combination of two of these three vectors perpendicular to G. In this case, the code is

$$\mathcal{C} = \ker(H) = \left\{ \begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix} \right\} = \{000, 111\} \tag{8.150}$$

Note that vectors with a single 1 *or two* 1*s would not work.*

Theorem 22
A pair (H, G) for the same code $\mathcal{C}$ always satisfies the relation

$$HG = 0 \tag{8.151}$$

Proof.

$$(HG)_{ij} = \sum_{k=1}^{n} H_{ik} G_{kj} \tag{8.152}$$

$$= \sum_{k} (y_i)_k \, G_{kj} \tag{8.153}$$

$$= y_i \cdot g_j = 0 \tag{8.154}$$

where y_j is a row from H and g_j a column of G, which were chosen perpendicular to each other! □

If for a given $[n, k]$ code the matrix H is in it's standard form $H = [A \mid \mathbb{1}_{n-k}]$, where A is a $(n-k) \times k$ matrix, then one can immediately choose G in the form of

$$G = \left[\frac{\mathbb{1}_k}{-A}\right] \tag{8.155}$$

were (mod 2) $A = -A$ holds.

Proof.

$$HG = [A \mid \mathbb{1}_{n-k}] \left[\frac{\mathbb{1}_k}{-A}\right] = \underbrace{A\mathbb{1}_k}_{(n-k)\times k} - \underbrace{\mathbb{1}_{n-k}A}_{(n-k)\times k} \tag{8.156}$$

$$= A - A = 0 \tag{8.157}$$

The columns of G are from the kernel of H. Because of the "head" $\mathbb{1}_k$, all the columns of G are linearly independent, making

$$\left[\frac{\mathbb{1}_k}{-A}\right] \tag{8.158}$$

a possible choice for G, indeed. □

With the parity check matrix H, errors are easily detected and identified: We encode x as $y = Gx$. An error e modifies y to $y' = y + e$ and the product $Hy' = Hy + He = He$ due to the linearity and effect of H on elements from the code. He is the so-called *error syndrome* and contains all information about the error e. Consider first the simplest case of at most one error. The error syndrome is 0 if no error has happened. The error syndrome is He_j if an error happened on the jth qubit, where $e_j = \left(\underbrace{0, \ldots, 0}_{j-1 \text{ entries}}, 1, 0, \ldots \right)$, i.e. in this case He_j denotes the jth column of H. As long as all columns of H differ from each other it is possible to uniquely identify the error and to also correct the error using a NOT operation. More generally, if multiple errors can happen, the error syndrome becomes a linear combination of the columns of H, where each flipped bit contributes with weight of 1. The number of errors which can be identified and corrected depends in this general case on the so-called *distance* of the code $\mathcal{C}$.

Definition 14 (Distance of $\mathcal{C}$)
The distance d of the code $\mathcal{C}$ is defined as

$$d(\mathcal{C}) \equiv \min_{\substack{x,y \in \mathcal{C}, \\ x \neq y}} d(x, y), \tag{8.159}$$

where $d(x, y)$ denotes the Hamming distance of x and y, i.e. the number of bits in which x and y differ from each other:

$$d(x, y) \equiv \sum_{i=1}^{n} |x_i - y_i|. \tag{8.160}$$

The Hamming distance of the word x from 0 is called "the weight wt *of x" ,*

$$\text{wt}(x) \equiv \sum_{i=1}^{n} x_i = d(x, 0). \tag{8.161}$$

Example 28
Examples for the Hamming distance are

- $d(0, 1) = 1$
- $d(00, 01) = 1$
- $d(000, 111) = 3$.

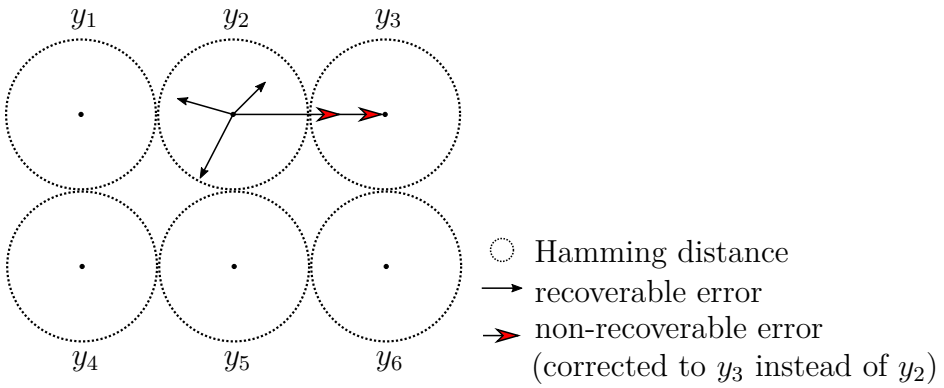


Figure 8.5: Code words $y_i \in \mathcal{C}$ and the distance for which an error modifying the word can be corrected, represented as circles. A *non-correctable* error on e.g. y_2 has a smaller distance to y_3 than to y_2 and therefore gets wrongly corrected to y_3.

Since $|x_i - y_i| = (x_i + y_i) \,(\mathrm{mod}\ 2) = |(x_i + y_i) \,(\mathrm{mod}\ 2) - 0|$, we find for the Hamming distance

$$d\,(x, y) = \mathrm{wt}\,[(x + y) \,(\mathrm{mod}\ 2)] = \mathrm{wt}(x \oplus y). \tag{8.162}$$

This leads to

$$d\,(\mathcal{C}) = \min_{\substack{x,y\in\mathcal{C},\\ x\neq y}} \mathrm{wt}\,(x + y) = \min_{\substack{x\in\mathcal{C}\\ x\neq 0}} \mathrm{wt}(x), \tag{8.163}$$

since if $x, y \in \mathcal{C}$, also $x + y \in \mathcal{C}$.

If we assume the probability of a bit flip to be $p < 1/2$, then the most probable code word y associated with the erroneous code word $y' = y + e$, is the code word with the smallest Hamming distance to y'. If the code has a minimum distance of $d\,(\mathcal{C}) = 2t + 1$, then for a maximum of t errors this y is unique and the error can thus be corrected in the usual sense, i.e. the probability of the corrected word to be wrong (wrongly corrected to another, not the original, word) is smaller than the probability of the error itself happening.

A linear code $[n, k]$ with the distance d is called a $[n, k, d]$ code. We can directly determine the distance $d\,(\mathcal{C})$ from the parity check matrix H:

Lemma 7
Let an arbitrary set of $d - 1$ columns of H be linearly independent, but let there exist a set of d linearly dependent columns of H. Then the distance of the code defined by the matrix H has distance d.

Proof.

Assume there exists a $x \neq 0$, with $\mathrm{wt}\,(x) \leq d-1$ while $Hx = 0$. Since all possible sets of $d-1$ columns of H are linearly independent, there can be no linear combination of $(d-1)$ columns of H with coefficients $\neq 0, \cdots, 0$ that results in 0. This contradicts $x \neq 0$, thus $\min \mathrm{wt}\,(x) \geq d$.

On the other hand, since d columns are linearly dependent, and $\mathrm{wt}(x)$ counts the number of columns that get linearly superposed in Hx, we have $\mathrm{wt}\,(x) = d$ for some x that fulfills $Hx = 0$. Hence, the smallest weight of an $x \in \mathcal{C}$, is $\mathrm{wt}\,(x) = d$. Hence,

$$d\,(\mathcal{C}) = d. \tag{8.164}$$

□

Lemma 8 (Singelton bound)
This directly leads to the Singelton bound: for a $[n, k, d]$ linear code we have

$$n - k \geq d - 1 \tag{8.165}$$

Proof.

Since H is a $(n-k) \times n$ matrix (n column-vectors of dimension $n-k$), there are at most $n-k$ linearly independent vectors in the columns of H. Therefore in any case at least $n-k+1$ vectors have to be linearly dependent, in which case we can use the previous Lemma 7 to find

$$d = n - k + 1\,. \tag{8.166}$$

Of course, even fewer than $n-k$ columns can be linearly independent, therefore we always find

$$d \leq n - k + 1. \tag{8.167}$$

□

8.8 Hamming Code

A *Hamming code* is a linear code for which the columns of the parity check matrix H consist of all binary words with a length of $r = n - k$, except for $\begin{pmatrix} 0 & \dots & 0 \end{pmatrix}^T$. Then $2^r - 1 = n$ different words exist and the Hamming code turns out to be a $[2^r - 1, 2^r - r - 1]$ linear code (H is a $(n-k) \times n$ matrix, then $r = n - k$ and $n = 2^r - 1$, giving $k = n - r = 2^r - r - 1$).

Example 29
$r = 2$ gives a $[3, 1]$ code with

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \tag{8.168}$$

and

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \tag{8.169}$$

where obviously $HG = 0$ and the code words are $0 \mapsto 000$, $1 \mapsto 111$. Any two columns of H are linearly independent, but three columns are linearly dependent, i.e. $d = 3$.

One can directly see that any Hamming code has $d = 3$ as a distance, because for any $r \geq 2$, the matrix H in (8.168) is kept as the lower left corner of H, while the first lines of the first three columns are filled up with 0s. Thus, the first three columns remain linearly dependent just as for $r = 2$, whereas any two columns remain independent: either both columns will get identical zeros or ones in the lines above, in which case they remain linearly independent in the same subspace that is indexed by the additional zeros or ones, or the zeros and ones added differ, which cannot render the two initially linearly independent vectors parallel either. Hamming codes are therefore $[2^r - 1, 2^r - r - 1, 3]$ linear codes and can therefore only recover from single errors.

Error analysis and correction is especially easy for Hamming codes: He_j is the jth column of H and the binary representation of j, i.e. the error syndrome He_j directly tells us (as a binary code), which of the $2^r - 1$ bits used for encoding was flipped. While simple, these codes are clearly highly inefficient.

8.9 Dual Codes

For every linear code with a generator G and a parity check matrix H we can define a dual code $\mathcal{C}^\perp$ with a generator $G\left(\mathcal{C}^\perp\right) := H^T(\mathcal{C})$ and a parity check matrix $H\left(\mathcal{C}^\perp\right) := G^T(\mathcal{C})$. This is equivalent to defining a code with all the code words $y \in \mathcal{C}^\perp$ to be perpendicular to any code word $x \in \mathcal{C} \pmod 2$.

A code is called *weakly self-dual* if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and *strictly self-dual* (or simply *self-dual*) if $\mathcal{C} = \mathcal{C}^\perp$. Dual codes play an important role in the construction of q-error correction codes.

Example 30 *1. For $n = 2$ and $k = 1$*

$$G = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad H = \begin{pmatrix} 0, 1 \end{pmatrix} \tag{8.170}$$

$$\Rightarrow \quad G\left(\mathcal{C}^{\perp}\right) = H^T = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{8.171}$$

and

$$H\left(\mathcal{C}^{\perp}\right) = G^T = \begin{pmatrix} 1, 0 \end{pmatrix} \tag{8.172}$$

The codes are then $\mathcal{C} = \{00, 10\}$ and $\mathcal{C}^{\perp} = \{00, 01\}$. $\mathcal{C}$is obviously neither self-dual nor weakly self-dual. As a side note, also notice $\mathcal{C} \cup \mathcal{C}^{\perp} \neq \mathbb{Z}_2^2$.

2. For

$$G = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad H = \begin{pmatrix} 1, 1 \end{pmatrix} \tag{8.173}$$

$$\Rightarrow \quad G\left(\mathcal{C}^{\perp}\right) = H^T = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = G, \qquad H\left(\mathcal{C}^{\perp}\right) = G^T = \begin{pmatrix} 1, 1 \end{pmatrix} = H \tag{8.174}$$

The codes are then $\mathcal{C} = \{00, 11\} = \mathcal{C}^{\perp}$, i.e. $\mathcal{C}$is self-dual.

Note that in both cases the elements of $\mathcal{C}^{\perp}$ can also be formed simply by the requirement that they must be perpendicular to all of the elements of $\mathcal{C}$. Note also that $x \in \mathcal{C}$ and $y \in \mathcal{C}^{\perp}$ have the same dimensions: G of dimensions $n \times k$ implies H is $(n - k) \times n$, which in turn implies that $G(\mathcal{C}^{\perp}) = H^t$ is $n \times (n - k)$, i.e. both generators $G = G(\mathcal{C})$ and $G(\mathcal{C}^{\perp})$ have the same first dimension n. For $\mathcal{C} = \mathcal{C}^{\perp}$ this implies obviously that all elements of $\mathcal{C}$must be perpendicular to each other. In general, we have the following Lemma:

Lemma 9
A code $\mathcal{C}$is weakly self-dual if and only if

$$G^T G = 0\,. \tag{8.175}$$

Proof.

$\Rightarrow$:

$$\mathcal{C} \subseteq \mathcal{C}^{\perp} \tag{8.176}$$

thus $\forall \{x \mid Hx = 0\}$ also

$$G^T x = 0 \tag{8.177}$$

since $x \in \mathcal{C}$ and therefore $x \in \mathcal{C}^{\perp}$ where $H\left(\mathcal{C}^{\perp}\right) = G^T$. For any $x \in \mathcal{C}$ and $y_j \in \mathbb{Z}_2$:

$$x = \sum_{j=1}^{k} G_{ij} y_j = Gy. \tag{8.178}$$

Hence,

$$G^T G y = 0 \qquad \forall y \in \mathbb{Z}_2^k \tag{8.179}$$

$\Rightarrow \quad G^T G = 0.$

$\Leftarrow$:
Because

$$G^T G = 0 \Rightarrow H\left(\mathcal{C}^{\perp}\right) G = 0 \tag{8.180}$$

If $x \in \mathcal{C}$, then x is a linear combination of the columns of G. $H\left(\mathcal{C}^{\perp}\right) G = 0$ therefore also implies

$$H\left(\mathcal{C}^{\perp}\right) x = 0 \tag{8.181}$$

$\Rightarrow \quad x \in \mathcal{C}^{\perp}$ for any $x \in \mathcal{C}$. Hence, if $x \in \mathcal{C} \Rightarrow x \in \mathcal{C}^{\perp}$.

$$\Rightarrow \quad \mathcal{C} \subseteq \mathcal{C}^{\perp} \tag{8.182}$$

□

For q-error correction codes we need the following Lemma as well.

Lemma 10
Let $\mathcal{C}$ be a linear code. Then the following holds

$$\sum_{y \in \mathcal{C}} (-1)^{x \cdot y} = \begin{cases} |\mathcal{C}| & x \in \mathcal{C}^{\perp} \\ 0 & x \notin \mathcal{C}^{\perp} \end{cases} \tag{8.183}$$

where $|\mathcal{C}|$ specifies the number of elements in $\mathcal{C}$, i.e. the cardinality of the set.

Proof.

1. If $x \in \mathcal{C}^\perp$, then $x \cdot y = 0$ for all $x \in \mathcal{C}^\perp$ and $y \in \mathcal{C}$. Then

$$\sum_{y \in \mathcal{C}} (-1)^{x \cdot y} = \sum_{y \in \mathcal{C}} 1 = |C| \tag{8.184}$$

2. If $x \notin \mathcal{C}^\perp$: $y = Gz \in \mathcal{C}$ is a linear combination of the columns of G (g_i)

$$y = \sum_{i=1}^{k} z_i g_i \tag{8.185}$$

then

$$x \cdot y = \sum_{i=1}^{k} z_i x \cdot g_i \,(\text{mod } 2) = \sum_{i=1}^{k} (z_i s_i) \,(\text{mod } 2) \tag{8.186}$$

where $s_i \equiv x \cdot g_i \,(\text{mod } 2) \in \{0, 1\}$. Then the product reads

$$\sum_{y \in \mathcal{C}} (-1)^{x \cdot y} = \sum_{z \in \mathbb{Z}_2^k} (-1)^{\sum_{i=1}^{k} z_i s_i (\text{mod } 2)} \tag{8.187}$$

$$= \prod_{i=1}^{k} \sum_{z_i = 0,1} (-1)^{z_i s_i (\text{mod } 2)} \tag{8.188}$$

$$= \prod_{i=1}^{k} \left[(-1)^0 + (-1)^{s_i (\text{mod } 2)} \right] \tag{8.189}$$

$$= \prod_{i=1}^{k} \left(2\delta_{s_i (\text{mod } 2), 0} \right) . \tag{8.190}$$

If $x \notin \mathcal{C}^\perp$, then there exists such an i where

$$s_i = x \cdot g_i \,(\text{mod } 2) \neq 0 \tag{8.191}$$

thus

$$\delta_{s_i (\text{mod } 2), 0} = 0 \tag{8.192}$$

and therefore also

$$\sum_{y \in \mathcal{C}} (-1)^{x \cdot y} = 0. \tag{8.193}$$

□

8.10 Calderbank-Shor-Steane Codes

Calderbank-Shor-Steane codes [10,39] are an important sub-class of q-error correction codes of the so-called *stabiliser codes*. (*[?]*).

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be $[n, k_1]$ (and respectively $[n, k_2]$) classical, linear codes and $\mathcal{C}_2 \subset \mathcal{C}_1$. Also let $\mathcal{C}_1$ and $\mathcal{C}_2^{\perp}$ correct t errors each. We can then define a $[n, k_1 - k_2]$ q-error correction code $\mathrm{CSS}\,(\mathcal{C}_1, \mathcal{C}_2)$, the "CSS-code of $\mathcal{C}_1$ over $\mathcal{C}_2$", which can correct errors on t qubits, and which we can construct as follows.

First, let $x \in \mathcal{C}_1$ be an arbitrary code word in $\mathcal{C}_1$. Define

$$|x + \mathcal{C}_2\rangle := \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |x + y \,(\mathrm{mod}\ 2)\rangle \tag{8.194}$$

where the notation $|x + \mathcal{C}_2\rangle$ denotes a co-set notation: As can be shown (see exercises), a linear code constitutes a group with the bit-wise addition $\oplus \equiv +\,(\mathrm{mod}\ 2)$ as the group's operator. Since $\mathcal{C}_2 \subset \mathcal{C}_1$ is a code it is a group as well and hence $\mathcal{C}_2$ is a subgroup of $\mathcal{C}_1$. An element $x \in C_1$ generates a left co-set $\mathcal{C}_1/\mathcal{C}_2$ ("$\mathcal{C}_1$ over $\mathcal{C}_2$"), defined as

$$\mathcal{C}_1/\mathcal{C}_2 \equiv \{y \mid y = x \cdot z \ \forall z \in \mathcal{C}_2\}\,. \tag{8.195}$$

The group's operation $\cdot$ is in our case $\oplus$, i.e. the bitwise *XOR*. The element $x \in \mathcal{C}_1$ is fixed and indicates a chosen co-set. Correspondingly, a right coset can be defined as $\{y | y = z \cdot x \quad \forall\ z \in \mathcal{C}_2\}$, but here there is no difference between right and left co-sets, as the group is Abelian. The co-sets have all the same dimension as the sub-group, i.e. here $\mathcal{C}_2$. The union of all distinct cosets gives back the full group, here $\mathcal{C}_1$.

Example 31
Let $\mathcal{G} = \{0, 1, 2, 3, 4\}$ be the group $\mathbb{Z}_4$ with group operation = addition modulo 4. It has a subgroup $\mathcal{H} = \{0, 2\}$. The left coset for element $0 \in \mathcal{G}$ is always the subgroup itself. The left coset of element 1 is $\{(1 + h) mod\, 4 \mid h \in \mathcal{H}\} = \{1, 3\}$; and the left cosets of elements 2 and 3 are, respectively, $\{(2 + h) mod\, 4 \mid h \in \mathcal{H}\} = \{0, 2\} = \mathcal{H}$ and $\{(3 + h) mod\, 4 \mid h \in \mathcal{H}\} = \{3, 1\}$. So the two different left co-sets $\mathcal{G}/\mathcal{H}$ are $\{0, 2\}$ and $\{1, 3\}$.

Using the definition in Equation 8.194 one can see, that if $x, x' \in \mathcal{C}_1$ and $y' :=$

$x - x' \in \mathcal{C}_2$, then $|x + \mathcal{C}_2\rangle = |x' + \mathcal{C}_2\rangle$, since

$$|x' + \mathcal{C}_2\rangle = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |x' \oplus y\rangle \tag{8.196}$$

$$= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |x \oplus \underbrace{y' \oplus y}_{:= y'' \in \mathcal{C}_2}\rangle \tag{8.197}$$

$$= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y'' \in \mathcal{C}_2} |x \oplus y''\rangle = |x + \mathcal{C}_2\rangle \,. \tag{8.198}$$

In (8.197) we used that $x' = x \ominus y' = x \oplus y'$. From this we see that states $|x + \mathcal{C}_2\rangle$ and $|x' + \mathcal{C}_2\rangle$ where x, x' differ by an element of $\mathcal{C}_2$ are identical. In other words, states $|x + \mathcal{C}_2\rangle$ can indeed be parametrised using $x \in \mathcal{C}_1/\mathcal{C}_2$, i.e. x needs to be specified only "modulo the subgroup $\mathcal{C}_2$". If x and x' belong to different co-sets $\mathcal{C}_1/\mathcal{C}_2$, then the labels $x \oplus y$ and $x' \oplus y$ occurring in the linear combinations do not have a common element, no matter how we choose x, x', y. $|x + \mathcal{C}_2\rangle$ and $|x' + \mathcal{C}_2\rangle$ are then perpendicular to each other.

Definition 15
The q-error correction code $\mathrm{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ *is defined as the vector space spanned by the states* $|x + \mathcal{C}_2\rangle$*, for all* $x \in \mathcal{C}_1$*:*

$$\mathrm{CSS}(\mathcal{C}_1, \mathcal{C}_2) = \mathrm{span}\left\{|x + \mathcal{C}_2\rangle \,, \forall x \in \mathcal{C}_1/\mathcal{C}_2\right\}. \tag{8.199}$$

The number of co-sets of $\mathcal{C}_2$ in $\mathcal{C}_1$ is $|\mathcal{C}_1| \,/\, |\mathcal{C}_2|$ and the dimension of $\mathrm{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ is therefore $|\mathcal{C}_1| \,/\, |\mathcal{C}_2| = 2^{k_1 - k_2}$. The $\mathrm{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ is thus a $[n, k_1 - k_2]$ q-code.

Using the $\mathrm{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ code we can detect up to t bit- and phase-flip errors and also recover from them by using the error correction properties of classical codes $\mathcal{C}_1$ and ${\mathcal{C}_2}^{\perp}$:

Let the bit-flip errors be represented by a vector e_1 with the entry "1" for every flipped bit and "0" otherwise. Correspondingly, let the phase flip errors be represented by a vector e_2. Both errors combined then act as:

$$|x + \mathcal{C}_2\rangle \overset{\text{error}}{\longmapsto} \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} (-1)^{(x+y)\cdot e_2 \,\downarrow \text{phase flip}} |x + y + \underset{\uparrow \text{bit flip}}{e_1}\rangle \tag{8.200}$$

To detect the bit flip, the error syndrome linked to the parity check matrix H_1 of $\mathcal{C}_1$ is calculated in an auxiliary register that was initialised to all $|0\rangle$:

$$|x + y + e_1\rangle\,|0\rangle \mapsto |x + y + e_1\rangle\,|H_1\,(x + y + e_1)\rangle = |x + y + e_1\rangle\,|H_1 e_1\rangle \tag{8.201}$$

because $(x+y) \in \mathcal{C}_1$ (remember that $y \in \mathcal{C}_2 \subset \mathcal{C}_1$) and therefore $H_1(x+y) = 0$. This results in

$$|x+\mathcal{C}_2\rangle |0\rangle \xmapsto{\text{error and calc. of} H_1 e_1} \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y\in\mathcal{C}_2} (-1)^{(x+y)\cdot e_2} |x+y+e_1\rangle |H_1 e_1\rangle \quad (8.202)$$

The auxiliary register is then measured in the computational basis. We especially note, that the state in Eq.(8.202) is not entangled since the state $|H_1 e_1\rangle$ is always the same state for all $y \in \mathcal{C}_2$, i.e. the state remains a product state. The measurement collapses $|H_1 e_1\rangle$ onto itself and results in a classical error syndrome $H_1 e_1$. This error syndrome is used to identify the qubit in the main register that needs to be flipped back to its original state. This is possible since $\mathcal{C}_1$ can correct up to t errors. The auxiliary register is then no longer needed and can be reset back to $|0\rangle$ and used again. We then have the state

$$|\psi'\rangle \equiv \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y\in\mathcal{C}_2} (-1)^{(x+y)\cdot e_2} |x+y\rangle . \quad (8.203)$$

Phase flips can be detected by again converting them into an equivalent bit flip in a rotated basis by applying Hadamard gates to every single qubit. A quick reminder: For a register of n qubits,

$$H|x\rangle = \frac{1}{\sqrt{2^n}} \sum_z (-1)^{x\cdot z} |z\rangle \quad (8.204)$$

$$\Rightarrow \; |\psi''\rangle = H^{\otimes n} |\psi'\rangle = \frac{1}{\sqrt{|\mathcal{C}_2|\, 2^n}} \sum_{z\in\mathbb{Z}_2^n} \sum_{y\in\mathcal{C}_2} (-1)^{(x+y)(e_2+z)} |z\rangle \quad (8.205)$$

$$= \frac{1}{\sqrt{|\mathcal{C}_2|\, 2^n}} \sum_{z'} \sum_{y\in\mathcal{C}_2} (-1)^{(x+y)\cdot z'} |z'+e_2\rangle \quad (8.206)$$

where $z' := e_2 + z$ and $z = z' - e_2 = z' + e_2 \,(\text{mod } 2)$. Using Lemma 10, hence $\sum_{y\in\mathcal{C}_2} (-1)^{y\cdot z'} = |\mathcal{C}_2|$ for $z' \in \mathcal{C}_2^\perp$ and 0 else, this state then becomes

$$|\psi''\rangle = \sqrt{\frac{|\mathcal{C}_2|}{2^n}} \sum_{z'\in{\mathcal{C}_2}^\perp} (-1)^{x\cdot z'} |z'+e_2\rangle , \quad (8.207)$$

where only the contributions from $z' \in \mathcal{C}_2^\perp$ remain.

This now looks the same like in the case of a bit flip. Now reversibly apply the parity check matrix $H\left(\mathcal{C}_2^\perp\right) =: H_2$ in an auxiliary register and then use the result to correct the error e_2:

$$\Rightarrow \sqrt{\frac{|\mathcal{C}_2|}{2^n}} \sum_{z'\in\mathcal{C}_2^\perp} (-1)^{x\cdot z'} |z'\rangle \quad (8.208)$$

We are now left with the task to transform back to the old (original) basis by applying Hadamard gates to each qubit again, taking advantage of the identity $H^2 = \mathbb{1}$. This brings us back to the state $|\psi'\rangle$ in Eq.(8.203) but now with $e_2 = 0$, i.e.

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |x + y\rangle = |x + \mathcal{C}_2\rangle \,, \tag{8.209}$$

which is the original code word!

Since this is valid for any basis state $|x + \mathcal{C}_2\rangle$ of the CSS $(\mathcal{C}_1, \mathcal{C}_2)$ code, the approach therefore can be used to protect an arbitrary superposition $|\psi\rangle$ of states $|x + \mathcal{C}_2\rangle$ against up to t bit flips and t phase flips. Due to the discretisation of errors (Theorem 21) the state $|\psi\rangle$ is thus protected against *any* error on up to t qubits.

In summary, if $\mathcal{C}_1$ and $\mathcal{C}_2$ are $[n, k_1]$ and $[n, k_2]$ classical linear codes, respectively, with $\mathcal{C}_1 \subset \mathcal{C}_2$ and both $\mathcal{C}_1$ and $\mathcal{C}_2^\perp$ correct errors on up to t bits, then CSS $(\mathcal{C}_1, \mathcal{C}_2)$ is an $[n, k_1 - k_2]$ q-error correcting code which can correct arbitrary errors on up to t qubits. The computation of the error syndromes and the error correction can be performed efficiently with *CNOT*gates and Hadamard gates only (the number of gates is linear in n), and measurement of an ancilla register in the computational basis. It can also be shown that coding and decoding can be done with a number of gates linear in n.

Example 32 (7 qubit Steane code)
This code is based on the $[7, 4, 3]$ *Hamming code with*

$$H(\mathcal{C}_1) = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \tag{8.210}$$

a 3×7 *matrix. We define* $\mathcal{C}_1 := \mathcal{C}$ *and* $\mathcal{C}_2 := \mathcal{C}^\perp$. *As* $n - k = 3$, $n = 7$, *we have* $k = 4$ *and* G *is a* $n \times k = 7 \times 4$ *matrix.*

$$H(\mathcal{C}_2) = H\left(\mathcal{C}^\perp\right) = G^T(\mathcal{C}) \,. \tag{8.211}$$

We first bring H *to its canonical form. Replacing row 1 by rows 1+2, row 2 by rows 1+3, and row 3 by row 2 we find*

$$H' = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}. \tag{8.212}$$

Replacing row 3 by rows 2+3 gives the canonical form

$$\rightarrow H'' = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} = [A \mid \mathbb{1}_{n-k}] \tag{8.213}$$

$$\Rightarrow G = \begin{pmatrix} \mathbb{1}_k \\ \hline -A \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \tag{8.214}$$

$$\Rightarrow H(\mathcal{C}_2) = G^T(\mathcal{C}) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{8.215}$$

We see that the 4*th line of* $H(\mathcal{C}_2)$ *is the same as the* 1*st line of* $H(\mathcal{C}_1)$*. The* 2*nd plus* 3*rd line of* $H(\mathcal{C}_2)$ *give the* 2*nd line of* $H(\mathcal{C}_1)$ *and the* 1*st plus* 3*rd line of* $H(\mathcal{C}_2)$ *give the* 3*rd line of* $H(\mathcal{C}_1)$*. Thus*

$$\operatorname{span}(rows(H(\mathcal{C}_1))) \subset \operatorname{span}(rows(H(\mathcal{C}_2))). \tag{8.216}$$

Since the codes $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *are all code words perpendicular to these rows of* $H(\mathcal{C}_1)$ *and* $H(\mathcal{C}_2)$*, respectively, it follows*

$$\mathcal{C}_2 \subset \mathcal{C}_1 \iff \mathcal{C}^\perp \subset \mathcal{C} \tag{8.217}$$

and

$$\mathcal{C}_2^\perp = \left(\mathcal{C}^\perp\right)^\perp = \mathcal{C} = \mathcal{C}_1 \tag{8.218}$$

so both $\mathcal{C}_2^\perp$ *and* $\mathcal{C}_1$ *are distance* 3 *codes that can correct errors on a single qubit (*$\mathcal{C}_1 \equiv \mathcal{C}$ *definitely is, and since* $\mathcal{C}_2^\perp = \mathcal{C}_1$*, so is* $\mathcal{C}_2^\perp$*).* $\mathcal{C}_1$ *is a* $[7,4]$ *code, therefore* $\mathcal{C}_2$ *is a* $[7,3]$ *code. Thus* $\mathrm{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ *is a* $[7,1]$ *code which encodes a single (logical) qubit into* 7 *(physical) qubits.*

What are the explicit code words?
We can generate $|0\rangle_L$ *as* $|0\rangle_L = |x + \mathcal{C}_2\rangle$ *with some* $x \in \mathcal{C}_1$*. E.g.* $x = 0$ *gives*

$$|0\rangle_L \equiv |0 + \mathcal{C}_2\rangle = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |0 + y\rangle = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |y\rangle \tag{8.219}$$

The code words $y \in \mathcal{C}_2$ are generated from $G(\mathcal{C}_2) = H(\mathcal{C}_1)^T$ by

$$000 \mapsto \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad 100 \mapsto \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad 010 \mapsto \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad 001 \mapsto \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \tag{8.220}$$

$$110 \mapsto (y_{010} + y_{100})\,(mod\ 2) = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{8.221}$$

$$101 \mapsto (y_{100} + y_{001})\,(mod\ 2) = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{8.222}$$

$$011 \mapsto (y_{001} + y_{010})\,(mod\ 2) = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \tag{8.223}$$

$$111 \mapsto (y_{110} + y_{001})\,(mod\ 2) = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{8.224}$$

So

$$|0\rangle_L = \frac{1}{\sqrt{8}}\Big[\,|0000000\rangle + |0001111\rangle + |0110011\rangle + |1010101\rangle \tag{8.225}$$

$$+ |0111100\rangle + |1011010\rangle + |1100110\rangle + |1101001\rangle\,\Big]. \tag{8.226}$$

Correspondingly we can generate $|1\rangle_L$ *as* $|x' + \mathcal{C}_2\rangle$*,*

$$|1\rangle_L = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |x' + y\rangle \tag{8.227}$$

with some $x' \neq x, \quad x' \in \mathcal{C}_1$ *but* $x' - x = x' \notin \mathcal{C}_2$*. An example is* $x' = 1111111$ *which makes that* $|1\rangle_L$ *has all qubits flipped with respect to* $|0\rangle_L$ *and is therefore definitely perpendicular to* $|0\rangle_L$*.*

8.11 Stabilizer Codes

The Stabilizer formalism

Idea: States can be specified by giving the eigenvalues corresponding to a complete set of observables e.g. H-atom{n,l,m,s_z}. Here we will fix (somewhat arbitrarily) all eigenvalues of a certain set of observables as all equal to 1, and then different sets of obervables define different codes, i.e. different subspace of Hilbert space $\mathcal{H}$, and the observables chosen will in general not specify a state completely, but rather a whole space code $\mathcal{C}$.

It will turn out that this leads to a rather efficient specification of error-correcting codes and a characterization of their properties. But the application of stabilizer formalism is beyond quantum error correction. Notably it also leads to a powerful theorem with a sufficient condition that a quantum algorithm can be efficiently simulated classically.

Definition 16
A state $|\psi\rangle$ is said to be stabilized by an observable A if $A|\psi\rangle = |\psi\rangle$.

Which observable A to choose? Daniel Gottesmann showed in his PhD thesis that useful sets of observables are obtained as certain subgroups of the so-called Pauli groups G_n on qubits.

Definition 17
The Pauli groups $G_n = \left\{ e^{i\frac{\pi}{2}s_0} \bigotimes_{i=1}^{n} X_{s_i}^{(i)} \right\}_s$, *where,* $s = (s_0, .., s_n), s_i \in \left\{0,1,2,3\right\} \forall i = 0, 1, \ldots, n$ $X_0^{(i)} = I^{(i)}, X_1^{(i)} = \sigma_x^{(i)} \equiv X, X_2^{(i)} = \sigma_y^{(i)} \equiv Y, X_3^{(i)} = \sigma_z^{(i)} \equiv Z$.

The label s specifies a group element. So the Pauli group G_n consists of all tensor products of Pauli matrices or the identity on n qubits, multiplied with overall phase factors ± 1 or $\pm i$. Hence, $|G_n| = 4^{n+1}$. The group operation is matrix multiplication. E.g.

$$G_1 = \left\{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\right\}$$

$$G_n = \left\{1, i, -1, -i\right\} \otimes \left\{I, X, Y, Z\right\}^{\otimes n}$$

The phase factors are needed to close the group under multiplication.

According to the theorem by Caley, every finite group of order n is isomorphic to a subgroup of the symmetric groups S_n (group of all permutations of n objects). However, even for n=1, $|G_1| = 16$, clearly allowing for quite non-trivial subgroups

of S_{16}. One shows, however, that all cycles of the permutations generated by elements of G_1, $g' \to f_g(g') = gg'$ are of length 1,2 or 4.

We now consider subgroups of G_n.

Definition 18
Let S be a subgroup of G_n. Then we call V_s the "vector space stabilized by S" the set of all n-qubit states that are stabilized by all elements of S, i.e.

$$V_s = \left\{ |\psi\rangle \mid g\,|\psi\rangle = |\psi\rangle \; \forall g \in S \right\}.$$

Clearly, V_s is a subspace of the full Hilbert space of all n-qubit states. Furthermore, it is closed under linear combination of elements of V_s,

$$|\psi_1\rangle, |\psi_2\rangle \in V_s \implies \alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle \in V_s, \text{ as}$$

$$g(\alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle) = \alpha g\,|\psi_1\rangle + \beta g\,|\psi_2\rangle = \alpha\,|\psi_2\rangle + \beta\,|\psi_2\rangle$$

$\implies$ V_s is indeed a vector subspace of V_s. It is the intersection of all subspaces stabilized by the individual elements of S ,

$$V_s = \bigcap_{i=1}^{|S|} V_s(g_i), \text{ where } V_s(g_i) = \left\{ |\psi\rangle \; |g_i\,|\psi\rangle = |\psi\rangle \right\}$$

Example 33
n=3, $S = \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$. We first check that S is a subgroup of the Pauli-group G_3 : Obviously all $g_i \in S$ are $\in G_3$.

Multiplication Table				
	I	Z_1Z_2	Z_2Z_3	Z_1Z_3
I	I	Z_1Z_2	Z_2Z_3	Z_1Z_3
Z_1Z_2	Z_1Z_2	I	Z_1Z_3	Z_2Z_3
Z_2Z_3	Z_2Z_3	Z_1Z_3	I	Z_1Z_2
Z_1Z_3	Z_1Z_3	Z_2Z_3	Z_1Z_2	I

$\iff$

Multiplication Table					
	1	*2*	*3*	*4*	*Permutation*
1	*1*	*2*	*3*	*4*	*{}*
2	*2*	*1*	*4*	*3*	*{(12),(34)}*
3	*3*	*4*	*1*	*2*	*{(13),(24)}*
4	*4*	*3*	*2*	*1*	*{(14),(23)}*

We see that S is a group that is non-empty and closed under multiplication and inverses, and that S is abelian (symmetric multiplication table). It is isomorphic to a subgroup of S_{16}, containing the permutations $\{\{\}, \{(12),(34)\}, \{(13),(24)\}, \{(14),(23)\}\}$ written in cycle form. The empty set is used here to indicate that no non-trivial cycles exist, meaning cycles of length >1. I.e. $\{\}$ is the identity permutation.

What are the states stabilized by S?

- I does not restrict $|\psi\rangle$, $I|\psi\rangle = |\psi\rangle \,\forall\, |\psi\rangle$.
- $Z_1Z_2|\psi\rangle = |\psi\rangle \implies |\psi\rangle \in \left\{|00b\rangle, |11b\rangle \, b \in \{0,1\}\right\} = \left\{|000\rangle, |110\rangle, |001\rangle, |111\rangle\right\}$
- $Z_2Z_3|\psi\rangle = |\psi\rangle \implies |\psi\rangle \in \left\{|000\rangle, |011\rangle, |100\rangle, |111\rangle\right\}$
- $Z_1Z_3|\psi\rangle = |\psi\rangle \implies |\psi\rangle \in \left\{|000\rangle, |101\rangle, |010\rangle, |111\rangle\right\}$

$\implies V_s = \left\{|000\rangle, |111\rangle\right\}$

We also see that it would have been enough to consider only Z_1Z_2 and Z_2Z_3 in order to find V_s. This turns out to be due to the fact that $Z_1Z_3 = Z_1Z_2.Z_2Z_3$. So if $Z_2Z_3|\psi\rangle = |\psi\rangle$ and $Z_1Z_2|\psi\rangle = |\psi\rangle \implies Z_1Z_3|\psi\rangle = Z_1Z_2.Z_2Z_3|\psi\rangle = |\psi\rangle$. This can be made general by introducing the concepts of generator of a group.

Definition 19
A set $\{g_i\}_{i=1}^k \in S$ is said to generate the group S (or is a set of generators of S) if $\forall g \in S$ we can write $g = \prod_l g_{i_l}, i_l \in \{1,\ldots,k\}$, i.e. as a product (group operation) of elements of the set of generator. Notation: $S = \langle g_1,\ldots,g_k\rangle$.

The set of generators is called "independent", if removing any element makes the generated set smaller,

$$\langle g_1,..,g_{i-1},g_{i+1},..,g_k\rangle \neq \langle g_1,\ldots,g_k\rangle .$$

We then have the following proposition:

Proposition 1
Let V_s be the vector space stabilized by $S = \langle g_1,\ldots,g_k\rangle$, i.e. the group generated by $g_1,\ldots,g_k$. Then $|\psi\rangle \in V_s \iff g_i|\psi\rangle = |\psi\rangle \,\forall g_i \in \{g_1,\ldots,g_k\}$, i.e. it is necessary and sufficient that $|\psi\rangle$ be stabilized by all generators of S.

Proof.

" $\implies$ " is trivial, as $|\psi\rangle \in V_s \iff g|\psi\rangle = |\psi\rangle \;\forall g \in S$ and $g_i \in S$.
Conversely, let $g_i|\psi\rangle = |\psi\rangle \,\forall g_i \in \{g_i,\ldots,g_k\}$. Since $g = \prod_l g_{i_l}$ it follows that $g|\psi\rangle = \prod_l g_{i_l}|\psi\rangle = |\psi\rangle$, as all $g_{i_l} \in \{g_1,\ldots,g_k\}$, applied successively to $|\psi\rangle$ give $g_{i_l}|\psi\rangle = |\psi\rangle$. Hence, $|\psi\rangle \in V_s$. □

This allows an even more compact description of stabilized vector spaces. In the above example of $V_s = \langle Z_1 Z_2, Z_2 Z_3 \rangle$ we see that we have stabilized the 3 qubit bit-flip code. Furthermore, the generators correspond to the non-local measurements we introduced for syndrom measurements. This turns out to be a general structure. Here are for example the generators that stabilize the 7 qubit Steane code:

g_1	I	I	I	X	X	X	X
g_2	I	X	X	I	I	X	X
g_3	X	I	X	I	X	I	X
g_4	I	I	I	Z	Z	Z	Z
g_5	I	Z	Z	I	I	Z	Z
g_6	Z	I	Z	I	Z	I	Z

$$\mathrm{H}(\mathcal{C}_1) = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = \mathrm{H}(\mathcal{C}_2^{\perp}) \, .$$

We see that g_1, g_2, g_3 are direct translations of the parity check matrix $H(\mathcal{C}_1)$ of the Steane code with $0 \leftrightarrow I, 1 \leftrightarrow X$. Generators g_4, g_5, g_6 are obtained in general from $H(\mathcal{C}_2^{\perp})$ by $0 \leftrightarrow I, 1 \leftrightarrow Z$. Here, for the 7 qubit Steane code, remember that $\mathcal{C}_1 = \mathcal{C}_2^{\perp}$ so the 2 parity check matrices are the same.

So far we have not yet shown error correcting properties of the vector spaces V_s stabilized by (generators of) a subgroup S of the Pauli group G_n. Before getting there it is useful to make a few more general statements about V_s and the corresponding S.

Indeed, it is clear that not every subgroup $S \subset G_n$ will generate a non-trivial V_s.

Proposition 2
V_s is only non-trivial, i.e. $V_s \neq \{0\}$, the vector space containing the zero element of Hilbert space only, if

- *all elements of S commute AND*
- *$-I \notin V_s$.*

Proof.

Since all $g \in S$ are tensor products of Pauli-matrices I,X,Y,Z, up to a multiplicative prefactor, and two Pauli matrices either commute or anti-commute, $g, g' \in S$ either

commute or anti-commute. So for $[g, g'] \neq 0 \implies gg' = -g'g$. On the other hand $gg' |\psi\rangle = g'g |\psi\rangle = |\psi\rangle$ as both g, g' stabilize V_s, so $gg' |\psi\rangle = -g'g |\psi\rangle \implies |\psi\rangle = 0$.

Thus all $g \in S$ must commute for V_s to be non-trivial. This was to be expected as otherwise they could not have a common eigenstate. Similarly, $-I \in S \implies -I |\psi\rangle = - |\psi\rangle = |\psi\rangle \implies |\psi\rangle = 0 \implies V_s$ trivial. □

Now, all $g \in S$ commute $\iff$ all generators g_i commute.

Proof.

" $\implies$ ": is trivial as $g_i \in S$. Conversely, since $g = \prod_l g_{i_l}, g' = \prod_l g_{j_l}$ and $[g_{i_l}, g_{j_l}] = 0$ we have also $[g, g'] = 0$. □

The fact that $-I \notin S$ also implies $\pm iI \notin S$, as otherwise $(\pm iI)^2 = -I \in S$. Furthermore we have:

Proposition 3
Let S be a subgroup of G_n with $-I \notin S$. Then $g^2 = I \, \forall g \in S$.

Proof.

Proof: We first show the corresponding statement for the generators g_i, S=$\langle g_1, \ldots, g_k \rangle$. Suppose $g_i^2 \neq I$ for some g_i. But

$$g_i = e^{i\frac{\pi}{2}s_0} \bigotimes_{j=1}^{n} X_{s_j}, \; s_i \in \{0, 1, 2, 3\} \forall i = 0, \ldots, n$$

$$\implies g_i^2 = e^{i\pi s_0} \bigotimes_{j=1}^{n} X_{s_j}^2 = e^{i\pi s_0} I = \pm I$$

So for $g_i^2 \neq I \implies g_i^2 = -I \implies$ contradiction $\implies g_i^2 = I \forall j$.

Now $g = \prod g_i \implies g^2 = \prod_i g_i \prod_j g_j$. Since $-I \notin S \implies [g_i, g_j] = 0 \forall i, j \implies g^2 = \prod g_i^2 = \prod I = I$. □

The independence of a set of generator can be checked with the so called "check matrix" R_1 defined in the following way:
Let $S = \langle g_1, \ldots, g_l \rangle$ then R is a $l \times 2n$ matrix with entries $\in \{0, 1\}$ where row $r(g_s)$ corresponds to generator g_s. There are two $l \times n$ blocks arranged next to each other. In the left block we have a 1 for each X, in the right a 1 for each Z, and a 1 in both blocks for each Y. With $g_s = e^{i\frac{\pi}{2}s_0} \bigotimes_{j=1}^{n} X_{s_j}^{(j)}$, the bits $r(g_s)_{j+n}$ and $r(g_s)_j$

S_j	$r(g_s)_{j+n}$	$r(g_s)_j$	$X_{s_j}^{(j)}$
0	0	0	I
1	0	1	X
2	1	1	Y
3	1	0	Z

hence represent a binary code for $S_j, j = 1 \ldots, n$. The index s_0 is not coded. In other words, the entries of the rows of R are given by

Note the inverted order of the binary code. This is so because $-iY = XZ$, hence Y contains both X, Z. Concerning the binary code, it would have been more natural to have ordered Pauli's matrices as I, X, Z, Y.

E.g. $S = \langle Z_1 Z_2, Z_2 Z_3 \rangle$, a subgroup of G_3

$$\Longrightarrow R = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right).$$

Or for the 7 qubit Steane code:

$$R = \left[\begin{array}{ccccccc|ccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & . & . & . & . & . & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & . & . & . & . & . & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & . & . & . & . & . & 0 \\ 0 & . & . & . & . & . & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & . & . & . & . & . & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & . & . & . & . & . & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right].$$

Proposition 4
Let $S=\langle g_1, \ldots, g_l \rangle$ and $-I \notin S$. The generators $g_1, \ldots, g_l$ are independent iff the rows of the corresponding check matrix are linearly independent.

Proof.

Observe that addition of rows corresponds to matrix multiplications: $r(g) + r(g') = r(gg')$. This can be checked bitwise, and holds since $I \hat{=} 0$, and $XZ = -iY \hat{=} 10 + 01 = 11 \hat{=} Y$.

$\Longrightarrow$ A linear combination $r = \sum_i a_i r(g_i), a_i \in \{0, 1\}$ corresponds to $= r(\prod)\{a_i = 1\} g_i) = r(\prod_{i=1}^n g_i^{a_i})$ and $r = 0 = r(I) \iff \prod_{i=1}^n g_i^{a_i} = I$. Multiply from the right with

a $|g_j$ with $a_j = 1$. $\implies \prod_{i\neq j} g_i^{a_i} = g_i$, where $-I \notin S$ and hence $g_j^2 = I$ was used. So $r = \sum_{i=1}^n a_i r(g_i) = 0$ with some $a_i = 1 \iff \{r(g_i)\}$ linearly dependent $\iff \prod_{i\neq j} g_i^{a_i} = g_j$ for some j with $a_j = 1$, and thus g_j can be expressed as product of the other g_i's and the g_i are therefore not independent. □

The check matrix also provides a simple way of checking if two elements g, g' of the Pauli group commute. To this end, one defines $r(g)$ and $r(g')$ just as if g and g' were generators. Then we have

Proposition 5

$[g, g'] = 0$, *with* $g, g' \in G_n \iff r(g)\Lambda r(g')^T = 0$ *where* $\Lambda = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$.

Note that Λ leads to a blochwise exchange of the two halfs of $r(g')$. Before proving the proposition, here are some examples:

1. $g = XZ, g' = ZX$ (meaning $g = X \otimes Z, g' = Z \otimes X$)

   $\implies [g, g'] = XZ.ZX - ZX.XZ = XZ \otimes ZX - ZX \otimes XZ$

   $= -iY \otimes iY - iY \otimes (-iY) = YY.YY - YY.YY = 0$

   $r(g) = [\underbrace{10}_{\text{from X}} | \overbrace{01}^{\text{from Z}}], r(g') = [01|10] \implies \Lambda r(g')^T = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

   $\implies C_{gg'} \equiv r(g)\Lambda r(g')^T = 2 = 0 \bmod 2$.

2. $g = XX$, $g' = ZZ$
   $\implies [g, g'] = [XX, ZZ] = XZ \otimes ZX - ZX \otimes XZ = (-iY) \otimes (-iY) - (iY)(iY) = 0$

   $r = 1010$, $r' = 0101$, $r\Lambda r'^T = \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = 2 = 0 \bmod 2$

3. $g = IX$, $g' = IZ$
   $\implies [g, g'] = IX.IZ - IZ.IX = I \otimes [X, Z] = I \otimes (-iY) \neq 0$

   $\implies r\Lambda r'^T = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} \Lambda \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 1 \neq 0 \bmod 2$.

a_i	b_i	a'_i	b'_i	$a_ib'_i + b_ia'_i$	
0	1	1	0	1	valid pairs (contribute 1 to n_g)
0	1	1	1	1	
1	0	0	1	1	
1	0	1	1	1	
0	1	0	0	0	some invalid pairs. Always get 0
0	1	0	1	0	
1	0	0	0	0	
1	0	1	0	0	
1	1	0	0	0	
1	1	0	1	1	valid pairs (contribute 1 to n_g)
1	1	1	0	1	
1	1	1	1	0	

Table 8.2: Some combinations of a_i, b_i, a'_i, b'_i used in the proof of proposition 5.

Proof.

Proof of proposition: We can restrict ourselves to elements g, g' without the prefactors $\pm 1, \pm i$, as they do not influence the commutation properties nor the check matrix.

So $g = \bigotimes_{i=1}^n X_{s_i}^{(i)}, g' = \otimes_{i=1}^n X_{s'_i}^{(i)}$ without restriction of generality.
$\implies gg' = \otimes_{i=1}^n X_{s_i}^{(i)} X_{s'_i}^{(i)}$

$= (i)^{n_{gg'}} g = \otimes_{i=1}^n X_{p_i}^{(i)}$, where $n_{gg'}$ = number of qubits for which both s_i and $s'_i \neq 0$, and $s_i \neq s'_i$, i.e. two non-trivial ($\neq I$) different Pauli matrices meet. This also implies

$gg' = (i)^{-n_{gg'}} \otimes_{i=1}^n X_{p_i}^{(i)}$ with the same p_i and $n_{gg'}$.

Still $p_i \in \{0, 1, 2, 3\}$, but it is irrelevant which one. $n_{gg'}$ is coded by $r(g)$ and $r(g')$: Let $r(g) = (a, b)$, where $a_i, b_i \in \{0, 1\}, i = 1, 2, ..n, a = (a_1, .., a_n), b = (b_1, ..b_n)$, and correspondingly for $r(g') = (a', b')$. Then $n_{gg'}$ = number of pairs (a_i, b_i) and (a'_i, b'_i) with $(a_i, b_i) \neq (a'_i, b'_i)$ and $(a_i, b_i) \neq (0, 0) \neq (a'_i, b'_i)$. In this notation, $r(g)\Lambda r g' = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} b' \\ a' \end{pmatrix} = \sum_i^n (a_i b'_i + b_i a'_i)$. $\implies r(g)\Lambda r(g') = n_{gg'}$.

On the other hand, $[g, g'] = gg' - g'g = (i^{n_{gg'}} - i^{-n_{gg'}}) \bigotimes X_{p_i}^{(i)} = 0 \iff i^{2n_{gg'}} = 1 \iff n_{gg'}$ even $= 0 \bmod 2$

$\iff r(g)\Lambda r(g') = 0 \bmod 2$. □

This together with another little proposition allows one to find the dimension of V_s.

Proposition 6
Let $S = \langle g_1, \ldots, g_l \rangle$ be generated by l independent generators and $-I \notin S$. Then $\exists$ $g \in G_n$ such that for a given $i \in \{1, \ldots, l\}, g g_i g^\dagger = -g_i$ and $g g_j g^\dagger = g_j \ \forall j \neq i$.

Proof.

Since the generators $g_1, \ldots, g_l$ are independent the rows of the check matrix R are linearly independent.

$\exists$ y $\in \mathbb{Z}_2^{2n}$, such that $Ry = e_i = \{0, .., 0_{i-1}, 1, 0_{i+1}, .., 0\}$. Define x by $x = \Lambda y \iff y = \Lambda x$, as $\Lambda^2 = I_{2n}$. $\implies \exists x \in \mathbb{Z}_2^{2n}$ such that $R\Lambda x = e_i$ for the given fixed e_i.

For a given row j of R, this means

$$r(g_j)\Lambda x = \begin{cases} 0, & j \neq i \\ 1, & j = i \, . \end{cases}$$

Since $x \in \mathbb{Z}_2^{2n}$, it also codes an element (without prefactor $\pm 1, \pm i$) of G_n, call it g, i.e. $r(g) = x^T$

$$\implies r(g_i)\Lambda r(g)^T = \begin{cases} 0, \iff [g_i, g] = 0 & j \neq i \\ 1, \iff [g_j, g] = 0 & j = i \end{cases} .$$

In the 1^{st} case $g_j g = g g_j \qquad | \cdot g$, use $g^2 = \boldsymbol{I} \iff g g_j g = g_j \qquad | g = g^\dagger$ for elements of G_n without prefactor $\pm i$

$\iff g g_j g^\dagger = g_j, \qquad j \neq i$

On the other hand if $[g_j, g] \neq 0 \implies \{g_j, g\} = 0$, i.e g_j, g <u>anti-commute</u>

$\implies g_i g = -g g_i \qquad$ (for $j = i$, already used) $\iff g g_i g^\dagger = -g_i$. $\square$

Proposition 13.1: Let S=$\langle g_1, \ldots, g_{n-k} \rangle$ be generated by n-k independent and commuting elements of G_n such that $-I \notin S$. Then V_s is a 2^k dimensional vector space.

Proof: For $X = (X_1, .., X_{n-k})$, define a projector

$$P^x = \frac{1}{2^{n-k}} \prod_{j=1}^{n-k} (\boldsymbol{I} + (-1)^{X_j} g_j) \qquad \text{(here } X_i \in \{0, 1\})$$

Note that $(\boldsymbol{I}+g_i)^2 = I + 2g_i + g_i^2 = 2(I+g_i)$ and $(I+g_i)(I-g_i) = I - g_i^2 = I - I = 0 \implies$ orthogonal projection. since all g_i commute, we have immediately that

$$P^x P^{x'} = \frac{1}{2^{2(n-k)}} \prod_{j=1}^{n-k} (\boldsymbol{I} + (-1)^{X_j} g_j)(\boldsymbol{I} + (-1)^{X'_j} g_j)$$

$$= \begin{cases} \frac{1}{2^{2(n-k)}} \prod_j 2(\boldsymbol{I} + (-1)^{X_j} g_j) = P^x, & \text{for } x = x' \\ 0, & \text{for } x \neq x' \end{cases}$$

i.e. $P^x P^{x'} = P^x \delta_{xx'}$, projector onto orthogonal subspaces for $x \neq x'$

For $X = 0$, we have $P^{(0\ldots0)} = P_1^{(1)} P_1^{(2)} \ldots P_1(n-k)$ where $P_{\pm1}^{(l)}$ projects onto the ±1 eigenspace of generator g_l. Thus, $P^{(0\ldots0)} = P_{V_s}$, the projector onto the common subspace V_s stabilized by all g_l.

Furthermore, according to proposition 6, for each e_i, $\exists g_{e_i} \in G_n$ such that $g_{e_i} g_j g_{e_i}^\dagger = g_j$ and $\forall j \neq i, \quad g_{e_i} g_i g_{e_i}^\dagger = -g_i$.

Thus,

$$g_{e_i} P^{(0\ldots0)} g_{e_i}^\dagger = \frac{1}{2^{n-k}} g_{e_i} P_1^{(1)} g_{e_i}^\dagger \ldots g_{e_i} P_1^{(i-1)} g_{e_i}^\dagger \overbrace{g_{e_i} P_1^{(i)} g_{e_i}^\dagger}^{\text{flip sign}} g_{e_i} P_1^{(i+1)} g_{e_i}^\dagger \ldots g_{e_i} P_1^{(n-k)} g_{e_i}^\dagger$$

$$= \frac{1}{2^{n-k}} P_1^{(1)} \ldots P_1^{(i-1)} P_{-1}^{(i)} P_1^{(i+1)} \ldots P_1^{(n-k)} = P^{0\ldots \overbrace{1}^{\text{pos i}} \ldots 0}$$

Continuing this process with g_{e_i} for each e_i such that $X_i = 1$, we can create any P^x.

$\implies g_x P^{(0\ldots0)} g_x^\dagger = P^x$ with $g_x = g_{e_1} \ldots g_{e_{n-k}} \implies \dim P^{(0\ldots0)} = \dim P^x$, as the g_x are unitary.

Finally,

$$\sum_{X=0}^{2^{n-k}-1} P^x = \frac{1}{2^{n-k}} \underbrace{\prod_{j=1}^{n-k} \sum_{X_j=0,1} (I + (-1)^{X_j} g_j)}_{2I} = I$$

$$\implies 2^{n-k} \dim P^x = 2^n \implies \dim P^x = \dim P^0 = 2^k$$

In summary, a set of $n-k$ independent commuting generators $g_i \in G'_n$ generate a subgroup S=$\langle g_1, \ldots, g_{n-k} \rangle$ of G_n that for $-I \notin S$ stabilizes a 2^k dim vectorspace V_s.

Unitary gates and the Stabilizer formalism

- How does the vectorspace V_s stabilized by $S \subset G_n$ evolve under unitary dynamics?
- What are the corresponding mapping of the elements of G_n in the Heisenberg picture?

The answer to the 1^{st} question is simple:

Let $|\psi\rangle \in V_s$. Then for any $g \in S$,

$U|\psi\rangle = Ug|\psi\rangle = UgU^\dagger|\psi\rangle$

$\Longrightarrow$ $U|\psi\rangle$ is stabilized by $UgU^\dagger$, with

UV_s " " " $USU^\dagger \equiv \{UgU^\dagger \,\|g \in S\}$

Note also that if S=$\langle g_1, \ldots, g_n\rangle$, then $USU^\dagger = \langle Ug_1U^\dagger, \ldots, Ug_nU^\dagger\rangle$ generated by all transformed generators.

For arbitrary U, in general $USU^\dagger$ may not be $< G_n$! However the stabilizer formalism turns out to be very powerful just due to the fact that for a large class of U's $USU^\dagger$ is $\subset G_n$. In such cases one gets a very compact and efficient description of a q-circuit, as one need not follow the gate of 2^n complex amplitudes but just the mappings of the elements of S (which can be———).

For example, let S=$\langle Z_1, .., Z_n\rangle$ $\Longrightarrow$ $V_s = |0\rangle^{\otimes n}$. Now apply a H on each qubit.

$$HXH^\dagger = Z, \quad HYH^\dagger = -Y, \quad HZH^\dagger = X$$

as is seen e.g. by direct multiplication.

$\Longrightarrow$ $USU^\dagger = \langle X_1, .., X_n\rangle$, and $UV_s = |+\rangle^{\otimes n}$, which contains 2^n amplitudes in the computational basis. Still one might argue that $|+\rangle^{\otimes n}$ is just as compact a description of the final state. Howeverm it turns out that the stabilizer formalism can also describe certain entangled states, as $|C_{12} = CNOT$ also transforms $G_n \to G_n$:

$$C_{12} \underbrace{X_1}_{\equiv X_1 \otimes I_2} C_{12}^\dagger = X_1 \otimes X_2$$

Other useful mappings are:

U	Input	Output
C_{12}	X_1	X_1X_2
	X_1	X_2
	Z_1	Z_1
	Z_1	Z_1Z_2
H	X	Z
	Z	X

U	Input	Output
X	X	X
	Z	-Z
Y	X	-X
	Z	-Z
Z	X	-X
	Z	Z
S	X	Y
	Z	Z

Use S=$\begin{pmatrix} 1 & \\ & i \end{pmatrix}$, the phase matrix.

Other mappings can be found from this table, e.g. $Y_1 = iX_iZ_i \implies UY_1U^\dagger - iUX_1U^\dagger UZ_1U^\dagger$, e.g. $U = C_{12}$

$C_{12}Y_1C_{12}^\dagger = iX_1 \otimes X_2.Z_1 = iX_1Z_1 \otimes X_2 = Y_1X_2$

Following the fate of the elements of G_n can be an alternative way of following through the action of a q-circuit in fact, for this it is enough to follow the facts of $\{\boldsymbol{I}_i, X_i.., Z_i\}_{i=1...,n}$ for each qubit, i.e. 3n operators, where in addition $\boldsymbol{I}_i$ are mapped trivially $UI_iU^\dagger = I_i$. So one only needs to map 2n operators $\{X_i, .., Z_i\}_{i=1..n}$.

Propositions: $\forall \quad R \in \{X_i, \ldots, Z_i\}_{i=1,..,n}$ we have for 2 unitaries U,V that $URU^\dagger = VRV^\dagger$, then U=V.

Proof :"$\Longleftarrow$" trivial

"$\Longrightarrow$" From $UX_iU^\dagger = VX_iV^\dagger$ and $UZ_iU^\dagger = VZ_iV^\dagger$

$\implies$ also $UY_iU^\dagger = VY_iV^\dagger$(as $Y_i = iX_iZ_i$)

And e.g. $UX_1 \otimes X_2U^\dagger = U \underbrace{X_1 \otimes I_j}_{j \neq 1} \otimes I_J \underbrace{\otimes}_{j \neq 2} X_2U^\dagger$

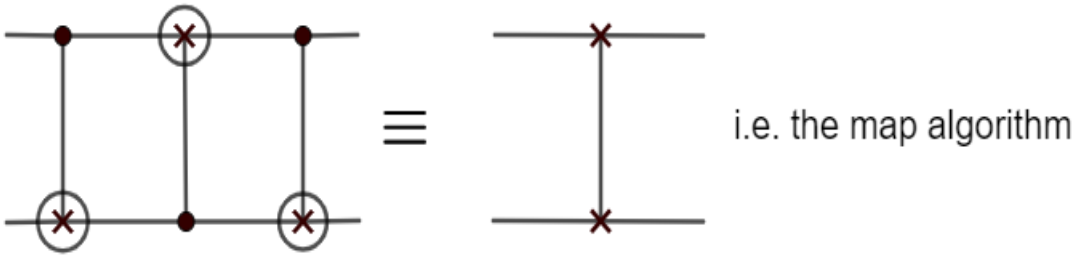
$=UX_1U^\dagger.UX_2U^\dagger = VX_1X_2V^\dagger$

$\implies URU^\dagger = URU^\dagger$
$forall\ R \in \{\boldsymbol{I}, X, Y, Z\}^{\otimes n}$, and since this ——- set is a complete basis of all density matrices acting on —— $\implies$ the 2q-circuit agree.

Example of application:

Show that

Proof:



$X_1 \xrightarrow{C_{12}} X_1X_2 \xrightarrow{C_{21}} X_1.X_1X_2 = X_2 \xrightarrow{C_{12}} X_2$

$X_2 \to X_2 \to X_1X_2 \qquad \xrightarrow{C_{12}} X_1X_2X_2 = X_1$

$Z_1 \xrightarrow{C_{12}} Z_1 \xrightarrow{C_{12}} Z_1Z_2 \qquad \xrightarrow{C_{12}} Z_1Z_1Z_2 = Z_2$

$Z_1 \to Z_1Z_2 \to Z_1Z_2Z_2 = Z_1 \qquad \xrightarrow{C_{12}} Z_1$

So $\{X_1, Z_1\} \leftrightarrow \{X_2, Z_2\}$, which is clearly the action of the swap gate on these operator $\implies$ the 2-q-circuits are identical.

However, not all unitaries can be described by the stabilizer formalism, in fact most cannot, even though the fact that the CNOT can, implies that non-trivial and in particular entanglement generating matrices can be described by the stabilizer formalism.

Theorem : Let u be any unitary operator s.t. $\forall\ g \in G_n \implies UgU^\dagger \in G_n$. Then up to a global phase, U maybe composed from $O(n^2)$ Hadamand phase, and CNOT gates.

Definition 20
The set $\{U|\forall\ g \in G_n, UgU^\dagger \in G_n\}$ *is called the ——- * $N(G_n)$ *of* G_n*. It is also called the Clifford group.*

We first show that $N(G_n)$ is indeed a group(with regular matrix multiplication as group operation).

Proof :

- $U_1, U_2 \in N(G_n) \implies U_igU_i^\dagger \in G_n \forall g \in G_n$
  $\implies U_1(U_2gU_2^\dagger)U_1^\dagger = U_1\tilde{g}U_1^\dagger \in G_n$ as $\tilde{g} = U_2gU_2^\dagger \in G_n \implies U_1U_2 \in G_n$
- $U_1(U_2U_3) = (U_1U_2)U_3$ by associativity of matrix multiplication.

- $\exists\ I$ with $UI = U$
- $\exists\ U^{-1} \forall U \in G_n$, s.t. $U^{-1}U = I$ with $g_1 \neq g_2 \implies Ug_1U^\dagger \neq Ug_2U^\dagger$ by using $U^{-1} = U^\dagger$ with assumption of $U^{-1} \in N(G_n)$. So U must map all $g_i \in G_n$ to difficult $g_i \in G_n \implies U \equiv$ permutation $\implies$ it has an inverse.

Second, we realize that the $g_i \in G_n$ are $\in N(G_n)$, as $g_i g g_i^\dagger = g_i g g_i \in G_n$ by definition of the propagator $G_n = \{g_i\} \forall g \in G_n \implies G_n \subseteq N(G_n)$

Third, not all mappings of $g \in G_n$ to another $g' \in G_n$ are possible. Suppose e.g.$UXU^\dagger = iX, UXU^\dagger = -iX \implies UXU^\dagger = 0$ { to $detX = det(UXU^\dagger) = -1$

Proof of theorem :

- First consider all normalizing operators on a single qubit i.e. U s.t $UXU^\dagger = X' \in G_1 \forall X \in G_1$. ——— $U = \exp i\alpha.sigma, \alpha \in \boldsymbol{R}^3$, one shows that U leads to a notation of the "Bloch Vector" i.e. for $X = n_i X_i \quad i = 1, 2, 3$ we have also $X' = n_i' X_i$, and by direct calculation

$$\boldsymbol{n} = \cos 2|\alpha|\boldsymbol{n} + \sin 2|\alpha|\boldsymbol{n} \times \hat{\alpha} + 2\sin^2|\alpha|(\boldsymbol{n}.\hat{\alpha})\hat{\alpha}$$

  This is a proper rotation about axis $\hat{\alpha}$ with rotation angle $|\alpha| : \boldsymbol{n'}.\boldsymbol{\alpha} = \boldsymbol{n}.\alpha$, in particular sign($\boldsymbol{n'}.\boldsymbol{\alpha}$)=sign($\boldsymbol{n}.\boldsymbol{\alpha}$), whereas for an improper rotation (rotation followed by inversion), the sign would be opposite.

  $\implies \{X, Y, Z\}$ are mapped by a rotation matrix R with detR=1. Since at the same time this rotation must be a ——- up to ± 1 signs ($\boldsymbol{n'} \in \boldsymbol{R}^3$ for $\boldsymbol{n} \in \boldsymbol{R}^3$!), we only have other 1 component fixed

$$\implies R_1 = \begin{pmatrix} 0 & \mp 1 & \\ \pm 1 & 0 & \\ & & 1 \end{pmatrix} = iY \text{ or } R_2 = \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix} = R_1^2 (\text{ rotation}$$

  about Z by angle $\pm\frac{\pi}{2}$ or π; correspondingly for rotation about X or Y axis)

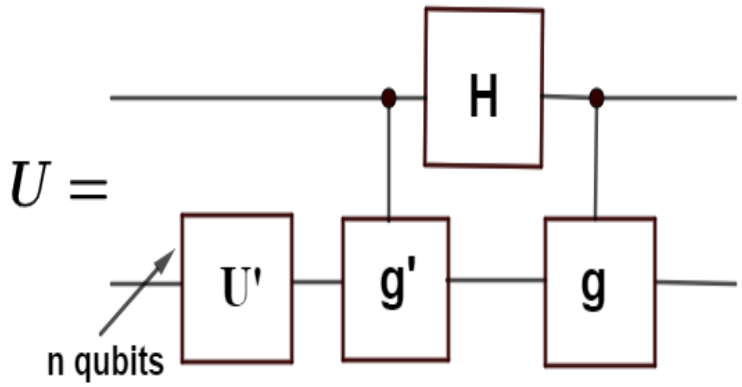
  or 0 component fixed

$$\implies R_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \text{ or } R_4 = R_3^2 \iff \text{rotation about space diagonal}$$

  $(1,1,1)/\sqrt{3}$, angle $\frac{2\pi}{3}$

  All of these have $detR_i = +1$, and these are all permutation matrices (upto signs, with detR=+1) of 3———. Furthermore,

  R_1 is created by S:$X \to Y, Y \to -X, Z \to Z$



R_3 is created by SH: $SHX(SH)^\dagger = Z, SHY(SH)^\dagger = X, SHZ(SH)^\dagger = Y$

So S and H suffice to generate N(G_n)

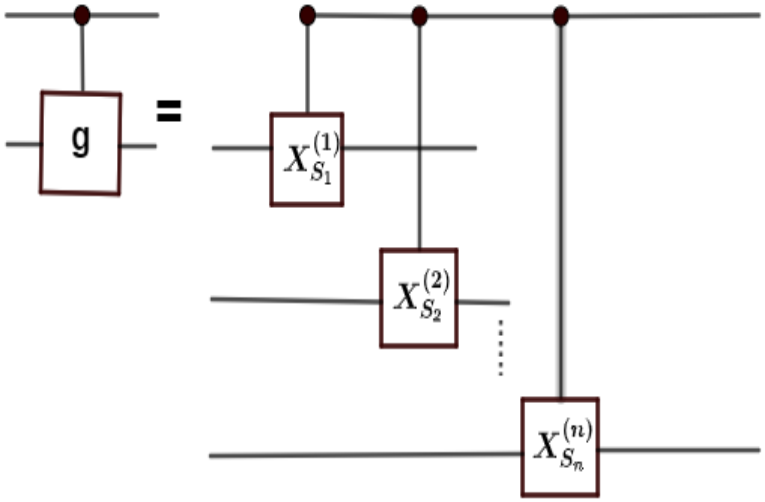
- Consider the q-circuit

with $U' \in N(G_n),\ g, g' \in G_n$. One easily checks that U performs the following transformations of the input states $|0\rangle |\psi\rangle$ and $|1\rangle |\psi\rangle$, where $|\psi\rangle$ is initial state. If the n lower qubits:

$U |0\rangle |\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle U' |\psi\rangle + |1\rangle gU' |\psi\rangle$

$U |1\rangle |\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle g'U' |\psi\rangle - |1\rangle gg'U' |\psi\rangle)$

$\implies \sqrt{2} \langle 0| U |0\rangle |\psi\rangle = U' |\psi\rangle$, which connects U and U'. Now determine how U transforms $Z_1 = (|0\rangle \langle 0| - |0\rangle \langle 0|) \otimes \boldsymbol{I}_n$:



$UZ_1 \otimes \boldsymbol{I}_n U^\dagger = \sum_{s=0}^{2^n-1} UZ_1 \otimes |s\rangle \langle s| U^\dagger, \quad |s\rangle$ computational basis state.

$$= \sum_s U|0\rangle |S\rangle \langle S| \langle 0| U^\dagger - \sum_s U|1\rangle |S\rangle \langle S| \langle 1| U^\dagger$$

$$= \frac{1}{2}\sum_s \Big\{ \Big(|0\rangle U'|S\rangle + |1\rangle gU'|S\rangle\Big)\Big(\langle 0| \langle s| U^\dagger + \langle 1| \langle S| U^\dagger g\Big) - \Big(|0\rangle g'U^\dagger |S\rangle - |1\rangle gg'U'|S\rangle\Big)\Big(\langle 0| \langle S| U'^\dagger g' - \langle 1| \langle S| U'^\dagger gg'\Big)\Big\}$$

$$= \frac{1}{2}\Big\{ |0\rangle \langle 0| \Big(\underbrace{U'\boldsymbol{I}_n U'^\dagger}_{\boldsymbol{I}_n} - \underbrace{g'\boldsymbol{I}g'}_{\boldsymbol{I}_n}\Big) + |0\rangle \langle 1| \Big(U'\boldsymbol{I}_n U'^\dagger g + g'U'\boldsymbol{I}_n U'^\dagger g'g\Big) +$$

$$|1\rangle \langle 0| \Big(U'\boldsymbol{I}_n U'^\dagger + gg'\boldsymbol{I}_n g'\Big) + |1\rangle \langle 1| \Big(g\boldsymbol{I}g - gg'U'\boldsymbol{I}_n U'^\dagger g'g\Big)\Big\} = \Big(|0\rangle \langle 1| + |1\rangle \langle 0|\Big)g = X_1 \otimes g$$

Similarly one shows that $UX_1 \otimes \boldsymbol{I}_n U^\dagger = Z_1 \otimes g'$. Thus, U maps any $g \in G_1$ acting on the 1^{st} qubit on a $\tilde{g} \in G_{n+1}$. Thus, if $U' \in N(G_n)$ (i.e. maps $g \in G_n$ to $g \in G_n$) $\implies$ $U \in N(G_{n+1})$, as $UZ_1 \otimes g_n U^\dagger = UZ_1 \otimes \boldsymbol{I}_n . \boldsymbol{I}_n \otimes g_n U^\dagger = UZ_1 \otimes \boldsymbol{I}_n U^\dagger U \boldsymbol{I}_2 \otimes g_n U^\dagger = \Big(Z_1 \otimes g'_n\Big)\Big(\boldsymbol{I}_2 \otimes U' g_n U^\dagger\Big) == \Big(Z_1 \otimes g'_n\Big)\Big(\boldsymbol{I}_2 \otimes g''_n\Big) = Z_1 \otimes g'_n g''_n = Z_1 \otimes g'''_n \in G_{n+1}$ and correspondingly for $X_1 \otimes g_n$.

Since all elements of G_{n+1} are generated from $\{X, Z\} \otimes G_n$, the q-circuit U does generate the full $N(G_{n+1})$ if U' generates the full $N(G_n)$.

- Number of gates

here upto a phase $X_{S_n}^{(i)} \in \{X, Y, Z\}$. But $Z = S^2$, $Y = iXZ$ and $X = HZH = HS^2H$

$C - X = C$

So $C - Y = iC - XZ = iCS^2 (C = CNOT)$

$C - Z = HCH$

$\Longrightarrow$ $C - X_{s_i}^(i)$ can be decomposed from at most 3 gates $\in \{C, S, H\}$.

$\Longrightarrow$ for n qubits, $C - g$ is implemented with $\leq$ 3n gates $\in \{C, S, H\}$ $\Longrightarrow$ U implemented with $N(G_{n+1} \leq G_{n+1} + N(G_n))$ gates

$\Longrightarrow$ Complete ——— allows to conclude that $N(G_n)$ can be implemented with

$N(G_n) \leq 6 \sum_{j=1}^{n} j + n = 6\frac{n}{2}(n+1) + n = 3n^2 + 4n = O(n^2)$

gates $\in \{S, H, CNOT\}$!

Examples of gates that are not in $N(G_n)$ include the ———- gate U_T(=doubly controlled CNOT), and the $\frac{\pi}{8}$ gate T. One checks that $TXT = \frac{X+Y}{\sqrt{2}} \notin G_1$ and $UX_1Y^\dagger = X_1 \otimes \frac{1}{2}(I + Z_2 + X_3 - Z_2X_3) \notin G_3$

Measurement and state preparation in the stabilizer formalism

Suppose one measures an operator $g \in G_n$ on the n-qubit. Assume here that $g = \pm >>> \otimes_{i=1}^{n} X_{s_i}^{(i)}$. i.e. with phase factor $\pm i$, such that $g = g^\dagger$, and we can ——— indeed g as a legitimate measurement operator.

Note that this includes measurement in computational basis ($\rightarrow$ an ensemble of measurement operator $\{Z_i\}$, not $Z_1 \otimes \ldots \otimes Z_n$: n outcomes , not(!).

Let the system be in $|\psi\rangle$ stabilized by $S = \langle g_1, \ldots, g_n \rangle$. Can the post-measurement state $|\psi\rangle$ still be described by stabilizer, and if so which one?

The answer to the 1^{st} question is :YES!

There are two cases

- g commutes with all generators of S So $g_j g |\psi\rangle = g g_j |\psi\rangle = g |\psi\rangle \ \forall \ g_j \in S \Longrightarrow g |\psi\rangle \in V_s$, as it is stabilized by g_j. Now for $g \in G_n$ and $g = g^\dagger$, $g^2 = I \Longrightarrow g |\psi\rangle = \pm |\psi\rangle \Longrightarrow$ either g or $-g \in S$. (not both as $-\boldsymbol{I} \in S$!)

  If $g \in S \Longrightarrow g |\psi\rangle = |\psi\rangle$, with the measurement of g yields the result $+1$ with probability 1 and does not disturb the state $\Longrightarrow$ S left invariant.

If $-g \in S \implies g|\psi\rangle = -|\psi\rangle$, with the measurement of g yields the result -1 with probability 1, and state undisturbed $\implies$ S left invariant as well (-g$\in$ S!)

- g anti-commutes with one or more generators of S

  Suppose $\{g, g_l\} = 0$ whereas $[g, g_j] = 0 \; \forall j = 2, .., n$. In fact if also $\{g, g_2\} = 0$, then $[g, g_1, g_2] = gg_1g_2 - g_1g_2g = -g_1gg_2 - g_1g_2g = g_1g_2g - g_1g_2g = 0$, we can replace g_2 by g_1g_2 in the list of generator (which does not change S, since $g_1.g_1g_2 = g_2$ gives back g_2) and then have that g only anti-commutes with g_1.

Since $g^2 = \boldsymbol{I}$, g has eigenvalues ± 1, and the projectors onto the corresponding eigenstates are $\frac{\boldsymbol{I} \pm g}{2} \implies$ The probabilities for finding ± 1 are given as

$P(\pm 1) = tr(\frac{\boldsymbol{I} \pm g}{2}|\psi\rangle\langle\psi|) = tr(\frac{\boldsymbol{I} \pm g}{2} g_1|\psi\rangle\langle\psi|) = tr(g_1\frac{\boldsymbol{I} \mp g}{2}|\psi\rangle\langle\psi|) = tr(\frac{\boldsymbol{I} \mp g}{2}|\psi\rangle\langle\psi|) = P(\mp 1) \implies P(+1) = P(-1) = \frac{1}{2}$

If the result $+1$ is found, the new state of the ——— is $|\psi^+\rangle = (\boldsymbol{I} + g)|\psi\rangle / \sqrt{2}$, which has stabilizer $\langle g, g_2, \ldots, g_n\rangle$. If the result -1 is found the new state is $|\psi^-\rangle = (\boldsymbol{I} - g)|\psi\rangle / \sqrt{2}$.

So in both the cases, we have again a stabilizer state, and the stabilizer is updated to $\langle \pm g, g_2, .., g_n\rangle$

The Gottesman-Knill Theorem

Theorem: A q-operator involving only state preparation in the computational basis, Hadamard gates, phase gates, CNOT gates, Pauli gates, and measurement of g$\in G_n$ (including measurement in the computational basis, by $Z_i, i = 1, .., n$) can be efficiently simulated on a classical computer.

Proof: The initial computational basis state in stabilized by the set $\pm Z_{ii=1..n}$ with $+Z_i$ if $|0\rangle$, $-Z_i$ if $|1\rangle$ for qubit i.e. the initial state is a stabilizer state. All other operations listed transform stabilizer states into stabilizer states, i.e. we can follow the dynamics by updating the list of stabilizer in each step. For this we have seen it is enough to update the list of generator of the stabilizer in each step. Furthermore one shows that for a group of order N, there are at most $\log_2 N$ independent generators.

Suppose that for a set of generators $g_1, \ldots, g_l$ of a subgroup S , $g \notin \langle g_1, \ldots, g_l\rangle \equiv S$, but $f \in S$

$\implies$ $fg \notin S$, as otherwise $g = f^{-1}fg \in S \implies (f^{-1} \in S$ as this is a subgroup, thus with $f \in S \implies f^{-1} \in S) \implies \forall f \in S, \exists fg \in \langle g_1, \ldots, g_l, g\rangle$ but

not $\in S$, i.e. with every generator added the size of the subgroup doubles at least.

$\implies \exists$ at most $\log_2 N$ independent generators.

Here we have $N = 4^{n+1}$ (Pauli group) $\implies \exists$ at most $2(n+1)$ independent generators of G_n.

$\implies$ In each step of the q-computation one only needs to update a list of at most $2(n+1)$ elements $\implies$ Such a q-algorithm with 'm' steps can be ——— with at most $m.4(n+1)^2$ generators.

$\implies$ This can be done efficiently on a classical computer. This implies that many q-algorithms that generate highly entangled states can be efficiently simulated on a classical computer.

There is also a more general statement by Jozsa and Linden which ——— says that a q-algorithm that produces only pure state entanglement of the cluster of qubits bounded in size can be efficiently simulated on a classical computer[*Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 459(2036), 2011-2032*]

Construction of stabilizer q-EC codes

Definition 21
Stabilizer Code

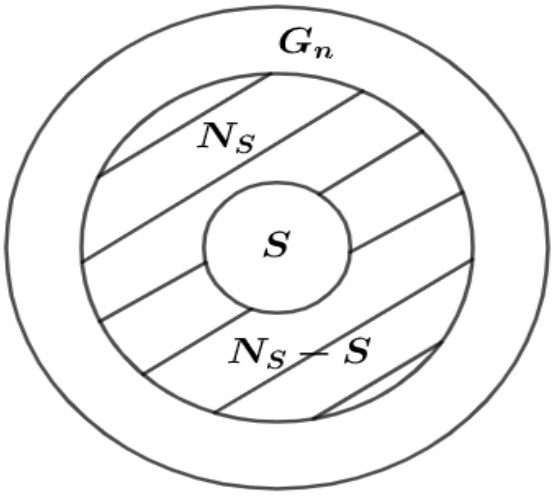
Theorem 28.1: (Error correction condition for stabilizer codes)

Let S be the stabilizer for a stabilizer code C(S). Suppose $\{E;\}$ is a set of operator in G_n such that $E_j^\dagger E_k \notin N(S) - S$ for all j and k, where $N(S) = \{E \in G_n | EgE^\dagger \in S \forall g \in S\}$ is the "normalizer" of S in G_n. Then $\{E_j\}$ is a set of correctable errors for the code C(S).

Note used with notation V_s for C(S). In any case, $C(S) \implies \{|\psi\rangle\, |g\,|\psi\rangle\, \forall g \in S\}$

Proof: We first show $S \subseteq N(S)$ for any subgroup $S = \langle g_1, .., g_{n-k}\rangle$ of G_n generated by $g_i, i = 1, .., n-k$.

So let $E \in S \implies E = \prod_i g_{l_i}$, and —— —— $g \in S, g = \prod_j g_{k_j} \implies EgE^\dagger = \prod g_{l_i} \prod g_{k_j} \prod g_{l_i}^\dagger = \prod g_{k_i}$ is still a product of generator of S $\forall g \in S$ and thus $EgE^\dagger \in S \implies E \in N(S)$. So$E \in S \implies E \in N(S) \implies S \subseteq N(S)$. So we have a structure



So if $E_j^\dagger E_k \notin N(S) - S \implies E_j^\dagger E_k \in S$ or $E_j^\dagger E_k \in G_n - N(S)$. Let P be the projector onto code C(S).

Consider 1_{st} case:

$PE_j^\dagger E_k P = P$ since P is invariant under multiplication of elements of S, and $E_j^\dagger E_k \in S$. So $PE_j^\dagger E_k P \propto P$, and the QEC condition is satisfied.

Consider 2_{nd} case:

$E_j^\dagger E_k \in G_n - N(S)$. Since the E_j are $\in G_n$ they either commute or anticommute with all elements of S since they are also in G_n (i.e. tensor products of Pauli matrices). If $E_j^\dagger E_k$ commuted with all $g \in S \implies E_j^\dagger E_k \in N(S)$, but since $E_j^\dagger E_k \notin N(S) \implies$ it must anti-commute with some element g of S.

The projector P can be written explicitly

$$P = \frac{\prod_{l=1}^{n-k}(I + g_l)}{2^{n-k}}$$

remember that the — of g_l are $\in \{\pm 1\}$, so $I + g_l$ has — 0 0r 1, so does the product, and $\frac{I+g_l}{2^{n-k}}$ has thus — $\in \{0, 1\}$ and is thus a projector onto C(S))

$\implies E_j^\dagger E_k P = (I - g_1) E_j^\dagger E_k \frac{\prod_{l=2}^{n-k} I+g_l}{2^{n-k}}$ due to anti-commutativity of g_1 with $E_j^\dagger E_k$ (whereas all g_l commute).

$(I+g_l)(I-g_l) = I^2 - g_1^2 = I - I = 0 \implies P(I-g_1) = 0$(as P contains $(I+g_l)$ as a factor and all factor commute)

$\implies PE_j^\dagger E_k P = 0 \implies$ QEC conditions are satisfied as well. $\implies \{E_j\}$ is a set of correctable error.

Intuitively this means that we can correct errors $E \in G_n$ that would take us outside S (namely into $G_n - N(S)$, where E anti-commutes with at least one $g_i \in S$, taking C(S) to an orthogonal subspace). If $E \in S$ than E has no effect an C(S) at all, as it is also a stabilizer.the problematic E_s are thus only those $E \notin S$ that nevertheless commute with all $g \in S$,i.e. $\in N(S) - S$, which is why they are excluded in the theorem.

Proposition: If a product of error $E_j^\dagger E_k$ commutes with at least one element $g \in S \implies E_j^\dagger E_k \notin N(S) - S$

Proof: Normalizer N(S)=$\{E \in G_n | EgE^\dagger \in S \forall g \in S\}$. Suppose $\exists g \in S$ s.t. $\{E_j^\dagger E, g\} = 0 \iff E_j^\dagger E_k g + g E_j^\dagger E_k = 0 \implies E_k^\dagger E_j \implies (E_j^\dagger E_k) g (E_j^\dagger E_k)^\dagger = -g \underbrace{(E_j^\dagger E_k)(E_j^\dagger E_k)^\dagger}_{=+\mathrm{I}}$

Note that $\forall E \in G_n EE^\dagger = +I$(whereas $E^2 = \pm I$, due to possible prefactor $\pm i$, which make $E^\dagger = \pm E$). Now with $g \in S \implies -g \notin S$. For suppose that both $g, -g \in S \implies -g^2 \in S$. But $g^2 = +I$, since $-I \in S \implies -g^2 = -I \in S \implies$ to definition that $-I \in S$. So now $EgE^\dagger = -g \notin S$ with $E = E_j^\dagger E_k$, so $E_j^\dagger E_k \notin N(S)$ and thus $\notin N(S) - S$.

So in order to show that a st of error $\{E_j\}$ is correctable it is enough to show that either all $E_j^\dagger E_k \in S$ or $\{E_j^\dagger E_k, g\} = 0$ for ar least one $g \in S$ (which may depend on E).

Theorem 28.1 motivates the definition of the distance for a stabilizer code.

Def: The weight of an error $E \in G_n$ is the number of the —— in the tensor product that are $\notin I$. E.g. $X_1 Y_4 Y_5 Z_8$ has weight 4. the distance d of a stabilizer code C(S) is the minimum weight of an element $g \in N(S) - S$. An $[n, k]$ code C(S) is then called a $[n, k, d]$ code.

Proposition: A $[n, k, 2t+!]$ stabilizer code can correct arbitrary errors on upto t qubits.

Proof: let $\xi_t \equiv \{E_j | \mathrm{wt}(E_j) \leq t\}$ be the set of all errors on up to t qubits. Then $E_j^\dagger E_k$ with $E_j, E_k \in \xi_t$ is an error with error or up to 2t qubits. But since the minimum weight of $g \in N(S) - S$ for an $[n, k, 2t+1]$ code is 2t+1,

it follows that $E_j^\dagger E_k \notin N(S) - S \forall E_j, E_k \in \xi_t \implies \xi_t$ is a set of correctable error.

Ex: 10.45 in N.C.

Construction of code-words for a stabilizer code

For an $[n,k]$ stabilizer code we know that all $|\psi\rangle \in C(S)$ are stabilized by $g_1,..,g_{n-k}$. this leaves an 2^k dim subspace in which we could just choose as many basis states. In practice, one complements the $g_1,..,g_{n-k}$ by k logical Pauli matrices $\bar{Z}_j, j = 1,..,k$ whose eigenvalues determines together with the $g_1,\ldots,g_{n-k}$ the code-words uniquely.

i.e. one adds additional stabilizer, $(-1)^l\bar{Z}_1,\ldots,(-1)^k\bar{Z}_k$ to the set $\{g_1,\ldots,g_k\}$, such that the full set $\{g_1,\ldots,g_{n-k}(-1)^{\bar{Z}_1}\bar{Z}_1,\ldots,(-1)^{\bar{Z}_k}\bar{Z}_k\}$ is till an independent and commuting set $\forall\{\bar{Z}_1,\ldots,\bar{Z}_k\}$ and forms a complete set of observables, i.e. a given logical computational basis state $|\bar{Z}_1,\ldots,\bar{Z}_k\rangle$ is stabilized and uniquely determined by the $\bar{Z}_i \in \{\pm 1\}$.

So $\bar{Z}_j|\psi\rangle = (-1)^{\bar{Z}_j}|\psi\rangle$, if $|\psi\rangle$ is stabilized by $\{(-1)^{\bar{Z}_j}\bar{Z}_j\}$, i.e. $(-1)^{\bar{Z}_j}\bar{Z}_j|\psi\rangle = |\psi\rangle$.

In addition, one also may introduce other logical operator such as $\bar{X}_j$, which flips logical qubit j. This implies immediately the name commutation relations for the $\bar{X}_j,\bar{Z}_j$ (and $\bar{Y}_j = i\bar{X}_j\bar{Z}_j$ as for the standard physical operator X_j,Y_j,Z_j

Example: 1) The 9-qubit Shor code

$|0\rangle_L = \frac{1}{2\sqrt{2}}(|000\rangle+|111\rangle)^{\otimes 3}$, $|1\rangle_L = \frac{1}{2\sqrt{2}}(|000\rangle-|111\rangle)^{\otimes 3}$

Recall that we can detector but — error by Z_1Z_2, Z_2Z_3, etc, and phase. Flip error by $X_1\ldots X_6,\ X_4\ldots X_9$. So we can take these operator as generator of the stabilizer.

$g_1 = ZZIIIIIII$

$g_2 = IZZIIIIII$

$g_3 = IIIZZIIII$

$g_4 = IIIIZZIII$

$g_5 = IIIIIIZZI$

$g_6 = IIIIIIIZZ$

$g_7 = XXXXXXIII$

$g_8 = IIIXXXXXX$

There is only operator $\bar{Z}$, as we have only one logical qubit. Can set $\bar{Z} = XX$, as $\bar{Z}|0\rangle_L = |0\rangle_L$, $\bar{Z}|1\rangle_L = -|1\rangle_L$

So $|0\rangle_L$ is established by $\bar{Z}$, $|1\rangle_L$ by $-\bar{Z}$.

For $\bar{X}$, can use $\bar{X} = Z \quad Z$ ZZZ$(|000\rangle + |111\rangle) = |000\rangle - |111\rangle$, So $\bar{X}$ indeed acts as $\bar{X}\,|0\rangle_L = |1\rangle_L$ logical bit flips. Note that given just $g_1, \ldots, g_8$ arbitrary —— of $|0\rangle_L, |1\rangle_L$ would have still been possible as logical states 0 and 1, with correspondingly different $|Z\rangle$ and $|X\rangle$. the independence of $\bar{Z}$ and the $\{g_i\}$ can be shown with the check matrix $(r(\bar{Z}) = \underbrace{1\ldots1}_{g}\ \underbrace{0\ldots0}_{g})$. Note that since Shor's code is a $[9,1,3]$ code, $n = 9, k = 1 \implies$ 8 generators $g_1, \ldots, g_{n-k}$. Note that $\bar{X}$ and $\bar{Z}$ cannot, be chosen simultaneously in the set of generators as they anticommute.

Example: 2) The five qubit code Hamming bound or singleton bound $\implies$ at least n=5 physical qubits are needed to note k=1 logical qubit on which any error can be connected (t=1)

$\implies n - k = 4$ generators g_i needed that commute, are independent, and lead to a normalizer N(S) with ——- wt(t)≥ 3.

Such a code was found (through a different approach, namely entanglement purification + ——— search) by Bennett, ———,——- and ————————————-, and through more systematic approach exploiting orthogonality relation by ——— -, ————————————-. Still another version is described in ———- and ————:

$g_1 = IZXXZ, g_2 = ZIZXX, g_3 = XZIZX, g_4 = XXZIZ$

- We check easily that $g_i^2 = I, i = 1, \ldots, 4$ as no generator contains a prefactors i.
- $[g_i, g_i] = 0\ \forall i, j$

  e.g.$[g_1, g_2] = IZXXZ.ZIZXX - \underbrace{ZIZXX.IZXXZ}_{\equiv Z}$

  $= ZZ\underbrace{(XZ)}_{=-iY} I \underbrace{(ZX)}_{=iY} - ZZ\underbrace{(ZX)}_{=iY} I \underbrace{(XZ)}_{=-iY} = ZZYIY - ZZYIY = 0$

We see that there are always two pairs X,Z and Z,X that ———-. Now can contract the logical basis states by projecting successively onto the +1 eigenspaces of the g_i

stating from either $|0000\rangle$ or $|1111\rangle$:

$$\begin{aligned}|0\rangle_L &= \frac{1}{4}(I+g_1)(I+g_2)(I+g_3)(I+g_4)\,|0000\rangle \\ &= \frac{1}{4}(|00000\rangle + |11000\rangle + |01100\rangle + |10001\rangle - |10100\rangle - \\ &\quad |01010\rangle - |00101\rangle - |10010\rangle - |01001\rangle - |11110\rangle - \\ &\qquad\qquad |01111\rangle - |10111\rangle - |11011\rangle - |11101\rangle)\end{aligned}$$

and $|1\rangle_L$ is obtained by flipping all bits.

Example: 3) CSS order

Let C_1, C_2 be $[n, k_1]$ and $[n, k_2]$ classical linear codes respectively with $C_2 \subseteq C_1$ and both C_1 and $C_2^\dagger$ both correct t error. Define check matrix R that determines the generator generally as

$$R = \left(\begin{array}{c|c} H(C_2^\dagger) & 0 \\ 0 & H(C_1) \end{array}\right)$$

where $H(C_2^\dagger), H(C_1)$ are the parity check matrices of $C_2^\dagger$ and C_1. We had that all bases of these have to be basically independent for a classical linear code, which implies immediately that the sets of generators $g_1, \ldots, g_{k_1}$ coded by the k_1 first bases $r(g_1) \ldots r(g_{k_1})$ of R and thus containing only X are independent, and correspondingly for the generators coded by the k_1 last bases, containing only Z's. However, we have

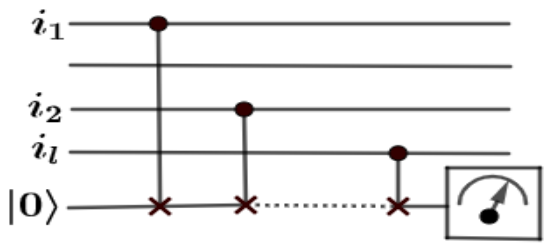
$r(g)\Lambda r(g') = H(C_2^\dagger)_g . H(C_1)_{g'} = (H(C_2^\dagger)H(C_1)^T)_{gg'} \stackrel{T}{=} (H(C_1)H^T(C_2^\dagger))_{g'g} = 0$, as $C_2 \subset C_1$

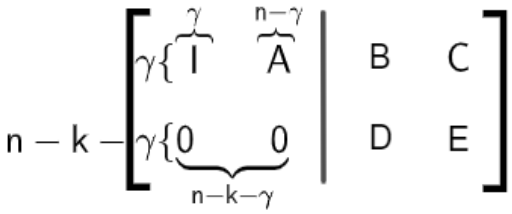
So also the generator g, g' are all independent and therefore can generate a stabilizer code.

Now recall that measuring a stabilizer $Z_{i_1}, Z_{i_2} \ldots, Z_{i_l}$ can be done by writing the result 0 or 1 into another bit. If $|X\rangle$ is a code -word, then

$$\underbrace{(Hx)_g}_{\text{value of bit number g after action of k}} = \underbrace{H(g).X}_{\text{line number g}} = \text{number of —— of ——- of X in bits}$$

where H has 1s. If that number is —— $\Longrightarrow$ $(HX)_0 = 0$, and it the same time even number of bit flips of ——— bit $\Longrightarrow$ ——$= |0\rangle$ iff $(Hx)_g = 0$ and thus we measure the error syndrome of $r(g)$ coded in the corresponding line of R(i.e. Z's where has 1s). Correspondingly with q-circuit containing additional H's before and after the CNOTs on the controls.



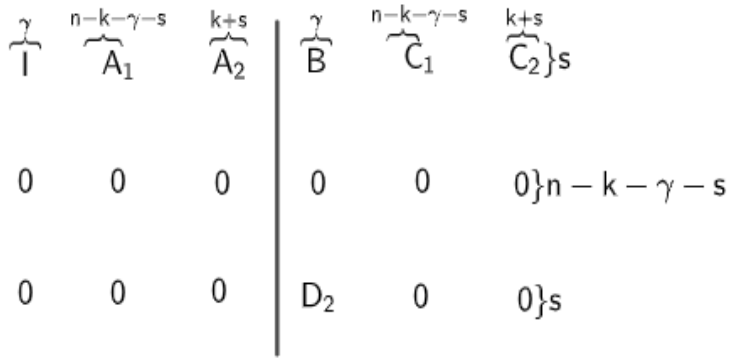


So we see that measuring the error syndrome is equivalent to the calculation of $|H(C_1)X\rangle$ for $|X\rangle$ in the ——- register, and correspondingly for $|H(C_2^\dagger)X\rangle$, one error syndrome corresponding to one ——— bit at a time. Since the CSS(C_1, C_2) code was defined aas the code such that all these error syndromes of C_1 and $C_2^\dagger$ are 0, this stabilizer code is exactly the CSS(C_1, C_2) code. It remains to find encoded $Z($ and possibly X) operator. For this one brings the check matrix R to a standard form: Let $R = \begin{pmatrix} R_1 & | & R_1 \end{pmatrix}$ for a [n,k] stabilizer code C. Let γ be the ran of R, R has $n-k$ rows. Multiplying generator onto iher corresponds to adding rows and does not change C. Swapping columns in parallel in R_1, R_2 corresponds to swapping ——. With this one can do Gauss elimination without changing C obtaing a form ————. In addition create identity matrix $I_{\gamma\times\gamma}$, which ——— occurrence into r, —— columns.

Similarly one can now do Gaussian elimination on E. Working in parallel on columns of A and C, but not touching E, is ——- with this we ——- the E block correspondingly into

$\Longrightarrow$ I is $n-k-\gamma-s \times n-k-\gamma-s$, which defines column structure. $\Longrightarrow$ Now $r(\delta)\Lambda r(g') \stackrel{!}{=} 0 \quad \forall g \in 1\ldots,\gamma, \quad r' \in n-k-s,\ldots,n-k$ (last s columns)

$$\begin{matrix} I_1 & E_2 \\ 0 & 0 \end{matrix} \begin{matrix} \} n-k-\gamma-s \\ \} n-k-\gamma-s \end{matrix}$$



$$\begin{array}{cccc|ccc} \mathrm{I} & A_1 & A_2 & \mathrm{B} & C_1 & C_2 \}\gamma \\ 0 & 0 & 0 & \mathrm{D} & \mathrm{I} & \mathrm{E} \}n-k-\gamma-s \end{array}$$

for these generators to commute $\implies \sum D_2 = 0 \implies D_2 = 0$, but then S=0, otherwise ——- not linearly independent. $\implies R \to$ We can still add —— of the last $n-k-\gamma$ block onto the 1^{st} ones to obtain $C_1 = 0$, which leads to the standard form.

Now logical t operators are obtained from a $k \times 2n$ matrix $G_a = (0\,0\,0 \mid A_2^T\ 0\ I_{k\times k})$. ($A_2$ is $r \times k \to A_2^T = k \times r$), $R\Lambda G_z = 0$(——— $\implies$ the generators coded by G_z commute with the generator of C coded in R there the 6 blocks in G_z have the corresponding number of columns,$r, n-k-r, k, r, n-k-r, k$). Furthermore, they commute amongst each other as they contain only Z's. For the same reason they also commute with the generator coded by the $n-k-r$ last rows of R. $\implies$ Use the kadder l generator $\bar{Z}_i$ coded by G_z to uniquely specify the code-word.

Similarly one vary find k generator $\bar{X}_i$ k×2n check matrix $[0E^T I|C^T 00]$. For CSS codes, things are already a bit simple, since we start with $B = C = 0$ from the beginning $\implies$ just need to create the I s. e.g. the t qubit ——- code has

$$R = \begin{array}{c} \\ \gamma\{ \\ n-k-\gamma\{ \end{array} \begin{array}{ccc} \overbrace{I}^{\gamma} & \overbrace{A_1}^{n-k-\gamma} & \overbrace{A_2}^{k} \\ 0 & 0 & 0 \end{array} \left| \begin{array}{ccc} B & O & C \\ D & I & E \end{array} \right.$$

$$\left(\begin{array}{c|c|c|c|c} \boldsymbol{I_3} & \begin{matrix}0\,1\,1\\1\,0\,1\\1\,1\,1\end{matrix} & \begin{matrix}1\\1\\0\end{matrix} & \begin{matrix}\mathbf{0}\\1\,0\,1\\0\,1\,1\\1\,1\,1\end{matrix} & \begin{matrix}\mathbf{0}\\\\\boldsymbol{I_3}\end{matrix} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & & \end{array}\begin{matrix}\\\\\\1\\1\\0\end{matrix}\right)$$

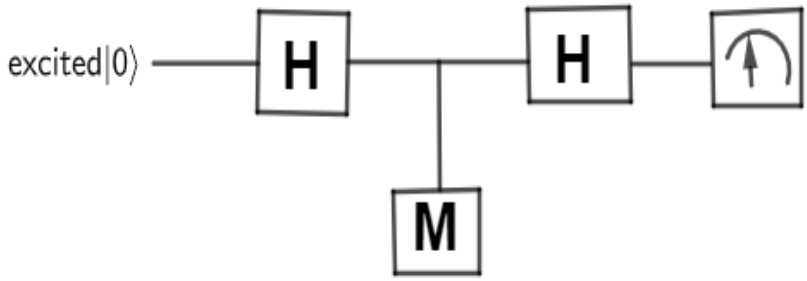
standard form $\implies$ $A_z = \begin{pmatrix}1\\1\\0\end{pmatrix}$ $\implies$ $G_z = 0000000|110|000|1$, which codes $Z_1 Z_2 Z_z$.

However, this form is obtained by mapping some qubits. Swapping back we get $\bar{Z} = Z_2 Z_4 Z_6$. We may also multiply by $Z_1 Z_3 Z_5 Z_7 \in C(S)0$ to get $\bar{Z} =>>\overset{7}{_{i=1}}> \otimes Z_i$.

Coding and decoding

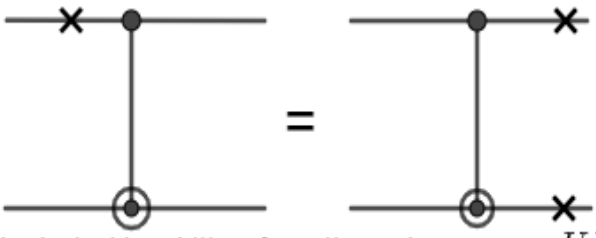
The stabilizer formalism enables systematic construction procedures for coding and decoding states in addition code (is addition to QEC). Suppose e.g. we want to prepare a coded $|0\rangle_L^{\otimes} K$ state, i.e. a state in the Hilbert space of n qubits coding k logical qubits in logical states 0 each. The ——— approach is to start with any state (not even pure); and measure the stabilizer $g_1, \ldots, g_{n-k}$ of the code C as well as the logical Z-operator $\bar{Z}_1, \ldots, \bar{Z}_k$. The outcomes will be ± 1 (or 0,1) for all $g_i, \ldots, \bar{Z}_g$ and a correspondingly resulting pure state. Which we can equivalently——— of as states stabilized by $\pm g_1, \ldots, \pm g_{n-k}, \pm\bar{Z}_1, \ldots, \pm\bar{Z}_k$, with the corresponding signs.But now we can unitarily transform this state into one stabilized by $+g_1, \ldots, +g_{n-k}, +\bar{Z}_1, \ldots, +\bar{Z}_k$ by applying corresponding elements of G_n (see proposition 12.1- a g$\in G_n$ always exists that flips the sign of a specific g_i, but not the other), and the $\bar{X}_i$ for which $\bar{Z}_i$ gave -1.

Arbitrary other logical states can be prepared by afterwards applying additional $\bar{X}_j$ operations. Decoding is actually rarely needed as we will work always with coded stated till the very end. However, there exists a purely unitary version of initial state preparation that works on pure states and which can be inverted ($\rightarrow$ not treated here, see problem 10.4 in NC), based on standard form of stabilizer



code. Arbitrary multi-qubit operators M such as the g_i or $\bar{Z}_i$ with eigenvalues ± 1 can be measured using an ———- bit.

See exercise $\rightarrow$ direct construction of measurement of stabilizers generator g_i



(most easily checked with stabilizer formalism, where we saw $UX_1U^\dagger = X_1X_2$)

8.12 Fault-tolerant QC

8.12.1 Introduction

QEC is nice, but not enough to make a QC work: assumed that operations for coding/de-coding, measurement and even logical operations will work perfectly, which is of course unrealistic. All operations of the QC are prove to error, and with QEC we have even added additional steps FT-QC one allows error in all operations:
− Coding

−logical operations

−simple Q-wires (≡ storage)

−error correction (EC)

−decoding

−measurement

Periodically doing EC is not enough, as a) EC can introduce error itself due to the logical operations, coding measurement not taken into account so —, and

b) the probability of error propagation

EX: CNOT + error on control :

However, in this example, if each qubit was coded with an 1-qubit error correcting code (e.g. 7 qubit Steame code), we could still correct it if of the coding qubits in each block at most one qubit was affected.

Def: A procedure (such as coding, logical ops etc, see above), is said to be fault-tolerant if it has the property that if only one component (such as elementary gate,

measurement,q-wire, or state preparation) fails then the failure causes at most one error in each coded block of output qubits. For a measurement we require in addition that the result should be correct up to $O(p^2)$ probability, if a single component fails with prob $O(p)$.

8.12.2 FT Q-logic

Any unitary q-circuit can be approximation terms of normalizer operations ($H, S = ('i)$) (phase, and CNOT) and the $\frac{\pi}{8}$ gate ($T = ('e^{i\frac{\pi}{4}})$) upto arbitrary precision. Here we first examine how to perform the normalizer operations fault-tolerantly. All following construction will assume the 7-qubit Steame code, unclear otherwise noted.

The logical $\bar{Z}$ and $\bar{X}$ operators for the Steame code are $\bar{Z} => >^{7}_{i=1}> \otimes Z_i$, $\bar{X} => >^{7}_{i=1}> \otimes X_i$.

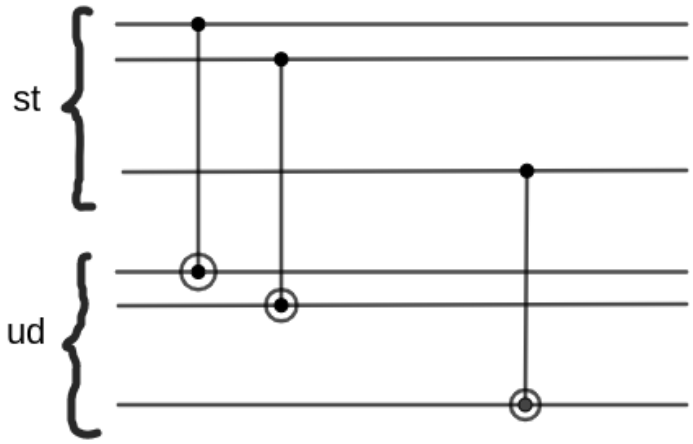
For an encoded $\bar{H}$ we want $\bar{H}\bar{Z}\bar{H} = \bar{X}$ and $\bar{H}\bar{X}\bar{H} = \bar{Z}$. This is obviously achieved by,$\bar{H} => >^{7}_{i=1}> \otimes H_i$.

One also checks that $\bar{H}\left|0\right\rangle_L = \frac{1}{\sqrt{2}}(\left|0\right\rangle_L + \left|1\right\rangle_L)$ and $\bar{H}\left|1\right\rangle_L = \frac{1}{\sqrt{2}}(\left|0\right\rangle_L - \left|1\right\rangle_L)$ follows directly from the above exchange of $\bar{X} \overset{\bar{H}}{\leftrightarrow} \bar{Z}$ in the stabilizer formalism: $\bar{Z}\left|0\right\rangle_L = \left|0\right\rangle_L = \bar{Z}\bar{H}\bar{H}\left|0\right\rangle_L \implies \bar{H}\bar{Z}\bar{H}\bar{H}\left|0\right\rangle_L = \bar{X}\bar{H}\left|0\right\rangle_L = \bar{H}\left|0\right\rangle_L$, so $\bar{H}\left|0\right\rangle_L$ is eigenstate of $\bar{X}$ with $\exists W + 1$, i.e. $\frac{\left|0\right\rangle_L + \left|0\right\rangle_L}{\sqrt{2}}$ and correspondingly for $\left|1\right\rangle_L$.

The logical gates $\bar{x}, \bar{Z}$ and $\bar{H}$ are said to be "transversal" (i.e. a parallel operation all qubits). A transversal construction of a logical gate makes it fault tolerant:

Suppose e.g. that a single error say Z ocuured on the 1^{st} qubit just before applying $\bar{H}$. So really HZ is applied on the 1^{st} qubit $HZ = HZH^{\dagger}H = XH$, so this is equivalent to actively applying the perfect $\bar{H}$ on all 7 qubits, but then have the 1^{st} qubit flips. So the single qubit error has not spread any further. An error may also
during the $\bar{H}$ and then have an error with some probability on the affected qubit(assumption once more that only one component, i.e. one H or q-wire here is affected) $\implies$ same result; only one qubit in the block of output qubits coding the single logical qubit is affected.

With $\bar{X}$ and $\bar{Z}$ FT, we also obtain $\bar{Y} = i\bar{X}\bar{Z}$ FT.



The obvious choice for S would be $\otimes S_i$, but $\bar{S}$ should do $\bar{S}\bar{Z}\bar{S}^\dagger = \bar{Z}$ and $\bar{S}\bar{X}\bar{S}^\dagger = \bar{Y}$, whereas $\otimes S_i$ flips $\bar{S}$ to $\bar{Y}$. This can be fixed by applying $\bar{Z}$ afterwards. So $\bar{S} = \bar{Z} > >^{7}_{i=1} > \otimes S_i$. Which is also transversal and thus FT.

Even the FT CNOT can be constructed this way:

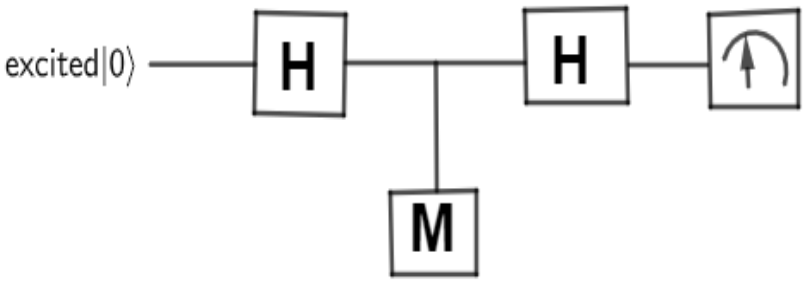
As we saw before, a single error is the input does propagate to 2 errors in the output-but they are on two different output blochs and thus the construction does qualify as FT.

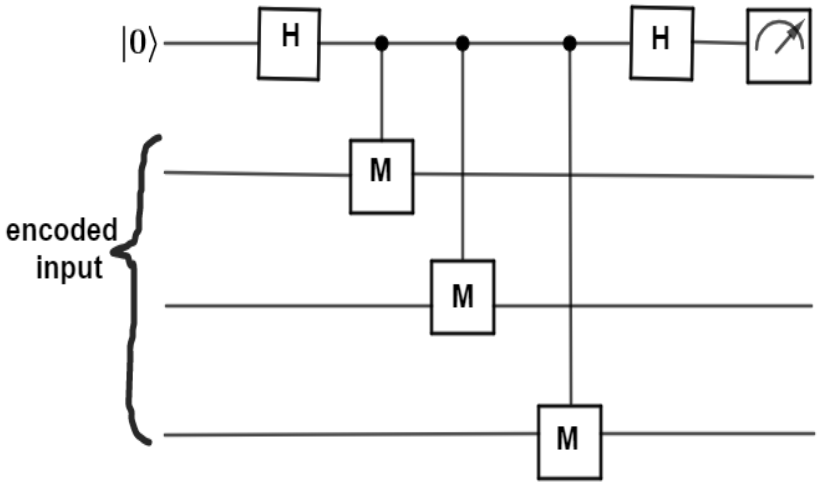
Before leaving how to make the $\frac{\pi}{8}$ gate FT we first study FT measurement.

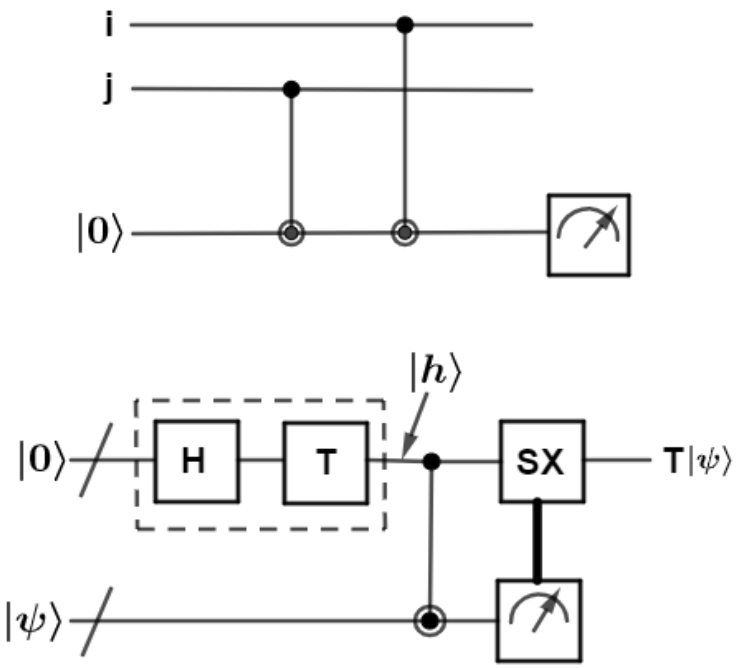
8.12.3 FT measurement

We have seen that an arbitrary measurement M with eigenvalues ± 1 on a single qubit can always be implemented with an aucilla in state $|0\rangle$ initially and the following q-circuit: One is tempted to try a transversal version on coded data: But this is not FT: a single error on the —— at the beginning will affect all output qubits on the bloch of coded data. The situation can be revealed by using an ——-qubit for each encoded input qubit. In comparison to the CNOT we still need to prepare the initial state of the —— outputs them into the cat-state(GHZ-state) .

$\frac{|00...0\rangle + |11...1\rangle}{\sqrt{2}}$ and verifies that one actually got that stat. The verification is done by a pair of Z_iZ_j measurements, which are themselves implemented us-


excited|0⟩
H
H
M


|0⟩
H
H
M
M
M
encoded
input



ing an —— and 2CNOTS + measurement in the computational basis of —— .

Basis of ——: Verify $Z_iZ_j = 1 \quad (\rightarrow 0)$. If not, start GHZ preparation again! Since $U_{CNOT}X_2U_{CNOT}^{\dagger} = X_2$, but $U_{CNOT}Z_2U_{CNOT}^{\dagger} = Z_1Z_2$, only phase flip error can propagate from the ——- to the ——, and by definition there can be at most one phase flip error on the GHZ state(which becomes $\frac{|00...0\rangle - |11...1\rangle}{\sqrt{2}}$ no matter where a phase flip occurred).

The GHZ state is required since we want to apply all M's or no M at all.

If (an add # og) phase flips in the GHZ occurred, then the encoded data are still not affected, but will lead to wrong measurement result after decoding. So far we had obtain a measurement error with probability p. It can be reduced by the standard technique of applying the whole measurement procedure 3 times and taking a majority —— to $O(p^2)$.

8.12.4 FT $\frac{\pi}{8}$ gate(T gate)

This gate can be implemented in a FT ——— by the following q-circuit:

Both input outputs are logical ones (i.e. containing 7 physical qubits in the case of the Steame code). The dashed box produces the state $|\theta_L\rangle = \frac{|0_L\rangle + \exp\frac{i\pi}{4}|1_L\rangle}{\sqrt{2}}$ (=TH$|0\rangle$) in terms of logical states $|0_L\rangle, |1_L\rangle$. In reality one does not perform these two gates HT as we don't know yet, how to perform T in the 1^{st} place FTly. But note that since $|0\rangle$ is stabilized by $Z, T\overbrace{HZH}^{X}T^\dagger = TXT^\dagger = \exp\frac{-i\pi}{4}SX$ stabilize the desired logical state $|\theta\rangle$! And we know how to perform S,X FTly (in transverse fashion). So the —— of the fault tolerant preparation of θ is to measure $\exp\frac{-i\pi}{4}SX$ FTly as seen in 3.3. If the result is +1 $\implies$ Ok, if -1 either repeat or apply Z FTly, as $ZSXZ = -SX \implies$ now have $EW + 1$. So now have $|\theta\rangle$ prepared FTly. The FT CNOT makes

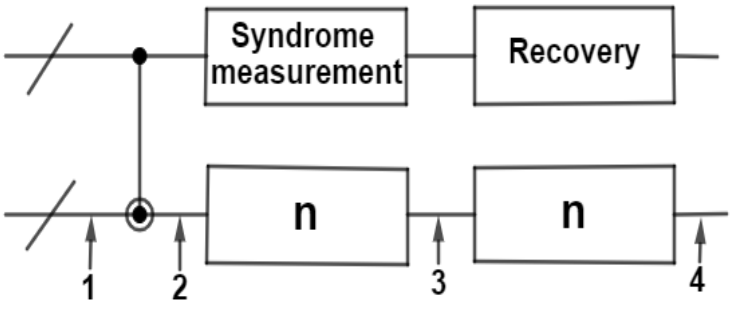
$$\frac{1}{\sqrt{2}}\Big[|0\rangle_L (a|0\rangle_L + b|1\rangle_L) + \exp\frac{i\pi}{4}|1\rangle_L \underbrace{(a|1\rangle_L + b|0\rangle_L)}_{\text{bits flipped for control=1}}\Big]$$

if $|\psi\rangle$ was $|\psi\rangle = a|0\rangle_L + b|1\rangle_L = \frac{1}{\sqrt{2}}\Big[(a|0\rangle_L + b\exp\frac{i\pi}{4})|0\rangle_L + (b|0\rangle_L + a\exp\frac{i\pi}{4})|1\rangle_L\Big]$. Now measure data bits. If it is $|0\rangle_L$ we are done, as now we have $T|\psi\rangle$ mapped into the ———- which from now on is considered data. If result is $|1\rangle_L$, apply $\bar{S}\bar{X}$. When $|1\rangle_L$ was found, ——— are in $b|0\rangle_L + a\exp\frac{i\pi}{4}|1\rangle_L \xrightarrow{\bar{X}} b|1\rangle_L + a\exp\frac{i\pi}{4}|0\rangle_L \xrightarrow{\bar{S}}$ $a\exp\frac{i\pi}{4}|0\rangle_L + b\exp\frac{i\pi}{2}|1\rangle_L = \exp\frac{i\pi}{4}|\psi\rangle$,—— to a total irrelevant phase we have performed T in both cases. Altogether we see that we have replaced FTT by FT measurement of SX + maps ————-.

8.12.5 The Threshold Theorem

We have now at our disposal FT logic, measurement and state preparation. These procedures can be combined, and one can estimate at each step of a given circuit the probability that two error in a coded bloch occur. The goal is to —— that this probability is at most of O(p^2) (with some prefactor to be determined), if so for in te q-circuit the probability of a single component failure was O(P). this is simply done by looking at all possibilities how 2 error can occur. Illustration at the example of an FT CNOT : The inputs are logical qubits, coded e.g. with the Steame code, 2 error in a single coded bloch can arise from

1. two error onto(one in each bloch) and CNOT propagates one to the other bloch
2. a single error ——- another happens in the CNOT
3. 2 errors happen in the CNOT in the 1^{st} bloch.



4. .

   .

   .

   .

One then counts the number of different possibilities how these error can happen from single component failure. E.g. possibility (1) implies an error in the previous stage of syndrome mesurement and recovery in each bloch. For the qubit Steame code there are 6 syndrome measurement with ——— location where failure may occur. Together with the recovery ———-(7 ———-) $\Longrightarrow$ $\sqrt{C_o p^2} = C_0 p^2 = 6.10{+}7 = 67 \approx 10^2$ possibilities. The probability for two ——— failures in 1^{st} bloch is thus ———, and thus is in fact the ——— contribution compared to all other possibilities, all of which lead to come $c_i p^2$. In the end one finds probability for 2 failures in 1^{st} bloch is therefore $\sum_i c_i p^2 \equiv c p^2 \approx 10^4 p^2$.

The crucial idea in the derivation of the threshold theorem in that this probability can be suppressed even further by concatenating levels of encoding. Example 9-qubit Shor code:

$$|0^1\rangle = \Big(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\Big)^{\otimes 3}, |1^1\rangle = \Big(\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)\Big)^{\otimes 3}$$

Then,

$$|0^{k+1}\rangle = \Big(\frac{1}{\sqrt{2}}(|0^k 0^k 0^k\rangle + |1^k 1^k 1^k\rangle)\Big)^{\otimes 3}, |1^{k+1}\rangle = \Big(\frac{1}{\sqrt{2}}(|0^k 0^k 0^k\rangle - |1^k 1^k 1^k\rangle)\Big)^{\otimes 3}$$

One continues this to a desired level. If at level 0 the probability for failure of any component if p, then at level (1) it is cp^2, at level $2 : c(cp^2)^2$, at level K:$(cp)^{2^k}/c$.(Remember: c counts of components or coding thereof, i.e. property of coding scheme and q-circuit, not of device). If the q-circuit which we want to implement

contains N gates that is a polynomial q(n), n numbers of original bits, and we wish to achieve a final error probability ϵ, than each (encoded) gate must fail with probability smaller than.

$$\frac{\epsilon}{N} \geq \frac{(cp)^{2^k}}{c}$$

For $p > \frac{1}{c}$, clearly such a k exists for any $\epsilon > 0$. Thus in the threshold condition !

The use of the kth level encoded q-circuit(for a single gate) grows as d^k where d is some constant counting the max number of gates used is an FT procedure for an encoded gate.

Above equation $\Longrightarrow$

$$k \geq \log\left(\log\left(c\epsilon/N\right)/\log cp\right) \implies d^k \geq 2^{\log d \log\left(\log c\epsilon/N/\log cp\right)}$$

$$= \left(\frac{\log \frac{c\epsilon}{N}}{\log cp}\right)^{logd} = \left(\frac{\log \frac{N}{c\epsilon}}{\log cp}\right)^{logd} = O(poly \log \frac{N}{\epsilon})$$

i.e. a polynomial of fixed order in $\log \frac{N}{\epsilon}$. So the total circuit size is $O(poly(\log \frac{N}{\epsilon})N)$ gates, which is only poly.logarithmally larger than the size of the original q-circuit N.

$\Longrightarrow$ **Threshold theorem for q-computation:**

A q-circuit containing N gates may be implemented with error probability $\geq \epsilon$ using $O(poly(\log \frac{N}{\epsilon})N)$ gates on hardware whose components fails with probability at most p, provided $p < p + h$.

The actual value of $p+h$ depends on assumptions about the hardcore, e.g. if one can perform gates only on nearest neighbour qubits is an array or between all qubits, but $p + h \approx 10^{-4}$ more optimistic values even $10^{-3} - 10^{-2}$.

A Acknowledgements

- Pictures of the Bloch sphere created using *QuTiP* `http://qutip.org/`
- Quantum circuits created using *Qcircuit* LaTeX package `http://physics.unm.edu/CQuIC/Qcircuit/`
- Remaining graphics and images created using *Inkscape* `https://inkscape.org/`

Bibliography

[1] A. Barenco. A universal two-qubit gate for quantum computation. *Proc. R. Soc. Lond. A*, 449:679, 1995.

[2] A Barenco, C Bennett, R Cleve, D DiVincenzo, and N Margolus. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457, 1995.

[3] C. H. Benett and G. Brassard, editors. *Quantum cryptography: Public key distribution and coin tossing.*

[4] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992.

[5] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[6] Alexandre Blais, Ren-Shou Huang, Andreas Wallraff, S. M. Girvin, and R. J. Schoelkopf. Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation. *Physical Review A*, 69(6), 2004.

[7] Rainer Blatt and David Wineland. Entangled states of trapped atomic ions. *Nature*, 453(7198):1008–1015, June 2008. Number: 7198 Publisher: Nature Publishing Group.

[8] V Bouchiat, D Vion, P Joyez, D Esteve, and M H Devoret. Quantum coherence with a single cooper pair. *Physica Scripta*, 1998(T76):165, 1998.

[9] H.-P. Breuer and F. Petruccione. Concepts and Methods in the Theory of Open Quantum Systems. In F. Benatti and R. Floreanini, editors, *Irreversible Quantum Dynamics*, volume 622 of *Lecture Notes in Physics, Berlin Springer Verlag*, pages 65–79, 2003.

[10] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[11] Yu Chen, C. Neill, P. Roushan, N. Leung, M. Fang, R. Barends, J. Kelly, B. Campbell, Z. Chen, B. Chiaro, A. Dunsworth, E. Jeffrey, A. Megrant, J. Y. Mutus, P. J. J. O'Malley, C. M. Quintana, D. Sank, A. Vainsencher, J. Wenner, T. C. White, Michael R. Geller, A. N. Cleland, and John M. Martinis. Qubit architecture with high coherence and fast tunable coupling. *Phys. Rev. Lett.*, 113:220502, Nov 2014.

[12] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975.

[13] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74:4091–4094, May 1995.

[14] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proc. Roy. Soc. Lond. A*, 400:97, 1985.

[15] D. Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271 – 272, 1982.

[16] David P DiVincenzo. Two-bit gates are universal for quantum computation. *Physical Review A*, 51(2):1015, 1995.

[17] David P. DiVincenzo. Topics in quantum computers. 1996.

[18] David P. DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik*, 48(9-11):771–783, 2000.

[19] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[20] R. P. Feynman. Simulating Physics with Computers. *International Journal of Theoretical Physics*, 21:467–488, June 1982.

[21] M.P. Frank. Approaching the Physical Limits of Computing. In *35th International Symposium on Multiple-Valued Logic (ISMVL'05)*, pages 168–185, Calgary, Canada, 2005. IEEE.

[22] Michael R. Geller, Emmanuel Donate, Yu Chen, Michael T. Fang, Nelson Leung, Charles Neill, Pedram Roushan, and John M. Martinis. Tunable coupler for superconducting Xmon qubits: Perturbative nonlinear model. *Physical Review A*, 92(1):012320, July 2015.

[23] M. GÃ¶ppl, A. Fragner, M. Baur, R. Bianchetti, S. Filipp, J. M. Fink, P. J. Leek, G. Puebla, L. Steffen, and A. Wallraff. Coplanar waveguide resonators for circuit quantum electrodynamics. *Journal of Applied Physics*, 104(11):113904, December 2008.

[24] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.

[25] A. A. Houck, Jens Koch, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf. Life after charge noise: recent results with transmon qubits. *Quantum Information Processing*, 8(2):105–115, 2009.

[26] Donald E. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison Wesley Longman Publishing Co., Inc., 1997.

[27] Jens Koch, Terri M. Yu, Jay Gambetta, A. A. Houck, D. I. Schuster, J. Majer, Alexandre Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf. Charge-insensitive qubit design derived from the cooper pair box. *Phys. Rev. A*, 76:042319, Oct 2007.

[28] A. Kossakowski. On quantum statistical mechanics of non-hamiltonian systems. *Reports on Mathematical Physics*, 3(4):247 – 274, 1972.

[29] G. Lindblad. On the generators of quantum dynamical semigroups. *Communications in Mathematical Physics*, 48(2):119–130, 1976.

[30] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland. Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.*, 75:4714–4717, Dec 1995.

[31] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[32] A. Peres. *Quantum Theory: Concepts and Methods*. Fundamental Theories of Physics. Springer, 1995.

[33] M. G. Raizen, J. M. Gilligan, J. C. Bergquist, W. M. Itano, and D. J. Wineland. Ionic crystals in a linear Paul trap. *Physical Review A*, 45(9):6493–6501, May 1992. Publisher: American Physical Society.

[34] Kyle J. Ray and James P. Crutchfield. Gigahertz Sub-Landauer Momentum Computing. *arXiv:2202.07122 [cond-mat, physics:nlin, physics:physics]*, February 2022. arXiv: 2202.07122.

[35] Ferdinand Schmidt-Kaler, Hartmut Haffner, Mark Riebe, Stephan Gulde, Gavin P. T. Lancaster, Thomas Deuschle, Christoph Becher, Christian F. Roos, Jurgen Eschner, and Rainer Blatt. Realization of the cirac-zoller controlled-not quantum gate. *Nature*, 422(6930):408–411, Mar 2003.

[36] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.

[37] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[38] Anders SÃ¸rensen and Klaus MÃ¸lmer. Quantum Computation with Ions in Thermal Motion. *Physical Review Letters*, 82(9):1971–1974, March 1999.

[39] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77:793–797, Jul 1996.

[40] D. Vion, A. Aassime, A. Cottet, P. Joyez, H. Pothier, C. Urbina, D. Esteve, and M. H. Devoret. Manipulating the Quantum State of an Electrical Circuit. *Science*, 296:886–889, May 2002.

[41] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, Oct 1982.