Quantum Computing: from Basics to the cutting Edge

Tatiana Yu. Golubeva

Sergey S. Sysoev

Kirill S. Tikhonov

Evgenii Vashukevich

Sergei Korolev

Ivan Vybornyi

(edited by Benjamin Köhler)

This book is based on my notes taken in the lecture series of the same name by the St. Petersburg State University. If you have the opportunity, you should try to find videos of his lecture and listen to those. The style of presentation is much beyond my ability to write down this outstanding lecturers' wonderful humour and insightful remarks.

In the first part based on the lectures given by Sergey S. Sysoev, a very shallow overview over the field of quantum computing is given. It should enable you the reader to appreciate the beauty of quantum computing and understand its working principle without too much mathematical exposure. It begins by introducing the basic notions of quantum mechanics and the most important physical phenomena that can be used for computation. Furthermore, it gives you a overview on the mathematics and shows you the limitations and opportunities arising from quantum mechanics. Also, it give examples of quantum circuits that realise quantum algorithms. At the end, two quantum cryptography protocols are discussed.

This part should enable you to join in conversations about quantum computing without embarrassing yourself too soon. You will also be able to understand popular books written by the pioneers of quantum computing. The Feynman lectures on computation and the books by David Deutsch are recommendable. I hope you enjoy this short part and feel motivated to dive deeper into the field and will read the other three parts that are more rigorous and will enhance your understanding and allow you to read more advanced literature and become a true expert in the field.

In the second part of the book which is based on the lectures given by Evgenii Vashukevich and Ivan Vybornyi, the physical basics of quantum mechanics are introduced. It presents the main mathematical objects and physical phenomena that allow for quantum computing to be so powerful. You will be introduced to important principles that enhance your understanding of quantum computing and allow you to appreciate it more. This part explains the quantum circuit model starting from the elementary classical logic operations and then introduces the quantum counterparts.

This part introduces the first quantum algorithms and helps you gain a good understanding of them. After reading the respective chapters, you can start to read the literature that hardly has more complicated algorithms and you will be able to appreciate the advantage of these algorithms over their classical counter parts.

At the end of this part, the principles of error correction are discussed. You will understand that the correction of errors is one of the main limitation of realising quantum computers that can actually help in solving real world problems. If your follow the presentation to the end, you will know enough to advance to more complicated error correction schemes that use less qubits to correct errors.

The third part that is based on the lectures by Sergey S. Sysoev, enlarges upon the content of the first part. You will learn about the class of oracle function algorithms, Shor's algorithm, and Grover's algorithm. The last two are the first examples of algorithms that can actually solve real world tasks much more efficiently than classical computers can. You will also learn about the limitations of quantum computers.

The fourth and last part is based on the lectures by Evgenii Vashukevich and Ivan Vybornyi. Here, you are introduced to the one-way computing approach to quantum computation which is used in photonic systems where the qubits vanish after one measurement and can not be used afterwards. You will understand that this approach is very beneficial and effective. Especially, it allows for a quick realisation of quantum operations and in principle of error correction. Although, this part is mathematically more challenging, you are still encouraged to read along as after reading this part, you will have a much better idea of how quantum computations are actually realised in a quantum system.

I hope this book helps you to get started in the field of quantum computing as it did for me. I am very thankful to these authors for sharing their bright minds. For this I will be thankful to them forever.

-Benjamin Köhler
Leipzig, 2023

Contents

Part I

Quantum Computing: Less Formulas - more understanding

Chapter 1

Basic notions

There are three essential demands on a quantum computer:

1. continuum of states
2. true randomness
3. interference

We explore all three aspects of this in the next sections and point out that only when all three properties are fulfilled, the resulting computer is superior to a regular computer. A side effect of these considerations is that we encounter and introduce many useful concepts and notations from quantum mechanics that are necessary to understand all main principles of quantum computing.

1.1 The state space

A **qubit** has a continuum of possible states in contrast to a bit (which is either 0 or 1) as it can be a superposition of $|0\rangle$ and $|1\rangle$. A quantum bit can, therefore, store an infinite number of information/values, e.g. as a point on the unit circle[1]

$$|\Phi\rangle = \cos\phi|0\rangle + \sin\phi|1\rangle. \tag{1.1}$$

Theoretically a classical pendulum can represent an infinite number of states/a point on the unit circle too. A quantum bit is **much more**!

1.2 True randomness

This property of a quantum computer is often underestimated. A coin toss is not truly random (Laplace demon). **True randomness** means that the universe can not predict the outcome. The double slit experiment shows that this is possible, i.e. there are true random processes. A qubit state is a superposition of many base states. The measurement destroys this superposition. Random behaviours enable one to get many more outcomes by the same input. Many quantum computers do the same task, but are differently successful. A pendulum will always be in only one state and is, therefore, not truly random.
Imagine the following function that takes one bit as input

$$f(x) = \begin{cases} f(|0\rangle) = f_0 \\ f(|1\rangle) = f_1 \end{cases} \tag{1.2}$$

The state

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{1.3}$$

[1] We later demonstrate that the actual state space is much larger as $|\Phi\rangle = \frac{1}{\sqrt{2}}\phi|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$ is also a valid state which, however, does not lie on the unit circle.

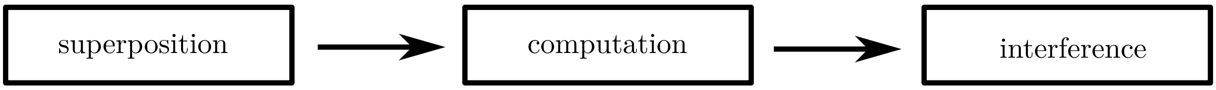


Figure 1.1: Basic principle of quantum computing. The last step allows to extract the quantum nature of a qubit.

can be the one of a qubit and passed to the function, but this state can not be represented by the pendulum. A qubit can be in infinitely many states **and** have two values **simultaneously**. The pendulum can only store one value at a time.

1.3 Interference

An observer makes the wave function collapse and measures only one of the two possible values in equation (1.2), i.e. after the measurement, every consecutive measurement returns the same value as was obtained in the initial measurement. After the measurement, the state is either $|0\rangle$ or $|1\rangle$ and no longer a superposition. In the multiverse interpretation one considers the universe to split into two versions where in one $|0\rangle$ and in the other $|1\rangle$ was observed. The observer **entangles** himself with the qubit.
We want to use both outcomes for our calculations. **Interference** makes this possible. Here, the result of the observation is a superposition of the base states (interference pattern in the double slit experiment), i.e. there is an interaction of the base states:

$$f(x)|+\rangle = \frac{f(x)}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] = \frac{1}{\sqrt{2}}\left[f_0|0\rangle + f_1|1\rangle\right] \neq \left\{ \begin{array}{l} f_0|0\rangle \\ f_1|1\rangle \end{array} \right. . \tag{1.4}$$

The basic principle of quantum computations is illustrated in Figure 1.1. The last step allows to extract the quantum nature of the qubit. For quantum computations to be reliable, there **must** be no other interaction destroying the interference. Therefore, the computation process must be:

1. fast
2. cold
3. isolated (probably the hardest)

1.4 Classical and quantum particles

The double slit experiment can be used to distinguish classical (bullet-like) and quantum (wave-like) particles:

- For **classical particles** the resulting pattern is the sum of two one-slit experiments
- For **quantum particles** the resulting pattern is the superposition of of the two one-slit experiment's intensities (amplitudes squared)
- Heavier particles have a smaller wavelength, i.e. more concentrated wave functions
- The intensity of the wave function is the probability to observe the particle in a particular state

The wave-function needs to be square-integrable ($\mathcal{L}^2$) and non-zero.

1.5 Exercises

1. The demands for a physical implementation of a quantum computer, which we deduced from the mathematical model of quantum computing, are:

   ○ truly random events must be employed

   ○ interference must be possible

   ○ instead of bits we need qubits which can have an infinite number of possible states

   ○ computation must be fast

   ○ qubit implementation must be cold

2. Check all true random events in the list below:

   ○ A flipping coin lands on the table with tails up or down

   ○ An electron hits either upper or lower detection in Young's interferometer

   ○ A stock price unexpectedly falls or grows

   ○ Photon either passes through or reflects from the piece of glass

   ○ A radioactive isotope either decays or not during a period of time

3. Qubit state $|+\rangle$ is:

   ○ $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

   ○ $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

   ○ $|0\rangle + |1\rangle$

   ○ $|0\rangle - |1\rangle$

4. Is the following proposition correct?

   Interference sometimes allows us to read more information from a superposition state of a system than the simple observation of the state.

5. Should we literally believe in the existence of parallel universes which contain different copies of us and other objects?

   ○ Science is not about out believes. The multiverse is just a convenient mathematically model which allows us to interpret and explain superposition states. To our current knowledge there is no experiment which can prove or refute the existence of the multiverse.

   ○ Yes, of course! And there exists a universe where birds and bees talk about quantum mechanics in pure English.

Chapter 2

Mathematical background and physical notions of quantum mechanics

Mathematically wave functions form a vector space, i.e. if $\mathbb{F}$ is a linear vector space then

$$\begin{aligned}
&A, B \in \mathbb{F},\ \alpha, \beta \in \mathbb{C}\\
1.\ &\alpha A \in \mathbb{F}\\
2.\ &A + B \in \mathbb{F}\\
\Rightarrow &f(x) : \int f^2(x)\mathrm{d}x < \infty\\
&g(x) = af(x) \Rightarrow \int g^2(x)\mathrm{d}x = a^2 \int f^2(x)\mathrm{d}x < \infty\\
&(f+g)(x) = f(x) + g(x) \in \mathbb{F}
\end{aligned}$$

The dimensionality of square-integrable functions is infinite, i.e. there will be infinitely many basis functions. Measurements make the wave function collapse and entangle the observer with a basis function of the measurement. Dirac-delta functions form the basis of the vector space $\mathcal{L}^2$-function strictly speaking (δ-distribution are orthonormal basis functions). Measurements transform the wave function composition into one (**randomly selected**) vector of that composition:

$$x = \sum_{i=1}^{n} x_i \boldsymbol{e}_i \to \boldsymbol{e}_i \qquad \text{(measurement)} \tag{2.1}$$

$$P(\boldsymbol{e}_a) = x_a^2 \qquad \text{(probability)} \tag{2.2}$$

$$f(x) = \int\limits_{-\infty}^{\infty} f(a)\delta(x-a)\,\mathrm{d}a \ \to\ \delta(x-a) \qquad \text{(measurement with probability } f(a)\text{)} \tag{2.3}$$

The last integral is a **Lebesque integral**.

2.1 State space

The **state space** is a isomorphism of a general vector

$$x = \sum_{i=1}^{N} x_i \boldsymbol{e}_i = \begin{pmatrix} x_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ x_N \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_N \end{pmatrix}. \tag{2.4}$$

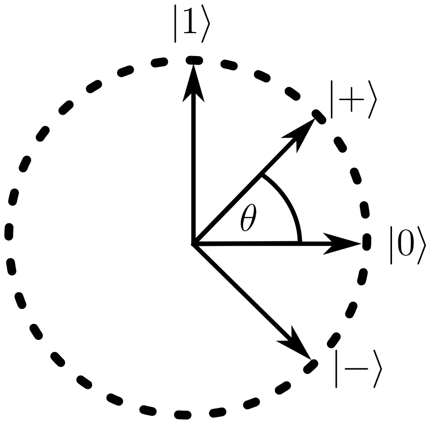


Figure 2.1: The rotation of the polarisation filter also rotates the basis of possible outcomes of the measurement. By rotating the filter, the basis can be manipulated.

This reduces the dimensionality of the state. Such a finite representation and in particular the **two-state-representation** is most interesting for quantum computing. The latter is realised, e.g. by the polarisation of light which is the plane of oscillation of electro-magnetic waves (light). Polarisation filter are composed of dipol ordered atoms. These block out one polarisation (all other polarised waves interfere destructively). A **single** photon can either pass or not through the filter. This is the measurement of the photon's polarisation. The reflected light will have the opposite polarisation. The photon polariser has a state space of dimension 2. This is the so called **qubit-realisation**.

With the polariser at $\theta = \frac{\pi}{4}$ the basis is

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

which is also illustrated in Figure 2.1. By rotating the polariser, the measurement can be tuned/the basis be manipulated.

The polarisation of light oscillates with period T or frequency ω

$$|P(t)\rangle = \frac{1}{\sqrt{2}}[\cos(\omega t)|0\rangle + \sin(\omega t)|1\rangle] = |+\rangle(t) \qquad \text{(clockwise rotation)} \tag{2.5}$$
$$|-\rangle = \frac{1}{\sqrt{2}}[\cos(\omega t)|0\rangle - \sin(\omega t)|1\rangle] \qquad \text{(anti-clockwise rotation)} \tag{2.6}$$
$$|+\rangle = \frac{1}{\sqrt{2}}\left[\mathrm{e}^{\mathrm{i}\omega t}|0\rangle + \mathrm{i}\mathrm{e}^{\mathrm{i}\omega t}|1\rangle\right] = |+\rangle(t) \tag{2.7}$$
$$|-\rangle = \frac{1}{\sqrt{2}}\left[\mathrm{e}^{\mathrm{i}\omega t}|0\rangle - \mathrm{i}\mathrm{e}^{\mathrm{i}\omega t}|1\rangle\right] = |+\rangle(t). \tag{2.8}$$

As phases do not matter, we can cancel the time dependence:

$$|+\rangle = \frac{1}{\sqrt{2}}\Big[|0\rangle + \mathrm{i}|1\rangle\Big] \tag{2.9}$$
$$|-\rangle = \frac{1}{\sqrt{2}}\Big[|0\rangle - \mathrm{i}|1\rangle\Big] \tag{2.10}$$

or alternatively

$$|+\rangle = \frac{\mathrm{e}^{\mathrm{i}\omega t}}{\sqrt{2}}\Big[|0\rangle + |1\rangle\Big] \tag{2.11}$$
$$|-\rangle = \frac{\mathrm{e}^{-\mathrm{i}\omega t}}{\sqrt{2}}\Big[|0\rangle + |1\rangle\Big]. \tag{2.12}$$

2.2 Bloch sphere

The general two-qubit state can be expressed as

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}\mathrm{e}^{\mathrm{i}\phi}|1\rangle \tag{2.13}$$

where the argument of the trigonometric functions is to ensure that $|0\rangle$ and $|1\rangle$ are on opposite on the so called **Bloch sphere** which is illustrated in Figure 2.2. With these two angles, six special states for quantum computing applications are defined:

$$\begin{aligned}
&\theta = 0, && \phi = 0: && |\Psi\rangle = |0\rangle,\\
&\theta = \pi/2, && \phi = 0: && |\Psi\rangle = |+\rangle,\\
&\theta = \pi, && \phi = 0: && |\Psi\rangle = |1\rangle,\\
&\theta = 3\pi/2, && \phi = 0: && |\Psi\rangle = |-\rangle,\\
&\theta = \pi/2, && \phi = \pi/2: && |\Psi\rangle = |\circlearrowleft\rangle,\\
&\theta = -\pi/2, && \phi = \pi/2: && |\Psi\rangle = |\circlearrowright\rangle.
\end{aligned}$$

The Bloch sphere is applicable to any two state systems, e.g. the Stern Gerlach experiment[1].

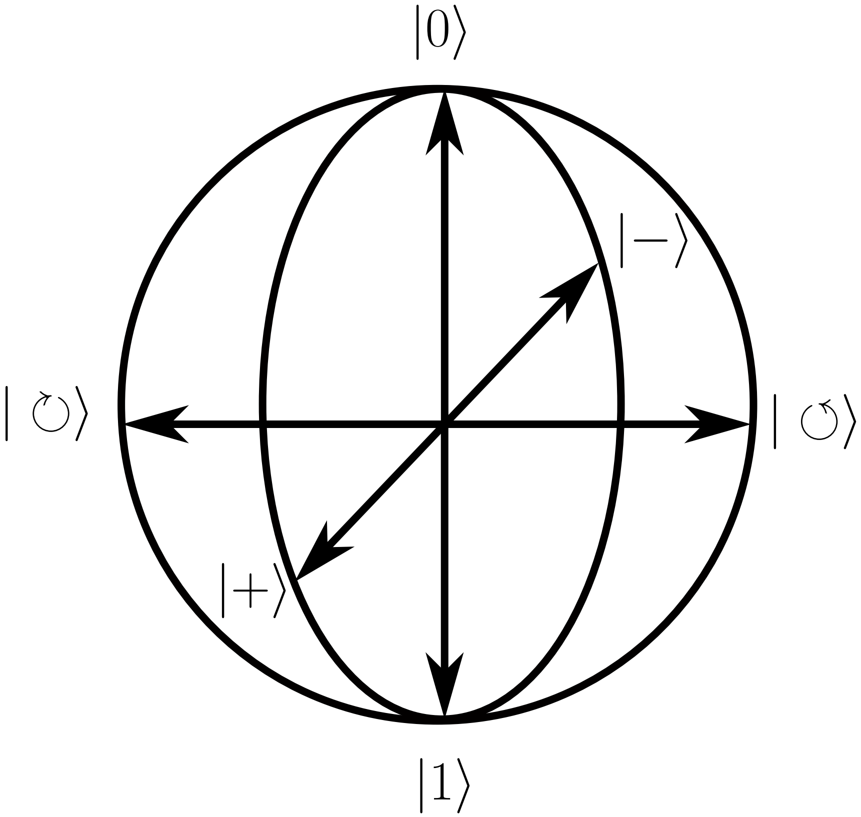


Figure 2.2: The Bloch sphere with the six most important states in quantum computing

[1] Silver atoms in a magnetic field, deflection to north or south because of the electron spin

2.3 Entanglement

One qubit is not enough for quantum computing. There is no problem with creating more qubits, e.g. by having many atoms, photons, or spins, **but** they need to be **entangled** to truly be powerful tools in quantum computing. Else, the qubits do not depend on one another and calculations need to collapse the wavefunctions (normal qubit). For example the so called **conditional NOT (CNOT)**-gate flips the state of a qubit if another qubit is in state $|1\rangle$ and leaves it as it is if the other qubit is in state $|0\rangle$. The wavefunctions do not collapse in this process. The state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$ is transformed into the state $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle))$[2]. In this state, both qubits are indistinguishably entangled. As of now (2022) entangling is a complicated process and the basis of any practicable application of quantum computations.

2.4 Systems with many qubits

For two qubits, there are four possible basis states: $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ and $|1\rangle|1\rangle$. There are states that can be expressed as results of tensor products of two states

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \tag{2.14}$$

and states like

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{2.15}$$

Both types of states can exist physically. The notation we use here is

$$|\alpha\beta\rangle = \begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} \otimes \begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix} = \begin{pmatrix}\alpha_0\begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}\\ \\ \alpha_1\begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\end{pmatrix}\\ \\ \begin{pmatrix}\alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix} \tag{2.16}$$

This scheme generalises to many qubits and the basis notation yields the binary representation of numbers. The dimension of the basis is 2^n where n is the number of qubits in the system.

2.5 Mathematics of quantum computing

- **inner products**

$$\begin{aligned}
&\cdot : \mathcal{H} \times \mathcal{H} \to \mathbb{C}\\
&\quad \boldsymbol{x}, \boldsymbol{y} \in \mathcal{H}, \alpha \in \mathbb{C}\\
&1.\ \boldsymbol{x} \cdot \boldsymbol{y} = \overline{\boldsymbol{y} \cdot \boldsymbol{x}}\\
&2.\ \boldsymbol{x} \cdot (\alpha \boldsymbol{y}) = \alpha(\boldsymbol{x} \cdot \boldsymbol{y}) \quad \text{(only second component!!!)}\\
&3.\ \boldsymbol{x} \cdot \boldsymbol{x} \geq 0\ \ (\boldsymbol{x} \cdot \boldsymbol{x} = 0 \Leftrightarrow \boldsymbol{x} = \boldsymbol{0})
\end{aligned}$$

$$\text{in Hilbert space: } \boldsymbol{x} \cdot \boldsymbol{y} = \sum_{i=1}^{n} x_i^* y_i,\ \ f \cdot g = \int f^*(x) g(x)\,\mathrm{d}x$$

- **conjugate space**

$$\boldsymbol{x} \in \mathcal{H},\ f_{\boldsymbol{x}} : \boldsymbol{y} \to \boldsymbol{x} \cdot \boldsymbol{y}\ \forall \boldsymbol{y} \in \mathcal{H},\ f - x \in \mathcal{H}^*$$

$$\left.\begin{aligned}|x\rangle &\in \mathcal{H}\\ \langle x| &\in \mathcal{H}^*\end{aligned}\right\}\text{Bra-Ket notation}$$

$$f_{\boldsymbol{x}} = \langle x|$$

$$\langle x|y\rangle = \boldsymbol{x} \cdot \boldsymbol{y}$$

[2] This is one of the Bell states which we encounter later

- **representations**

$$|x\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \qquad \langle x| = \begin{pmatrix} x_1^*, \ldots, x_n^* \end{pmatrix}$$

- **hermitian conjugation**

$$\alpha^* = \overline{\alpha}, \quad |x\rangle^* = \langle x|, \quad \langle x|^* = |x\rangle$$

- **linear operators**

  ...are the tool to to manipulate the states or qubits

$$\begin{aligned} A :\ & \mathcal{H} \to \mathcal{H} \\ & A(\alpha|x\rangle + \beta|y\rangle) = \alpha A|x\rangle + \beta A|y\rangle \end{aligned}$$

  A are operators represented by matrices.

$$\begin{aligned} A|x\rangle &= A_{ij}|x\rangle_j \quad \text{(Einstein summation)} \\ A_{ij} &= (A|j\rangle)_i \quad \text{where } |j\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \leftarrow \text{j'th position} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \ldots \text{ j'th basis vector} \end{aligned}$$

  In general, two operators do not commute and, therefore, the order of multiplication is important. The commutator

$$[A, B] = AB - BA \tag{2.17}$$

  is very important.

- **hermitian operators**

  ...are operators with the following property:

$$\begin{aligned} \langle y|A|x\rangle = \langle y|\Big(A|x\rangle\Big) &= \Big(\langle y|A\Big)|x\rangle \\ &= \langle y|\Big(A^*|x\rangle\Big), \end{aligned}$$

  i.e. $A = A^*$ or $\left(\langle\phi|A\right)^* = A^*|\phi\rangle$.

- **hermitian conjugation**

  ...is defined as

$$\left(\alpha|a\rangle\langle b|\langle c|ABC|d\rangle\right)^* = \overline{\alpha}\langle d|C^*B^*A^*|c\rangle|b\rangle\langle a|.$$

  Hermitian operators represent observables. They have real eigenvalues and orthogonal eigenstates.

- **eigenvalue equation**

  ...is

$$A|\Phi\rangle = \lambda|\Phi\rangle.$$

There are many eigenvalues λ (degeneracy possible) and eigenstates $|\Phi\rangle$ (up to normalisation), but[3] the same amount.

The eigenvalues of hermitian operators are real because

$$\begin{aligned} \langle x|A|x\rangle &\overset{A=A^*}{=} ((\langle x|A)|x\rangle = \lambda^* \|x\| \\ \langle x|A|x\rangle &= \langle x|(A|x\rangle) = \lambda \ \|x\| \end{aligned}$$

and, therefore, $\lambda = \lambda^*$.

The eigenstates are orthogonal, because

$$\begin{aligned} A|x\rangle &= \lambda|x\rangle \\ A|y\rangle &= \mu|y\rangle \\ \langle x|A|y\rangle &= \lambda\langle x < y\rangle \overset{A=A^*}{=} \mu\langle x|y\rangle \end{aligned}$$

and, therefore, $\langle x|y\rangle = 0$[4].

In the language of quantum mechanics,

- the observables are hermitian operators
- the eigenvectors are the states the system ¨collapses¨ to
- the eigenvalues are the measurement outcomes

For degenerate eigenvalues, one can use a complete set of commuting observables **(CSCO)**.

Here are some examples for hermitian operators

◇ **projection operator** $P = |\Phi\rangle\langle\Phi|$
which projects any state collinearly to the state $|\Phi\rangle$ or some (possibly non-complete) set of operators

$$P = \sum_i |\Phi_i\rangle \langle\Phi_i| \,.$$

The eigenvalues of P_i are

$$\begin{aligned} \lambda_1 &= 1, \quad \text{degeneracy=1} \\ \lambda_2 &= 0, \quad \text{degeneracy=n-1} \end{aligned}$$

◇ **operator** $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$\begin{aligned} X|0\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \\ X|1\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \end{aligned}$$

This is the quantum mechanical analogue of a NOT-operator in classical computing. The eigenvalues and eigenvectors of X are

$$\begin{aligned} X|+\rangle &= \frac{1}{2}\left(X|0\rangle + X|1\rangle\right) = |+\rangle \;\rightarrow\; \lambda_1^X = 1,\ |\Phi_1^X\rangle = |+\rangle \\ X|-\rangle &= \frac{1}{2}\left(X|0\rangle - X|1\rangle\right) = -|-\rangle \;\rightarrow\; \lambda_2^X = -1,\ |\Phi_2^X\rangle = |-\rangle \end{aligned}$$

The operator X is the rotation around the vector along the x-axis of the Bloch sphere.

[3] up to degeneracy

[4] Strictly this only goes for non-degenerate eigenvalues ($\lambda \neq \mu$). For the degenerate subspace, one can orthogonalise the eigenstates that span it.

◇ **Pauli-matrices**

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

with the additional eigenvalues and -vectors

$$\begin{aligned} \lambda_1^Y &= 1: \; |\Phi_1^X\rangle = |\circlearrowleft\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{i}|1\rangle\right), \\ \lambda_2^Y &= -1: \; |\Phi_2^Y\rangle = |\circlearrowright\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - \mathrm{i}|1\rangle\right), \\ \lambda_1^Z &= 1: \; |\Phi_1^Z\rangle = |0\rangle, \\ \lambda_2^Z &= -1: \; |\Phi_2^Z\rangle = |1\rangle. \end{aligned}$$

◇ **Hadamard transform** $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ (very important for quantum algorithms)

$$\begin{aligned} H|0\rangle &= |+\rangle, \; H|+\rangle = |0\rangle, \\ H|1\rangle &= |-\rangle, \; H|-\rangle = |1\rangle. \end{aligned}$$

The eigenvalues and eigenvectors are

$$\begin{aligned} \lambda_1^H &= 1: |\Phi_1^H\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, \\ \lambda_2^H &= -1: |\Phi_2^H\rangle = \cos\frac{\pi}{8}|1\rangle - \sin\frac{\pi}{8}|0\rangle. \end{aligned}$$

◇ **conditional NOT (CNOT) operator**
...is another important unitary operator (which was introduced when we talked about entanglement in section 2.3) acting in a two-qubit space

$$\begin{aligned} \mathrm{CNOT} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ \mathrm{CNOT}|00\rangle &= |00\rangle \\ \mathrm{CNOT}|01\rangle &= |01\rangle \\ \mathrm{CNOT}|10\rangle &= |11\rangle \\ \mathrm{CNOT}|11\rangle &= |10\rangle \end{aligned}$$

- **evolution of quantum systems**

  The basis of a quantum system is changed according to

$$\begin{aligned} |\Phi\rangle &= \sum_{i=1}^{n} \alpha_i |\mathrm{e}_i\rangle = \sum_{i=1}^{n} \alpha_i \mathrm{I} |\mathrm{e}_i\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i |s_j\rangle\langle s_j|\mathrm{e}_i\rangle \\ &= \sum_{i=1}^{n} \alpha_i \sum_{j=1}^{n} |s_j\rangle \underbrace{\langle s_j|\mathrm{e}_i\rangle}_{U_{ji}/\alpha_i} = \sum_{j=1}^{n} U_{ij}|s_j\rangle \end{aligned}$$

The matrix U transforms from basis $\{|\mathrm{e}_i\rangle\}$ to $\{|\mathrm{s}_i\rangle\}$. Because $U^{-1} = U^*$, it is a unitary operator. Only unitary transformations can be used for computations (all quantum gates are unitary). All the before encountered operators (X, Y, Z, H) are unitary.

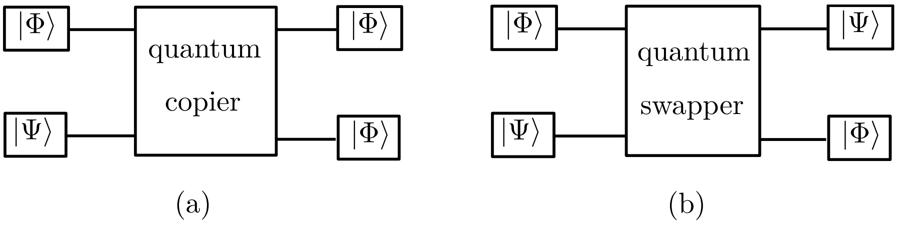


Figure 2.3: A schematic illustration of a quantum copier that overwrites the state $|\Psi\rangle$ in order to create a copy of $|\Phi\rangle$ in (a) and the quantum swapper that exchanges the states $|\Phi\rangle$ and $|\Psi\rangle$ from one quantum system to the other preserving angles and information in (b).

2.6 No cloning theorem

Can we make a copy of quantum data? Copying is some kind of observation. One can not read a quantum state without altering it. Maybe one can transfer the information to another quantum system without destroying the initial one.

We illustrate quantum algorithms by a special kind of notation. On the left side we write down all the quantum states that are utilised in the algorithm. From left to right we insert quantum gates that operate on those states. Gates on the left act before gates more right of them. The states and gates are connected by lines which indicate that those gates act on these specific states. So called conditional gates, i.e. gates that only act on qubits when other qubits are in particular states (here this is the $|1\rangle$ state), are illustrated with filled dots on the lines of the qubits that determine whether the gates act on the qubits with the gate on their respective line. An example can be seen in the SWAP operator in Figure 2.4 which employs several CNOT-gates. Conditional measurement gates are depicted by open circles like in the quantum teleportation operator in Figure 2.5.

In Figure 2.3(a), we show a schematic of a **quantum copier** that copies the state $|\Phi\rangle$ by overwriting the state $|\Psi\rangle$. Such a quantum copier can not be unitary as the state $|\Psi\rangle$ does not enter the result, i.e. it does not preserve angles. This result is known as the **No cloning theorem** and was proven by J. Park in 1970 and independently by W. Wooster, W. Zurek, and D. Dieks in 1982. An alternative to the quantum copier is the so called **quantum swap** and the **quantum teleportation** operations that can be seen in Figure 2.3(b). Hefig. re the information from one system whose state one wants wants to transfer to another system with a random state one does not care about. This is a weaker copy function which is unitary and can, hence, be implemented by quantum operations.

2.6.1 Quantum swap operator

The quantum SWAP operator is a operator that acts in the two-qubit space in the following way

$$\text{SWAP}|00\rangle = |00\rangle \tag{2.18}$$
$$\text{SWAP}|01\rangle = |10\rangle \tag{2.19}$$
$$\text{SWAP}|10\rangle = |01\rangle \tag{2.20}$$
$$\text{SWAP}|11\rangle = |11\rangle \tag{2.21}$$

and is, therefore, in the above basis represented by

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.22}$$

It can be realised by the quantum circuit in Figure 2.4 which is the **quantum swap algorithm**.

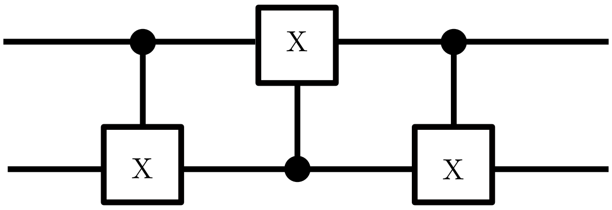


Figure 2.4: Quantum circuit realisation of the SWAP operator using CNOT gates

2.6.2 Quantum teleportation

In the quantum teleportation algorithm, the state of one qubit is transferred into another one by performing a preparation of the **destination qubit** and the **auxiliary qubit** which start of in the $|0\rangle$ state. After this preparation all three qubits are entangled and information can be transferred to the destination state, if one performs certain operations to it which depend on the outcomes of specific measurements on the other two qubits. The **quantum teleportation circuit**[5] is shown in Figure 2.5. In the following, I show the evolution of the states after the application of the respective gates. At the start, the three-qubit state is

$$|\Phi\rangle|0\rangle|0\rangle = (\alpha|0\rangle + \beta|1\rangle)\,|0\rangle|0\rangle, \tag{2.23}$$

because the state $|\Phi\rangle$ is an arbitrary state that we want to transfer. The state after the preparation (before the conditional measurement gates) is

$$\mathrm{H_1H_1C_1Z_2C_2X_3H_2}|\Phi\rangle|0\rangle|0\rangle \tag{2.24}$$

where the subscripts refer to the qubits that they act or on which they depend on, e.g. the gate $\mathrm{C_1Z_2}$ acts with a Z-gate on the second qubit when the first qubit is in the state $|1\rangle$. The qubits are enumerated from top to bottom, so the full initial state is $|\Phi\rangle_1|0\rangle_2|0\rangle_3$ and I drop the subscripts in the following. Next, I successively let the operators act:

$$\begin{aligned}
\mathrm{H_1H_1C_1Z_2C_2X_3H_2}|\Phi\rangle|0\rangle|0\rangle &= \mathrm{H_1H_2C_1Z_2C_2X_3}|\Phi\rangle|+\rangle|0\rangle \\
&= \mathrm{H_1H_2C_1Z_2}\frac{1}{\sqrt{2}}|\Phi\rangle\left(|00\rangle + |11\rangle\right) \\
&= \mathrm{H_1H_2}\frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle - \beta|111\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(\alpha|++0\rangle + \alpha|+-1\rangle + \beta|-+0\rangle - \beta|--1\rangle\right).
\end{aligned}$$

Now, we can simplify the resulting state further:

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\left(\alpha|++0\rangle + \alpha|+-1\rangle + \beta|-+0\rangle - \beta|--1\rangle\right) \\
&\quad = \frac{1}{2\sqrt{2}}\Big[(\alpha+\beta)|000\rangle + (\alpha+\beta)|010\rangle + (\alpha-\beta)|100\rangle + (\alpha-\beta)|110\rangle + (\alpha-\beta)|001\rangle \\
&\qquad\quad - (\alpha-\beta)|011\rangle + (\alpha+\beta)|101\rangle - (\alpha+\beta)|111\rangle\Big].
\end{aligned}$$

[5] The Nobel prize in physics was awarded to Anton Zeilinger in the year 2022 for the successful realisation of this algorithm by photons over a distance from the earth's surface to a satellite in the earths orbit.

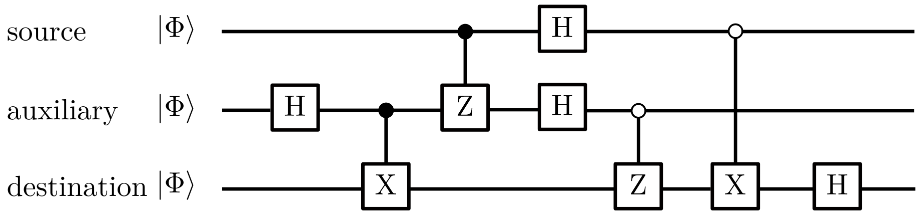


Figure 2.5: The quantum teleportation circuit which transfers the state of an arbitrary qubit $|\Phi\rangle$ into an destination state by appropriate pre- and postprocessing before and after successive measurements on this state and an auxiliary qubit

The measurements entangles the observer to the first two qubits. I indicate this by the subscript obs. It can easily be checked that the state after the measurements is

$$\begin{aligned}\frac{1}{2}\Big[\quad & |00\rangle_{\text{obs}}\left(\frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right) \\ & + |01\rangle_{\text{obs}}\left(\frac{\alpha+\beta}{\sqrt{2}}|0\rangle - \frac{\alpha-\beta}{\sqrt{2}}|1\rangle\right) \\ & + |10\rangle_{\text{obs}}\left(\frac{\alpha-\beta}{\sqrt{2}}|0\rangle + \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right) \\ & + |11\rangle_{\text{obs}}\left(\frac{\alpha-\beta}{\sqrt{2}}|0\rangle - \frac{\alpha+\beta}{\sqrt{2}}|1\rangle\right)\Big].\end{aligned}$$

The observer can recreate the initial state $|\Phi\rangle$ by applying the operator H_3 to the state in the first line, i.e. when he measured the state $|00\rangle$, the operator $(\mathrm{ZH})_3$ to the state in the second line, i.e. when he measured the state $|01\rangle$, the operator $(\mathrm{XH})_3$, i.e. when he measured the state $|10\rangle$, and the operator $(\mathrm{ZXH}_3$, i.e. when he measured the state $|11\rangle$. This is exactly what can be seen in the quantum teleportation circuit in Figure 2.5. Although the state $|\Phi\rangle$ is transferred into the destination state, this transfer needs the results of the measurement and, therefore, the information does not travel faster than light. The information in the state $|\Phi\rangle$ is destroyed by the measurement.

2.7 Exercises

1. We fired one electron from our electron gun. The position of the electron is defined by the wavefunction $f(r)$. What is the integral of $f^2(r)$ over the whole space?

2. Select all correct statements:

   ○ Multiplying a wavefunction by a number does not change its physical meaning. It still corresponds to the same physical state.

   ○ The set of all possible outcomes of the measurement forms the basis in the vector space of wavefunctions.

   ○ Light does not show interference in Young's interferometer. In 1905 Einstein showed that there is no interference of light on two slits, because light consists of invisible packets he called photons.

   ○ The set of all possible outcomes of the measurement is always infinite.

3. Is the Dirac delta function a square-integrable function?

4. Suppose we want to obtain more from the measurement process, se we perform it twice using the same observables. Select the correct statements:

   ○ Sometimes it might help...

○ The second measurement with the same observables does not help us to obtain more information, since after the first measurement the wavefunction collapses to one of the basis states, defined by the observable. The wavefunction decomposition after the first measurement becomes just this basis state with the probability amplitude equal to 1. So, the second measurement will give us the same state.

5. Do photons always travel in straight lines?

6. What is the dimensionality of the vector $|01101\rangle$?

7. If we measure the state $\frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$ in the basis $\{\,|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle\,\}$, we can obtain:

   ○ $|01\rangle$ with probability $\frac{1}{2}$ or $|10\rangle$ with probability $\frac{1}{2}$

   ○ $|00\rangle$ with probability $\frac{1}{2}$ or $|11\rangle$ with probability $\frac{1}{2}$

   ○ $|00\rangle$ with probability $\frac{1}{\sqrt{2}}$ or $|11\rangle$ with probability $\frac{1}{\sqrt{2}}$

8. Is the equality $|00\rangle + |11\rangle = (\,|0\rangle + |1\rangle\,) \otimes (\,|0\rangle + |1\rangle\,)$ correct?

9. The Stern-Gerlach experiment shows us that:

   ○ Some particles have a measurable property called spin. For silver atoms and electrons their spin along any axis has two distinguished values, thus they represent two-level systems and can be used for implementation of qubits.

   ○ Electrons in any atom rotate around its core in the same plane everywhere in the universe. Niels Bohr called this the greatest mystery of quantum mechanics.

10. The entangled states like $\frac{1}{\sqrt{2}}(\,|00\rangle+|11\rangle\,)$ or $\frac{1}{\sqrt{2}}(\,|01\rangle+|10\rangle\,)$ are interesting because (choose all correct answers):

    ○ These states appear when particles interact with each other. We can not prepare such states without particles interacting.

    ○ These are 4-qubit states the, the only known up to this moment.

    ○ If we measure one particle in this state, we actually measure both of them (even if the other particle is far away).

    ○ These are the states of two particles, however each of these particles does not have its own state.

    ○ These are the only quantum states we can implement on flipping coins.

11. $[X, Z] = \dots$

    ○ Y

    ○ $2XZ$

    ○ $0_{2,2}$

12. $X^* = \dots$

    ○ Y

    ○ Z

    ○ X

13. Is the identity operator I an observable?

    ○ Yes, however a useless one, since its only eigenvalue is n-fold degenerate.

    ○ No

14. $\langle -|1\rangle = \ldots$

    ○ $-\frac{1}{\sqrt{2}}$

    ○ 0

    ○ $\sqrt{2}$

    ○ $\frac{1}{\sqrt{2}}$

15. $\big(|\phi\rangle\langle\psi|AB\big)^* = \ldots$

    ○ $B^*A^*|\psi\rangle\langle\phi|$

    ○ $\langle\phi|\psi\rangle A^*B^*$

Chapter 3

Quantum cryptography protocols

The no-cloning theorem from section 2.6 forbids the interception of a quantum state without destroying it. This fact is of utmost importance for cryptography, because it allows for safe exchange of keys. The standard formulation of **quantum cryptography** is that Alice and Bob want to correspond without Eve listening [1]. Alice and Bob have a secret key (shared key). While RSA is a much used classical message transfer system which is considered secure[2], I present the BB84 and the E91 quantum message transfer systems in the following two sections.

3.1 BB84 (C. Bennett, G. Brassard)

In this protocol Alice and Bob follow many steps:

1. Alice and Bob generate long enough sequences (from e.g. photon experiments). Alice needs two sequences A1 and A2 and Bob only needs only one B1.

2. They open a channel of communication (e.g. by exchanging photons)

3. The sequence A1 determines the basis in which Alice sends photon the photon: She sends it in the $\{|0\rangle, |1\rangle\}$ basis if her qubit in A1 is $|0\rangle$, and she transforms her photon into the Hadamard basis, if her photon in A1 is in state $|1\rangle$

4. The sequence A2 determines the value (polarisation) of the photon she sends: If her qubit in A2 is in state $|0\rangle$ she sends it in the state $|0\rangle$ and if her qubit is in state $|1\rangle$ in A2, she sends it in the state $|1\rangle$.

   The photons sent by Alice are random in two senses (basis and value)!!!

5. Bob receives random message B2 by Alice and measures his qubits according to his sequence B1

   $|0\rangle \rightarrow$ Bob measures in $\{|0\rangle, |1\rangle\}$ basis

   $|1\rangle \rightarrow$ Bob measures in Hadamard basis

6. Bob only obtains clear result when the sequences A1 and B1 coincide, else the result is random.

7. Bob saves his results.

8. Bob calls Alice and she gives him A1.

9. Bob returns correctly measured photons but **not** the results of the measurement.

[1] Often the names are shortened to A, B, and E

[2] A procedure we will learn how to break by the Shore quantum algorithms in section 7.5 and 11!

10. They both have a secure code no one else knows (shared secret key).

    If Eve listens, the photons disappear and Alice and Bob will find out if Eve does not send another photon to Bob. Eve can, however, not duplicate the photons because of the no cloning theorem. She can only send the same measured photon, but she does not know the basis she should choose (neither Bob's nor Alice's). Only with probability $P = \frac{1}{2} + \left(\frac{1}{2}\right)^3 = \frac{5}{8}$ is she correct in one qubit[3]. Hence, the probability of being right in every transferred qubit goes to zero as the number of bits grows.

11. Final Check: they choose a number of bits to exchange and test whether those are still correct (if Eve has not listened or made no mistake, there will be nothing wrong)

12. If something is wrong, they create a new key.

3.2 E91 (A. Eckard)

In this protocol, a third party (C) can help with the initial key creation which does not even need to be trusted. The third party gives Alice and Bob a pair of **entangled** photons (for each bit). Alice gets one and Bob the other. The measurement yields the same for Alice and Bob, (because the state is $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$). C does not know the result of the measurement, though! If Eve infiltrates C and sends photons in the non-entangled states $|00\rangle$ and $|11\rangle$, Alice and Bob can still communicate securely. Alice and Bob must agree beforehand for each photon pair whether they measure in the σ_Z or the Hadamard basis. This information can be shared by any insecure line. In the Hadamard basis, the result is just $|++\rangle$ or $|--\rangle$ when the entangled state is sent and Alice and Bob should receive the same result. This is not true when the non-entangled states are sent. So Alice and Bob can check whether their communication is secure by randomly checking measurement outcomes in the Hadamard basis and, therefore, discover Eve's intrusion.

3.3 Exercises

1. In the E91 protocol, if Alice and Bob successfully check 5 randomly chosen bits from their shared key, they obtain:

   ○ more than 96% confidence about the absence of intrusion
   ○ exactly 95% confidence about the absence of intrusion
   ○ more than 99% confidence about the absence of intrusion

2. The BB84 protocol is based on:

   ○ indivisibility of photons
   ○ the RSA algorithm
   ○ the no-cloning theorem
   ○ complexity of factoring composite numbers

3. Does quantum teleportation allows to transfer messages faster than light?

4. The no-cloning theorem is about:

   ○ impossibility to create a copy of an unknown quantum state
   ○ impossibility to create a copy of a known quantum state

[3] She either is correct in her chosen basis and measures the right result or she measures in the wrong basis, but by chance she measures the correct state and by chance Bob's measurement yields the correct result.

○ moral consequences of cloning a human being

5. SWAP$|0+\rangle = \ldots$:

○ $|1-\rangle$

○ $|-1\rangle$

○ $|+0\rangle$

Part II

Physical basics of quantum computing

Chapter 4

Introduction

The **qubit** is the unit amount of information in quantum computing. It has two orthonormal basis states $|0\rangle$ and $|1\rangle$ and can exist in a superposition of both states

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle,\ \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1.$$

4.1 Di Vincenzo criteria

The **Di Vincenzo criteria** list the minimal conditions on a system to realise a good basis for quantum computations:

1. A quantum physical system on which a qubit is realised must have two **distinguishable** orthogonal basis quantum states.

2. It must be **possible to prepare the system in any of these two quantum states**.

3. There must be a **procedure for measuring the qubit** (macroscopical distinguishability of the basis states).

4. One must be able to create a**universal set of quantum logic gates** (gates) for the qubit.

5. The **decoherence time** must be longer than the operating time of the quantum logic elements.

There is an additional condition to make the system useful for practical applications: The qubits and gates must be scalable, i.e. it must be possible to realise an arbitrary number of qubits and quantum gates.
Here are some examples:

- Polarisation of a photon

- Two level atoms (ground state and first excited state are energetically well-separated to all other excited states)

- Spin 1/2 systems

- Stern-Gerlach spin 1/2 systems

4.2 The Bloch sphere

A classical bit can store the information of a two-state object and n bits can store the information of a 2^n state system. The information capacity of a qubit can be seen in the **Bloch sphere**:

$$
\begin{aligned}
|\Psi\rangle &= \alpha|0\rangle + \beta|1\rangle \\
&\left.\begin{aligned}\alpha &= a\,\mathrm{e}^{\mathrm{i}\varphi} \\ \beta &= b\,\mathrm{e}^{\mathrm{i}\vartheta} \\ a^2+b^2 &= 1\end{aligned}\right\} a, b, \varphi, \vartheta \in \mathbb{R} \\
|\Psi\rangle &= \underbrace{\cos\frac{\theta}{2}}_{a}\mathrm{e}^{\mathrm{i}\varphi}|0\rangle + \underbrace{\sin\frac{\theta}{2}}_{b}\mathrm{e}^{\mathrm{i}\vartheta}|1\rangle \\
&= \mathrm{e}^{\mathrm{i}\varphi}\left(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}\mathrm{e}^{\mathrm{i}(\vartheta-\varphi)}|1\rangle\right) \\
&\simeq \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}\mathrm{e}^{\mathrm{i}\gamma}|1\rangle.
\end{aligned}
$$

To express the value/state of a qubit one needs only two real numbers θ and $\gamma(=\vartheta-\varphi)$.

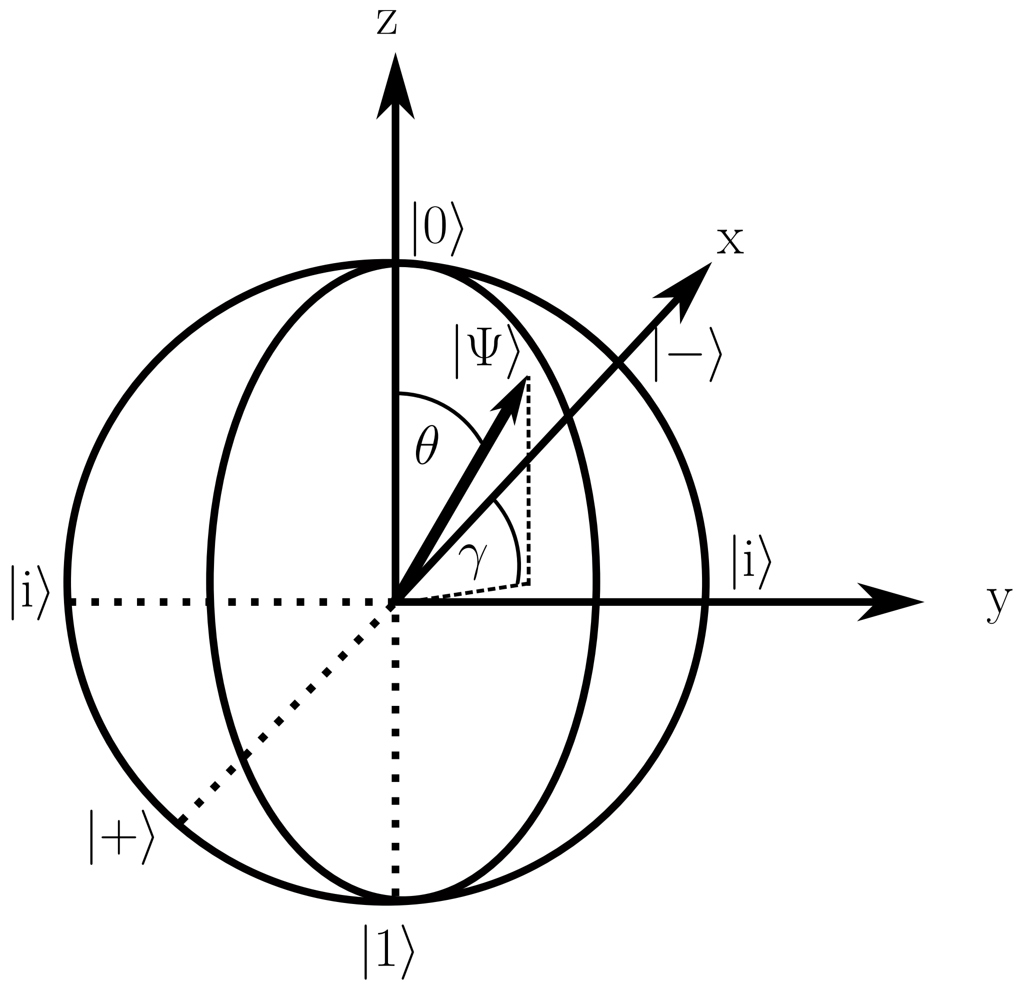


Figure 4.1: The Bloch sphere with the six most important basis states and the two angles γ (angle between state and z-axis) and θ (polar angle in the x-y axis) necessary to describe a general state $|\Psi\rangle$

The six states shown in Figure 4.1 are

$$\begin{aligned}
&|0\rangle,\ |1\rangle \text{ basis states belongs to z-axis,}\\
&|+\rangle \ = \frac{1}{\sqrt{2}}\left(|0\rangle +\ |1\rangle\right),\ |-\ \rangle\ = \frac{1}{\sqrt{2}}\left(|0\rangle -\ |1\rangle\right) \text{ belongs to x-axis,}\\
&|\mathrm{i}\rangle \quad = \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{i}|1\rangle\right),\ |-\mathrm{i}\rangle\ = \frac{1}{\sqrt{2}}\left(|0\rangle - \mathrm{i}|1\rangle\right) \text{ belongs to y-axis.}
\end{aligned}$$

For the case of a photon, the Bloch sphere is called a **Poincare sphere** and the states have a clear physical interpretation:

$$\begin{aligned}
|0\rangle &\hat{=} \text{ polarisation along y-axis,}\\
|1\rangle &\hat{=} \text{ polarisation along z-axis,}\\
|+\rangle &\hat{=} \text{ polarisation } \frac{\pi}{4} \text{ to z-axis (and lying in the y-z plane),}\\
|-\rangle &\hat{=} \text{ polarisation } \frac{\pi}{2} \text{ to z-axis (and lying in the y-z plane),}\\
|\ \ \mathrm{i}\rangle &\hat{=} \text{ right-hand circular polarised light,}\\
|-\mathrm{i}\rangle &\hat{=} \text{ left-hand circular polarised light.}
\end{aligned}$$

An infinite number of information can be encoded into one qubit, **BUT** one measurement will only give one of the two basis values. By measuring an ensemble of qubits in the same quantum state, one is able to know the **true** quantum state in the ensemble and, therefore, the encoded information. The full power of quantum computing can only be realised through the use of **entanglement** and **superposition**.

4.3 Quantum statistics of qubits

There are two kinds of states of a qubit system that need to be distinguished:

1. **pure states:** These states can be expressed as a superposition of basis states in a Hilbert space. A superposition of pure states is also a pure state:

$$|\Psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle + \cdots + c_N|\psi_N\rangle \tag{4.1}$$

the c_i are the probability amplitudes to observe the state $\psi_i\rangle$ after a measurement of the quantum system.

2. **mixed states:** These states are a statistical ensemble of pure states $\Big\{\{|\Psi_1\rangle, w_1\}, \{|\Psi_2\rangle, w_1\}, \ldots, \{|\Psi_N\rangle, w_N\}\Big\}$ with a classical probability w_k to be in state $\Psi_i\rangle$. Such states can **not** be expressed a superposition of pure states or a single ket vector. One uses the density matrix ϱ to describe the mixed states:

$$\varrho = \sum_{i=1}^{n} w_i|\Psi_i\rangle\langle\Psi_i|. \tag{4.2}$$

For a pure state $\varrho = |\Psi\rangle\langle\Psi|$.

4.3.1 Properties of the density matrix

- **positive semi-definiteness:** $\langle\Psi|\varrho|\Psi\rangle \geq 0\ \forall\ \Psi \in \mathcal{H}$
- **self-adjoint:** $\varrho = \varrho^\dagger$

- **trace one:** $\mathrm{Tr}(\varrho) = 1$

  proof:

$$\begin{aligned}\mathrm{Tr}(\varrho) &= \sum_i \langle n_i|\varrho|n_i\rangle = \sum_{i,j} w_j \langle n_i|\Psi_j\rangle\langle\Psi_j|n_i\rangle \\ &= \sum_j \langle\Psi| \sum_i |n_i\rangle\langle n_i|\Psi_j\rangle w_j = \sum_j w_j \langle\Psi_j|\mathrm{I}|\Psi_i\rangle = 1\end{aligned}$$

- **averaging property:**

$$\begin{aligned}\langle A\rangle = \mathrm{Tr}(\varrho A) &= \sum_i \langle n_i|\varrho A|n_i\rangle = \sum_{i,j} w_j \langle n_i|\Psi_j\rangle\langle\Psi_j|A|n_i\rangle = \sum_j w_j \langle\Psi_j|A \underbrace{\sum_i |n_i\rangle\langle n_i|}_{\mathrm{I}} \Psi_j\rangle \\ &= \sum_j w_j \langle\Psi_j|A|\Psi_j\rangle = \underline{\underline{\langle A\rangle}}\end{aligned}$$

If a closed quantum system is in a mixed state and is described by a density matrix ϱ, then its evolution is described using the Liouville quantum equation (von Neumann equation):

$$\mathrm{i}\hbar \frac{\partial}{\partial t}\varrho = [H, \varrho]. \tag{4.3}$$

The implementation of a quantum computer requires a physical system consisting of a large number of qubits. The Hilbert space of a physical system consisting of two qubits with Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, is a tensor product $\mathcal{H}^4 = \mathcal{H}_1^2 \otimes \mathcal{H}_2^2$. If $\Big\{|\Psi_1\rangle, |\Psi_2\rangle\Big\}$ is a basis in $\mathcal{H}_1^2$ and $\Big\{|\Phi_1\rangle, |\Phi_2\rangle\Big\}$ is a basis in $\mathcal{H}_2^2$, then the basis in $\mathcal{H}^4$ is a set $\Big\{|\Psi_i\rangle \otimes |\Phi_j\rangle\Big\}_{i,j=1}^2$ $\Big(\text{or } \Big\{|\Psi_i\Phi_j\rangle\Big\}_{i,j=1}^2\Big)$.
The same goes for operators, **but be careful**: $A \otimes B \neq B \otimes A$!
For states with more than one qubit, entangled states arise.
A two qubit state $|\zeta\rangle = \sum\limits_{i=1}^{2}\sum\limits_{j=1}^{2} c_{ij}|\psi_i\rangle \otimes |\phi\rangle$ is pure if $|\zeta\rangle = |\zeta_1\rangle + |\zeta_2\rangle$ with $|\zeta_1\rangle \in \mathcal{H}_1, |\zeta_2\rangle \in \mathcal{H}_2$. Such states are called **separable** and otherwise the state is **entangled** (or **inseparable**). A similar definition holds for mixed states and the density matrix, i.e. $\varrho = \varrho_1 \otimes \varrho_2$ is called separable and $\varrho \neq \varrho_1 \otimes \varrho_2$ is inseparable.

4.3.2 Reduced density matrix

If a system consists of two subsystems A and B which is described by a density operator ϱ_{AB}, then one can define so-called **reduced density operators** of the subsystems $\varrho_{\mathrm{A/B}}$ with expectation values of operators $L_{\mathrm{A/B}}$ in the subsystems

$$\langle L_\mathrm{A}\rangle_\mathrm{A} = \mathrm{Tr}(L_\mathrm{A}\varrho_\mathrm{A}) \quad \text{with } \varrho_\mathrm{A} = \mathrm{Tr}_\mathrm{B}(\varrho_\mathrm{AB}) \tag{4.4}$$

$$\varrho_\mathrm{A} = \sum_{j=1}^{M} \left(\mathrm{I}_\mathrm{A}^{N\times N} \otimes \langle\xi_j|\right) \varrho_\mathrm{AB} \left(\mathrm{I}_\mathrm{A}^{N\times N} \otimes |\xi_j\rangle\right) \tag{4.5}$$

$$\varrho_\mathrm{B} = \sum_{j=1}^{N} \left(\langle\zeta_j| \otimes \mathrm{I}_\mathrm{B}^{M\times M}\right) \varrho_\mathrm{AB} \left(|\zeta_j\rangle \otimes \mathrm{I}_\mathrm{B}^{M\times M}\right) \tag{4.6}$$

here $\mathrm{Tr}_{\mathrm{A/B}}(\dots)$ is the trace over the basis in the respective subsystem, e.g.
$\mathrm{Tr}_\mathrm{A}(\dots) = \sum\limits_i \langle\Psi_\mathrm{A}| \otimes \mathrm{I}_\mathrm{B}(\dots)|\Psi_\mathrm{A}\rangle \otimes \mathrm{I}_\mathrm{B}$. These reduced density matrices have the following properties:

- **self-conjugation** $\varrho_\mathrm{A} = \varrho_\mathrm{A}^\dagger$, $\varrho_\mathrm{B} = \varrho_\mathrm{B}^\dagger$

- **positive definiteness**

$$\begin{array}{ll}\langle\Psi_{\mathrm{A}}|\varrho_{\mathrm{A}}|\Psi_{\mathrm{A}}\rangle & \geq 0 \;\forall\; \Psi_{\mathrm{A}} \in \mathcal{H}_{\mathrm{A}} \\ \langle\Phi_{\mathrm{B}}|\varrho_{\mathrm{B}}|\Phi_{\mathrm{B}}\rangle & \geq 0 \;\forall\; \Phi_{\mathrm{B}} \in \mathcal{H}_{\mathrm{B}}\end{array}$$

- **equality in retracing**

$$\begin{array}{lcl}\mathrm{Tr}_{\mathrm{A}}(\varrho_{\mathrm{AB}}) & \neq & \mathrm{Tr}_{\mathrm{B}}(\varrho_{\mathrm{AB}}) \\ \mathrm{Tr}(\varrho_{\mathrm{B}}) & = & \mathrm{Tr}(\varrho_{\mathrm{A}})\end{array}$$

- **equality of determinants**

$$\begin{array}{lcl}\det\left(\mathrm{Tr}_{\mathrm{A}}(\varrho_{\mathrm{AB}})\right) & = & \det\left(\mathrm{Tr}_{\mathrm{B}}(\varrho_{\mathrm{AB}})\right) \\ \det\varrho_{\mathrm{B}} & = & \det\varrho_{\mathrm{A}}\end{array}$$

For a separable system no information is lost in the tracing process over one of the subsystems, but for entangled states some information on the subsystem that is traced out is lost.

4.3.3 Schmidt decomposition

Theorem: For a pure state $|\Psi^{\mathrm{AB}}\rangle$ of a composite quantum system "A+B" there exists a set of orthonormal states $\{|\xi_i^{\mathrm{A}}\rangle\}$ of system "A" and a set of orthonormal states $\{|$
$phi_i^{\mathrm{B}}\rangle\}$ of system "B" such that

$$|\Psi^{\mathrm{AB}}\rangle = \sum_i \sqrt{\lambda_i}|\xi_i^{\mathrm{A}}\rangle \otimes |\phi_i^{\mathrm{B}}$$

with $\{\sqrt{\lambda_i}\}$ being non-negative real numbers such that $\sum\limits_i \lambda_i = 1$. The numbers $\{\sqrt{\lambda_i}\}$ are called the **Schmidt coefficients**. The number of non-zero Schmidt coefficients is called the **Schmidt number**. A pure quantum state is called separable if the Schmidt number is one, i.e. the composite system state vector can be represented as a tensor product of each of the state's vectors:

$$|\Psi^{\mathrm{AB}}\rangle = |\xi^{\mathrm{A}}\rangle \otimes |\phi^{\mathrm{B}}\rangle.$$

A pure state is called entangled if the Schmidt number is greater than one. Therefore, the Schmidt number can be used as a criterion of a state's separability.

4.4 Bell states (EPR pairs)

The most entangled states of two qubits are called **Bell states**. These are the four states

$$
\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big)\\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big)\\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big)\\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big)
\end{aligned}
$$

All of these states are either totally correlated or anticorrelated. Most entangled means that

$$
\begin{aligned}
\varrho_{\mathrm{A}} &= \mathrm{Tr}_{\mathrm{B}}\Big(|\beta_{ij}\rangle\langle\beta|\Big) = \frac{1}{2}\mathrm{I}_{\mathrm{A}}\\
\varrho_{\mathrm{B}} &= \mathrm{Tr}_{\mathrm{A}}\Big(|\beta_{ij}\rangle\langle\beta|\Big) = \frac{1}{2}\mathrm{I}_{\mathrm{B}}
\end{aligned}
$$

for the reduced density matrices, i.e. the result of a measurement is completely random!!!
The four Bell states form an orthonormal basis for a two qubit Hilbert space. Therefore, the measurement of qubits should be proceeded in the appropriate basis. The measurement of a qubit in a Bell state could be done using the scheme (Bell measurements) shown in Figure 4.2 which transform the Bell states in the following way:

$$|\beta_{00}\rangle \to |00\rangle,\ |\beta_{01}\rangle \to |01\rangle,\ |\beta_{10}\rangle \to |10\rangle,\ |\beta_{11}\rangle \to |11\rangle.$$

Entangled states are particularly interesting as they manifest correlations which do not have any classical analogues. The intrinsic feature of the correlation is their **nonlocality**. To entangle a pair of quantum systems one should bring them into interaction with each other (directly or via a auxiliary system), i.e. one should perform a **collective unitary** transformation on the composed system. Bell states are widely used in quantum informatics and quantum telecommunication, e.g. in superdense coding and quantum teleportation which we will discuss soon!

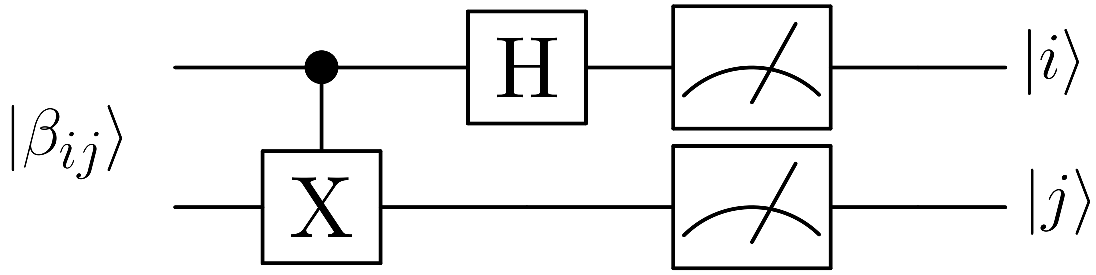


Figure 4.2: The quantum circuit for a Bell measurement. The input $|\beta_{ij}\rangle$ is one of the Bell state and the result is a certain measurement of the separable state $|i\rangle \otimes |j\rangle$.

4.4.1 Bell inequalities

The theory of hidden variables is contrary to quantum mechanics. Bell inequalities are a set of experiments which allow one to compare the predictions of hidden variables conception and quantum mechanics predictions: A quantum system composed of two subsystems "A+B" with observables L_{A} and L'_{A} in system A and observables M_{B} and M'_{B} in system B with a simple spectrum $\{-1, 1\}$ for each observable. If these observables are physical reality, i.e. their eigenvalues are possible, there should exist a spectrum $\{l_i^{\mathrm{A}}, l_j'^{\mathrm{A}}, m_k^{\mathrm{B}}, m_n'^{\mathrm{B}}\}_{i,j,k,n=1,2}$ which could have been obtained. This gives rise to 16 states/possibilities/sets defined by the observable

$$s_{ijkn} = \Big(l_i^{\mathrm{A}} + l_j'^{\mathrm{A}}\Big)m_k^{\mathrm{B}} + \Big(-l_i^{\mathrm{A}} + l_j'^{\mathrm{A}}\Big)m_n'^{\mathrm{B}}.$$

Obviously, $|s_{ijkn}| \leq 2$, so when taking the ensemble average $(N \gg 1)$, we get

$$\begin{aligned}|\langle S\rangle| = \frac{1}{N}\Bigg|\sum_{i,j,k,n} s_{ijkn} \underbrace{N_{ijkn}}_{\text{number of results with } s_{ijkn}}\Bigg| &= \Bigg|\sum_{i,j,k,n} s_{ijkn} \underbrace{p_{ijkn}}_{\text{probability of } s_{ijkn}}\Bigg| \\ \leq 2\Bigg|\sum_{i,j,k,n} p_{ijkn}\Bigg| &= 2.\end{aligned}$$

Therefore, $|\langle S\rangle| \leq 2$ or in other words by using the definition of S

$$|\langle S\rangle| = \Big|\langle L_{\mathrm{A}}M_{\mathrm{B}}\rangle - \langle L_{\mathrm{A}}M'_{\mathrm{B}}\rangle + \langle L'_{\mathrm{A}}M_{\mathrm{B}}\rangle + \langle L'_{\mathrm{A}}M'_{\mathrm{B}}\rangle\Big| \leq 2.$$

These are the famous **Bell inequalities**.
In the quantum version

$$[L_{\mathrm{A}}, L'_{\mathrm{A}}] \neq 0 \text{ and } [M_{\mathrm{A}}, M'_{\mathrm{A}}] \neq 0.$$

Because of the spectrum of all operators

$$L_{\mathrm{A}}^2 = L_{\mathrm{A}}'^2 = M_{\mathrm{B}}^2 = M_{\mathrm{B}}'^2 = \mathrm{I}$$

We can define the operator $\hat{S}$ analogues to the classical S

$$\hat{S} = L_{\mathrm{A}}M_{\mathrm{B}} - L_{\mathrm{A}}M'_{\mathrm{B}} + L'_{\mathrm{A}}M_{\mathrm{B}} + L'_{\mathrm{A}}M'_{\mathrm{B}}.$$

The **Tsirelson bound** for $|\hat{S}|$ is

$$\begin{aligned}2\sqrt{2}\mathrm{I} - \hat{S} &= \frac{2\sqrt{2}}{4}\Big(L_{\mathrm{A}}^2 + L_{\mathrm{A}}'^2 + M_{\mathrm{B}}^2 + M'^2\Big) - \hat{S} \\ &= \frac{1}{\sqrt{2}}\Big(L'_{\mathrm{A}} - \frac{M_{\mathrm{B}} + M'_{\mathrm{B}}}{\sqrt{2}}\Big)^2 + \Big(L_{\mathrm{A}} - \frac{M_{\mathrm{B}} - M'_{\mathrm{B}}}{\sqrt{2}}\Big)^2 \Rightarrow \underline{\underline{0 \leq 2\sqrt{2}\langle\mathrm{I}\rangle - \langle\hat{S}\rangle}}\end{aligned}$$

and therefore $\langle\hat{S}\rangle \leq 2\sqrt{2}$ and analogously one shows $\langle\hat{S}\rangle \geq -2\sqrt{2}$ and, hence, for the quantum system $|\langle\hat{S}\rangle| \leq 2\sqrt{2}$. When the Tsirelson bound is reached in an experiment, then the Bell inequalities are violated and quantum theory can be considered to be correct.

4.5 Exercises

1. In classical information theory, how much bits are required to describe a certain value, if it can take n possible values?

   ○ $\exp\left(n^2\right)$

   ○ $\log_2 n$

   ○ $2\log n$

   ○ $\log n^2$

2. What is the correct way to write a qubit $|\phi\rangle = \frac{\mathrm{e}^{\mathrm{i}\alpha}}{\sqrt{5}}|0\rangle - \sqrt{\frac{4}{5}}|1\rangle$ in the form of a two-dimensional column vector?

   ○ $\begin{pmatrix} \mathrm{e}^{2\mathrm{i}\alpha}/5 \\ 4/5 \end{pmatrix}$

   ○ $\begin{pmatrix} \mathrm{e}^{\mathrm{i}\alpha}/5 \\ -\sqrt{4/5} \end{pmatrix}$

   ○ $\begin{pmatrix} \mathrm{e}^{\mathrm{i}\alpha}/5 \\ \sqrt{4/5} \end{pmatrix}$

   ○ $\begin{pmatrix} 1/5 \\ 4/5 \end{pmatrix}$

3. Match the positive directions of the axes on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|0\rangle$

   ○ positive direction x

   ○ negative direction x

   ○ positive direction y

   ○ negative direction y

   ○ positive direction z

   ○ negative direction z

4. Match the positive directions of the axies on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|1\rangle$

   ○ positive direction x

   ○ negative direction x

   ○ positive direction y

   ○ negative direction y

   ○ positive direction z

   ○ negative direction z

5. Match the positive directions of the axies on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|+\rangle$

   ○ positive direction x

   ○ negative direction x

○ positive direction y

○ negative direction y

○ positive direction z

○ negative direction z

6. Match the positive directions of the axies on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|-\rangle$

   ○ positive direction x

   ○ negative direction x

   ○ positive direction y

   ○ negative direction y

   ○ positive direction z

   ○ negative direction z

7. Match the positive directions of the axies on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|\mathrm{i}\rangle$

   ○ positive direction x

   ○ negative direction x

   ○ positive direction y

   ○ negative direction y

   ○ positive direction z

   ○ negative direction z

8. Match the positive directions of the axies on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|-\mathrm{i}\rangle$

   ○ positive direction x

   ○ negative direction x

   ○ positive direction y

   ○ negative direction y

   ○ positive direction z

   ○ negative direction z

9. What physical systems (and their characteristics) can be used to implement the qubit? (Select all that applies)

   ○ two orthogonal photon polarisations

   ○ projection of electron spin on the selected direction

   ○ energy levels of the ¨two-level atom¨

10. Which of the following expressions describe the pure state of a quantum system in the two-dimensional Hilbert space? $|\psi_1\rangle$ and $|\psi_2\rangle$ are elements of the considered space, constituting its complete set ($|c_1|^2 + |c_2|^2 = 1$)

    (Select all that applies)

○ $c_1 |\psi_2\rangle + c_2\big(|\psi_1\rangle\big)^{1/2}$

○ $\sqrt{\frac{3}{5}}\,|\psi_1\rangle - \sqrt{\frac{2}{5}}\,|\psi_2\rangle$

○ $c_1 |\psi_1\rangle + c_2 |\psi_2\rangle$

○ $\hat{\varrho} = |\phi_2\rangle \langle\phi_2|$

11. Select the correctly written statistical operators, if $\omega_1 + \omega_2 + \omega_3 = 1$:

○ $\hat{\varrho} = \frac{1}{2}\,|\phi_1\rangle\langle\phi_2| + \sum\limits_{i=2}^{3} \omega\,|\phi_i\rangle\langle\phi_i|$

○ $\hat{\varrho} = \omega_1 |\phi_1\rangle\langle\phi_1| + \omega_2^2 |\phi_2\rangle\langle\phi_2| + \omega_3^3 |\phi_3\rangle\langle\phi_3|$

○ $\hat{\varrho} = \omega_1 |\phi_1\rangle\langle\phi_1| + \omega_2^2 |\phi_2\rangle\langle\phi_2| + \omega_3^3 |\phi_3\rangle\langle\phi_3|$

○ $\hat{\varrho} = \frac{\sqrt{2}}{9}\,|\phi_1\rangle\langle\phi_1| + \frac{5-\sqrt{2}}{9}\,|\phi_2\rangle\langle\phi_2| + \frac{4}{9}\,|\phi_3\rangle\langle\phi_3|$

○ $\hat{\varrho} = \omega_2 |\phi_1\rangle\langle\phi_1| + \omega_3 |\phi_2\rangle\langle\phi_2|$

12. Choose the correct properties of the density matrix, if $\langle\hat{A}\rangle$ is the average value of the operator $\hat{A}$.

○ $\hat{\varrho}^\dagger = \hat{\varrho}$

○ $\langle\psi|\hat{\varrho}|\psi\rangle = 1/2$

○ $0 \le \mathrm{Tr}(\hat{\varrho}) \le 1$

○ $\langle\hat{A}\rangle = \mathrm{Tr}(\hat{A}\hat{\varrho})$

13. Is the following statement true? If an open quantum system is in a mixed state, then its evolution can be described using the Liouville quantum equation $i\hbar\frac{\partial}{\partial t}\hat{\varrho} = [\hat{H}, \hat{\varrho}]$.

14. The operators $\hat{A}_1^{(1)}, \hat{A}_2^{(1)}, \hat{A}_3^{(1)}$ act only on qubit ¨1¨,$\hat{B}_1^{(2)}, \hat{B}_2^{(2)}$ act only on qubit ¨2¨, and $\hat{C}^{(3)}$ act only on qubit ¨3¨. Choose identical equations that correspond to the action of all these operators on the system consisting of given independent qubits

(a) $\hat{A}_1^{(1)}\hat{A}_1 \otimes \hat{B}^{(2)} \otimes \hat{C}^{(3)}$ where $\hat{A}^{(1)} = \hat{A}_2^{(1)}\hat{A}_3^{(1)}, \hat{B}^{(2)} = \hat{B}_1^{(2)}\hat{B}_2^{(2)}$

(b) $\hat{C}^{(3)}\hat{B}_1^{(2)}\hat{B}_2^{(2)}\hat{A}_1^{(1)}\hat{A}_2^{(1)}\hat{A}_3^{(1)}$

(c) $\hat{A}_1^{(1)}\hat{A}_2^{(1)}\hat{A}_3^{(1)}\hat{C}^{(3)}\hat{B}_1^{(2)}\hat{B}_2^{(2)}$

(d) $\hat{A}_1^{(1)}\hat{A}_2^{(1)}\hat{A}_3^{(1)}\hat{B}_1^{(2)}\hat{B}_2^{(2)}\hat{C}^{(3)}$

○ only (d)

○ only (a) and (c)

○ only (b), (c), and (d) are identical to each other

○ all equations are identical

15. Can an entangled state be pure?

16. Can a mixed state of two systems be inseparable?

17. Is the state $|\psi_1\rangle \otimes |\psi_2\rangle$ indicating that the two systems are inseparable?

18. Is the state characterised by the statistical operator $\sum\limits_{k=1}^{n} \omega_k \hat{\varrho}_1^k \otimes \hat{\varrho}_2^k$ separable, if $\hat{\varrho}_1^k$ and $\hat{\varrho}_2^k$ are mixed states in the Hilbert spaces $\mathcal{H}_1^2$ and $\mathcal{H}_2^2$, respectively, and with $\sum\limits_{k=1}^{n} \omega_k = 1$?

19. There is a physical system consisting of two subsystems ¨A¨ and ¨B¨ and described by a density matrix $\hat{\varrho}_{A,B}$. Which of the following equations can be used to find the reduced density matrix $\hat{\varrho}_B$?

   ○ $\hat{\varrho}_B = \mathrm{Tr}_A(\hat{\varrho}_{AB})$

   ○ $\hat{\varrho}_B = \mathrm{Tr}_B(\hat{\varrho}_{AB})$

20. Select the correct properties of the reduced density matrix

   ○ $\hat{\varrho}_A \neq \hat{\varrho}_B^\dagger$

   ○ $\mathrm{Tr}\Big(\mathrm{Tr}_A(\hat{\varrho}_{AB})\Big) \neq \mathrm{Tr}\Big(\mathrm{Tr}_B(\hat{\varrho}_{AB})\Big)$

   ○ $\langle\psi_A|\hat{\varrho}_A|\psi_A\rangle \geq 0, \langle\psi_B|\hat{\varrho}_B|\psi_B\rangle \leq 0$ where $\forall\,|\psi_A\rangle \in \mathcal{H}_A,\ |\psi_B\rangle \in \mathcal{H}_B$

21. A pair of qubits are in states written as column vectors:

$$|\psi_1\rangle = \begin{pmatrix} \cos\theta_1 \\ \sin\theta_1 \end{pmatrix},$$
$$|\psi_2\rangle = \begin{pmatrix} \cos\theta_2 \\ \sin\theta_2 \end{pmatrix}.$$

   Each of these states is normalised to one. For which $\theta_1 - \theta_2$ will the expression $|\psi_1\rangle - |\psi_2\rangle$ also be normalised?

   ○ $\pm\pi/3$

   ○ $\pm\pi/4$

   ○ $\pm 3\pi/4$

   ○ $\pm 2\pi/3$

22. Where is the state vector

$$\frac{1}{\sqrt{2+\sqrt{2}}}\left(\frac{\sqrt{2}+1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\right)$$

   directed on the Bloch sphere?

   ($\mathrm{e}_x, \mathrm{e}_y, \mathrm{e}_z$ are the unit vectors on the Bloch sphere)

   ○ It coincides with the direction of the vector $\mathrm{e}_z + \mathrm{e}_x$

   ○ It coincides with the direction of the vector $\mathrm{e}_z - \mathrm{e}_y$

   ○ It coincides with the direction of the vector $\mathrm{e}_x + \mathrm{e}_y$

   ○ It coincides with the direction of the vector $\mathrm{e}_z - \mathrm{e}_x$

23. Based on the definition of the statistical operator and the identity operator, determine whether the equality

$$\mathrm{Tr}\left(\hat{L}\hat{\varrho}\right) = \mathrm{Tr}\left(\hat{\varrho}\hat{L}\right)$$

   is true or false.

   Here $\hat{L}$ is an operator acting in the state space $|u_k\rangle$, $\hat{\varrho} = \sum\limits_n p_n\,|\psi_n\rangle\,\langle\psi_n|$ with the probability p_n that the system is described by a state vector $|\psi_n\rangle$ and $\sum\limits_n p_n = 1$, as well as $\mathrm{I} = \sum\limits_{k=1}^{n} |u_k\rangle\,\langle u_k|$ with $\{\,|u_k\rangle\,\}$ are basic states that form a complete orthonormal set and $|\psi_n\rangle$ are pure states formed by linear combination of $|u_k\rangle$.

24. Based on the definition, find the density matrices for the following states and match them with the suggested answer choices.

    $\{(|0\rangle, p_0 = 2/3), (|1\rangle, p_0 = 1/3)\}$ where p_0 and p_1 are the probabilities that the system is described by the state vectors $|0\rangle$ and $|1\rangle$, respectively. $p_0 + p_1 = 1$.

    ○ $\frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$

    ○ $\frac{2}{3}|0\rangle\langle 1| + \frac{1}{3}|1\rangle\langle 0|$

    ○ $\frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1| + \frac{\sqrt{2}}{3}(|0\rangle\langle 1| + |1\rangle\langle 0|)$

    ○ $\frac{2}{3}|0\rangle\langle 1| + \frac{1}{3}|1\rangle\langle 0| + \frac{\sqrt{2}}{3}(|0\rangle\langle 0| + |1\rangle\langle 1|)$

25. Based on the definition, find the density matrices for the following states and match them with the suggested answer choices.

    $\sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$

    ○ $\frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$

    ○ $\frac{2}{3}|0\rangle\langle 1| + \frac{1}{3}|1\rangle\langle 0|$

    ○ $\frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1| + \frac{\sqrt{2}}{3}(|0\rangle\langle 1| + |1\rangle\langle 0|)$

    ○ $\frac{2}{3}|0\rangle\langle 1| + \frac{1}{3}|1\rangle\langle 0| + \frac{\sqrt{2}}{3}(|0\rangle\langle 0| + |1\rangle\langle 1|)$

26. Is it true that for an arbitrary state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the state basis $\{|0\rangle, |1\rangle\}$ the inequality

    $$\mathrm{Tr}(|\phi\rangle\langle\phi|) \geq \mathrm{Tr}(\langle\phi|\phi\langle)$$

    holds?

27. Let $|\psi\rangle = \sin\theta|0\rangle + \mathrm{e}^{\mathrm{i}(\phi+\tan\theta)}\cos\theta|1\rangle$ with $\theta, \phi \in \mathbb{R}$. Determine whether $\hat{\varrho} = |\psi\rangle\langle\psi|$ is a statistical operator

    (Hint check the three basic properties of a density matrix:

    1. $\hat{\varrho}^\dagger = \hat{\varrho}$

    2. $\mathrm{Tr}(\hat{\varrho}) = 1$

    3. $\langle\alpha|\hat{\varrho}|\alpha\rangle \geq 0$, here $|\alpha\rangle$ is a state vector from the same state space $\{|0\rangle, |1\rangle\}$ in which $|\psi\rangle$ is defined, i.e. $|\alpha\rangle$ is some linear superposition of state vectors $|0\rangle$ and $|1\rangle$.)

28. The quantum system consists of 3 subsystems. Its state is defined by Schmidt decomposition $\left|\psi^{ABC}\right\rangle = \sum_{i=1}^{n}\sqrt{\lambda_i}\left|\phi_i^A\right\rangle\left|\phi_i^B\right\rangle\left|\phi_i^C\right\rangle$. What is the state of the system if the number of expansion coefficients λ_i is $n = 1$.

    ○ entangled state (inseparability)

    ○ separable state

29. The quantum system consists of 3 subsystems. Its state is defined by Schmidt decomposition $\left|\psi^{ABC}\right\rangle = \sum_{i=1}^{n}\sqrt{\lambda_i}\left|\phi_i^A\right\rangle\left|\phi_i^B\right\rangle\left|\phi_i^C\right\rangle$. What is the state of the system if the number of expansion coefficients λ_i is $n = 4$.

    ○ entangled state (inseparability)

    ○ separable state

30. Which of the Bell states is called the ¨singlet state¨?

    ○ $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

- ○ $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle\,)$
- ○ $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$
- ○ $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle - |10\rangle\,)$

31. A pair of electrons is in a joint state $\frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$ is passing through a Stern-Gerlach device. One of the electrons leans upwards. Where will the other electron deviate in this case?

    - ○ upwards
    - ○ downwards
    - ○ leftwards
    - ○ rightwards

32. A pair of particles is in the Bell state $\frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle\,)$. One of the particles is measured in the corresponding basis $\{\,|0\rangle\,, |1\rangle\,\}$. What is the probability of the second particle becoming $|1\rangle$ at the moment when the first particle has been measured?

    - ○ $1/2^{1/4}$
    - ○ $1/2^{1/2}$
    - ○ $1/2$
    - ○ 1

33. Answer yes or no: The Copenhagen interpretation of quantum mechanics (Niels Bohr) is based on Laplace determinism.

34. Answer yes or no: The concept of hidden parameters (Albert Einstein) suggests that the values we get during an experiment are determined in advance. But since there are a lot of variables, we do not take them all into account. Therefore, the values in the course of the experiment seem random and we only produce a statistical averaging over them.

35. Answer yes or no: The Copenhagen interpretation argues that there is no point in discussing any physical results without additional description of the instruments which they were obtained with.

36. Answer yes or no: In the concept of hidden variables the process of measurement of an observable $\hat{L}$ is as follows: The device decomposes the quantum state of the system on its own basis of macroscopically distinguishable states. Then, in the measurement process, one of these basis states is triggered.

37. What did the experiment to test Bell's inequality determine?

    - ○ The classical concept of hidden variables does not describe the quantum behaviour of systems.
    - ○ The Copenhagen interpretation of quantum mechanics is consistent with the experiments.
    - ○ Laplace determinism allows us to describe the behaviour of quantum systems.

38. If Bell's inequalities are violated:

    - ○ Quantum mechanics is correct
    - ○ The concept of hidden variables is correct

39. If Bell's inequalities are satisfied:

○ Quantum mechanics is correct

○ The concept of hidden variables is correct

40. Bell's inequalities are constructed on the basis of classical probability theory. As a result, there is an estimated value S_{cl} which can be measured in the experiment. Quantum theory also gives the value of the quantity S_q. Which of the values is greater in case of violation of the inequalities?

○ $S_{cl} < S_q$

○ $S_{cl} > S_q$

○ $S_{cl} = S_q$

41. Find the Schmidt decomposition coefficients λ_i (i=1,2,3,4) for the states of the composite system A+B

$$\left|\psi^{AB}\right\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$$

Here the state of each subsystem belongs to a two-dimensional basis $\{\,|0\rangle\,,|1\rangle\,\}$, i.e. the vectors $\left|\psi^{AB}\right\rangle$ belong to a four-dimensional Hilbert space $\{\,|00\rangle\,,|01\rangle\,,|10\rangle\,,|11\rangle\,\}$.

○ $\lambda_1 = 1/2, \lambda_2 = 0, \lambda_3 = 0, \lambda_4 = 1/2$

○ $\lambda_1 = 1, \lambda_2 = 0, \lambda_3 = 0, \lambda_4 = 0$

42. Find the Schmidt decomposition coefficients λ_i (i=1,2,3,4) for the states of the composite system A+B

$$\left|\psi^{AB}\right\rangle = |00\rangle$$

Here the state of each subsystem belongs to a two-dimensional basis $\{\,|0\rangle\,,|1\rangle\,\}$, i.e. the vectors $\left|\psi^{AB}\right\rangle$ belong to a four-dimensional Hilbert space $\{\,|00\rangle\,,|01\rangle\,,|10\rangle\,,|11\rangle\,\}$.

○ $\lambda_1 = 1/2, \lambda_2 = 0, \lambda_3 = 0, \lambda_4 = 1/2$

○ $\lambda_1 = 1, \lambda_2 = 0, \lambda_3 = 0, \lambda_4 = 0$

43. There are two subsystems, A and B, in one of the Bell states. Find the reduced density matrix $\hat{\varrho}_B = \mathrm{Tr}_A(\varrho_{AB})$ for the Bell state

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$$

○ $\begin{pmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix}$

○ $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$

○ $\begin{pmatrix} 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 \end{pmatrix}$

○ $\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$

44. There are two subsystems, A and B, in one of the Bell states. Find the reduced density matrix $\hat{\varrho}_B = \mathrm{Tr}_A(\varrho_{AB})$ for the Bell state

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle\,)$$

○ $\begin{pmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix}$

○ $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$

○ $\begin{pmatrix} 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 \end{pmatrix}$

○ $\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$

45. There are two subsystems, A and B, in one of the Bell states. Find the reduced density matrix $\hat{\varrho}_B = \mathrm{Tr}_A(\varrho_{AB})$ for the Bell state

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$$

○ $\begin{pmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix}$

○ $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$

○ $\begin{pmatrix} 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 \end{pmatrix}$

○ $\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$

46. There are two subsystems, A and B, in one of the Bell states. Find the reduced density matrix $\hat{\varrho}_B = \mathrm{Tr}_A(\varrho_{AB})$ for the Bell state

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle - |10\rangle\,)$$

○ $\begin{pmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix}$

○ $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$

○ $\begin{pmatrix} 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 \end{pmatrix}$

○ $\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$

47. The quantum system consists of two qubits and is in the Bell state of the form $\frac{1}{\sqrt{2}}(\,|10\rangle - |01\rangle\,)$. Which statistical operator will describe the system after averaging over the states of the second qubit?

○ $\frac{1}{\sqrt{2}}(\,|0\rangle\langle 0| + |1\rangle\langle 1|\,)$

○ $\frac{1}{\sqrt{2}}(\,|0\rangle\langle 0| - |1\rangle\langle 1|\,)$

○ $\frac{1}{2}(\,|0\rangle\langle 0| + |1\rangle\langle 1|\,)$

○ $\frac{1}{2}(\,|0\rangle\langle 0| - |1\rangle\langle 1|\,)$

48. What are the Bell states in the matrix representation if the basis vectors are written as $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$; $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. Match the Bell state $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)$ to a vector column:

○ $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$

○ $\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$

○ $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}$

○ $\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$

49. What are the Bell states in the matrix representation if the basis vectors are written as $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$; $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. Match the Bell state $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$ to a vector column:

○ $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$

○ $\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$

○ $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}$

○ $\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$

Chapter 5

General principles of classical computations

According to the **Church-Turing thesis**, the computational problem can be solved on some physically reliable computer only if it is solvable on the simplest abstract "machine" called the **Turing machine** (see Figure 5.1). A Turing machine is equivalent to the **circuit computational model** (see Figure 5.2). In the following, we discuss the most important logical gates.

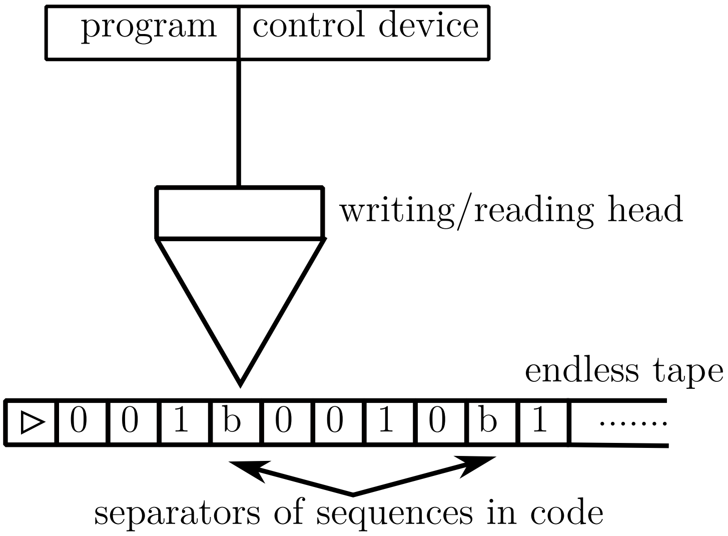

program
control device
writing/reading head
endless tape
▷ 0 0 1 b 0 0 1 0 b 1 ....
separators of sequences in code

Figure 5.1: Sketch of the Turing machine

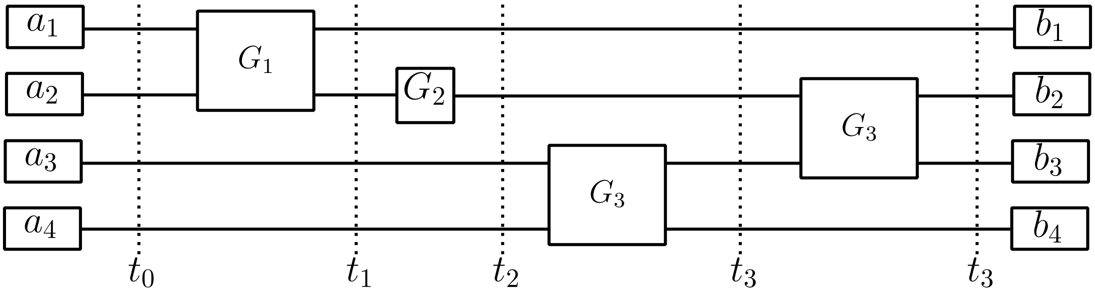
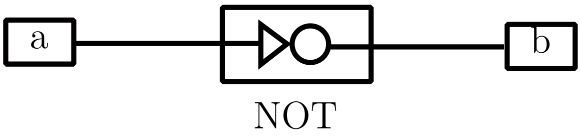


Figure 5.2: Sketch of the circuit computational model. Here G_i are logical gates applied at times t_i that take the bits from their initial state a_j into their final state b_j.

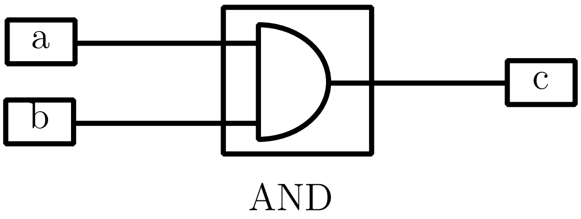
5.1 Elementary logic gates

- **NOT element:** the NOT element (negation) changes the value of a bit to the opposite: $b = a \oplus_2 1 = \mathrm{mod}_2(a+1) = (a+1)\%2$



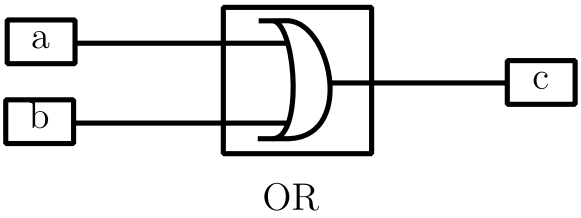
a	b
0	1
1	0

- **AND element:** the AND element (conjugation) produces a logical multiplication: $c = a \cdot b = \min(a,b)$



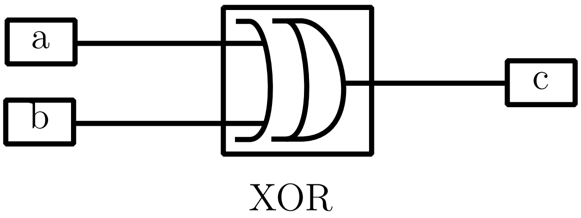
a	b	c
0	0	0
0	1	0
1	0	0
1	1	1

- **OR element:** the OR element (disjunction) returns the largest value: $c = a + b - a \cdot b = \max(a,b)$



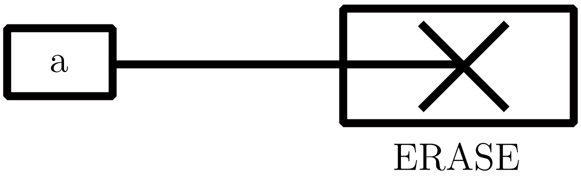
a	b	c
0	0	0
0	1	1
1	0	1
1	1	1

- **XOR element:** the XOR element (strict disjunction) is addition modulo two: $c = (a+b)\%2 = a \otimes_2 b = \max(a,b) - \min(a,b)$



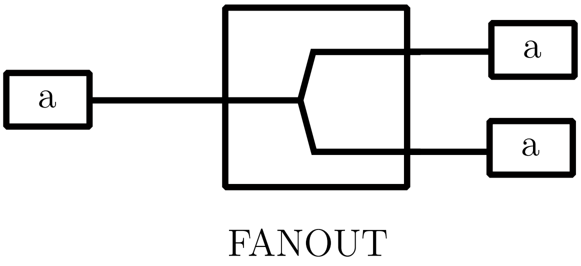
a	b	c
0	0	0
0	1	1
1	0	1
1	1	0

- **ERASE element:** the ERASE element removes a bit



a	b
0	-
1	-

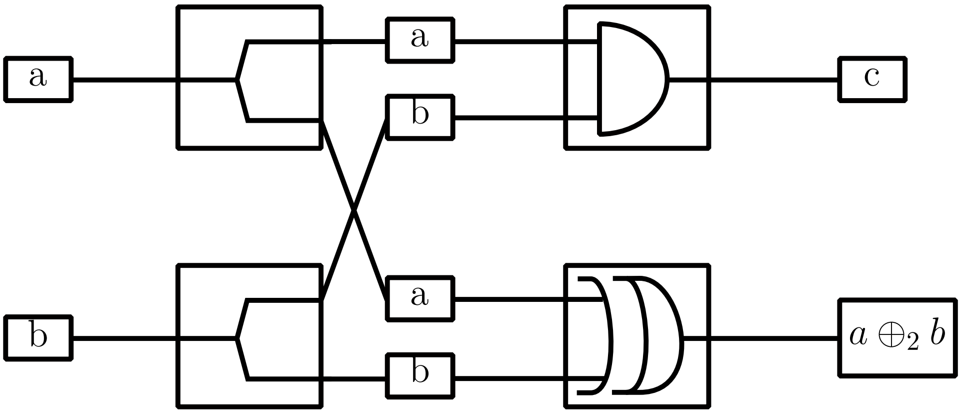
- **FANOUT element:** the FANOUT element duplicates a bit



a	b	c
0	0	0
1	1	1

5.2 The simplest classical computations

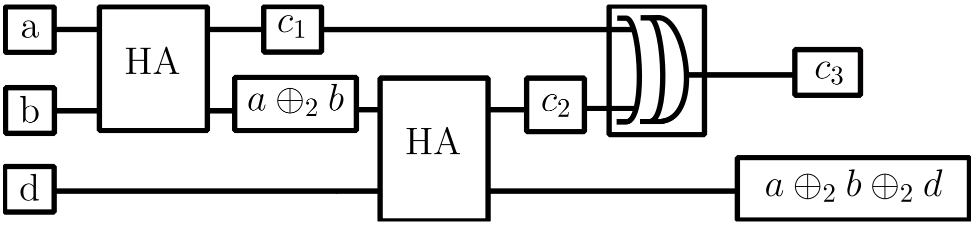
5.2.1 Half-adder



a	b	c	$a \oplus_2 b$	R_2	R_{10}
0	0	0	0	00	0
0	1	0	1	01	1
1	0	0	1	01	1
1	1	1	0	10	2

The half-adder is insufficient for adding more than two single bits (two in and outputs).

5.2.2 Full-adder



a	b	d	c_1	$a \oplus_2 b$	d	c_1	c_2	$a \oplus_2 b \oplus_2 d$	c_3	$a \oplus_2 b \oplus_2 d$
0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	1	0	0	0	1	0	1
1	0	0	0	1	0	0	0	1	0	1
1	1	0	1	0	0	1	0	0	1	0
0	0	1	0	0	1	0	0	1	0	1
0	1	1	0	1	1	0	1	0	1	0
1	0	1	0	1	1	0	1	0	1	0
1	1	1	1	0	1	1	0	1	1	1

For adding multi-digit numbers, one needs a cascade of half- and full-adders.

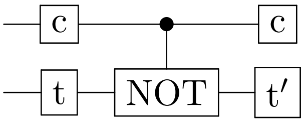
5.3 Landauer principle/reversible gates

AND, OR, and XOR gates are irreversible logic elements, i.e. one can not recover the full information of the two input bits from the one output bit (in all cases). All logic gates that use irreversible elements for their switches are also irreversible, e.g. half-adder and full-adder. The Landauer principle states the following:

- demolition of information is a dissipative process, i.e. it can not be reversed
- loss (destruction) of one bit of information, therefore, leads to the release of energy (heat) $W = k_{\mathrm{B}} T \log 2$
- it is not important for classical computations but plays a very crucial role in quantum computing → any heating can lead to decoherence
- Landauer found that any computation can be performed using **only reversible logic operations (gates)**

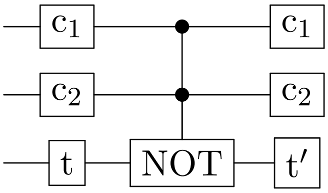
The NOT element is a reversible logic element. The following logic elements are very important:

- **CNOT element:** the CNOT element (controlled negation) changes the value of a bit to the opposite for a certain value of the control bit (1). The resulting truth table is the same as for XOR. It copies the target bit t if the control bit c is given as 0 to the CNOT gate.



t	c	t'
0	0	0
0	1	1
1	0	1
1	1	0

- **CCNOT element:** the CCNOT element (Toffoli element) changes the value of a bit to the opposite for certain values of the two control bits (1). The resulting truth table is the same as for XOR. It copies the target bit t if the control bit c is given as 0 to the CNOT gate. For choosing $t = 0$ one gets the AND gate for the other two bits with result t' (XOR for $c_1 = 1$ or $c_2 = 1$), a OR gate for $a = 0$ and $c_1 \rightarrow \mathrm{NOT}(c_1)$,$c_2 \rightarrow \mathrm{NOT}(c_2)$, a NOT gate for $c_1 = c_2 = 1$ and a FANOUT is realised for $c_2 = 1, a = 0$. Applying CCNOT another time to the result reverses the effect.



c_1	c_2	t	t'
0	0	0	0
0	1	0	0
1	0	0	0
1	1	0	1
0	0	1	1
0	1	1	1
1	0	1	1
1	1	1	0

With these two gates we can build the a reversible version of the half- and of the full-adder as shown in Figures 5.3 and 5.4.

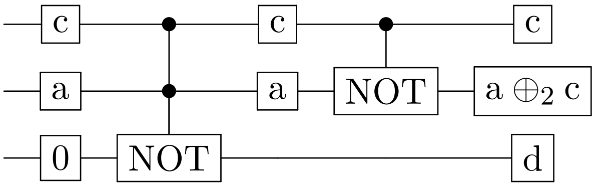


Figure 5.3: scheme of the reversible half-adder

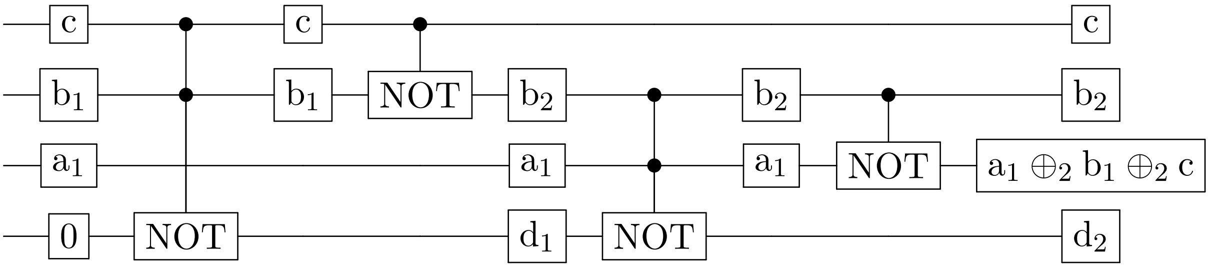
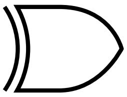
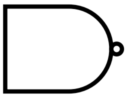
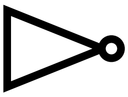
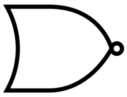


Figure 5.4: scheme of the reversible full-adder

5.4 Exercises

1. Find a schematic drawing of the XOR element:

○  ○  ○  ○ 

2. Which operation corresponds to the action of the logical AND?

○ addition modulo

○ logical multiplication

○ delete a bit

○ logical negation

3. What is the value of the output bit c of the logical gate OR if the input bits are $a = 0; b = 1$?

○ $c = 0$

○ $c = 1$

4. If someone sends $a = 1$ and $b = 1$ to the input of the half-adder, what is the value of the carry bit c?

○ $c = 0$

○ $c = 1$

5. If someone sends $a = 1$, $b = 1$, and $d = 1$ to the input of the full-adder, what is the value of the carry bit c_3?

   ○ $c_3 = 0$
   ○ $c_3 = 1$

6. Choose a row that contains only irreversible logic gates:

   ○ NOT, CNOT, CCNOT
   ○ NOT, OR, CNOT
   ○ CNOT, CCNOT, AND
   ○ AND, OR, XOR

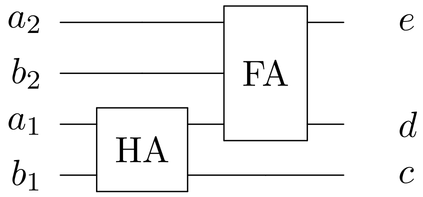
7. What should be the value of the control bit c on the input of the CNOT gate, so that CNOT works as a logical FANOUT element to the target bit a?

   ○ $c = 1$
   ○ $c = 0$

8. If someone sends $a_1 = 1$, $b_1 = 1$, and $c = 1$ to the input of the full-adder with reversible elements, what are the values of the b_2 and d_2 on the output of the scheme?

   ○ $b_2 = 0; d_2 = 0$
   ○ $b_2 = 1; d_2 = 0$
   ○ $b_2 = 0; d_2 = 1$
   ○ $b_2 = 1; d_2 = 1$

9. You can see in the Figure below a cascade circuit that allows someone to add two-digit numbers in the binary numerical system. Here a_1 and b_1 are the first digits starting from the right side of the numbers, that are added together, a_2 and b_2 the second ones. If someone wants to calculate the sum of 1 and 3, what are the values of c, d, e and what is the meaning of these numbers?



   ○ $e = 0$ the first digit starting from the right side; $d = 0$ the second; $c = 1$ the third
   ○ $c = 0$ the first digit starting from the right side; $d = 1$ the second; $c = 1$ the third
   ○ $c = 0$ the first digit starting from the right side; $d = 0$ the second; $c = 1$ the third
   ○ $e = 0$ the first digit starting from the right side; $d = 1$ the second; $c = 1$ the third

Chapter 6

General principles of quantum computations

6.1 Pauli matrices

The three Pauli matrices are

$$X = \sigma_x = \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \sigma_y = \sigma_2 = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad Z = \sigma_z = \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Properties:

- They form the basis of all 2×2 hermitian matrices with zero trace and together with the identity matrix they form the basis of all hermitian 2×2 matrices, i.e. any hermitian operator A acting on $\mathcal{H}^2$ can be represented as a linear combination of the Pauli matrices:

  $$A = c_0 \mathrm{I}_2 + \sum_{i=1}^{3} c_i \sigma_i$$

  and any operator function of the Pauli matrices can be represented as a linear combination of the Pauli matrices:

  $$f\big(\{\sigma_i\}_{i=1,2,3}\big) = a_0 \mathrm{I}_2 + \sum_{i=1}^{3} a_i \sigma_i.$$

  In particular, the rotation operators $R_{\boldsymbol{n}}(\varphi)$ which rotate the system around the axis directed along $\boldsymbol{n}$ by the angle φ are

  $$R_{\boldsymbol{n}}(\varphi) = \mathrm{I}_2 \cos\frac{\varphi}{2} - \mathrm{i}(\boldsymbol{\sigma} \cdot \boldsymbol{n}) \sin\frac{\varphi}{2}.$$

- Their squares yield the identity matrix $\sigma_i^2 = \mathrm{I}_2$

- They have trace zero $\mathrm{Tr}\sigma_i = 0$

- Their determinant is -1 $\det\sigma_i = -1$

- Their commutator $[\sigma_i, \sigma_j]_- = 2\mathrm{i}\epsilon_{ijk}\sigma_k$

- Because of $\sigma_i\sigma_j = \mathrm{i}\epsilon_{ijk}\sigma_k$, their anticommutator is zero

6.2 Single-qubit gates

Like classical computations, quantum computations can be represented by quantum switching boards (quantum circuit computation models). Quantum information theory operates with logical elements whose actions can be described using certain **unitary** quantum transformations, i.e. their actions are **reversible**[1].

- **X element:** In the σ_z-basis this operation is represented by σ_x. It realises a NOT operation.

$$-\boxed{\alpha|0\rangle + \beta|1\rangle}-\boxed{\mathrm{X}}-\boxed{\alpha|1\rangle + \beta|0\rangle}-$$

- **Z element:** In the σ_z-basis this operation is represented by σ_z. It shifts the relative phase of a superposition

$$-\boxed{\alpha|0\rangle + \beta|1\rangle}-\boxed{\mathrm{Z}}-\boxed{\alpha|0\rangle - \beta|1\rangle}-$$

It is the NOT element in the **Hadamard** basis:

$$Z|+\rangle = Z\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |-\rangle, \quad Z|-\rangle = Z\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |+\rangle$$

- **Y element:** In the σ_z-basis this operation is represented by σ_y. It realises a NOT operation and a phase shift

$$-\boxed{\alpha|0\rangle + \beta|1\rangle}-\boxed{\mathrm{Y}}-\boxed{\mathrm{i}(\alpha|1\rangle - \beta|0\rangle)}-$$

The X,Y,Z elements rotate the states around the respective axes of the Bloch sphere (by π).

- **Hadamard or Hadamard-Walsh element:** H performs the transition from one basis to another (computational to Hadamard and Hadamard to the computational basis)

$$H|0\rangle = |+\rangle, \quad H|1\rangle = |-\rangle, \quad H|+\rangle = |0\rangle, \quad H|-\rangle = |1\rangle$$

In the z-basis $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H^2 = \mathrm{I}_2$.

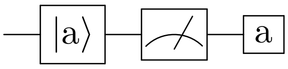
- $\pi/8$ **phase element T:**

$$T\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle$$

In the z-basis $T = \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\pi/8} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/8} \end{pmatrix} \simeq \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/4} \end{pmatrix}$.

A set of unitary elements is called **universal** for single-qubit elements, if any other single-qubit unitary element can be obtained through a quantum circuit built only on elements from this set. The sets $\{H, T\}$ and $\{I, X, Y, Z\}$ are universal sets for single-qubit elements.

- **The measurement element:** It turns a state into a result of the calculation (the state is destroyed and a real number obtained) → the qubit is destroyed.

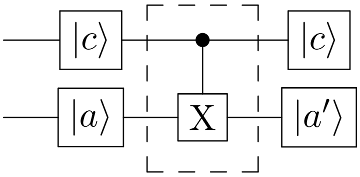


[1] This ensures that the quantum computer does not heat up and results are lost due to decoherence

6.3 Controlled quantum logic gates

To perform quantum computations one needs controlled quantum elements that act on several qubits at once in addition to single-qubit logic elements. Qubits are divided into **control** and **target** qubits as in classical computations. A logical operation on the target qubits is determined by the state of the control qubits. If the control qubits are in a superposition of states, each term of the superposition must be considered separately.

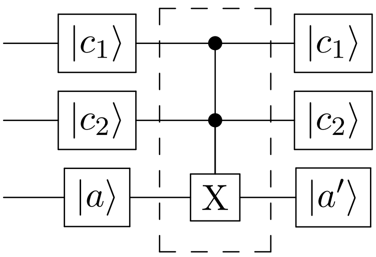
- **CNOT element (CX):** The CNOT element is a controlled ¨NOT". It changes the value of the qubit $|a\rangle$ to the opposite if the control qubit $|c\rangle = |1\rangle$ and it does not change the state $|a\rangle$.



$$|c\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |a\rangle = \gamma|0\rangle + \delta|1\rangle$$
$$|c\rangle \otimes |a\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$
$$C_1X_2|c\rangle \otimes |a\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle$$

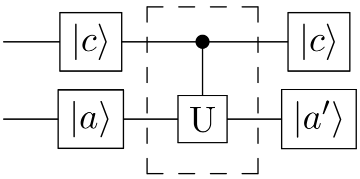
For $\delta = 0, \gamma = 1$ the states are entangled after the CX $\alpha|00\rangle + \beta|11\rangle$!

- **CCNOT element (CCX):** The CCX is the quantum Toffoli element. It changes the state of the target element $|a\rangle$ to the opposite if both qubits are in the states $|c_i\rangle = |1\rangle$ and does not change it if either is in the state $|c_i\rangle = |0\rangle$



$$|c_1\rangle = \alpha|0\rangle + \beta|1\rangle,\ |c_2\rangle = \gamma|0\rangle + \delta|1\rangle,\ |a\rangle = \epsilon|0\rangle + \phi|1\rangle$$
$$\begin{aligned} |c_1\rangle \otimes |c_2\rangle \otimes |a\rangle &= \alpha\gamma\epsilon 000\rangle + \alpha\gamma\phi|001\rangle + \alpha\delta\epsilon|010\rangle \\ &+ \alpha\delta\phi|011\rangle + \beta\gamma\epsilon|100\rangle + \beta\gamma\phi|101\rangle \\ &+ \beta\delta\epsilon|110\rangle + \beta\delta\phi|111\rangle \\ C_1C_2X_3|c_1\rangle \otimes |c_2\rangle \otimes |a\rangle &= \alpha\gamma\epsilon 000\rangle + \alpha\gamma\phi|001\rangle + \alpha\delta\epsilon|010\rangle \\ &+ \alpha\delta\phi|011\rangle + \beta\gamma\epsilon|100\rangle + \beta\gamma\phi|101\rangle \\ &+ \beta\delta\epsilon|111\rangle + \beta\delta\phi|110\rangle \end{aligned}$$

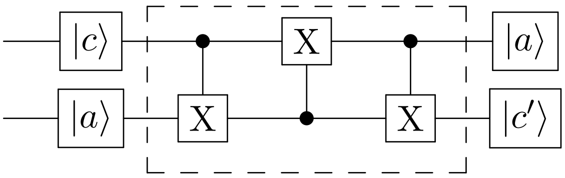
- **CU element:** The CU element changes the state of the qubit $|a\rangle$ to $U|a\rangle$ if the qubit $|c\rangle = |1\rangle$ and leaves it as it is otherwise.



$$|c\rangle \otimes |a\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$
$$C_1U_2|c\rangle \otimes |a\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|1\rangle U|0\rangle + \beta\delta|1\rangle U|1\rangle$$

The set of elements $\{H, T, CX\}$ is a **universal** set for any unitary element, i.e. a quantum computation circuit of arbitrary complexity can be constructed from these and only these elements.

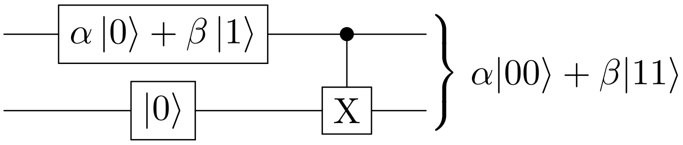
The SWAP circuit changes the order of the input qubits



$$\begin{aligned}
|c\rangle \otimes |a\rangle &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \\
C_1X_2|c\rangle \otimes |a\rangle &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle \\
C_2X_1C_1X_2|c\rangle \otimes |a\rangle &= \alpha\gamma|00\rangle + \alpha\delta|11\rangle + \beta\gamma|01\rangle + \beta\delta|10\rangle \\
C_1X_2C_2X_1C_1X_2|c\rangle \otimes |a\rangle &= \alpha\gamma|00\rangle + \alpha\delta|10\rangle + \beta\gamma|01\rangle + \beta\delta|11\rangle \\
&= (\gamma|0\rangle + \delta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\
&= |a\rangle \otimes |c\rangle
\end{aligned}$$

6.4 No-cloning theorem

There is no quantum realisation of the classical FANOUT gate. This is known as the **No-cloning theorem**. The naive approach inspired by the classical gate might be


$\alpha\,|0\rangle + \beta\,|1\rangle$
$|0\rangle$
X
$\alpha|00\rangle + \beta|11\rangle$

For a general state as the target, we get

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \epsilon|1\rangle) \overset{?}{=} \alpha|00\rangle + \beta|11\rangle$$

Unfortunately, this is only true for an eigenstate. This means that an eigenstate can be copied but not a general state. One can proof that there is no unitary operation that does copy an arbitrary state into another one.
Proof:

$$\begin{aligned}
U|\Psi\rangle|\Xi\rangle|\text{in}\rangle &\to |\Psi\rangle|\Psi\rangle|\text{out}_\Psi\rangle \\
U|\xi\rangle|\Xi\rangle|\text{in}\rangle &\to |\Xi\rangle|\Psi\rangle|\text{out}_\Xi\rangle \\
\langle\text{out}_\Psi|\text{out}_\Xi\rangle &\neq 1 \\
U^\dagger = U^{-1} &\Rightarrow U^\dagger U = \text{I}
\end{aligned}$$

Multiplying the upper left state with the down left state:

$$\begin{aligned}
\langle\Psi|\langle\Xi|\langle\text{in}|U^\dagger U|\Xi\rangle|\Xi\rangle|\text{in}\rangle \quad &\overset{\text{right}}{\underset{\text{equations}}{=}} \quad (\langle\Psi|\langle\Psi|\langle\text{out}_\Psi|)|\Xi\rangle|\Xi\rangle|\text{out}_\Xi\rangle \\
&= \quad |(\langle\Psi|\Xi\rangle)|^2\langle\text{out}_\Psi|\text{out}_\Xi\rangle
\end{aligned}$$

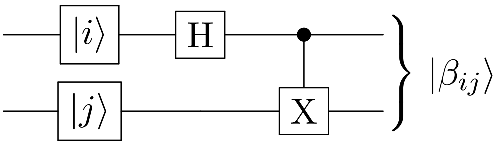
Because of the normalisation

$$\begin{aligned}
\langle\Psi|\Xi\rangle &= (\langle\Psi|\Xi\rangle)^2\langle\text{out}_\Psi|\text{out}_\Xi\rangle \\
\text{I} &= \langle\Psi|\Xi\rangle\langle\text{out}_\Psi|\text{out}_\Xi\rangle
\end{aligned}$$

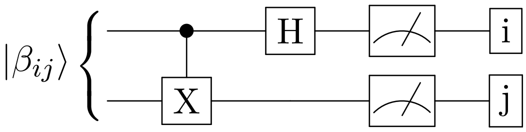
As $|\langle\Psi|\Xi\rangle| < 1$ and $\langle\text{out}_\Psi|\text{out}_\Xi\rangle \leq 1$ the above equality is a contradiction. Therefore, only eigenstates can be copied and all logical operations and calculations need to be carried out before a measurement, i.e. obtaining an result. **This is bad for quantum computing, but very good for quantum cryptography**.

6.5 Superdense coding

One first generates a Bell state[2]



The reverse scheme is used for the measurement of the Bell state[3]



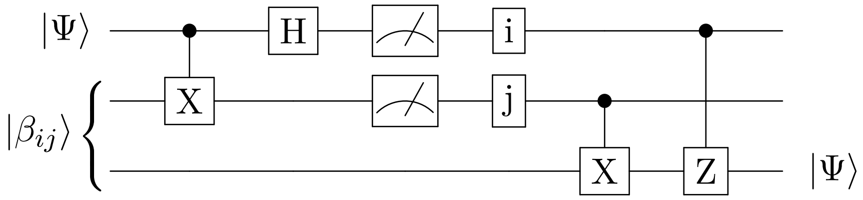
The quantum entanglement between two qubits allows one to encode information using the qubits' **relative phase** and **not only** the qubits' **values**. One can transfer two classical bits of information using only a single qubit via the **superdense coding** protocol:

1. A specific Bell state is prepared, e.g. $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
2. Alice gets the first qubit (photon) of the Bel state and performs a operation I to encode the information "00", the operation X to encode "01", the operation Z to encode "10" or the operation ZX to encode the information "11"
3. Alice sends her photon to Bob
4. Bob performs a Bell measurement

By only operations to one qubit, a two bit message can be encoded.

6.6 Quantum teleportation

Quantum teleportation is a way to transfer a quantum state over long distances using spatially separated entangled EPR/Bell state pair and a classical communication channel. By this way of transferring information, the quantum state of one physical system is **destroyed** at the transmission point during the measurement and **recreated** at the reception point on the other physical system.
Protocol



[2] This procedure is not used in practice to obtain a Bell state as it is much easier to obtain them through actual physical processes.

[3] The calculation was carried out in I

For $|\beta_{00}\rangle$:
At the beginning, the state is

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

After C_1X_2:

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

After H_1:

$$\begin{aligned} &= \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] \\ &= \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)] \end{aligned}$$

After the two control gates, the final state is

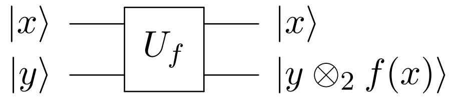
$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes |\Psi\rangle.$$

The state $|\Psi\rangle$ has been successfully copied into the state of the Bell state's second qubit, but has been destroyed in the initial qubit through the measurement. One can use quantum teleportation to perform quantum logical operations.

6.7 Quantum parallelism

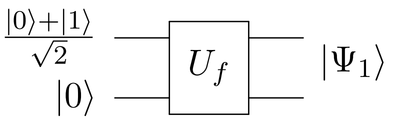
Quantum parallelism is a fundamental property of any quantum algorithm based on the quantum superposition principle. In quantum computational devices it allows one to obtain several values of a certain function $f(x)$ in points $\{x_1, x_2, \ldots, x_n\}$ simultaneously. It means that only **one** unitary logical operation $U_f : \{x_1, x_2, \ldots, x_n\} \to \{f(x_1), f(x_2), \ldots, f(x_n)\}$ is needed. A typical logical transformation (black box) is e.g. $f : \{0,1\} \to \{0,1\}$.

$$U_f : |x, y\rangle \to |x, y \otimes_2 f(x)\rangle.$$



The first register (x) is called the **data register** and the second register (y and $y \otimes_2 f(x)$) is called the value register.
Simultaneous computation of two values of $f(x)$:

$$U_f : \tfrac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \to \tfrac{1}{\sqrt{2}}(|0, f(0)\rangle + |1f(1)\rangle)$$



After the U_f transformation, every superposition term keeps information on **different** required function values. In contrast to classical computations, because of quantum parallelism one only needs one logical operation for calculating the values of $f(x)$. Like for the classical computer, one only obtains one value when measuring the superposition state $f(0)$ or $f(1)$. To get more practical benefits from quantum computations, we have to learn how to extract more information from the superposition $\frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1f(1)\rangle)$. In the next chapter, we will look at different **quantum algorithms** that give recipes for how this can be done. All obtained results can be generalised to a multidimensional case.

6.8 Exercises

1. What is the value of the commutator $[\sigma_y, \sigma_x]$

   ○ $\begin{pmatrix} 2\mathrm{i} & 0 \\ 0 & -2\mathrm{i} \end{pmatrix}$

   ○ $\begin{pmatrix} -2\mathrm{i} & 0 \\ 0 & 2\mathrm{i} \end{pmatrix}$

   ○ $\begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}$

   ○ $\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$

2. Choose a matrix that corresponds to the rotating operator on the angle $\pi/2$ around the x-axis:

   ○ $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -\mathrm{i} \\ -\mathrm{i} & 1 \end{pmatrix}$

   ○ $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$

   ○ $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \mathrm{i} \\ \mathrm{i} & 1 \end{pmatrix}$

   ○ $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

3. Choose a row that contains the universal set of gates for single-qubit elements:

   ○ $\{H, Y\}$

   ○ $\{H, X\}$

   ○ $\{H, \mathrm{I}\}$

   ○ $\{\mathrm{I}, X, Y, Z\}$

4. What is the result of the operation $ZH\,|1\rangle$?

   ○ $|-\rangle$

   ○ $|+\rangle$

   ○ $|0\rangle$

   ○ $|1\rangle$

5. If someone sends $|a\rangle = |1\rangle$ and $|c\rangle = |1\rangle$ to the input of the CNOT element, what is the value of the target qubit on the output of the scheme?

   ○ $|a'\rangle = |0\rangle$

   ○ $|a'\rangle = |1\rangle$

6. Select the correct set of equalities:

   ○ $YR_1(\phi)Y = -R_1(\phi)$; $YR_2(\phi)Y = -R_2(\phi)$; $YR_3(\phi)Y = R_3(-\phi)$

   ○ $YR_1(\phi)Y = R_1(-\phi)$; $YR_2(\phi)Y = R_2(\phi)$; $YR_3(\phi)Y = R_3(-\phi)$

   ○ $YR_1(\phi)Y = R_1(-\phi)$; $YR_2(\phi)Y = R_2(-\phi)$; $YR_3(\phi)Y = -R_3(\phi)$

○ $YR_1(\phi)Y = -R_1(\phi)$; $YR_2(\phi)Y = R_2(\phi)$; $YR_3(\phi)Y = -R_3(\phi)$

7. Represent the sequence of the single-qubit gates HXH in the form of the rotation on the Bloch sphere:

○ $HXH = -X$

○ $HXH = Y$

○ $HXH = Z$

○ $HXH = X$

8. The qubit in the state $|\Psi\rangle = \frac{\mathrm{i}-\sqrt{2}}{3}|0\rangle - \frac{2+\mathrm{i}\sqrt{2}}{3}|1\rangle$ is measured in the Hadamard basis $\{\,|+\rangle\,, |-\rangle\,\}$. What is the probability of detecting a qubit in the state $|-\rangle$ after the measurement?

○ $\frac{9+2\sqrt{2}}{36}$

○ $\frac{9+2\sqrt{2}}{18}$

○ $\frac{9-2\sqrt{2}}{18}$

○ $\frac{9-2\sqrt{2}}{36}$

9. Select a correct matrix representation of the CU gate if U = Z:

○ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

○ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

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

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

10. If someone sends $|a\rangle = |-\rangle$ and $|c\rangle = |+\rangle$ to the input of the CNOT element, what are the values of the target and control qubits on the output of the scheme?

○ $|a'\rangle = |-\rangle\,, |c'\rangle = |-\rangle$

○ $|a'\rangle = |+\rangle\,, |c'\rangle = |+\rangle$

○ $|a'\rangle = |+\rangle\,, |c'\rangle = |-\rangle$

○ $|a'\rangle = |-\rangle\,, |c'\rangle = |+\rangle$

Chapter 7

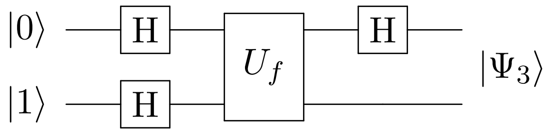
Quantum algorithms

7.1 Deutsch algorithm

The **Deutsch problem** uses a function $f:\ \{0,1\}^n \to \{0,1\}$, i.e. the domain of the function f consists of 2^n various n-bit sequences. The range of the function contains only the two elements 0 and 1:

$$\begin{aligned}
&D(f) = \{|0_0 0_1 \dots 0_n\rangle, |1_0 0_1 \dots 0_n\rangle, \dots, |1_0 1_1 \dots 1_n\rangle\}\,,\\
&E(f) = \{|0\rangle, |1\rangle\}\,.
\end{aligned}$$

A function is called **constant** if $f(x) = 0$ or $f(x) = 1$ $\forall x \in D(f)$. If for 2^{n-1} values of x the condition $f(x) = 0$ and for the other half $f(x) = 1$, then the function is called **balanced**. The Deutsch problem is to determine whether the function is constant or balanced.
Classically one needs to calculate $2^{n-1} - 1$ of its values to surely be able to solve the problem. The quantum Deutsch algorithm allows one to solve this problem after calculating only 1 value of $f(x)$! The scheme of this algorithm is the following



$$\begin{aligned}
|\Psi_0\rangle &= |0\rangle|1\rangle\\
|\Psi_1\rangle &= H_1 H_2 |\Psi_0\rangle = |+\rangle|-\rangle = \frac{1}{\sqrt{2}}|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\\
U_f|\Psi_1\rangle &= \frac{1}{\sqrt{2}}|0\rangle\left(\frac{|f(0)\rangle - |1+f(0)\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}|1\rangle\left(\frac{|f(1)\rangle - |1+f(1)\rangle}{\sqrt{2}}\right)\\
\text{for } f(x) = 1:\ \ & \frac{1}{\sqrt{2}}|x\rangle\left(\frac{|f(x)\rangle - |1+f(x)\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}|x\rangle(-1)^{f(x)}\left(|0\rangle - |1\rangle\right)\\
\text{for } f(x) = 0:\ \ & \frac{1}{\sqrt{2}}|x\rangle\left(\frac{|f(x)\rangle - |1+f(x)\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}|x\rangle\left(|0\rangle - |1\rangle\right)\\
\Rightarrow\ \ & \frac{1}{\sqrt{2}}|x\rangle\left(\frac{|f(x)\rangle - |1+f(x)\rangle}{\sqrt{2}}\right) = (-1)^{f(x)}|x\rangle\frac{|0\rangle - |1\rangle}{2}\\
\Rightarrow\ |\Psi_2\rangle &= U_f|\Psi_1\rangle = \frac{(-1)^{f(0)}}{2}\left(|00\rangle - |01\rangle\right) + \frac{(-1)^{f(1)}}{2}\left(|10\rangle - |11\rangle\right)\\
|\Psi_3\rangle &= H_1|\Psi_2\rangle = \frac{1}{2\sqrt{2}}\left[(-1)^{f(0)}|+\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}(|-\rangle(|0\rangle - |1\rangle)\right]\\
&= \frac{1}{\sqrt{8}}\left[(-1)^{f(0)}\left(|00\rangle + |10\rangle - |01\rangle - |11\rangle\right) + (-1)^{f(1)}\left(|00\rangle - |10\rangle - |01\rangle + |11\rangle\right)\right]
\end{aligned}$$

$$\begin{aligned}\text{for } f(x) \text{ constant}: \quad |\Psi_3\rangle &= \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle)\\ \text{for } f(x) \text{ balanced}: \quad |\Psi_3\rangle &= \frac{1}{\sqrt{2}}|1\rangle \otimes (|0\rangle - |1\rangle)\end{aligned}$$

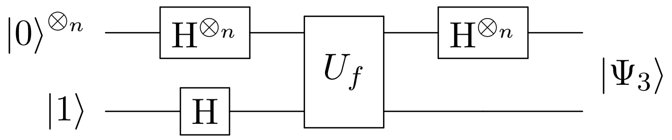
By measuring the first qubit (in the computational basis) it is revealed whether the function is constant or balanced if it can only be one of the two[1].

7.2 Deutsch-Josza algorithm

The **Deutsch-Josza algorithm** is a generalisation of the Deutsch algorithm when the argument is multidimensional (2^n values; n-qubits) and solves the general Deutsch problem, when the oracle function $f(x)$ is either constant or balanced with $f(x) \in \{0, 1\}$. We define the two-qubit/n-qubit Hadamard transformation:

$$\begin{aligned}H^{\otimes 2}|\alpha_1\alpha_2\rangle &= \frac{1}{2}\left(|00\rangle + |11\rangle + (-1)^{\alpha_1}|10\rangle + (-1)^{\alpha_2}|01\rangle\right)\\ H^{\otimes n}\bigotimes_{i=1}^{n}|\alpha_i\rangle &= \frac{1}{2^{n/2}}\bigotimes_{i=1}^{n}\left(|0\rangle + (-1)^{\alpha_i}|1\rangle\right)\end{aligned}$$

Acting with $H^{\otimes n}$ on the state $|0\rangle^{\otimes n}$ yields every possible state. The scheme of the Deutsch-Josza algorithm:



$$|\Psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$$

$$|\Psi_1\rangle = H^{\otimes n}H_{n+1}|\Psi_0\rangle = \frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$|\Psi_2\rangle = \frac{1}{2^{n/2}}U_f\left[\sum_{x\in\{0,1\}^n}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right] = \frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$\begin{aligned}H^{\otimes n}|x\rangle &= H^{\otimes n}|x_1\rangle|x_2\rangle\dots|x_n\rangle = \frac{1}{2^{n/2}}\left[(|0\rangle + (-1)^{x_1}|1\rangle)\otimes(|0\rangle + (-1)^{x_2}|1\rangle)\otimes\cdots\otimes(|0\rangle + (-1)^{x_n}|1\rangle)\right]\\ &= \frac{1}{2^{n/2}}\sum_{z_1\in\{0,1\},z_2\in\{0,1\},\dots,z_n\in\{0,1\}}(-1)^{x_1z_1+\dots x_nz_n}|z1\rangle\otimes\cdots\otimes|z_n\rangle = \frac{1}{2^{n/2}}\sum_{\boldsymbol{z}\in\{0,1\}^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{z}}|\boldsymbol{z}\rangle\end{aligned}$$

$$\begin{aligned}|\Psi_3\rangle = H^{\otimes n}|\Psi_2\rangle &= \left[\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\frac{1}{2^{n/2}}\sum_{\boldsymbol{z}\in\{0,1\}^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{z}}|\boldsymbol{z}\rangle\right]\otimes\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\\ &= \frac{1}{2^n}\sum_{\boldsymbol{z}\in\{0,1\}^n}\left(\sum_{x\in\{0,1\}^n}(-1)^{f(x)+\boldsymbol{x}\cdot\boldsymbol{z}}\right)|z\rangle\otimes\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\end{aligned}$$

The term $\sum\limits_{x\in\{0,1\}^n}(-1)^{f(x)+\boldsymbol{x}\cdot\boldsymbol{z}}$ is the full amplitude of the state $|z\rangle$ and if we assume $|z\rangle = |0\rangle^{\otimes n}$:

$$\sum_{x\in\{0,1\}^n}(-1)^{f(x)+\boldsymbol{x}\cdot\boldsymbol{z}} = \sum_{x\in\{0,1\}^n}(-1)^{f(x)}\forall x \quad \begin{array}{l} f(x) = 0 \;\rightarrow\; \sum\limits_{x\in\{0,1\}^n}(-1)^{f(x)} = 1\\ f(x) = 1 \;\rightarrow\; \sum\limits_{x\in\{0,1\}^n}(-1)^{f(x)} = -1\end{array}$$

[1] Which you should check that it can only be constant or balanced :)

If $f(x)$ is balanced, the amplitude vanishes for $|z\rangle = |0\rangle^{\otimes n}$ and if $f(x)$ is constant, all other amplitudes vanish!!!
By measuring the value of the first n qubits in the computational basis, one can determine whether the function is constant or balanced: measurement is $|0\rangle$ then $f(x)$ is constant, else it is balanced.

7.3 Quantum Fourier transform

The Fourier transformation changes the basis according to

$$|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i} jk/N} |k\rangle \qquad \text{(orthonormal basis)}$$

$$\sum_{j=0}^{N-1} x_j |j\rangle = \sum_{k=0}^{N-1} y_k |k\rangle \text{ with } y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \mathrm{e}^{2\pi \mathrm{i} jk/N} \qquad \text{(arbitrary state)}$$

The notation is the following

$$\left.\begin{array}{l} |0\rangle^{H^2} \otimes |0\rangle^{H^2} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = |0\rangle^{H^4}, \quad |0\rangle^{H^2} \otimes |1\rangle^{H^2} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = |1\rangle^{H^4} \\ \\ |1\rangle^{H^2} \otimes |0\rangle^{H^2} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = |2\rangle^{H^4}, \quad |1\rangle^{H^2} \otimes |1\rangle^{H^2} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = |3\rangle^{H^4} \end{array}\right\} H^4 \text{ (computational basis)}$$

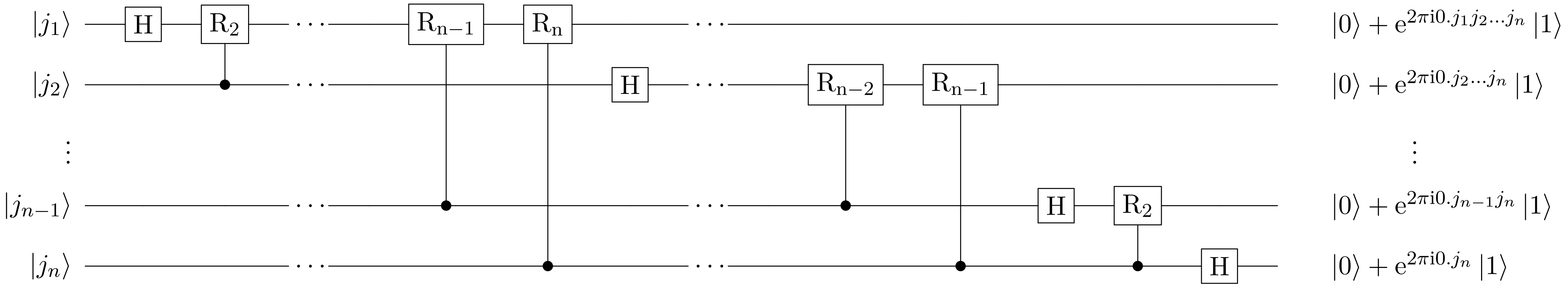
A more convenient form for the **quantum Fourier transform**:

$$N = 2^n, n \in \mathbb{N} : \Big\{|0\rangle, |1\rangle, |2\rangle, \ldots, |2^{n-1}\rangle\Big\} \to |j\rangle = |j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle$$

$$\begin{aligned} \text{different representations : } |j\rangle &= j_1 \cdot 2^{n-1} + j_2 \cdot 2^{n-2} + \cdots + j_n \cdot 2^0 \text{ (real number)} \\ |j\rangle &= \frac{j_1}{2} + \frac{j_2}{4} + \cdots + \frac{j_n}{2^n} \text{ (rational number)} \\ |j\rangle &= \frac{1}{2^{n/2}} \sum_{k=0}^{2^{n-1}} \mathrm{e}^{2\pi \mathrm{i} jk/2^n} |k\rangle = \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} |k_l\rangle \\ &= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} \mathrm{e}^{2\pi \mathrm{i} k_l/2^l} |k_l\rangle \right] = \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \Big[|0\rangle + \mathrm{e}^{2\pi \mathrm{i} k_l/2^l} |1\rangle \Big] \\ |j_1, j_2, \ldots, j_n\rangle &= \frac{1}{2^{n/2}} \Big[\Big(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.j_n} |1\rangle \Big) \otimes \cdots \otimes \Big(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.j_1 j_2 \ldots j_n} |1\rangle \Big) \Big] \end{aligned}$$

here $0.j_1 j_2 \ldots j_n$ is a binary string. Using the notation $R_k = \begin{pmatrix}1 & 0\\ 0 & \mathrm{e}^{2\pi \mathrm{i}/2^k}\end{pmatrix}$ we can write down the **Quantum Fourier Transform** on the next page.

This is the Quantum Fourier transform scheme


$|j_1\rangle$
$|j_2\rangle$
$\vdots$
$|j_{n-1}\rangle$
$|j_n\rangle$
H
$\mathrm{R_2}$
$\mathrm{R_{n-1}}$
$\mathrm{R_n}$
H
$\mathrm{R_{n-2}}$
$\mathrm{R_{n-1}}$
H
$\mathrm{R_2}$
H
$|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.j_1 j_2 \dots j_n} |1\rangle$
$|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.j_2 \dots j_n} |1\rangle$
$\vdots$
$|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.j_{n-1} j_n} |1\rangle$
$|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.j_n} |1\rangle$

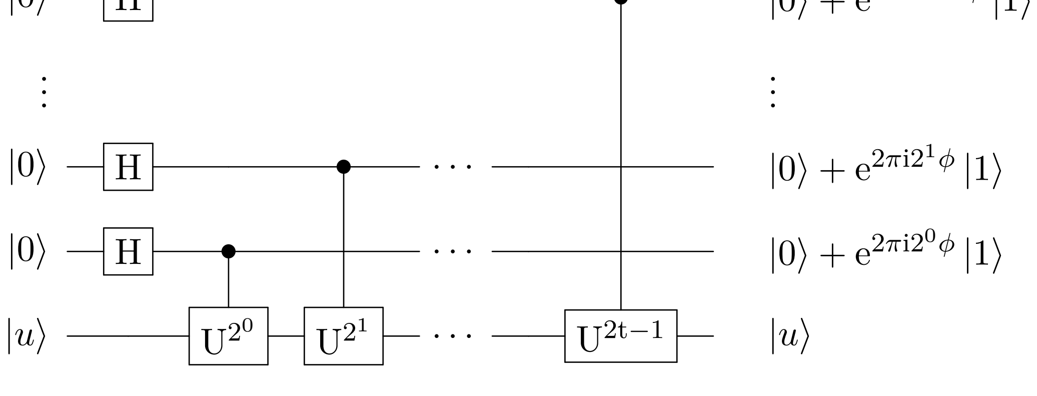
Following the scheme from the last page, we get

$$\begin{aligned}
H_1|j_1^{(0)}\rangle &= \frac{1}{2^{1/2}}\left(|0\rangle + \mathrm{e}^{2\pi\mathrm{i}\cdot j_1/2}|1\rangle\right)|j_2\dots j_n\rangle \\
&\overset{\text{binary}j's}{=} \frac{1}{2^{1/2}}\left(|0\rangle + \mathrm{e}^{2\pi\mathrm{i}\cdot 0.j_1}|1\rangle\right)|j_2\dots j_n\rangle = |j_1^{(1)}\rangle \\
\mathrm{CR}_2|j_1^{(1)}\rangle &= \frac{1}{2^{1/2}}\left(|0\rangle + \underbrace{\mathrm{e}^{2\pi\mathrm{i}\cdot 0.j_1}\mathrm{e}^{2\pi\mathrm{i}\cdot 0.0j_2}}_{\mathrm{e}^{2\pi\mathrm{i}\cdot 0.j_1j_2}}|1\rangle\right)|j_2j_3\dots j_n\rangle = |j_1^{(2)}\rangle \\
\mathrm{CR}_3\dots\mathrm{CR_n}|j_1^{(2)}\rangle &= \frac{1}{2^{1/2}}\left(|0\rangle + \mathrm{e}^{2\pi\mathrm{i}\cdot 0.j_1j_2\dots j_n}|1\rangle\right)|j_2j_3\dots j_n\rangle = |j_1^{(n)} \\
|j_k^{(n-k)}\rangle &= \frac{1}{2^{1/2}}(|0\rangle + |1\rangle)\otimes\dots\otimes\underbrace{\left(|0\rangle + \mathrm{e}^{2\pi\mathrm{i}\cdot 0.j_kj_{k-1}\dots j_n}|1\rangle\right)}_{\text{kth term}}\otimes\dots\otimes(|0\rangle + |1\rangle) \\
\text{state at the end: } |j^{(2n)}\rangle &= |j_1^{(n)}\rangle\otimes|j_2^{(n-1)}\rangle\otimes\dots|j_k^{(n-k)}\rangle\otimes\dots\otimes|j_n^{(1)}\rangle
\end{aligned}$$

which is a superposition of all states on the right end of the scheme. To complete the Fourier transform, the qubits need to be exchanged by using the exchange operator. The resulting scheme can be reversed, so it is unitary. The quantum Fourier transform requires $\mathcal{O}(n^2)$ operations[2], while the classical Fourier transform requires $\mathcal{O}(2^n \cdot n)$ operations. Because of the collapse after the measurement, the quantum Fourier transform can not be used just to obtain the Fourier transform.

7.4 Eigenvalue algorithm

Let an unitary operator U have an eigenvector $|u\rangle$ and an eigenvalue $\mathrm{e}^{2\mathrm{i}\pi\phi}$, where ϕ is to be determined. The goal of the **eigenvalue algorithm** is to find and estimate ϕ. In order to determine the eigenvalue, we use controlled quantum logic gates to prepare the state $|u\rangle$ and perform the operation U^{2j} for the non-negative j. The procedure uses two registers: the first contains t qubits which are initially in state $|0\rangle$. The number t of qubits determines how accurately we want to determine ϕ. The second register contains as many qubits as needed to write $|u\rangle$ and its initial state is $|u\rangle$. During the procedure, the state of the second register remains the same (unchanged).



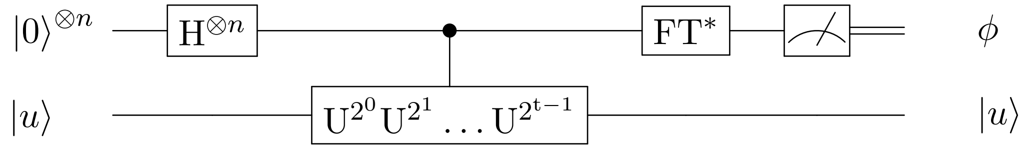
$|0\rangle$
H
$|0\rangle + \mathrm{e}^{2\pi\mathrm{i}2^{t-1}\phi}|1\rangle$
$\vdots$
$\vdots$
$|0\rangle$
H
$|0\rangle + \mathrm{e}^{2\pi\mathrm{i}2^{1}\phi}|1\rangle$
$|0\rangle$
H
$|0\rangle + \mathrm{e}^{2\pi\mathrm{i}2^{0}\phi}|1\rangle$
$|u\rangle$
U^{2^0}
U^{2^1}
$\mathrm{U}^{2\mathrm{t}-1}$
$|u\rangle$
$\cdots$

[2] $\frac{n(n+1)}{2}$ operations in the scheme and $\frac{n}{2}$ exchange operations

The final state of the first register is

$$\begin{aligned}|0\rangle^{2^t}_{\text{end}} &= \frac{1}{2^{t/2}}\left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 2^{t-1}\phi}|1\rangle\right)\left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 2^{t-2}\phi}|1\rangle\right)\dots\left(|0\rangle + \mathrm{e}^{2\pi \mathrm{i}\phi}|1\rangle\right)\\ &= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}\mathrm{e}^{2\pi \mathrm{i}\phi k}|k\rangle\end{aligned}$$

and the overall state is $|0\rangle_{\text{end}}|u\rangle$. The scheme for determining the eigenvalue is



Before and after the inverse Fourier transform

$$\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}\mathrm{e}^{2\pi \mathrm{i}\phi k}|k\rangle|u\rangle \to \left|\tilde{\phi}\right\rangle|u\rangle\,.$$

7.5 Shor-algorithm for integer factorisation

The goal of the famous **Shor-algorithm** is to factorise a given integer $M = p \cdot q$ into its prime factors p and q. This problem can be reduced to determining **the order r** of a certain periodic function

$$y_M(x) = a^x \mathrm{mod} M,$$

where $x = 0, 1, \dots, N-1$ and $L = \lceil \log_2 N \rceil$ is the number of bits needed for recording x, $a < M$ is an arbitrary number that does not have common divisors with the considered number M[3]. The order r is defined according to $a^r \mathrm{mod} M \equiv 1$. When the order (period) r is known, the factors of the number M are determined using the **Euclidean algorithm** as the greatest common divisors of numbers $a^{r/2} \pm 1$ and M, e.g.

$$\begin{aligned}y_{15}(x) = 2^x \mathrm{mod} 15, r = 4 \Leftrightarrow & 2^4 \bmod 15 = 1\\ & 2^5 \bmod 15 = 2\\ & 2^6 \bmod 15 = 4\\ & 2^7 \bmod 15 = 8\\ & 2^8 \bmod 15 = 1\\ & 2^9 \bmod 15 = 4\\ & \vdots\end{aligned}$$

$$\begin{aligned}(a^r - 1)\mathrm{mod} M &= 0\\ (a^{r/2} - 1)(a^{r/2} + 1)\mathrm{mod} M &= 0\\ (a^{r/2} - 1)(a^{r/2} + 1)\mathrm{mod} M &= \lambda M, \lambda \in \mathbb{Z}\end{aligned}$$

None of the two factors $a^{r/2} - 1$ nor $a^{r/2} + 1$ has to be devisable by M or r to be odd[4]. In all other cases ($r = 2n$ and $a^{r/2} \pm 1 \neq Mn$) one of the factors must have a common divisor with M.

[3] If it had, the problem would be solved...oops

[4] the probability for that is smaller than 1/2

7.5.1 Euclidean algorithm

Example for gcd(408, 112)

$$\begin{aligned} 408 \bmod 112 &= 72 \\ 112 \bmod 72 &= 40 \\ 72 \bmod 40 &= 32 \\ 40 \bmod 32 &= 8 \\ 32 \bmod 8 &= 0 \rightarrow \gcd(408,112) = 8 \end{aligned}$$

7.5.2 First stage of Shor's algorithm

Two registers X and Y with an equal number of qubits L initialised in the zero-state $|X\rangle|Y\rangle = |0\rangle^{\otimes L}|0\rangle^{\otimes L}$ where L is such that $2^L \geq M^2 \gg r^2$. The register X contains the arguments (natural numbers) of the function $y_M(x)$ and register Y is used to keep the value of the function $y_M(x)$. We start by applying $H^{\otimes L}$ to X to create equiprobable superpositions of all Boolean states

$$|X\rangle = |X_{L-1}X_{L-2}\dots X_0\rangle$$
$$|\phi[x,0]\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|X\rangle|0\rangle$$

Next, the register Y is filled with values $y_M(x) = 2^x \bmod M$ using a reversible logical operation and the following superposition is obtained

$$|\phi[x,y_M(x)]\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|X\rangle|Y_M(X)\rangle\,.$$

There arises a period sequence of certain states in the Y states, i.e. in the amplitudes in the X register

$$\Rightarrow\ |\phi[x,y_M(x)]\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|X\rangle \qquad \underbrace{|Y(X)\rangle}_{\substack{\text{certain subset}\\ \text{of states from}\\ \{|0\rangle,\dots,|M\rangle\}}}$$

7.5.3 Shor's algorithm second stage

Fix $y_M(x)$ value:

$$|\phi[x,r]\rangle = \frac{1}{\sqrt{N}}\left(|l\rangle + |l+r\rangle + \dots + |rA+l\rangle\right)|n\rangle = \frac{1}{\sqrt{A+1}}\sum_{j=0}^{A}|rj+l\rangle|r\rangle$$

with $A = \left(\frac{N}{r}-1\right)$ being the integer part. The second register is used to prepare a periodic superposition in the first register ($x = rj+l$), i.e. now we can find a period r!
Fourier-transform of the first register:

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{A}|rj+l\rangle \rightarrow \sum_{k=0}^{N-1}f_l(k)|k\rangle\,, \quad \text{with } f_l(k) = \frac{\sqrt{r}}{N}\sum_{j=0}^{A}\exp\left(\frac{2\pi\mathrm{i}(jr+l)k}{N}\right).$$

The probability of determining state $|k\rangle$ is

$$p(k) = |f_l(k)|^2 = \frac{r}{N^2}\left|\sum_{j=0}^{A}\exp\left[\frac{2\pi\mathrm{i}jrk}{N}\right]\right|^2.$$

Hence, the main contribution comes from the terms with $-\frac{r^2}{2} \leq rk \bmod N \leq \frac{r}{2}$. It follows that with probability $4/\pi^2 \approx 0.405$, k will take discrete values, i.e. after quantum Fourier-transform, we obtain an equiprobable superposition with a period N/r. Measuring the probability, one can determine the values $k = \nu\frac{N}{r}, \nu = 0, 1, \ldots, r-1$. If one knows $\frac{k}{N}$ and $k = \nu\frac{N}{r}$, one can find the ration $\frac{\nu}{r}$ and find the period r by transforming this ratio to an irreducible form. Then, knowing the ratio r, one can use the classical Euclidean algorithm.

7.6 Exercises

1. If we are given a function $f(x) : \{0,1\} \to \{0,1\}$ and $f(0) = 1, f(1) = 1$. In this case, $f(x)$ is

   ○ constant

   ○ balanced

2. If the first qubit is turned to be in the state $|0\rangle$ after the implementation of Deutsch's algorithm, then the function $f(x)$ is

   ○ constant

   ○ balanced

3. If we are given a function $f(x) : \{0,1\}^2 \to \{0,1\}$ and $|00\rangle = 0$, $f(01) = 1$, $f(10) = 0$, $f(11) = 1$. In this case, $f(x)$ is

   ○ constant

   ○ balanced

4. If all measured qubits are turned out to be in the state $|0\rangle$ after the implementation of the Deutsch-Josza algorithm, then the function $f(x)$ is

   ○ constant

   ○ balanced

5. If we are given a function $f(x) : \{0,1\}^2 \to \{0,1\}$ and $|00\rangle = 0$, $f(01) = 1$, $f(10) = 0$, $f(11) = 1$. What is the result of the action $\mathrm{U}_f\,|10\rangle\,|1\rangle$

   ○ $|10\rangle\,|0\rangle$

   ○ $|01\rangle\,|1\rangle$

   ○ $|10\rangle\,|1\rangle$

   ○ $|01\rangle\,|0\rangle$

6. Rewrite the binary fraction 0.101 as an ordinary fraction:

   ○ $\frac{7}{8}$

   ○ $\frac{1}{4}$

   ○ $\frac{5}{8}$

   ○ $\frac{5}{16}$

7. Which gate performs the quantum Fourier transform with one qubit?

   ○ Y element

   ○ X element

   ○ phase element T

○ Hadamard element H

8. Calculate quantum Fourier transform on $|\psi\rangle = \frac{3}{\sqrt{10}}|0\rangle + \frac{1}{\sqrt{10}}|1\rangle$ and select the right answer:

   ○ $|\psi\rangle = \frac{1}{\sqrt{10}}|0\rangle + \frac{3}{\sqrt{10}}|1\rangle$

   ○ $|\psi\rangle = \frac{3}{\sqrt{10}}|0\rangle + \frac{1}{\sqrt{10}}|1\rangle$

   ○ $|\psi\rangle = \frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle$

   ○ $|\psi\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$

9. Choose the eigenvector that corresponds to the eigenvalue $\mathrm{e}^{\mathrm{i}\pi}$ for the X element:

   ○ $|1\rangle$

   ○ $\frac{1}{\sqrt{2}}(\,|0\rangle + |1\rangle\,)$

   ○ $|0\rangle$

   ○ $\frac{1}{\sqrt{2}}(\,|0\rangle - |1\rangle\,)$

10. Choose the correct matrix representation for the inverse single-qubit quantum Fourier transform:

   ○ $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

   ○ $\sqrt{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

   ○ $\frac{1}{\sqrt{2}}\begin{pmatrix}-1 & -1\\ -1 & 1\end{pmatrix}$

   ○ $\sqrt{2}\begin{pmatrix}-1 & -1\\ -1 & 1\end{pmatrix}$

11. Assume $|u\rangle$ is an eigenvector for the X element with the eigenvalues to $\mathrm{e}^{\mathrm{i}\pi}$: in which state will the qubit from the first register be in after the application of the phase estimation algorithm?

   ○ $\frac{1}{\sqrt{2}}(\,|0\rangle + |1\rangle\,)$

   ○ $|0\rangle$

   ○ $\frac{1}{\sqrt{2}}(\,|0\rangle - |1\rangle\,)$

   ○ $|1\rangle$

12. Find the order of $a = 5$ modulo $M = 21$

   ○ $r = 3$

   ○ $r = 4$

   ○ $r = 5$

   ○ $r = 6$

13. If someone knows the order r of a modulo M, then the prime numbers p and q can be found as

   ○ $\gcd(a^r \pm 1, M)$

   ○ $\gcd(a^{r/2} \pm 1, M)$

○ $\gcd(a^{r/2}, M)$

○ $\gcd(a^{r}, M)$

14. In which state will the qubits be after the first stage of Shor's algorithm?

○ $\frac{1}{\sqrt{N}}\sum\limits_{x=0}^{N-1} |0\rangle\, |y_M(x)\rangle$

○ $\frac{1}{\sqrt{N}}\sum\limits_{x=0}^{N-1} |1\rangle\, |1\rangle$

○ $\frac{1}{\sqrt{N}}\sum\limits_{x=0}^{N-1} |x\rangle\, |0\rangle$

○ $\frac{1}{\sqrt{N}}\sum\limits_{x=0}^{N-1} |x\rangle\, |y_M(x)\rangle$

15. Let us assume that the first stage of Shor's algorithm, after measuring the second register $|Y\rangle$, we obtain the state $|2\rangle$. Select the row that contains the first three terms of the first register $|X\rangle$ up to the common factor?

○ $|0\rangle, |4\rangle, |8\rangle$

○ $|1\rangle, |5\rangle, |9\rangle$

○ $|2\rangle, |6\rangle, |10\rangle$

○ $|3\rangle, |7\rangle, |11\rangle$

16. Select the correct matrix representation for the unitary transformation U_f in the case of $f(x)$ is balanced and $f(0) = 1$, $f(1) = 0$:

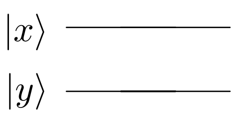
○ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

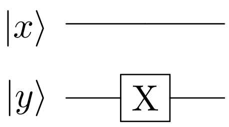
○ $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

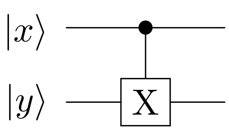
○ $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

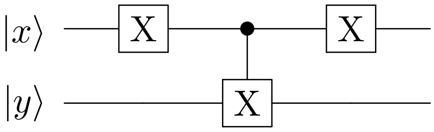
○ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

17. Let $f(x)$ be a balanced function and $f(0) = 0$, $f(1) = 1$: Select the correct schematic drawing of U_f for the above function:

○ 

○ 

○ 

○ 

18. If we are given a function $f(x) : \{0,1\}^2 \to \{0,1\}$ and $f(00) = 1,\ f(01) = 0,\ f(10) = 1, f(11) = 0$, in which state will the measured qubits be after an implementation of the Deutsch-Josza algorithm with accuracy up to the phase factor?

   ○ $|10\rangle$

   ○ $|01\rangle$

   ○ $|11\rangle$

   ○ $|00\rangle$

19. Calculate the quantum Fourier transform on $|\psi\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle - |11\rangle\,\big)$:

   ○ $\frac{1+\mathrm{i}}{2\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|10\rangle + \frac{1-\mathrm{i}}{2\sqrt{2}}\,|11\rangle$

   ○ $\frac{1+\mathrm{i}}{2\sqrt{2}}\,|01\rangle + \frac{1}{\sqrt{2}}\,|10\rangle + \frac{1-\mathrm{i}}{2\sqrt{2}}\,|11\rangle$

   ○ $\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1-\mathrm{i}}{2\sqrt{2}}\,|10\rangle + \frac{1+\mathrm{i}}{2\sqrt{2}}\,|11\rangle$

   ○ $\frac{1}{\sqrt{2}}\,|01\rangle + \frac{1+\mathrm{i}}{2\sqrt{2}}\,|10\rangle + \frac{1-\mathrm{i}}{2\sqrt{2}}\,|11\rangle$

20. If $y_{21}(x) = 5^x \bmod 21$ in Shor's algorithm, then before measuring the second register $|Y\rangle$, the first seven states of the qubits from the first and second register can be written with accuracy up to the common factor as

   ○ $|0\rangle\,|1\rangle\,,\ |1\rangle\,|5\rangle\,,\ |2\rangle\,|4\rangle\,,\ |3\rangle\,|20\rangle\,,\ |4\rangle\,|16\rangle\,,\ |5\rangle\,|17\rangle\,,\ |6\rangle\,|1\rangle$

   ○ $|0\rangle\,|1\rangle\,,\ |1\rangle\,|5\rangle\,,\ |2\rangle\,|4\rangle\,,\ |3\rangle\,|21\rangle\,,\ |4\rangle\,|16\rangle\,,\ |5\rangle\,|1\rangle\,,\ |6\rangle\,|2\rangle$

   ○ $|0\rangle\,|1\rangle\,,\ |1\rangle\,|5\rangle\,,\ |2\rangle\,|4\rangle\,,\ |3\rangle\,|20\rangle\,,\ |4\rangle\,|17\rangle\,,\ |5\rangle\,|16\rangle\,,\ |6\rangle\,|1\rangle$

   ○ $|0\rangle\,|1\rangle\,,\ |1\rangle\,|5\rangle\,,\ |2\rangle\,|4\rangle\,,\ |3\rangle\,|21\rangle\,,\ |4\rangle\,|16\rangle\,,\ |5\rangle\,|17\rangle\,,\ |6\rangle\,|2\rangle$

Chapter 8

Quantum error correction

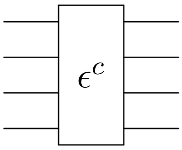
8.1 Features of classical error correction

There are three main tasks of error correction theory:

1. analyse errors occurring in the data channel to describe them in terms of a certain mathematical model
2. encode information so that data can be recovered after errors occur
3. create algorithms and procedures of error elimination

The information channel is a description of a bit set's evolution between two moments in time. The mathematical models of errors distinguish

- **bit flip errors:** the probability of bit flip errors is p and the probability of no error is $1 - p$ or there is a different probability for a bit flip to occur for each bit state
- **correlated bit errors:** occurrence leads to uncontrollable modification of several bits at once depicted by the symbol



Error correction algorithms of multi-bit errors are based on single bit correction algorithms. The term **information encoding** includes the following important aspects

- encoding provides information with more sustainability to errors from a given class or allows one to reverse their effect completely
- encoding is based on the **principle of redundancy**, which includes the addition of extra bits and the creation of codewords
- **redundancy** within information coding corresponds to a **certain error type**

An example is the **three-bit code**: From one bit one constructs a logical bit with the bit value encoded via codewords: $0 \to 0_L = 000$, $1 \to 1_L = 111$. Generally the information encoding can be represented as an action of a certain reversible logic element $\mathcal{G}_{\text{enc}}$ which transforms an initial bit A and an auxiliary bit Z into a codeword A_{enc}.

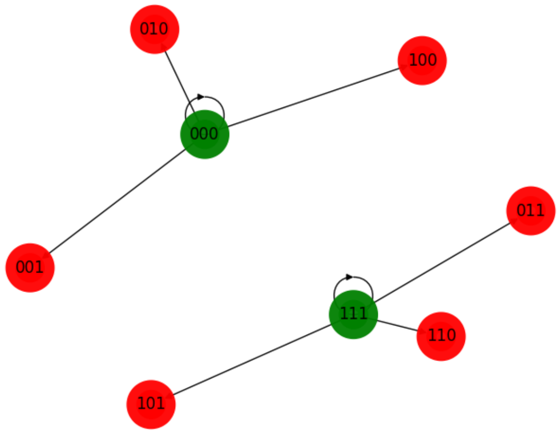
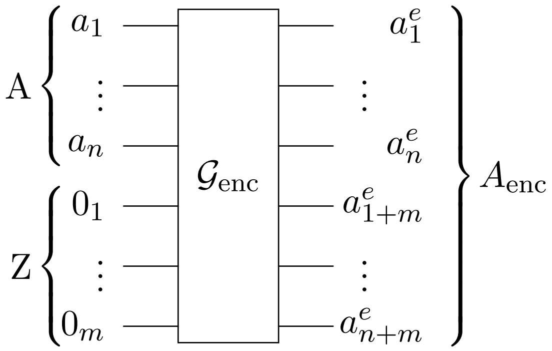
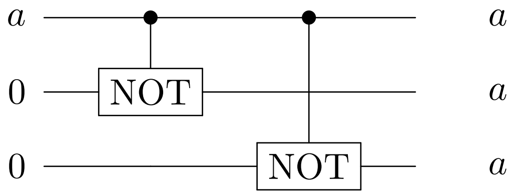


Figure 8.1: The codewords for the three-bit-code. In green are the initial codewords and in red their respective recovery codes, e.g. if ¨001¨ is read out at the computer, it is interpreted as a logical 0_L.



For **error recovery** the codewords need to be distinguishable after the affection of errors for decoding. **Correctable codewords** are those for which the codewords A_{enc} and B_{enc} after the affection of errors ϵ_i and ϵ_j remain distinguishable, i.e. $\epsilon_i(A_{\text{enc}}) \neq \epsilon_j(B_{\text{enc}} \forall i,j \in \{0,1,\ldots,n\}$. The example for the three bit code can be seen in Figure 8.1. The initial redundant state is prepared by



There are four different error processes:

$$\left.\begin{array}{ll}\text{no error} & (1-p)^3\\ \text{one error} & 3p(1-p)^2\end{array}\right\}\ \text{control codeword does not change}$$

$$\left.\begin{array}{ll}\text{two errors} & 3p^2(1-p)\\ \text{three errors} & p^3\end{array}\right\}\text{control codeword changes}$$

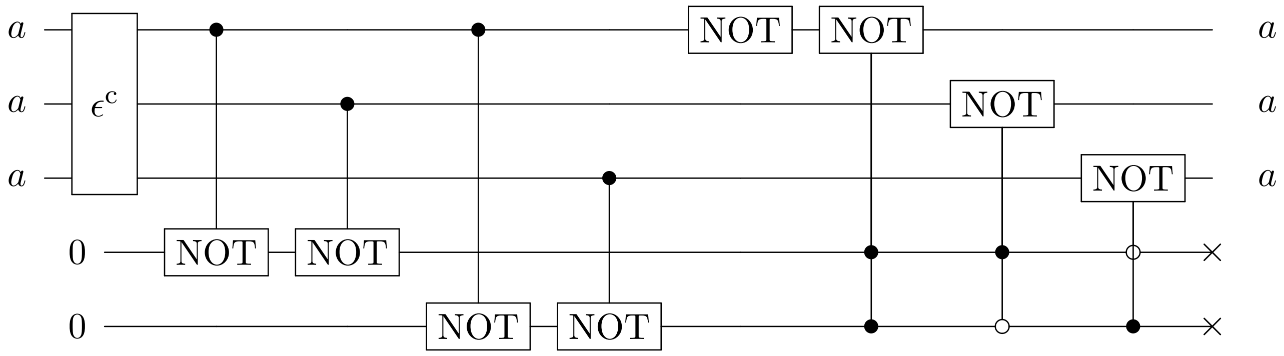
Hence, the three error code is **effective** if the following inequality holds:

$$3p^2(1-p)+p^3 < p \to p < \frac{1}{2}.$$

If no error or only one error occurred, then the correct result can be extracted. This is not true in general, e.g. for XOR of two bits (only one error):

- first codeword bit has the same parity as others → there is no error
- first codeword bit has other parity as only one other auxiliary bit → error in auxiliary bit
- first bit has different parity as the others → error in the first bit

Simply comparing the bits **parity** (not their values!) is sufficient to correct the errors. The error correction procedure for the three bit code is



The first two controlled-NOT operations after the error module compare the parity of the first two bits and the next two controlled-NOT operations compare the parity of the first and last bit.

8.2 Features of quantum error correction

The evolution of a qubit is a **continuous** physical process. Within the **projective measurement** of the qubit, the quantum reduction occurs and the qubit's superposition state turns into one of its **basis** states. It is impossible to to create an identical copy of a qubit in an **arbitrary quantum state**. The application of logical gates will not rotate always by the same angle, but will have some error due to the environment. The quantum error correction theories main problems are

- analysation of possible errors
- information encoding that allows to restore it after an error has occurred
- development of error correction procedures and algorithms

The models for a single qubit errors are

- the physical environment of a qubit acts as a **quantum information channel**

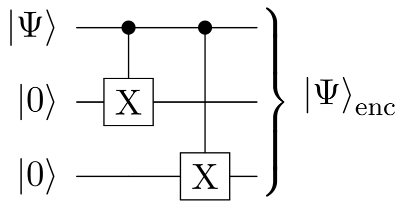
- result of the interaction between the qubit and the information channel can be represented by superposition of four discrete transformations:

$$\begin{aligned}\underbrace{\Big(\alpha_0\,|0\rangle+\alpha_1\,|1\rangle\Big)}_{|\Psi\rangle}|E\rangle \to \quad & \frac{1}{2}\,|\Psi\rangle\Big(\beta_1\,|E_1\rangle+\beta_3\,|E_3\rangle\Big)\text{ (no error)}\\ & +\frac{1}{2}\mathrm{Z}\quad|\Psi\rangle\Big(\beta_1\,|E_1\rangle-\beta_3\,|E_3\rangle\Big)\text{ (phase error)}\\ & +\frac{1}{2}\mathrm{X}\quad|\Psi\rangle\Big(\beta_2\,|E_2\rangle+\beta_4\,|E_4\rangle\Big)\text{ (bit flip error error)}\\ & -\frac{1}{2}\mathrm{XZ}\,|\Psi\rangle\Big(\beta_2\,|E_2\rangle-\beta_4\,|E_4\rangle\Big)\text{ (phase and bit flip error at once)}\end{aligned}$$

Despite the continuous evolutionof the ¨qubit + quantum¨ channel, all errors can be reduced to the four discrete operations. As any single-qubit operator can be represented by a linear combination of I, X, Y, Z, one can correct the errors using those operators (and their linear combination).

8.2.1 Information encoding

Due to the no-cloning theorem which forbids one to use codes with repetition, the encoding is based on the **redundancy principle** with respect to errors occurring in the quantum channel $|\Psi\rangle \to |\Psi\rangle\otimes|0_1 0_2\dots 0_m\rangle \to |\Psi\rangle_{\text{enc}}$.



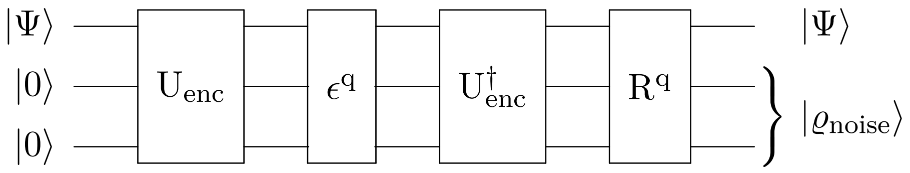
$$\begin{aligned}|\Psi\rangle_{\text{enc}} &= \mathrm{C_1X_2C_1X_3}\,|\Psi 00\rangle\\ &= \mathrm{C_1X_2}\Big[\alpha_0\,|000\rangle+\alpha_1\,|110\rangle\Big]\\ &= \alpha_0\,|000\rangle+\alpha_1\,|111\rangle\end{aligned}$$

8.2.2 Error recovery

Not all errors are correctable. Different code words must be distinguishable, i.e. $|\Phi\rangle_{\text{enc}} \neq |\Psi\rangle_{\text{enc}}$, after the error occurring in the channel:

$$\langle\Phi|_{\text{enc}}\,(\epsilon_i^q)^\dagger\epsilon_i^q\,|\Psi\rangle_{\text{enc}} = 0,\ \forall i,j\ \big(\,|\Phi\rangle_{\text{enc}} \neq |\Psi\rangle_{\text{enc}}\,\big).$$

Then the information before the error can be recovered by a set of gates $\mathrm{R^q}$.



8.2.3 Three-qubit code

If the bit flip errors can occur in the channel, the three-qubit code may be used. The quantum state of such a channel is represented by the following density matrix:

$$\rho = |\Psi\rangle\langle\Psi| \to \rho_{\mathrm{f}} = (1-p)\,|\Psi\rangle\langle\Psi| + p\mathrm{X}\,|\Psi\rangle\langle\Psi|\,\mathrm{X}.$$

If there are bit errors in the channel, the three-qubit code has the form:

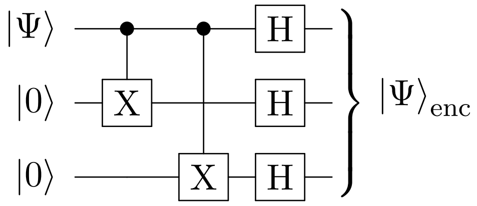
$$|\Psi\rangle \otimes |00\rangle = \big(\alpha_0 |0\rangle + \alpha_1 |1\rangle\,\big) \otimes |00\rangle \to \alpha_0 |000\rangle + \alpha_1 |111\rangle = |\Psi\rangle_{\mathrm{enc}}\,.$$

If a phase error can appear in the channel, it can be described by the density operator:

$$\rho = |\Psi\rangle \langle\Psi| \to \rho_{\mathrm{f}} = (1-p)\,|\Psi\rangle \langle\Psi| + p\mathrm{Z}\,|\Psi\rangle \langle\Psi|\,\mathrm{Z}.$$

the three-qubit code then has the form:

$$|\Psi\rangle \otimes |00\rangle = \big(\alpha_0 |0\rangle + \alpha_1 |1\rangle\,\big) \otimes |00\rangle \to \alpha_0 |000\rangle + \alpha_1 |111\rangle = |\Psi\rangle_{\mathrm{enc}}\,.$$



One, then, encodes into the Hadamard-basis:

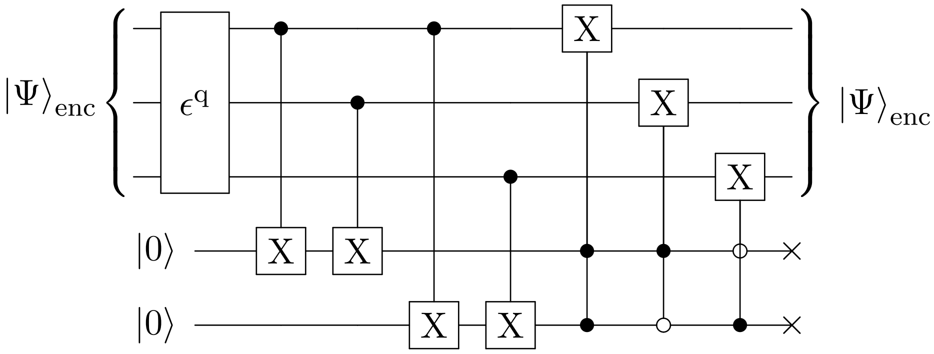
$$|\Psi\rangle_{\mathrm{enc}} = \alpha_0 |+++\rangle + \alpha_1 |---\rangle$$

The new codewords are

$$|0\rangle \to |+++\rangle\,,$$
$$|1\rangle \to |---\rangle\,.$$

Phase errors become bit flip errors, but in the Hadamard-basis.

8.2.4 Correction of bit-flip errors



Before the error block, the state is

$$|\Psi\rangle_{\mathrm{enc},0} = \alpha\,|000\rangle + \beta\,|111\rangle$$

After a bit-flip error in the first qubit, the state becomes:

$$|\Psi\rangle_{\mathrm{enc}} = \alpha\,|100\rangle + \beta\,|011\rangle\,.$$
$$|\Psi\rangle_{\mathrm{full}} = \alpha\,|100\rangle\,|00\rangle + \beta\,|011\rangle\,|00\rangle\,.$$

After the CX's on the auxiliary bits

$$|\Psi\rangle_{\mathrm{full}} = \alpha\,|100\rangle\,|11\rangle + \beta\,|011\rangle\,|11\rangle = \Big(\alpha\,|100\rangle + \beta\,|011\rangle\Big)\,|11\rangle\,.$$

After the Toffoli (correction) gates

$$|\Psi\rangle_{\mathrm{full}} = \Big(\alpha\,|000\rangle + \beta\,|111\rangle\Big)\,|11\rangle\,,$$

i.e. we recovered the initial state! For the phase correction, the CX elements will be CX in the Hadamard-basis ($\mathrm{H}_i\mathrm{C}_j\mathrm{X}_i\mathrm{H}_i$)

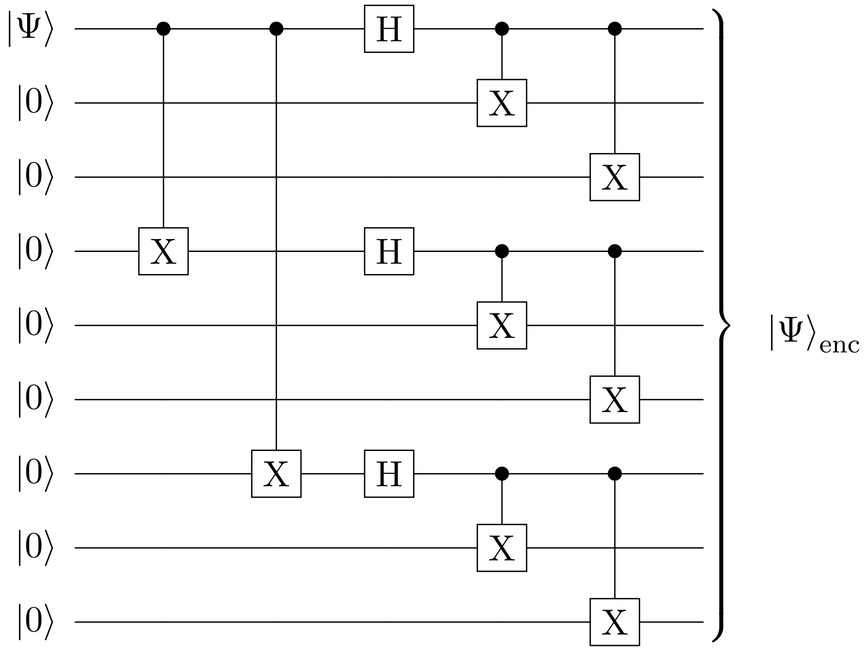
8.2.5 Nine-qubit Shor code

For bit-flip and phase errors in the channel, the three bit code can not be used. The density operator is

$$\rho = |\Psi\rangle \langle\Psi| \to \rho_{\mathrm{f}} = (1-p)\, |\Psi\rangle \langle\Psi| + p\mathrm{XZ}\, |\Psi\rangle \langle\Psi|\, \mathrm{ZX}.$$

and the **nine-qubit Shor encoding** is used

$$|0\rangle \to \frac{1}{2\sqrt{2}}\Big(|000\rangle + |111\rangle\Big) \otimes \Big(|000\rangle + |111\rangle\Big) \otimes \Big(|000\rangle + |111\rangle\Big)$$
$$|1\rangle \to \frac{1}{2\sqrt{2}}\Big(|000\rangle - |111\rangle\Big) \otimes \Big(|000\rangle - |111\rangle\Big) \otimes \Big(|000\rangle - |111\rangle\Big)$$



The error can be corrected using the same scheme described for the three-qubit code for the individual blocks of bit-flip and phase errors.

8.3 Exercises

1. Which errors are correctable?

   ○ Errors that keep different codewords distinguishable
   ○ Errors that transform one codewords into another
   ○ Errors that change only one of the codewords

2. What are the probabilities of the three-bit error code being effective?

   ○ $P < 1/2$
   ○ $P > 1/3$
   ○ $P = 1$
   ○ $P < 1/3$

3. When comparing parity in the case of a three-bit error code, we receive that the 1st bit in the codeword does not match the parity of the service bits. It means that:

○ An error did not occur

○ An error occurred in the service bit

○ An error occurred in the first bit

4. What type of errors correspond to the action of the logical operator Z on the qubits?

○ The phase error

○ The bit error

○ Phase and bit error

5. Select the operators that transform the states $|000\rangle$ and $|111\rangle$ into the state $|110\rangle$:

○ $X_1 \otimes X_2 \otimes I_3$ and $X_1 \otimes I_2 \otimes I_3$

○ $I_1 \otimes X_2 \otimes Z_3$ and $X_1 \otimes X_2 \otimes I_3$

○ $X_1 \otimes X_2 \otimes I_3$ and $I_1 \otimes I_2 \otimes X_3$

○ $X_1 \otimes Z_2 \otimes I_3$ and $Z_1 \otimes X_2 \otimes I_3$

6. What phase errors listed below can be corrected using three-qubit quantum error correction codes?

○ $I_1 \otimes Z_2 \otimes I_3$

○ $Z_1 \otimes I_2 \otimes Z_3$

○ $I_1 \otimes I_2 \otimes Z_3$

○ $Z_1 \otimes Z_2 \otimes Z_3$

7. Which error occurred with a logical qubit in a three-qubit error correction code, if the error syndrome is 01?

○ X_1

○ X_2

○ X_3

8. What phase error occurred with a logical qubit in a three-qubit error correction code, if the measurement of the auxiliary qubits yields $|-+\rangle$?

○ Z_1

○ Z_2

○ Z_3

9. Suppose that after the measurement of the syndrome in the nine-qubit Shor code, we know that there is a phase error in the eighth qubit. What transformations can we make to correct this error?

○ $I_1 \otimes I_2 \otimes I_3 \otimes Z_4 \otimes Z_5 \otimes I_6 \otimes I_7 \otimes Z_8 \otimes I_9$

○ $I_1 \otimes I_2 \otimes I_3 \otimes I_4 \otimes X_5 \otimes I_6 \otimes I_7 \otimes I_8 \otimes I_9$

○ $I_1 \otimes I_2 \otimes I_3 \otimes I_4 \otimes I_5 \otimes I_6 \otimes I_7 \otimes X_8 Z_8 \otimes I_9$

○ $I_1 \otimes I_2 \otimes I_3 \otimes I_4 \otimes I_5 \otimes I_6 \otimes I_7 \otimes Z_8 \otimes I_9$

Part III

Introduction to quantum computing

literature

- John Preskill's lecture notes on quantum computing
- Umesh Vazirani's lectures on quantum computing
- popular science books by David Deutsch

Chapter 9

Quantum Computing and Information Theory

9.1 Computing and Computers

A **computation** is a physical process which is finite in time with a fixed set of states. **Information** is an interpretation of a particular system's state from a set of distinguishable states. The quantity of information I can be expressed by the **Shannon entropy** from the probability of the states being populated p_i

$$I = -\sum_{i=1}^{N} p_i \log p_i .$$

For $p_i = 1$ and $p_j = 0 \forall\, j \neq i$ this function has a minimum ($I = 0$) and for equiprobable states it has a maximum ($I = \log N$).
In Figure 9.1, **Szillard's engine** is depicted. It is a system that can store one bit of information. A computation corresponds to pushing the pistons in or out and moving the particle inside. The work needed to change the state is $W = k_\mathrm{B} T \log \frac{V_1}{V_2} = k_\mathrm{B} T \log 2$. A NOT function is realised by pushing one of the pistons in and then out again. We can also let the particle push the piston back and regain the energy $\simeq$ ERASE function, i.e. the information equals the energy!
The characteristics of a computational system are

1. information capacity (Shannon formula)
2. speed (switching between states)
3. universality (what problems can be solved)

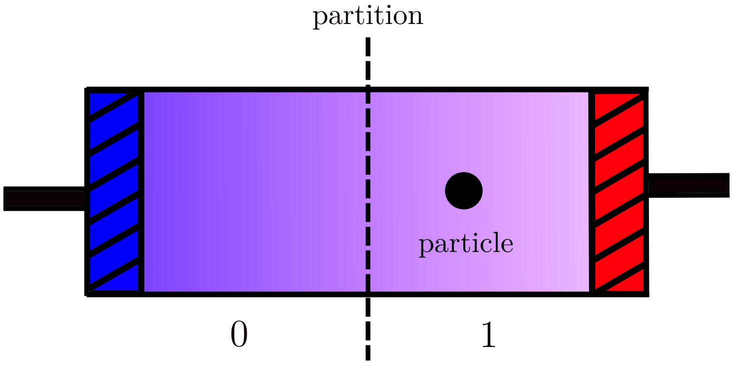


Figure 9.1: Szillard's engine

In order to make smaller devices (consume less energy, can be packed closer together, have less inertia and can, therefore, switched faster) than 10nm (about 100 hydrogen atoms), computers need to be quantum.

The goal of every computation is to determine the value of a function $\left\{f:\mathbb{N}\to\{0,1\}\right\}$, $f: \forall x\in\mathbb{N}\ f(x)$. For this an **algorithm** is needed. An algorithm is a deterministic Turing machine (DTM).

How many algorithms are there?	→	The set of algorithms is countable
How many functions are there?	→	There is a continuum of functions.
Are there uncomputable functions?	→	There are almost no uncomputable functions and some are helpful.

A computer can calculate more than we can analyse.

9.2 Computational complexity

For a graph, there are two famous problems:

1. **Euler path:** visits every edge once
2. **Hamilton path:** visits each vertex exactly once

The first problem is easy and the second one is extremely hard[1]. To determine the complexity of an algorithm, one uses the number of steps/operations in it as a function of the inputs state size, e.g. $\boldsymbol{a}+\boldsymbol{b}=\sum\limits_i(a_i+b-i)\boldsymbol{e}_i\to 2n$ steps $\mathcal{O}(n)$ or $\boldsymbol{a}.\boldsymbol{b}=\sum\limits_{ij}a_ib_j\boldsymbol{e}_i.\boldsymbol{e}_j\to n^2$ steps $\mathcal{O}(n^2)$. For any finite power in $\mathcal{O}(n^p)$ the problem is is called **P** (tractable), for all others the problem is called **NP** (hard). It is clear that P ⊂ NP, but P < NP is unproven and the famous **P=NP problem**.

9.3 Quantum computing and quantum information

Quantum computing uses quantum effects which are hard to model. The quantum system is used as a computer and the superposition of classical states is used for superior computation abilities. The quantum computer has to be a closed system during the calculation, i.e. before the result is read out through a measurement and the observer and the computer entangle (observer and observation).

The smallest unit of quantum information is the **qubit**. It describes the state of a system with two-dimensional state space $|\Phi\rangle\in\mathcal{H}, \|\Phi\|=1, \dim\mathcal{H}=2$. Angles between states are given by

$$\frac{|\langle x|\,|y\rangle|}{\|x\|\|y\|}=\cos\alpha\Rightarrow\alpha\in\left[0,\frac{\pi}{2}\right]$$

The last property for α is different to classical (real) vector spaces. A general qubit state $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$ with $\alpha,\beta\in\mathbb{C}$ and $|\alpha|^2+|\beta|^2=1$ live in a (4-1)-dimensional space that is called the **Bloch sphere**. Choosing the right basis is important to extract the most information from a state, e.g. for light, the polarisation (its optical axis) can be used to encode information 0 (light is vertically polarised) or 1 (light is horizontally polarised) into a single photon. Rotation of the polarisers is equivalent to choosing another basis.

Many qubits can be combined to have more involved computations possible and entangled to utilise the full power of quantum computing: n qubits belong to $\mathcal{H}^n$ and have dimension 2^n. There are many-qubit states that can not be represented by tensor products of single-qubit

[1] It is unclear whether an algorithm exists or not

states. Those are called **entangled**. **Quantum gates** are mathematically represented by unitary operators and are used to manipulate quantum states of qubits, e.g.

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\ \mathrm{X} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\ \mathrm{Z} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\ \mathrm{CX} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}.$$

and the many-qubit Hadamard transform

$$\mathrm{H}^n \left|x\right\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y} \left|y\right\rangle$$

with $x \cdot y = x_0y_0 \oplus x_1y_1 \oplus \cdots \oplus x_{n-1}y_{n-1}$ inner product of $\mathbb{Z}_2^n$)

here $\oplus$ is the modulo 2 addition.

9.4 Exercises

1. The advantages of quantum computers are...

   ○ Possibly smaller size and thus smaller inertia of the computational process base element

   ○ Quantum computers are analogue computers, so their repertoire is larger

   ○ The ability to employ all copies of the computational system in the multiverse to store and process data.

2. Is a tornado a computational process?

   ○ Yes

   ○ No

   ○ It can be, if we learn to distinguish its states and control their switching

3. Which of the following is **not** a necessary characteristic of a computational process?

   ○ The process must be a physical process, not a mathematical model or a thought experiment

   ○ The process must be deterministic

   ○ The process must have states that we can distinguish

4. Assume that you have to transfer a message over a corrupted channel which can randomly flip one of the bits in your message. You are allowed to send n bits and you can use this channel only once. You do not know which bit is going to be corrupted. There are many possible ways to encode your data so that there will be no information loss (for example you can transfer a message of length $n/3$ three times so the receiver will be able to choose the correct value for each bit comparing the values of it from different copies of the message). How many bits can you correctly transfer with the best possible strategy?

   ○ $\log_2 n$

   ○ $\frac{n}{3}$

   ○ $n - 1$

   ○ $n - \log_2{(n+1)}$

   ○ $\frac{n}{2}$

5. Assume that you have to use the channel from the previous question which allows you to send 7 bits. Messages of which length (in bits) can you transfer over this channel with no data loss?

6. $\sin \mathrm{i} = \ldots$

   ○ $\frac{1-\mathrm{e}^2}{2\mathrm{ei}}$

   ○ This value is undefined

   ○ $\frac{1+\mathrm{e}^2}{2\mathrm{e}}$

   ○ $\frac{1-\mathrm{i}}{2}$

7. The state $|\Phi\rangle = \frac{1-\sqrt{2}\mathrm{i}}{4}|0\rangle - \frac{3-2\mathrm{i}}{4}|1\rangle$ is measured in the Hadamard basis $\{\,|+\rangle, |-\rangle\,\}$. What is the probability to obtain $|+\rangle$ as a measurement result?

   ○ $\frac{5-2\sqrt{2}}{16}$

   ○ $\frac{7}{16}$

   ○ $\frac{11}{32}$

   ○ $\frac{5-2\sqrt{2}}{32}$

8. What share of non-polarised light passes through the linear polariser?

   $\int\limits_{0}^{2\pi} \cos^2(\phi) \frac{\mathrm{d}\phi}{2\pi}$

   ○ $\frac{2}{\pi}$

   ○ $\frac{1}{2}$

   ○ $\frac{1}{3}$

   ○ $\frac{3}{\pi}$

9. The first qubit of the state $|\Phi\rangle = \frac{1+\sqrt{3}\mathrm{i}}{4}|00\rangle + \frac{1-\sqrt{3}\mathrm{i}}{4}|01\rangle + \frac{1-\sqrt{3}\mathrm{i}}{4}|10\rangle + \frac{1+\sqrt{3}\mathrm{i}}{4}|11\rangle$ was measured in the Hadamard basis with the result $|-\rangle$. What is the probability to obtain the vector $|0\rangle$ as the result of measuring the second qubit in the standard basis $\{\,|0\rangle, |1\rangle\,\}$?

   ○ 0

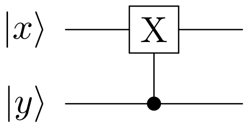
   ○ $\frac{1}{2}$

   ○ $\frac{3}{16}$

   ○ 1

   ○ $\frac{1}{16}$

10. What is the matrix (in the standard basis) implemented by this scheme?



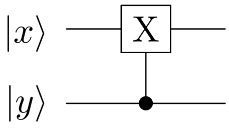
   ○ $\begin{pmatrix} \mathrm{X} & 0 \\ 0 & X \end{pmatrix}$

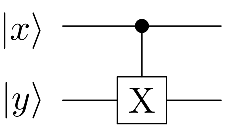
○ $\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

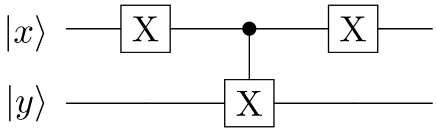
○ $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

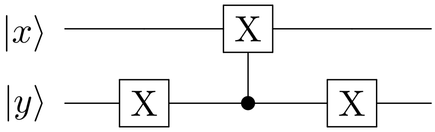
○ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

11. Which circuit scheme implements the operator $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

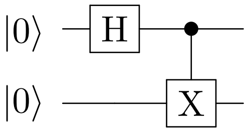
○ 

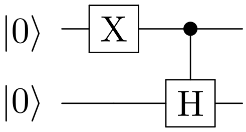
○ 

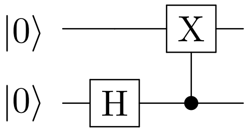
○ 

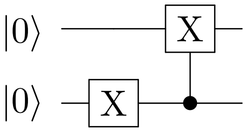
○ 

12. Which circuit scheme implements the operation $|00\rangle \rightarrow \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$?

○ 

○ 

○ 

○ 

Chapter 10

Oracle functions

10.1 Deutsch's problem

Deutsch's problem refers to the task of determining whether a (black box) function $f : \{0,1\} \to \{0,1\}$ is constant or balanced. Classically one has to evaluate the function twice to decide, while with a quantum computer, one only needs one sweep!
The quantum oracle is

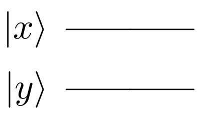
$$\begin{aligned} U_f \left|x\right\rangle \left|0\right\rangle &\to \left|x\right\rangle \left|f(x)\right\rangle \\ \left|00\right\rangle &\to \left|0f(0)\right\rangle \\ \left|10\right\rangle &\to \left|1f(1)\right\rangle \\ U_f \left|x\right\rangle \left|1\right\rangle &\to \left|x\right\rangle \left|1 \oplus f(x)\right\rangle \\ U_f \left|x\right\rangle \left|y\right\rangle &\to \left|x\right\rangle \left|x \oplus f(x)\right\rangle \text{ (quantum oracle)} \end{aligned}$$

Applying the oracle to a special superposition state

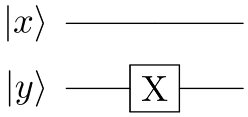
$$U_f \frac{1}{\sqrt{2}} \left|x\right\rangle \Big(\left|0\right\rangle - \left|1\right\rangle \Big) = \frac{1}{\sqrt{2}} \Big(U_f \left|x\right\rangle \left|0\right\rangle - U_f \left|x\right\rangle \left|1\right\rangle \Big) = \frac{1}{\sqrt{2}} \Big(\left|x\right\rangle \left|f(x)\right\rangle - \left|x\right\rangle \left|1 \oplus f(x)\right\rangle \Big)$$

with the result for $f(x)$ being constant:

$$f(x) = 0 \ \to U_f = \mathrm{I}$$

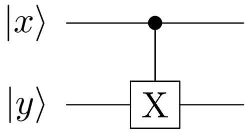


$$f(x) = 1 \ \to U_f = \mathrm{X}_2 = \mathrm{I} \otimes \mathrm{X}$$

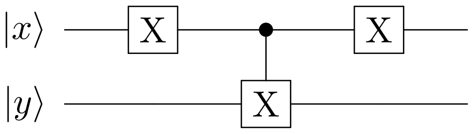


and the result with $f(x)$ being balanced:

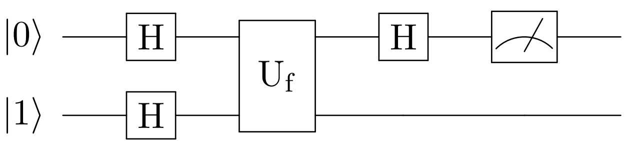
$$f(x) = x \ \to \left.\begin{array}{lcl} \left|00\right\rangle & \to & \left|00\right\rangle \\ \left|01\right\rangle & \to & \left|01\right\rangle \\ \left|10\right\rangle & \to & \left|11\right\rangle \\ \left|11\right\rangle & \to & \left|10\right\rangle \end{array}\right\} U_f = \mathrm{C}_1\mathrm{X}_2$$



$$f(x) = \overline{x} \ \to \left.\begin{array}{lcl} \left|00\right\rangle & \to & \left|01\right\rangle \\ \left|01\right\rangle & \to & \left|00\right\rangle \\ \left|10\right\rangle & \to & \left|10\right\rangle \\ \left|11\right\rangle & \to & \left|11\right\rangle \end{array}\right\} U_f = \mathrm{X}_1\mathrm{C}_1\mathrm{X}_2\mathrm{X}_1$$



The quantum circuit for Deutsch's algorithm is



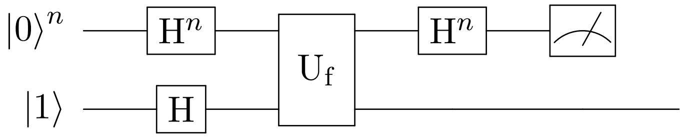
The state evolution is

$$\begin{aligned}
\mathrm{H}_1\mathrm{H}_2\left|01\right\rangle &= \left|+-\right\rangle = \frac{1}{2}\Big[\left|0\right\rangle\big(\left|0\right\rangle - \left|1\right\rangle\big) + \left|1\right\rangle\big(\left|0\right\rangle - \left|1\right\rangle\big)\Big] \\
\mathrm{U_f}\left|+-\right\rangle &= \frac{1}{2}\Big[\left|0\right\rangle\left|0+f(0)\right\rangle - \left|0\right\rangle\left|1+f(0)\right\rangle + \left|1\right\rangle\left|0+f(1)\right\rangle - \left|1\right\rangle\left|1+f(1)\right\rangle\Big] \\
&= \frac{(-1)^{f(0)}}{\sqrt{2}}\left|0\right\rangle\left|-\right\rangle + \frac{(-1)^{f(1)}}{\sqrt{2}}\left|1\right\rangle\left|-\right\rangle \\
\mathrm{H}_1U_f\left|+-\right\rangle &= \frac{1}{\sqrt{2}}\Big[(-1)^{f(0)}\left|+\right\rangle + (-1)^{f(1)}\left|-\right\rangle\Big]\left|-\right\rangle \\
&= \frac{1}{2}\Big[(-1)^{f(0)}\big(\left|0\right\rangle + \left|1\right\rangle\big) + (-1)^{f(1)}\big(\left|0\right\rangle - \left|1\right\rangle\big)\Big]\left|-\right\rangle = \left|\Psi\right\rangle_{\mathrm{end}}
\end{aligned}$$

For a constant $f(x)$ the final state is $\left|\Psi\right\rangle_{\mathrm{end}} = \left|0\right\rangle\left|-\right\rangle$ and the measurement yields $\left|0\right\rangle$ with probability 1. For a balanced $f(x)$ the final state is $\left|\Psi\right\rangle_{\mathrm{end}} = \left|1\right\rangle\left|-\right\rangle$ and the measurement yields $\left|1\right\rangle$ with probability 1.

10.2 Bernstein-Vazirani

The problem of the **Bernstein-Vazirani problem** is given a function $f : \{0,1\}^n \to \{0,1\}$ $f(x) = \big(\boldsymbol{a}\cdot\boldsymbol{x}\big) \bmod 2$ to find the secret key vector $\boldsymbol{a}$. Classically one needs N queries of the oracle (one per bit of $\boldsymbol{a}$). In the quantum case, one only needs one query. The Bernstein-Vazirani algorithm is



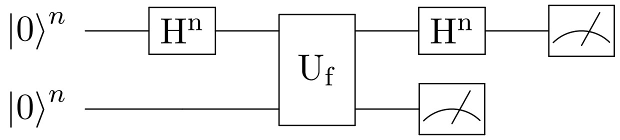
The evolution of the quantum system for this circuit is the following

$$\begin{aligned}
\mathrm{H}^n\left|0\right\rangle^n\left|1\right\rangle &= \frac{1}{2^{(n+1)/2}}\left(\sum_{x=0}^{2^n-1}\left|x\right\rangle\right)\big(\left|0\right\rangle - \left|1\right\rangle\big) \\
\mathrm{U_f}\mathrm{H}^n\left|0\right\rangle^n\left|1\right\rangle &= \frac{1}{2^{(n+1)/2}}\underbrace{\left(\sum_{x=0}^{2^n-1}(-1)^{f(x)}\left|x\right\rangle\right)}_{\mathrm{H}\left|a\right\rangle}\big(\left|0\right\rangle - \left|1\right\rangle\big)
\end{aligned}$$

and the measurement at the end yields $\left|a\right\rangle$ and with it $f(x) = \big(\boldsymbol{a}\cdot\boldsymbol{x}\big) \bmod 2$ in one query.

10.3 Simon's problem

In **Simon's problem** the oracle function is $f : \{0,1\}^n \to \{0,1\}^n \, \exists a \neq 0 : \forall x \, f(x) = f(y) \Leftrightarrow y = x \oplus a$ and the task is to find a. The algorithm for it is



Here is the state's evolution up to the first measurement

$$\mathrm{U_f H^n}\,|0\rangle^n\,|0\rangle^n = \frac{1}{2^{n/2}}\mathrm{U_f}\sum_{x=0}^{2^n-1}|x\rangle\,|0\rangle^n = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle\,|f(x)\rangle$$

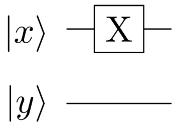
and the resulting state is $\frac{1}{\sqrt{2}}\big(\,|x_0\rangle + |x_0 \oplus a\rangle\,\big)\,|f(x_0)\rangle$. After the n-qubit Hadamard gate the state of the remaining not measured quantum state is

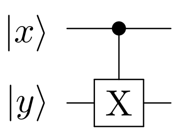
$$\begin{aligned}\mathrm{H^n}\big(\,|x_0\rangle + |x_0 \oplus a\rangle\,\big) &= \frac{1}{2^{(n+1)/2}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}\,|y\rangle + \frac{1}{2^{(n+1)/2}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot(y\oplus a)}\,|y\rangle \\ &= \frac{1}{2^{(n+1)/2}}\sum_{y=0}^{2^n-1}\Big((-1)^{x\cdot y} + (-1)^{x\cdot y \oplus a\cdot y}\Big)\,|y\rangle = \frac{1}{2^{(n+1)/2}}\sum_{y:a\cdot y=0}|y\rangle\end{aligned}$$

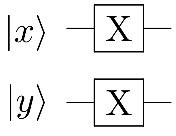
and after the second measurement, we have obtained one y that satisfies $a \cdot y = 0$. Hence, we need to run the algorithm (at least) $\mathcal{O}(n)$ times to solve the problem.

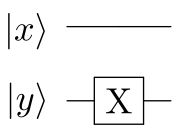
10.4 Exercises

1. Which of the following circuit schemes implements the operator $U = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$?

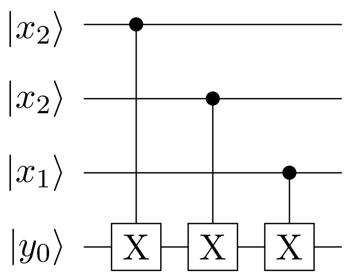
○ 

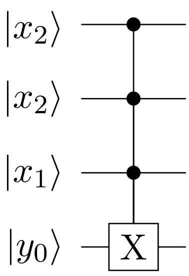
○ 

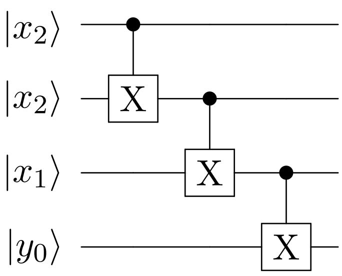
○ 

○ 

2. Choose the correct implementation of the U$_f$ operator for the function $f(x) :\ \{\,|0\rangle\,,|1\rangle\,\}^3 \to \{\,|0\rangle\,,|1\rangle\,\}\ f(x) = 7 \cdot x$ (the bitwise vector product between 7 and the state modulo 2)

○ 

○ 

○ 

3. The function $f(x):\ \{\,|0\rangle\,,|1\rangle\,\}^2 \to \{\,|0\rangle\,,|1\rangle\,\}\ f(x_1,x_0)=x_0$ returns the least significant bit of its argument. Solve the Simon's problem for this function and write down the number a in the decimal numeral system.

4. The function $f(x):\ \{\,|0\rangle\,,|1\rangle\,\}^2 \to \{\,|0\rangle\,,|1\rangle\,\}\ f(x_1,x_0)=x_0$ returns the least significant bit of its argument. What is the U_f operator for this function?

   ○ $\mathrm{CNOT}\otimes\mathrm{I}$

   ○ $\mathrm{X}\otimes\mathrm{X}\otimes\mathrm{X}$

   ○ $\mathrm{X}\otimes\mathrm{I}\otimes\mathrm{X}$

   ○ $\mathrm{I}\otimes\mathrm{CNOT}$

5. In the Simon's algorithm, we used the intermediary measurement of the value register $|y\rangle$. If we remove this measurement step, how will it change the result of the algorithm?

   ○ The algorithm will work incorrectly (giving us no information about the number a)

   ○ The algorithm will work correctly but slower, since there are more states to process.

   ○ Nothing will change. This intermediary measurement was introduced to clarify the algorithm's action. Otherwise, we would have had to write more sum signs.

Chapter 11

Shor-algorithm

The task of the Shor algorithm is to factor $N = p \cdot q$ into its two prime factors p and q. A brute force search needs to check all numbers from $[2, \sqrt{N}]$, i.e. as many divisions and one more square root operation. There is no (known) classical algorithm that can perform much better. Factoring takes very long on classical computers and is, therefore, used cryptography (https, RSA). Shor's algorithm solves the problem much faster.

11.1 The RSA algorithm

First one creates a number $N = pq$ by multiplying two (different) prime numbers p, q. Then, one calculates the Euler ϕ-function of N $\phi(N) = (p-1)(q-1)$ and chooses a number e for which $\gcd(e, N) = 1$ and $\gcd(e, \phi(N)) = 1$. Then there is another number $d < N$ for which $ed \bmod \phi(N) = 1$ and, therefore, there exists a k for which $ed + \phi(N)k = 1$. Now one uses the duplet (e, N) as public and the duplet (d, N) as private key.
The RSA-algorithm for encryption of a message m encodes it such that $\gcd(m, N) = 1$, then $m^{ed} \bmod N = m^1 \cdot \underbrace{m^{\phi(N)\cdot k} \bmod N}_{=1} = m$.

11.1.1 example

$$\begin{aligned}
&p = 11,\ q = 13 \rightarrow N = 143, \phi(143) = 120 \\
&\text{choose } e = 17,\ m = 7 \rightarrow \text{ encrypt } (17, 143) \\
&7^{17} \bmod 143 = 7 \cdot \underbrace{(49)^8}_{\substack{(50-1)^2 \\ = 2500 - 100 + 1 \\ = 2401 \bmod 143 = 113}} \bmod 143 = 7 \cdot 113^4 \\
&113 = -30 \bmod 143 = 900 \bmod 143 = 42 \bmod 143 \\
&\Rightarrow 7^17 \bmod 143 = 7 \cdot 42^2 \bmod 143 = 7 \cdot 48 \bmod 143 = 50 \, (\textbf{encrypted message})
\end{aligned}$$

$$\begin{aligned}
&\text{decryption: public key (17,143) enc(m)=50} \\
&\text{private key : } 17d = 1 + 120k \\
&\text{for d=-7, k=-1 it is fulfilled} \rightarrow d = 113 \\
&50^{113} \bmod 143 = 7 \rightarrow \textbf{original message}
\end{aligned}$$

11.1.2 Factoring and period finding

For $N = pq$ and for all $a < N, (a, N) = 1$ the greatest common divisor is either p or q. We define the function $f_a(x) = a^x \bmod N$ then there is an r for which $a^{x+r} \bmod N = a^x \cdot \underbrace{a^r \bmod N}_{=1} = a^x \bmod N$ and for all $r_1 < r$ we have $a^{r_1} \neq 1 \bmod N$. Then $r \bmod 2 = 0$ so that $(a^r - 1) \bmod N = 0$ and, therefore, $(a^{r/2} + 1)(a^{r/2} - 1) \bmod N = 0$ if we assume $r \bmod 2 = 0$ (r is even) and $a^{r/2} \bmod N \neq -1$. This means that $p, q = \gcd(a^{r/2} \pm 1, N)$ meaning that if we can find the period r we can easily determine the factorisation of N by determining the greatest common divisor of a randomly selected number a raised to the power of $r/2$ and N. This can be done using the **Euclidean algorithm**.

11.2 Quantum Fourier Transformation

The n-dimensional quantum Fourier transformation is defined by $(N = 2^n)$

$$|x\rangle = \frac{\|x\|}{\sqrt{N}} \sum_{y=0}^{N-1} \mathrm{e}^{2\pi\mathrm{i}\frac{xy}{N}} |y\rangle .$$

It is unitary:

$$\|\mathrm{QFT}\|^2 = \frac{\|x\|^2}{N} \sum_{y} \mathrm{e}^{-2\pi\mathrm{i}\frac{xy}{N}} \left\langle y \middle| \sum_{y'} \mathrm{e}^{2\pi\mathrm{i}\frac{xy'}{N}} \middle| y' \right\rangle = \frac{\|x\|^2}{N} \Big(\sum_{y \neq y'} \mathrm{e}^{\cdots} \underbrace{\langle y|\,|y'\rangle}_{=0} + \sum_{y=y'} \mathrm{e}^{2\pi\mathrm{i}x(y-y')/N} \langle y|\,|y'\rangle \Big)$$

$$= \frac{\|x\|^2}{N} N = \|x\|^2.$$

Angles remain unchanged. Consider the inner product for two states with $\|x_1\| = \|x_2\| = 1$ and $\langle x_1|\,|x_2\rangle = 0$:

$$\langle x_1|\,\mathrm{QFT}^\dagger \mathrm{QFT}\,|x_2\rangle = \frac{1}{N} \Big(\sum_{y_1} \langle y_1|\, \mathrm{e}^{-2\pi\mathrm{i}\frac{y_1 \cdot x_1}{N}} \Big) \Big(\sum_{y_2} \langle y_2|\, \mathrm{e}^{2\pi\mathrm{i}\frac{y_2 \cdot x_2}{N}} \Big)$$

$$= \frac{1}{N} \sum_{y_1 = y_2} 2\pi\mathrm{i} \frac{\mathrm{y_1(x_2 - x_1}}{\mathrm{N}} = 0 \text{ (sum over full period).}$$

Implementation

Keep only the fractional part of $\frac{x \cdot y}{N}$:

$$x = x_0 + 2x_1 + 2^2 x_2 + \cdots + 2^{n-1} x_{n-1}$$

$$y = y_0 + 2x_1 + 2^2 y_2 + \cdots + 2^{n-1} y_{n-1}$$

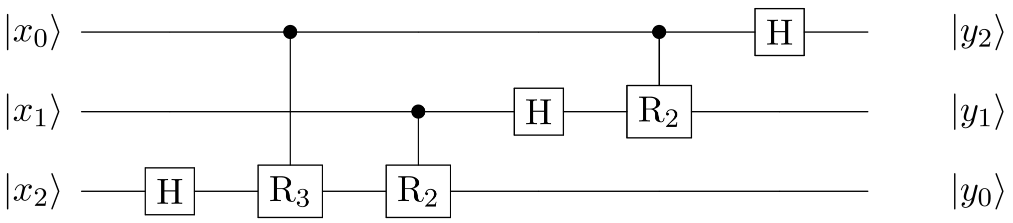
$$\frac{y_j x_{n-j}}{N} = \frac{2^n y_j x_{n-j}}{2^n} = y_j x_{n-j}$$

$$\to \frac{xy}{N} = \frac{y_{n-1} x_0}{2} + \frac{y_{n-2} x_1}{4} + \cdots + y_0 \Big(\frac{x_0}{2^n} + \frac{x_1}{2^{n-1}} + \frac{x_{n-1}}{2} \Big).$$

Putting this into the exponent:

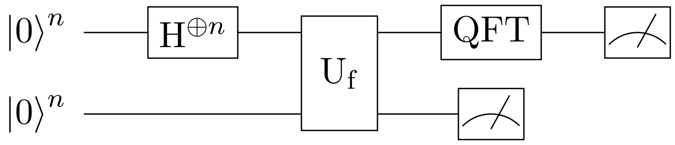
$$\begin{aligned}
\mathrm{QFT}\,|x\rangle &= \frac{1}{\sqrt{N}}\sum_{y_0=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i} y_{n-1}\frac{x_0}{2}}\mathrm{e}^{2\pi \mathrm{i} y_{n-2}\left(\frac{x_0}{4}+\frac{x_1}{2}\right)} \times \dots \times \mathrm{e}^{2\pi \mathrm{i} y_0\left[\frac{x_0}{2^n}+\frac{x_1}{2^{n-1}}+\dots+\frac{x_{n-1}}{2}\right]}\,|y\rangle \\
&= \frac{1}{\sqrt{2}}\mathrm{e}^{2\pi \mathrm{i}\cdot 0}\,|0\rangle \cdot \frac{1}{2^{n-1/2}}\sum_{y_0=0}^{2^{n-1}-1} \dots + \frac{1}{\sqrt{2}}\mathrm{e}^{2\pi \mathrm{i}\cdot 1\frac{x_0}{2}}\,|1\rangle \\
&= \frac{1}{\sqrt{2}}\Big(\,|0\rangle + \mathrm{e}^{2\pi \mathrm{i}\frac{x_0}{2}}\,|1\rangle\Big) \otimes \frac{1}{2^{n-1/2}}\sum_{y=0}^{2^{n-1}-1} \mathrm{e}^{2\pi \mathrm{i} y_{n-2}(\dots)}\dots|y_{n-2}\dots y_0\rangle \\
&= \frac{1}{\sqrt{2}}\Big(\,|0\rangle + \mathrm{e}^{2\pi \mathrm{i}\frac{x_0}{2}}\,|1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(\,|0\rangle + \mathrm{e}^{2\pi \mathrm{i}(\frac{x_0}{4}+\frac{x_1}{2})}\,|1\rangle\Big) \otimes \dots \\
&\quad \otimes \frac{1}{\sqrt{2}}\Big(\,|0\rangle + \mathrm{e}^{2\pi \mathrm{i}\left(\frac{x_0}{2^n}+\frac{x_1}{2^{n-1}}+\dots+\frac{x_{n-1}}{2}\right)}\,|1\rangle\Big)
\end{aligned}$$

Instead of $\mathcal{O}(N^2)$ multiplications, one has only $\mathcal{O}(N)$ multiplications. Introducing the operator $\mathrm{R}_k = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{2\pi\mathrm{i}/2^k}\end{pmatrix}$, $k \in \mathbb{N}, k \geq 1$, $k \leq N$ the QFT for three qubits is



11.3 Shor's algorithm

The quantum circuit for Shor's algorithm is the following



Up to the first measurement the state is

$$|0\rangle^n\,|0\rangle^n \overset{\mathrm{U_f H^{\oplus n}}}{\Rightarrow} \frac{1}{2^{n/2}}\sum_{x=0}^{N-1}|x\rangle\,|f(x)\rangle$$

and after measuring y

$$\frac{1}{\sqrt{A}}\sum_{j=0}^{A-1}|x_0+jr\rangle\,|f(x_0)\rangle\,,\ A \approx \frac{N}{r}$$

and after the QFT

$$\frac{1}{\sqrt{AN}}\sum_{j=0}^{A-1}\sum_{y=0}^{N-1}\mathrm{e}^{2\pi\mathrm{i}\frac{x_0 y}{N}}\mathrm{e}^{2\pi\mathrm{i}\frac{jry}{N}}\,|y\rangle = \frac{1}{\sqrt{AN}}\sum_{y=0}^{N-1}\mathrm{e}^{2\pi\mathrm{i}\frac{x_0 y}{N}}\sum_{j=0}^{A-1}\mathrm{e}^{2\pi\mathrm{i}\frac{jry}{N}}\,|y\rangle$$

The probability to measure a particular y is

$$p(y) = \frac{1}{AN}\left|\sum_{j=0}^{A-1}\mathrm{e}^{2\pi\mathrm{i}\frac{jry}{N}}\right|^2 = \frac{1}{AN}\left|\sum_{j=0}^{A-1}\mathrm{e}^{\mathrm{i}j\theta_y}\right|^2$$

where in the last equality we changed to the variable $\theta_y = 2\pi \frac{ry(N)}{N}$. For the y's in the range for which $A|\theta_y| \in [0, \pi]$ the probability is

$$\left| \sum_{j=0}^{A-1} \mathrm{e}^{\theta_y \mathrm{i} j} \right|^2 = \left| \frac{\mathrm{e}^{A\theta_y \mathrm{i}} - 1}{\mathrm{e}^{\theta_y \mathrm{i}} - 1} \right|^2 .$$

The numerator can be approximated as

$$\begin{aligned}
\left| \mathrm{e}^{A\theta_y \mathrm{i}} - 1 \right| &= |\cos(A\theta_y) - 1 + \mathrm{i}\sin(A\theta_y)| = \sqrt{\cos^2(A\theta_y) - 2\cos(A\theta_y) + \sin^2(A\theta_y)} \\
&= \sqrt{2 - 2\cos(A\theta_y)} = \sqrt{2\big(\cos^2 \frac{\theta_y A}{2} + \sin^2 \frac{\theta_y A}{2}\big) - 2\cos^2 \frac{\theta_y A}{2} + 2\sin^2 \frac{\theta_y A}{2}} \\
&= 2\sin \frac{|\theta_y A|}{2} \geq \frac{2A|\theta_y|}{\pi} \quad (\sin x \geq x \text{ in the interval } [0, \pi]) \\
\Rightarrow \sin \frac{A|\theta_y|}{2} &\geq \frac{A|\theta_y|}{\pi}
\end{aligned}$$

and for the denominator we can use

$$\left| \mathrm{e}^{\theta_y \mathrm{i}} - 1 \right| \leq |\theta_y|$$

as the arc is always longer than the cord! The overall result is

$$p(y) \geq \frac{1}{AN} \frac{4A^2|\theta_y|^2}{\pi^2|\theta_y|^2} = \frac{4A}{N\pi^2} \overset{A\approx\frac{N}{r}}{\approx} \frac{4}{\pi^2 r}.$$

For those arguments $A|\theta_y| \in [0, \pi]$:

$$\begin{aligned}
-\pi \leq 2\pi \frac{ryA(r)}{N} &\leq \pi \\
-\frac{\pi}{2} \leq ry(N) &\leq \frac{r}{2} \\
Nk - \frac{r}{2} \leq ry &\leq Nk + \frac{r}{2} \\
k = 0 \to y = 0, &k = 1 \to y = \ldots
\end{aligned}$$

There are only a finite number of good y for which

$$p(y = \text{¨good¨}) = \frac{4}{\pi^2} \approx 0.406\ldots$$

These are good because

$$\begin{aligned}
Nk - \frac{r}{2} \leq yr &\leq Nk + \frac{r}{2} \\
\frac{k}{r} - \frac{1}{2N} \leq \frac{<}{N} &\leq \frac{k}{r} + \frac{1}{2N}
\end{aligned}$$

and close to $\frac{y}{N}$ there is a number $\frac{k}{r}$ which is closer to it than $\frac{1}{2N}$ and $|\frac{y}{r} - \frac{k}{r}| \leq \frac{1}{2N}$. $\frac{y}{r}$ we have measured already and, because of

$$\begin{aligned}
r < \sqrt{N}, r_1 : r_1 < \sqrt{N}, r_2 : r_2 < \sqrt{N} \\
\left| \frac{a}{r_1} - \frac{b}{r_2} \right| = \frac{|ar_2 - br_1|}{r_1 r_2} \overset{r_1 \neq r_2, a,b \in \mathbb{N}}{\geq} \frac{1}{r_1 r_2} \geq \frac{1}{N}
\end{aligned}$$

we have the neighbourhood $\frac{1}{N}$ from which we can get $\frac{k}{r}$ or one of its denominators (with high probability).

example

$n = 10 \quad N = 2^10 = 1024, \sqrt{N} = 32$

$y = 139$ (from measurement)

$\dfrac{139}{1024} = \dfrac{1}{1024/139} = \dfrac{1}{7 + 51/139} \rightarrow$ first guess is 7

if not close enough: $\dfrac{1}{7 + 51/139} = \dfrac{1}{7 + \frac{1}{139/51}} = \dfrac{1}{7 + \frac{1}{2+37/51}}$

next estimation is $\dfrac{1}{7 + 1/2} = \dfrac{2}{7}$

next estimation is $\dfrac{1}{7 + \frac{1}{2+\frac{1}{51/37}}} = \dfrac{1}{7 + \frac{1}{2+\frac{1}{1+14/37}}} \approx \dfrac{1}{7 + 1/3} \approx \dfrac{3}{22}$

next estimation: . . . $\dfrac{8}{59}$ which does not fulfill the condition for the denominator to be $< \sqrt{N}$

number must be in the interval $\left[\dfrac{y}{N} - \dfrac{r}{N}, \dfrac{y}{N} + \dfrac{r}{N}\right]$

11.4 Exercises

1. The public key for the RSA algorithm is (e,N)=(53,299). The message m was encrypted by this public key: encode(m)=171. Decrypt the message m and write it down as decimal number.

2. $N = pq = 11409407$ and $f(x) = 19^x \bmod N$. We found the period of $f : r = 475090$. Also we computed $19^{r/2} = 7533861$. Find p and q and write any of them as an answer.

3. The value $\mathrm{e}^{\frac{2\pi \mathrm{i}}{n}k}$, $(0 \leq k < n)$ is a root of unity of power n with number k. What is the sum of all roots of unity of power 2019?

4. x is a 4-bit number: $x_3x_2x_1x_0$. Function $f(x) = 7^x \bmod 15$ maps 4 bits to 4 bits.

   ○ $f(x) = 7^{x_0} \cdot 7^{2x_1} \cdot 7^{4x_2} \cdot 7^{8x_3} \bmod 15$

   ○ $f(x) = 7^{x_0} \cdot 7^{2x_1} \cdot 7^{3x_2} \bmod 15$

   ○ $f(x) = 7^{x_0} \cdot 7^{2x_1} \bmod 15$

   ○ $f(x) = 7^{x_0} \cdot 7^{x_0} \cdot 4^{x_1} \bmod 15$

5. We have ran the Shor's algorithm ($n = 8$, $N = 2^8 = 256$) and measure the value $y = 165$. Suppose we are lucky and on the interval $\left[\frac{165}{256} - \frac{1}{512}, \frac{165}{256} + \frac{1}{512}\right]$ there is a rational number $\frac{k}{r}$ with denominator $r < \sqrt{N} = 16$. Find this rational number and write down its denominator. If there is no such number, write 0.

Chapter 12

Grover's algorithm

General questions

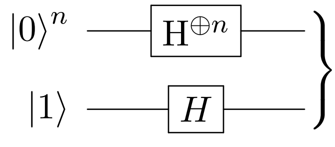
- Are quantum computers always better?
- Can we effectively solve any problem from NP? → Yes! Grover proved it (unsorted database search). The solution of a problem can be checked easily, but not found easily. Any problem that can be solved by brute force, reduces to the unsorted database problem. If one has an oracle function $f(a) = b$ where a is the name path and b the number length (phone book, travelling salesman) the **Grover algorithm** helps to solve the problem faster with a quantum computer than with a classical computer.

The algorithm

For the function $f : \{0,1\}^n \to \{0,1\}^n$ there exists one ω for which $f(\omega) = a$, and as a result, there is a function $f_\omega(x) = \delta_{x=\omega}, \{0,1\}^n \to \{0,1\},\ f_\omega(x \neq \omega) = 0$ and $f_\omega(\omega) = 1$. The oracle function $\mathrm{U_f}$ for the quantum algorithm is

$$\begin{aligned}
\mathrm{U_f} \left|x\right\rangle \left|y\right\rangle &= \left|x\right\rangle \left|y \oplus f_\omega(x)\right\rangle \\
\mathrm{U_f} \frac{1}{\sqrt{2}} \left|x\right\rangle (\left|0\right\rangle - \left|1\right\rangle) &= \frac{1}{\sqrt{2}} \left|x\right\rangle (\left|0 \oplus f_\omega(x)\right\rangle - \left|1 \oplus f_\omega(x)\right\rangle) = \frac{1}{\sqrt{2}} (-1)^{f_\omega(x)} \left|x\right\rangle \big(\left|0\right\rangle - \left|1\right\rangle \big) \\
\mathrm{U}_\omega \left|x\right\rangle = (-1)^{f_\omega(x)} \left|x\right\rangle &= \begin{cases} \left|x\right\rangle & \forall \left|x\right\rangle \neq \left|\omega\right\rangle \\ -\left|\omega\right\rangle & \forall \left|x\right\rangle = \left|\omega\right\rangle \end{cases} \\
\mathrm{U}_\omega &= \mathrm{I} - 2 \left|\omega\right\rangle \left\langle\omega\right|
\end{aligned}$$

The initial state



$$\frac{1}{2^{(n+1)/2}} \sum_{x=0}^{2^n-1} \left|x\right\rangle \big(\left|0\right\rangle - \left|1\right\rangle \big)$$

$$\begin{aligned}
\left|s\right\rangle &= H \left|0\right\rangle^n = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} \left|x\right\rangle \\
\mathrm{U_s} &= 2 \left|s\right\rangle \left\langle s\right| - \mathrm{I}
\end{aligned}$$

The iteration

Grover's algorithm iterates the state multiple times with the operation $\mathrm{R_{Grover}} = \mathrm{U_s U_\omega} \rightarrow {\mathrm{R_{Grover}}}^k |s\rangle$. The projection of the state $|s\rangle$ onto the state $|\omega\rangle$ that we are looking for is $1/\sqrt{N} = \sin\theta$. Because the angle is very small $\sin\theta = \theta$. U_ω reflects the state $|s\rangle$ on the orthogonal hyperplane, i.e. $\theta \rightarrow -\theta$. $\mathrm{U_s}$ reflects the resulting state on the vector $|s\rangle$, i.e. $-\theta \rightarrow 3\theta$. $\mathrm{R_{Grover}}$ rotates the state $|s\rangle$ towards the state $|\omega\rangle$ by an angle θ. After the second iteration, the angle is $\theta + 4\theta = 5\theta$ (reflection on hyperplane is 3θ and reflection on $|s\rangle$ is θ). Every iteration increases the angle by 2θ. We can count the iterations T that are necessary to reach $|\omega\rangle$

$$\theta + 2\theta T = \frac{\pi}{2} \rightarrow \theta \simeq \frac{1}{\sqrt{N}}$$

$$\frac{1}{\sqrt{N}}(1+2T) = \frac{\pi}{2} \rightarrow T \simeq \frac{\pi\sqrt{N}}{4} = \frac{\pi\sqrt{2^n}}{4}$$

Instead of $\mathcal{O}(N)$ necessary iterations as in the classical case, the quantum algorithm only has a complexity of $\mathcal{O}(\sqrt{N})$.

A closer look

Why did we choose the state $|s\rangle$? It is the only vector we know the angle to our unknown state to (it has equal angle to all the basis vectors)!
What if we have more than one special point?

$$\begin{array}{l} \omega_1, \omega_2, \ldots, \omega_k \\ f_\omega(\omega_i) = 1 \end{array} \rightarrow \text{angle is } \frac{\sqrt{k}}{\sqrt{2^n}}$$

$$T \approx \frac{\pi}{4\theta} \simeq \frac{\pi\sqrt{N}}{4\sqrt{K}}$$

To employ Grover's algorithm, we need to know the number of states in order to choose the right amount of operations!
Why did we choose the operator $\mathrm{U_s}$? It is the only vector we know the result of the reflection of. Therefore, one can only obtain an exponential speed-up with a von Neumann architecture by using intermediate system states (half, quarter, eighth, etc. of the way) as reflective lines. There is no prove that such an architecture can be realised by a quantum computer, though.

12.1 Proof of the optimality of Grover's algorithm

Be $|omega\rangle$ the special vector one looks for and $\mathrm{U}(\omega, t) = \mathrm{U}_t \mathrm{U}_\omega \mathrm{U}_{t-1} \mathrm{U}_\omega \ldots \mathrm{U}_1 \mathrm{U}_\omega$ the operator we assume performs better than Grover. $|\Psi_0\rangle$ is the initial state and $|\Psi_t\rangle = \mathrm{U}(\omega, t)|\Psi_0\rangle$ the state after t operations. T then is defined by $\mathrm{U}(\omega, T)|\Psi_0\rangle = |\Psi_T\rangle \approx |\omega\rangle$ and $|\Psi_\omega\rangle = |\Psi_T\rangle$. The dimension of the state space is 2^n. The idea is to find a state $|\Phi\rangle$ that fulfils the inequality

$$\underbrace{4T^2}_{\substack{\text{number of iterations} \\ \text{of the most} \\ \text{effective algorithm}}} \geq \sum_{\omega=0}^{N-1} \| |\Psi_\omega\rangle - |\Phi\rangle \|^2 \geq \underbrace{2N - 2\sqrt{N}}_{\substack{\text{number of queries} \\ \text{to the oracle}}}$$

as the middle does not depend on the state $|\Phi\rangle$, only the right-most expression should be compared (the inequality holds for both sides)

$$4T^2 \geq 2N - 2\sqrt{N} \Rightarrow T \approx \sqrt{\frac{N}{2}}, T_{\mathrm{Grover}} \approx \frac{\pi}{4}\sqrt{N}.$$

The right side is

$$\begin{aligned}
&\langle \Psi_{\omega_i} | \Big| \Psi_{\omega_j} \Big\rangle =: \Delta_{i,j}, \quad |\Delta_{i,j}| \approx 0 \\
&\sum_{\omega=0}^{N-1} \| |\Psi_\omega\rangle - |\Phi\rangle \|^2 = \sum_\omega \|\psi_\omega\|^2 + \sum_\omega \|\phi\|^2 - \sum_\omega \langle \Psi_\omega | \Phi \rangle - \sum_\omega \langle \Phi | \Psi_\omega \rangle \\
&\Rightarrow |\Phi\rangle = (x_1, x_2, \dots, x_N) \forall j \in [1, N],\, x_j = a_j + \mathrm{i} b_j \\
&\sum_{\omega=0}^{N-1} \| |\Psi_\omega\rangle - |\Phi\rangle \|^2 = 2N - \sum_{j=1}^{N} (x_j + x - j^*) = 2N - 2\sum_{j=1}^{N} a_j.
\end{aligned}$$

We can use the following Lemma to simplify the calculations:

$$\left(\sum_{j=1}^{K} c_j \right)^2 \leq K \sum_{j=1}^{K} c_j^2$$

$$\begin{aligned}
\left(\sum_{j=1}^{K} c_j \right)^2 + \frac{1}{2} \sum_{i,j}^{K} \left(c_i - c - j \right)^2 &= \sum_{i,j=1}^{K} c_i c_j + \frac{1}{2} \sum_{i,j=1}^{K} c_i^2 + c_j^2 - 2 c_i c_j \\
&= \sum_{i,j=1}^{K} c_i c_j + \frac{K}{2} \sum_{i=1}^{K} c_i^2 + \frac{K}{2} \sum_{j=1}^{K} c_j^2 - \sum_{i,j=1}^{K} c_i c_j \\
&\overset{\text{change of summation variable}}{=} K \sum_{j=1}^{K} c_j^2 \text{ which proves the lemma.}
\end{aligned}$$

With this at hand:

$$\begin{aligned}
&\langle \phi | \phi \rangle = \sum_{j=0}^{N-1} x_j x_j^* = \sum_j \left(a_j^2 + b_j^2 \right) = 1 \\
&\Rightarrow N \sum_{j=0}^{N-1} a_j^2 \leq N \Rightarrow \left(\sum_j a_j \right)^2 \leq N \sum_{j=0}^{N-1} a_j^2 \leq N \\
&\Rightarrow \sum_{j=0}^{N-1} a_j \leq \sqrt{N} \Rightarrow \sum_{\omega=0}^{N-1} \| |\Psi_\omega\rangle - |\Phi\rangle \|^2 \leq 2N - 2\sqrt{N}.
\end{aligned}$$

For the left side we find:

$$\begin{aligned}
\mathrm{U}(\omega, t) &= \mathrm{U}_t \underbrace{\mathrm{U}_\omega}_{=\mathrm{I}} \mathrm{U}_{t-1} \underbrace{\mathrm{U}_\omega}_{=\mathrm{I}} \dots \mathrm{U}_1 \underbrace{\mathrm{U}_\omega}_{=\mathrm{I}} \\
|\phi_t\rangle &= \mathrm{U}_t \mathrm{U}_{t-1} \dots \mathrm{U}_1 |\Psi_0\rangle
\end{aligned}$$

Calculating the error E corresponding to the deviation from the optimal path in each step due to replacing U_ω by I:

$$\begin{aligned}
E(\omega, t) &:= \| (\mathrm{U}_\omega - 1) |\Psi_t\rangle \| = \| \Big(\mathrm{I} - 2 |\omega\rangle \langle \omega| - \mathrm{I} \Big) |\Psi_t\rangle \\
&= 2 \| \langle \omega | \phi_t \rangle \|
\end{aligned}$$

The deviation of the correct, optimal state vector to the erroneous one

$$\begin{aligned}
F(t) &:= \| |\Psi_t\rangle - |\phi_t\rangle \| = \| \underbrace{\mathrm{U}_t}_{\substack{\text{unitary can be}\\ \text{removed from}\\ \text{the norm}}} \mathrm{U}_\omega |\Psi_{t-1}\rangle - \underbrace{\mathrm{U}_t}_{\substack{\text{unitary can be}\\ \text{removed from}\\ \text{the norm}}} |\phi_{t-1}\rangle \| \\
&= \| \underbrace{\mathrm{U}_\omega |\Psi_{t-1}\rangle - |\Psi_{t-1}\rangle}_{E(\omega, t-1)} + \underbrace{|\Psi_{t-1}\rangle - |\phi_{t-1}\rangle}_{F(t-1)} \|
\end{aligned}$$

Using the triangle inequality:

$$\begin{aligned}
&F(t) \leq F(t-1) + E(\omega, t-1)\\
\Rightarrow &F(T) = \||\Psi_\omega\rangle - |\phi_T\rangle\|^2 \leq \left(2\sum_{t=1}^{T} |\langle\omega|\Psi_{t-1}\rangle|\right)^2\\
\Rightarrow &\||\Psi_\omega\rangle - |\phi_T\rangle\|^2 \leq 4\left(\sum_{t=1}^{T} |\langle\omega|\Psi_{t-1}\rangle|\right)^2
\end{aligned}$$

From the Lemma:

$$\begin{aligned}
\||\Psi_\omega\rangle - |\Phi_T\rangle\|^2 &\leq 4\left(\sum_{t=1}^{T} |\langle\omega|\Psi_{t-1}\rangle|\right)^2 \leq 4T\sum_{t=1}^{T} |\langle\omega|\Psi_{t-1}\rangle|^2\\
\sum_{\omega=0}^{N-1} \||\Psi_\omega\rangle - |\Phi_T\rangle\|^2 &\leq 4T\sum_{\omega=0}^{N-1}\sum_{t=1}^{T} |\langle\omega|\Psi_{t-1}\rangle|^2 = 4T\sum_{t=1}^{T}\sum_{\omega=0}^{N-1} |\langle\omega|\Psi_{t-1}\rangle|^2 = \underline{\underline{4T^2}}
\end{aligned}$$

This proves the inequality and with it that the optimal algorithm is not much better than Grover's algorithm.

Are quantum computers always better?

Consider a function

$$\begin{aligned}
f(x) : \{0,1\}^n &\rightarrow \{0,1\}\\
x(f) &= x_{N-1}x_{N-2}\ldots x_0 \quad N = 2^n \forall j x_j = f(j)\ j \in [0, N-1]\\
\mathrm{U_f}\,|x\rangle\,|y\rangle &= |x\rangle\,|y \oplus f(x)\rangle\\
\mathrm{U_f}\,|j\rangle\,|y\rangle &= x_j\,|x\rangle\,|y \oplus 1\rangle + (1-x_j)\,|j\rangle\,|y\rangle\\
\tilde{x} &= 1 - 2x_i\\
\mathrm{Parity}(\tilde{x}) &= \prod_{i=0}^{N-1} \tilde{x}_i = \begin{cases} 1 & , \text{ even number of 1's}\\ -1 & , \text{ otherwise}\end{cases}
\end{aligned}$$

How much would it cost to compute the parity of $f(x)$? Classically, it is $\mathcal{O}(N)$. On a quantum computer $(T < N/2)$

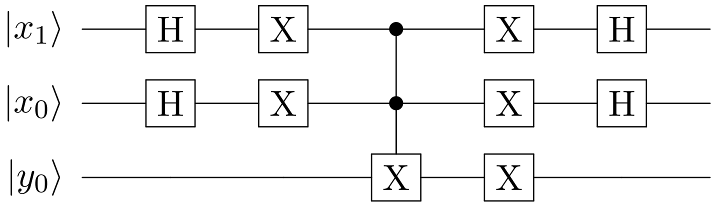
$$\mathrm{U_f^T}\,|x\rangle\,|y\rangle = \underbrace{\mathrm{Parity}^T(\tilde{x})}_{\text{polynom of degree T}} \overset{\text{after measurement}}{=} \mathrm{Parity}^{2T}_{\text{even}}(\tilde{x})$$

$$\begin{aligned}
\sum_{\tilde{x}} \mathrm{Parity}^{2T}_{\text{even}}(\tilde{x}) \prod_{i=0}^{N-1} \tilde{x}_i &= \sum_{\tilde{x}:\tilde{x}_i=1} \mathrm{Parity} \prod_{i\neq j}^{N-1} \tilde{x}_i - \sum_{\tilde{x}:\tilde{x}_j=-1} \mathrm{Parity}_{\text{even}} \prod_{i\neq j} \tilde{x}_j = 0\\
\sum_{\tilde{x}} \mathrm{Parity}^{2T}_{\text{even}}(\tilde{x}) \prod_{i=0}^{N-1} \tilde{x}_i &= \sum_{\tilde{x}:\tilde{x}_{\text{even}}} \mathrm{Parity}^{2T}_{\text{even}} - \sum_{\tilde{x}:\tilde{x}_{\text{odd}}} \mathrm{Parity}_{\text{even}}\\
\Rightarrow \sum_{\tilde{x}:\tilde{x}_{\text{even}}} \mathrm{Parity}^{2T}_{\text{even}} &= \sum_{\tilde{x}:\tilde{x}_{\text{odd}}} \mathrm{Parity}^{2T}_{\text{even}}
\end{aligned}$$

We can not say anything about whether the function is even or odd after $2T < N$ iterations. The quantum computer can not be twice better than the classical computer.

12.2 Exercises

1. The U_f operator for a 3-qubit state is implemented by this circuit scheme. The value qubit $|y_0\rangle = \mathrm{H}\,|1\rangle$. Check all the correct statements:



   - ○ The gates H and X applied to $|x_0\rangle$ and $|x_1\rangle$ on the first 2 steps rotate the space so that the vector $|s\rangle$ is mapped to $|11\rangle$.
   - ○ The gates H and X applied to $|x_0\rangle$ and $|x_1\rangle$ on the first 2 steps rotate the space so that the vector $|s\rangle$ is mapped to $|00\rangle$.
   - ○ The CNOT gate acts only on the vector $|11y_0\rangle$, other vectors are untouched by it. So in our rotated space, it acts on the image of vector $|s\rangle$.
   - ○ The CNOT gate multiplies the vector $|11y_0\rangle$ by -1.
   - ○ The gates H and X applied to $|x_0\rangle$ and $|x_1\rangle$ after CNOT rotate the space back so that the vector $|11\rangle$ is mapped back to $|s\rangle$.
   - ○ The gate X on the qubit $|y_0\rangle$ multiplies the system by -1. Thus it returns back the vector $|11y_0\rangle$ and multiplies by -1 all other basis vectors. Among with CNOT it implements the reflection of the state over $|11y_0\rangle$.

2. Is the functional $f(|x\rangle) = \langle x|x\rangle$ differentiable in the linear space over the field of complex numbers?

   - ○ Yes, the Cauchy-Riemann conditions are met
   - ○ No, the Cauchy-Riemann conditions are not met

3. We are going to solve the travelling salesman problem on the graph with 10 vertices with Grover's algorithm. How many Grover iterations are we going to need?

   - ○ $\lfloor 2^{\frac{\lceil \log_{10} \rceil}{2}-2}\pi \rfloor = 1608$
   - ○ $\lfloor \frac{\sqrt{10}\pi}{4} \rfloor = 1496$
   - ○ $\lfloor \frac{10!\pi}{4} \rfloor = 2850052$

4. A small leak from the oracle's function black box allows us to modify the initial state $|s\rangle = \frac{1}{\sqrt{N+2}} \sum\limits_{x \neq \omega} |x\rangle + \sqrt{\frac{3}{N+2}}\,|\omega\rangle$ and the operator U_f for the Grover's algorithm. For big enough N this will allow us

   - ○ to reduce the number over Grover's iterations 3 times
   - ○ to reduce the number over Grover's iterations $\sqrt{3}$ times
   - ○ to reduce the number over Grover's iterations 9 times
   - ○ nothing. It does not alter the number of iterations.

5. In the following list check all the functions, for which the function ¨Parity¨, introduced in the last lecture, gives 1 (all ¨even¨ functions). All functions in the list map n bit to 1 bit, $n > 1$.

   ○ Function f, which returns the least significant bit of its arguments

   ○ Function f, which returns the bit with number j of its arguments

   ○ the constant function $f(x) = 1$

   ○ the constant function $f(x) = 0$

   ○ an indicator (characteristic) function of the set $S = \{2, 4, 6, 8, 10\}$

Part IV

One-way quantum computation

Chapter 13

Quantum Computation - a motivation

13.1 Quantum complexity and quantum computing schemes

Tasks are distinguished according to their computational complexity:

- **class P (polynomial**
  - integer addition
  - multiplication, division
  - matrix multiplication
- **class NP (non-deterministic polynomial)**
  - factorisation of numbers
  - travelling salesman problem
- **class EXP (exponential)**
  - the problem of modelling quantum systems
- **class BQP (bounded error quantum polynomial time)**
  - finding prime divisors of numbers (Shor's algorithm)
  - finding a solution to equations (Grover's algorithm)
  - simulation of quantum mechanical systems and others

Even the most powerful classical computer is not able to solve some problems from the BQP class, e.g. a quantum system of 500 two level atoms can be in 2^{500} states, a number that is greater than the number of atoms in the universe, i.e. in a classical computer such a state can not even be saved.

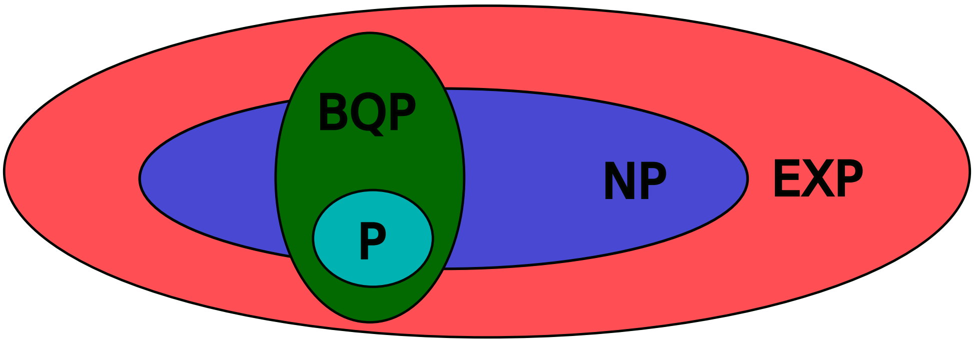


Figure 13.1: The complexity classes described in the text and the Venn-diagrammatic relationship

Quantum computers have the advantage over classical computers that they can store a continuum in a single qubit instead of only one value

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle , \, \alpha, \beta \in \mathbb{C}.$$

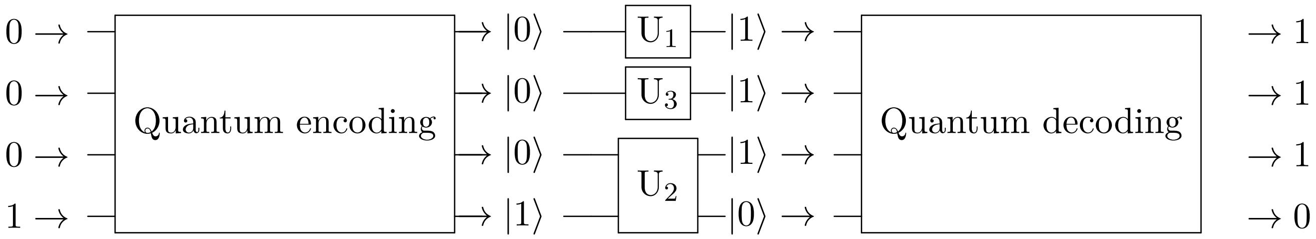
The state can, however, not be read out by a single measurement, but it can be represented by on the Bloch sphere (see Figure 4.1)

$$|\Psi\rangle = \cos\frac{\theta}{2} |0\rangle + \mathrm{e}^{\mathrm{i}\phi} \sin\frac{\theta}{2}.$$

A generalisation of the concept to many (entangled) qubits is missing unfortunately.
The presence of superposition properties in the quantum world are referred to as **quantum parallelism**. These make a quantum computer a powerful device. While a classical computer always operators with one state of n bits, a quantum computer can operate immediately with 2^n states of n qubits. This allows quantum computers to solve some tasks much faster. Here are some practical examples how qubits can be implemented:

- electron spin projection
- direction of nuclear spin in a magnetic field
- two states of an electron in a single atom
- two linear (or circular) polarisations of photons

The scheme of **universal quantum computation** is the following



Here, the gates $\mathrm{U_i}$ realise the quantum computations. Any transformation over qubits can be represented as a product of elementary logical transformations (gates). The Pauli matrices together with the identity operation form a basis to construct **any one-qubit operation**. An arbitrary hermitian matrix is

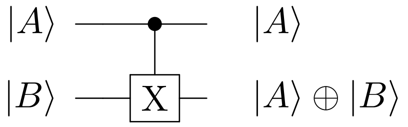
$$A = a_x X + a_y Y + a_z Z \text{ where (we assume) } \sqrt{a_x^2 + a_y^2 + a_z^2} = 1$$

and an arbitrary one-qubit unitary operator can be written as

$$U(\theta, \boldsymbol{a}) = \mathrm{e}^{\mathrm{i}\frac{1}{2}A} = \mathrm{e}^{\mathrm{i}\frac{\theta}{2}\boldsymbol{\sigma}\cdot\boldsymbol{a}}$$
$$\rightarrow U(\theta, \boldsymbol{a}) = \cos\frac{\theta}{2}\mathrm{I} - \mathrm{i}\boldsymbol{a}\cdot\boldsymbol{\sigma}\sin\frac{\theta}{2}$$

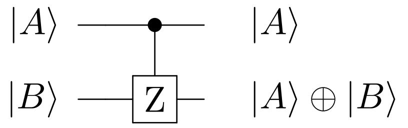
which follows from using the properties of the Pauli matrices in the series expansion of the exponential $A^{2n} = \mathrm{I}, A^{2n+1} = A$. Only three rotations around the basis axis of the coordinate system are needed to transform a state into another arbitrary state rotation around the axis $\boldsymbol{a}$ by above transformation.
For two (or more)-qubit transformations one needs to remember that the elements should be described by unitary transformations. An analogue, e.g. of the XOR function/operator or any

operator that looses information in the process, can not be implemented since it is not unitary[1]. The CNOT gate has the same output in the last qubit as XOR



$$\begin{aligned}
|00\rangle &\rightarrow |00\rangle \\
|01\rangle &\rightarrow |01\rangle \\
|10\rangle &\rightarrow |11\rangle \\
|11\rangle &\rightarrow |10\rangle \\
|A\rangle\,|B\rangle &\rightarrow |A\rangle\,|A \oplus B\rangle \\
\Rightarrow\ \mathrm{CNOT} &= |0\rangle\,\langle 0|\,\mathrm{I} + |1\rangle\,\langle 1| \otimes \mathrm{X}
\end{aligned}$$

There are also gates that change the phase of a qubit in the superposition, e.g. cPhase



$$\begin{aligned}
|00\rangle &\rightarrow |00\rangle \\
|01\rangle &\rightarrow |01\rangle \\
|10\rangle &\rightarrow |10\rangle \\
|11\rangle &\rightarrow -\,|11\rangle \\
|A\rangle\,|B\rangle &\rightarrow (-1)^{AB}\,|A\rangle\,|B\rangle \\
\Rightarrow\ \mathrm{cPhase} &= |0\rangle\,\langle 0|\,\mathrm{I} + |1\rangle\,\langle 1| \otimes \mathrm{Z}
\end{aligned}$$

Any many-qubit operator can be expressed by CNOT, cPhase, and the set of all single-qubit gates.

There are different models to describe the evolution of the quantum system:

- In the **circuit model**, devices are performing elementary unitary transformations to realise operations on input states. The **decoherence process** interferes with the full implementation of this mode. In practise, this is hard to realise. Hence, alternative models were looked for that are harder conceptually, but easier to implement in reality/practise.
- The **adiabatic computational model** follows these steps:
  1. determine the Hamiltonian H, the ground state of which encodes the solution to the problem
  2. determine the initial Hamiltonian H_0, the ground state of which is easy to create experimentally
  3. select $\tilde{H}(s)$ to interpolate from H_0 to H for $0 \leq s \leq 1$:
  $$\tilde{H}(s) = (1-s)H_0 + sH$$
  4. The time of the adiabatic evolution is
  $$T = \mathcal{O}\left(\frac{1}{\Delta^2}\right) \text{ where } \Delta = \min_{s\in[0,1]} \left|E_1(s) - E_0(s)\right|$$
- The **topological computation model** is more robust against computational errors by using topological states of a system (proposed by A. Y. Kitaev). The idea behind topological quantum computation is to implement computations in the topological computation model which uses quasiparticles called anyons living in 2d systems (or low-dimensional systems) for which
$$\begin{aligned}
\text{Fermions:}\Psi(r_1, r_2) &= -\Psi(r_2, r_1) \\
\text{Bosons:}\Psi(r_1, r_2) &= \Psi(r_2, r_1) \\
\text{Anyons:}\Psi(r_1, r_2) &= \mathrm{e}^{\mathrm{i}\phi}\Psi(r_2, r_1)
\end{aligned}$$

[1] With the output value we will not be able to say in which state the system was initially.

During the computation the topology of the system will be preserved if no error occurs, Hence, errors can be detected. The necessary steps of the topological quantum computations are:

1. Anyons (threads) are prepared in the initial state
2. They begin to change places with each other (weave)

As a result of such interlacing, topologically distinguishable quantum states of the system are obtained. If we use anyons with $\phi = \pi/4$, then $2n$ such particles have 2^{n-1} topologically distinguishable states.

13.2 Quantum teleportation

Quantum teleportation allows us to transmit a state that is in one place (Alice) to an object in another place (Bob).

$$\begin{array}{cc} |\Psi\rangle & \rightarrow |\Psi\rangle \\ \text{Alice} & \text{Bob} \end{array}$$

To implement such a teleportation, it is necessary to have two additional systems in an **entangled state**. Quantum systems A and B are entangled if their density matrix ϱ is not factorised by the direct product of the density matrices of these subsystems

$$\varrho \neq \sum_i \lambda_i \varrho_{i,A} \otimes \varrho_{i,B}$$

where λ_i is the probability of the system being in the state $\varrho_{i,A} \otimes \varrho_{i,B}$. For quantum teleportation of the state of one qubit $|\Psi\rangle$, two additional qubits are required which are in one of the four Bell states:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,),\ |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle\,),\ |\beta_{10}\rangle = \frac{1}{\sqrt{2}}(\,|10\rangle - |01\rangle\,)$$

For the teleportation state $|\Psi\rangle$, Alice and Bob each hold one qubit from the entangled pair $|\beta_{00}\rangle$. The wave function of all three qubits can be written as

$$|\Phi\rangle_{123} = |\Psi\rangle_1 \otimes |\beta_{00}\rangle_{23} = \frac{1}{\sqrt{2}}\,|\Psi\rangle_1 \otimes (\,|0\rangle_2\,|0\rangle_3 + |1\rangle_2\,|1\rangle_3\,)$$

In the next step, Alice brings her qubits into interaction with a Bell state's measuring device. By decomposing the state above, we see what possible states Bob has as a result of this:

$$|\Phi\rangle_{123} = \frac{1}{2}[\,|\beta_{00}\rangle_{12} \otimes |\Psi\rangle_3 + |\beta_{10}\rangle_{12} \otimes (\mathrm{Z}\,|\Psi\rangle_3) + |\beta_{01}\rangle_{12} \otimes (\mathrm{X}\,|\Psi\rangle_3) + |\beta_{11}\rangle_{12} \otimes (\mathrm{XZ}\,|\Psi\rangle_3)]$$

Given the results (information of the measurement of Alice), Bob can choose a transformation that completes the teleportation of the unknown quantum state $|\Psi\rangle$.

13.3 Quantum gate teleportation

By modifying the teleportation protocol, quantum computing can be implemented. To do this, instead of the $|\beta_{00}\rangle$ state, the modified state $\mathrm{U}\,|\beta_{00}\rangle$ is used.

$$\begin{array}{cc} |\Psi\rangle & \to \mathrm{U}\,|\Psi\rangle \\ \text{Alice} & \text{Bob} \end{array}$$

If one carries out all the stages of quantum teleportation with this state, then as a result Bob will have a transformed state $U\,|\Psi\rangle$. Practically, it is hard to implement as it necessitates the arbitrary preparation of unitary transformed Bell states.

13.4 Exercises

1. What tasks can a quantum computer solve?

   ○ all tasks from the NP class
   ○ all tasks from the EXP class
   ○ all tasks from the BQP class
   ○ all tasks from the P class

2. What class does the factorisation problem belong to?

   ○ to the class NP
   ○ to the class EXP
   ○ to the class P

3. Choose the correct characteristics for a qubit:

   ○ a qubit can be in a superposition state
   ○ a qubit is a quantum system with two basis states
   ○ a qubit is a classical system with two basis states
   ○ a qubit is a quantum system with n basis states

4. How many states can m qubits be in simultaneously?

   ○ 2^n
   ○ 2^m
   ○ m
   ○ $m + 2$

5. Choose the correct form of the universal one-qubit unitary transformation operator, taking into account that X, Y, Z are Pauli operators:

   ○ $\mathrm{U}(\theta, \boldsymbol{a}) = \cos\frac{\theta}{2}\mathrm{I} - \mathrm{i}(a_x\mathrm{X} + a_y\mathrm{Y} + a_z\mathrm{Z})\sin\frac{\theta}{2}$
   ○ $\mathrm{U}(\boldsymbol{a}) = a_x\mathrm{X} + a_y\mathrm{Y} + a_z\mathrm{Z}$
   ○ $\mathrm{U} = \mathrm{X} + \mathrm{Y} + \mathrm{Z}$

6. What condition must the operator of all quantum gates satisfy?

   ○ operator must be hermitian
   ○ operator must be unitary

○ operator must be self-adjoint

7. Suppose that we send a control qubit in the state $|0\rangle$ and a target qubit in the state $|1\rangle$ to the input of the CNOT transformation. What state will the target qubit have at the output?

   ○ $|0\rangle$
   ○ $|1\rangle$
   ○ $|0\rangle|0\rangle$
   ○ $|1\rangle|1\rangle$

8. How is the circuit model of quantum computation similar to the model of classical computation?

   ○ The circuit model uses auxiliary devices that implement logic gates
   ○ Quantum computation in the circuit model does not surpass classical computation in power
   ○ To implement computation in the circuit model, the classical operations AND, XOR, and others are used.

9. What is the principle behind adiabatic quantum computation?

   ○ The principle of fast excitation of the ground state of the system
   ○ The of slow evolution of the ground state of the system
   ○ The principle of system evolution through the sequential application of quantum transformations (quantum gates)

10. What is the difference between an anyon and a fermion?

   ○ An anyon is no different from a fermion
   ○ An anyon is a quasiparticle ¨living¨ on a 2D plane
   ○ An anyon has arbitrary statistics
   ○ When two anyons swap places, the phase of their common wave function does not change

11. What auxiliary states are needed to implement quantum teleportation?

   ○ a specific one-qubit state
   ○ two-qubit states whose density matrices can be factorised in the form $\hat{\varrho}_1 \otimes \hat{\varrho}_2$
   ○ squeezed states

12. Choose the Bell state $|\beta_0\rangle$:

   ○ $\frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$
   ○ $\frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$
   ○ $\frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle\,)$
   ○ $\frac{1}{\sqrt{2}}(\,|01\rangle - |10\rangle\,)$

13. What is the final step of the quantum teleportation protocol?

   ○ Creation of the entangled state
   ○ Alice measuring her qubits
   ○ Bob's correction of his qubit

14. How can the quantum teleportation protocol be modified to be used for quantum computation?

    ○ Use transformed Bell states $\mathrm{U}\,|\beta\rangle$

    ○ Use other entangled states instead of Bell states

    ○ Use other multiparticle entangled states instead of Bell states, which will be measured locally in different basis states

    ○ One cannot change the quantum teleportation protocol so that it can be used to implement quantum computation

Chapter 14

Measurement-based quantum computation

To implement the scheme described at the end of the last chapter, an entangled state is used that does not need to be transformed all the time. Computations are realised due to local measurements of the multipartite-entangled state by devices. The basis states of these can be chosen arbitrarily. The states Bob receives in this method have the form $U|\Psi\rangle$, where the U transformation is completely set by the choice of bases of Alice's measuring devices, i.e. the measurement devices determine the computation carried out on the state. **The computations can not be reversed and are, therefore, called *one-way*.**

14.1 Cluster states in discrete variables

Definition

An **undirected mathematical graph** is a pair $\mathcal{G} = (V, E)$, where $V = \{1, \ldots, n\}$ is a finite set of vertices, and the edges $E \subseteq V \times V$ are a set of pairs of vertices that are connected to each other. For example $V = \{1, 2, 3\}$, $E = \{(1, 2), (2, 3)\}$ describes a graph where the middle vertex ¨2¨ is connected to the two vertices ¨1¨ and ¨3¨. In quantum computing **vertices** play the role of **physical systems** and **edges** represent **entanglement**.
The **adjacency matrix** is a square matrix A such that its elements A_{ij} are one when there is an edge from vertex i to vertex j, and zero otherwise $A_{ij} = \begin{cases} 0 & , \quad \text{vertices } i, j \text{ is not connected} \\ 1 & , \quad \text{vertices } i, j \text{ are connected} \end{cases}$.
For the example from before $A_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$
To generate a **cluster state** that satisfies a particular graph $\mathcal{G} = (V, E)$, we use the following algorithm:

- to each node $i \in V$ in the graph $\mathcal{G}$ we associate the qubit in the state $|+\rangle_i$
- next, all pairs of qubits with numbers $i, j) \in E$ are entangled by the operator $\mathrm{cPhase}_{i,j}$

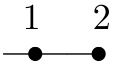
$$\mathrm{cPhase}_{i,j} = |0\rangle_i\, {}_i\langle 0| \otimes \mathrm{I}_j + |1\rangle_i\, {}_i\langle 1| \otimes \mathrm{Z}_j$$

as a result, the cluster state can be written as

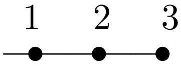
$$|G\rangle = \prod_{(i,j)\in E} \mathrm{cPhase}_{i,j} |+\rangle_i^{\oplus n}$$

Here are two examples:

$$|G\rangle_2 = \mathrm{cPhase}_{1,2}\,|+\rangle_1\,|+\rangle_2 = \frac{1}{2}\mathrm{cPhase}_{1,2}(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,)$$
$$= (\,|00\rangle + |01\rangle + |10\rangle - |11\rangle\,) = \frac{1}{\sqrt{2}}(\,|0\rangle\,|+\rangle + |1\rangle\,|-\rangle\,)$$
$$|G\rangle_3 = \mathrm{cPhase}_{2,3}(\mathrm{cPhase}_{1,2}\,|+\rangle_1\,|+\rangle_2\,|+\rangle_3\,) = \mathrm{cPhase}_{2,3}\,|G\rangle_2\,|+\rangle_3 = \frac{|+\rangle_1\,|0\rangle_2\,|+\rangle_3 + |-\rangle_1\,|1\rangle_2\,|-\rangle_3}{\sqrt{2}}$$



$|G\rangle_2$



$|G\rangle_3$

It is more convenient to define a clustered state is by using **stabilizers**: An operator S is a stabilizer of the quantum state $|\Psi\rangle$ if this state is eigenstate with an eigenvalue equal to 1 ($S\,|\Psi\rangle = |\Psi\rangle$). For example the stabilizer for the state $|0\rangle$ is the Pauli operator Z and the stabilizer of the state $|+\rangle$ is the Pauli operator X.
Let $S_i\,|\Psi\rangle = |\Psi\rangle$ and $S_j\,|\Psi\rangle = |\Psi\rangle$. Then $S_iS_j\,|\Psi\rangle = S_jS_i\,|\Psi\rangle$ and moreover

$$S_j^{-1}\,|\Psi\rangle = S_j^{-1}(S_j\,|\Psi\rangle) = \mathrm{I}\,|\Psi\rangle = \Psi.$$

All stabilizer operators $\{S_i\}_{i=1}^m$ of the state $|\Psi\rangle$ form an **Abelian group** by multiplication. Such a group defines a single quantum state. The evolution of a set of stabilizers $\{S_i\}_{i=1}^m$ of the state $|\Psi\rangle$ under the action of the unitary operator U:

$$\mathrm{U}\,|\Psi\rangle = \mathrm{US}_i\,|\Psi\rangle = \mathrm{US}_i\mathrm{U}^\dagger\mathrm{U}\,|\Psi\rangle = (\mathrm{US}_i\mathrm{U}^\dagger)\mathrm{U}\,|\Psi\rangle\,.$$

The operators $\{\mathrm{US}_i\mathrm{U}^\dagger\}_{i=1}^m$ are stabilizers of the state $\mathrm{U}\,|\Psi\rangle$, e.g. the stabilizer of $|1\rangle = \mathrm{X}\,|0\rangle$ is XZX and the stabilizer of $|-\rangle = \mathrm{Z}\,|+\rangle$ is ZXZ!
To generate cluster states, we need to use qubits in the $|+\rangle_i$ state

$$|\Phi\rangle = |+\rangle_1\,|+\rangle_2\,|+\rangle_3\ldots|+\rangle_n\,.$$

The stabilizers of the state $|\Phi\rangle$ are $\{x_i\}_{i=1}^n$ and the cluster state

$$|G\rangle = \mathrm{U}\,|\Phi\rangle = \prod_{(i,j)\in E}\mathrm{cPhase}_{i,j}\,|\Phi\rangle$$

has stabilizers $\{\mathrm{UX}_i\mathrm{U}^\dagger\}_{i=1}^n$. These evolve the operator X_i by the cPhase operators:

$$\mathrm{cPhase}_{i,j}\mathrm{X}_i\mathrm{cPhase}_{i,j} = \mathrm{X}_i\mathrm{Z}_j,$$
$$\mathrm{cPhase}_{i,k}(\mathrm{X}_i\mathrm{Z}_j)\mathrm{cPhase}_{i,k} = \mathrm{X}_i\mathrm{Z}_j\mathrm{Z}_k.$$

The cluster stabilizers are, therefore,

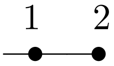
$$\mathrm{UX}_i\mathrm{U}^\dagger = \mathrm{X}_i\prod_{j\in N(i)}\mathrm{Z}_j.$$

Here are two examples:

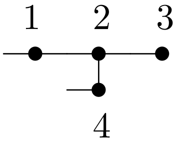
$$S_1 = \mathrm{X}_1\mathrm{Z}_2,\ S_2 = \mathrm{X}_2\mathrm{Z}_1$$

$$S_1 = \mathrm{X}_1\mathrm{Z}_2,\ S_2 = \mathrm{X}_2\mathrm{Z}_1\mathrm{Z}_3\mathrm{Z}_4$$
$$S_3 = \mathrm{X}_3\mathrm{Z}_2,\ S_4 = \mathrm{X}_4\mathrm{Z}_2$$

Two node-cluster state



Four node-cluster state



The cluster state stabilizers are

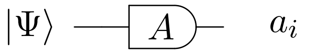
$$S_i = \mathrm{X}_i \prod_{\substack{j \in N(i) \\ E_j}} \mathrm{Z}_j .$$

Let $\alpha_x(i)$ be the result of the measurement X operator on the ith cluster state node, and $\alpha_z(j)$ be the result of the measurement Z operator on the jth cluster state node. After the measurement, $\alpha_x(i)$ and $\alpha_z(j)$ are individually random, but their combination is

$$\alpha_x(i) \prod_{j \in N(i)} \alpha_z(j) = 1$$

Quantum Measurement

When we measure the (hermitian) operator A, we get its eigenvalues $A\,|a_i\rangle = a_i\,|a_i\rangle$.



The wave function of a quantum system is

$$|\Psi\rangle = \sum_m |\Psi_m\rangle_M \, |\Phi_m\rangle_E$$

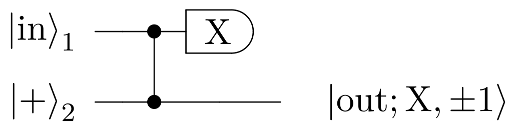
where $|\Psi_m\rangle$ and $|\Phi_m\rangle$ are the eigenstates of the measurement system and the external device, respectively. The probability of a measurement outcome is defined as

$$P_m = {}_E\langle\Phi|\Phi\rangle_E$$

and the reduced wave function after measurements is

$$\left|\Phi_n^{(r)}\right\rangle = \frac{1}{V_E\langle\Phi_n|\Phi_n\rangle} \, |\Phi_n\rangle_E \, .$$

For example



The state after the cPhase$_{1,2}$

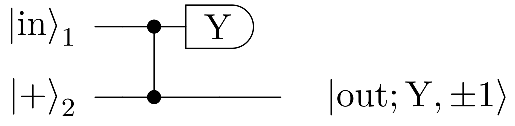
$$\begin{aligned} |\Psi\rangle_{1,2} = \alpha\,|0\rangle_1\,|+\rangle_2 + \beta\,|1\rangle_1\,|-\rangle_2 &= \frac{1}{\sqrt{2}}\,|+\rangle_1\,(\alpha\,|+\rangle_2 + \beta\,|-\rangle_2\,) + \frac{1}{\sqrt{2}}\,|-\rangle_1\,(\alpha\,|+\rangle_2 - \beta\,|-\rangle_2\,) \\ &= \frac{1}{\sqrt{2}}\,|+\rangle\,(\mathrm{H}_2\,|\mathrm{in}\rangle_2\,) + \frac{1}{\sqrt{2}}\,|-\rangle\,(\mathrm{H}_2\mathrm{Z}_2\,|\mathrm{in}\rangle_2\,) \end{aligned}$$

State after the measurement of the Pauli operator X:

$$\begin{aligned} \text{result } +1 :\ |\mathrm{out}; X, +1\rangle &= \sqrt{2}\,{}_1\langle+|\Psi\rangle_{1,2} = \mathrm{H}_2\,|\mathrm{in}\rangle_2\,, \\ \text{result } -1 :\ |\mathrm{out}; X, -1\rangle &= \sqrt{2}\,{}_1\langle-|\Psi\rangle_{1,2} = \mathrm{H}_2\mathrm{Z}_2\,|\mathrm{in}\rangle_2\,. \end{aligned}$$

The first qubit is transported into the second qubit by the measurement accompanied by an additional transformation.

The other two basis measurements in this scheme are:
Y-Basis



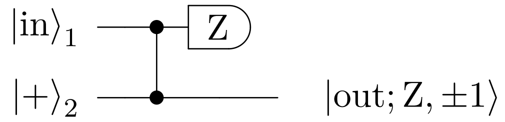
The measurement in the basis of above scheme, yields

$$|y\rangle_1 = \frac{1}{\sqrt{2}}(\,|0\rangle + \mathrm{i}\,|1\rangle\,)$$
$$|y\rangle_2 = \frac{1}{\sqrt{2}}(\,|0\rangle - \mathrm{i}\,|1\rangle\,)$$

and the state after the measurement is

$$\text{result } +1: \; |\text{out}; Y, +1\rangle = \sqrt{2}\,{}_1\langle y_1|\Psi\rangle_{1,2} = \mathrm{H}_2 e^{\frac{\mathrm{i}\pi}{4}\mathrm{Z}_2}\,|\text{in}\rangle_2\,,$$
$$\text{result } -1: \; |\text{out}; Y, -1\rangle = \sqrt{2}\,{}_1\langle y_2|\Psi\rangle_{1,2} = \mathrm{H}_2 e^{\frac{\mathrm{i}\pi}{4}\mathrm{Z}_2}\mathrm{Z}_2\,|\text{in}\rangle_2\,.$$

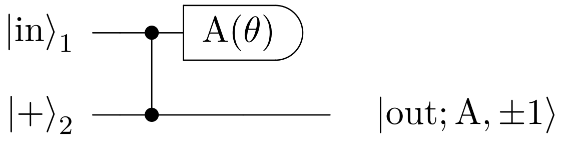
Z-Basis



The state after the measurement is

$$\text{result } +1: \; |\text{out}; Z, +1\rangle = \frac{\sqrt{2}}{a}\,{}_1\langle 0|\Psi\rangle_{1,2} = |+\rangle_2\,,$$
$$\text{result } -1: \; |\text{out}; Z, -1\rangle = \frac{\sqrt{2}}{b}\,{}_1\langle 1|\Psi\rangle_{1,2} = |-\rangle_2\,.$$

Only by employing different measurements on the first qubit, we realised different operations on the initial state, the result of which is contained in the second qubit.
A general scheme is



With $A = \cos\theta\mathrm{X} + \sin\theta\mathrm{Y} = \begin{pmatrix} 0 & e^{-\mathrm{i}\theta} \\ e^{\mathrm{i}\theta} & 0 \end{pmatrix}$ (in the computational basis). The eigenvalues and eigenvectors are

$$\begin{array}{ll} \mathrm{A}(\theta)\,|e_1\rangle & = |e_1\rangle \\ \mathrm{A}(\theta)\,|e_2\rangle & = |e_2\rangle \end{array} \quad \text{where} \quad \begin{array}{ll} |e_1\rangle & = \frac{1}{\sqrt{2}}(\,|0\rangle + e^{\mathrm{i}\theta}\,|1\rangle\,) \\ |e_2\rangle & = \frac{1}{\sqrt{2}}(\,|0\rangle - e^{\mathrm{i}\theta}\,|1\rangle\,) \end{array}\,.$$

The resulting state after the measurement is

$$\text{result } +1: \; |\text{out}; \mathrm{A}(\theta), +1\rangle = \sqrt{2}\,{}_1\langle e_1|\Psi\rangle_{1,2} = \mathrm{H}_2 e^{\frac{\mathrm{i}\theta}{2}\mathrm{Z}_2}\,|\text{in}\rangle_2\,,$$
$$\text{result } -1: \; |\text{out}; \mathrm{A}(\theta), +1\rangle = \sqrt{2}\,{}_1\langle e_2|\Psi\rangle_{1,2} = \mathrm{H}_2 e^{\frac{\mathrm{i}\theta}{2}\mathrm{Z}_2}\mathrm{Z}_2\,|\text{in}\rangle_2\,,$$

or in general

$$|\text{out}; \mathrm{A}(\theta), s\rangle_2 = \mathrm{H}_2 e^{\frac{\mathrm{i}\theta}{2}\mathrm{Z}_2}\mathrm{Z}_2^s\,|\text{in}\rangle_2$$

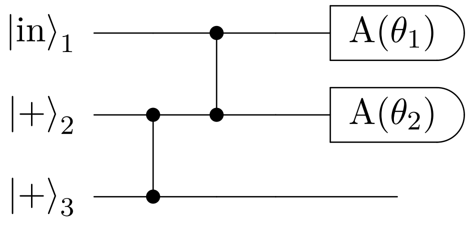
where s specifies an eigenvalue $(-1)^s$ for $s = 0, 1$.

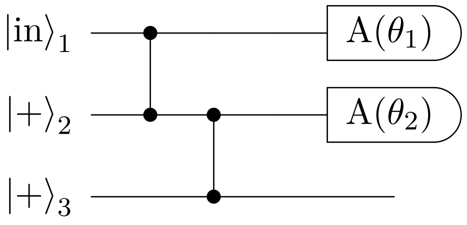
single qubit transformation

The three stages of one-way quantum computations are

1. cluster state representation
2. entanglement of qubits in input states to some nodes of a cluster state
3. local measurement of some nodes of the resulting state

The unmeasured qubits will be in the output state, which is related to the input state by a quantum transformation.
The two two-node cluster states are equivalent as cPhase operations commute and can be swapped:





The computational result is

$$|\mathrm{out}\rangle_3 = \left(\mathrm{H}_3 \mathrm{e}^{\mathrm{i}\frac{\theta_2}{2}\mathrm{Z}_3}\mathrm{Z}_3^{s_2}\right)\mathrm{H}_3 \mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\mathrm{Z}_3}\mathrm{Z}_3^{s_1}\,|\mathrm{in}\rangle_3\,.$$

It can further be simplified by using the relations

$$[\mathrm{e}^{\mathrm{i}\phi\mathrm{Z}},\mathrm{Z}] = 0,\ \mathrm{HX} = \mathrm{ZH}$$

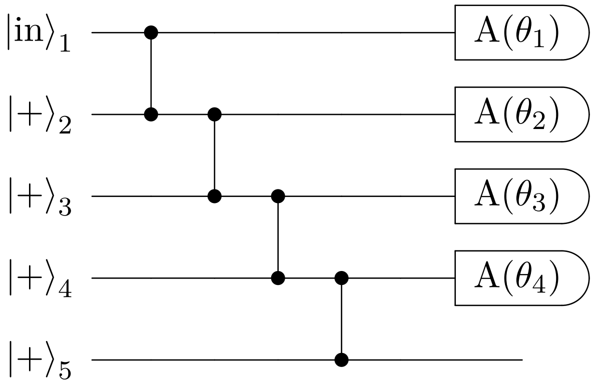
to obtain

$$|\mathrm{out}\rangle_3 = \mathrm{X}_3{}^{s_2}\mathrm{Z}_3{}^{s_1}\mathrm{e}^{\mathrm{i}(-1)^{s_1}\frac{\theta_2}{2}\mathrm{X}_3}\mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\mathrm{Z}_3}\,|\mathrm{in}\rangle_3\,.$$

A universal single-qubit transformation is

$$|\mathrm{out}\rangle = \mathrm{e}^{\mathrm{i}\phi_3\mathrm{X}}\mathrm{e}^{\mathrm{i}\phi_2\mathrm{Z}}\mathrm{e}^{\mathrm{i}\phi_1\mathrm{X}}\,|\mathrm{in}\rangle$$

where $\{\phi_1, \phi_2, \phi_3\}$ are the **Euler angles**. The two-node cluster transformation is not universal! For a universal transformation, one needs the **four-node linear cluster state**



The result of the computation on the four-node cluster state is

$$|\mathrm{out}\rangle_5 = \mathrm{X}^{s_4}\mathrm{Z}^{s_3}\mathrm{e}^{\mathrm{i}(-1)^{s_3}\frac{\theta_4}{2}\mathrm{X}}\mathrm{e}^{\mathrm{i}\frac{\theta_3}{2}\mathrm{Z}}\left(\mathrm{X}^{s_2}\mathrm{Z}^{s_1}\mathrm{e}^{\mathrm{i}(-1)^{s_1}\frac{\theta_2}{2}\mathrm{X}}\mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\mathrm{Z}}\right)|\mathrm{in}\rangle\,.$$

Let $\theta_1 = 0$ then we rewrite the state in the form:

$$|\mathrm{out}\rangle_5 = \mathrm{X}^{s_4+s_2}\mathrm{Z}^{s_3+s_1}\mathrm{e}^{\mathrm{i}(-1)^{s_3+s_1}\frac{\theta_4}{2}\mathrm{X}}\mathrm{e}^{\mathrm{i}\frac{\theta_3}{2}\mathrm{Z}}\mathrm{e}^{\mathrm{i}(-1)^{s_1}\frac{\theta_2}{2}\mathrm{X}}\,|\mathrm{in}\rangle\,.$$

Considering the computation results, we get the resulting state

$$|\mathrm{out}\rangle_5 = \mathrm{X}^{s_2+s_4}\mathrm{Z}^{s_1+s_3}\,\overline{|\mathrm{out}\rangle}_5 = \mathrm{e}^{\mathrm{i}\phi_1\mathrm{X}}\mathrm{e}^{\mathrm{i}\phi_2\mathrm{Z}}\mathrm{e}^{\mathrm{i}\phi_3\mathrm{X}}\,|\mathrm{in}\rangle$$

where $\phi_1 = (-1)^{s_1+s_3}\frac{\theta_4}{2}$, $\phi_2 = \frac{\theta_3}{2}$, $\phi_3 = (-1)^{s_1}\frac{\theta_2}{2}$.
Example:
Suppose we want to implement the unitary transformation U_1 over a single-qubit input state $|\mathrm{in}\rangle$

$$U_1 = \begin{pmatrix} -\frac{1}{2\sqrt{2}} & \sqrt{\frac{1}{8}+\frac{\mathrm{i}\sqrt{3}}{2}} \\ \frac{\mathrm{i}(\sqrt{3}+2\mathrm{i}}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} \end{pmatrix}.$$

We need to understand which angles should chosen. Considering $\mathrm{e}^{\mathrm{i}\phi\mathrm{X}} = \cos\phi\mathrm{I} + \mathrm{i}\sin\phi\mathrm{X}$ and $\mathrm{e}^{\mathrm{i}\phi\mathrm{Z}} = \cos\phi\mathrm{I} + \mathrm{i}\sin\phi\mathrm{Z}$, we can rewrite the operator $U = \mathrm{e}^{\mathrm{i}\phi_1\mathrm{X}}\mathrm{e}^{\mathrm{i}\phi_2\mathrm{Z}}\mathrm{e}^{\mathrm{i}\phi_3\mathrm{X}}$ in the matrix form

$$U = \begin{pmatrix} \cos\frac{\phi_2}{2}\cos\frac{\phi_-}{2} - \mathrm{i}\cos\frac{\phi_+}{2}\sin\frac{\phi_2}{2} & \sin\frac{\phi_2}{2}\sin\frac{\phi_-}{2} - \mathrm{i}\cos\frac{\phi_2}{2}\sin\frac{\phi_+}{2} \\ -\sin\frac{\phi_2}{2}\sin\frac{\phi_-}{2} - \mathrm{i}\cos\frac{\phi_2}{2}\sin\frac{\phi_+}{2} & \cos\frac{\phi_2}{2}\cos\frac{\phi_-}{2} + \mathrm{i}\cos\frac{\phi_+}{2}\sin\frac{\phi_2}{2} \end{pmatrix}$$

where $\phi_\pm = \phi_3 \pm \phi_1$ and, therefore, $\phi_1 = \frac{5\pi}{6}$, $\phi_2 = \frac{\pi}{2}$, $\phi_3 = -\frac{\pi}{6}$. With the previous relations, this means

$$\theta_2 = \frac{(-1)^{s_1+1}\pi}{3},\ \theta_3 = \pi,\ \theta_4 = \frac{(-1)^{s_3+s_1}5\pi}{3}.$$

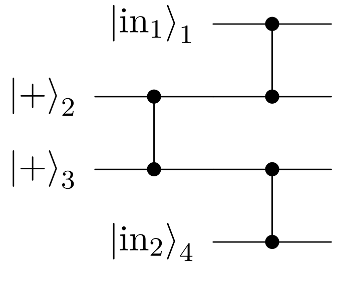
two qubit CNOT transformation

We carry out a computation on the two-node cluster state with the input states

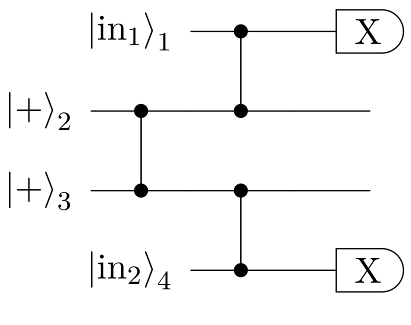
$$|\mathrm{in}_1\rangle_1 = a\,|0\rangle_1 + b\,|1\rangle_1$$
$$|\mathrm{in}_2\rangle_4 = c\,|0\rangle_4 + d\,|1\rangle_4$$

and the resource state

$$|\Psi\rangle_{1234} = \frac{c}{\sqrt{2}}\,|0\rangle_4\,|0\rangle_2\,|+\rangle_3\,(a\,|0\rangle_1 + b\,|1\rangle_1\,) + \frac{c}{\sqrt{2}}\,|0\rangle_4\,|1\rangle_2\,|-\rangle_3\,(a\,|0\rangle_1 - b\,|1\rangle_1\,)$$
$$+\frac{d}{\sqrt{2}}\,|1\rangle_4\,|0\rangle_2\,|-\rangle_3\,(a\,|0\rangle_1 + b\,|1\rangle_1\,) + \frac{d}{\sqrt{2}}\,|1\rangle_4\,|1\rangle_2\,|+\rangle_3\,(a\,|0\rangle_1 - b\,|1\rangle_1\,).$$



Let us measure the first and fourth qubit in the basis of the operator X



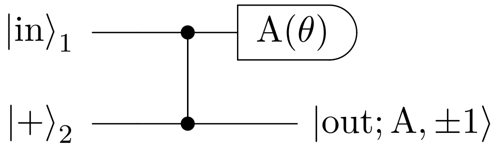
We write the eigenvalues of these operators as $(-1)^{s_1}$ and $(-1)^{s_4}$. If we get $s_1 = s_4 = 0$, then the resulting state is:

$$|\Psi'\rangle_{23} = 2\,{}_1\langle +|\,{}_4\langle +||\Psi\rangle_{123} = \mathrm{H}_3\mathrm{C}_2\mathrm{X}_3\Big(\mathrm{H}_2\,|\mathrm{in}_1\rangle_2\,|\mathrm{in}_2\rangle_3\Big)$$

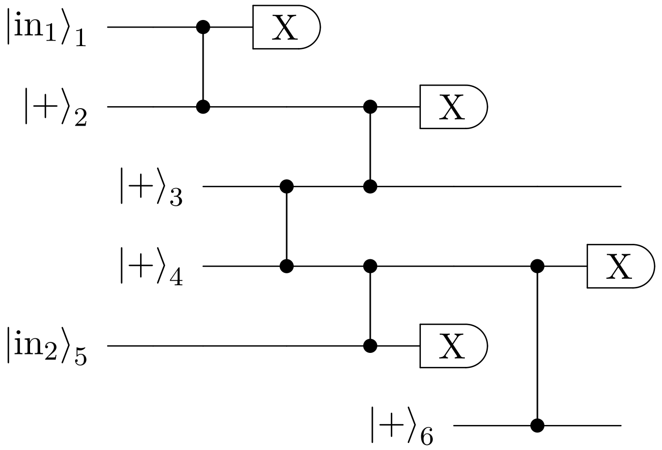
and in the general case

$$|\Psi'\rangle_{23} = \Big(\mathrm{Z}_2\mathrm{X}_3\Big)^{s_4}\Big(\mathrm{Z}_3\mathrm{X}_2\Big)^{s_1}\mathrm{H}_3\mathrm{C}_2\mathrm{X}_3\Big(\mathrm{H}_2\,|\mathrm{in}_1\rangle_2\,|\mathrm{in}_2\rangle_3\Big).$$

All the additional operations can be fixed after knowing the measurement results. Using the presented scheme, we can implement the one-qubit transformation



with $|\mathrm{out}, \mathrm{A}(\theta)\rangle_2 = \mathrm{H}e^{\mathrm{i}\frac{\theta}{2}\mathrm{Z}}\,|\mathrm{in}\rangle_2$. If we put $\theta = 0$, we get the Hadamard transform $|\mathrm{out}, \mathrm{A}(\theta)\rangle_2 = \mathrm{H}\,|\mathrm{in}\rangle_2$. The CNOT transformation is, therefore, implemented by a four-node cluster state in the following way



with

$$|\Psi\rangle_{34} = \mathrm{H}_4\mathrm{C}_3\mathrm{X}_4\,|\mathrm{in}_1\rangle_3\,|\mathrm{in}_2\rangle_4 \;\rightarrow\; |\Psi\rangle_{35} = \mathrm{C}_3\mathrm{X}_5\,|\mathrm{in}_1\rangle_3\,|\mathrm{in}_2\rangle_5\,.$$

This is, however, by no means the only implementation of the CNOT transformation.

14.2 Practical implementation and difficulties

To create a cluster state, we need to

1. prepare the qubits in state $|+\rangle$
2. entangle the pairs of qubits using the cPHASE operation

The implementation of qubits can be

- ions in optical traps
- superconducting qubits
- photonic qubits
- Rydberg atoms in optical traps

An ideal system for cluster states has not been found so far, though.

14.2.1 Photonic qubits

The qubit is encoded in the polarisation

$$|0\rangle \equiv |H\rangle = |1\rangle_H |0\rangle_V$$
$$|1\rangle \equiv |V\rangle = |0\rangle_H |1\rangle_V$$

Pros:

- almost not subjected to decoherence
- ease of implementation of single-qubit transformations
- relative ease of implementation of local measurements

Cons:

- probabilistic nature of single photon generation
- Kerr nonlinearity

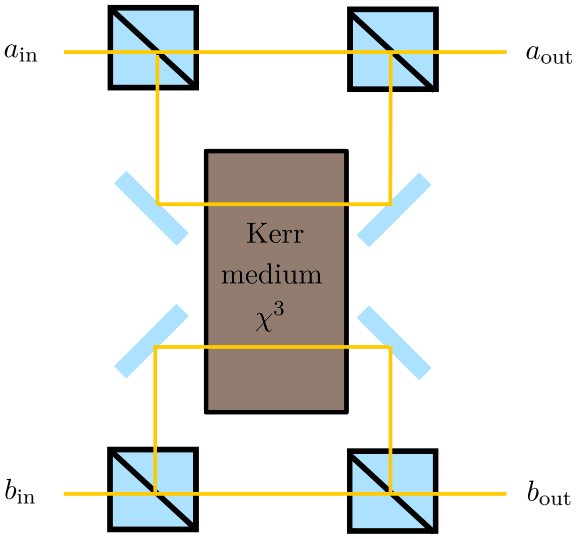
$$H_{\mathrm{Kerr}} = \kappa n_a n_b$$

where n_a, n_b are particle number operators for the signal and probe beams, respectively. The result of the transformation is given by the following expression

$$a_{\mathrm{out}} = a_{\mathrm{in}} \mathrm{e}^{-\mathrm{i}\kappa t n_b} b_{\mathrm{out}} = b_{\mathrm{in}} \mathrm{e}^{-\mathrm{i}\kappa t n_a}.$$

There is no direct interaction between photons (almost none) and, therefore, a material medium needs to be used to entangle the qubits.

14.2.2 Implementation of the cPhase transformation using the Kerr nonlinearity



$$|0\rangle_a |0\rangle_b \rightarrow |0\rangle_a |0\rangle_b$$
$$|1\rangle_a |0\rangle_b \rightarrow |1\rangle_a |0\rangle_b$$
$$|0\rangle_a |1\rangle_b \rightarrow |0\rangle_a |1\rangle_b$$
$$|1\rangle_a |1\rangle_b \rightarrow \mathrm{e}^{\mathrm{i}\kappa t} |1\rangle_a |1\rangle_b$$

If $\kappa t = \pi$, then we have the cPhase transformation.
In reality $\kappa t \approx 10^{-18} \ll \pi$.

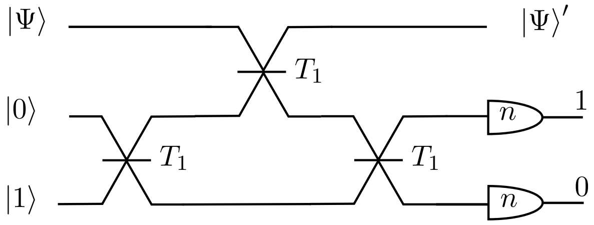
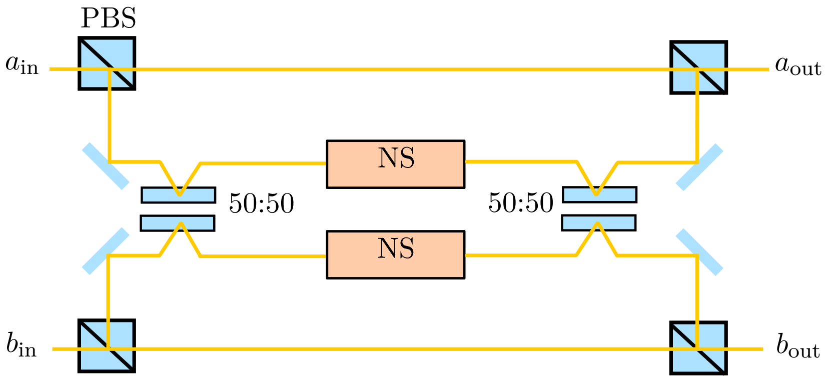


Figure 14.1: scheme of the nonlinear sign transformation

14.2.3 Nonlinear sign (NS) transformation

The nonlinear sign transformation (NS) does the following: $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle + c\,|2\rangle \to a\,|0\rangle + b\,|1\rangle - c\,|2\rangle$ and is realised by the scheme in Figure 14.1. There $T_1 = \frac{1}{4-2\sqrt{2}}, T_2 = 3 - 2\sqrt{2}$ and the probability $P_{\text{NS}} = \frac{1}{4}$.
Then the implementation of the cPhase (CZ) transformation using NS gates is



$$a_H b_H \to a'_H b'_H$$
$$a_H b_V \to a'_H b'_V$$
$$a_V b_H \to a'_V b'_H$$
$$a_V b_V \to -a'_V b'_V$$

The probability of implementing the CZ transformation is $P_{\text{CZ}} = P_{\text{NS}}^2 \approx \frac{1}{16}$. Hence, the more nodes in a cluster, the lower is the probability to implement the cluster state, i.e. a long waiting times for the quantum computation.

14.3 Continuous variable systems

The canonical formalism in the description of classical systems is **Hamilton's equation of motion**

$$\frac{\partial H}{\partial p} = \dot{q},\ \frac{\partial H}{\partial q} = -\dot{p}$$

where H is the system's Hamiltonian, q and p are its generalised coordinates and momenta, respectively. For the harmonic oscillator, we have

$$H = \frac{p^2}{2} + \frac{\omega^2 q^2}{2} \to p = \dot{q},\ \omega^2 q = -\dot{p}$$

$$\text{oscillator equation: } \ddot{q} + \omega^2 q = 0$$

The **Poisson brackets** are defined as

$$\{F, G\} = \frac{\partial F}{\partial q}\frac{\partial G}{\partial p} - \frac{\partial F}{\partial p}\frac{\partial G}{\partial q}.$$

Consider an arbitrary function $f(q, p, t)$, then from the multivariate chain rule,

$$\frac{\mathrm{d}f}{\mathrm{d}t} = \frac{\partial f}{\partial t} + \frac{\partial f}{\partial q}\frac{\partial q}{\partial t} + \frac{\partial f}{\partial p}\frac{\partial p}{\partial t} = \frac{\partial f}{\partial t} + \frac{\partial f}{\partial q}\frac{\partial H}{\partial p} - \frac{\partial f}{\partial p}\frac{\partial f}{\partial p}\frac{\partial H}{\partial q} = \frac{\partial f}{\partial t} + \{f, H\}$$

$$\Rightarrow\ \{q, p\} = \frac{\partial q}{\partial q}\frac{\partial p}{\partial p} - \frac{\partial q}{\partial p}\frac{\partial p}{\partial q} = 1$$

To get from a classical to a quantum theory, one performs **quantisation steps**: Canonically conjugate variables are declared Hermitian operators that correspond to observables

$$p \to \hat{p} = \hat{p}^\dagger, \ q \to \hat{q} = \hat{q}^\dagger.$$

In this case, the canonical Hamiltonian equations are preserved in the form

$$\frac{\partial H}{\partial \hat{p}} = \dot{\hat{q}}, \ \frac{\partial H}{\partial \hat{q}} = -\dot{\hat{p}}.$$

The classical Poisson brackets are replaced by quantum brackets:

$$\mathrm{i}\hbar\{F, G\} \to [\hat{F}, \hat{G}] \equiv \hat{F}\hat{G} - \hat{G}\hat{F}.$$

Canonical quantum variables are related by the following commutation rule:

$$[\hat{q}, \hat{p}] = \hat{q}\hat{p} - \hat{p}\hat{q} = \mathrm{i}\hbar$$

and the equation for the evolution of an arbitrary operator $\hat{F}$ has the form:

$$\frac{\mathrm{d}\hat{F}}{\mathrm{d}t} = \frac{\partial \hat{F}}{\partial t} - \frac{\mathrm{i}}{\hbar}[\hat{F}, \hat{H}] \qquad \textbf{(Heisenberg equation)}$$

where $\hat{H} = f(\hat{q}, \hat{p})$ is the Hamilton operator.
In the Heisenberg picture, the state of the system at the initial moment of time is given by the density matrix ϱ in the Hilbert space. This density matrix does not change throughout the development of the system. Using this matrix, one can calculate the average value of an operator:

$$\langle \hat{F} \rangle_t = \mathrm{Tr}\left(\hat{F}(t)\hat{\varrho}\right).$$

For the quantum oscillator, we have

$$H = \frac{p^2}{2} + \frac{\omega^2 q^2}{2} \to \frac{\hat{p}^2}{2} + \frac{\omega^2 \hat{q}^2}{2} = \hat{H}$$
$$[\hat{q}, \hat{H}] = [\hat{q}, \frac{\hat{p}^2}{2}] = \mathrm{i}\hbar\hat{p}, \ [\hat{p}, \hat{H}] = [\hat{p}, \frac{\omega^2\hat{q}^2}{2}] = -\mathrm{i}\hbar\omega^2\hat{q}$$

with the equation for the evolution of the operators $\hat{p}$ and $\hat{q}$:

$$\frac{\mathrm{d}\hat{q}}{\mathrm{d}t} = -\frac{\mathrm{i}}{\hbar}[\hat{q}, \hat{H}] = \hat{p}, \ \frac{\mathrm{d}\hat{p}}{\mathrm{d}t} = \frac{\mathrm{i}}{\hbar}[\hat{p}, \hat{H}] = \omega^2\hat{q}.$$

14.3.1 Continuous variables

Continuous variable systems are described by two operators $\hat{q}$ and $\hat{p}$ which correspond to observables. These observables must satisfy the canonical commutation relations

$$[\hat{q}, \hat{p}] = \mathrm{i}\hbar.$$

We can extent the commutation relations to include multiple modes by ordering the operators in canonical pairs as $\hat{R} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots, \hat{q}_N, \hat{p}_N)$. Then

$$[\hat{R}_i, \hat{R}_j] = \mathrm{i}\hbar\Omega_{ij}, \qquad i, j = 1, \ldots, 2N$$

where Ω_{ij} is the element of the matrix $\Omega = \bigoplus_{k=1}^{N} \xi$, and where $\xi = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

14.3.2 Quantisation of the electromagnetic field

The classical field is the solution of Maxwell's equations

$$\boldsymbol{E}(\boldsymbol{r},t)=\sum_{k}\mathrm{i}\left(\frac{\hbar\omega}{2\epsilon_0 V}\right)^{1/2}\boldsymbol{e_k}a_{\boldsymbol{k}}\mathrm{e}^{-\mathrm{i}\omega_{\boldsymbol{k}}t+\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}+\mathrm{c.c}$$

$$\boldsymbol{H}(\boldsymbol{r},t)=\sum_{k}\mathrm{i}\left(\frac{\hbar\omega}{2\epsilon_0 V}\right)^{1/2}\frac{\boldsymbol{k}\times\boldsymbol{e_k}}{\mu_0\omega_{\boldsymbol{k}}}a_{\boldsymbol{k}}\mathrm{e}^{-\mathrm{i}\omega_{\boldsymbol{k}}t+\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}+\mathrm{c.c}$$

The energy of the electromagnetic field is

$$W=\frac{1}{2}\int_V \mathrm{d}^3\boldsymbol{r}\left(\epsilon_0\boldsymbol{E}^2(\boldsymbol{r},t)+\mu_0\boldsymbol{H}^2(\boldsymbol{r},t)\right).$$

Substituting $\boldsymbol{E}$ and $\boldsymbol{H}$ in the energy equation, we get:

$$W=\sum_{k}\hbar\omega_{\boldsymbol{k}}|a_{\boldsymbol{k}}|^2$$

We can introduce the generalised canonically conjugate momenta and coordinates $\hat{p}$ and $\hat{q}$, respectively

$$a_{\boldsymbol{k}}\mathrm{e}^{-\mathrm{i}\omega_{\boldsymbol{k}}t}=\frac{1}{\sqrt{2\hbar\omega_{\boldsymbol{k}}}}(\omega_{\boldsymbol{k}}\hat{q}_{\boldsymbol{k}}+\mathrm{i}\hat{p}_{\boldsymbol{k}}).$$

The energy is then rewritten in the form

$$W=\sum_{\boldsymbol{k}}\left(\frac{\hat{p}_{\boldsymbol{k}}^2}{2}+\frac{\omega_{\boldsymbol{k}}^2\hat{q}_{\boldsymbol{k}}}{2}\right)$$

and the quantum electromagnetic field is

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t)=\sum_{\boldsymbol{k}}\mathrm{i}\left(\frac{\hbar\omega_{\boldsymbol{k}}}{2\epsilon_0 V}\right)^{1/2}\boldsymbol{e_k}\hat{a}_{\boldsymbol{k}}\mathrm{e}^{-\mathrm{i}\omega_{\boldsymbol{k}}t+\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}+\mathrm{h.c.}$$

$$\hat{\boldsymbol{H}}(\boldsymbol{r},t)=\sum_{\boldsymbol{k}}\mathrm{i}\left(\frac{\hbar\omega_{\boldsymbol{k}}}{2\epsilon_0 V}\right)^{1/2}\frac{\boldsymbol{k}\times\boldsymbol{e_k}}{\mu_0\omega_{\boldsymbol{k}}}\hat{a}_{\boldsymbol{k}}\mathrm{e}^{-\mathrm{i}\omega_{\boldsymbol{k}}t+\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}+\mathrm{h.c.}$$

where $\left[\hat{a}_{\boldsymbol{k}},\hat{a}_{\boldsymbol{k}'}\right]=\delta_{\boldsymbol{k},\boldsymbol{k}'}$, and the energy is equal to

$$\hat{H}=\sum_{\boldsymbol{k}}\left(\frac{\hat{p}_{\boldsymbol{k}}^2}{2}+\frac{\omega_{\boldsymbol{k}}^2\hat{q}_{\boldsymbol{k}}}{2}\right)=\sum_{\boldsymbol{k}}\hbar\omega_{\boldsymbol{k}}\left(\hat{a}_{\boldsymbol{k}}^\dagger\hat{a}_{\boldsymbol{k}}+\frac{1}{2}\right).$$

14.3.3 Fock states

Suppose we have a single mode field with frequency ω. In this case, the Hamiltonian of this field is

$$\hat{H}=\hbar\omega(\hat{a}^\dagger\hat{a}+\frac{1}{2}).$$

For the Hermitian operator $\hat{n}=\hat{a}^\dagger\hat{a}$, we can write the eigenvalue equation as

$$\hat{n}\left|n\right\rangle=n\left|n\right\rangle$$

where n is the real eigenvalue of $\hat{n}$ and $\left|n\right\rangle$ is the corresponding eigenvector. These eigenvectors form a complete set of orthogonal states. From

$$\langle n|\hat{n}|n\rangle\equiv\langle n|\hat{a}^\dagger\hat{a}|n\rangle=n=|\hat{a}\left|n\right\rangle|^2\geq 0$$

follows $n \geq 0$. Using $\left[\hat{a}, \hat{a}^\dagger\right] = 1$, we find that

$$\hat{n}(\hat{a}\,|n\rangle\,) = (n-1)(\hat{a}\,|n\rangle\,)$$

and, therefore, $\hat{a}\,|n\rangle$ is also an eigenvector with eigenvalue $n-1$, which we call $A_n\,|n-1\rangle$. Here, A_n is the normalisation constant. Since all eigenvalues are non-negative, there has to be an eigenstate $|0\rangle$ with $\hat{a}\,|0\rangle = 0$. The state $|0\rangle$ is called the **vacuum state**. Similarly, we find $\hat{n}(\hat{a}^\dagger\,|n\rangle\,) = (n+1)(\hat{a}^\dagger\,|n\rangle\,)$. The operators $\hat{a}^\dagger$ are called **creation operators** and the operators $\hat{a}$ are called **annihilation operators**.
Using the creation operators, one can write the **Fock state** $|n\rangle$ through the vacuum state:

$$|n\rangle = C_n (\hat{a}^\dagger)^n\,|0\rangle$$

where C_n is the normalisation constant. From $1 = \langle n|n\rangle = C_n^2 \langle 0|\hat{a}^n (\hat{a}^\dagger)^n|0\rangle = C_n^2 n!$ we infer

$$|n\rangle = \frac{1}{\sqrt{n!}}\left(\hat{a}^\dagger\right)^n |0\rangle\,.$$

The Fock states are eigenstates of the field Hamiltonian

$$\hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|n\rangle = \hbar\omega\left(\hat{n} + \frac{1}{2}\right)|n\rangle$$

and, therefore the energy of the vacuum state is equal to

$$E_0 = \langle 0|\hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|0\rangle = \frac{\hbar\omega}{2}.$$

Variance

The variance of an operator is

$$\Delta A^2 = \langle A^2\rangle - \langle A\rangle^2.$$

The generalised coordinate and momentum operators are

$$\hat{p} = \sqrt{\frac{\hbar\omega}{2}}\frac{(\hat{a} - \hat{a}^\dagger}{\mathrm{i}}, \quad \hat{q} = \sqrt{\frac{\hbar}{2\omega}}(\hat{a} + \hat{a}^\dagger)$$

in the Fock state

$$\langle\hat{q}\rangle = \langle\hat{p}\rangle = 0.$$

Therefore,

$$\Delta\hat{p}_{\mathrm{FS}}^2 = \langle\hat{p}^2\rangle = \hbar\omega\left(n + \frac{1}{2}\right), \quad \Delta\hat{q}_{\mathrm{FS}}^2 = \langle\hat{q}^2\rangle = \frac{\hbar}{\omega}\left(n + \frac{1}{2}\right).$$

The uncertainty relation for generalised coordinate and momentum are

$$\Delta\hat{q}_{\mathrm{FS}}\Delta\hat{p}_{\mathrm{FS}} = \hbar\left(n + \frac{1}{2}\right).$$

Multimode case

$$\hat{H} = \sum_{\boldsymbol{k}} \hbar\omega_{\boldsymbol{k}}\left(\hat{a}_{\boldsymbol{k}}^\dagger\hat{a}_{\boldsymbol{k}} + \frac{1}{2}\right) = \sum_{\boldsymbol{k}} \hat{H}_{\boldsymbol{k}}$$

$$\hat{H}_{\boldsymbol{k}}\,|n_{\boldsymbol{k}}\rangle = \hbar\omega_{\boldsymbol{k}}\left(\hat{a}_{\boldsymbol{k}}\hat{a}_{\boldsymbol{k}} + \frac{1}{2}\right)|n_{\boldsymbol{k}}\rangle = \hbar\omega_{\boldsymbol{k}}\left(n_{\boldsymbol{k}} + \frac{1}{2}\right)|n_{\boldsymbol{k}}\rangle$$

A generalised eigenstate can be written as

$$|n_{\boldsymbol{k}_1}, n_{\boldsymbol{k}_2}, n_{\boldsymbol{k}_3}, \ldots, n_{\boldsymbol{k}_l}, \ldots\rangle \equiv |\{n_{\boldsymbol{k}}\}\rangle\,.$$

14.3.4 Coherent states

A **coherent state** $|\alpha\rangle$ is defined by

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,, \text{ with } \alpha = |\alpha|\mathrm{e}^{\mathrm{i}\theta}.$$

It has the following useful properties:

- It can be expressed through Fock states in the form
$$|\alpha\rangle = \mathrm{e}^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,.$$
- It is a partition of unity
$$\int \mathrm{d}^2\alpha\,|\alpha\rangle\,\langle\alpha| = \pi\mathrm{I}, \quad \text{where } \mathrm{d}^2\alpha = \mathrm{d}(\mathrm{Re}\alpha)\mathrm{d}(\mathrm{Im}\alpha).$$
- Coherent states corresponding to different eigenvalues are not orthogonal
$$|\langle\alpha|\beta\rangle|^2 = \exp\left(-|\alpha-\beta|^2\right).$$
- Coherent states form an over-complete basis. i.e. any coherent state can be expressed in terms of other coherent states:
$$|\alpha\rangle = \frac{1}{\pi}\int \mathrm{d}^2\alpha\,|\alpha'\rangle\,\langle\alpha'|\,\alpha\rangle.$$

Variance

$$\begin{aligned}
\langle\hat{p}\rangle &= \sqrt{2\hbar\omega}\alpha'', & \langle\hat{q}\rangle &= \sqrt{2\hbar/\omega}\alpha' \quad \text{with } \alpha = \alpha' + \mathrm{i}\alpha''\\
\langle\hat{p}^2\rangle &= \frac{\hbar\omega}{2}\left(4(\alpha'')^2+1\right), & \langle\hat{q}^2\rangle &= \frac{\hbar}{2\omega}\left(4(\alpha')^2+1\right)\\
\Delta\hat{p}^2_{\mathrm{CS}} &= \frac{\hbar\omega}{2}, & \Delta\hat{q}^2_{\mathrm{CS}} &= \frac{\hbar}{2\omega}\\
\text{uncertainty relation: } \Delta\hat{q}_{\mathrm{CS}}\Delta\hat{p}_{\mathrm{CS}} &= \frac{\hbar}{2}
\end{aligned}$$

$$\text{displacement operator:} \qquad \hat{D}(\alpha) = \mathrm{e}^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}},\ |\alpha\rangle = \hat{D}(\alpha)\,|0\rangle$$

Quadratures

The **Hermitian quadrature operators** are

$$\hat{a} = \hat{X} + \mathrm{i}\hat{Y}, \qquad \hat{a}^\dagger = \hat{X} - \mathrm{i}\hat{Y}$$
$$\hat{X} = \frac{1}{2}\left(\hat{a}^\dagger + \hat{a}\right),\ \hat{Y} = \frac{1}{2\mathrm{i}}\left(\hat{a} - \hat{a}^\dagger\right)$$

The variance of the quadrature operators is

$$\Delta\hat{X}^2_{\mathrm{CS}} = \frac{1}{4},\ \Delta\hat{Y}^2_{\mathrm{CS}} = \frac{1}{4}$$

and their uncertainty relations in the coherent state are

$$\Delta\hat{X}_{\mathrm{CS}}\Delta\hat{Y}_{\mathrm{CS}} = \frac{1}{4}.$$

It is often more convenient to use the phase space of quadratures of continuous variables, because they yield valuable information as one follows the operator's values instead of the operator quantities (real numbers). A coherent state look like a circle in the phase space with its center being the mean value α of the state and the radius given by the variance of the quadrature in the coherent state.

14.3.5 Squeezed states

A **squeezed state** is a state for which the uncertainty relation is fulfilled, but the variances are larger than for a coherent state:

$$\Delta\hat{X}_{\mathrm{SS}}\Delta\hat{Y}_{\mathrm{SS}} = \frac{1}{4},$$

and, e.g.

$$\Delta\hat{X}_{\mathrm{SS}} < \frac{1}{4},\ \Delta\hat{Y}_{\mathrm{SS}} > \frac{1}{4}.$$

The **squeezed operator** is

$$\hat{S}(r) = \mathrm{e}^{\frac{1}{2}r\left(\hat{a}^2-(\hat{a}^\dagger)^2\right)}$$

where r determines the amount of squeezing. A squeezed state is constructed by

$$|\alpha, r\rangle = \hat{S}(r)\,|\alpha\rangle = \hat{S}(r)\hat{D}(\alpha)\,|0\rangle\,.$$

In the phase space, a squeezed state looks like an ellipsis with its center around α and the squeezing according to r. The squeezing operator transforms the annihilation and quadrature operators as follows:

$$\begin{aligned}
\hat{S}^\dagger(r)\hat{a}\hat{S}(r) &= \hat{a}\cosh r - \hat{a}^\dagger \sinh r\\
\hat{S}^\dagger(r)\hat{a}^\dagger\hat{S}(r) &= \hat{a}^\dagger\cosh r - \hat{a}\sinh r\\
\hat{S}^\dagger(r)\hat{X}\hat{S}(r) &= \mathrm{e}^{-r}\hat{X}\\
\hat{S}^\dagger(r)\hat{Y}\hat{S}(r) &= \mathrm{e}^{r}\hat{Y}
\end{aligned}$$

The variance of squeezed quadratures is

$$\Delta\hat{X}^2_{\mathrm{SS}} = \frac{1}{4}\mathrm{e}^{-2r},\ \Delta\hat{Y}^2_{\mathrm{SS}} = \frac{1}{4}\mathrm{e}^{2r}$$

and the corresponding uncertainty remains

$$\Delta\hat{X}_{\mathrm{SS}}\Delta\hat{Y}_{\mathrm{SS}} = \frac{1}{4}.$$

Squeezed states are used to entangle states with continuous variables.

14.4 Probability functions

14.4.1 Glauber-Sudarshan P representation

The density operator of an arbitrary state can be expanded over the full set of vectors in the form:

$$\hat{\varrho} = \sum_{m,l} p_{m,l}\,|\Phi_m\rangle\,\langle\Phi_l|$$

or in its diagonal basis

$$\hat{\varrho} = \sum_{m} p_{m}\,|\Psi_m\rangle\,\langle\Psi_m|\,.$$

Since coherent states form an over-complete set, one can decompose any state diagonally using it[1]

$$\hat{\varrho} = \int P(\alpha)\,|\alpha\rangle\,\langle\alpha|\,\mathrm{d}^2\alpha.$$

[1] This does not mean that the coherent states are eigenstates of the density operator, though!

The **Glauber function** can be calculated using the following integral relation:

$$P(\alpha) = \frac{1}{\pi^2} \int \mathrm{d}^2\beta \, \langle -\beta | \, \hat{\varrho} \, |\beta\rangle \, \mathrm{e}^{|\alpha|^2 + |\beta|^2 - \beta\alpha^* + \beta^*\alpha}.$$

The Glauber function has the following properties:

- P is real

$$\hat{\varrho} = \hat{\varrho}^* \Rightarrow P(\alpha) = P^*(\alpha)$$

- P is normalised

$$\mathrm{Tr}(\hat{\varrho}) = 1 \Rightarrow \int P(\alpha) \mathrm{d}^2\alpha = 1$$

- It is convenient for calculating normally ordered operators

$$\langle (\hat{a}^\dagger)^m \hat{a}^n \rangle = \int \mathrm{d}^2\alpha (\alpha^*)^m \alpha^n P(\alpha)$$

- The P-function can be used to calculate the average value of non-normally ordered operators:

$$\langle \hat{a}\hat{a}^\dagger \rangle = \int \mathrm{d}^2 \left(\alpha - \frac{\partial}{\partial \alpha^*} \right) \left(\alpha^* - \frac{\partial}{\partial \alpha} \right) P(\alpha)$$

- The Glauber function of quantum states has negative values or even singularities.

14.4.2 Husimi Q representation

The **Husimi function Q** is

$$Q(\alpha) = \frac{1}{\pi} \langle \alpha | \, \hat{\varrho} \, | \alpha \rangle$$

with

$$\int Q(\alpha) \mathrm{d}^2\alpha = 1$$

and as a result

$$Q(\alpha) = \frac{1}{\pi} \sum_m P_m \left| \langle \Psi | \alpha \rangle \right|^2 \to 0 \leq Q(\alpha) \leq \frac{1}{\pi},$$
$$0 \leq \left| \langle \Psi | \alpha \rangle \right|^2 \leq 1.$$

The relation between the P- and the Q-function is

$$Q(\alpha) = \frac{1}{\pi} \int P(\alpha') \mathrm{e}^{-|\alpha - \alpha'|^2} \mathrm{d}^2\alpha'.$$

The Q-function is convenient to calculate anti-normally ordered expectation values:

$$\left\langle \hat{a}^n \left(\hat{a}^\dagger \right)^m \right\rangle = \int \alpha^n (\alpha^*)^m Q(\alpha) \, \mathrm{d}^2\alpha.$$

14.4.3 Wigner quasiprobability distribution

The **Wigner function** W is defined as

$$W(q,p) = \frac{1}{\pi}\int \mathrm{d}y\, \mathrm{e}^{-2\mathrm{i}yp/\hbar} \langle q-y|\,\hat{\varrho}\,|q+y\rangle$$

and the **characteristic function** is

$$\chi(\beta) = \mathrm{Tr}\left(\mathrm{e}^{\mathrm{i}\beta\hat{a}^\dagger + \mathrm{i}\beta^*\hat{a}}\hat{\varrho}\right).$$

Both functions are related by

$$W(\alpha) = \frac{1}{\pi^2}\int \mathrm{d}^2\beta\, \chi(\beta)\mathrm{e}^{-\mathrm{i}\beta\alpha^* - \mathrm{i}\beta^*\alpha}.$$

With the Wigner function, one can conveniently calculate symmetrically ordered operators:

$$\frac{1}{2}\langle \hat{a}\hat{a}^\dagger + \hat{a}^\dagger\hat{a}\rangle = \int \alpha\alpha^* W(\alpha)\,\mathrm{d}^2\alpha.$$

For Fock states, the Wigner function is

$$W_n(q,p) = \frac{(-1)^n}{\pi}\exp\left[-(q^2+p^2)\right] L_n\left(2(q^2+p^2)\right)$$

where L_n are Laguerre polynomials. For Fock states with $n > 0 \rightarrow W < 0$ and

$$\int W_n(q,p)\,\mathrm{d}q\mathrm{d}p = 1\,\forall n \in \mathbb{N}^0.$$

The Wigner function has the following properties

- T-symmetry:
$$t \rightarrow -t \Leftrightarrow W(q,p,t) \rightarrow W(q,-p,-t)$$
- X-symmetry:
$$q \rightarrow -q \Leftrightarrow W(q,p,t) \rightarrow W(-q,-p,t)$$
- translational invariance:
$$q \rightarrow q+a \Leftrightarrow W(q,p,t) \rightarrow W(q+a,p,t)$$
- it is bounded
$$|W(q,p,t)|^2 \leq \frac{1}{\pi}$$
- it is orthonormal
$$\left|\int \mathrm{d}q\ \Psi^*(q)\Phi(q)\right|^2 = 2\pi\int \mathrm{d}q \int \mathrm{d}p W_\Psi(q,p)W_\Phi(q,p)$$
  if the states are orthonormal then
$$\int \mathrm{d}q \int \mathrm{d}p W_\Psi(q,p)W_\Phi(q,p) = 0$$
- the q and p probability distributions are given by marginals
$$\int \mathrm{d}p W(q,p) = \langle p|\,\hat{\varrho}\,|p\rangle\,, \int \mathrm{d}q W(q,p) = \langle q|\,\hat{\varrho}\,|q\rangle$$
  where $\hat{X}\,|q\rangle = q\,|q\rangle\,,\ \hat{Y}\,|p\rangle = p\,|p\rangle$

- the average value of an operator $\hat{A}$ in a state $\hat{\varrho}$ is

$$\mathrm{Tr}\left(\hat{\varrho}\hat{A}\right) = 2\pi \int \mathrm{d}q \int \mathrm{d}p \; W_{\hat{\varrho}}(q,p) W_{\hat{A}}(q,p)$$

- the Wigner functions of the N-mode quantum system is

$$W(q_1, q_2, \dots, q_N, p_1, p_2, \dots, p_N) =$$
$$\frac{1}{(2\pi)^N} \int \cdots \int \prod_{j=1}^{N} \mathrm{e}^{\mathrm{i}p_j x_j} \left\langle q_1 - x_1, \dots, q_N - x_N \right| \hat{\varrho} \left| q_1 + x_1, \dots, q_N + x_N \right\rangle \, \mathrm{d}q_j \mathrm{d}p_j.$$

Therefore, the Wigner function allows one to visualise the quantum state $\hat{\varrho}$ in phase space, variances and quadratures can be calculated easily using the Wigner functions, and they allow one to determine how classical the system under study can be.

14.5 Gaussian states

Gaussian states are states with Gaussian quasi-probability Wigner distributions on the multi-mode quantum phase space. Single-mode Gaussian state characterised by quadratures $\hat{X}$ and $\hat{Y}$. Any Gaussian state is characterised by the first and second moment of the quadrature operators:

$$\text{first moments:} \quad \boldsymbol{d} = \left(\langle \hat{X} \rangle, \langle \hat{Y} \rangle\right)^{\top}$$
$$\text{second moments:} \quad \sigma = \begin{pmatrix} 2\langle \hat{X}^2 \rangle - 2\langle \hat{X} \rangle^2 & \langle \hat{X}\hat{Y} + \hat{Y}\hat{X} \rangle - 2\langle \hat{X} \rangle \langle \hat{Y} \rangle \\ \langle \hat{Y}\hat{X} + \hat{X}\hat{Y} \rangle - 2\langle \hat{X} \rangle \langle \hat{Y} \rangle & 2\langle \hat{Y}^2 \rangle - 2\langle \hat{Y} \rangle^2 \end{pmatrix}$$

and for the N-mode Gaussian state

$$\boldsymbol{d} = \left(\langle \hat{\boldsymbol{R}}_1 \rangle, \langle \hat{\boldsymbol{R}}_2 \rangle, \dots, \langle \hat{\boldsymbol{R}}_{2N} \rangle\right)^{\top}$$
$$\sigma_{ij} = \langle \hat{\boldsymbol{R}}_i \hat{\boldsymbol{R}}_j + \hat{\boldsymbol{R}}_j \hat{\boldsymbol{R}}_i \rangle - 2\langle \hat{\boldsymbol{R}}_i \rangle \langle \hat{\boldsymbol{R}}_j \rangle$$
$$\text{where } \hat{\boldsymbol{R}} = \left(\hat{X}_1, \hat{Y}_1, \dots, \hat{X}_N, \hat{Y}_N\right)^{\top} \text{ is the quadrature vector.}$$

For a physical system $\hat{\varrho} \geq 0$, $\mathrm{Tr}(\hat{\varrho}big) = 1$ and, therefore,

$$\sigma + \mathrm{i}\Omega \geq 0 \text{ where } \Omega = \bigoplus_{k=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

An $2N \times 2N$ matrix (symmetric, real) is said to be positive semidefinite if $\boldsymbol{v}^{\top} M \boldsymbol{v} \geq 0$ for all non-zero $\boldsymbol{x} \in \mathbb{R}^{2N}$. Equivalently: A matrix $M \geq 0$ if and only if all of its eigenvalues are $\mu_i \geq 0$. The Wigner function of a Gaussian state is

$$W(\boldsymbol{R}) = \frac{1}{\pi^N \sqrt{\det \sigma}} \mathrm{e}^{(\boldsymbol{R}-\boldsymbol{d})^{\top} \sigma^{-1} (\boldsymbol{R}-\boldsymbol{d})}$$

where $\boldsymbol{R} = (q_1, p_1, \dots, q_N, p_N)^{\top}$ is the real phase-space vector. The characteristic function is

$$\chi(\boldsymbol{R}) = \exp\left[-\frac{1}{4}\boldsymbol{R}^{\top} \sigma \boldsymbol{R} + \mathrm{i}\boldsymbol{d}^{\top}\boldsymbol{R}\right].$$

The decomposition of the covariance matrix of a N-mode Gaussian state is

$$\sigma_{1,2,\dots,N} = \begin{pmatrix} \sigma_1 & C_{1,2} & \dots & C_{1,N} \\ C_{1,2}^{\top} & \sigma_2 & \vdots & C_{2,N} \\ \vdots & \ddots & \ddots & \vdots \\ C_{1,N}^{\top} & \dots & C_{N-1,N}^{\top} & \sigma_N \end{pmatrix}$$

where the $\{\sigma_i\}_{i=1}^{N}$ are local covariance matrices corresponding to the reduced model i and the C_{ij} are matrices encoding classical and quantum correlations between the ith and jth subsystems.

examples:

- vacuum state

$$\hat{a}\,|0\rangle = 0,\ \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ d_0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

- coherent state

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle\,,\ \sigma_{\text{CS}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ d_{\text{CS}} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$$

- squeezed vacuum state

$$|r,0\rangle = \hat{S}(r)\,|0\rangle\,,\ \sigma_{\text{SVS}} = \begin{pmatrix} \mathrm{e}^{-2r} & 0 \\ 0 & \mathrm{e}^{2r} \end{pmatrix},\ d_{\text{SVS}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Gaussian transformations

Linear transformations on canonical variables (symplectic) are

$$\hat{\boldsymbol{R}} \to \hat{\boldsymbol{R}}' = M\hat{\boldsymbol{R}} + \boldsymbol{d}$$

and since $\hat{\boldsymbol{R}}$ is canonical

$$[\hat{\boldsymbol{R}}_i, \hat{\boldsymbol{R}}_j] = \mathrm{i}\hbar\Omega_{ij} \Rightarrow M\Omega M^\top = \Omega$$

where $i,j = 1,\ldots,2N$ and $\Omega = \bigoplus_{k=1}^{N} \xi$ and $\xi = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. A linear canonical transformation corresponds to a unitary transformation in Hilbert space

$$\hat{\boldsymbol{R}}' = \hat{S}^\top \hat{\boldsymbol{R}} \hat{S} = M\hat{\boldsymbol{R}} + \boldsymbol{d}'.$$

Consequently,

$$\hat{D}(\boldsymbol{\xi}) = \mathrm{e}^{\mathrm{i}\boldsymbol{\xi}^\top \hat{\boldsymbol{R}}}$$

is transformed as

$$\hat{S}^\top \hat{\boldsymbol{D}}(\boldsymbol{\xi})\hat{S} = \mathrm{e}^{\mathrm{i}\boldsymbol{\xi}^\top M\hat{\boldsymbol{R}} + \mathrm{i}\boldsymbol{\xi}\cdot\boldsymbol{d}'} \equiv \hat{D}(M\boldsymbol{\xi})\mathrm{e}^{\mathrm{i}\boldsymbol{\xi}\cdot\boldsymbol{d}'}.$$

The characteristic function is

$$\mathrm{Tr}\left[\hat{S}\hat{\varrho}\hat{S}^\dagger \hat{D}(\boldsymbol{\xi})\right] = \mathrm{Tr}\left[\hat{\varrho}\exp\left(\mathrm{i}\boldsymbol{\xi}\hat{S}^\top \hat{\boldsymbol{R}}\hat{S}\right)\right] = \exp\left[\frac{1}{4}\boldsymbol{\xi}^\top \tilde{\sigma}\boldsymbol{\xi} + \boldsymbol{\xi}^\top \boldsymbol{d}''\right]$$

where $\tilde{\sigma} = M\sigma M^\top$ and $\boldsymbol{d}'' = M\boldsymbol{d} + \boldsymbol{d}'$. The transformed state is described by the characteristic function of the Gaussian state. Linear quadrature transformations transform one Gaussian state into another.

Because of the Heisenberg equation

$$\frac{\mathrm{d}\hat{F}}{\mathrm{d}t} = \frac{\mathrm{i}}{\hbar}[\hat{H}, \hat{F}]$$

will a transformation of $\hat{X}$ and $\hat{Y}$ operators with Hamiltonian $\hat{H} = \hat{H}(q,p)$ due to

$$[\hat{X}, \hat{Y}^m] = \frac{m}{2}\hat{Y}^{m-1} \text{ and } [\hat{X}^m, \hat{Y}] = \frac{m}{2}\hat{X}^{m-1}$$

result in a quadratic Hamiltonian in quadratures after a linear transformation. A **Gaussian transformation** is a transformation whose Hamiltonian does not exceed the second degree in quadratures.
Consider the phase shift operator as an example

$$\hat{H} = \frac{1}{2}\left(\hat{X}^2 + \hat{Y}^2\right) : \ M(t) = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix},$$

or the Beam-splitter operator

$$\hat{H}_{\mathrm{BS}} = T\left(\hat{X}_i\hat{Y}_j + \hat{Y}_j\hat{X}_i\right) : \ M_{\mathrm{BS}} = \begin{pmatrix} \sqrt{T} & 0 & \sqrt{1-T} & 0 \\ 0 & \sqrt{T} & 0 & \sqrt{1-T} \\ \sqrt{1-T} & 0 & -\sqrt{T} & 0 \\ 0 & \sqrt{1-T} & 0 & -\sqrt{T} \end{pmatrix}.$$

14.5.1 Quantum computing on systems in continuous variables

Encoding information

The following relations are true for the quadrature operators:

$$\begin{aligned} &\hat{X}\left|q\right\rangle_x = q\left|q\right\rangle_x, \ \hat{Y}\left|p\right\rangle_y = p\left|p\right\rangle_y \\ &{}_x\langle q|q'\rangle_x = \delta(q-q'), \ {}_y\langle p|p'\rangle_y = \delta(p-p') \\ &\int \mathrm{d}q \ \left|q\right\rangle_x {}_x\!\left\langle q\right| = \int \mathrm{d}p \ \left|p\right\rangle_y {}_y\!\left\langle p\right| = \hat{\mathrm{I}} \\ &\left|q\right\rangle_x = \frac{1}{\sqrt{2\pi}}\int \mathrm{e}^{-\mathrm{i}qp}\left|p\right\rangle_y \mathrm{d}p \\ &\left|p\right\rangle_y = \frac{1}{\sqrt{2\pi}}\int \mathrm{e}^{\mathrm{i}qp}\left|q\right\rangle_x \mathrm{d}q \end{aligned}$$

Any consistent development of a quantum system by a set of Hamiltonians $\{\pm\hat{H}_i\}$ is equivalent to the development by Hamiltonians of the form: $[\hat{H}_i, \hat{H}_j]$, $[\hat{H}_k, [\hat{H}_i, \hat{H}_j]]$, etc. This follows from the **Baker-Campbell-Hausdorff** formula[2] and

$$\mathrm{e}^{\mathrm{i}t\hat{H}_j}\mathrm{e}^{\mathrm{i}t\hat{H}_k}\mathrm{e}^{-\mathrm{i}t\hat{H}_j}\mathrm{e}^{-\mathrm{i}t\hat{H}_k} = \mathrm{e}^{-t^2[\hat{H}_j,\hat{H}_k]} + \mathcal{O}(t^3).$$

The set of Hamiltonians required for universal quantum computing = Universal quantum transformations in continuous variables

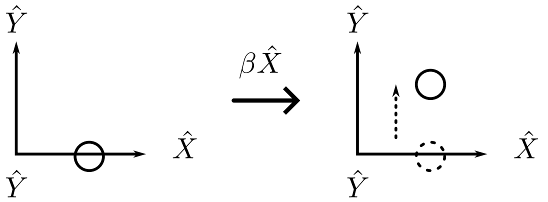
The operator temporal evolution is

$$\hat{W}(t) = \mathrm{e}^{-\mathrm{i}\hat{H}t}\hat{W}(0)\mathrm{e}^{\mathrm{i}\hat{H}t}.$$

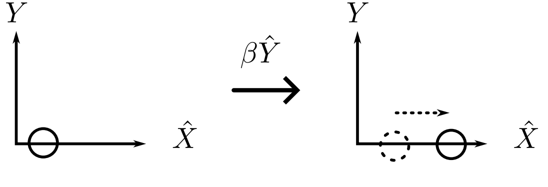
There are a few elementary operations:

- **linear Hamiltonian:**

  $\hat{H}_X = \beta\hat{X}$ and the quadrature transform is
  $\hat{X}(t) = \hat{X}(0), \ \hat{Y}(t) = \hat{Y}(0) - \beta t$

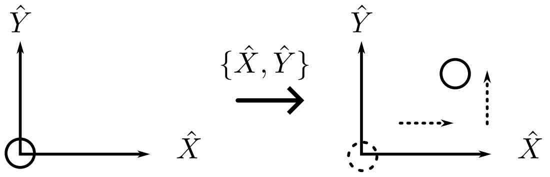


  $\hat{H}_Y = \beta\hat{Y}$ and the quadrature transform is
  $\hat{X}(t) = \hat{X}(0) - \beta t, \ \hat{Y}(t) = \hat{Y}(0)$



[2] The solution $\hat{Z}$ to the equation $\mathrm{e}^{\hat{X}}\mathrm{e}^{\hat{Y}} = \mathrm{e}^{\hat{Z}}$ is $\hat{Z} = \hat{X} + \hat{Y} + \frac{1}{2}\left[\hat{X}, \hat{Y}\right] + \frac{1}{12}\left[\hat{X}, [\hat{X}, \hat{Y}]\right] - \frac{1}{12}\left[\hat{Y}, [\hat{X}, \hat{Y}]\right] + \ldots$

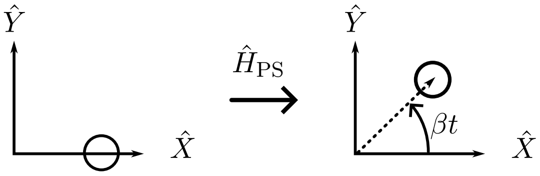
Sequentially applying the operators from the set $\hat{D} = \{\hat{X}, \hat{Y}\}$, we can implement only **displacement transformations**.



- **Phase shifting:**

  Hamiltonian $\hat{H}_{\mathrm{PS}} = \frac{\beta}{2}\left(\hat{X}^2 + \hat{Y}^2\right)$
  Quadrature transformation:

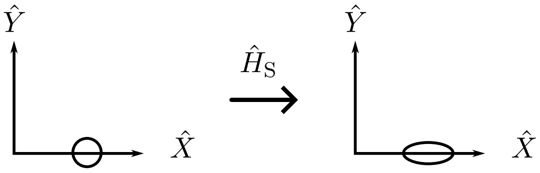
$$\begin{pmatrix} \hat{X}(t) \\ \hat{Y}(t) \end{pmatrix} = \begin{pmatrix} \cos\beta t & -\sin\beta t \\ \sin\beta t & \cos\beta t \end{pmatrix} \begin{pmatrix} \hat{X}(0) \\ \hat{Y}(0) \end{pmatrix}$$



- **Single mode squeezing**

  Hamiltonian = $\hat{H}_{\mathrm{S}} = \frac{\beta}{2}\left(\hat{X}\hat{Y} + \hat{Y}\hat{X}\right)$
  Quadrature transformation:

$$\begin{pmatrix} \hat{X}(t) \\ \hat{Y}(t) \end{pmatrix} = \begin{pmatrix} \mathrm{e}^{\beta t} & 0 \\ 0 & \mathrm{e}^{-\beta t} \end{pmatrix} \begin{pmatrix} \hat{X}(0) \\ \hat{Y}(0) \end{pmatrix}$$



Sequentially applying the operators from the set $A = \{\hat{H}_{\mathrm{S}}, \hat{H}_{\mathrm{PS}}, \hat{X}, \hat{Y}\}$ we can implement any Gaussian transformation!
By adding Hamiltonians of non-Gaussian transformations like

$$\hat{H}_1 = \hat{X}^3$$

which has a quadrature transformations of

$$\begin{aligned} \hat{X}(t) &= \hat{X}(0), \\ \hat{Y}(t) &= \frac{3}{2}\hat{X}^2(t) + \hat{Y}(0), \end{aligned}$$

we can construct a Hamiltonian of any degree by quadratures. This can be seen by the commutation relations:

$$\begin{aligned} \left[\hat{Y}^3, \hat{Y}^m\hat{X}^n\right] &= \mathrm{i}\hat{Y}^{m+2}\hat{X}^{n-1} + \text{lower order terms}, \\ \left[\hat{X}^3, \hat{Y}^m\hat{X}^n\right] &= \mathrm{i}\hat{Y}^{m-2}\hat{X}^{n+2} + \text{lower order terms}. \end{aligned}$$

Two-node CZ transformation

A multi-mode system is characterised by a set of oscillators with quadratures $\{\hat{X}_i, \hat{Y}_i\}_{i=1}^N$. The CZ transform has the Hamiltonian

$$\hat{H}_{ij}^{\mathrm{CZ}} = 2\beta\hat{X}_i\hat{X}_j$$

and its corresponding quadrature transformation is

$$\begin{pmatrix} \hat{X}_i(t) \\ \hat{Y}_i(t) \\ \hat{X}_j(t) \\ \hat{Y}_j(t) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \beta t & 0 \\ 0 & 0 & 1 & 0 \\ \beta t & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \hat{X}_i(0) \\ \hat{Y}_i(0) \\ \hat{X}_j(0) \\ \hat{Y}_j(0) \end{pmatrix}$$

$B = \{\hat{H}_{\mathrm{S}}, \hat{H}_{\mathrm{PS}}, \hat{X}, \hat{Y}, \hat{H}_1, \hat{H}_{ij}^{\mathrm{CZ}}\}$ is a set of Hamiltonians that can be used to implement any quantum transformation. For universal quantum computing in continuous variables, one needs to implement three types of operations:

1. arbitrary single-mode operations
2. two-mode Gaussian mode interaction operations
3. one non-linear operations

14.6 Cluster state generation

14.6.1 Continuous-variable cluster states

One-way computing has the following stages:

1. continuous variable **cluster state** preparation
2. entanglement of continuous variable systems in input states with some nodes of a **cluster state**
3. local measurements of some subsystem of the resulting state
4. post-correction of unmeasured subsystem taking into account the measurement results

The **Heisenberg-Weyl operators** are

$$\hat{X}(s) = \mathrm{e}^{-2\mathrm{i}s\hat{Y}},\ \hat{Z}(r) = \mathrm{e}^{2\mathrm{i}r\hat{X}} \text{ where } [\hat{X}, \hat{Y}] = \frac{\mathrm{i}}{2}.$$

They are not commutative

$$\hat{X}(s)\hat{Z}(r) = \mathrm{e}^{-2\mathrm{i}sr}\hat{Z}(r)\hat{X}(s).$$

The continuous Pauli operators act on the basis states of the $\hat{x}$ and $\hat{y}$ operators as follows:

$$\begin{array}{rclrcl} \hat{X}(s)\left|q\right\rangle_x & = & \left|q+s\right\rangle_x, & \hat{X}(s)\left|p\right\rangle_y & = & \mathrm{e}^{-2\mathrm{i}sp}\left|p\right\rangle_y \\ \hat{Z}(s)\left|q\right\rangle_x & = & \mathrm{e}^{2\mathrm{i}sq}\left|q\right\rangle_x, & \hat{Z}(s)\left|p\right\rangle_y & = & \left|p+s\right\rangle_y \end{array}$$

Comparing the relation in the discrete state

$$\hat{X}\left|+\right\rangle = \left|+\right\rangle$$

to the one for the continuous case

$$\hat{X}(s)\left|0\right\rangle_y = \mathrm{e}^0\left|0\right\rangle_y = \left|0\right\rangle_y$$

we see that the state $\left|0\right\rangle_y$ is infinitely squeezed in a $\hat{y}$-quadrature since is has the variances

$${}_y\langle 0|\delta\hat{y}^2\left|0\right\rangle_y = 0,\ {}_y\langle 0|\delta\hat{x}^2\left|0\right\rangle_y = \infty$$

Such a state can not be realised in practise as it requires infinite energy.
The CZ-transformation is

$$\hat{\mathrm{C}}_{z,ij} = \mathrm{e}^{2g_{ij}\hat{x}_i\hat{X}_j}$$

with g_{ij} being the coupling constant between two modes. With this, the following relations hold:

$$\begin{array}{ll} \hat{\mathrm{C}}^\dagger_{z,ij}\hat{X}_i\hat{\mathrm{C}}_{z,ij} = \hat{X}_i, & \hat{\mathrm{C}}^\dagger_{z,ij}\hat{Y}_i\hat{\mathrm{C}}_{z,ij} = \hat{Y}_i + g_{ij}\hat{X}_j, \\ \hat{\mathrm{C}}^\dagger_{z,ij}\hat{X}_j\hat{\mathrm{C}}_{z,ij} = \hat{X}_j, & \hat{\mathrm{C}}^\dagger_{z,ij}\hat{Y}_j\hat{\mathrm{C}}_{z,ij} = \hat{Y}_j + g_{ij}\hat{X}_i. \end{array}$$

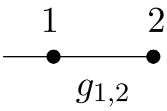
To generate a continuous cluster state that satisfies a particular graph $\mathcal{G} = (V, E)$, we use the following algorithm:

- To each node $i \in V$ in the graph we associate the system in state $\left|0\right\rangle_{i,y}$
- Next, all pairs of systems with numbers $(i, j) \in E$ are entangled by the operator $\hat{\mathrm{C}}_{z,ij} = \mathrm{e}^{2\mathrm{i}g_{ij}\hat{X}_i\hat{X}_j}$

As a result, the cluster state can be written as

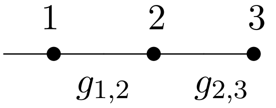
$$|G\rangle = \hat{\mathrm{C}}_{z,ij}\,|0\rangle_y^{\otimes n} = \left(\prod_{(i,j)\in E} \mathrm{e}^{2\mathrm{i}g_{ij}\hat{X}_i\hat{X}_j}\right)|0\rangle_{y,1}\,|0\rangle_{y,2}\cdots|0\rangle_{y,n}$$

example: two-node cluster state



$$\begin{aligned}|G\rangle_2 &= \hat{\mathrm{C}}_{z,1,2}\,|0\rangle_{y,1}\,|0\rangle_{y,2} = \hat{\mathrm{C}}_{z,1,2}\int\frac{\mathrm{d}s}{\sqrt{2\pi}}\,|s\rangle_{x,1}\,|0\rangle_{y,2}\\ &= \mathrm{e}^{2\mathrm{i}g_{1,2}\hat{X}_1\hat{X}_2}\int\frac{\mathrm{d}s}{\sqrt{2\pi}}\,|s\rangle_{x,1}\,|0\rangle_{y,2} = \frac{1}{\sqrt{2\pi}}\int\mathrm{d}s\,|s\rangle_{x,1}\,\mathrm{e}^{2\mathrm{i}g_{1,2}s\hat{X}_2}\,|0\rangle_{y,2}\\ &= \frac{1}{\sqrt{2\pi}}\int\mathrm{d}s\,|s\rangle_{x,1}\,|g_{1,2}s\rangle_{y,2}\end{aligned}$$

example: three-node cluster state



$$\begin{aligned}|G\rangle_3 &= \hat{\mathrm{C}}_{z,1,2}\hat{\mathrm{C}}_{z,2,3}\,|0\rangle_{y,1}\,|0\rangle_{y,2}\,|0\rangle_{y,3}\\ &= \mathrm{e}^{2\mathrm{i}g_{1,2}\hat{X}_1\hat{X}_2}\mathrm{e}^{2\mathrm{i}g_{2,3}\hat{X}_2\hat{X}_3}\int\frac{\mathrm{d}s}{\sqrt{2\pi}}\,|0\rangle_{y,1}\,|s\rangle_{x,2}\,|0\rangle_{y,3}\\ &= \frac{1}{\sqrt{2\pi}}\int\mathrm{d}s\,\mathrm{e}^{2\mathrm{i}g_{1,2}\hat{X}_1\hat{X}_2}\mathrm{e}^{2\mathrm{i}g_{2,3}\hat{X}_2\hat{X}_3}\,|0\rangle_{y,1}\,|s\rangle_{x,2}\,|0\rangle_{y,3}\\ &= \frac{1}{\sqrt{2\pi}}\int\mathrm{d}s\,|g_{1,2}s\rangle_{y,1}\,|s\rangle_{x,2}\,|g_{2,3}s\rangle_{y,3}\end{aligned}$$

14.6.2 Continuous variable cluster state stabilizers

To generate a cluster state, we need the system in the $|0\rangle_{i,y}$ state $|\Phi\rangle = |0\rangle_{1,y}\,|0\rangle_{2,y}\cdots|0\rangle_{n,y}$ the stabilizers of this state are $\{\hat{X}(s)\}_{i=1}^n$. The cluster state definition is

$$|G\rangle = \hat{\mathrm{C}}_{z,\mathrm{total}}\,|\Phi\rangle = \left(\prod_{(i,j)\in E}\mathrm{e}^{2\mathrm{i}g_{ij}\hat{X}_i\hat{X}_j}\right)|\Phi\rangle$$

and its stabilizers are

$$\{\hat{\mathrm{C}}_{z,\mathrm{total}}\hat{X}_i(s)\hat{\mathrm{C}}_{z,\mathrm{total}}^\dagger\}_{i=1}^n$$

as

$$\hat{\mathrm{C}}_{z,\mathrm{total}}\hat{X}_i\hat{\mathrm{C}}_{z,\mathrm{total}}^\dagger = \exp\left[-2\mathrm{i}s(\hat{Y}_i - \sum_{j\in N(i)} g_{ij}\hat{X}_j)\right] = \hat{X}_i(s)\prod_{j\in N(i)}\hat{Z}_j(g_{ij}s) = \exp\left[-2\mathrm{i}s\hat{N}_i\right].$$

From

$$\hat{S}_i\,|G\rangle = \exp\left[-2\mathrm{i}s\hat{N}_i\right]|G\rangle = |G\rangle$$

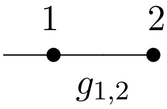
it follows that

$$\hat{N}_i\,|G\rangle = \left(y_i - \sum_{j\in N(i)} g_{ij}\hat{X}_j\right)|G\rangle = 0,$$

i.e. the state of **nullifier operators** $\{\hat{N}_i\}_{i=1}^n$ completely defines the cluster state. It is convenient to write the entire set of cluster state nullifiers in vector form

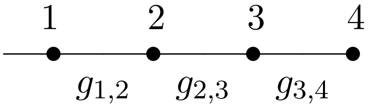
$$\hat{\boldsymbol{N}} = \hat{\boldsymbol{y}} - A\hat{\boldsymbol{x}}$$

where A is the adjacency matrix of the cluster graph and $\hat{x}, \hat{y}$ are the quadrature vectors of the cluster state.
example: two-node cluster state



$$
\begin{aligned}
N(1) &= \{2\}\\
N(2) &= \{1\}\\
\text{adjacency matrix: } A &= \begin{pmatrix} 0 & g_{1,2} \\ g_{1,2} & 0 \end{pmatrix}\\
\text{cluster state nullifiers: } \hat{N}_1 &= \hat{y}_1 - g_{1,2}\hat{x}_2 \;\rightarrow\; \hat{N}_1 \left|G_2\right\rangle = 0\\
\hat{N}_2 &= \hat{y}_2 - g_{1,2}\hat{x}_1 \;\rightarrow\; \hat{N}_2 \left|G_2\right\rangle = 0
\end{aligned}
$$

example: four-node cluster state



$$
\begin{aligned}
&N(1) = \{2\},\; N(2) = \{1,3\}\\
&N(3) = \{2,4\},\; N(4) = \{3\}\\
\text{adjacency matrix: } A = &\begin{pmatrix} 0 & g_{1,2} & 0 & 0 \\ g_{1,2} & 0 & g_{2,3} & 0 \\ 0 & g_{2,3} & 0 & g_{34} \\ 0 & 0 & g_{34} & 0 \end{pmatrix}\\
\text{cluster state nullifiers: } &\hat{N}_1 = \hat{y}_1 - g_{1,2}\hat{x}_2,\; \hat{N}_2 = \hat{y}_2 - g_{1,2}\hat{x}_1 - g_{2,3}\hat{x}_3,\\
&\hat{N}_3 = \hat{y}_3 - g_{2,3}\hat{x}_2 - g_{34}\hat{x}_4,\; \hat{N}_4 = \hat{y}_4 - g_{34}\hat{x}_3\\
\Rightarrow\; &\hat{N}_i \left|G_4\right\rangle = 0 \; i = 1,2,3,4
\end{aligned}
$$

14.6.3 The van Loock-Fukusawa separability criterion

To study entanglement in cluster states, it is convenient to use the **van Loock-Fukusawa separability criterion**:
Let $\mathcal{S}$ be a set consisting of N elements, which are represented by the canonical variables $\{x_i, y_i\}_{i=1}^{N}$. We assume that this set is divided into M independent subsets $\mathcal{S}_r$ $(r = 1, \ldots, M)$. For each subset $\mathcal{S}_r$, we introduce into consideration two auxiliary Hermitian operators as linear combinations of entities $\hat{x}_i$ and $\hat{y}_i$:

$$
\hat{u}_r = \sum_{k \in \mathcal{S}_r} \left[h_k \hat{x}_k + g_k \hat{y}_k\right],\; \hat{v}_r = \sum_{k \in \mathcal{S}_r} \left[\tilde{h}_k \hat{x}_k + \tilde{g}_k \hat{y}_k\right]
$$

in addition, we introduce the auxiliary operators $\hat{U}$ and $\hat{V}$

$$
\hat{U} = \sum_{k=1}^{M} \hat{u}_r,\; \hat{V} = \sum_{k=1}^{M} \hat{v}_r.
$$

The inequality

$$
\left\langle \left|\delta\hat{u}_r + \mathrm{i}\hat{v}_r\right|^2 \right\rangle \geq 0
$$

is evident.
After term squaring under the average sign, we can write

$$
\langle \delta\hat{u}_r^2 \rangle + \langle \delta\hat{v}_r^2 \rangle \geq \left|\langle [\hat{u}_r, \hat{v}_r] \rangle\right|.
$$

The commutator on the right-hand side of the equation is written in terms of a combination of real coefficients

$$
[\hat{u}_r, \hat{v}_r] = \frac{\mathrm{i}}{2} \sum_{k \in \mathcal{S}_r} (h_k \tilde{g}_k - g_k \tilde{h}_k).
$$

Summing over all values of r:

$$\langle \delta \hat{U}^2 \rangle + \langle \delta \hat{V}^2 \rangle \geq \frac{1}{2} \sum_{r=1}^{M} \left| \sum_{k \in \mathcal{S}_r} \left(h_k \tilde{g}_k - g_k \tilde{h}_k \right) \right| .$$

This inequality is taken as the basis of the van Loock-Fukusawa separability criterion: If the formulated inequality holds, then the set can be divided into M independent subsets. Else, there is some entanglement.
The values of $\langle \delta \hat{U}^2 \rangle$ and $\langle \delta \hat{V}^2 \rangle$ need to be known. The Loock-Fukusawa criterion can only detect entanglement, but not rule it out completely.
The cluster state is defined by its set of nullifiers

$$\hat{N}_i \left| G \right\rangle = \left(\hat{y}_i - \sum_{j \in N(i)} g_{ij} \hat{x}_j \right) \left| G \right\rangle = 0, \ i = 1, \ldots, n$$

Hence, the variance of the nullifiers should be equal to zero:

$$\left\langle G \right| \delta \hat{N}_i^2 \left| G \right\rangle = 0 \ \forall i \in \{1, \ldots, n\}.$$

If one uses operators with finite squeezing

$$\left\langle G \right| \delta \hat{N}_i^2 \left| G \right\rangle \to 0 \text{ for } \langle \delta \hat{y}_s^2 \rangle \to 0.$$

The van Loock-Fukusawa criterion for cluster states is

$$\begin{aligned} &\langle \delta \hat{N}_i^2 \rangle + \langle \delta \hat{N}_j^2 \rangle \geq 0, \text{ if} \, i \notin N(j) \, \text{(useless, always true)}, \\ &\langle \delta \hat{N}_i^2 \rangle + \langle \delta \hat{N}_j^2 \rangle \geq |g_{ij}|, \text{ if} \, i \in N(j). \end{aligned}$$

It follows from this that the cluster state will be entangled, if

$$\langle \delta \hat{\mathbf{N}}_\mathbf{i} \rangle + \langle \delta \hat{\mathbf{N}}_\mathbf{j} \rangle < |\mathbf{g_{ij}}|.$$

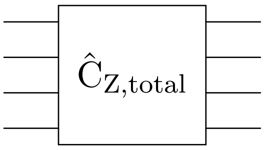
If the inequality holds true for all neighbours of a certain state, it is entangled and can be represented by the desired graph, if it holds for all nodes of it.

14.6.4 Linear transformations and generation of multipartite cluster states

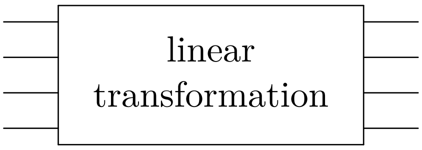
To calculate the cluster state's variances, we need to know the relationship between the cluster state's quadratures and the quadratures of squeezed oscillators.

$$\begin{aligned} \hat{y}_i &= f_i(\hat{x}_{s,1}, \hat{x}_{s,2}, \ldots, \hat{x}_{s,n}, \hat{y}_{s,1}, \hat{y}_{s,2}, \ldots, \hat{y}_{s,n}) \\ \hat{x}_i &= g_i(\hat{x}_{s,1}, \hat{x}_{s,2}, \ldots, \hat{x}_{s,n}, \hat{y}_{s,1}, \hat{y}_{s,2}, \ldots, \hat{y}_{s,n}) \end{aligned}$$

Cluster state generation in theory



Cluster state generation in practice



The general form of the linear transformation necessary to generalise a cluster state is

$$\hat{\boldsymbol{X}} + \mathrm{i}\hat{\boldsymbol{Y}} = U\Big(\hat{\boldsymbol{x}} + \mathrm{i}\hat{\boldsymbol{y}}\Big) = \Big(\mathrm{Re}\, U + \mathrm{i}\mathrm{Im}\, U\Big)\Big(\hat{\boldsymbol{x}} + \mathrm{i}\hat{\boldsymbol{y}}\Big) = \Big(\mathrm{Re}\, U \hat{\boldsymbol{x}}_s - \mathrm{Im}\, U \hat{\boldsymbol{y}}_s\Big) + \mathrm{i}\Big(\mathrm{Re}\, U \hat{\boldsymbol{y}}_s + \mathrm{Im}\, U \hat{\boldsymbol{x}}_s\Big).$$

Substituting the obtained vector into the vector of nullifier operators:

$$\begin{aligned}\hat{\boldsymbol{N}} &= \hat{\boldsymbol{Y}} - A\hat{\boldsymbol{X}} = \mathrm{Re}\,U\hat{\boldsymbol{y}}_s + \mathrm{Im}\,U\hat{\boldsymbol{x}}_s - A\Big(\mathrm{Re}\,U\hat{\boldsymbol{x}}_s - \mathrm{Im}\,U\hat{\boldsymbol{y}}_s\Big)\\ &= \Big(\mathrm{Im}\,U - A\mathrm{Re}\,U\Big)\hat{\boldsymbol{x}}_s + \Big(\mathrm{Re}\,U + A\mathrm{Im}\,U\Big)\hat{\boldsymbol{y}}_s\end{aligned}$$

and, therefore, for nullifiers to tend to zero, it is necessary that $\mathrm{Im}\,U = A\mathrm{Re}\,U$. The vector of nullifiers and the transformation matrix are

$$U = (\mathrm{I} + \mathrm{i}A)\ \mathrm{Re}\,U,\ \hat{N} = \Big(\mathrm{I} + A^2\Big)\ \mathrm{Re}\,U\hat{\boldsymbol{y}}_s.$$

To define $\mathrm{Re}\,U$, we use the unitary condition for U:

$$\begin{aligned}&U^\dagger U = \left((\mathrm{I} + \mathrm{i}A)\,\mathrm{Re}\,U\right)^\dagger (\mathrm{I} + \mathrm{i}A)\,\mathrm{Re}\,U = (\mathrm{Re}\,U)^\dagger (\mathrm{I} + A^2)\,\mathrm{Re}\,U = \mathrm{I},\\ &\mathrm{Re}\,U = (\mathrm{I} + A^2)^{-1/2} Q.\end{aligned}$$

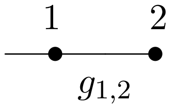
Since the matrix $(\mathrm{I} + A^2) \geq 0$, it has exactly one positive definite square root:

$$U = (\mathrm{I} + \mathrm{i}A)(\mathrm{I} + A^2)^{-1/2} Q.$$

This is a relation between the vector of cluster state nullifiers and the vectors of squeezed quadratures of the used quantum oscillators

$$\hat{N} = \Big(\mathrm{I} + A^2\Big)^{1/2} Q\hat{y}_s.$$

Therefore, the cluster state can be prepared with 100% certainty using linear transformations and continuous variable. The matrix Q is arbitrary and is determined by the generation scheme. **example:** The two-node cluster state



$$A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\text{linear transformation: } U_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \mathrm{i} \\ \mathrm{i} & 1 \end{pmatrix}$$

$$\hat{N} = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix}\begin{pmatrix} \hat{y}_{s,1} \\ \hat{y}_{s,2} \end{pmatrix}$$

$$\langle \delta \hat{N}_1^2 \rangle = 2\langle \delta \hat{y}_s^2 \rangle$$

$$\langle \delta \hat{N}_2^2 \rangle = 2\langle \delta \hat{y}_s^2 \rangle$$

The inseparability criterion is

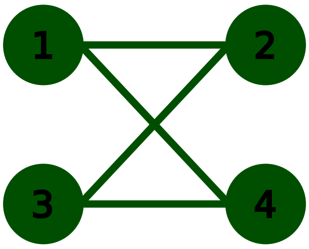
$$\begin{aligned}&\langle \delta \hat{N}_1^2 \rangle + \langle \delta \hat{N}_2^2 \rangle = 4\langle \delta \hat{y}_s^2 \rangle < 1\\ &\Rightarrow\ \langle \delta \hat{y}_s^2 \rangle < \frac{1}{4}\end{aligned}$$

Hence, the squeezing of oscillators required for generating a two-node cluster state is

$$s = 10\log_{10}\left[4\langle \delta \hat{y}_s^2 \rangle\right] < 0\mathrm{dB}.$$

14.7 Exercises

1. Which adjacency matrix does represented graph below correspond to?



- ○ $A = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$
- ○ $A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$
- ○ $A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$
- ○ $A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

2. Choose the wave function that will be obtained after applying the CPhase operation to the two-qubit state $|-\rangle_1 |-\rangle_2$

- ○ $|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle_1 |-\rangle_2 - |1\rangle_1 |+\rangle_2 \big)$
- ○ $|\Psi\rangle = |0\rangle_1 |-\rangle_2 - |1\rangle_1 |+\rangle_2$
- ○ $|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle_1 |-\rangle_2 + |1\rangle_1 |+\rangle_2 \big)$
- ○ $|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle_1 |+\rangle_2 - |1\rangle_1 |-\rangle_2 \big)$

3. Choose the wave function of the cluster state, represented by the graph of exercise 1:

- ○ $|G\rangle = \text{CPhase}_{1,2}\text{CPhase}_{1,4}\text{CPhase}_{2,3}\text{CPhase}_{3,4} |+\rangle_1 |+\rangle_2 |+\rangle_3 |+\rangle_4$
- ○ $|G\rangle = \text{CPhase}_{1,2}\text{CPhase}_{1,3}\text{CPhase}_{2,4}\text{CPhase}_{3,4} |+\rangle_1 |+\rangle_2 |+\rangle_3 |+\rangle_4$
- ○ $|G\rangle = \text{CPhase}_{2,1}\text{CPhase}_{2,3}\text{CPhase}_{4,1}\text{CPhase}_{4,3} |+\rangle_1 |+\rangle_2 |+\rangle_3 |+\rangle_4$
- ○ $|G\rangle = \text{CPhase}_{1,3}\text{CPhase}_{2,3}\text{CPhase}_{1,4}\text{CPhase}_{4,3} |+\rangle_1 |+\rangle_2 |+\rangle_3 |+\rangle_4$

4. What condition must be satisfied so that the operator $\hat{S}$ is a stabilizer?

- ○ $\hat{S} |\Psi\rangle = -|\Psi\rangle$
- ○ $\hat{S} |\Psi\rangle = s |\Psi\rangle$
- ○ $\hat{S} |\Psi\rangle = 0$
- ○ $\hat{S} |\Psi\rangle = |\Psi\rangle$

5. Choose the number of the cluster state nodes that are neighbours of the node with the number 3 (in the graph of exercise 1):

- ○ 2,1,4

○ 2,1

○ 2,4

○ 1,4

6. Choose a three-node cluster state stabilizer:

○ $\hat{X}_1\hat{Z}_2\hat{Z}_3$

○ $\hat{X}_1\hat{X}_2\hat{Z}_3$

○ $\hat{Y}_1\hat{X}_2\hat{Z}_3$

○ $\hat{X}_1\hat{Y}_2\hat{Y}_3$

7. Choose the operators of the cluster state stabilizers for the graph in exercise 1

○ $\hat{X}_1\hat{Z}_2\hat{Z}_4$

○ $\hat{X}_2\hat{Z}_1\hat{Z}_3$

○ $\hat{X}_3\hat{Z}_1\hat{Z}_4$

○ $\hat{X}_4\hat{Z}_2\hat{Z}_3$

8. What property should an operator have for it to be measured experimentally?

○ An operator must be Hermitian

○ An operator must be unitary

○ An operator can be arbitrary

9. Let $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle$ be the wave function of the state before measurement. What is the probability that when we measure the Pauli operator $\hat{X}$, we get an eigenvalue equal to +1.

○ $p = \frac{(a+b)^2}{2}$

○ $p = \frac{a}{2}$

○ $p = a$

○ $p = \frac{1}{2}$

10. Suppose we have the wave function of the multiparticle state $|\Psi\rangle_{12} = a\,|0\rangle_1\,|0\rangle_2 + b\,|1\rangle_1\,|1\rangle_2$ before measurement. Choose the wave function of the second particle after measuring the first particle in the basis of the Pauli operator $\hat{X}$. It is known that the measurement result was an eigenvalue equal to +1.

○ $|\Psi\rangle_{12} = \frac{1}{\sqrt{2}}(a\,|0\rangle_2 + b\,|1\rangle_2)$

○ $|\Psi\rangle_{12} = a\,|0\rangle_2 + b\,|1\rangle_2$

○ $|\Psi\rangle_{12} = |0\rangle_2 + |1\rangle_2$

○ $|\Psi\rangle_{12} = |0\rangle_2$

11. Choose the wave function obtained as a result of computations on a two-node cluster state, provided that, during the measurements, we had got the values $s_1 = s_2 = 0$.

○ $|\text{out}\rangle = \mathrm{e}^{\mathrm{i}\frac{\theta_2}{2}\hat{X}}\mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\hat{Z}}\,|\text{in}\rangle$

○ $|\text{out}\rangle = \mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\hat{Z}}\,|\text{in}\rangle$

○ $|\text{out}\rangle = \mathrm{e}^{\mathrm{i}\frac{\theta_2}{2}\hat{X}}\,|\text{in}\rangle$

○ $|\text{out}\rangle = \mathrm{e}^{\mathrm{i}\frac{\theta_2}{2}\hat{Z}}\mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\hat{X}}\,|\text{in}\rangle$

12. Suppose we want to implement an one-qubit transformation, which is characterised by three Euler angles $\varphi_1, \varphi_2, \varphi_3$. What angles, when measuring a four-node linear cluster state, should we choose to get such a transformation.

   ○ $\theta_1 = 0, \theta_2 = 2\varphi_3, \theta_3 = 2\varphi_2, \theta_4 = 2\varphi_1$
   ○ $\theta_1 = \pi/2, \theta_2 = 3\varphi_3, \theta_3 = 2\varphi_2, \theta_4 = 2(-1)^{s_1+s_3}\varphi_1$
   ○ $\theta_1 = 0, \theta_2 = 2(-1)^{s_1}\varphi_3, \theta_3 = 2\varphi_2, \theta_4 = 2(-1)^{s_1+s_3}\varphi_1$

13. Can the CNOT transformation be implemented using a four-node cluster state?

14. What is the main problem of practically implementing cluster states using single photons?

   ○ Photons move at a high speed
   ○ Probabilistic nature of photon generation
   ○ Photons are subject to decoherence

15. What operation does the NS gate implement?

   ○ $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle \rightarrow a\,|0\rangle - b\,|1\rangle$
   ○ $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle + c\,|2\rangle \rightarrow a\,|0\rangle + b\,|1\rangle + c\,|3\rangle$
   ○ $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle + c\,|2\rangle \rightarrow a\,|0\rangle + b\,|1\rangle - c\,|3\rangle$
   ○ $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle + c\,|2\rangle \rightarrow b\,|1\rangle - c\,|3\rangle$

16. Choose the Hamiltonian of the harmonic oscillator

   ○ $H = \frac{p^2}{2}$
   ○ $H = \frac{\omega^2 q^2}{2}$
   ○ $H = \frac{p^2}{2} + \frac{\omega^2 q^2}{2}$

17. What is the name of the operator $\{F, G\} = \frac{\partial F}{\partial q}\frac{\partial G}{\partial p} - \frac{\partial F}{\partial p}\frac{\partial G}{\partial q}$

   ○ Poisson brackets
   ○ Pauli brackets
   ○ commutator

18. How do Poisson brackets change in canonical quantisation?

   ○ $\{F, G\} \rightarrow [\hat{F}, \hat{G}]$
   ○ $\mathrm{i}\hbar\{F, G\} \rightarrow [\hat{F}, \hat{G}]$
   ○ $\hbar\{F, G\} \rightarrow [\hat{F}, \hat{G}]$

19. What does the commutator relation look like between the operator $\hat{a}$ and $\hat{a}^\dagger$?

   ○ $[\hat{a}, \hat{a}^\dagger] = 1$
   ○ $[\hat{a}, \hat{a}^\dagger] = \frac{1}{2}$
   ○ $[\hat{a}, \hat{a}^\dagger] = \mathrm{i}\hbar$

20. Choose the operator for which the Fock state is an eigenstate?

   ○ $\hat{n} = \hat{a}^\dagger\hat{a}$
   ○ $\hat{a}^\dagger$
   ○ $\hat{a}$

21. What operator is called the annihilation operator?

   ○ $\hat{n} = \hat{a}^\dagger \hat{a}$
   ○ $\hat{a}^\dagger$
   ○ $\hat{a}$

22. What is the eigenvalue of the number of particles operator $\hat{n}$ in the state $\hat{a}^\dagger |n\rangle$?

   ○ n
   ○ $n+1$
   ○ $n-1$

23. How to define the Fock state with the number n using creation operators $\hat{a}^\dagger$?

   ○ $\hat{n} = \left(\hat{a}^\dagger\right)^n |0\rangle$
   ○ $\hat{n} = \frac{1}{\sqrt{n!}} (\hat{a})^n |0\rangle$
   ○ $\hat{n} = \frac{1}{\sqrt{n!}} \left(\hat{a}^\dagger\right)^n |0\rangle$
   ○ $\hat{n} = \hat{a} |0\rangle$

24. What is the variance of the generalised coordinate operator in the Fock state?

   ○ $\Delta \hat{q}^2 = \hbar\omega(n + \frac{1}{2})$
   ○ $\Delta \hat{q}^2 = n + \frac{1}{2}$
   ○ $\Delta \hat{q}^2 = \frac{\hbar}{\omega}(n + \frac{1}{2})$

25. Choose the correct uncertainty relation between the generalised coordinate and the momentum for the vacuum state:

   ○ $\Delta\hat{q}\Delta\hat{p} = \frac{3\hbar}{2}$
   ○ $\Delta\hat{q}\Delta\hat{p} = \frac{\hbar}{2}$
   ○ $\Delta\hat{q}\Delta\hat{p} = \frac{5\hbar}{2}$
   ○ $\Delta\hat{q}\Delta\hat{p} = \hbar$

26. Choose the operator for which the Coherent state is an eigenstate?

   ○ $\hat{n} = \hat{a}^\dagger \hat{a}$
   ○ $\hat{a}^\dagger$
   ○ $\hat{a}$

27. What basis do coherent states form?

   ○ complete basis
   ○ overcomplete basis
   ○ non-complete basis

28. What is the average value of the generalised momentum operator in a coherent state $|\alpha\rangle$?

   ○ $\langle\hat{p}\rangle = \sqrt{2\hbar\omega}\mathrm{Im}(\alpha)$
   ○ $\langle\hat{p}\rangle = \sqrt{\frac{2\hbar}{\omega}}\mathrm{Re}(\alpha)$
   ○ $\langle\hat{p}\rangle = \sqrt{2\hbar\omega}\alpha$
   ○ $\langle\hat{p}\rangle = 2\hbar\omega\mathrm{Im}(\alpha)$

29. What operator is used to relate the coherent state $|\alpha\rangle$with the vacuum state $|0\rangle$?

    ○ $\hat{n} = \hat{a}^\dagger\hat{a}$
    ○ $\hat{D}(\alpha) = \mathrm{e}^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$
    ○ $\hat{S}(r) = \mathrm{e}^{\frac{1}{2}r\left(\hat{a}^2 - (\alpha\hat{a}^\dagger)^2\right)}$

30. What operator is used to relate the squeezed and coherent states of the field?

    ○ $\hat{n} = \hat{a}^\dagger\hat{a}$
    ○ $\hat{D}(\alpha) = \mathrm{e}^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$
    ○ $\hat{S}(r) = \mathrm{e}^{\frac{1}{2}r\left(\hat{a}^2 - (\alpha\hat{a}^\dagger)^2\right)}$

31. What is the x-quadrature variance in the squeezed state?
    (The parameter $r > 0$)

    ○ $\Delta\hat{X}^2 = \frac{1}{4}\mathrm{e}^{-2r},\ \Delta\hat{Y}^2 = \frac{1}{4}\mathrm{e}^{2r}$
    ○ $\Delta\hat{X}^2 = \frac{1}{4}\mathrm{e}^{2r},\ \Delta\hat{Y}^2 = \frac{1}{4}\mathrm{e}^{-2r}$
    ○ $\Delta\hat{X}^2 = \Delta\hat{Y}^2 = \frac{1}{4}$

32. Choose the right uncertainty relation between $\hat{X} = \frac{1}{2}(\hat{a}+\hat{a}^\dagger)$ and $\hat{Y} = \frac{1}{2\mathrm{i}}(\hat{a}-\hat{a}^\dagger)$ quadratures for the squeezed state?

    ○ $\Delta\hat{X}\Delta\hat{Y} = \frac{1}{4}\mathrm{e}^{-4r}$
    ○ $\Delta\hat{X}\Delta\hat{Y} = \frac{1}{4}$
    ○ $\Delta\hat{X}\Delta\hat{Y} = \frac{\hbar}{4}$
    ○ $\Delta\hat{X}\Delta\hat{Y} = 1$

33. For calculating which average values it is most convenient to use the Glauber-Sudarshan P representation?

    ○ normal ordered operators
    ○ anti-normal ordered operators
    ○ symmetric ordered operators

34. Is the Husimi Q function positive-definite?

35. For calculating which average values it is most convenient to use the Husimi representation?

    ○ normal ordered operators
    ○ anti-normal ordered operators
    ○ symmetric ordered operators

36. If we integrate the Wigner function over one quadrature, we get:

    ○ Probability distribution by another quadrature
    ○ 0
    ○ 1

37. What condition must the Wigner function satisfy for the state to be Gaussian?

    ○ It must be non-Gaussian
    ○ It must be a Gaussian function
    ○ It must be positive-definite

38. What is the minimum number of moments to describe any Gaussian state?

    ○ First, second, and third moment

    ○ First and second moment

    ○ The first four moments

39. What does the vacuum state covariance matrix look like?

    ○ $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

    ○ $\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

    ○ $\sigma = \begin{pmatrix} \mathrm{e}^{-2r} & 0 \\ 0 & \mathrm{e}^{2r} \end{pmatrix}$

40. Choose the correct definition of Gaussian transformations:

    ○ Gaussian transformations are transformations that can only be applied to Gaussian state

    ○ Gaussian transformations are transformations that do not deduce Gaussian states from Gaussian states from the Gaussian class

    ○ Gaussian transformations are transformations that convert non-Gaussian states to Gaussian ones

41. Suppose that we can apply transformations with Hamiltonians $\hat{H}_1$ and $\hat{H}_2$ to the system. Can we also apply the transformation $\hat{H}_3 = \Big[[\hat{H}_1, \hat{H}_2], \hat{H}_1\Big]$ to this system?

42. Choose the transformations you need to be able to perform in order to implement an universal quantum computation?

    ○ Arbitrary Gaussian transformations and non-Gaussian transformation

    ○ One arbitrary non-Gaussian transformation and one arbitrary Gaussian transformation

    ○ One Gaussian transformation and arbitrary Gaussian transformations

43. Is it possible to implement universal quantum transformations using quadrature displacement, squeezing, and CZ transformations?

44. What is the first step in an one-way quantum computation?

    ○ Implementation of a local measurement

    ○ Creation of a cluster state

    ○ Mixing input states to cluster state

45. Which states required to generate a continuous-variable cluster state?

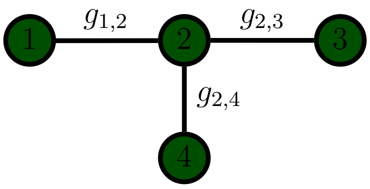
    ○ Squeezed states

    ○ Coherent states

    ○ Fock states

    ○ Arbitrary Gaussian states

46. Choose the general definition of the wave function of the cluster state corresponding to this graph:



○ $|G\rangle = \mathrm{e}^{2\mathrm{i}g\hat{x}_1\hat{x}_2}\mathrm{e}^{2\mathrm{i}g\hat{x}_2\hat{x}_3}\mathrm{e}^{2\mathrm{i}g\hat{x}_2\hat{x}_4}\,|0\rangle_{y,1}\,|0\rangle_{y,2}\,|0\rangle_{y,3}\,|0\rangle_{y,4}$

○ $|G\rangle = \mathrm{e}^{2\mathrm{i}g_{1,2}\hat{x}_1\hat{x}_2}\mathrm{e}^{2\mathrm{i}g_{2,3}\hat{x}_2\hat{x}_3}\mathrm{e}^{2\mathrm{i}g_{2,4}\hat{x}_2\hat{x}_4}\,|0\rangle_{y,1}\,|0\rangle_{y,2}\,|0\rangle_{y,3}\,|0\rangle_{y,4}$

○ $|G\rangle = \mathrm{e}^{2\mathrm{i}g_{1,2}\hat{x}_1\hat{x}_3}\mathrm{e}^{2\mathrm{i}g_{2,3}\hat{x}_2\hat{x}_3}\mathrm{e}^{2\mathrm{i}g_{2,4}\hat{x}_2\hat{x}_1}\,|0\rangle_{y,1}\,|0\rangle_{y,2}\,|0\rangle_{y,3}\,|0\rangle_{y,4}$

47. Choose the correct definition of the cluster state nullifier operator

○ $\hat{y}_i - \sum_{j\in N(i)} g_{i,j}\hat{x}_j$

○ $\hat{y}_1 - \hat{y}_2 - \hat{x}_3$

○ $\hat{x}_i - \sum_{j\in N(i)} g_{i,j}\hat{x}_j$

48. What are the nullifiers in the graph of exercise 46?

○

$$\begin{aligned}&\hat{y}_1 - \hat{x}_2,\\&\hat{y}_2 - \hat{x}_1 - \hat{x}_3 - \hat{x}_4,\\&\hat{y}_3 - \hat{x}_2,\\&\hat{y}_4 - \hat{x}_2\end{aligned}$$

○

$$\begin{aligned}&\hat{y}_1 - g_{1,2}\hat{x}_2,\\&\hat{y}_2 - g_{1,2}\hat{x}_1 - g_{2,3}\hat{x}_3 - g_{2,4}\hat{x}_4,\\&\hat{y}_3 - g_{2,3}\hat{x}_2,\\&\hat{y}_4 - g_{2,4}\hat{x}_2\end{aligned}$$

○

$$\begin{aligned}&\hat{y}_1 - g_{1,2}\hat{x}_2,\\&\hat{y}_2 - g_{1,2}\hat{x}_1,\\&\hat{y}_3 - g_{2,3}\hat{x}_2,\\&\hat{y}_4 - g_{2,4}\hat{x}_2\end{aligned}$$

49. Choose the correct vector representation of the nullifier operators

○ $\hat{\boldsymbol{N}} = \hat{\boldsymbol{y}} - A\hat{\boldsymbol{x}}$

○ $\hat{\boldsymbol{N}} = \hat{\boldsymbol{y}} - \hat{\boldsymbol{x}}$

○ $\hat{\boldsymbol{N}} = \hat{\boldsymbol{x}} - A\hat{\boldsymbol{y}}$

50. What does the van Loock-Furusawa separability criterion look like for the first and second cluster nodes if the cluster state graph is the one from exercise 46?

○ $\langle\delta\hat{N}_2^2\rangle + \langle\delta\hat{N}_4^2\rangle < |g_{1,2}|$

○ $\langle\delta\hat{N}_2^2\rangle + \langle\delta\hat{N}_4^2\rangle < 1$

○ $\langle\delta\hat{N}_1^2\rangle + \langle\delta\hat{N}_2^2\rangle < |g_{1,2}|$

51. Let us assume that the nullifiers's variance for the first and second cluster state node are greater than 1/2. Will these nodes be entangled if the weight coefficient $g_{1,2}$ between them is equal to one?

○ Nodes will be entangled

○ Nodes will not be entangled

52. What transformations can be used to create a cluster state from a set of squeezed oscillators?

○ linear transformations

○ any non-linear transformation

○ cubic phase-transformations

53. What is the form of the linear transformation matrix that has to be performed to transform independent oscillators in squeezed states into oscillators in a cluster state?

○ $U = (\mathrm{I} + \mathrm{i}A)(\mathrm{I} + A)^{-1/2}Q$

○ $U = (\mathrm{I} + \mathrm{i}A)Q$

○ $U = (\mathrm{I} + \mathrm{i}A)(\mathrm{I} + A^2)^{-1/2}Q$

54. Suppose that to generate a cluster state, we use oscillators whose variance of the squeezed quadratures are less than 1/8. What is the squeezing of these oscillators in decibel units?

○ about -6dB

○ about -2dB

○ about -3dB

Chapter 15

Measurement-based quantum computation in continuous variables

15.1 Homodyne measurements

The basic concept for a **homodyne measurement** is depicted in 15.1. The beamer splitter transformation matrix U_{BS} is

$$U_{\text{BS}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and the field amplitudes after a beam splitter are

$$\begin{aligned} \hat{a}_1 &= \frac{1}{\sqrt{2}} (\hat{a} + \alpha) \\ \hat{a}_2 &= \frac{1}{\sqrt{2}} (\hat{a} - \alpha) \end{aligned}$$

Operators for the number of particles of the measured fields are

$$\begin{aligned} \hat{n}_1 = \hat{a}_1^\dagger \hat{a}_1 &= \frac{1}{2} \left(\hat{a}^\dagger \hat{a} + \alpha \hat{a}^\dagger + \alpha^* \hat{a} + |\alpha|^2 \right) \\ \hat{n}_2 = \hat{a}_2^\dagger \hat{a}_2 &= \frac{1}{2} \left(\hat{a}^\dagger \hat{a} - \alpha \hat{a}^\dagger - \alpha^* \hat{a} + |\alpha|^2 \right) \end{aligned}$$

and the result of the homodyne measurement then is

$$\hat{n}_- = \hat{n}_1 - \hat{n}_2 = 2|\alpha| \left(\cos\theta \hat{X} + \sin\theta \hat{Y} \right)$$

so that one can measure the quadratures of the system! The measurement basis is given by the local oscillator.

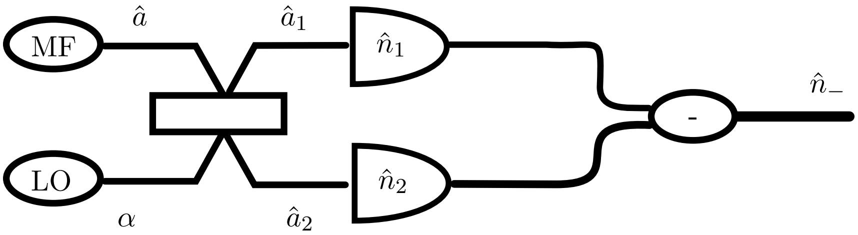


Figure 15.1: basic concept of a homodyne measurement where MF is a measurable field and LO is a local oscillator, respectively

15.2 Single mode quantum Gaussian computation

The quantum computation on a two-node cluster state is shown in Figure 15.2. The linear transformation is $U = \frac{1}{\sqrt{1+g^2}}\begin{pmatrix} 1 & \mathrm{i}g \\ \mathrm{i}g & 1 \end{pmatrix}$. Hence, the relationship between quadratures of cluster states and quadratures of squeezed oscillators is

$$\begin{pmatrix} \hat{X}_1 + \mathrm{i}\hat{Y}_1 \\ \hat{X}_2 + \mathrm{i}\hat{Y}_2 \end{pmatrix} = \frac{1}{\sqrt{1+g^2}} \begin{pmatrix} \hat{x}_{s,1} - g\hat{y}_{s,2} + \mathrm{i}\big(g\hat{x}_{s,2} + \hat{y}_{s,1}\big) \\ \hat{x}_{s,2} - g\hat{y}_{s,1} + \mathrm{i}\big(g\hat{x}_{s,1} + \hat{y}_{s,2}\big) \end{pmatrix}.$$

After a beam-splitter transformation, the quadratures become

$$\begin{aligned} \hat{X}_1' &= \frac{1}{\sqrt{2}}\left(\hat{x}_{\mathrm{in}} + \frac{1}{\sqrt{1+g^2}}\big(\hat{x}_{s,1} - g\hat{y}_{s,2}\big)\right), \\ \hat{Y}_1' &= \frac{1}{\sqrt{2}}\left(\hat{y}_{\mathrm{in}} + \frac{1}{\sqrt{1+g^2}}\big(g\hat{x}_{s,2} + \hat{y}_{s,1}\big)\right), \\ \hat{x}_{\mathrm{in}}' &= \frac{1}{\sqrt{2}}\left(\hat{x}_{\mathrm{in}} - \frac{1}{\sqrt{1+g^2}}\big(\hat{x}_{s,1} - \hat{y}_{s,2}\big)\right), \\ \hat{y}_{\mathrm{in}}' &= \frac{1}{\sqrt{2}}\left(\hat{x}_{\mathrm{in}} - \frac{1}{\sqrt{1+g^2}}\big(\hat{x}_{s,2} - \hat{y}_{s,1}\big)\right). \end{aligned}$$

With this the amplitudes of the photocurrents in a homodyne measurement are

$$\begin{cases} \hat{I}_1 = \cos\theta_1 \hat{X}_1' + \sin\theta_1 \hat{Y}_1 \\ \hat{I}_2 = \cos\theta_2 \hat{x}_{\mathrm{in}}' + \sin\theta_2 \hat{y}_{\mathrm{in}} \end{cases}.$$

This system can be solved with respect to stretching quadratures

$$\begin{aligned} \hat{x}_{s,1} &= f\big(\hat{x}_{\mathrm{in}}, \hat{y}_{\mathrm{in}}, \hat{y}_{s,1}, \hat{y}_{s,2}\big) \\ \hat{x}_{s,2} &= g\big(\hat{x}_{\mathrm{in}}, \hat{y}_{\mathrm{in}}, \hat{y}_{s,1}, \hat{y}_{s,2}\big) \end{aligned}$$

and furthermore, the obtained solution must be substituted into the unmeasured quadratures $\hat{X}_2$ and $\hat{Y}_2$.

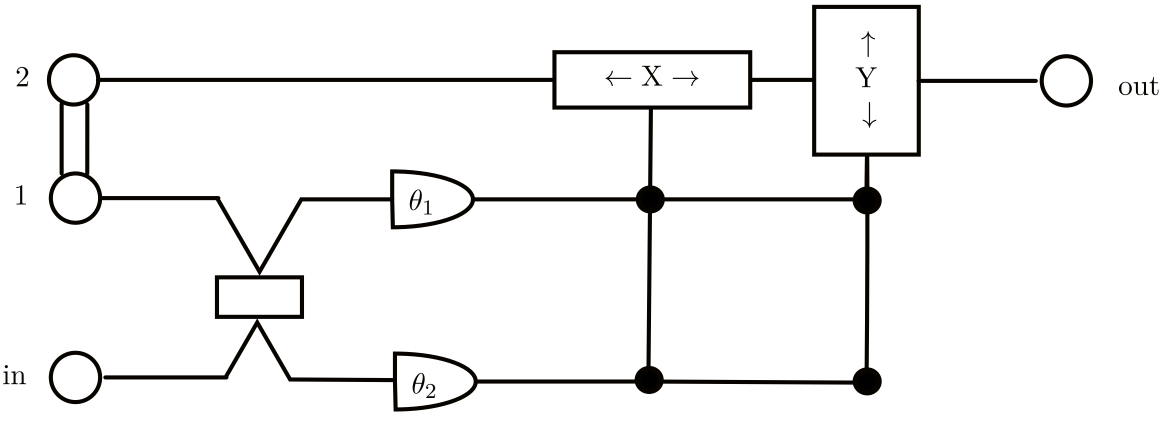


Figure 15.2: quantum computation on a two-node cluster state

As a result, we get an expression describing the change in the unmeasured quadratures

$$\begin{pmatrix}\hat{X}_2'\\ \hat{Y}_2'\end{pmatrix} = \frac{1}{\sin\theta_-}\begin{pmatrix}1/g & 0\\ 0 & g\end{pmatrix}\begin{pmatrix}\cos\theta_+ + \cos\theta_- & \sin\theta_+\\ -\sin\theta_+ & \cos\theta_+ - \cos\theta_-\end{pmatrix}\begin{pmatrix}\hat{x}_{\text{in}}\\ \hat{y}_{\text{in}}\end{pmatrix} + \sqrt{1+g^2}\begin{pmatrix}\hat{y}_{s,1}/g\\ y_{s,2}\end{pmatrix}$$
$$+\frac{\sqrt{2}}{\sin\theta_-}\begin{pmatrix}1/g & 0\\ 0 & g\end{pmatrix}\begin{pmatrix}\cos\theta_2 & \cos\theta_1\\ -\sin\theta_2 & -\sin\theta_1\end{pmatrix}\begin{pmatrix}\hat{I}_1\\ \hat{I}_2\end{pmatrix}$$

where $\theta_\pm = \theta_1 \pm \theta_2$.

For our expressions to reflect the entire physics of the process of quantum computing, we need to replace the operators of the photocurrent with real numbers, i.e.

$$\hat{I}_1 \to I_1, \quad \hat{I}_2 \to I_2.$$

Applying the operators to the output states:

$$\hat{X} = \left(\sqrt{2}\frac{\cos\theta_2 I_1 + \cos\theta_1 I_2}{g\sin\theta_-}\right) \text{ and } \hat{Z} = \left(\sqrt{2}g\frac{-\sin\theta_2 I_1 - \sin\theta_1 I_2}{\sin\theta_-}\right)$$

we can fully compensate for the classical term. The resulting state after a displacement of the quadratures is

$$\begin{pmatrix}\hat{x}_{\text{out}}\\ \hat{y}_{\text{out}}\end{pmatrix} = \frac{1}{\sin\theta_-}\begin{pmatrix}1/g & 0\\ 0 & g\end{pmatrix}\begin{pmatrix}\cos\theta_+ + \cos\theta_- & \sin\theta_+\\ -\sin\theta_+ & \cos\theta_+ - \cos\theta_-\end{pmatrix}\begin{pmatrix}\hat{x}_{\text{in}}\\ \hat{y}_{\text{in}}\end{pmatrix} + \sqrt{1+g^2}\begin{pmatrix}\hat{y}_{s,1}/g\\ y_{s,2}\end{pmatrix}.$$

The main transformation can be decomposed into the product of the simplest rotation and squeezing matrices

$$\begin{pmatrix}\hat{x}_{\text{out}}\\ \hat{y}_{\text{out}}\end{pmatrix} = S[\log g]R(-\frac{1}{2}\theta_+)S(\log[\tan\frac{\theta_-}{2}])R(-\frac{1}{2}\theta_+)\begin{pmatrix}\hat{x}_{\text{in}}\\ \hat{y}_{\text{in}}\end{pmatrix} + \sqrt{1+g^2}\begin{pmatrix}\hat{y}_{s,1}/g\\ \hat{y}_{s,2}\end{pmatrix}.$$

According to the Bloch-Messiah reduction theorem, the universal single mode Gaussian transformation must decompose into the product of three matrices: rotation, squeezing, and other rotation $U = R(\phi_1)S[r]R(\phi_2)$. The transformation matrix in our case is decomposed as follows:

$$U_1 = R\left(-\frac{1}{2}\theta_+\right)S\left[\log\left(\tan\frac{\theta_-}{2}\right)\right]R\left(-\frac{1}{2}\theta_+\right).$$

We see that the transformation we receive is very close to universal.

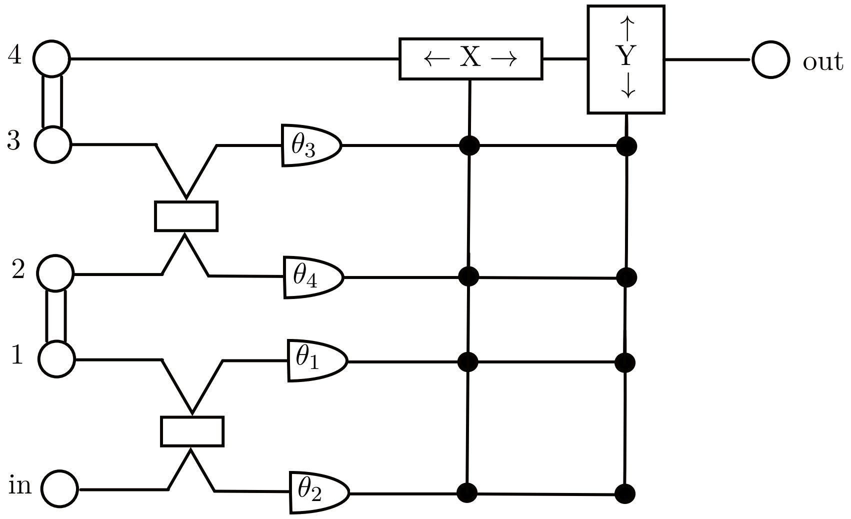


Figure 15.3: Quantum computation on two two-node cluster states realising a universal Gaussian transformation

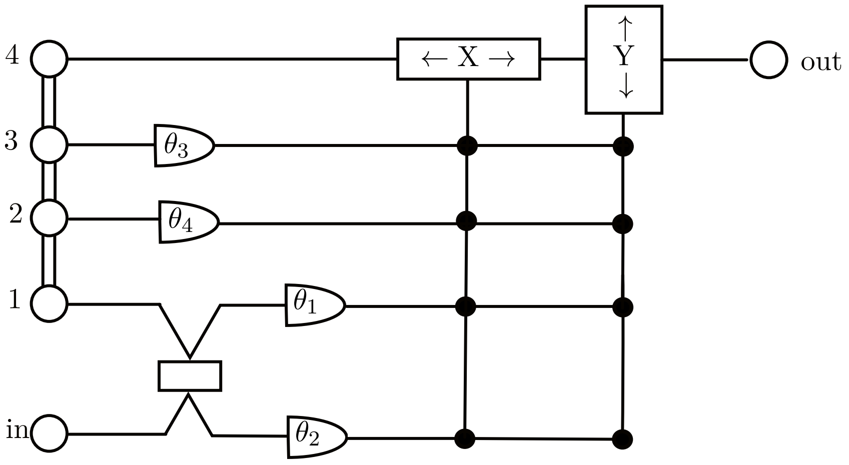


Figure 15.4: Quantum computation on one four-node cluster state realising a universal Gaussian transformation

Let us send the computation result from a two-node cluster state to another using exactly the same computation scheme like in Figure 15.3. The result of the calculations on a pair of two-node cluster states is

$$\begin{pmatrix} \hat{x}'_{\text{out}} \\ \hat{y}'_{\text{out}} \end{pmatrix} = \tilde{U} \begin{pmatrix} \hat{x}_{\text{in}} \\ \hat{y}_{\text{in}} \end{pmatrix} + U_2 \begin{pmatrix} \hat{y}_{s,1} \\ \hat{y}_{s,2} \end{pmatrix} + \begin{pmatrix} \hat{y}_{s,3} \\ \hat{y}_{s,4} \end{pmatrix}.$$

where the transformation matrix $\tilde{U}$ is

$$\tilde{U} = U_1 U_2 = R\left(-\frac{1}{2}\theta_{+,2}\right) S\left[\log\left(\tan\frac{\theta_{-,2}}{2}\right)\right] R\left(-\frac{1}{2}\theta_{+,2}\right) R\left(-\frac{1}{2}\theta_{+,1}\right) S\left[\log\left(\tan\frac{\theta_{-,1}}{2}\right)\right] R\left(-\frac{1}{2}\theta_{+,1}\right).$$

If in such a transformation we put $\theta_{-,2} = \frac{\pi}{2}$, then we get

$$\tilde{U} = U_1 U_2 = R\left(-\frac{1}{2}\theta_{-,1} - \theta_{+,2}\right) S\left[\log\left(\tan\frac{\theta_{-,1}}{2}\right)\right] R\left(-\frac{1}{2}\theta_{+,1}\right).$$

Therefore, a pair of two-node cluster states is sufficient to implement a universal Gaussian transformation.

It is also possible to realise a universal Gaussian transformation on a four-node cluster state as shown in Figure 15.4.

The main stages in obtaining an result of one-way quantum computations on a four-node cluster state:

1. get the relation between a cluster state's quadratures and the squeezed oscillators quadratures
2. write down the beam splitter transformation for the quadrature of the input state and the state of the first node of the cluster
3. write four equations for the photocurrents of the measured quadratures
4. solve these equations for stretched quadratures and substitute the solution into the quadratures of the unmeasured state

The final expression is

$$\begin{aligned} \begin{pmatrix} \hat{x}_{\text{out}} \\ \hat{y}_{\text{out}} \end{pmatrix} &= \begin{pmatrix} \cot\theta_4 \cot\theta_3 - 1 & \cot\theta_4 \\ -\cot\theta_3 & -1 \end{pmatrix} R\left(-\frac{1}{2}\theta_+\right) S\left[\log\left(\tan\frac{\theta_-}{2}\right)\right] R\left(-\frac{1}{2}\theta_+\right) \begin{pmatrix} \hat{x}_{\text{in}} \\ \hat{y}_{\text{in}} \end{pmatrix} \\ &+ \hat{\boldsymbol{E}}_r(\hat{y}_{s,1}, \hat{y}_{s,2}, \hat{y}_{s,3}, \hat{y}_{s,4}) \end{aligned}$$

where $\theta_\pm = \theta_1 \pm \theta_2$ and $\hat{\boldsymbol{E}}_r$ is an error vector proportional to the squeezed quadratures.

15.3 Two-mode CZ transformation

The two-mode CZ-transformation can be implemented using a four-node linear cluster state with the adjacency matrix

$$A_4' = \begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

It is realised by the scheme in Figure 15.5. Choosing the angles $\theta_3 = \theta_2 = -\theta_1 = -\theta_4 = \pi/2$. the transformation of the unmeasured states is

$$\begin{pmatrix} \hat{X}_{\text{out},1} \\ \hat{X}_{\text{out},2} \\ \hat{Y}_{\text{out},1} \\ \hat{Y}_{\text{out},2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \hat{x}_{\text{in},1} \\ \hat{x}_{\text{in},2} \\ \hat{y}_{\text{in},1} \\ \hat{y}_{\text{in},2} \end{pmatrix}.$$

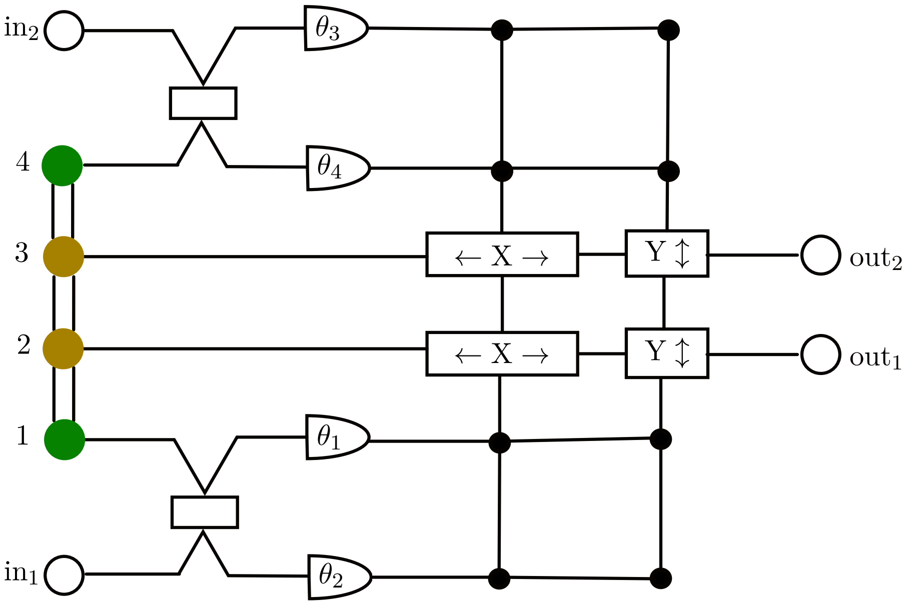


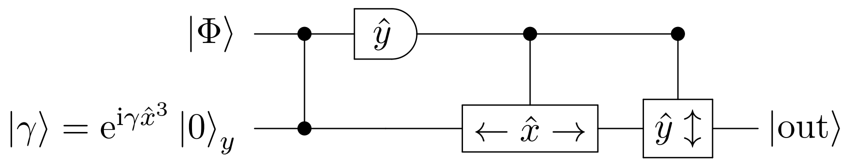
Figure 15.5: Realisation of a two-mode CZ-transformation using a linear four-node cluster state (same phases in same colours)

15.4 Non-Gaussian operations and difficulties in implementing continuous variable computations

We still have to implement a non-Gaussian transformation after the single-node Gaussian universal transformation. Let us consider the cubic phase transformation $\hat{H}_1 = \gamma \hat{x}^3$. Such a Hamiltonian transforms the quadratures of the input states in the form:

$$\hat{x}_{\text{out}} = \hat{x}_{\text{in}}, \quad \hat{y}_{\text{out}} = \hat{y}_{\text{in}} - \frac{3}{2}\gamma \hat{x}_{\text{in}}^2.$$

Non-linear transformations of quadratures occur in parametric processes. Coupling constants are small ($\gamma \ll 1$). For arbitrary quantum computing, we need transformations with arbitrary γ. Hence, parametric transformations are not suitable for us. The implementation scheme of the cubic phase transformations is


$|\Phi\rangle$
$\hat{y}$
$|\gamma\rangle = \mathrm{e}^{\mathrm{i}\gamma\hat{x}^3}\,|0\rangle_y$
$\leftarrow \hat{x} \rightarrow$
$\hat{y} \updownarrow$
$|\mathrm{out}\rangle$

The result of the computation on the presented scheme is

$$|\mathrm{out}\rangle = R(\frac{\pi}{2})\left(\mathrm{e}^{\mathrm{i}\gamma\hat{x}^3}\,|\Phi\rangle\right).$$

Annihilation operators for the first and second states are

$$\hat{a}_1 = \hat{x}_1 + \mathrm{i}\left(\hat{y}_1 - \frac{3}{2}\gamma\hat{x}_1^2\right), \quad \hat{a}_{\mathrm{in}} = \hat{x}_{\mathrm{in}} + \mathrm{i}\hat{y}_i n.$$

We entangle the states by using the CZ-transformation

$$\hat{a}_1' = \hat{x}_1 + \mathrm{i}\left(\hat{y}_1 - \frac{3}{2}\gamma\hat{x}_1^2 + \hat{x}_{\mathrm{in}}\right), \quad \hat{a}_{\mathrm{in}}' = \hat{x}_{\mathrm{in}} + \mathrm{i}\left(\hat{y}_i n + \hat{x}_1\right).$$

and measure the y-quadrature for the first state:

$$y_m = \hat{y}_{\mathrm{in}} + \hat{x}_1 \;\Rightarrow \hat{x}_1 = y_m - \hat{y}_{\mathrm{in}}.$$

Substituting the resulting value into the unmeasured quadratures, we get

$$\hat{a}_{\mathrm{out}} = -\hat{y}_{\mathrm{in}} + \mathrm{i}\left(\hat{x}_{\mathrm{in}} + \frac{3}{2}\gamma\hat{y}_i n^2 + \hat{y}_1\right).$$

The cubic phase transformation is implemented in the following scheme with a two-node cluster state in Figure 15.6. Here, S_1 and S_2 are oscillators in squeezed vacuum states

$$\langle\delta y_1^2\rangle = \langle\delta y_2^2\rangle = \frac{1}{4}\mathrm{e}^{-2r}$$

with a $\hat{x}$-quadrature displacement $d \gg r$. As the states are correlated after the CZ-transformation, it follows that knowing the quadratures of one state, we can know the quadratures of another state, too.

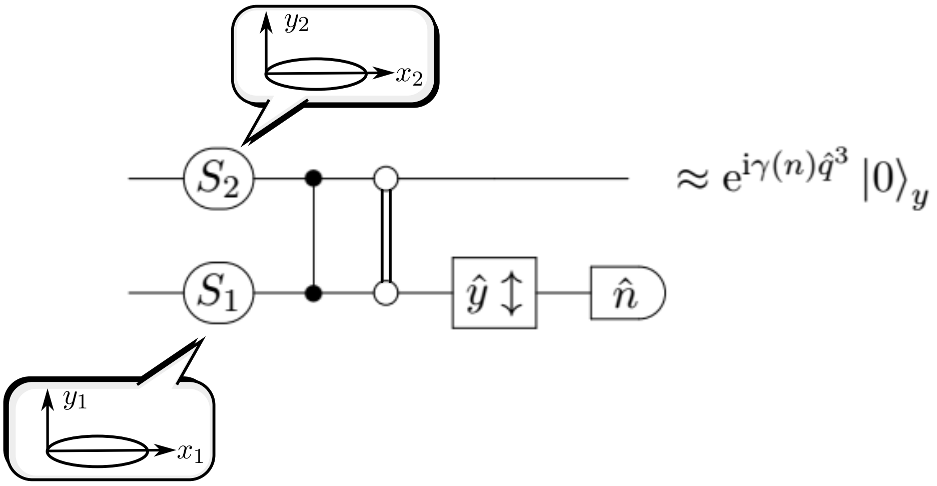
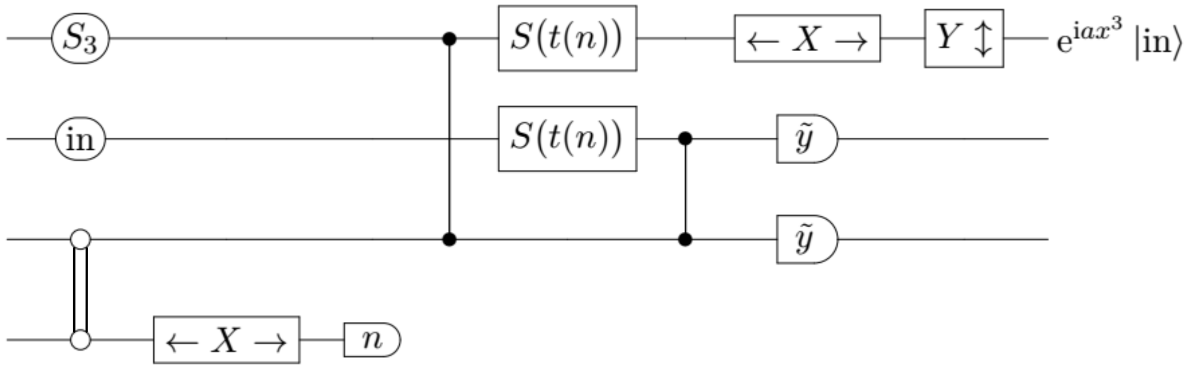

y_2
x_2
S_2
$\approx \mathrm{e}^{\mathrm{i}\gamma(n)\hat{q}^3}\,|0\rangle_y$
S_1
$\hat{y} \updownarrow$
$\hat{n}$
y_1
x_1

Figure 15.6: Scheme for generating a cubic phase transformation with a two-node cluster state

The Figure 15.7 illustrate this. The implementation scheme of the complete cubic phase transformation is


S_3
in
$S(t(n))$
$S(t(n))$
$\leftarrow X \rightarrow$
$Y \updownarrow$
$e^{iax^3}|\text{in}\rangle$
$\tilde{y}$
$\tilde{y}$
$\leftarrow X \rightarrow$
n

If we choose $t(n) = \left(\frac{a}{\gamma(n)}\right)^{1/3}$, then this scheme can implement the transformation of the cubic phase.

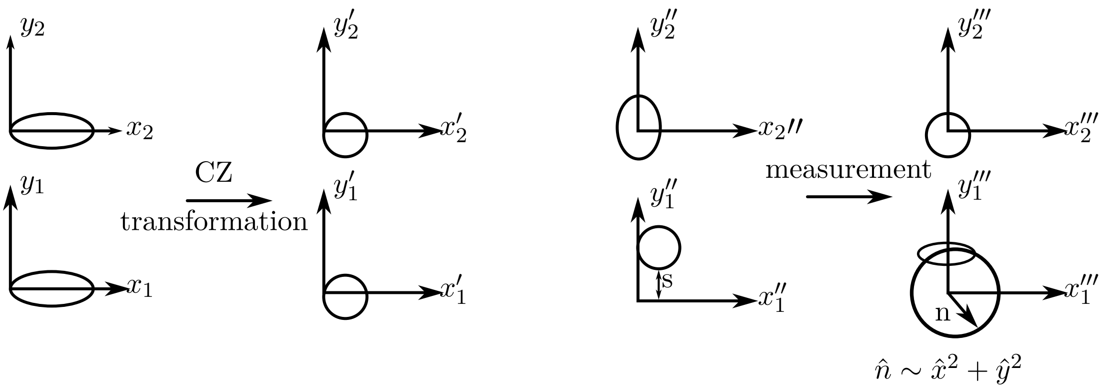


Figure 15.7: Effect of the transformations realising the cubic phase transformation.

15.5 Difficulties implementing continuous variable one-way quantum computations

The advantage of one-way quantum computation in continuous variables is that cluster states with an arbitrary graph $\mathcal{G}$ are generated deterministically.

The disadvantage is that as the number of nodes in a cluster state grows, the error in the calculation results will accumulate. For the schemes presented to be resistant against the accumulation of errors, one needs well squeezed oscillators of -18dB to -20.5dB. The maximum of squeezing implemented as of the time this is written is -15dB. Furthermore, the experimental implementation of a non-Gaussian transformation is of a high complexity. To implement cubic phase transformations in the described circuit, we need to apply quadrature displacement operations. The magnitude of the shift should be greater than the variance of the stretched quadratures of the oscillators. For such a a displacement, according to a rough estimate, we need a field with an energy of several Megajoule. Hence, we need to implement error correcting codes. These we discuss in the next chapter.

15.6 Exercises

1. What field characteristics can be measured with homodyne detectors?

   ○ Combinations of field quadratures
   ○ field frequency
   ○ field polarisation

2. What is the final stage of continuous variable one-way quantum computations?

   ○ Displacement of x and y quadratures
   ○ Creating a cluster state
   ○ Local homodyne measurements

3. What cluster states are needed to implement universal single-mode Gaussian transformations?

   ○ A pair of two-node cluster states
   ○ A two-node cluster state
   ○ A four-node linear cluster state
   ○ A three-node cluster state

4. What is the minimum number of nodes that must be in a cluster state in order to be able to implement the two-mode Gaussian CZ transformation?

   ○ 2
   ○ 3
   ○ 4
   ○ 5

5. With the help of the measurement of which operator can the transformation of the cubic phase be realised?

   ○ Particle number operator $\hat{n}$
   ○ Quadrature operator $\hat{x}$
   ○ Quadrature operator $\hat{y}$
   ○ Combination of quadrature operators

6. What are the main difficulties for practical implementation of the cubic phase transformation?

   ○ Difficulty of measuring the particle number operator
   ○ The problem of creating a two-mode entangled state
   ○ Difficulty in the practical implementation of quadrature displacement transformations with large displacement parameters

Chapter 16

Quantum codes for error correction for measurement-based quantum computing

Errors in the n-qubit state can be expressed by operators of the set $\{\mathrm{I}, \mathrm{X}, \mathrm{Z}, \mathrm{Y}\}^{\otimes n}$. Any evolution under the influence of unitary errors for the n-qubit state $|\Phi\rangle$ and its environment can be written as the following superposition

$$|\Phi\rangle \otimes |0\rangle_E \to \sum_a E_a |\Psi\rangle \otimes |e_a\rangle_E$$

with the index a running over all 2^{2n} values, E_a being the n-qubit Pauli operators, and $|e_a\rangle$ are the states of the environment.
We are assigning a weight to each operator from the Pauli group $P_n = \{\mathrm{I}, \mathrm{X}, \mathrm{Z}, \mathrm{Y}\}^{\otimes n}$. The weight is an integer $0 \leq t \leq n$ indicating the number of qubits acted upon by non-trivial (non-unit) Pauli operators. Take for example the Pauli operators

- with weight equal to one

$$\mathrm{X} \otimes \mathrm{I} \otimes \mathrm{I} \otimes \mathrm{I},$$
$$\mathrm{I} \otimes \mathrm{Z} \otimes \mathrm{I} \otimes \mathrm{I},$$
$$\mathrm{I} \otimes \mathrm{I} \otimes \mathrm{I} \otimes \mathrm{Y}.$$

- with weight equal to three

$$\mathrm{X} \otimes \mathrm{X} \otimes \mathrm{Z} \otimes \mathrm{I},$$
$$\mathrm{I} \otimes \mathrm{Z} \otimes \mathrm{Y} \otimes \mathrm{Y},$$
$$\mathrm{X} \otimes \mathrm{Z} \otimes \mathrm{I} \otimes \mathrm{Y}.$$

To construct a quantum error correction code, we need to select the error operators that we want to correct, e.g. errors with weight not greater than some t. All errors form a subgroup of the Pauli group P_n:

$$\mathcal{E} = \{E_a^k\}_{k=1}^t \subset P_n$$

For example, suppose we have a five qubit code and we want to correct errors with a weight of no more than two. In this case, we must be able to correct all 15 errors with weight one:

$$\{\mathrm{X} \otimes \mathrm{I} \otimes \mathrm{I} \otimes \mathrm{I}, \mathrm{Y} \otimes \mathrm{I} \otimes \mathrm{I} \otimes \mathrm{I}, \mathrm{Z} \otimes \mathrm{I} \otimes \mathrm{I} \otimes \mathrm{I}, \ldots, \mathrm{I} \otimes \mathrm{I} \otimes \mathrm{I} \otimes \mathrm{Z}\}$$

and all 90 errors with weight two:

$$\{\mathrm{X} \otimes \mathrm{X} \otimes \mathrm{I} \otimes \mathrm{I}, \mathrm{X} \otimes \mathrm{Y} \otimes \mathrm{I} \otimes \mathrm{I}, \mathrm{X} \otimes \mathrm{Z} \otimes \mathrm{I} \otimes \mathrm{I}, \ldots, \mathrm{I} \otimes \mathrm{I} \otimes \mathrm{Z} \otimes \mathrm{Z}\}$$

In all quantum error correction codes, k qubits that one wants to correct are encoded by $n > k$ qubits. To construct the theory of quantum error correcting codes, we need to highlight the main properties of the elements of the Pauli group P_n:

- each element of P_n is unitary
- $\forall M \in P_n$, either $M^2 = \mathrm{I}$ or $M^2 = -1$
- either two elements M and N from P_M commute $big[M, N]\_ = 0$ or anti-commute $\{M, N\}_+ = 0$

Choose the subgroup $S \subset P_n$ which consists of commuting operators, i.e. $M, N \in S \; big[M, N]\_ = 0 \forall M, N \in S$. This subgroup defines a common eigenspace $\mathcal{H}_S \subset \mathcal{H}_{2^n}$ which is called **code space**. The properties of this space are

- if the group S has $n-k$ generators, the space $\mathcal{H}_S$ has 2^k dimensions
- operators from the group S are stabilizers for states from $\mathcal{H}_S$ that is $\forall \left|\Phi\right\rangle \in \mathcal{H}_S$ and $\forall M \in S \; M\left|\Phi\right\rangle = \left|\Phi\right\rangle$

The constructed code is capable of correcting errors whose operators $E_a \in \mathcal{E}$ anti-commute with operators from the group S. Indeed, let $E_a \in \mathcal{E}$ anti-commute with $M \in S$, then for $\left|\Psi\right\rangle \in \mathcal{H}_S$:

$$ME_a \left|\Psi\right\rangle = -E_a M \left|\Psi\right\rangle = -E_a \left|\Psi\right\rangle .$$

This means that the state $E_a \left|\Psi\right\rangle$ is an eigenstate of M with eigenvalue -1. If the eigenvalue of the operator M is equal to -1, then the state is affected by the error E_a.
A necessary and sufficient condition for error correction in the quantum case is

$${}_L\langle i|E_a^\dagger E_b \left|j\right\rangle_L = \delta_{ab}\delta_{ij}$$

where $\left|i\right\rangle_L$ and $\left|j\right\rangle_L$ are two code words that belong to the space $\mathcal{H}_S$. E_a and E_b are two different mistakes that we want to correct. Take the three qubit code for bit-flip errors: Three physical qubits are used to encode one logical bit ($n = 3$ and $k = 1$). Here, $\mathcal{E} = \{\mathrm{X}\otimes\mathcal{I}\otimes\mathrm{I}, \mathrm{I}\otimes\mathcal{X}\otimes\mathrm{I}, \mathrm{I}\otimes\mathcal{I}\otimes\mathrm{X}\}$. Selecting from the three qubit Pauli group all operators that commute with each other and anti-commute with operators from $\mathcal{E}$, we obtain the following stabilizers $= \{\mathrm{Z}\otimes\mathcal{Z}\otimes\mathrm{I}, \mathrm{I}\otimes\mathcal{Z}\otimes\mathrm{Z}, \mathrm{Z}\otimes\mathcal{I}\otimes\mathrm{Z}\}$. This code defines a logical qubit with the following eigenstates:

$$\left|0\right\rangle_L = \left|000\right\rangle , \quad \left|1\right\rangle_L = \left|111\right\rangle .$$

For the three-qubit phase errors:

$$\begin{aligned} \mathcal{E}_1 &= \{\mathrm{Z}\otimes\mathcal{I}\otimes\mathrm{I}, \mathrm{I}\otimes\mathcal{Z}\otimes\mathrm{I}, \mathrm{I}\otimes\mathcal{I}\otimes\mathrm{Z}\}, \\ S_1 &= \{\mathrm{X}\otimes\mathrm{X}\otimes\mathrm{I}, \mathrm{I}\otimes\mathrm{X}\otimes\mathrm{X}, \mathrm{X}\otimes\mathrm{I}\otimes\mathrm{X}\}, \\ \left|+\right\rangle_L &= \left|+++\right\rangle , \quad \left|-\right\rangle_L = \left|---\right\rangle . \end{aligned}$$

16.1 Hamming Bound

The number of errors with weight m in an n-qubit code is given by the following expression:

$$\chi(m) = 3^m \binom{n}{m} .$$

The total number of errors with a weight not exceeding t is given by the sum:

$$N(t) = \sum_{m=1}^{t} 3^m \binom{n}{m} .$$

If we have k logical qubits and want to use them to correct any errors with a weight of at most t, then we must have a quantum space of dimension n which contains all $N(t)2^k$ states. In other words, the following condition must be met:

$$N(t)2^k \leq 2^n \quad \textbf{(Hamming quantum bound)}$$

The Hamming bound in case of encoding a single qubit ($k = 1$) that is robust to any one-qubit errors ($t = 1$), is $2 \cdot (1 + 3n) \leq 2^n$. This condition starts to be fulfilled at $n = 5$, i.e. to correct any one qubit error, we need to use a quantum code that is encoded with five or more qubits. In case of the nine qubit code

$$|0\rangle_L = \frac{1}{2\sqrt{2}}\big(\,|000\rangle + |111\rangle\,\big)^{\otimes 3},$$
$$|1\rangle_L = \frac{1}{2\sqrt{2}}\big(\,|000\rangle - |111\rangle\,\big)^{\otimes 3}.$$

The algorithm for constructing a quantum error correction code follows these steps:

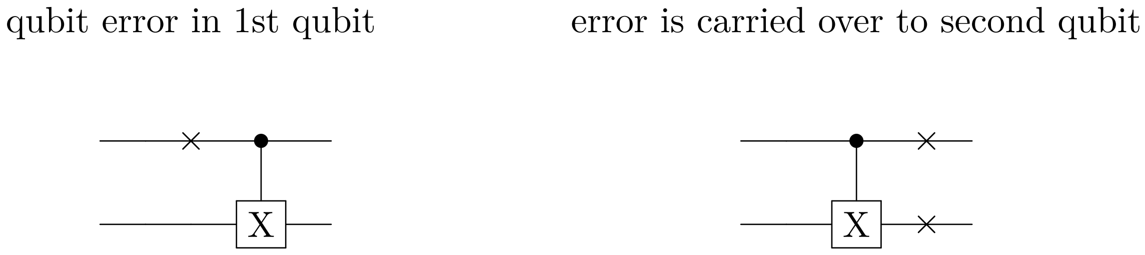
1. decide on the errors that can occur in our quantum system
2. based on the Hamming bound, one has to determine how many physical qubits are enough to encode a logical qubit that is resistant to these errors
3. match operators to all errors
4. choose operators from Pauli group that commute with each other and anti-commute with the error operators → these operators define the space of error-resistant codewords

16.2 Fault-tolerant quantum computation and displacement errors

The root causes of quantum computing errors are:

- errors in qubits
- errors in quantum gates
- increased errors in quantum transformations

e.g. look at the increased errors in a CNOT transformation



A computation scheme is fault-tolerant if a failure in one component of the scheme results in at most one error in each output block of qubits. The computation scheme will be non-fault tolerant, if two or more errors appear in each logical qubit at each computation stage. Let the computational error in one physical qubit at any step of the process be equal to p, then the probability of non-fault-tolerant computations will be estimated as $\mathcal{O}(p^2)$. For most quantum computing schemes, the probability of two errors in one logical error qubit does not exceed 10^6p^2. For the error to obtain incorrect computation results that are negligible, we need the probability of errors at each step of the computation scheme be less than $p < 10^{-3}$.

16.2.1 Quadrature displacement error correcting code

The result of a continuous variable one-way quantum computation is

$$\begin{pmatrix}\hat{X}_{\text{out}}\\ \hat{Y}_{\text{out}}\end{pmatrix} = U\begin{pmatrix}\hat{x}_{\text{in}}\\ \hat{y}_{\text{in}}\end{pmatrix} + M_{\text{err}}\hat{y}_s$$

where $\hat{y}_s$ is a vector consisting of squeezing oscillators' quadratures. Quadrature displacement errors are those which cause the following transformation

$$y \rightarrow \hat{D}_y^\dagger(\nu) y \hat{D}_y^\dagger(\nu) = y + \nu, \quad x \rightarrow \hat{D}_x^\dagger(\mu) x \hat{D}_x^\dagger(\mu) = x + \mu$$

where ν, μ are random variables and $\hat{D}_x^\dagger(\mu) = \mathrm{e}^{-\mathrm{i}\mu\hat{y}}$, $\hat{D}_y^\dagger(\nu) = \mathrm{e}^{-\mathrm{i}\nu\hat{x}}$ are **displacement operators**. There are two types of displacement errors:

1. rare displacement errors by large values
2. frequent displacement errors by small values

16.2.2 Gottesman-Kitaev-Preskill states

The generators of the operator group for fault-tolerant states are $S = \left\{\mathrm{e}^{2\sqrt{\pi}\mathrm{i}\hat{x}}, \mathrm{e}^{-2\sqrt{\pi}\mathrm{i}\hat{y}}\right\}$. The Gottesman-Kitaev-Preskill (GKP) states are

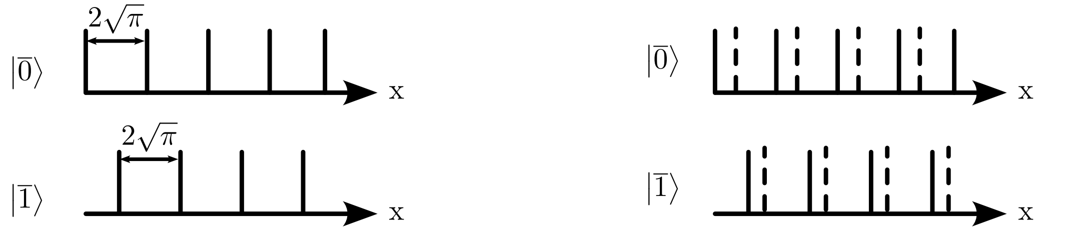
$$\begin{aligned}\left|\bar{0}\right\rangle &= \sum_{n\in\mathbb{Z}} \left|2n\sqrt{\pi}\right\rangle_x,\\ \left|\bar{1}\right\rangle &= \sum_{n\in\mathbb{Z}} \left|(2n+1)\sqrt{\pi}\right\rangle_x.\end{aligned}$$

In Figure 16.1 is an illustration of the GKP states with and without displacement errors.
Here is the mathematic proof: Let the input state be encoded as follows

$$\begin{aligned}&\left|\Psi\right\rangle = a\left|\bar{0}\right\rangle + b\left|\bar{1}\right\rangle\\ \text{since }\ &\mathrm{e}^{2\sqrt{\pi}\mathrm{i}\hat{x}}\left|\bar{0}\right\rangle = \left|\bar{0}\right\rangle \quad \text{and } \mathrm{e}^{-2\sqrt{\pi}\mathrm{i}\hat{x}}\left|\bar{1}\right\rangle = \left|\bar{1}\right\rangle,\\ \text{then }\ &\mathrm{e}^{2\sqrt{\pi}\mathrm{i}\hat{x}}\left|\bar{\Psi}\right\rangle = \left|\bar{\Psi}\right\rangle\end{aligned}$$

Let the state $\left|\bar{\Psi}\right\rangle$ be affected by the displacement error of the $\hat{x}$-quadrature by the value μ, then

$$\begin{aligned}\mathrm{e}^{2\sqrt{\pi}\mathrm{i}\hat{x}}\left(\mathrm{e}^{-\mathrm{i}\mu\hat{y}}\left|\bar{\Psi}\right\rangle\right) &= \mathrm{e}^{-\mathrm{i}\mu\hat{y}}\mathrm{e}^{2\sqrt{\pi}\mathrm{i}\hat{x}}\mathrm{e}^{2\sqrt{\pi}\mu\left[\hat{x},\hat{y}\right]}\left|\bar{\Psi}\right\rangle\\ &= \mathrm{e}^{\mathrm{i}\sqrt{\pi}\mu}\left(\mathrm{e}^{-\mathrm{i}\mu\hat{y}}\left|\bar{\Psi}\right\rangle\right).\end{aligned}$$


$2\sqrt{\pi}$
$\left|\bar{0}\right\rangle$
x
$2\sqrt{\pi}$
$\left|\bar{1}\right\rangle$
x
$\left|\bar{0}\right\rangle$
x
$\left|\bar{1}\right\rangle$
x

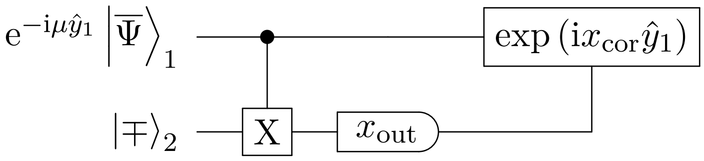
GKP states without displacement errors

GKP states with displacement errors

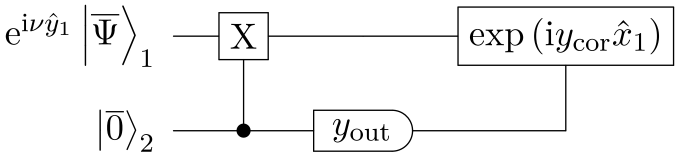
Figure 16.1: GKP states with and without displacement errors. The condition for the value of the displacement is $|u| < \frac{\sqrt{\pi}}{2}$.

16.2.3 Error correction schemes using GKP states

An error correction scheme in $\hat{x}$-quadratures


$\mathrm{e}^{-\mathrm{i}\mu\hat{y}_1}\left|\overline{\Psi}\right\rangle_1$
$|\mp\rangle_2$
X
x_{out}
$\exp\left(\mathrm{i}x_{\text{cor}}\hat{y}_1\right)$

and an error correction scheme in $\hat{y}$-quadratures


$\mathrm{e}^{\mathrm{i}\nu\hat{y}_1}\left|\overline{\Psi}\right\rangle_1$
$|\overline{0}\rangle_2$
X
y_{out}
$\exp\left(\mathrm{i}y_{\text{cor}}\hat{x}_1\right)$

The state after the SUM transformation:

$$\mathrm{e}^{\mathrm{i}\mu\hat{y}_1}\left|\overline{\Psi}\right\rangle_1 |\mp\rangle_2 \overset{\text{SUM}}{\to} \sum_{n,n_0\in\mathbb{Z}}\left(a\left|2n_0\sqrt{\pi}+\mu\right\rangle_{x,1}+b\left|(2n_0+1)\sqrt{\pi}+\mu\right\rangle_{x.1}\right)\otimes\left|n\sqrt{\pi}+\mu\right\rangle_{x,2}.$$

Thanks to entanglement, we have reflected the error μ in an auxiliary state. When measuring the $\hat{x}$-quadrature of the auxiliary state, we get the result:

$$x_{\text{out}}=\mu+m\sqrt{\pi}$$

where m is an arbitrary integer. To correct the error, we must displace the input state by:

$$x_{\text{cor}}=x_{\text{out}} \bmod \sqrt{\pi},\ \text{ for } \mu<\sqrt{\pi}/2.$$

16.2.4 Imperfect GKP states

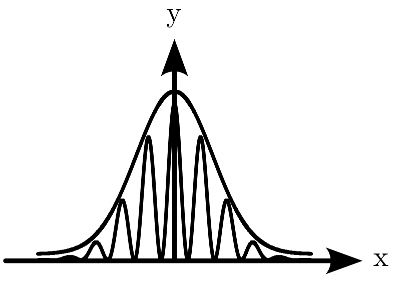
The ideal GKP states are infinitely squeezed, therefore, in reality, **non-ideal** GKP states are used which are defined by the following expressions

$$|\tilde{0}\rangle=N_0\sum_{s\in\mathbb{Z}}\mathrm{e}^{-\frac{\xi^2}{2}\left(2s\sqrt{\pi}\right)^2}\hat{T}(2s\sqrt{\pi})\,|\Psi_0\rangle$$
$$|\tilde{1}\rangle=N_1\sum_{s\in\mathbb{Z}}\mathrm{e}^{-\frac{\xi^2}{2}\left((2s+1)\sqrt{\pi}\right)^2}\hat{T}((2s+1)\sqrt{\pi})\,|\Psi_0\rangle$$

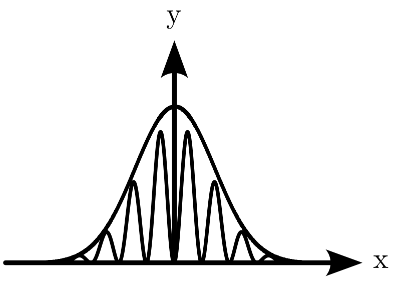
where N_0, N_1 are the normalising constants, $\hat{T}(\alpha)$ is the translation operator, δ is the peak width in the comb, ξ^{-1} is the envelope width of the whole comb:

$$|\Psi_0\rangle=\int_{-\infty}^{\infty}\frac{\mathrm{d}q}{\left(\pi\Delta^2\right)^{1/4}}\mathrm{e}^{-\frac{q^2}{2\Delta^2}}\,|q\rangle_x=\int_{\infty}^{\infty}\frac{\mathrm{d}p}{\left(\pi/\Delta^2\right)^{1/4}}\mathrm{e}^{-\frac{p^2\Delta^2}{2}}\,|q\rangle_y\,.$$

Non-ideal GKP states are not orthogonal $\langle\tilde{0}|\tilde{1}\rangle\neq 0$. Hence, there is some probability to measure the state $|\tilde{0}\rangle$ and to interpret it as a state $|\tilde{1}\rangle$ and vice versa. The probability of interpreting the



$|\tilde{0}\rangle$



$|\tilde{1}\rangle$

state $|\tilde{0}\rangle$ as state $|\tilde{1}\rangle$ is equal to the probability that when we measure the $\hat{x}$-quadrature of the state $|\tilde{0}\rangle$, we get an odd value of the factor m in $m\sqrt{\pi}$:

$$P_{0\to 1} = \sum_{n=-\infty}^{\infty} \int\limits_{2\sqrt{\pi}n-\sqrt{\pi}/2}^{2\sqrt{\pi}n+\sqrt{\pi}/2} \left|\langle x|\tilde{0}\rangle\right|^2 \mathrm{d}x.$$

For $\Delta = \xi = 0.25$ the probability $P_{0\to 1} \approx 0.01$ and for $\Delta = \xi = 0.125$ the probability $P_{0\to 1} \approx 10^{-6}$.

To examine the effect of squeezing on the error correction process, we introduce the **displacement state**

$$|\mu, \nu\rangle = \frac{1}{\pi^{1/4}} \mathrm{e}^{\mathrm{i}\mu\hat{x}} \mathrm{e}^{-\mathrm{i}\nu\hat{y}} \left|\overline{0}\right\rangle.$$

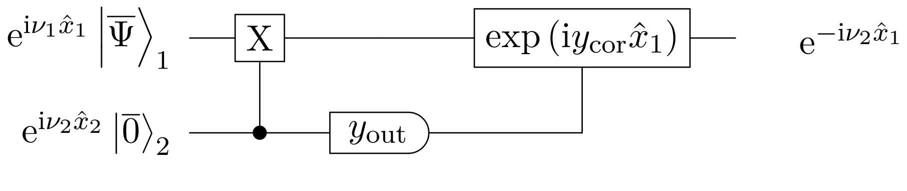
The displacement states are orthogonal:

$$\langle \mu', \nu' | \mu, \nu \rangle = \delta(\mu - \mu')\delta(\nu - \nu')$$

and they form a complete set. Therefore, they can be used to decompose any quantum state:

$$|\Phi\rangle = \int\limits_{-\sqrt{\pi}/2}^{\sqrt{\pi}/2} \mathrm{d}\mu \int\limits_{-\sqrt{\pi}/2}^{\sqrt{\pi}/2} \mathrm{d}\nu \langle \mu, \nu | \Phi\rangle \, |\mu, \nu\rangle .$$

The error correction scheme using displacement states is


$\mathrm{e}^{\mathrm{i}\nu_1\hat{x}_1} \left|\overline{\Psi}\right\rangle_1$
$\mathrm{e}^{\mathrm{i}\nu_2\hat{x}_2} \left|\overline{0}\right\rangle_2$
X
y_{out}
$\exp\left(\mathrm{i}y_{\mathrm{cor}}\hat{x}_1\right)$
$\mathrm{e}^{-\mathrm{i}\nu_2\hat{x}_1}$

The state after the SUM transformation:

$$\mathrm{e}^{\mathrm{i}\nu_1\hat{x}_1} \left|\overline{\Psi}\right\rangle_1 \mathrm{e}^{\mathrm{i}\nu_2\hat{x}_2} \left|\overline{0}\right\rangle_2 \overset{\mathrm{SUM}}{\to} \mathrm{e}^{\mathrm{i}\nu_1\hat{x}_1} \mathrm{e}^{\mathrm{i}(\nu_1+\nu_2)\hat{x}_2} \left|\overline{\Psi}\right\rangle_1 \left|\overline{0}\right\rangle_2 .$$

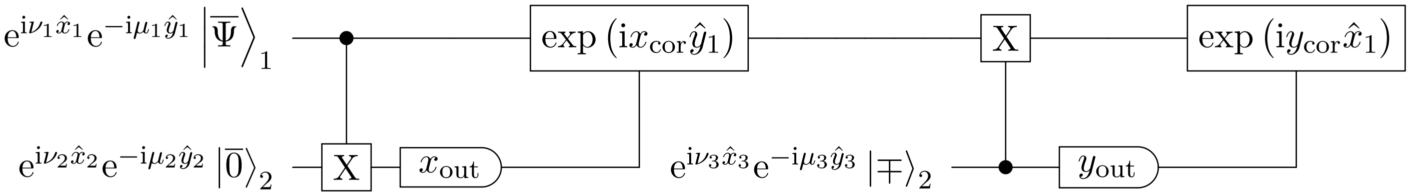
When measuring the $\hat{y}$-quadrature of the auxiliary state, the result is

$$y_{\mathrm{out}} = \nu_1 + \nu_2 + m\sqrt{\pi}.$$

After using the modulo operation, we have

$$y_{\mathrm{cor}} = \nu_1 + \nu_2, \text{ for } |\nu_1 + \nu_2| < \frac{\sqrt{\pi}}{2}.$$

The displacement error correction scheme in two quadratures is


$e^{i\nu_1\hat{x}_1}e^{-i\mu_1\hat{y}_1}\left|\overline{\Psi}\right\rangle_1$
$e^{i\nu_2\hat{x}_2}e^{-i\mu_2\hat{y}_2}\left|\overline{0}\right\rangle_2$
X
x_{out}
$\exp\left(ix_{\text{cor}}\hat{y}_1\right)$
$e^{i\nu_3\hat{x}_3}e^{-i\mu_3\hat{y}_3}\left|\mp\right\rangle_2$
X
y_{out}
$\exp\left(iy_{\text{cor}}\hat{x}_1\right)$

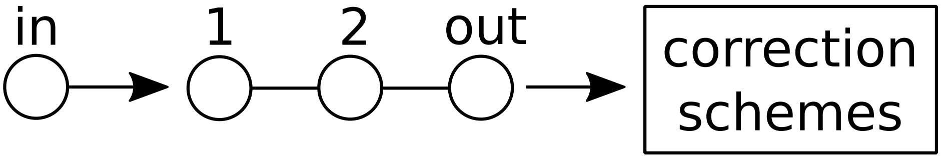
The main stages of error correction in this scheme are

1. Correction for $\hat{x}$-quadrature errors: $\mu_1, \nu_1 \to -\mu_2, \nu_1 + \nu_2$ provided that $|\mu_1 + \mu_2| < \frac{\sqrt{\pi}}{2}$
2. Correction for $\hat{y}$-quadrature errors: $-\mu_2, \nu_1 + \nu_2 \to -\mu_2 + \mu_3, \nu_3$ for $|\nu_1 + \nu_2 + \nu_3| < \frac{\sqrt{\pi}}{2}$

The error correction scheme will be fault-tolerant if $|\nu_i| < \frac{\sqrt{\pi}}{6}$ and $|\mu_i| < \frac{\sqrt{\pi}}{6}$.

16.3 Error correction using imperfect GKP states

For a three-node cluster state: The first node is mixed with the input state and the third node is the output and not measured: To correct displacement errors, we need to follow a few steps:



- We need to encode input information using GKP states
- With the input GKP states, we will carry out standard one-way quantum computations
- Over each input node we need to carry out the described correction procedure with auxiliary states

The probability of correcting displacement errors is equal to the probability of finding these errors in the range from $-\frac{\sqrt{\pi}}{2}$ to $\frac{\sqrt{\pi}}{2}$.
Since displacement errors belong to the Gaussian class, they have normal distribution and, therefore, the probability of their correction is given by the following:

$$P_{\text{corr}} = \frac{1}{\sqrt{4\pi\sigma^2}} \int_{-\frac{\sqrt{\pi}}{2}}^{\frac{\sqrt{\pi}}{2}} \exp\left(-\frac{t^2}{4\sigma^2}\right) \mathrm{d}t$$

where $\sigma = a + b$ is the resulting variance which is the sum of the computation error variance a and the variance of the peak of the GKP state b.
The probability of an incorrect displacement error correction:

$$1 - P_{\text{corr}} = 1 - \frac{1}{\sqrt{4\pi\sigma^2}} \int_{-\frac{\sqrt{\pi}}{2}}^{\frac{\sqrt{\pi}}{2}} \exp\left(-\frac{t^2}{4\sigma^2}\right) \mathrm{d}t < 10^{-6}.$$

Based on this estimation of these probabilities, we will be able to answer the question regarding the fault-tolerance of continuous variable one-way quantum computing schemes. We can find a and b and estimate the squeezing necessary for fault-tolerant one-way quantum computation. The continuous variable one-way computation model will be completely fault-tolerant if the squeezing of the quantum oscillators is greater than -20.5dB.

16.4 Exercises

1. What are the principles of any error correcting code?

   ○ It is necessary to have an idea of the errors we want to correct

   ○ Principle of information redundancy. All information is redundantly encoded

   ○ Principle of Quantum Superposition

   ○ One can build a code that can correct any possible error

2. What operator sets the qubit-flip error in one qubit?

   ○ Pauli $\hat{\mathrm{X}}$ operator

   ○ Pauli $\hat{\mathrm{Z}}$ operator

   ○ Pauli $\hat{\mathrm{Y}}$ operator

3. Choose operators of 4-qubit errors with weight of 3:

   ○ $\mathrm{Z}_1 \otimes \mathrm{Z}_2 \otimes \mathrm{I}_3 \otimes \mathrm{I}_4$

   ○ $\mathrm{I}_1 \otimes \mathrm{Z}_2 \otimes \mathrm{Y}_3 \otimes \mathrm{X}_4$

   ○ $\mathrm{Z}_1 \otimes \mathrm{Z}_2 \otimes \mathrm{Z}_3 \otimes \mathrm{I}_4$

   ○ $\mathrm{X}_1 \otimes \mathrm{I}_2 \otimes \mathrm{I}_3 \otimes \mathrm{Y}_4$

4. What principle must the error satisfy to be detected by the stabilising code with generators $\{\hat{S}_i\}_i$?

   ○ Error operator must commute with all code generators

   ○ Error operator must anti-commute with all code generators

5. Suppose we have a quantum error correction code that is defined by the codewords $|i\rangle_L$. Choose a necessary and sufficient condition that errors must obey so that they can be compensated for by this code.

   ○ ${}_L\langle i|E_a^\dagger E_b\,|j\rangle_L = \delta_{ab}\delta_{ij}$

   ○ ${}_L\langle i|E_a^\dagger E_b\,|j\rangle_L = \frac{1}{2}$

   ○ ${}_L\langle i|E_a^\dagger E_b\,|j\rangle_L = 0$

6. What errors can a three-qubit code with two codewords $|0\rangle_L = |000\rangle$ and $|1\rangle_1 = |111\rangle$ correct?

   ○ Phase errors

   ○ Qubit-flip errors

   ○ Phase and qubit-flip errors

7. What errors can a three-qubit code with two codewords $|+\rangle_L = |+++\rangle$ and $|-\rangle_1 = |---\rangle$ correct?

   ○ Phase errors

   ○ Qubit-flip errors

   ○ Phase and qubit-flip errors

8. How many errors weighing not more than two can occur in a 7-qubit code?

   ○ 210

   ○ 100

- ○ 81
- ○ 9

9. What computational scheme is fault-tolerant?

   - ○ A scheme in which failure in one component of the scheme results in at most one error in each output block of qubits
   - ○ A scheme in which one error leads to more than one error in each output block of qubits
   - ○ A scheme in which errors occur only during the transmission of qubits

10. What is the operator for the displacement x-quadrature errors?

    - ○ $\hat{D}_x(u) = \mathrm{e}^{-\mathrm{i}u\hat{y}}$
    - ○ $\hat{D}_x(u) = \mathrm{e}^{-\mathrm{i}u\hat{x}}$
    - ○ $\hat{D}_x(u) = \mathrm{e}^{-\mathrm{i}u\hat{x}\hat{y}}$

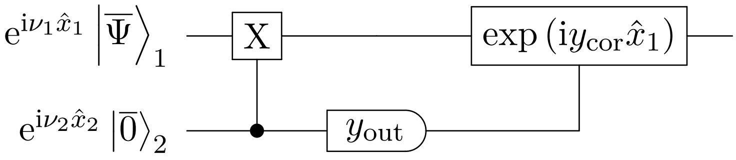
11. What are the two codewords for the GKP state?

    - ○
    $$|0\rangle = \sum_{n\in\mathbb{Z}} |2n\sqrt{\pi}\rangle_x\,,$$
    $$|1\rangle = \sum_{n\in\mathbb{Z}} |(2n+1)\sqrt{\pi}\rangle_x$$
    - ○
    $$|1\rangle = \sum_{n\in\mathbb{Z}} |2n\sqrt{\pi}\rangle_x\,,$$
    $$|0\rangle = \sum_{n\in\mathbb{Z}} |(2n+1)\sqrt{\pi}\rangle_x$$
    - ○
    $$|0\rangle = \sum_{n\in\mathbb{Z}} |2n\rangle_x\,,$$
    $$|1\rangle = \sum_{n\in\mathbb{Z}} |(2n+1)\rangle_x$$

12. How does the GKP state comb transform under the displacement error?

    - ○ The comb displaces
    - ○ The comb stretches
    - ○ The comb squeezes

13. What error can be corrected using the scheme


$\mathrm{e}^{\mathrm{i}\nu_1\hat{x}_1}\left|\overline{\Psi}\right\rangle_1$
X
$\exp\left(\mathrm{i}y_{\mathrm{cor}}\hat{x}_1\right)$
$\mathrm{e}^{\mathrm{i}\nu_2\hat{x}_2}\left|\overline{0}\right\rangle_2$
y_{out}

- ○ A displacement error in x quadrature
- ○ A displacement error in y quadrature

14. What is the difference between ideal and imperfect GKP states?

- ○ The imperfect state is displaced relative to the ideal one
- ○ The peaks of the imperfect state are farther apart than the peaks of the ideal state
- ○ The imperfect state has peaks of finite width

15. Is it possible to completely compensate for a quadrature displacement error using imperfect GKP states?

- ○ Yes
- ○ It is impossible to compensate for the error

16. Which cluster state node should be mixed with GKP states to perform displacement error correction?

- ○ Nodes that are also mixed with input states
- ○ Nodes that are measured in the process of computation
- ○ Unmeasured nodes that will be in the output state

Appendix A

Solutions to exercises

A.1 Chapter 1

1. The demands for a physical implementation of a quantum computer, which we deduced from the mathematical model of quantum computing, are:

   ✓ truly random events must be employed
   ✓ interference must be possible
   ✓ instead of bits we need qubits which can have an infinite number of possible states
   ✘ computation must be fast
   ✘ qubit implementation must be cold

2. Check all true random events in the list below:

   ✘ A flipping coin lands on the table with tails up or down
   ✓ An electron hits either upper or lower detection in Young's interferometer
   ✘ A stock price unexpectedly falls or grows
   ✓ Photon either passes through or reflects from a piece of glass
   ✓ A radioactive isotope either decays or not during a period of time

3. Qubit state $|+\rangle$ is:

   ✓ $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
   ✘ $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
   ✘ $|0\rangle + |1\rangle$
   ✘ $|0\rangle - |1\rangle$

4. Is the following proposition correct?

   Interference sometimes allows us to read more information from a superposition state of a system than the simple observation of the state. → **It is correct**

5. Should we literally believe in the existence of parallel universes which contain different copies of us and other objects?

   ✓ Science is not about out believes. The multiverse is just a convenient mathematically model which allows us to interpret and explain superposition states. To our current knowledge there is no experiment which can prove or refute the existence of the multiverse.

   ✘ Yes, of course! And there exists a universe where birds and bees talk about quantum mechanics in pure English.

A.2 Chapter 2

1. We fired one electron from our electron gun. The position of the electron is defined by the wavefunction $f(r)$. What is the integral of $f^2(r)$ over the whole space? → **1**

2. Select all correct statements:

   ✓ Multiplying a wavefunction by a number does not change its physical meaning. It still corresponds to the same physical state.

   ✓ The set of all possible outcomes of the measurement forms the basis in the vector space of wavefunctions.

   ✘ Light does not show interference in Young's interferometer. In 1905 Einstein showed that there is no interference of light on two slits, because light consists of invisible packets he called photons.

   ✘ The set of all possible outcomes of the measurement is always infinite.

3. Is the Dirac delta function a square-integrable function? → **No**

4. Suppose we want to obtain more from the measurement process, se we perform it twice using the same observables. Select the correct statements:

   ✘ Sometimes it might help...

   ✓ The second measurement with the same observables does not help us to obtain more information, since after the first measurement the wavefunction collapses to one of the basis states, defined by the observable. The wavefunction decomposition after the first measurement becomes just this basis state with the probability amplitude equal to 1. So, the second measurement will give us the same state.

5. Do photons always travel in straight lines? → **No, there is no such thing as a trajectory of a photon.**

6. What is the dimensionality of the vector $|01101\rangle$? → $\mathbf{2^5 = 32}$

7. If we measure the state $\frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$ in the basis $\{\,|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle\,\}$, we can obtain:

   ✘ $|01\rangle$ with probability $\frac{1}{2}$ or $|10\rangle$ with probability $\frac{1}{2}$

   ✓ $|00\rangle$ with probability $\frac{1}{2}$ or $|11\rangle$ with probability $\frac{1}{2}$

   ✘ $|00\rangle$ with probability $\frac{1}{\sqrt{2}}$ or $|11\rangle$ with probability $\frac{1}{\sqrt{2}}$

8. Is the equality $|00\rangle + |11\rangle = (\,|0\rangle + |1\rangle\,) \otimes (\,|0\rangle + |1\rangle\,)$ correct? → **No**

9. The Stern-Gerlach experiment shows us that:

   ✓ Some particles have a measurable property called spin. For silver atoms and electrons their spin along any axis has two distinguished values, thus they represent two-level systems and can be used for implementation of qubits.

   ✘ Electrons in any atom rotate around its core in the same plane everywhere in the universe. Niels Bohr called this the greatest mystery of quantum mechanics.

10. The entangled states like $\frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$ or $\frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle\,)$ are interesting because (choose all correct answers):

    ✓ These states appear when particles interact with each other. We can not prepare such states without particles interacting.

    - These are 4-qubit states the, the only known up to this moment.

- ✓ If we measure one particle in this state, we actually measure both of them (even if the other particle is far away). (*This was probably not mentioned in the lecture*)
- ✓ These are the states of two particles, however each of these particles does not have its own state.
- ✗ These are the only quantum states we can implement on flipping coins.

11. $[X, Z] = \dots$
    - ✗ Y
    - ✓ $2XZ$
    - ✗ $0_{2,2}$

12. $X^* = \dots$
    - ✗ Y
    - ✗ Z
    - ✓ X

13. Is the identity operator I an observable?
    - ✓ Yes, however a useless one, since its only eigenvalue is n-fold degenerate.
    - ✗ No

14. $\langle -|1\rangle = \dots$
    - ✓ $-\frac{1}{\sqrt{2}}$
    - ✗ 0
    - ✗ $\sqrt{2}$
    - ✗ $\frac{1}{\sqrt{2}}$

15. $\left(|\phi\rangle \langle\psi| AB\right)^* = \dots$
    - ✓ $B^*A^* |\psi\rangle \langle\phi|$
    - ✗ $\langle\phi|\psi\rangle A^*B^*$

A.3 Chapter 3

1. In the E91 protocol, if Alice and Bob successfully check 5 randomly chosen bits from their shared key, they obtain:
    - ✓ more than 96% confidence about the absence of intrusion
    - ✗ exactly 95% confidence about the absence of intrusion
    - ✗ more than 99% confidence about the absence of intrusion

2. The BB84 protocol is based on:
    - ✓ indivisibility of photons
    - ✗ the RSA algorithm
    - ✓ the no-cloning theorem
    - ✗ complexity of factoring composite numbers

3. Does quantum teleportation allows to transfer messages faster than light? → **No**

4. The no-cloning theorem is about:

- ✓ impossibility to create a copy of an unknown quantum state
- ✘ impossibility to create a copy of a known quantum state
- ✘ moral consequences of cloning a human being

5. $\mathrm{SWAP}|0+\rangle = \ldots$:

   - ✘ $|1-\rangle$
   - ✘ $|-1\rangle$
   - ✓ $|+0\rangle$

A.4 Chapter 4

1. In classical information theory, how much bits are required to describe a certain value, if it can take n possible values?

   - ✘ $\exp\left(n^2\right)$
   - ✓ $\log_2 n$
   - ✘ $2\log n$
   - ✘ $\log n^2$

2. What is the correct way to write a qubit $|\phi\rangle = \frac{\mathrm{e}^{\mathrm{i}\alpha}}{\sqrt{5}}|0\rangle - \sqrt{\frac{4}{5}}|1\rangle$ in the form of a two-dimensional column vector?

   - ✘ $\begin{pmatrix} \mathrm{e}^{2\mathrm{i}\alpha}/5 \\ 4/5 \end{pmatrix}$
   - ✓ $\begin{pmatrix} \mathrm{e}^{\mathrm{i}\alpha}/5 \\ -\sqrt{4/5} \end{pmatrix}$
   - ✘ $\begin{pmatrix} \mathrm{e}^{\mathrm{i}\alpha}/5 \\ \sqrt{4/5} \end{pmatrix}$
   - ✘ $\begin{pmatrix} 1/5 \\ 4/5 \end{pmatrix}$

3. Match the positive directions of the axes on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|0\rangle$

   - ✘ positive direction x
   - ✘ negative direction x
   - ✘ positive direction y
   - ✘ negative direction y
   - ✓ positive direction z
   - ✘ negative direction z

4. Match the positive directions of the axies on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|1\rangle$

   - ✘ positive direction x
   - ✘ negative direction x
   - ✘ positive direction y

- ✘ negative direction y
- ✘ positive direction z
- ✓ negative direction z

5. Match the positive directions of the axies on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|+\rangle$

   - ✓ positive direction x
   - ✘ negative direction x
   - ✘ positive direction y
   - ✘ negative direction y
   - ✘ positive direction z
   - ✘ negative direction z

6. Match the positive directions of the axies on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|-\rangle$

   - ✘ positive direction x
   - ✓ negative direction x
   - ✘ positive direction y
   - ✘ negative direction y
   - ✘ positive direction z
   - ✘ negative direction z

7. Match the positive directions of the axies on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|\mathrm{i}\rangle$

   - ✘ positive direction x
   - ✘ negative direction x
   - ✓ positive direction y
   - ✘ negative direction y
   - ✘ positive direction z
   - ✘ negative direction z

8. Match the positive directions of the axies on the Bloch sphere to the directions of the basis vectors $|0\rangle$ and $|1\rangle$ and their linear combinations:

   positive direction $|-\mathrm{i}\rangle$

   - ✘ positive direction x
   - ✘ negative direction x
   - ✘ positive direction y
   - ✓ negative direction y
   - ✘ positive direction z
   - ✘ negative direction z

9. What physical systems (and their characteristics) can be used to implement the qubit? (Select all that applies)

- ✓ two orthogonal photon polarisations
- ✓ projection of electron spin on the selected direction
- ✓ energy levels of the ¨two-level atom¨

10. Which of the following expressions describe the pure state of a quantum system in the two-dimensional Hilbert space? $|\psi_1\rangle$ and $|\psi_2\rangle$ are elements of the considered space, constituting its complete set ($|c_1|^2 + |c_2|^2 = 1$)

    (Select all that applies)

    - ✗ $c_1 |\psi_2\rangle + c_2\big(|\psi_1\rangle\big)^{1/2}$
    - ✓ $\sqrt{\frac{3}{5}}\,|\psi_1\rangle - \sqrt{\frac{2}{5}}\,|\psi_2\rangle$
    - ✓ $c_1 |\psi_1\rangle + c_2 |\psi_2\rangle$
    - ✓ $\hat{\varrho} = |\phi_2\rangle\langle\phi_2|$

11. Select the correctly written statistical operators, if $\omega_1 + \omega_2 + \omega_3 = 1$:

    - ✓ $\hat{\varrho} = \frac{1}{2}|\phi_1\rangle\langle\phi_2| + \sum\limits_{i=2}^{3} \omega\,|\phi_i\rangle\langle\phi_i|$
    - ✗ $\hat{\varrho} = \omega_1|\phi_1\rangle\langle\phi_1| + \omega_2^2|\phi_2\rangle\langle\phi_2| + \omega_3^3|\phi_3\rangle\langle\phi_3|$
    - ✓ $\hat{\varrho} = \frac{\sqrt{2}}{9}|\phi_1\rangle\langle\phi_1| + \frac{5-\sqrt{2}}{9}|\phi_2\rangle\langle\phi_2| + \frac{4}{9}|\phi_3\rangle\langle\phi_3|$
    - ✓ $\hat{\varrho} = \omega_2|\phi_1\rangle\langle\phi_1| + \omega_3|\phi_2\rangle\langle\phi_2|$

12. Choose the correct properties of the density matrix, if $\langle\hat{A}\rangle$ is the average value of the operator $\hat{A}$.

    - ✓ $\hat{\varrho}^\dagger = \hat{\varrho}$
    - ✗ $\langle\psi|\hat{\varrho}|\psi\rangle = 1/2$
    - ✗ $0 \le \mathrm{Tr}(\hat{\varrho}) \le 1$
    - ✓ $\langle\hat{A}\rangle = \mathrm{Tr}(\hat{A}\hat{\varrho})$

13. Is the following statement true? If an open quantum system is in a mixed state, then its evolution can be described using the Liouville quantum equation $\mathrm{i}\hbar\frac{\partial}{\partial t}\hat{\varrho} = [\hat{H}, \hat{\varrho}]$.

    → **It is false, because the system is open.**

14. The operators $\hat{A}_1^{(1)}, \hat{A}_2^{(1)}, \hat{A}_3^{(1)}$ act only on qubit ¨1¨,$\hat{B}_1^{(2)}, \hat{B}_2^{(2)}$ act only on qubit ¨2¨, and $\hat{C}^{(3)}$ act only on qubit ¨3¨. Choose identical equations that correspond to the action of all these operators on the system consisting of given independent qubits

    (a) $\hat{A}_1^{(1)}\hat{A}_1 \otimes \hat{B}^{(2)} \otimes \hat{C}^{(3)}$ where $\hat{A}^{(1)} = \hat{A}_2^{(1)}\hat{A}_3^{(1)}, \hat{B}^{(2)} = \hat{B}_1^{(2)}\hat{B}_2^{(2)}$

    (b) $\hat{C}^{(3)}\hat{B}_1^{(2)}\hat{B}_2^{(2)}\hat{A}_1^{(1)}\hat{A}_2^{(1)}\hat{A}_3^{(1)}$

    (c) $\hat{A}_1^{(1)}\hat{A}_2^{(1)}\hat{A}_3^{(1)}\hat{C}^{(3)}\hat{B}_1^{(2)}\hat{B}_2^{(2)}$

    (d) $\hat{A}_1^{(1)}\hat{A}_2^{(1)}\hat{A}_3^{(1)}\hat{B}_1^{(2)}\hat{B}_2^{(2)}\hat{C}^{(3)}$

    - ✗ only (d)
    - ✗ only (a) and (c)
    - ✗ only (b), (c), and (d) are identical to each other
    - ✓ all equations are identical

15. Can an entangled state be pure? → **Yes**

16. Can a mixed state of two systems be inseparable? → **Yes**

17. Is the state $|\psi_1\rangle \otimes |\psi_2\rangle$ indicating that the two systems are inseparable? → **No**

18. Is the state characterised by the statistical operator $\sum\limits_{k=1}^{n} \omega_k \hat{\varrho}_1^k \otimes \hat{\varrho}_2^k$ separable, if $\hat{\varrho}_1^k$ and $\hat{\varrho}_2^k$ are mixed states in the Hilbert spaces $\mathcal{H}_1^2$ and $\mathcal{H}_2^2$, respectively, and with $\sum\limits_{k=1}^{n} \omega_k = 1$?

    → **Yes**

19. There is a physical system consisting of two subsystems ¨A¨ and ¨B¨ and described by a density matrix $\hat{\varrho}_{A,B}$. Which of the following equations can be used to find the reduced density matrix $\hat{\varrho}_B$?

    ✓ $\hat{\varrho}_B = \mathrm{Tr}_A(\hat{\varrho}_{AB})$
    ✗ $\hat{\varrho}_B = \mathrm{Tr}_B(\hat{\varrho}_{AB})$

20. Select the correct properties of the reduced density matrix

    ✓ $\hat{\varrho}_A \neq \hat{\varrho}_B^\dagger$
    ✗ $\mathrm{Tr}\Big(\mathrm{Tr}_A(\hat{\varrho}_{AB})\Big) \neq \mathrm{Tr}\Big(\mathrm{Tr}_B(\hat{\varrho}_{AB})\Big)$
    ✗ $\langle\psi_A|\hat{\varrho}_A|\psi_A\rangle \geq 0, \langle\psi_B|\hat{\varrho}_B|\psi_B\rangle \leq 0$ where $\forall\, |\psi_A\rangle \in \mathcal{H}_A,\ |\psi_B\rangle \in \mathcal{H}_B$

21. A pair of qubits are in states written as column vectors:

    $$|\psi_1\rangle = \begin{pmatrix} \cos\theta_1 \\ \sin\theta_1 \end{pmatrix},$$
    $$|\psi_2\rangle = \begin{pmatrix} \cos\theta_2 \\ \sin\theta_2 \end{pmatrix}.$$

    Each of these states is normalised to one. For which $\theta_1 - \theta_2$ will the expression $|\psi_1\rangle - |\psi_2\rangle$ also be normalised?

    ✓ $\pm\pi/3$
    ✗ $\pm\pi/4$
    ✗ $\pm 3\pi/4$
    ✗ $\pm 2\pi/3$

22. Where is the state vector

    $$\frac{1}{\sqrt{2+\sqrt{2}}}\left(\frac{\sqrt{2}+1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\right)$$

    directed on the Bloch sphere?

    ($\mathrm{e}_x, \mathrm{e}_y, \mathrm{e}_z$ are the unit vectors on the Bloch sphere)

    ✗ It coincides with the direction of the vector $\mathrm{e}_z + \mathrm{e}_x$
    ✗ It coincides with the direction of the vector $\mathrm{e}_z - \mathrm{e}_y$
    ✗ It coincides with the direction of the vector $\mathrm{e}_x + \mathrm{e}_y$
    ✓ It coincides with the direction of the vector $\mathrm{e}_z - \mathrm{e}_x$

23. Based on the definition of the statistical operator and the identity operator, determine whether the equality

    $$\mathrm{Tr}\left(\hat{L}\hat{\varrho}\right) = \mathrm{Tr}\left(\hat{\varrho}\hat{L}\right)$$

is true or false.

Here $\hat{L}$ is an operator acting in the state space $|u_k\rangle$, $\hat{\varrho} = \sum\limits_n p_n |\psi_n\rangle \langle\psi_n|$ with the probability p_n that the system is described by a state vector $|\psi_n\rangle$ and $\sum\limits_n p_n = 1$, as well as $\mathrm{I} = \sum\limits_{k=1}^{n} |u_k\rangle \langle u_k|$ with $\{\, |u_k\rangle \,\}$ are basic states that form a complete orthonormal set and $|\psi_n\rangle$ are pure states formed by linear combination of $|u_k\rangle$.

→ **It is true**

24. Based on the definition, find the density matrices for the following states and match them with the suggested answer choices.

    $\{(|0\rangle, p_0 = 2/3), (|1\rangle, p_0 = 1/3)\}$ where p_0 and p_1 are the probabilities that the system is described by the state vectors $|0\rangle$ and $|1\rangle$, respectively. $p_0 + p_1 = 1$.

    ✓ $\frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$
    ✗ $\frac{2}{3}|0\rangle\langle 1| + \frac{1}{3}|1\rangle\langle 0|$
    ✗ $\frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1| + \frac{\sqrt{2}}{3}(\,|0\rangle\langle 1| + |1\rangle\langle 0|\,)$
    ✗ $\frac{2}{3}|0\rangle\langle 1| + \frac{1}{3}|1\rangle\langle 0| + \frac{\sqrt{2}}{3}(\,|0\rangle\langle 0| + |1\rangle\langle 1|\,)$

25. Based on the definition, find the density matrices for the following states and match them with the suggested answer choices.

    $\sqrt{\frac{2}{3}}\,|0\rangle + \sqrt{\frac{1}{3}}\,|1\rangle$

    ✗ $\frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$
    ✗ $\frac{2}{3}|0\rangle\langle 1| + \frac{1}{3}|1\rangle\langle 0|$
    ✓ $\frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1| + \frac{\sqrt{2}}{3}(\,|0\rangle\langle 1| + |1\rangle\langle 0|\,)$
    ✗ $\frac{2}{3}|0\rangle\langle 1| + \frac{1}{3}|1\rangle\langle 0| + \frac{\sqrt{2}}{3}(\,|0\rangle\langle 0| + |1\rangle\langle 1|\,)$

26. Is it true or false that for an arbitrary state $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ in the state basis $\{\, |0\rangle, |1\rangle \,\}$ the inequality

    $$\mathrm{Tr}(\,|\phi\rangle\langle\phi|\,) \geq \mathrm{Tr}(\langle\phi|\phi\langle)$$

    holds?

    → **It is false.**

27. Let $|\psi\rangle = \sin\theta\,|0\rangle + \mathrm{e}^{\mathrm{i}(\phi+\tan\theta)}\cos\theta\,|1\rangle$ with $\theta, \phi \in \mathbb{R}$. Determine whether $\hat{\varrho} = |\psi\rangle\langle\psi|$ is a statistical operator

    (Hint check the three basic properties of a density matrix:

    1. $\hat{\varrho}^\dagger = \hat{\varrho}$

    2. $\mathrm{Tr}(\hat{\varrho}) = 1$

    3. $\langle\alpha|\hat{\varrho}|\alpha\rangle \geq 0$, here $|\alpha\rangle$ is a state vector from the same state space $\{\, |0\rangle, |1\rangle \,\}$ in which $|\psi\rangle$ is defined, i.e. $|\alpha\rangle$ is some linear superposition of state vectors $|0\rangle$ and $|1\rangle$.)

    → **It is a statistical operator.**

28. The quantum system consists of 3 subsystems. Its state is defined by Schmidt decomposition $\left|\psi^{ABC}\right\rangle = \sum\limits_{i=1}^{n} \sqrt{\lambda_i}\left|\phi_i^A\right\rangle\left|\phi_i^B\right\rangle\left|\phi_i^C\right\rangle$. What is the state of the system if the number of expansion coefficients λ_i is $n = 1$.

    ✗ entangled state (inseparability)

✓ separable state

29. The quantum system consists of 3 subsystems. Its state is defined by Schmidt decomposition $\left|\psi^{ABC}\right\rangle = \sum_{i=1}^{n} \sqrt{\lambda_i} \left|\phi_i^A\right\rangle \left|\phi_i^B\right\rangle \left|\phi_i^C\right\rangle$. What is the state of the system if the number of expansion coefficients λ_i is $n = 4$.

    ✓ entangled state (inseparability)
    ✘ separable state

30. Which of the Bell states is called the ¨singlet state¨?

    ✘ $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$
    ✘ $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle\,)$
    ✘ $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$
    ✓ $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle - |10\rangle\,)$

31. A pair of electrons is in a joint state $\frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$ is passing through a Stern-Gerlach device. One of the electrons leans upwards. Where will the other electron deviate in this case?

    ✓ upwards
    ✘ downwards
    ✘ leftwards
    ✘ rightwards

32. A pair of particles is in the Bell state $\frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle\,)$. One of the particles is measured in the corresponding basis $\{\,|0\rangle\,, |1\rangle\,\}$. What is the probability of the second particle becoming $|1\rangle$ at the moment when the first particle has been measured?

    ✘ $1/2^{1/4}$
    ✘ $1/2^{1/2}$
    ✓ $1/2$
    ✘ 1

33. Answer yes or no: The Copenhagen interpretation of quantum mechanics (Niels Bohr) is based on Laplace determinism.

    → **No**

34. Answer yes or no: The concept of hidden variables (Albert Einstein) suggests that the values we get during an experiment are determined in advance. But since there are a lot of variables, we do not take them all into account. Therefore, the values in the course of the experiment seem random and we only produce a statistical averaging over them.

    → **Yes**

35. Answer yes or no: The Copenhagen interpretation argues that there is no point in discussing any physical results without additional description of the instruments which they were obtained with.

    → **Yes**

36. Answer yes or no: In the concept of hidden variables the process of measurement of an observable $\hat{L}$ is as follows: The device decomposes the quantum state of the system on its own basis of macroscopically distinguishable states. Then, in the measurement process, one of these basis states is triggered.

    → **No**

37. What did the experiment to test Bell's inequality determine?

    ✓ The classical concept of hidden variables does not describe the quantum behaviour of systems.

    ✓ The Copenhagen interpretation of quantum mechanics is consistent with the experiments.

    ✘ Laplace determinism allows us to describe the behaviour of quantum systems.

38. If Bell's inequalities are violated:

    ✓ Quantum mechanics is correct

    ✘ The concept of hidden variables is correct

39. If Bell's inequalities are satisfied:

    ✓ Quantum mechanics is correct

    ✓ The concept of hidden variables is correct

40. Bell's inequalities are constructed on the basis of classical probability theory. As a result, there is an estimated value S_{cl} which can be measured in the experiment. Quantum theory also gives the value of the quantity S_q. Which of the values is greater in case of violation of the inequalities?

    ✓ $S_{cl} < S_q$

    ✘ $S_{cl} > S_q$

    ✘ $S_{cl} = S_q$

41. Find the Schmidt decomposition coefficients λ_i (i=1,2,3,4) for the states of the composite system A+B

$$\left|\psi^{AB}\right\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$$

    Here the state of each subsystem belongs to a two-dimensional basis $\{\,|0\rangle, |1\rangle\,\}$, i.e. the vectors $\left|\psi^{AB}\right\rangle$ belong to a four-dimensional Hilbert space $\{\,|00\rangle, |01\rangle, |10\rangle, |11\rangle\,\}$.

    ✓ $\lambda_1 = 1/2, \lambda_2 = 0, \lambda_3 = 0, \lambda_4 = 1/2$

    ✘ $\lambda_1 = 1, \lambda_2 = 0, \lambda_3 = 0, \lambda_4 = 0$

42. Find the Schmidt decomposition coefficients λ_i (i=1,2,3,4) for the states of the composite system A+B

$$\left|\psi^{AB}\right\rangle = |00\rangle$$

    Here the state of each subsystem belongs to a two-dimensional basis $\{\,|0\rangle, |1\rangle\,\}$, i.e. the vectors $\left|\psi^{AB}\right\rangle$ belong to a four-dimensional Hilbert space $\{\,|00\rangle, |01\rangle, |10\rangle, |11\rangle\,\}$.

    ✘ $\lambda_1 = 1/2, \lambda_2 = 0, \lambda_3 = 0, \lambda_4 = 1/2$

    ✓ $\lambda_1 = 1, \lambda_2 = 0, \lambda_3 = 0, \lambda_4 = 0$

43. There are two subsystems, A and B, in one of the Bell states. Find the reduced density matrix $\hat{\varrho}_B = \mathrm{Tr}_A(\varrho_{AB})$ for the Bell state

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$$

- ✘ $\begin{pmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix}$
- ✓ $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$
- ✘ $\begin{pmatrix} 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 \end{pmatrix}$
- ✘ $\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$

44. There are two subsystems, A and B, in one of the Bell states. Find the reduced density matrix $\hat{\varrho}_B = \mathrm{Tr}_A(\varrho_{AB})$ for the Bell state

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle\,)$$

- ✘ $\begin{pmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix}$
- ✓ $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$
- ✘ $\begin{pmatrix} 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 \end{pmatrix}$
- ✘ $\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$

45. There are two subsystems, A and B, in one of the Bell states. Find the reduced density matrix $\hat{\varrho}_B = \mathrm{Tr}_A(\varrho_{AB})$ for the Bell state

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$$

- ✘ $\begin{pmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix}$
- ✓ $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$
- ✘ $\begin{pmatrix} 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 \end{pmatrix}$
- ✘ $\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$

46. There are two subsystems, A and B, in one of the Bell states. Find the reduced density matrix $\hat{\varrho}_B = \mathrm{Tr}_A(\varrho_{AB})$ for the Bell state

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle - |10\rangle\,)$$

- ✘ $\begin{pmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix}$
- ✓ $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$
- ✘ $\begin{pmatrix} 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 \end{pmatrix}$

✘ $\begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$

47. The quantum system consists of two qubits and is in the Bell state of the form $\frac{1}{\sqrt{2}}(\,|10\rangle - |01\rangle\,)$. Which statistical operator will describe the system after averaging over the states of the second qubit?

    ✘ $\frac{1}{\sqrt{2}}(\,|0\rangle\langle 0| + |1\rangle\langle 1|\,)$
    ✘ $\frac{1}{\sqrt{2}}(\,|0\rangle\langle 0| - |1\rangle\langle 1|\,)$
    ✓ $\frac{1}{2}(\,|0\rangle\langle 0| + |1\rangle\langle 1|\,)$
    ✘ $\frac{1}{2}(\,|0\rangle\langle 0| - |1\rangle\langle 1|\,)$

48. What are the Bell states in the matrix representation if the basis vectors are written as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Match the Bell state $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$ to a vector column:

    ✘ $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

    ✘ $\frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$

    ✓ $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$

    ✘ $\frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$

49. What are the Bell states in the matrix representation if the basis vectors are written as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Match the Bell state $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle - |10\rangle\,)$ to a vector column:

    ✘ $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

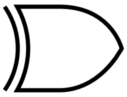
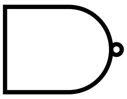
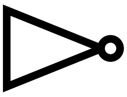
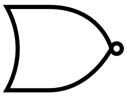
    ✓ $\frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$

    ✘ $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$

    ✘ $\frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$

A.5 Chapter 5

1. Find a schematic drawing of the XOR element:

[✓]  [✘]  [✘]  [✘] 

2. Which operation corresponds to the action of the logical AND?

    ✘ addition modulo

    ✓ logical multiplication

    ✘ delete a bit

    ✘ logical negation

3. What is the value of the output bit c of the logical gate OR if the input bits are $a = 0; b = 1$?

    ✘ $c = 0$

    ✓ $c = 1$

4. If someone sends $a = 1$ and $b = 1$ to the input of the half-adder, what is the value of the carry bit c?

    ✘ $c = 0$

    ✓ $c = 1$

5. If someone sends $a = 1$, $b = 1$, and $d = 1$ to the input of the full-adder, what is the value of the carry bit c_3?

    ✘ $c_3 = 0$

    ✓ $c_3 = 1$

6. Choose a row that contains only irreversible logic gates:

    ✘ NOT, CNOT, CCNOT

    ✘ NOT, OR, CNOT

    ✘ CNOT, CCNOT, AND

    ✓ AND, OR, XOR

7. What should be the value of the control bit c on the input of the CNOT gate, so that CNOT works as a logical FANOUT element to the target bit a?

    ✘ $c = 1$

    ✓ $c = 0$

8. If someone sends $a_1 = 1$, $b_1 = 1$, and $c = 1$ to the input of the full-adder with reversible elements, what are the values of the b_2 and d_2 on the output of the scheme?

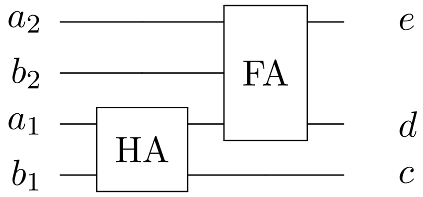
    ✘ $b_2 = 0; d_2 = 0$

    ✘ $b_2 = 1; d_2 = 0$

    ✓ $b_2 = 0; d_2 = 1$

    ✘ $b_2 = 1; d_2 = 1$

9. You can see in the Figure below a cascade circuit that allows someone to add two-digit numbers in the binary numerical system. Here a_1 and b_1 are the first digits starting from the right side of the numbers, that are added together, a_2 and b_2 the second ones. If someone wants to calculate the sum of 1 and 3, what are the values of c, d, e and what is the meaning of these numbers?



✘ $e = 0$ the first digit starting from the right side; $d = 0$ the second; $c = 1$ the third

✘ $c = 0$ the first digit starting from the right side; $d = 1$ the second; $c = 1$ the third

✓ $c = 0$ the first digit starting from the right side; $d = 0$ the second; $c = 1$ the third

✘ $e = 0$ the first digit starting from the right side; $d = 1$ the second; $c = 1$ the third

A.6 Chapter 6

1. What is the value of the commutator $[\sigma_y, \sigma_x]$

✘ $\begin{pmatrix} 2\mathrm{i} & 0 \\ 0 & -2\mathrm{i} \end{pmatrix}$

✓ $\begin{pmatrix} -2\mathrm{i} & 0 \\ 0 & 2\mathrm{i} \end{pmatrix}$

✘ $\begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}$

✘ $\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$

2. Choose a matrix that corresponds to the rotating operator on the angle $\pi/2$ around the x-axis:

✓ $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -\mathrm{i} \\ -\mathrm{i} & 1 \end{pmatrix}$

✘ $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$

✘ $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \mathrm{i} \\ \mathrm{i} & 1 \end{pmatrix}$

✘ $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

3. Choose a row that contains the universal set of gates for single-qubit elements:

✘ $\{H, Y\}$

✘ $\{H, X\}$

✘ $\{H, \mathrm{I}\}$

✓ $\{\mathrm{I}, X, Y, Z\}$

4. What is the result of the operation $ZH\left|1\right\rangle$?

   ✘ $\left|-\right\rangle$

   ✓ $\left|+\right\rangle$

   ✘ $\left|0\right\rangle$

   ✘ $\left|1\right\rangle$

5. If someone sends $\left|a\right\rangle = \left|1\right\rangle$ and $\left|c\right\rangle = \left|1\right\rangle$ to the input of the CNOT element, what is the value of the target qubit on the output of the scheme?

   ✓ $\left|a'\right\rangle = \left|0\right\rangle$

   ✘ $\left|a'\right\rangle = \left|1\right\rangle$

6. Select the correct set of equalities:

   ✘ $YR_1(\phi)Y = -R_1(\phi)$; $YR_2(\phi)Y = -R_2(\phi)$; $YR_3(\phi)Y = R_3(-\phi)$

   ✓ $YR_1(\phi)Y = R_1(-\phi)$; $YR_2(\phi)Y = R_2(\phi)$; $YR_3(\phi)Y = R_3(-\phi)$

   ✘ $YR_1(\phi)Y = R_1(-\phi)$; $YR_2(\phi)Y = R_2(-\phi)$; $YR_3(\phi)Y = -R_3(\phi)$

   ✘ $YR_1(\phi)Y = -R_1(\phi)$; $YR_2(\phi)Y = R_2(\phi)$; $YR_3(\phi)Y = -R_3(\phi)$

7. Represent the sequence of the single-qubit gates HXH in the form of the rotation on the Bloch sphere:

   ✘ $HXH = -X$

   ✘ $HXH = Y$

   ✓ $HXH = Z$

   ✘ $HXH = X$

8. The qubit in the state $\left|\Psi\right\rangle = \frac{\mathrm{i}-\sqrt{2}}{3}\left|0\right\rangle - \frac{2+\mathrm{i}\sqrt{2}}{3}\left|1\right\rangle$ is measured in the Hadamard basis $\{\left|+\right\rangle, \left|-\right\rangle\}$. What is the probability of detecting a qubit in the state $\left|-\right\rangle$ after the measurement?

   ✘ $\frac{9+2\sqrt{2}}{36}$

   ✘ $\frac{9+2\sqrt{2}}{18}$

   ✓ $\frac{9-2\sqrt{2}}{18}$

   ✘ $\frac{9-2\sqrt{2}}{36}$

9. Select a correct matrix representation of the CU gate if U = Z:

   ✘ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

   ✓ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

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

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

10. If someone sends $|a\rangle = |-\rangle$ and $|c\rangle = |+\rangle$ to the input of the CNOT element, what are the values of the target and control qubits on the output of the scheme?

✓ $|a'\rangle = |-\rangle, |c'\rangle = |-\rangle$

✘ $|a'\rangle = |+\rangle, |c'\rangle = |+\rangle$

✘ $|a'\rangle = |+\rangle, |c'\rangle = |-\rangle$

✘ $|a'\rangle = |-\rangle, |c'\rangle = |+\rangle$

A.7 Chapter 7

1. If we are given a function $f(x) : \{0,1\} \to \{0,1\}$ and $f(0) = 1, f(1) = 1$. In this case, $f(x)$ is

✓ constant

✘ balanced

2. If the first qubit is turned to be in the state $|0\rangle$ after the implementation of Deutsch's algorithm, then the function $f(x)$ is

✓ constant

✘ balanced

3. If we are given a function $f(x) : \{0,1\}^2 \to \{0,1\}$ and $|00\rangle = 0$, $f(01) = 1$, $f(10) = 0$, $f(11) = 1$. In this case, $f(x)$ is

✘ constant

✓ balanced

4. If all measured qubits are turned out to be in the state $|0\rangle$ after the implementation of the Deutsch-Josza algorithm, then the function $f(x)$ is

✘ constant

✓ balanced

5. If we are given a function $f(x) : \{0,1\}^2 \to \{0,1\}$ and $|00\rangle = 0$, $f(01) = 1$, $f(10) = 0$, $f(11) = 1$. What is the result of the action $\mathrm{U}_f |10\rangle |1\rangle$

✘ $|10\rangle |0\rangle$

✘ $|01\rangle |1\rangle$

✓ $|10\rangle |1\rangle$

✘ $|01\rangle |0\rangle$

6. Rewrite the binary fraction 0.101 as an ordinary fraction:

✘ $\frac{7}{8}$

✘ $\frac{1}{4}$

✓ $\frac{5}{8}$

✘ $\frac{5}{16}$

7. Which gate performs the quantum Fourier transform with one qubit?

- ✘ Y element
- ✘ X element
- ✘ phase element T
- ✓ Hadamard element H

8. Calculate quantum Fourier transform on $|\psi\rangle = \frac{3}{\sqrt{10}}|0\rangle + \frac{1}{\sqrt{10}}|1\rangle$ and select the right answer:

   - ✘ $|\psi\rangle = \frac{1}{\sqrt{10}}|0\rangle + \frac{3}{\sqrt{10}}|1\rangle$
   - ✘ $|\psi\rangle = \frac{3}{\sqrt{10}}|0\rangle + \frac{1}{\sqrt{10}}|1\rangle$
   - ✓ $|\psi\rangle = \frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle$
   - ✘ $|\psi\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$

9. Choose the eigenvector that corresponds to the eigenvalue $e^{i\pi}$ for the X element:

   - ✘ $|1\rangle$
   - ✘ $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
   - ✘ $|0\rangle$
   - ✓ $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

10. Choose the correct matrix representation for the inverse single-qubit quantum Fourier transform:

    - ✓ $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$
    - ✘ $\sqrt{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$
    - ✘ $\frac{1}{\sqrt{2}}\begin{pmatrix}-1 & -1\\ -1 & 1\end{pmatrix}$
    - ✘ $\sqrt{2}\begin{pmatrix}-1 & -1\\ -1 & 1\end{pmatrix}$

11. Assume $|u\rangle$ is an eigenvector for the X element with the eigenvalues to $e^{i\pi}$: in which state will the qubit from the first register be in after the application of the phase estimation algorithm?

    - ✘ $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
    - ✘ $|0\rangle$
    - ✘ $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
    - ✓ $|1\rangle$

12. Find the order of $a = 5$ modulo $M = 21$

    - ✘ $r = 3$
    - ✘ $r = 4$
    - ✘ $r = 5$
    - ✓ $r = 6$

13. If someone knows the order r of a modulo M, then the prime numbers p and q can be found as

    - ✘ $\gcd(a^r \pm 1, M)$

- ✓ $\gcd(a^{r/2} \pm 1, M)$
- ✘ $\gcd(a^{r/2}, M)$
- ✘ $\gcd(a^{r}, M)$

14. In which state will the qubits be after the first stage of Shor's algorithm?

- ✘ $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |0\rangle\, |y_M(x)\rangle$
- ✘ $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |1\rangle\, |1\rangle$
- ✘ $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\, |0\rangle$
- ✓ $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\, |y_M(x)\rangle$

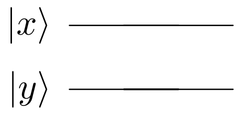
15. Let us assume that the first stage of Shor's algorithm, after measuring the second register $|Y\rangle$, we obtain the state $|2\rangle$. Select the row that contains the first three terms of the first register $|X\rangle$ up to the common factor?

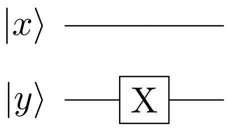
- ✘ $|0\rangle, |4\rangle, |8\rangle$
- ✓ $|1\rangle, |5\rangle, |9\rangle$
- ✘ $|2\rangle, |6\rangle, |10\rangle$
- ✘ $|3\rangle, |7\rangle, |11\rangle$

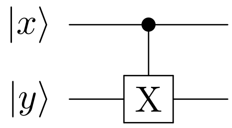
16. Select the correct matrix representation for the unitary transformation U_f in the case of $f(x)$ is balanced and $f(0) = 1,\ f(1) = 0$:

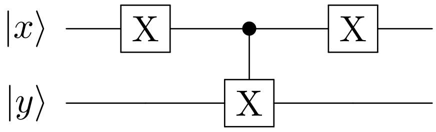
- ✘ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
- ✘ $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
- ✓ $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
- ✘ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

17. Let $f(x)$ be a balanced function and $f(0) = 0,\ f(1) = 1$: Select the correct schematic drawing of U_f for the above function:

✘ 

✘ 

✓ 

✗ 

18. If we are given a function $f(x) : \{0,1\}^2 \to \{0,1\}$ and $f(00) = 1,\ f(01) = 0,\ f(10) = 1, f(11) = 0$, in which state will the measured qubits be after an implementation of the Deutsch-Josza algorithm with accuracy up to the phase factor?

    - ✗ $|10\rangle$
    - ✓ $|01\rangle$
    - ✗ $|11\rangle$
    - ✗ $|00\rangle$

19. Calculate the quantum Fourier transform on $|\psi\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$:

    - ✗ $\frac{1+\mathrm{i}}{2\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle + \frac{1-\mathrm{i}}{2\sqrt{2}}|11\rangle$
    - ✓ $\frac{1+\mathrm{i}}{2\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + \frac{1-\mathrm{i}}{2\sqrt{2}}|11\rangle$
    - ✗ $\frac{1}{\sqrt{2}}|00\rangle + \frac{1-\mathrm{i}}{2\sqrt{2}}|10\rangle + \frac{1+\mathrm{i}}{2\sqrt{2}}|11\rangle$
    - ✗ $\frac{1}{\sqrt{2}}|01\rangle + \frac{1+\mathrm{i}}{2\sqrt{2}}|10\rangle + \frac{1-\mathrm{i}}{2\sqrt{2}}|11\rangle$

20. If $y_{21}(x) = 5^x \bmod 21$ in Shor's algorithm, then before measuring the second register $|Y\rangle$, the first seven states of the qubits from the first and second register can be written with accuracy up to the common factor as

    - ✓ $|0\rangle|1\rangle, |1\rangle|5\rangle, |2\rangle|4\rangle, |3\rangle|20\rangle, |4\rangle|16\rangle, |5\rangle|17\rangle, |6\rangle|1\rangle$
    - ✗ $|0\rangle|1\rangle, |1\rangle|5\rangle, |2\rangle|4\rangle, |3\rangle|21\rangle, |4\rangle|16\rangle, |5\rangle|1\rangle, |6\rangle|2\rangle$
    - ✗ $|0\rangle|1\rangle, |1\rangle|5\rangle, |2\rangle|4\rangle, |3\rangle|20\rangle, |4\rangle|17\rangle, |5\rangle|16\rangle, |6\rangle|1\rangle$
    - ✗ $|0\rangle|1\rangle, |1\rangle|5\rangle, |2\rangle|4\rangle, |3\rangle|21\rangle, |4\rangle|16\rangle, |5\rangle|17\rangle, |6\rangle|2\rangle$

A.8 Chapter 8

1. Which errors are correctable?

    - ✓ Errors that keep different codewords distinguishable
    - ✗ Errors that transform one codewords into another
    - ✗ Errors that change only one of the codewords

2. What are the probabilities of the three-bit error code being effective?

    - ✓ $P < 1/2$
    - ✗ $P > 1/3$
    - ✗ $P = 1$
    - ✓ $P < 1/3$

3. When comparing parity in the case of a three-bit error code, we receive that the 1st bit in the codeword does not match the parity of the service bits. It means that:

    - ✗ An error did not occur
    - ✗ An error occurred in the service bit

- ✓ An error occurred in the first bit

4. What type of errors correspond to the action of the logical operator Z on the qubits?
   - ✓ The phase error
   - ✘ The bit error
   - ✘ Phase and bit error

5. Select the operators that transform the states $|000\rangle$ and $|111\rangle$ into the state $|110\rangle$:
   - ✘ $X_1 \otimes X_2 \otimes I_3$ and $X_1 \otimes I_2 \otimes I_3$
   - ✘ $I_1 \otimes X_2 \otimes Z_3$ and $X_1 \otimes X_2 \otimes I_3$
   - ✓ $X_1 \otimes X_2 \otimes I_3$ and $I_1 \otimes I_2 \otimes X_3$
   - ✘ $X_1 \otimes Z_2 \otimes I_3$ and $Z_1 \otimes X_2 \otimes I_3$

6. What phase errors listed below can be corrected using three-qubit quantum error correction codes?
   - ✓ $I_1 \otimes Z_2 \otimes I_3$
   - ✘ $Z_1 \otimes I_2 \otimes Z_3$
   - ✓ $I_1 \otimes I_2 \otimes Z_3$
   - ✘ $Z_1 \otimes Z_2 \otimes Z_3$

7. Which error occurred with a logical qubit in a three-qubit error correction code, if the error syndrome is 01?
   - ✘ X_1
   - ✘ X_2
   - ✓ X_3

8. What phase error occurred with a logical qubit in a three-qubit error correction code, if the measurement of the auxiliary qubits yields $|-+\rangle$?
   - ✘ Z_1
   - ✓ Z_2
   - ✘ Z_3

9. Suppose that after the measurement of the syndrome in the nine-qubit Shor code, we know that there is a phase error in the eighth qubit. What transformations can we make to correct this error?
   - ✓ $I_1 \otimes I_2 \otimes I_3 \otimes Z_4 \otimes Z_5 \otimes I_6 \otimes I_7 \otimes Z_8 \otimes I_9$
   - ✘ $I_1 \otimes I_2 \otimes I_3 \otimes I_4 \otimes X_5 \otimes I_6 \otimes I_7 \otimes I_8 \otimes I_9$
   - ✘ $I_1 \otimes I_2 \otimes I_3 \otimes I_4 \otimes I_5 \otimes I_6 \otimes I_7 \otimes X_8 Z_8 \otimes I_9$
   - ✓ $I_1 \otimes I_2 \otimes I_3 \otimes I_4 \otimes I_5 \otimes I_6 \otimes I_7 \otimes Z_8 \otimes I_9$

A.9 Chapter 9

1. The advantages of quantum computers are...
   - ✓ Possibly smaller size and thus smaller inertia of the computational process base element
   - ✘ Quantum computers are analogue computers, so their repertoire is larger

- ✓ The ability to employ all copies of the computational system in the multiverse to store and process data.

2. Is a tornado a computational process?

   - ✘ Yes
   - ✘ No
   - ✓ It can be, if we learn to distinguish its states and control their switching

✘ Which of the following is **not** a necessary characteristic of a computational process?

- ✘ The process must be a physical process, not a mathematical model or a thought experiment
- ✓ The process must be deterministic
- ✘ The process must have states that we can distinguish

3. Assume that you have to transfer a message over a corrupted channel which can randomly flip one of the bits in your message. You are allowed to send n bits and you can use this channel only once. You do not know which bit is going to be corrupted. There are many possible ways to encode your data so that there will be no information loss (for example you can transfer a message of length $n/3$ three times so the receiver will be able to choose the correct value for each bit comparing the values of it from different copies of the message). How many bits can you correctly transfer with the best possible strategy?

   - ✘ $\log_2 n$
   - ✘ $\frac{n}{3}$
   - ✘ $n - 1$
   - ✓ $n - \log_2 (n+1)$
   - ✘ $\frac{n}{2}$

   As there are $\mathbf{n+1}$ equal probable states (one no error and n one-bit error states), the Shannon entropy of the resulting state is

$$S = -\sum_{i=0}^{n} \frac{1}{n+1} \log_2 \frac{1}{n+1} = \log_2 n + 1$$

   which effectively corresponds to the information of $\mathbf{n - \log_2 (n+1)}$ bits in this state.

4. Assume that you have to use the channel from the previous question which allows you to send 7 bits. Messages of which length (in bits) can you transfer over this channel with no data loss?

   → **According to the formula, we can transfer no more than 4 bits of information**

5. $\sin \mathrm{i} = \ldots$

   - ✓ $\frac{1-\mathrm{e}^2}{2\mathrm{ei}}$
   - ✘ This value is undefined
   - ✘ $\frac{1+\mathrm{e}^2}{2\mathrm{e}}$
   - ✘ $\frac{1-\mathrm{i}}{2}$

6. The state $|\Phi\rangle = \frac{1-\sqrt{2}\mathrm{i}}{4} |0\rangle - \frac{3-2\mathrm{i}}{4} |1\rangle$ is measured in the Hadamard basis $\{\, |+\rangle, |-\rangle \,\}$. What is the probability to obtain $|+\rangle$ as a measurement result?

   - ✓ $\frac{5-2\sqrt{2}}{16}$

- ✘ $\frac{7}{16}$
- ✘ $\frac{11}{32}$
- ✘ $\frac{5-2\sqrt{2}}{32}$

7. What share of non-polarised light passes through the linear polariser?

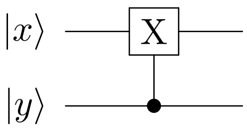
$\int\limits_0^{2\pi} \cos^2(\phi) \frac{\mathrm{d}\phi}{2\pi}$

- ✘ $\frac{2}{\pi}$
- ✓ $\frac{1}{2}$
- ✘ $\frac{1}{3}$
- ✘ $\frac{3}{\pi}$

8. The first qubit of the state $|\Phi\rangle = \frac{1+\sqrt{3}\mathrm{i}}{4}|00\rangle + \frac{1-\sqrt{3}\mathrm{i}}{4}|01\rangle + \frac{1-\sqrt{3}\mathrm{i}}{4}|10\rangle + \frac{1+\sqrt{3}\mathrm{i}}{4}|11\rangle$ was measured in the Hadamard basis with the result $|-\rangle$. What is the probability to obtain the vector $|0\rangle$ as the result of measuring the second qubit in the standard basis $\{\,|0\rangle, |1\rangle\,\}$?

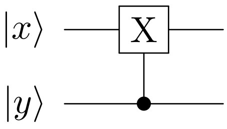
- ✘ 0
- ✓ $\frac{1}{2}$
- ✘ $\frac{3}{16}$
- ✘ 1
- ✘ $\frac{1}{16}$

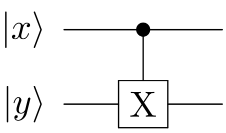
9. What is the matrix (in the standard basis) implemented by this scheme?

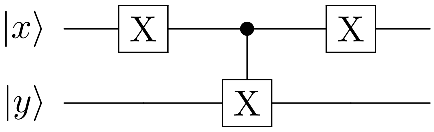


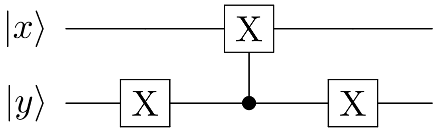
- ✘ $\begin{pmatrix} \mathrm{X} & 0 \\ 0 & X \end{pmatrix}$
- ✘ $\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$
- ✘ $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
- ✓ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

10. Which circuit scheme implements the operator $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

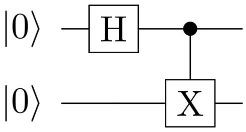
✘ 

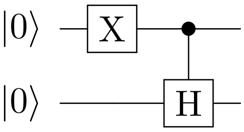
✘ 

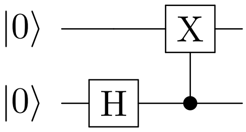
✘ 

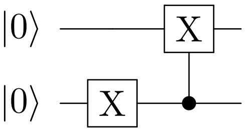
✓ 

11. Which circuit scheme implements the operation $|00\rangle \to \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$?

✓ 

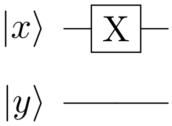
✘ 

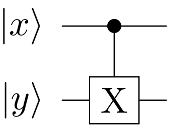
✓ 

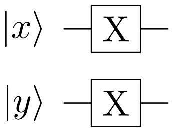
✘ 

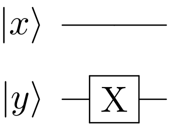
A.10 Chapter 10

1. Which of the following circuit schemes implements the operator $U = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$?

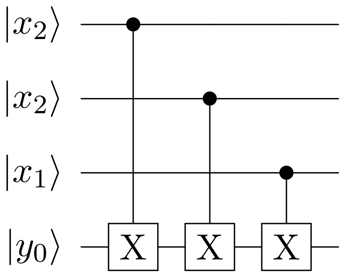
✘ 

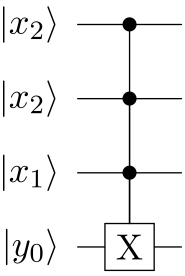
✘ 

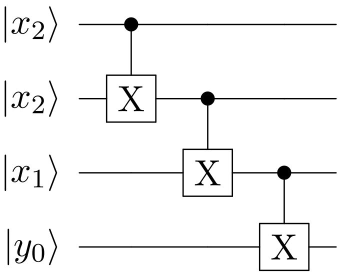
✓ 

✘ 

2. Choose the correct implementation of the U$_f$ operator for the function $f(x):\ \{\,|0\rangle\,, |1\rangle\,\}^3 \to \{\,|0\rangle\,, |1\rangle\,\}$ $f(x) = 7 \cdot x$ (the bitwise vector product between 7 and the state modulo 2)

✘ 

✘ 

✓ 

3. The function $f(x): \{\,|0\rangle, |1\rangle\,\}^2 \to \{\,|0\rangle, |1\rangle\,\}$ $f(x_1, x_0) = x_0$ returns the least significant bit of its argument. Solve the Simon's problem for this function and write down the number a in the decimal numeral system.

   The function maps the following pairs together:

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

   Therefore, the code is a = 10 or 2.

4. The function $f(x): \{\,|0\rangle, |1\rangle\,\}^2 \to \{\,|0\rangle, |1\rangle\,\}$ $f(x_1, x_0) = x_0$ returns the least significant bit of its argument. What is the U_f operator for this function?

   ✘ $\mathrm{CNOT} \otimes \mathrm{I}$

   ✘ $\mathrm{X} \otimes \mathrm{X} \otimes \mathrm{X}$

   ✘ $\mathrm{X} \otimes \mathrm{I} \otimes \mathrm{X}$

   ✓ $\mathrm{I} \otimes \mathrm{CNOT}$

5. In the Simon's algorithm, we used the intermediary measurement of the value register $|y\rangle$. If we remove this measurement step, how will it change the result of the algorithm?

   ✘ The algorithm will work incorrectly (giving us no information about the number a)

   ✘ The algorithm will work correctly but slower, since there are more states to process.

   ✓ Nothing will change. This intermediary measurement was introduced to clarify the algorithm's action. Otherwise, we would have had to write more sum signs.

A.11 Chapter 11

1. The public key for the RSA algorithm is (e,N)=(53,299). The message m was encrypted by this public key: encode(m)=171. Decrypt the message m and write it down as decimal number.

   The prime number decomposition is 299 = 13 · 23. Hence, $\Phi(N) = 12 \cdot 22 = 265$. **From 53d = 1 + 264k we extract d = 5, k = 1 and, therefore, $\mathbf{171^5 \bmod 299 = 19}$**

2. $N = pq = 11409407$ and $f(x) = 19^x \bmod N$. We found the period of f : $r = 475090$. Also we computed $19^{r/2} = 7533861$. Find p and q and write any of them as an answer.

   The greatest common divisor of 7533861 ± 1 and 11409407 is p = 2311 and q = 4937, respectively. These are the prime factors we looked for.

   (Here is the calculation for $p = 2311$

$$\begin{aligned}
11409407 \bmod 7533860 &= 3875547\\
7533860 \bmod 3875547 &= 3658313\\
3875547 \bmod 3658313 &= 217234\\
3658313 \bmod 217234 &= 182569\\
217234 \bmod 182569 &= 34665\\
182569 \bmod 34665 &= 9244\\
34665 \bmod 9244 &= 6933\\
9244 \bmod 6933 &= 2311\\
6933 \bmod 2311 &= 0
\end{aligned}$$

)

3. The value $\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}k}$, $(0 \leq k < n)$ is a root of unity of power n with number k. What is the sum of all roots of unity of power 2019?

   0

4. x is a 4-bit number: $x_3x_2x_1x_0$. Function $f(x) = 7^x \bmod 15$ maps 4 bits to 4 bits.

   ✓ $f(x) = 7^{x_0} \cdot 7^{2x_1} \cdot 7^{4x_2} \cdot 7^{8x_3} \bmod 15$

   ✘ $f(x) = 7^{x_0} \cdot 7^{2x_1} \cdot 7^{3x_2} \bmod 15$

   ✓ $f(x) = 7^{x_0} \cdot 7^{2x_1} \bmod 15$

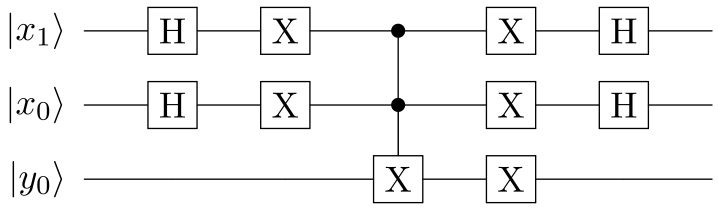
   ✓ $f(x) = 7^{x_0} \cdot 7^{x_0} \cdot 4^{x_1} \bmod 15$

5. We have ran the Shor's algorithm ($n = 8$, $N = 2^8 = 256$) and measure the value $y = 165$. Suppose we are lucky and on the interval $\left[\frac{165}{256} - \frac{1}{512}, \frac{165}{256} + \frac{1}{512}\right]$ there is a rational number $\frac{k}{r}$ with denominator $r < \sqrt{N} = 16$. Find this rational number and write down its denominator. If there is no such number, write 0.

   The sequence of continued fractions is $\mathbf{\frac{1}{2}, \frac{2}{3}, \frac{9}{14}, \frac{20}{31}, \frac{29}{45}, \ldots}$. Therefore, the correct answer is 14 as it is the closest denominator $\mathbf{r < \sqrt{N} = 16}$.

A.12 Chapter 12

1. The U_f operator for a 3-qubit state is implemented by this circuit scheme. The value qubit $|y_0\rangle = \mathrm{H}\,|1\rangle$. Check all the correct statements:



   ✓ The gates H and X applied to $|x_0\rangle$ and $|x_1\rangle$ on the first 2 steps rotate the space so that the vector $|s\rangle$ is mapped to $|11\rangle$.

   ✘ The gates H and X applied to $|x_0\rangle$ and $|x_1\rangle$ on the first 2 steps rotate the space so that the vector $|s\rangle$ is mapped to $|00\rangle$.

   ✓ The CNOT gate acts only on the vector $|11y_0\rangle$, other vectors are untouched by it. So in our rotated space, it acts on the image of vector $|s\rangle$.

   ✓ The CNOT gate multiplies the vector $|11y_0\rangle$ by -1.

   ✘ The gates H and X applied to $|x_0\rangle$ and $|x_1\rangle$ after CNOT rotate the space back so that the vector $|11\rangle$ is mapped back to $|s\rangle$.

   ✓ The gate X on the qubit $|y_0\rangle$ multiplies the system by -1. Thus it returns back the vector $|11y_0\rangle$ and multiplies by -1 all other basis vectors. Among with CNOT it implements the reflection of the state over $|11y_0\rangle$.

2. Is the functional $f(|x\rangle) = \langle x|x\rangle$ differentiable in the linear space over the field of complex numbers?

   ✘ Yes, the Cauchy-Riemann conditions are met

   ✓ No, the Cauchy-Riemann conditions are not met

3. We are going to solve the travelling salesman problem on the graph with 10 vertices with Grover's algorithm. How many Grover iterations are we going to need?

    - ✘ $\lfloor 2^{\frac{\lceil \log_{10} \rceil}{2}-2}\pi \rfloor = 1608$
    - ✓ $\lfloor \frac{\sqrt{10}\pi}{4} \rfloor = 1496$
    - ✘ $\lfloor \frac{10!\pi}{4} \rfloor = 2850052$

4. A small leak from the oracle's function black box allows us to modify the initial state $|s\rangle = \frac{1}{\sqrt{N+2}} \sum\limits_{x \neq \omega} |x\rangle + \sqrt{\frac{3}{N+2}}\, |\omega\rangle$ and the operator U_f for the Grover's algorithm. For big enough N this will allow us

    - ✘ to reduce the number over Grover's iterations 3 times
    - × to reduce the number over Grover's iterations $\sqrt{3}$ times
    - ✘ to reduce the number over Grover's iterations 9 times
    - ✘ nothing. It does not alter the number of iterations.

5. In the following list check all the functions, for which the function ¨Parity¨, introduced in the last lecture, gives 1 (all ¨even¨ functions). All functions in the list map n bit to 1 bit, $n > 1$.

    - ✓ Function f, which returns the least significant bit of its arguments
    - ✓ Function f, which returns the bit with number j of its arguments
    - ✘ the constant function $f(x) = 1$
    - ✓ the constant function $f(x) = 0$
    - ✘ an indicator (characteristic) function of the set $S = \{2, 4, 6, 8, 10\}$

A.13 Chapter 13

1. What tasks can a quantum computer solve?

    - ✘ all tasks from the NP class
    - ✘ all tasks from the EXP class
    - ✓ all tasks from the BQP class
    - ✓ all tasks from the P class

2. What class does the factorisation problem belong to?

    - ✓ to the class NP
    - ✘ to the class EXP
    - ✘ to the class P

3. Choose the correct characteristics for a qubit:

    - ✓ a qubit can be in a superposition state
    - ✓ a qubit is a quantum system with two basis states
    - ✘ a qubit is a classical system with two basis states
    - ✘ a qubit is a quantum system with n basis states

4. How many states can m qubits be in simultaneously?

    - ✘ 2^n
    - ✓ 2^m

- ✘ m
- ✘ $m+2$

5. Choose the correct form of the universal one-qubit unitary transformation operator, taking into account that X, Y, Z are Pauli operators:

   - ✓ $\mathrm{U}(\theta, \boldsymbol{a}) = \cos\frac{\theta}{2}\mathrm{I} - \mathrm{i}(a_x\mathrm{X} + a_y\mathrm{Y} + a_z\mathrm{Z})\sin\frac{\theta}{2}$
   - ✘ $\mathrm{U}(\boldsymbol{a}) = a_x\mathrm{X} + a_y\mathrm{Y} + a_z\mathrm{Z}$
   - ✘ $\mathrm{U} = \mathrm{X} + \mathrm{Y} + \mathrm{Z}$

6. What condition must the operator of all quantum gates satisfy?

   - ✘ operator must be hermitian
   - ✓ operator must be unitary
   - ✘ operator must be self-adjoint

7. Suppose that we send a control qubit in the state $|0\rangle$ and a target qubit in the state $|1\rangle$ to the input of the CNOT transformation. What state will the target qubit have at the output?

   - ✘ $|0\rangle$
   - ✓ $|1\rangle$
   - ✘ $|0\rangle|0\rangle$
   - ✘ $|1\rangle|1\rangle$

8. How is the circuit model of quantum computation similar to the model of classical computation?

   - ✓ The circuit model uses auxiliary devices that implement logic gates
   - ✘ Quantum computation in the circuit model does not surpass classical computation in power
   - ✘ To implement computation in the circuit model, the classical operations AND, XOR, and others are used.

9. What is the principle behind adiabatic quantum computation?

   - ✘ The principle of fast excitation of the ground state of the system
   - ✓ The principle of slow evolution of the ground state of the system
   - ✘ The principle of system evolution through the sequential application of quantum transformations (quantum gates)

10. What is the difference between an anyon and a fermion?

    - ✘ An anyon is no different from a fermion
    - ✓ An anyon is a quasiparticle ¨living¨ on a 2D plane
    - ✓ An anyon has arbitrary statistics
    - ✘ When two anyons swap places, the phase of their common wave function does not change

11. What auxiliary states are needed to implement quantum teleportation?

    - ✘ a specific one-qubit state
    - ✘ two-qubit states whose density matrices can be factorised in the form $\hat{\varrho}_1 \otimes \hat{\varrho}_2$
    - ✓ squeezed states

12. Choose the Bell state $|\beta_0\rangle$:

    ✓ $\frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$

    ✗ $\frac{1}{\sqrt{2}}(\,|00\rangle - |11\rangle\,)$

    ✗ $\frac{1}{\sqrt{2}}(\,|01\rangle + |10\rangle\,)$

    ✗ $\frac{1}{\sqrt{2}}(\,|01\rangle - |10\rangle\,)$

13. What is the final step of the quantum teleportation protocol?

    ✗ Creation of the entangled state

    ✗ Alice measuring her qubits

    ✓ Bob's correction of his qubit

14. How can the quantum teleportation protocol be modified to be used for quantum computation?

    ✓ Use transformed Bell states $\mathrm{U}\,|\beta\rangle$

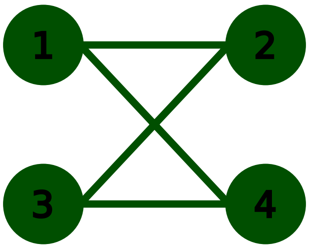
    ✗ Use other entangled states instead of Bell states

    ✓ Use other multiparticle entangled states instead of Bell states, which will be measured locally in different basis states

    ✗ One cannot change the quantum teleportation protocol so that it can be used to implement quantum computation

A.14 Chapter 14

1. Which adjacency matrix does represented graph below correspond to?



✓ $A = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

✗ $A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$

✗ $A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$

✗ $A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

2. Choose the wave function that will be obtained after applying the CPhase operation to the two-qubit state $|-\rangle_1 |-\rangle_2$

   ✓ $|\Psi\rangle = \frac{1}{\sqrt{2}}(\,|0\rangle_1 |-\rangle_2 - |1\rangle_1 |+\rangle_2\,)$
   ✘ $|\Psi\rangle = |0\rangle_1 |-\rangle_2 - |1\rangle_1 |+\rangle_2$
   ✘ $|\Psi\rangle = \frac{1}{\sqrt{2}}(\,|0\rangle_1 |-\rangle_2 + |1\rangle_1 |+\rangle_2\,)$
   ✘ $|\Psi\rangle = \frac{1}{\sqrt{2}}(\,|0\rangle_1 |+\rangle_2 - |1\rangle_1 |-\rangle_2\,)$

3. Choose the wave function of the cluster state, represented by the graph of exercise 1:

   ✓ $|G\rangle = \text{CPhase}_{1,2}\text{CPhase}_{1,4}\text{CPhase}_{2,3}\text{CPhase}_{3,4} |+\rangle_1 |+\rangle_2 |+\rangle_3 |+\rangle_4$
   ✘ $|G\rangle = \text{CPhase}_{1,2}\text{CPhase}_{1,3}\text{CPhase}_{2,4}\text{CPhase}_{3,4} |+\rangle_1 |+\rangle_2 |+\rangle_3 |+\rangle_4$
   ✓ $|G\rangle = \text{CPhase}_{2,1}\text{CPhase}_{2,3}\text{CPhase}_{4,1}\text{CPhase}_{4,3} |+\rangle_1 |+\rangle_2 |+\rangle_3 |+\rangle_4$
   ✘ $|G\rangle = \text{CPhase}_{1,3}\text{CPhase}_{2,3}\text{CPhase}_{1,4}\text{CPhase}_{4,3} |+\rangle_1 |+\rangle_2 |+\rangle_3 |+\rangle_4$

4. What condition must be satisfied so that the operator $\hat{S}$ is a stabilizer?

   ✘ $\hat{S}\,|\Psi\rangle = -\,|\Psi\rangle$
   ✘ $\hat{S}\,|\Psi\rangle = s\,|\Psi\rangle$
   ✘ $\hat{S}\,|\Psi\rangle = 0$
   ✓ $\hat{S}\,|\Psi\rangle = |\Psi\rangle$

5. Choose the number of the cluster state nodes that are neighbours of the node with the number 3 (in the graph of exercise 1):

   ✘ 2,1,4
   ✘ 2,1
   ✓ 2,4
   ✘ 1,4

6. Choose a three-node cluster state stabilizer:

   ✓ $\hat{X}_1\hat{Z}_2\hat{Z}_3$
   ✘ $\hat{X}_1\hat{X}_2\hat{Z}_3$
   ✘ $\hat{Y}_1\hat{X}_2\hat{Z}_3$
   ✘ $\hat{X}_1\hat{Y}_2\hat{Y}_3$

7. Choose the operators of the cluster state stabilizers for the graph in exercise 1

   ✓ $\hat{X}_1\hat{Z}_2\hat{Z}_4$
   ✓ $\hat{X}_2\hat{Z}_1\hat{Z}_3$
   ✘ $\hat{X}_3\hat{Z}_1\hat{Z}_4$
   ✘ $\hat{X}_4\hat{Z}_2\hat{Z}_3$

8. What property should an operator have for it to be measured experimentally?

   ✓ An operator must be Hermitian
   ✘ An operator must be unitary
   ✘ An operator can be arbitrary

9. Let $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle$ be the wave function of the state before measurement. What is the probability that when we measure the Pauli operator $\hat{X}$, we get an eigenvalue equal to +1.

✓ $p = \frac{(a+b)^2}{2}$
✘ $p = \frac{a}{2}$
✘ $p = a$
✘ $p = \frac{1}{2}$

10. Suppose we have the wave function of the multiparticle state $|\Psi\rangle_{12} = a\,|0\rangle_1\,|0\rangle_2 + b\,|1\rangle_1\,|1\rangle_2$ before measurement. Choose the wave function of the second particle after measuring the first particle in the basis of the Pauli operator $\hat{X}$. It is known that the measurement result was an eigenvalue equal to +1.

✘ $|\Psi\rangle_{12} = \frac{1}{\sqrt{2}}(a\,|0\rangle_2 + b\,|1\rangle_2)$
✓ $|\Psi\rangle_{12} = a\,|0\rangle_2 + b\,|1\rangle_2$
✘ $|\Psi\rangle_{12} = |0\rangle_2 + |1\rangle_2$
✘ $|\Psi\rangle_{12} = |0\rangle_2$

11. Choose the wave function obtained as a result of computations on a two-node cluster state, provided that, during the measurements, we had got the values $s_1 = s_2 = 0$.

✓ $|\text{out}\rangle = \mathrm{e}^{\mathrm{i}\frac{\theta_2}{2}\hat{X}}\mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\hat{Z}}\,|\text{in}\rangle$
✘ $|\text{out}\rangle = \mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\hat{Z}}\,|\text{in}\rangle$
✘ $|\text{out}\rangle = \mathrm{e}^{\mathrm{i}\frac{\theta_2}{2}\hat{X}}\,|\text{in}\rangle$
✘ $|\text{out}\rangle = \mathrm{e}^{\mathrm{i}\frac{\theta_2}{2}\hat{Z}}\mathrm{e}^{\mathrm{i}\frac{\theta_1}{2}\hat{X}}\,|\text{in}\rangle$

12. Suppose we want to implement an one-qubit transformation, which is characterised by three Euler angles $\varphi_1, \varphi_2, \varphi_3$. What angles, when measuring a four-node linear cluster state, should we choose to get such a transformation.

✘ $\theta_1 = 0, \theta_2 = 2\varphi_3, \theta_3 = 2\varphi_2, \theta_4 = 2\varphi_1$
✘ $\theta_1 = \pi/2, \theta_2 = 3\varphi_3, \theta_3 = 2\varphi_2, \theta_4 = 2(-1)^{s_1+s_3}\varphi_1$
✓ $\theta_1 = 0, \theta_2 = 2(-1)^{s_1}\varphi_3, \theta_3 = 2\varphi_2, \theta_4 = 2(-1)^{s_1+s_3}\varphi_1$

13. Can the CNOT transformation be implemented using a four-node cluster state?

→ **Yes, it can be.**

14. What is the main problem of practically implementing cluster states using single photons?

✘ Photons move at a high speed
✓ Probabilistic nature of photon generation
✘ Photons are subject to decoherence

15. What operation does the NS gate implement?

✘ $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle \to a\,|0\rangle - b\,|1\rangle$
✘ $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle + c\,|2\rangle \to a\,|0\rangle + b\,|1\rangle + c\,|3\rangle$
✓ $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle + c\,|2\rangle \to a\,|0\rangle + b\,|1\rangle - c\,|3\rangle$
✘ $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle + c\,|2\rangle \to b\,|1\rangle - c\,|3\rangle$

16. Choose the Hamiltonian of the harmonic oscillator

✘ $H = \frac{p^2}{2}$
✘ $H = \frac{\omega^2 q^2}{2}$
✓ $H = \frac{p^2}{2} + \frac{\omega^2 q^2}{2}$

17. What is the name of the operator $\{F, G\} = \frac{\partial F}{\partial q}\frac{\partial G}{\partial p} - \frac{\partial F}{\partial p}\frac{\partial G}{\partial q}$

    ✓ Poisson brackets
    ✘ Pauli brackets
    ✘ commutator

18. How do Poisson brackets change in canonical quantisation?

    ✘ $\{F, G\} \to [\hat{F}, \hat{G}]$
    ✓ $\mathrm{i}\hbar\{F, G\} \to [\hat{F}, \hat{G}]$
    ✘ $\hbar\{F, G\} \to [\hat{F}, \hat{G}]$

19. What does the commutator relation look like between the operator $\hat{a}$ and $\hat{a}^\dagger$?

    ✓ $[\hat{a}, \hat{a}^\dagger] = 1$
    ✘ $[\hat{a}, \hat{a}^\dagger] = \frac{1}{2}$
    ✘ $[\hat{a}, \hat{a}^\dagger] = \mathrm{i}\hbar$

20. Choose the operator for which the Fock state is an eigenstate?

    ✓ $\hat{n} = \hat{a}^\dagger\hat{a}$
    ✘ $\hat{a}^\dagger$
    ✘ $\hat{a}$

21. What operator is called the annihilation operator?

    ✘ $\hat{n} = \hat{a}^\dagger\hat{a}$
    ✘ $\hat{a}^\dagger$
    ✓ $\hat{a}$

22. What is the eigenvalue of the number of particles operator $\hat{n}$ in the state $\hat{a}^\dagger |n\rangle$?

    ✘ n
    ✓ $n + 1$
    ✘ $n - 1$

23. How to define the Fock state with the number n using creation operators $\hat{a}^\dagger$?

    ✘ $\hat{n} = \left(\hat{a}^\dagger\right)^n |0\rangle$
    ✘ $\hat{n} = \frac{1}{\sqrt{n!}} (\hat{a})^n |0\rangle$
    ✓ $\hat{n} = \frac{1}{\sqrt{n!}} \left(\hat{a}^\dagger\right)^n |0\rangle$
    ✘ $\hat{n} = \hat{a} |0\rangle$

24. What is the variance of the generalised coordinate operator in the Fock state?

    ✘ $\Delta\hat{q}^2 = \hbar\omega(n + \frac{1}{2})$
    ✘ $\Delta\hat{q}^2 = n + \frac{1}{2}$
    ✓ $\Delta\hat{q}^2 = \frac{\hbar}{\omega}(n + \frac{1}{2})$

25. Choose the correct uncertainty relation between the generalised coordinate and the momentum for the vacuum state:

    ✘ $\Delta\hat{q}\Delta\hat{p} = \frac{3\hbar}{2}$
    ✓ $\Delta\hat{q}\Delta\hat{p} = \frac{\hbar}{2}$

✘ $\Delta\hat{q}\Delta\hat{p} = \frac{5\hbar}{2}$

✘ $\Delta\hat{q}\Delta\hat{p} = \hbar$

26. Choose the operator for which the Coherent state is an eigenstate?

✘ $\hat{n} = \hat{a}^\dagger\hat{a}$

✘ $\hat{a}^\dagger$

✓ $\hat{a}$

27. What basis do coherent states form?

✘ complete basis

✓ overcomplete basis

✘ non-complete basis

28. What is the average value of the generalised momentum operator in a coherent state $|\alpha\rangle$?

✓ $\langle\hat{p}\rangle = \sqrt{2\hbar\omega}\mathrm{Im}(\alpha)$

✘ $\langle\hat{p}\rangle = \sqrt{\frac{2\hbar}{\omega}}\mathrm{Re}(\alpha)$

✘ $\langle\hat{p}\rangle = \sqrt{2\hbar\omega}\alpha$

✘ $\langle\hat{p}\rangle = 2\hbar\omega\mathrm{Im}(\alpha)$

29. What operator is used to relate the coherent state $|\alpha\rangle$with the vacuum state $|0\rangle$?

✘ $\hat{n} = \hat{a}^\dagger\hat{a}$

✓ $\hat{D}(\alpha) = \mathrm{e}^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$

✘ $\hat{S}(r) = \mathrm{e}^{\frac{1}{2}r\left(\hat{a}^2 - (\alpha\hat{a}^\dagger)^2\right)}$

30. What operator is used to relate the squeezed and coherent states of the field?

✘ $\hat{n} = \hat{a}^\dagger\hat{a}$

✘ $\hat{D}(\alpha) = \mathrm{e}^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$

✓ $\hat{S}(r) = \mathrm{e}^{\frac{1}{2}r\left(\hat{a}^2 - (\alpha\hat{a}^\dagger)^2\right)}$

31. What is the x-quadrature variance in the squeezed state?
(The parameter $r > 0$)

✓ $\Delta\hat{X}^2 = \frac{1}{4}\mathrm{e}^{-2r},\ \Delta\hat{Y}^2 = \frac{1}{4}\mathrm{e}^{2r}$

✘ $\Delta\hat{X}^2 = \frac{1}{4}\mathrm{e}^{2r},\ \Delta\hat{Y}^2 = \frac{1}{4}\mathrm{e}^{-2r}$

✘ $\Delta\hat{X}^2 = \Delta\hat{Y}^2 = \frac{1}{4}$

32. Choose the right uncertainty relation between $\hat{X} = \frac{1}{2}\left(\hat{a}+\hat{a}^\dagger\right)$ and $\hat{Y} = \frac{1}{2\mathrm{i}}\left(\hat{a}-\hat{a}^\dagger\right)$ quadratures for the squeezed state?

✘ $\Delta\hat{X}\Delta\hat{Y} = \frac{1}{4}\mathrm{e}^{-4r}$

✓ $\Delta\hat{X}\Delta\hat{Y} = \frac{1}{4}$

✘ $\Delta\hat{X}\Delta\hat{Y} = \frac{\hbar}{4}$

✘ $\Delta\hat{X}\Delta\hat{Y} = 1$

33. For calculating which average values it is most convenient to use the Glauber-Sudarshan P representation?

✓ normal ordered operators

- ✘ anti-normal ordered operators
- ✘ symmetric ordered operators

34. Is the Husimi Q function positive-definite?

    Yes

35. For calculating which average values it is most convenient to use the Husimi representation?

    - ✘ normal ordered operators
    - ✓ anti-normal ordered operators
    - ✘ symmetric ordered operators

36. If we integrate the Wigner function over one quadrature, we get:

    - ✓ Probability distribution by another quadrature
    - ✘ 0
    - ✘ 1

37. What condition must the Wigner function satisfy for the state to be Gaussian?

    - ✘ It must be non-Gaussian
    - ✓ It must be a Gaussian function
    - ✘ It must be positive-definite

38. What is the minimum number of moments to describe any Gaussian state?

    - ✘ First, second, and third moment
    - ✓ First and second moment
    - ✘ The first four moments

39. What does the vacuum state covariance matrix look like?

    - ✓ $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
    - ✘ $\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
    - ✘ $\sigma = \begin{pmatrix} \mathrm{e}^{-2r} & 0 \\ 0 & \mathrm{e}^{2r} \end{pmatrix}$

40. Choose the correct definition of Gaussian transformations:

    - ✘ Gaussian transformations are transformations that can only be applied to Gaussian state
    - ✓ Gaussian transformations are transformations that do not deduce Gaussian states from Gaussian states from the Gaussian class
    - ✘ Gaussian transformations are transformations that convert non-Gaussian states to Gaussian ones

41. Suppose that we can apply transformations with Hamiltonians $\hat{H}_1$ and $\hat{H}_2$ to the system. Can we also apply the transformation $\hat{H}_3 = \left[[\hat{H}_1, \hat{H}_2], \hat{H}_1\right]$ to this system?

    Yes

42. Choose the transformations you need to be able to perform in order to implement an universal quantum computation?

- ✓ Arbitrary Gaussian transformations and non-Gaussian transformation
- ✘ One arbitrary non-Gaussian transformation and one arbitrary Gaussian transformation
- ✘ One Gaussian transformation and arbitrary Gaussian transformations

43. Is it possible to implement universal quantum transformations using quadrature displacement, squeezing, and CZ transformations?

    No

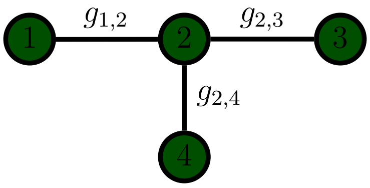
44. What is the first step in an one-way quantum computation?

    - ✘ Implementation of a local measurement
    - ✓ Creation of a cluster state
    - ✘ Mixing input states to cluster state

45. Which states required to generate a continuous-variable cluster state?

    - ✓ Squeezed states
    - ✘ Coherent states
    - ✘ Fock states
    - ✘ Arbitrary Gaussian states

46. Choose the general definition of the wave function of the cluster state corresponding to this graph:



- ✘ $|G\rangle = \mathrm{e}^{2\mathrm{i}g\hat{x}_1\hat{x}_2}\mathrm{e}^{2\mathrm{i}g\hat{x}_2\hat{x}_3}\mathrm{e}^{2\mathrm{i}g\hat{x}_2\hat{x}_4}\,|0\rangle_{y,1}\,|0\rangle_{y,2}\,|0\rangle_{y,3}\,|0\rangle_{y,4}$
- ✓ $|G\rangle = \mathrm{e}^{2\mathrm{i}g_{1,2}\hat{x}_1\hat{x}_2}\mathrm{e}^{2\mathrm{i}g_{2,3}\hat{x}_2\hat{x}_3}\mathrm{e}^{2\mathrm{i}g_{2,4}\hat{x}_2\hat{x}_4}\,|0\rangle_{y,1}\,|0\rangle_{y,2}\,|0\rangle_{y,3}\,|0\rangle_{y,4}$
- ✘ $|G\rangle = \mathrm{e}^{2\mathrm{i}g_{1,2}\hat{x}_1\hat{x}_3}\mathrm{e}^{2\mathrm{i}g_{2,3}\hat{x}_2\hat{x}_3}\mathrm{e}^{2\mathrm{i}g_{2,4}\hat{x}_2\hat{x}_1}\,|0\rangle_{y,1}\,|0\rangle_{y,2}\,|0\rangle_{y,3}\,|0\rangle_{y,4}$

47. Choose the correct definition of the cluster state nullifier operator

    - ✓ $\hat{y}_i - \sum\limits_{j\in N(i)} g_{i,j}\hat{x}_j$
    - ✘ $\hat{y}_1 - \hat{y}_2 - \hat{x}_3$
    - ✘ $\hat{x}_i - \sum\limits_{j\in N(i)} g_{i,j}\hat{x}_j$

48. What are the nullifiers in the graph of exercise 46?

    - ✘

$$\begin{aligned}&\hat{y}_1 - \hat{x}_2,\\ &\hat{y}_2 - \hat{x}_1 - \hat{x}_3 - \hat{x}_4,\\ &\hat{y}_3 - \hat{x}_2,\\ &\hat{y}_4 - \hat{x}_2\end{aligned}$$

✓

$$\begin{aligned}&\hat{y}_1 - g_{1,2}\hat{x}_2,\\&\hat{y}_2 - g_{1,2}\hat{x}_1 - g_{2,3}\hat{x}_3 - g_{2,4}\hat{x}_4,\\&\hat{y}_3 - g_{2,3}\hat{x}_2,\\&\hat{y}_4 - g_{2,4}\hat{x}_2\end{aligned}$$

✘

$$\begin{aligned}&\hat{y}_1 - g_{1,2}\hat{x}_2,\\&\hat{y}_2 - g_{1,2}\hat{x}_1,\\&\hat{y}_3 - g_{2,3}\hat{x}_2,\\&\hat{y}_4 - g_{2,4}\hat{x}_2\end{aligned}$$

49. Choose the correct vector representation of the nullifier operators

- ✓ $\hat{\boldsymbol{N}} = \hat{\boldsymbol{y}} - A\hat{\boldsymbol{x}}$
- ✘ $\hat{\boldsymbol{N}} = \hat{\boldsymbol{y}} - \hat{\boldsymbol{x}}$
- ✘ $\hat{\boldsymbol{N}} = \hat{\boldsymbol{x}} - A\hat{\boldsymbol{y}}$

50. What does the van Loock-Furusawa separability criterion look like for the first and second cluster nodes if the cluster state graph is the one from exercise 46?

- ✘ $\langle\delta\hat{N}_2^2\rangle + \langle\delta\hat{N}_4^2\rangle < |g_{1,2}|$
- ✘ $\langle\delta\hat{N}_2^2\rangle + \langle\delta\hat{N}_4^2\rangle < 1$
- ✓ $\langle\delta\hat{N}_1^2\rangle + \langle\delta\hat{N}_2^2\rangle < |g_{1,2}|$

51. Let us assume that the nullifiers's variance for the first and second cluster state node are greater than 1/2. Will these nodes be entangled if the weight coefficient $g_{1,2}$ between them is equal to one?

- ✘ Nodes will be entangled
- ✓ Nodes will not be entangled

52. What transformations can be used to create a cluster state from a set of squeezed oscillators?

- ✓ linear transformations
- ✘ any non-linear transformation
- ✘ cubic phase-transformations

53. What is the form of the linear transformation matrix that has to be performed to transform independent oscillators in squeezed states into oscillators in a cluster state?

- ✘ $U = (\mathrm{I} + \mathrm{i}A)(\mathrm{I} + A)^{-1/2}Q$
- ✘ $U = (\mathrm{I} + \mathrm{i}A)Q$
- ✓ $U = (\mathrm{I} + \mathrm{i}A)(\mathrm{I} + A^2)^{-1/2}Q$

54. Suppose that to generate a cluster state, we use oscillators whose variance of the squeezed quadratures are less than 1/8. What is the squeezing of these oscillators in decibel units?

- ✘ about -6dB
- ✘ about -2dB
- ✓ about -3dB

A.15 Chapter 15

1. What field characteristics can be measured with homodyne detectors?

   ✓ Combinations of field quadratures
   ✘ field frequency
   ✘ field polarisation

2. What is the final stage of continuous variable one-way quantum computations?

   ✓ Displacement of x and y quadratures
   ✘ Creating a cluster state
   ✘ Local homodyne measurements

3. What cluster states are needed to implement universal single-mode Gaussian transformations?

   ✓ A pair of two-node cluster states
   ✘ A two-node cluster state
   ✓ A four-node linear cluster state
   ✘ A three-node cluster state

4. What is the minimum number of nodes that must be in a cluster state in order to be able to implement the two-mode Gaussian CZ transformation?

   ✘ 2
   ✘ 3
   ✓ 4
   ✘ 5

5. With the help of the measurement of which operator can the transformation of the cubic phase be realised?

   ✓ Particle number operator $\hat{n}$
   ✘ Quadrature operator $\hat{x}$
   ✘ Quadrature operator $\hat{y}$
   ✘ Combination of quadrature operators

6. What are the main difficulties for practical implementation of the cubic phase transformation?

   ✘ Difficulty of measuring the particle number operator
   ✘ The problem of creating a two-mode entangled state
   ✓ Difficulty in the practical implementation of quadrature displacement transformations with large displacement parameters

A.16 Chapter 16

1. What are the principles of any error correcting code?

   ✓ It is necessary to have an idea of the errors we want to correct
   ✓ Principle of information redundancy. All information is redundantly encoded
   ✘ Principle of Quantum Superposition

✘ One can build a code that can correct any possible error

2. What operator sets the qubit-flip error in one qubit?

✓ Pauli $\hat{\mathrm{X}}$ operator
✘ Pauli $\hat{\mathrm{Z}}$ operator
✘ Pauli $\hat{\mathrm{Y}}$ operator

3. Choose operators of 4-qubit errors with weight of 3:

✘ $\mathrm{Z}_1 \otimes \mathrm{Z}_2 \otimes \mathrm{I}_3 \otimes \mathrm{I}_4$
✓ $\mathrm{I}_1 \otimes \mathrm{Z}_2 \otimes \mathrm{Y}_3 \otimes \mathrm{X}_4$
✓ $\mathrm{Z}_1 \otimes \mathrm{Z}_2 \otimes \mathrm{Z}_3 \otimes \mathrm{I}_4$
✘ $\mathrm{X}_1 \otimes \mathrm{I}_2 \otimes \mathrm{I}_3 \otimes \mathrm{Y}_4$

4. What principle must the error satisfy to be detected by the stabilising code with generators $\{\hat{S}_i\}_i$?

✘ Error operator must commute with all code generators
✓ Error operator must anti-commute with all code generators

5. Suppose we have a quantum error correction code that is defined by the codewords $|i\rangle_L$. Choose a necessary and sufficient condition that errors must obey so that they can be compensated for by this code.

✓ ${}_L\langle i|E_a^\dagger E_b\,|j\rangle_L = \delta_{ab}\delta_{ij}$
✘ ${}_L\langle i|E_a^\dagger E_b\,|j\rangle_L = \frac{1}{2}$
✘ ${}_L\langle i|E_a^\dagger E_b\,|j\rangle_L = 0$

6. What errors can a three-qubit code with two codewords $|0\rangle_L = |000\rangle$ and $|1\rangle_1 = |111\rangle$ correct?

✘ Phase errors
✓ Qubit-flip errors
✘ Phase and qubit-flip errors

7. What errors can a three-qubit code with two codewords $|+\rangle_L = |+++\rangle$ and $|-\rangle_1 = |---\rangle$ correct?

✓ Phase errors
✘ Qubit-flip errors
✘ Phase and qubit-flip errors

8. How many errors weighing not more than two can occur in a 7-qubit code?

✓ 210
✘ 100
✘ 81
✘ 9

$$\mathbf{3^1} \cdot \binom{7}{1} + \mathbf{3^2} \cdot \binom{7}{2} = 210$$

9. How many physical qubits does one need to have in a code that will be robust to errors with a weight of no more than 2?

✗ 3

✓ 10

✗ 8

✗ 9

From the previous exercise $N(2) = 210$ and with it, the Hamming bound becomes $210 \cdot 2^2 \leq 2^n$ we need $n = 10$ physical qubits to correct all errors up to an order of two

10. What computational scheme is fault-tolerant?

✓ A scheme in which failure in one component of the scheme results in at most one error in each output block of qubits

✗ A scheme in which one error leads to more than one error in each output block of qubits

✗ A scheme in which errors occur only during the transmission of qubits

11. What is the operator for the displacement x-quadrature errors?

✓ $\hat{D}_x(u) = \mathrm{e}^{-\mathrm{i}u\hat{y}}$

✗ $\hat{D}_x(u) = \mathrm{e}^{-\mathrm{i}u\hat{x}}$

✗ $\hat{D}_x(u) = \mathrm{e}^{-\mathrm{i}u\hat{x}\hat{y}}$

12. What are the two codewords for the GKP state?

✓

$$\begin{aligned} |0\rangle &= \sum_{n\in\mathbb{Z}} |2n\sqrt{\pi}\rangle_x \,, \\ |1\rangle &= \sum_{n\in\mathbb{Z}} \left|(2n+1)\sqrt{\pi}\right\rangle_x \end{aligned}$$

✗

$$\begin{aligned} |1\rangle &= \sum_{n\in\mathbb{Z}} |2n\sqrt{\pi}\rangle_x \,, \\ |0\rangle &= \sum_{n\in\mathbb{Z}} \left|(2n+1)\sqrt{\pi}\right\rangle_x \end{aligned}$$

✗

$$\begin{aligned} |0\rangle &= \sum_{n\in\mathbb{Z}} |2n\rangle_x \,, \\ |1\rangle &= \sum_{n\in\mathbb{Z}} \left|(2n+1)\right\rangle_x \end{aligned}$$

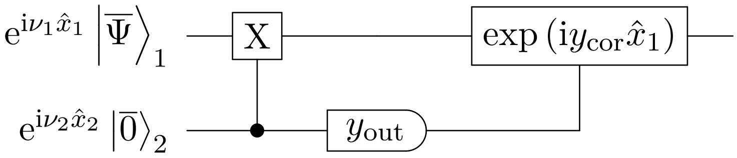
13. How does the GKP state comb transform under the displacement error?

✓ The comb displaces

✗ The comb stretches

✗ The comb squeezes

14. What error can be corrected using the scheme


$e^{i\nu_1 \hat{x}_1} \left|\overline{\Psi}\right\rangle_1$
$e^{i\nu_2 \hat{x}_2} \left|\overline{0}\right\rangle_2$
X
y_{out}
$\exp\left(i y_{\text{cor}} \hat{x}_1\right)$

- ✘ A displacement error in x quadrature
- ✓ A displacement error in y quadrature

15. What is the difference between ideal and imperfect GKP states?

    - ✘ The imperfect state is displaced relative to the ideal one
    - ✘ The peaks of the imperfect state are farther apart than the peaks of the ideal state
    - ✓ The imperfect state has peaks of finite width

16. Is it possible to completely compensate for a quadrature displacement error using imperfect GKP states?

    - ✘ Yes
    - ✓ It is impossible to compensate for the error

17. Which cluster state node should be mixed with GKP states to perform displacement error correction?

    - ✘ Nodes that are also mixed with input states
    - ✘ Nodes that are measured in the process of computation
    - ✓ Unmeasured nodes that will be in the output state