# Introduction to Quantum Informatics

Gniewomir Sarbicki

# Contents

# Convex sets

A subset of an affine space is called *convex*, if any line segment between points of the set is contained in it. Points, which cannot be realised as internal points of a line segment are called *extremal points*.

A compact, convex set is a *convex hull* of its extremal points, i.e. any point of the set can be expressed as a *convex combination* of its extremal points (Krein-Milman theorem). The Caratheodory theorem says, that any such a combination can be realised by a number of points less than dimension of the containing affine space plus one.

# Postulates of quantum mechanics and classical probability calculus

In the probability calculus the central role plays the triple: $(X, \mathcal{F}, \mu)$ - probability space, $\sigma$-algebra of its subsetsbe measure - a function countably-additive on disjoint subsets from $\mathcal{F}$ such that $\mu(X) = 1$ (normalised). A measurable function between probability spaces $f : (X, \mathcal{F}_X) \to (Y, \mathcal{F}_Y)$ is a function such that $\forall A \in \mathbb{F}_Y \ f^{-1}(A) \in \mathcal{F}_X$.

Since now we will focus of finite dimensional case $\#X = n < \infty$ i $\mathcal{F} = 2^X$. We will consider quantum mechanics in a finite-dimensional Hilbert space and probability calculus in a probability space of finite cardinality.

## States, observables, probabilities of results and expected values

Classically if one has a finite $\sigma$-algebra of sets, then an arbitrary probability measure (a state) can be represented by a vector $|p\rangle$ of their values on elementary events. Such a vector has non-negative components summing to 1. The set of states is an $n-1$ dimensional simplex $\Delta^{n-1} = \{(p_1, \ldots, p_n) \in \mathbb{R}^n_+ : \sum_i p_i = 1\}$. Extremal points of set of states are *pure states* - attaining value 1 for an elementary event.

Any function $f : X \to \mathbb{R}$ is now measurable and it is possible to represent it as a covector $\langle f|$ of its values.

The expected value is calculated as $\mathbb{E}_p(f) = \langle f|p\rangle$.

Probability of measuring a value $x$ of the measurable function $f$ is a measure (defined by a state) of preimage of this value: $p(x) = \mu(f^{-1}(x)) = \sum_{i:f_i=x} p_i$.

In Quantum mechanics states are represented by positive-semidefinite operators of unit trace (*density operators*). Extremal points of the set of states are rank-one states, i.e. projectors onto vectors in the Hilbert space (more precisely: onto one-dimensional subspaces). One ure state is represented by a set of unit vectors in the Hilbert space differing by a phase. The set of states is the complex projective space $\mathbb{C}P^{d-1}$.

Measurable quantities in quantum mechanics are represented by hermitian operators. Possible results of measurement of such quantities are eigenvalues of the corresponding operators.

The expected value of the obsevable $F$ in a state $\rho$ is calculated as $\mathrm{Tr}(\rho F)$.

Probability of obtaining an eigenvalue $f_i$ when measuring a quantity $f$ is equal: $\mathrm{Tr}(\rho P_i)$, where $P_i$ is a projector onto eigenspace related to the eigenvalue $f_i$.

## Composite systems

A composite $\sigma$-algebra of two events is a cartesian product of $\sigma$-algebras, among all joint distributions we distinguish independent distributions defined by a products $p_1 \times p_2$ of marginal distributions: $p_1 = \sum_j p_{ij}, p_2 = \sum_i p_{ij}$.

The Hilbert space of the composite system is a tensor product of Hilbert spaces of subsystems.

The marginals (states of subsystems) are defined by partial traces:

$$[\rho_A]_{ij} = \sum_k \rho_{ik,jk} \qquad \text{matrix of traces of blocks} \tag{1}$$

$$[\rho_B]_{ij} = \sum_k \rho_{ki,kj} \qquad \text{sum of diagonal blocks.} \tag{2}$$

If subsystems are independent, the state of the system is a tensor product of subsystems: $\rho = \rho_A \otimes \rho_B$.

## Classical and Quantum Channels

Mappings between probability distributions are called *information channels* and are (in case of finite $\sigma$-algebras) reprezented by stochastic matrices, i.e. of non-negative entries and columns summing to 1.

Quantum channel are positive maps (P), i.e. linear maps between operartor algebras, preserving positivity of operators. A stonger condition must hold: The map $I \otimes \Lambda$ has to be positive for all dimensions of ancilla. In this way we formulate the condition of *complete positivity* (CP), which is easier to solve. The Choi theorem states, that any completely positive map is of the form (Krauss form):

$$\rho \mapsto \sum_i A_i \rho A_i^\dagger, \tag{3}$$

Moreover, a channel should preserve the trace (CPTP). It induce the following condition on the Krauss operators:

$$\sum_i A_i^\dagger A_i = I \tag{4}$$

**Exercise 1** *Prove cyclicity of trace.*

## Measurements

A projective measurement of a measureable function $f$ is a map from the set of measurement results into the set of projectors (characteristic functions) $\chi_{A_i}$ for a splitting of the probability space into disjoint subsets, $f-$measurable (elements of $\sigma_f$). Probability of obtaining the $i$-th result is equal $\mu(A_i) = \int_\Omega \chi_{A_i} d\mu$. The state after measurement is: $\chi_{A_i}\mu/\mu(A_i)$.

A generalised measurement of a measurable function $f$ is a map from the set of measurement results into the set of non-negative, $f$-measurable functions $m_i$, summing to 1 (hence their vectors of values can be interpreted as columns of a stochastic matrix). The generalised measurement takes into account the measurement error - supports of functions $m_i$ overlap. The probability of the $i$-th result is $\int m_i d\mu = \langle m_i|\mu\rangle$.

Post-measurement states are defined by sub-stochastic matrices $K_i$ summing to a stochastic matrix: $K_i\,|\mu\rangle\,/\,\langle\mathbb{1}|\,K_i\,|\mu\rangle$. One has: $\langle m_i| = \langle\mathbb{1}|\,K_i$.

In QM, a projective measurement of an observable $F$ is a map from the set of measurement results into a decomposition of the idetity operator $\mathbb{I}_{\mathcal{H}}$ to a set of projectors $\{P_i\}$ commuting with $F$. The images of projectors are sums of invariant subspaces of $F$ ($F$-measurability of projectors). Probability of obtaining the $i$-th result is $\mathrm{Tr}(\rho P_i)$, and the post-measurement state: $P_i\rho P_i/\mathrm{Tr}(\rho P_i)$.

In QM, a generalised measurement is given by a set $\{\Lambda_i\}$ of subchannels summing to a channel. The probability of obtaining the $i$-th result is $\mathrm{Tr}(\Lambda_i(\rho))$. The post-measurement state is $\Lambda_i(\rho)/\mathrm{Tr}(\Lambda_i(\rho))$.

If we are interested only in the probability of a result, then using cyclicity of trace and linearity one has:

$$\mathrm{Tr}(\Lambda_i(\rho)) = \mathrm{Tr}(\sum_j A_j^{(i)}\rho A_j^{(i)\dagger}) = \sum_j \mathrm{Tr}(A_j^{(i)}\rho A_j^{(i)\dagger}) = \sum_j \mathrm{Tr}(A_j^{(i)\dagger}A_j^{(i)}\rho) = \mathrm{Tr}(\sum_j A_j^{(i)\dagger}A_j^{(i)}\rho) = \mathrm{Tr}(M_i\rho),$$

where $M_i$ are now positive-semidefinite operators summing to $\mathbb{I}$.

Let us check, what happens to the formulas of quantum mechanics, if we restrict ourselves to diagonal observables and states. Then on the diagonals we have the possible values of experiments and their probabilities. The formula for the expected value becomes the classical formula. The formulas for partial traces becomes formulas for marginal distributions. The formulas for probabilities of measurement results and post-mesurement states becomes classical.

Each hermitian matrix is diagonal in some orthonormal basis. These bases (eigenbases) are the same (can be the same if there is a degeneracy) iff the matrices commute. If all observables in a system commute, we won't observe quantum effects.

## Postulates of Quantum Mechanics

To any classical system we prescribe a certain phase space $X$ and to any quantum system we prescribe a certain complex Hilbert space $\mathcal{H}$. Quantum mechanics is a non-commutative generalisation of classical statistical mechanics and as such is a linear theory.

| | Postulate of quantum mechanics | Classical analog |
|---|---|---|
| Algebra of observables and space of states | | |
| 1.1 algebra of obserwables | $\mathcal{B}(\mathcal{H})$ | $L_\infty(X)$ |
| 1.2 space of states | $\mathcal{B}_T(\mathcal{H})$ | $L_\infty(X)^*$ |
| 1.3 pure states | $\rho = \|\psi\rangle\langle\psi\|$ | $\rho = \delta(x, x_0)$ |
| 1.4 space of states of a composite system | $\mathcal{B}(\mathcal{H}_1) \otimes \mathcal{B}(\mathcal{H}_2) \cong \mathcal{B}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ | $L_\infty(X_1)^* \otimes L_\infty(X_2)^* \cong L_\infty(X_1 \times X_2)^*$ |
| 1.5 states of subsystems | $\rho_1 = \mathrm{Tr}_2\rho$ | $\rho_1 = \int_{X_2} d\rho$ |
| Projective (ideal) measurement of an observable $A$ | | |
| 2.1 measuring instrument | mapping of the set of results $w$ into identity decomposition into a finite sum of orthogonal projectors: $a_i \to P_i$ | mapping of the set of results $w$ info finite decomposition of $X$ into disjoint subsets $a_i \to A_i$ |
| | $P_i$ is sum of projectors onto eigenvectors of $A$ (more general: a spectral measure of a subset of the spectrum of $A$) | any level set is contained in exactly one $A_i$ (each $A_i$ is $\sigma_A$-measurable) |
| 2.2 probability of obtaining result $a_i$ | $\mathrm{Tr}(\rho P_i)$ | $\rho(A_i)$ |
| 2.3 state after measurement with a result $a_i$ | $P_i\rho P_i/\mathrm{Tr}\rho P_i$ | $\rho\|_{A_i}/\rho(A_i)$ |
| Dynamics of a closed system (preserving pure states) | | |
| 3.1 evolution generator | arbitrary observable $H$ | arbitrary observable $H$ |
| 3.2 evolution equation | $i\hbar\partial_t\rho = [H, \rho]$ | $\partial_t\rho = \{H, \rho\}$ |
| 3.3 dynamical group | unitary transformations | simplectomorfisms |

Observe, that evolution maps pure states into pure states. If we denote a pure state $\rho(t)$ as $|\psi(t)\rangle\langle\psi(t)|$, then the vector $\psi(t)$ (called a vector state) is governed be the equation:

$$i\hbar\partial_t\psi = H\psi$$

known as Schrödinger equation. Classicaly: Hamilton equation.

**Exercise 2** *Prove, that for a hermitian matrix $H$ the matrix $\exp\left(-\frac{i}{\hbar}Ht\right)$ is unitary.*

# Bloch Ball

Quantum states of a two-level quantum system are represented by semipositive definite $2\times2$ trace-one hermitian matrices. Any such a matrix an be written as:

$$\rho = \frac{1}{2}\begin{bmatrix} 1+z & x-iy \\ x+iy & 1-z \end{bmatrix}. \tag{5}$$

Semipositive-definiteness condition can be expressed as $x^2+y^2+z^2 \leq 1$ - one gets a ball equation. This ball is called *Bloch ball*. On the boundary (on the Bloch sphere) lay rank-1 states - pure states. A trace-1 and rank-1 hermitian operator is a projector on a 1-dimensional subspace spanned by a certain vector $\psi$. If the vector $\psi$ is normalised, one can write down the projector as $|\psi\rangle\langle\psi|$. This vector is called a state vector and is defined up to a phase.

The set of state vectors is sphere $S^3$. The set of pure states is sphere $S^2$. Any pure state is related to a set of state vectors differing by a phase - to a sphere $S^1$. The sphere $S^3$ is then a fibre bundle over a base space $S^2$ with the fibre $S^1$:

$$S^3 \xrightarrow{S^1} S^2 \tag{6}$$

The above fibre is called the *first Hopf fibration*. It is not a trivial bundle ($S^3 \neq S^1 \times S^2$). We prove it showing, that there exists no global projection on $S^1$, so that it is not possible to prescribe to every point on the sphere a "state vector of a canonical phase" and "deviation from the canonical phase" continuously on the whole Bloch sphere.

**Exercise 3** *Introduce a spherical coordinate system $\theta, \phi$ on a Bloch sphere. Show, that it is not possible to prescribe a state vector to a point on the Bloch sphere continuously.*

Space of matrices over $\mathbb{C}$ is equipped in a natural (Hilbert-Schmidt) inner product:

$$\langle A|B\rangle_{HS} = \mathrm{Tr}A^\dagger B \tag{7}$$

**Exercise 4** *Show, that the HS inner product is invariant with respect to the action of unitary group.*

**Corollary:** The HS norm of a hermitian matrix is the euclidean norm of its spectrum.

**Exercise 5** *Show, that HS inner product of two density matrices given by Bloch-ball coordinates $\vec{r}_1 = [x_1, y_1, z_1], \vec{r}_2 = [x_2, y_2, z_2]$ is given by $\frac{1}{2} + \frac{1}{2}\vec{r}_1 \cdot \vec{r}_2$.*

**Exercise 6** *Show, that a pair of projectors onto orthogonal subspaces is related to a pair of antipodal points on the Bloch sphere.*

**Exercise 7** *Characterise the topology of the set of the states of all decompositions of $\mathbb{C}^2$ into a direct sum of two orthogonal subspaces.*

A spectral decomposition of a hermitian matrix is finding its decomposition into a linear combination of projectors onto orthogonal subspaces. In case of a trace-one semipositive definite matrix it will be a convex combination. Graphically, a spectral decomposition in the Bloch ball means to find a diameter passing through the given point, its common points with the Blosh sphere and the coefficients of the

combination. The decomposition is unique for all points except the point in the origin, which is a normalised identity and have the same form in any orthonormal basis.

Observe, that if we release the requirement of orthogonality of projectors in the decomposition, any density matrix can be decomposed in infinitely many ways as a combination of two projectors - one can draw infinitely many chords passing through a point in the Ball. More generally:

**Exercise 8** *Show, that if density matrix has two decompositions:* $\rho = \sum_i \alpha_i |\phi_i\rangle \langle\phi_i| = \sum_i \beta_i |\psi_i\rangle \langle\psi_i|$, *then* $\sqrt{\beta_i}\psi_i = \sum_j a_{ji}\sqrt{\alpha_i}\phi_j$, *and* $a_{ji}$ *are entries of a rectangular matrix* $A$ *with property* $A \cdot A^\dagger = I$.

If $H$ is a diagonal matrix, a solution of the Schrödinger equation

$$i\hbar\partial_t \Psi = H\Psi \tag{8}$$

is

$$\Psi(t) = \exp(-\frac{i}{\hbar}Ht)\Psi(0) = \begin{bmatrix} \exp(-\frac{i}{\hbar}E_0 t)\Psi_0(0) \\ \exp(-\frac{i}{\hbar}E_1 t)\Psi_1(0) \end{bmatrix}. \tag{9}$$

It is a uniform rotation of the Bloch ball around axis $z$. In case of general $H$, it will be a uniform rotation around the diameter spanned by projectors onto eigenvectors of $H$.

A non-informing measurement of an observable given by projectors $P_1, P_2$ in the spectral decomposition is related to a projection of the state onto the diameter spanned by $P_1$ and $P_2$. If the measurement is informing, than there happens a collapse to either $P_1$ or $P_2$ with probabilities proportional to lengths of line segments in the decompositions.

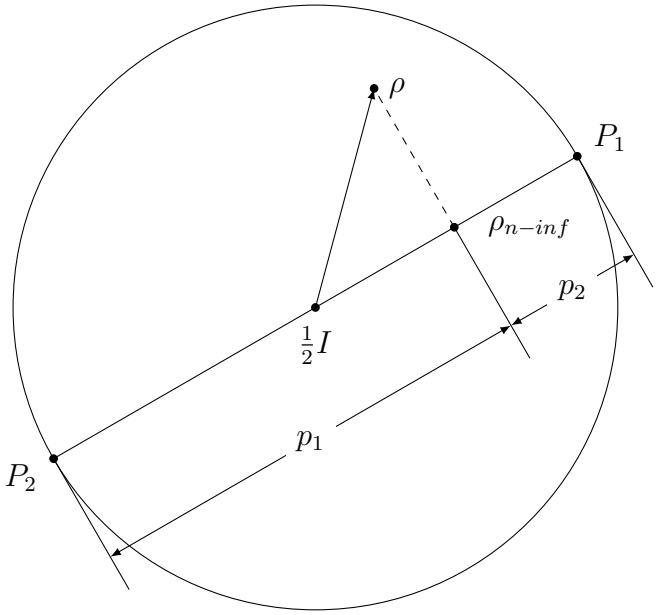



Figure 1: Projective measurement: non-informing (projection on the diameter) and informing (collapse) in the Bloch ball. Picture plane is defined by measuement projectors and the measured state.

# Uncertainty principle

A consequence of non-commutativity of observables is the uncertainty principle. If uncertainty of a certain observable in a certain state is 0, then the state has to be an eigenstate of the observable. For any other observable, non-commuting with the former one, the state is not an eigenstate and the uncertainty won't be 0.

In the information-theoretical approach, the uncertainty for a pair $A, B$ of observables we express as a sum of entopies of distribution of results for both observables in a given state. It's lower bound depends only on relations between their eigenbases. We have the following:

**Theorem (Maasen - Uffink)** Let $p$ and $q$ be probability distributions of measurement results of observables $A$ and $B$ respectively in a certain state $\rho$. The sum of their entropies is lower-bounded by a state-independent quantity:

$$H(p) + H(q) \geq -\log \max_{ij} |\langle a_i | b_j \rangle|^2, \tag{10}$$

where $\{a_i\}$, $\{b_i\}$ are eigenbases of $A$ and $B$ respectively.

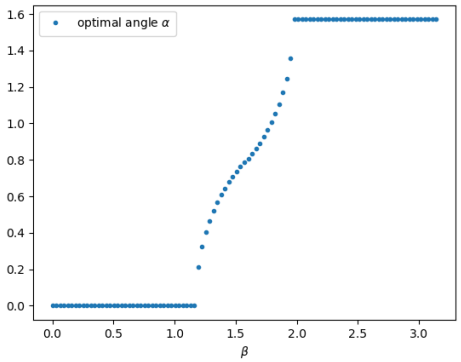
Observe, that one common eigenvector is enough, to make the lowerbound 0. In such case it is tight - choosing a projector onto the common eigenvector as a state, both entropies are zero, hence one can be sure about results of both observables simultaneously.

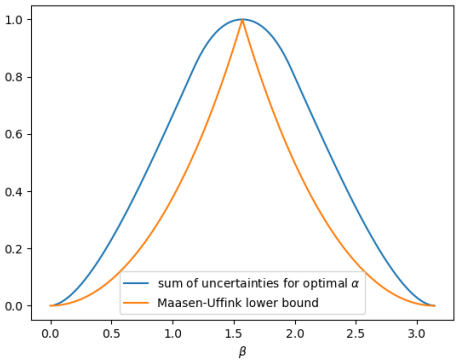
**Exercise 9** *Let $A$ i $B$ bę observables in $\mathbb{C}^2$, and $\beta$ be the angle between diameters of Bloch ball representing their eigenbases.*

- *Find the MU lowerbound for a sum of entropies of probability distributions of measurements of observables.*
- *Find a lowerbound for a sum of entropies of probability distributions of measurements of observables.for a given state and find its minimum.*
- *Show, that the lowerbound is higher (better) than the MU lowerbound.*

```
import numpy as np
from scipy.optimize import minimize

def H(p):
        """binary Shannon entropy of prob. distr. {p,1-p}"""
        res = -(p*np.log(p)+(1-p)*np.log(1-p))/np.log(2)
        res = res * (p < 1) * (p > 0) + 0 * (p == 0) + 0 * (p == 1)      # to handle 0log0
        return res

def sum_of_uncertainties(beta,alpha):
        """For two projective measurements of Bloch coordinates:
{[sin(beta/2),0,cos(beta/2)], [-sin(beta/2),0,-cos(beta/2)]}
{[-sin(beta/2),0,cos(beta/2)], [sin(beta/2),0,-cos(beta/2)]}
and state: [sin(alpha),0,cos(alpha)]
calculates H(p) + H(q), where p and q are prob. distr. of first and second PM respectively
"""
        return H((1+np.cos(beta/2-alpha))/2) + H((1+np.cos(beta/2+alpha))/2)

@np.vectorize
def alpha_opt(beta):
        """For given beta (parameter describing non-commutativity of PMs), returns value of alpha
(state parameter) minimising the function sum_of_uncertainties"""
        f = lambda alpha: sum_of_uncertainties(beta, alpha)
        res = min((minimize(f, np.random.rand()*np.pi/2) for _ in range(5)), key = lambda res: res.fun)
        res = np.abs(res.x) % np.pi
```

```
        if res > np.pi/2: res = np.pi - res
        return res


import matplotlib.pyplot as plt
beta = np.linspace(0,np.pi,101)                                    # range of beta
aa = alpha_opt(beta)                                               # corresponding optimal alphas
# plot optimal alpha in function of beta
plt.plot(beta,aa,'.', label = r'optimal␣angle␣$\alpha$')
plt.legend()
plt.xlabel(r'$\beta$')
plt.show()
# plot minimal sum_of_uncertainties in comparison to Maasen-Uffink bound.
plt.plot(beta,sum_of_uncertainties(beta,aa),label=r'sum␣of␣uncertainties␣for␣optimal␣$\alpha$')
plt.plot(beta,-np.log(np.maximum(np.cos(beta/2)**2,np.sin(beta/2)**2))/np.log(2),
                 label='Maasen-Uffink␣lower␣bound')
plt.legend()
plt.xlabel(r'$\beta$')
plt.show()
```




## MUBs

Two bases $\{e_i\}$ and $\{f_i\}$ in $\mathbb{C}^d$ are called *unbiased*, if $\forall i,j |\langle i|j\rangle|^2 = \frac{1}{d}$. A set of pairwise *unbiased* bases is called *mutually unbiased bases*. Such a set can contain at most $d+1$ bases. We are able to construct such sets when $d$ is a power of prime.

In case when $d$ is prime, the construction goes as follows: Using matrices:

$$X = \begin{bmatrix} & & 1 \\ 1 & & \\ & \ddots & \\ & 1 & \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & & & \\ & \omega & & \\ & & \ddots & \\ & & & \omega^{d-1} \end{bmatrix}$$

we construct matrices $X^\alpha Z^\beta$ of projective representation of the Weyl group. There are $d^2$ of them, and there is of course $I_d$ of them. For the remaining $d^2-1$ matrices we find eigenbases. It turns out, that there is $(d+1)$ such bases, and each of them is the eigenbasis for $(d-1)$ matrices. Obviously, the matrix $(I_d)$ is diagonal in each of them.

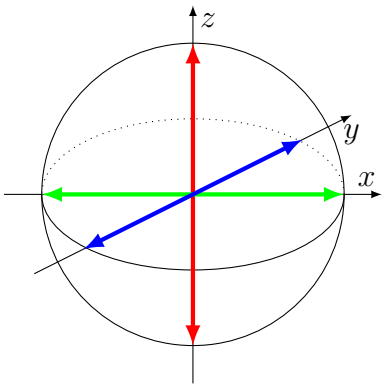
In $d=3$ the construction goes as follows:

| | $\beta = 0$ | $\beta = 1$ | $\beta = 2$ |
|---|---|---|---|
| $\alpha = 0$ | $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ | $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^* \end{bmatrix}$ | $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega^* & 0 \\ 0 & 0 & \omega \end{bmatrix}$ |
| $\alpha = 1$ | $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ | $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & \omega \\ \omega^* & 0 & 0 \end{bmatrix}$ | $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & \omega^* \\ \omega & 0 & 0 \end{bmatrix}$ |
| $\alpha = 2$ | $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ | $\begin{bmatrix} 0 & 0 & 1 \\ \omega & 0 & 0 \\ 0 & \omega^* & 0 \end{bmatrix}$ | $\begin{bmatrix} 0 & 0 & 1 \\ \omega^* & 0 & 0 \\ 0 & \omega & 0 \end{bmatrix}$ |

- basis: $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$
- basis: $\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ \omega \\ \omega^* \end{bmatrix}, \begin{bmatrix} 1 \\ \omega^* \\ \omega \end{bmatrix} \right\}$
- basis: $\left\{ \begin{bmatrix} \omega^* \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ \omega^* \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ \omega^* \end{bmatrix} \right\}$
- basis: $\left\{ \begin{bmatrix} \omega \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ \omega \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ \omega \end{bmatrix} \right\}$

While $d$ is prime, the projective representation of the Weyl group one can treat as a two-dimensional linear space over the field $\mathbb{Z}_d$ (denoted by $\mathbb{Z}_d^2$). It turns out, that elements $X^{\alpha_1}Z^{\beta_1}$ and $X^{\alpha_2}Z^{\beta_2}$ commute (up to a phase), if and only if $\alpha_1\beta_2 - \alpha_2\beta_1 = 0 \mod d$ i.e. when belongs to the same 1-dimensional subspace. Set of eigenbases of elements is hence isomorphic to the set of lines in $\mathbb{Z}_d^2$, hence with the space $\mathbb{Z}_d P^1$.

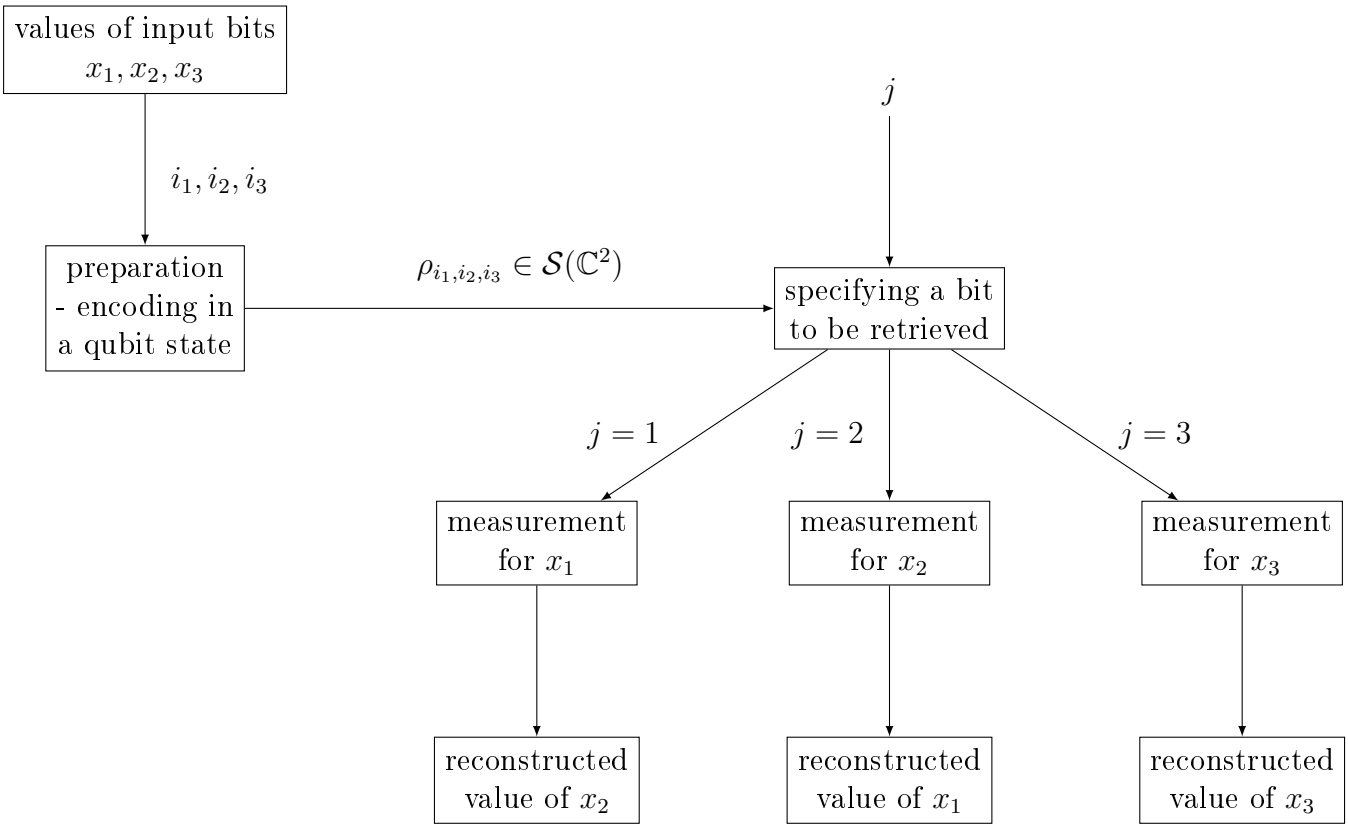
In case of qubit the construction leads to eigenbases of matrices $\sigma_z$, $\sigma_x$ i $\sigma_y \sim \sigma_x\sigma_z$. In the Bloch ball these bases are pair of projectors laying on axes of coordinates:




In $d = 2$, measuring an observables which eigenbases are the subsequent bases from the MUB set, we obtain three expected values equal to coordinates $x$, $y$, and $z$ coordinates of the measured state in the Bloch ball.

In higher dimensions the situation is similar - subspaces of operators diagonal in bases from a MUB set are mutually orthogonal, hence any state projects orthogonally on these $(d+1)$ subspaces. Probabilities of different results of a projective measurement in the given basis lets to reconstruct the value of projection onto a given subspace.

**Random access codes** Let our task be to encode values of three bits into one qubit, to maximise a probability of correct reconstruction of the value of one of the encoded bits, chosen with equal probabilities.




Classically, the maximal probability of a proper reconstruction is equal 2/3 (one qubit encoded, the remaining guessed at random). In quantum case we encode the state of three bits into eight qubit states with coordinates $[\pm 1/\sqrt{3}, \pm 1/\sqrt{3}, \pm 1/\sqrt{3}]$ in the Bloch ball. Depending on $j$ (the number of qubit to be retrieved) we perform a projective measurement in one of MUBs. The probability of correct reconstruction of the value of the choseb bit is $(1 + 1/\sqrt{3})/2 \approx 0.7887$. Using quantum resource we observe a gain in comparison to using classical resources.

# Quantum channels

Maps mapping semipositive definite matrices to semipositive definite matrices are called *positive maps* (P). Looking for a general form of a map mapping states to states one should pose a more restrictive condition: A map $I \otimes \Lambda$ acting on product states $\eta \otimes \rho$ should be positive as well for all possible dimensions of the additional subsystem. In this way we define the *complete positivity* (CP) condition, which is easier to solve. The Choi theorem says, that any completely positive map is of the form (Krauss form):

$$\rho \mapsto \sum_i A_i \rho A_i^\dagger \tag{11}$$

We have met maps of the above form already writing down classical channel in the matrix representation. Then the *phases* (in the polar decomposition) of matrices $A_i$ differed by a cyclic permutation. Releasing the bases gives a CP, trace-preserving map. It turns out, that it is already a most general form of a quantum channel.

We can ask, when two channels given in their Krauss forms represents the same channel. A *stacking technique*, i.e. writing down an $n \times n$ matrix as a vector of $n^2$ coefficients built from rows of the

matrix transposing each of them turns out to be useful here:

$$\rho = \sum_{ij} \rho_{ij} |e_i\rangle \langle e_j| \xrightarrow{\text{stacking}} \vec{\rho} = \sum_{ij} \rho_{ij} |e_i\rangle \otimes |e_j\rangle \tag{12}$$

Sandwiching $\rho$ by $A$ and $B$ is then related to the following mapping of the vector $\vec{\rho}$:

$$A\rho B \longrightarrow A \otimes B^T \ \vec{\rho} \tag{13}$$

In this representation the channel action can be written as

$$\vec{\rho} \mapsto \sum_i A_i \otimes A_i^* \vec{\rho} \tag{14}$$

The channel is uniquely determined by a matrix $\sum_i A_i \otimes A_i^*$, to check if two Krauss representations relate to the same channel, one has to compare the resulting matrices.

**Exercise 10** *Show, that two representations of a channel* $\sum_i A_i \rho A_i^\dagger$ *and* $\sum_i B_i \rho B_i^\dagger$ *are equivalent* $\iff$ $B_i = \sum_j U_{ij} A_j$, *where* $U$ *is a unitary matrix (use the fact, that* $AXB = (B^T \otimes A)\vec{X}$*).*

One can rewrite a matrix $\sum_i A_i^* \otimes A_i$ as $\sum_i \vec{A}_i^* \otimes \vec{A}_i$, what give a vector of $n^4$ entries. One can now "lay" the first term in the tensor produt to get a matrix $\sum_i \vec{A}_i^\dagger \otimes \vec{A}_i = \sum_i \left|\vec{A}_i\right\rangle \left\langle \vec{A}_i\right|$. The minimal length of a channel representation is the rank of the matrix $\sum_i \left|\vec{A}_i\right\rangle \left\langle \vec{A}_i\right|$. One can see that if for $\vec{A}_i$ one chooses eigenvectors of $\sum_i \left|\vec{A}_i\right\rangle \left\langle \vec{A}_i\right|$, then one gets a Krauss representation of the channel where all matrices $A_i$ are orthogonal in the HS inner product.

## CQ and QC channels

A channel, which maps an arbitrary density matrix to diagonal matrix in a fixed basis (reducing a non-commutative case to a commuting one) is called a quantum-classical channel.

**Exercise 11** *Show, that a quantum-classical channel is of the form:*

$$\rho \mapsto \sum_j \mathrm{Tr}(\rho M_j) |j\rangle \langle j| , \quad dla \quad \sum_j M_j = I. \tag{15}$$

Observe, that this is a POVM measurement - the most general linear map prescribing a probability measure to a density matrix.

Channel, which maps diagonal matrices into density matrices (a restriction of a quantum channel to a commuting subalgebra) is called a classical-quantum channel:

$$\rho \mapsto \sum_i \langle i| \rho |i\rangle \rho_i \tag{16}$$

such a channel is called *preparation*.

If $\{M_j\}$ commute, or if $\{\rho_i\}$ commute, then one gets a classical-classical channel.

## Qubit channels

Qubit channels are linear maps mapping Bloch ball into itself. The only surjective (so invertible) channels are rotations around an certain axis - they are represented by a sandwiching $\rho$ by unitary matrices. An image of any channel will be an ellipsoid contained in the Bloch ball.

**Exercise 12** *Which classical channels are invertible?*

Next class of channels, already not invertible are *random unitary* channels, when unitary rotations from a set are applied to a state according to a probability distribution.

**Exercise 13** *Find an image of the channel (bit flip channel):*

$$\rho \mapsto p\rho + (1-p)\sigma_x \rho \sigma_x^\dagger$$

**Exercise 14** *What is a Krauss representation of a channel, which performs scaling of Bloch ball in directions $x, y$ leaving the $z$ direction unchanged (phase flip channel)?*

**Exercise 15** *What is the representation of a channel, which scales the Bloch ball uniformly (depolarising channel)?*

All *random unitary* channels are unital (bistochastic). The opposite implication holds only for qubit.

An *amplitude damping* channel is represented by an isotropic shrinking of the Bloch ball towards its north pole. If the system is a two-level atom with a fixed photon emision probability per time unit, then change of a state of such system in a time interval will be represented by the *amplitude damping* channel.

**Exercise 16** *Find a Krauss representation of a amplitude damping channel. Find the general case of falling onto the Gibbs state.*

**Exercise 17** *How one can parametrise and characterise all qubit channels?*

**Exercise 18** *Show, that the set of qubit channels is 12-dimensional. What these dimensions are related to? How many dimensions has the set of unital channels?*

# Composite systems

**Schmidt decomposition** Let us perform an operation inverse to the stacking operation. A vector $\Psi$ w $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ can be written as a matrix $A$ of a size $d_2 \times d_1$. We can apply a singular value decomposition theorem to this matrix:

$$A = U\Lambda V^\dagger, \tag{17}$$

where $U$ and $V$ are unitary, and $\Lambda$ is positive and diagonal (in general rectangular). In other words:

$$A = \sum_i \lambda_i |u_i\rangle \langle v_i| , \tag{18}$$

for orthonormal sets $\{u_i\} \in \mathbb{C}^{d_2}$ i $\{v_i\} \in \mathbb{C}^{d_1}$. Hence the vector $\Psi$ can be written as $\sum_i \lambda_i v_i \otimes u_i$. We have proven in this way the Schmidt decomposition theorem. The numbers $\lambda_i$ are called Schmidt coefficients of the vector $\Psi$.

**Warning:** There is no simple analog of Schmidt decomposition for a state of a system composed of more than two subsystems.

**Separable and entangled states** If a vector $\Psi$ is a product vector, then the state $|\Psi\rangle \langle\Psi|$ is called a *pure separable state.* A pure state, which is not separable is called *entagled state.* In case of mixed states, a state is separable it can be decomposed into a convex combination of pure separable states. If it is not possible, the state is entangled. The definition applies to arbitrary number of subsystems. Problem of determining the separability of a state is a hard task, we will focus on it in the further parts of the lecture.

**Partial trae of a pure state** Considering partial traces of a vector $\Psi$ of a Schmidt decompostion $\sum_i \lambda_i v_i \otimes u_i$ we get: $\rho_1 = \sum_i \lambda_i^2 |v_i\rangle \langle v_i|$ and $\rho_1 = \lambda_i^2 \sum_i |u_i\rangle \langle u_i|$. Despite having maximal information about the state of the whole (it is in a pure state), we do not have full information about the parts (they are in mixed states). Such a phenomenon is absent in the commutative theory.

# Dilation theorems

**Theorem:** Any density matrix of a $d$-level quantum system can be represented as a partial trace of a pure state of a composed system. Such a pure state is called a *purification* of the state $\rho$.

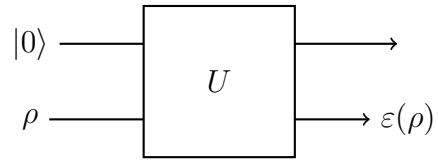
**Exercise 19** *What is the freedom of choice of the state of the composed system being a purification of a given state of a asubsystem?*

**Theorem:** Any quantum channel can be written as $\rho \mapsto \mathrm{Tr}_1(U\eta \otimes \rho U^\dagger)$.

**Proof:** Let us take $\eta = |e_1\rangle \langle e_1|$ and let $U_{ij}$ denote the $ij$-th block of the matrix $U$. Then $\mathrm{Tr}_1(U\eta \otimes \rho U^\dagger) = \sum_i U_{i1} \rho U_{i1}^\dagger$, hence it is in the Krauss form. To proof the opposite implication one has to prove that the matrix having its first column of blocks given can be fulfilled to a whole unitary matrix, under a certain assumption.

**Exercise 20** *Assume, that we have given the first column of blocks of a certain matrix. When it is possible to add a missing part to get a unitary matrix?*

We can describe in on a picture as follows:

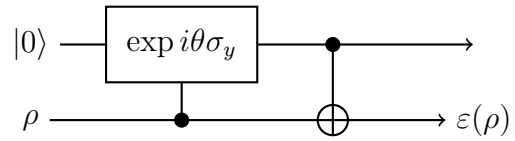



for the same $U$ we can exchange the roles of subsystems. Then we will get so-called *channel complementary* to $\varepsilon$.

**Exercise 21** *Show, that the amplitude damping channel:*

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, A_2 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$$

*can be realised as:*




*where* $\gamma = \sin^2\theta$.

A generalised measurement (POVM) is given by the formula (15), if we are interested only in the probability measure of the output. If in turn we are interested as well in what happens to the system after measurement, we get:

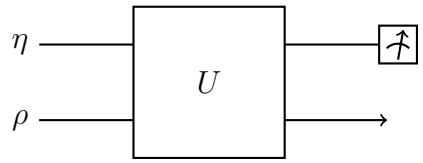
$$\rho \xrightarrow{p_i = \mathrm{Tr}\left(\rho \sum_j X_j^{(i)\dagger} X_j^{(i)}\right)} \frac{\sum_j X_j^{(i)} \rho X_j^{(i)\dagger}}{\mathrm{Tr}\left(\rho \sum_j X_j^{(i)\dagger} X_j^{(i)}\right)}, \quad \sum_{ij} X_j^{(i)\dagger} X_j^{(i)} = I \tag{19}$$

If we are interested only in the probabilities, we pass to the formula (15) by substitution: $M_i = \sum_j X_j^{(i)\dagger} X_j^{(i)}$

**Theorem:** Every generalised measurement on $\rho$ can be realised as a projective measurement of the system with an additional system attached, after a period of common evolution.

**Proof:** Similarly as in the previous proof we start from the state $|e_1\rangle\langle e_1| \otimes \rho$, but the basis of the attched system is indexed by all pairs $ij$. The measurement basis consists of projectors $|e_{ij}\rangle\langle e_{ij}|$, but after measurement a postselection happens causing glueing the results with the same $i$.

We can describe it on a picture as follows:



# POVM Theory

**Distinguishing quantum states - Hellstrøm theory** Assume, that a source produces two states $\rho_1$ and $\rho_2$ with probabilities $p_1$ and $p_2$ respectively. Our task is to construct a two-valued POVM, for which the probability of the orrect answer will be maximal.

Two-valued POVM is of the form $\{A, I - A\}$, dla $0 \leq A \leq I$. We look for the maximum of the expression $\mathrm{Tr}(Ap_1\rho_1) + \mathrm{Tr}((I - A)p_2\rho_2) = p_2 + \mathrm{Tr}(A(p_1\rho_1 - p_2\rho_2))$. We can see, that $A$ should be a projector onto a direct sum of eigenspaces of $p_1\rho_1 - p_2\rho_2$ related to positive eigenvalues.

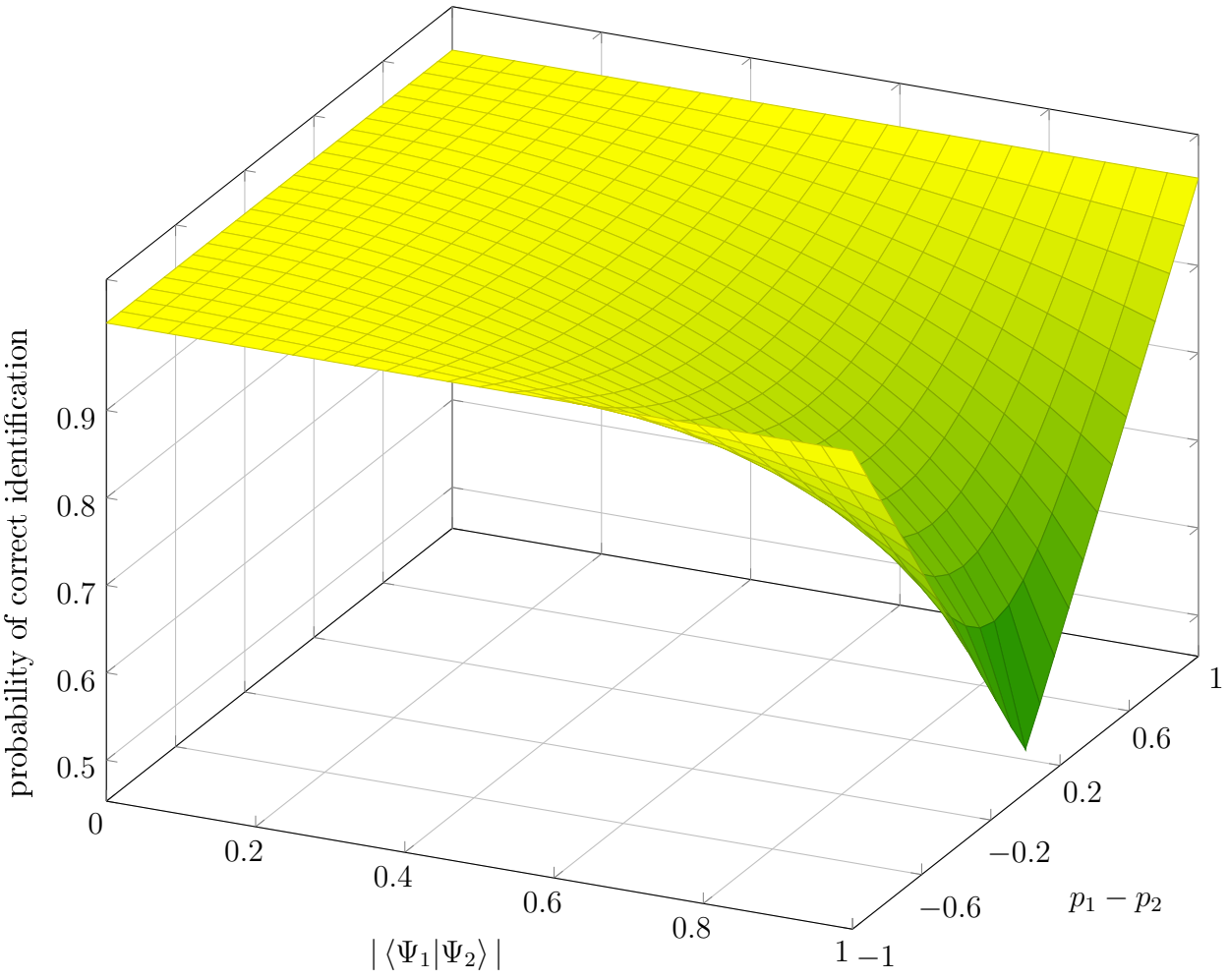
If $p_1\rho_1 \geq p_2\rho_2$, then $A = I$ - it is optimal just to bet on 1 without performing any mesurement.

The matrix $p_1\rho_1 - p_2\rho_2$ is called *Helstrøm matrix*. Probability of obtaining the proper result is equal:

$$p_{success} = \frac{1}{2}\left(1 + ||p_1\rho_1 - p_2\rho_2||_1\right), \tag{20}$$

where $||\cdot||_1$ is the trace norm - the sum of absolute values of eigenvalues.

**Exercise 22** *Derive formula for probability of successful distinguish of two pure states sent with arbitrary probabilities, in terms of* $p_1 - p_2$ *and* $|\langle\Psi_1|\Psi_2\rangle|^2$.

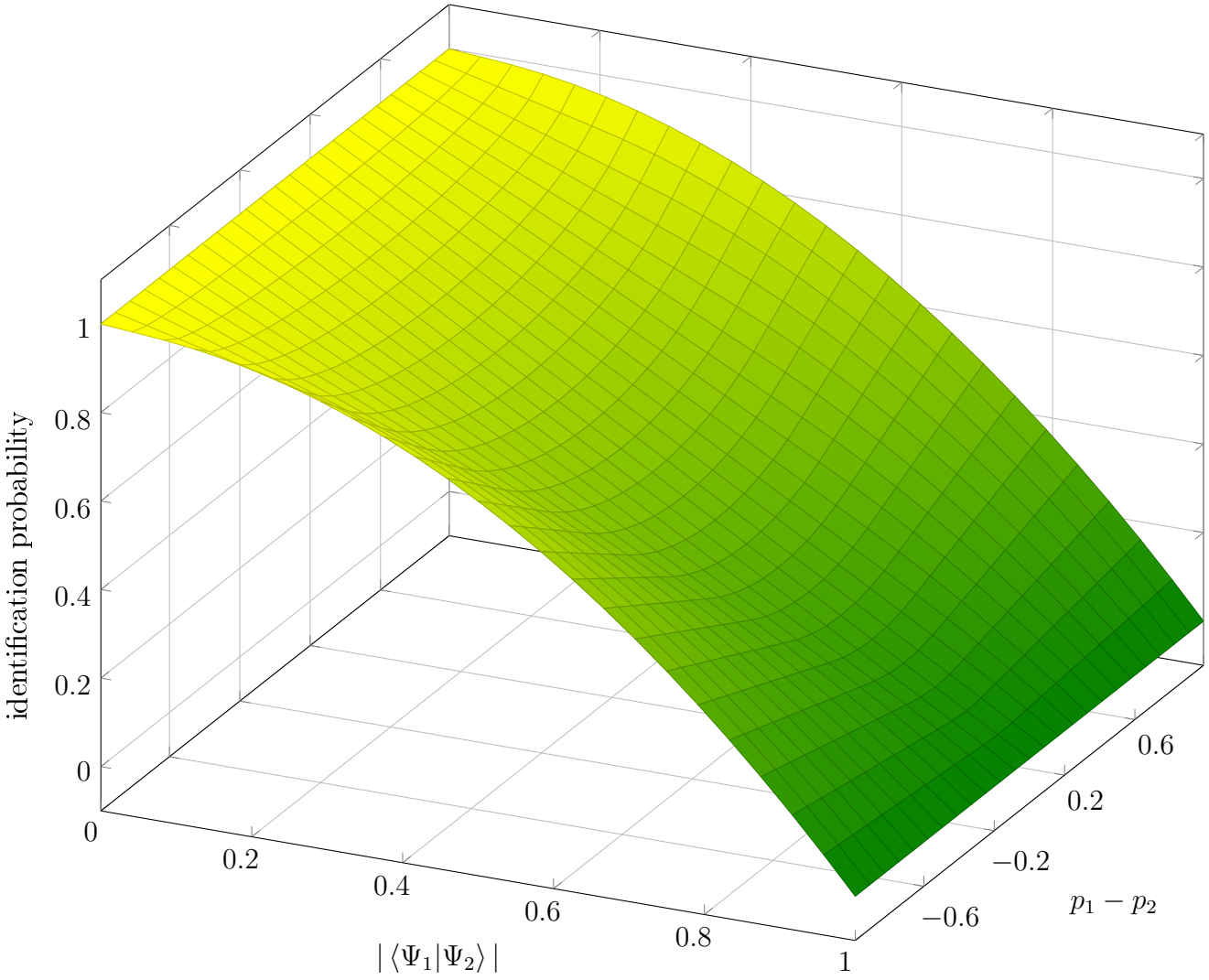



**Exercise 23** *Find a POVM with 3 outcomes: 1,2,? which detects non-orthogonal states (appearing with probabilities* $p_1$ *and* $p_2$*) without error (i.e. if outcome 1 or 2 appear, we can be sure, that a*

*corresponding input value has been sent) minimising probability of the outcome "?". Derive formula for the minimal $p_?$.*

**Ans.**

$$p_? = \begin{cases} p_1 + |\langle\Psi_1|\Psi_2\rangle|^2 p_2 & \text{if } p_2|\langle\Psi_1|\Psi_2\rangle|^2 \geq p_1 \\ p_2 + |\langle\Psi_1|\Psi_2\rangle|^2 p_1 & \text{if } p_1|\langle\Psi_1|\Psi_2\rangle|^2 \geq p_2 \\ 2|\langle\Psi_1|\Psi_2\rangle|\sqrt{p_1 p_2} & \text{else} \end{cases}$$



## Operations on photon polarisation

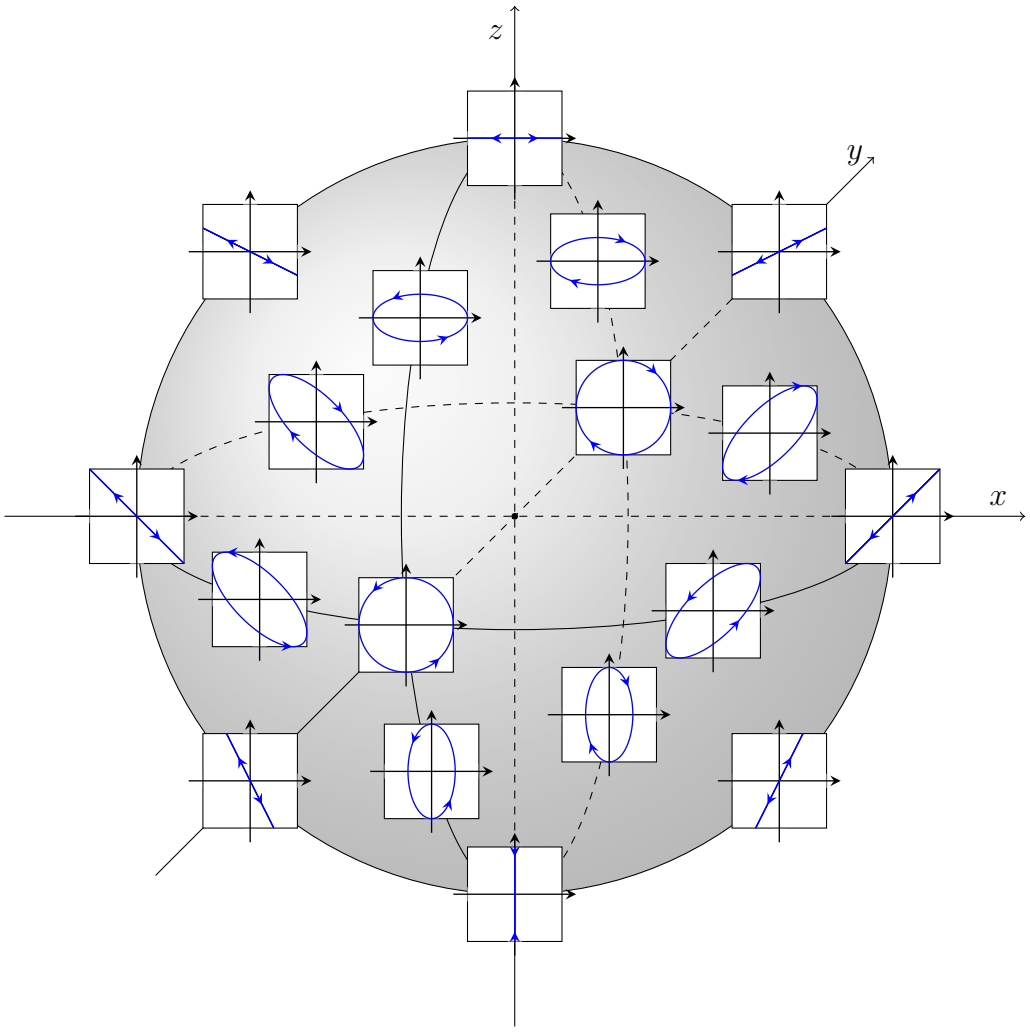
An electromagnetic wave propagating along the $z$-axis can have two polarisations - the horizontal and the vertical one or be a combination of these basic polarisations:

$e^{i\omega t}\begin{bmatrix}1\\0\end{bmatrix}$ – horizontal polarisation $\quad$ $e^{i\omega t}\begin{bmatrix}0\\1\end{bmatrix}$ – vertical polarization

$e^{i\omega t}\begin{bmatrix}1\\1\end{bmatrix}$ – 45°polarisation $\quad$ $e^{i\omega t}\begin{bmatrix}1\\-1\end{bmatrix}$ – - 45°polarisation

$e^{i\omega t}\begin{bmatrix}1\\i\end{bmatrix}$ – anti-clockwise polarisation $\quad$ $e^{i\omega t}\begin{bmatrix}1\\-i\end{bmatrix}$ – clockwise polarisation

For polarisation th wave amplitude and phase plays no role, so the set of all possible polarisations is again a sphere $S^2$ (so-called *Poincaré sphere*).




Photon energy is a squared norm of the electric field. From the energy conservation principle follows, that any optical element transforming a state of a photon conserving its energy must be a unitary operator. Similarly, an operator acting on two-photon states must be a $U(4)$ operation. Unitary operations acting on the Hilbert space of $n$ qubits are called *gates*, in analogy to classical $n$-bit gates.

We will consider the following optical elements:

Twisting polarisation plane by an angle $\alpha$ (gate $e^{i\alpha\sigma_y}$):

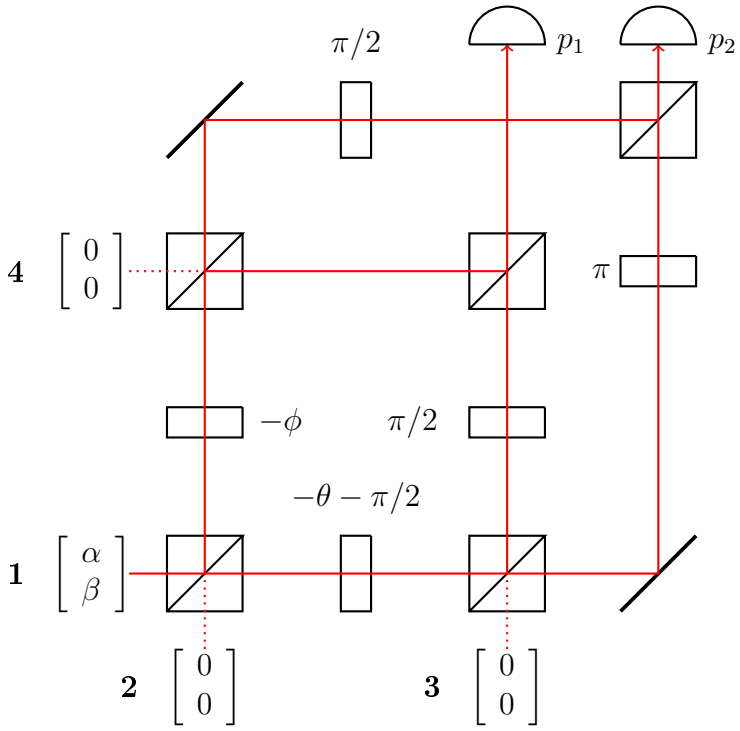
$$\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \tag{21}$$

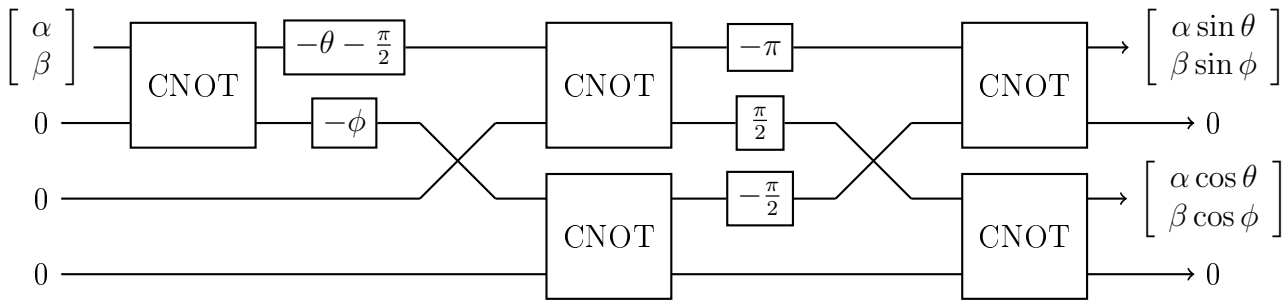
Polarising beam splitter, transmits the horizontal polarisation and reflects the vertical polarisation. Matrix in the basis $xh, xv, yh, yv$:

$$\begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \end{bmatrix} \tag{22}$$

This is a two-qubit gate CNOT (*controlled NOT*). The polarisation qubit is the control qubit and the path qubit is the controlled qubit.

Analise the setting on the picture:






$$\left[\begin{array}{c}\alpha\\ \beta\\ \hline 0\\ 0\\ \hline 0\\ 0\\ \hline 0\\ 0\end{array}\right] \longmapsto \left[\begin{array}{c}\alpha\\ 0\\ \hline 0\\ \beta\\ \hline 0\\ 0\\ \hline 0\\ 0\end{array}\right] \longmapsto \left[\begin{array}{c}-\alpha\sin\theta\\ \alpha\cos\theta\\ \hline -\beta\sin\phi\\ \beta\cos\phi\\ \hline 0\\ 0\\ \hline 0\\ 0\end{array}\right] \longmapsto \left[\begin{array}{c}-\alpha\sin\theta\\ 0\\ \hline -\beta\sin\phi\\ 0\\ \hline 0\\ \alpha\cos\theta\\ \hline 0\\ \beta\cos\phi\end{array}\right] \longmapsto \left[\begin{array}{c}\alpha\sin\theta\\ 0\\ \hline 0\\ \beta\sin\phi\\ \hline -\alpha\cos\theta\\ 0\\ \hline 0\\ \beta\cos\phi\end{array}\right] \longmapsto \left[\begin{array}{c}\alpha\sin\theta\\ \beta\sin\phi\\ \hline 0\\ 0\\ \hline -\alpha\cos\theta\\ \beta\cos\phi\\ \hline 0\\ 0\end{array}\right]$$

$$\Psi = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}, \qquad p_1 = \mathrm{Tr}\left(\begin{bmatrix}\cos^2\theta & 0\\ 0 & \cos^2\phi\end{bmatrix}|\Psi\rangle\langle\Psi|\right) \qquad p_2 = \mathrm{Tr}\left(\begin{bmatrix}\sin^2\theta & 0\\ 0 & \sin^2\phi\end{bmatrix}|\Psi\rangle\langle\Psi|\right),$$

**Exercise 24** *The above setting realises two-outcome one-qubit POVM with diagonal elements. How to realise arbitrary one-qubit POVM using this setting and one-qubit gates?*

## One-qubit gates

**Theorem:** Any $d$-ary logic gate can be realised as a composition of NAND gates.

**Twierdzenie:** Any $U(n)$ operation can be realised as a composition of one-qubit gates and the CNOT gate.

**Exercise 25** *Show that there exists no universal NOT gate for qubit.*

A retarding plate oriented in the standard basis $h, v$ (or squeezing an optical fibre in the horizontal direction) introducing a phase difference $\delta$ is given by the matrix:

$$\begin{bmatrix} e^{i\delta/2} & 0\\ 0 & e^{-i\delta/2}\end{bmatrix} \tag{23}$$

**Exercise 26** *Show, that any one-qubit gate an be realised as three squeezing of an optical fibre in directions* $0°, 45°, 0°$.

# No cloning, broadcasting, BB84

## No cloning and broadcasting

Let us try to construct an operation, which gets on the first input a fixed vector of the empty register $\psi$ and a vector state $\phi$ on the second input and produces on the output the vector $\phi \otimes \phi$. Let us consider, that the operation acts for two states:

$$U(\phi_1 \otimes \psi) = \phi_1 \otimes \phi_1$$
$$U(\phi_2 \otimes \psi) = \phi_2 \otimes \phi_2.$$

This operation should be unitary and hence we can see, that the state vectors $\phi_1, \phi_2$ have to be orthogonal. The cloning machine is possible only for a set of orthogonal pure states. Such a set of pure states, for which cloning is valid, determines completely the cloning machine. It is of the form: *measure in the orthogonal basis and basing on the result prepare two copies.* Convex combinations of cloned statees are not cloned, but *broadcasted* - we get a mixed state of many copies with proper marginal states, but correlated. The broadcasting structures appear in the mechanism of "quantum darwinism" - emerging the objective reality for a quantum object.

**Exercise 27** *Can adding an auxiliary Hilbert space can be helpful in constructing a cloning machine:* $U : |i\rangle \otimes |0\rangle \otimes |0\rangle \to |i\rangle \otimes |i\rangle \otimes |X_i\rangle$ *?*

The same restriction applies to classical states - all pure states can be cloned (while they are mutually orthogonal), but mixed states annot be cloned, but only broadcasted.

Although, we can try to find a cloning machine performing the task in an approximate way, minimising the cloning error (maximal or average).

The above observation can be rephrased as follows: assuming, that we have a channel of one output and two outputs $\Phi_{1,2} : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out1}) \otimes \mathcal{B}(\mathcal{H}_{out1})$. We can always trace off one of the outputs and obtain the marginal channels $\Phi_1$ i $\Phi_2$. Non-existence of a cloning machine means, that there exists no such a channel, having identity channels as both its marginals.

## BB84

In the BB84 protocol the parties A and B want to establish a common bit key, not known to third parties. The protocol lets to find a common key and be sure, that no one else has an information about it.

The A party tosses at random a sequence of values 0,1 of subsequent bits and a sequence of bases from the set

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

encodes the $i$-th bit in the $i$-th basis and send it to B. The party B tosses at random for each bit one of the basis from the above set and perform a measurement in the tossed basis. After sending all the bits, the party A informs publicly about the sequence of the bases used. The party B replies, which of its bases agreed with the bases of A. Bits measured in non-agreeing bases are removed and both parties have the same sequence of bits.

Let us assume now, that an eavesdropper enters the track and perform a measurement in one of the bases and next prepare a qubit in a state of the basis in agreement with the result of measurement. The eavesdropper guess the basis property for half of the bits on average - then it reads the proper value without disturbing it. The other half of the bits is measured in basis not agreed with the sender and then it reads a proper value with probability 1/2 and among these bits only 1/2 will have unchanged value when measured by the receiver. It means, that 1/4 of the sent bits will be eavesdropped incorrectly but also that 1/4 of the bits read by the sender will have a changed value. Sacrificing a part of sent bits lets for detection of the eavesdropper.

If the photon source of the A party is far from one-photon (encodes a bit in many photons), then the eavesdropper can put a beam spliiter into the track and it will be hard to detect (the party B cannot count photons). The beam-splitter will let a part of photons through and another part will be written in a quantum memory (for example will translate a photon state into a two-level atom state). Next, after revealing the bases and the information, which bits are abandoned and which are not, the eavesdropper perform measurements and obtain the key.

# Non-kolmogorovness of Quantum Mechanics

## CHSH inequality

Consider now four random variables $A_1, A_2, B_1, B_2$ defined on a probability space $\Omega$ and taking values $\pm 1$. Observe, that a bound $A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2 \leq 2$ holds for any point in the $\Omega$ (in a given point $x$ one has **either** $B_1(x) = B_2(x)$ **or** $B_1(x) = -B_2(x)$). Taking the average on gets

$$-2 \leq \mathbb{E}(A_1B_1) + \mathbb{E}(A_1B_2) + \mathbb{E}(A_2B_1) - \mathbb{E}(A_2B_2) \leq 2. \tag{24}$$

Assume, that we have a source of pairs of spin-1/2 particles, which disperse in opposite directions and then are measured at the same time in theo distinct laboratories. Each laboratory (A and B) chooses at rendom one of two spin directions (1 or 2) and performs a measurement. The measurement of a spin $i$ in a laboratory $C$ is a random variable $C_i$. Variables $A_1, A_2, B_1, B_2$ should satisfy the inequality (24). Let us see what will happen, if the measured observables are $\hat{A}_1 = \sigma_z, \hat{A}_2 = \sigma_x, \hat{B}_1 = (\sigma_x + \sigma_z)/\sqrt{2}, \hat{B}_2 = (\sigma_z - \sigma_x)/\sqrt{2}$, and the source produces a pure state represented by a vector $|\Psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

**Exercise 28** *Show that the CHSH inequality is not broken in separable states.*

In quantum mechanics the LHS of the inequality cannot exceed the value $2\sqrt{2}$ (Tsirelson's bound).

Let us now assume, that the only bound for correlations is, that they cannot carry information, i.e. if one party measures observable $A$ and the other party measures one of two values $B$ or $B'$, then the marginal distribution $p(a)$ cannot depend on the observable choosen on by the other party:

$$\forall B \ \sum_b P(a, b|A, B) = P(a|A) \tag{25}$$

Else, there a instantaneous transfer of information between parties would be possible. If only non-signaling condition constraints the correlations, then LHS of the CHSH inequality can reach the value 4.

**Exercise 29** *Assume, that*

$$p(ab|AB) = \left[\begin{array}{c|c|c|c} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \end{array}\right] \tag{26}$$

*Show, that such a matrix of conditional probabilities does not transfer information. What is the value of the LHS of the CHSH inequality for this matrix? How the matrix should be modified, to obtain a matrix where information transfer is possible?*

The Bell inequalities are derived under the assumption of existence of a common probability space for all random variables, what is one of the axioms of the classical probability theory (Komogorov axioms). Violating Bell inequalities in quantum mechanics shows, that the quantum theory does not satisfy Kolmogorov axioms - is nonkolmogorovian.

## Teleportation

Assume, that parties A and B share a pure entangled state of two qubits represented by a vector $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and the party A possess a qubit in a state $\alpha|0\rangle + \beta|1\rangle$. A performs on two possesed qubits a joint measurement in the *magical basis*:

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

With equal probabilities, after the measurement, the state of qubit possesed by B will be:

$$\alpha|0\rangle + \beta|1\rangle$$
$$\alpha|0\rangle - \beta|1\rangle$$
$$\alpha|1\rangle + \beta|0\rangle$$
$$\alpha|1\rangle - \beta|0\rangle$$

A informs about obtained result of measurement to B (sending 2 bits), who applying a proper initary transformation transforms the state of the possesed qubit to the initial state of qubit possesed by A. The entangled state shared between A and B is destroyed and A possess now two qubits in an entangled state represented by one of the vectors from the magical basis. To send one qubit one has to spend two bits and one pair in a maximally entangled state.

**Exercise 30** *Show, that states from the magical basis of two qubits can be transformed to each other by a local unitary transformation.*

**Exercise 31** *How the magical basis of two qutrits looks like? How to teleport a qutrit state using a maximally entangled state of two qutrits?*

**Exercise 32** *How to teleport a qutrit state using two pairs of entangled qubits?*

If we try to teleport a state using a pair in a pure state, not maximally entangled, then we get a transmission error, not possible to correct.

**Exercise 33** *Let the receiver and the sender share a pair in the pure state* $\gamma|00\rangle + \delta|11\rangle$*, where* $\gamma \geq \delta$*. Construct a POVM, which with the maximal probability will transform the post-measurement (unnormalised) state* $\alpha\gamma|00\rangle + \beta\delta|11\rangle)$ *to the input state :* $(\alpha|00\rangle + \beta|11\rangle)/\sqrt{2}$*. What is the value of the maximal probability? Repear the calculations for other post-measurement states. What is the total probability of a correct teleportation?*

# Measures and criteria of entanglement

## Entanglement measures

**LOCC** The LOCC operations are operations on states of composed system, where we can use local unitary operations and classical communication. An operation to be performed on a local subsystem can be conditioned by a result of measurement on an other subsystem, and vice-versa. We can in this way sequentially send results of local measurements and use these values to condition local operations performed on a state. This class is hard to characterise. Any well-defined measure of entanglement should be monotonic w.r. to LOCC, i.e. after performing such an operation, the considered measure of entanglement cannot grow.

**Destilation and formation of entanglement** Assume, that there exists a distillation protocol (a LOCC operation), which lets from $N$ copies of non-maximally entangled states to create $M$ copies of maximally entangled states:

$$\rho^{\otimes N} \underset{Formation}{\overset{Distilation}{\rightleftarrows}} \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes M} \otimes ... \tag{27}$$

For a given $N$ let us maximise the ratio $M/N$ over all possible LOCC protocols, and then go with $N \to \infty$. The obtained number is a measure of „quality“ (from the point of view of applications) of entanglement of the input state, called *entanglement of distilation* (EOD).

On the other side, one can ask how many pairs $M$ of maximally entangled states one has to use to create $N$ copies of a given state. We minimise the ratio $M/N$ over all possible LOCC protocols and we go with $N \to \infty$. The obtained number is called *entanglement of formation* (EOF).

For two-particle pure state, EOF is equal to EOD and both measures are equal to von Neumann entropy of a partial trace (Shannon entropy of the spectrum of the state). It is the only properly defined entanglement measure for pure states. For mixed states there is no uniquely defined measure of entanglement and EOD $\leq$ EOF. There exists entangled states from which it is not possible to distill pure maximally entangled states. Such entanglement is called *bound entanglement*.

In the special case of two qubits there exists a formula for EOF of a state. Let us define for a state a quantity *concurrence* by the formula: $C(\rho) = \max\{0, 2\lambda_{max} - 1\}$, where $\lambda_{max}$ denotes the maximal

eigenvalue of a hermitian matrix: $\sqrt{\sqrt{\rho}(\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)\sqrt{\rho}}$. For all states this number is in the range $[0, 1]$. It means, that the pair of numbers:

$$\frac{1+\sqrt{1-C(\rho)^2}}{2}, \quad \frac{1-\sqrt{1-C(\rho)^2}}{2} \tag{28}$$

is a probability distribution. The EOF of $\rho$ is the Shannon entropy of this distribution:

$$EOF = \frac{1+\sqrt{1-C(\rho)^2}}{2} \log_2 \frac{1+\sqrt{1-C(\rho)^2}}{2} + \frac{1-\sqrt{1-C(\rho)^2}}{2} \log_2 \frac{1-\sqrt{1-C(\rho)^2}}{2}. \tag{29}$$

Another measure of entanglement is *negativity*: $\mathcal{N}(\rho) = \frac{1}{2}(||\rho^\Gamma||_1 - 1)$ (where $||\cdot||_1$ denotes trace norm and $\rho^\Gamma$ is $\rho$ after partial transposition) and *logarithmic negativity*: $EN(\rho) = \log_2 ||\rho^\Gamma||_1$. The last one is the lower bound for EOD.

## Partial transposition criterion

If a state is separable, then its partial transposition $(I \otimes T)\rho$ is semi-positive definite. States detected by the partial transposition are called NPT (negative partial transposition).

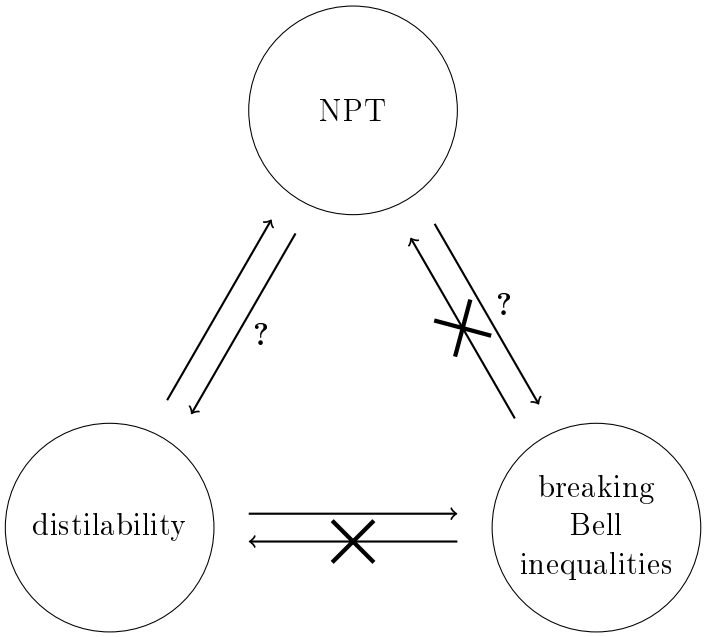
**Exercise 34** *Show, that partial transposition criterion detect all pure entangled states.*

In dimensions $2 \times 2$, $2 \times 3$, $3 \times 2$ partial transposition detect all entangled states. In higher dimensions there exist entangled (mixed) states with positive partial transposition (PPT).

**Exercise 35** *Find the subset of separable states in the simplex of states diagonal in the Bell basis of two qubits.*

**PPT entanglement** PPT (of positive partial transposition) entangled states we will find already for two qutrits. One can construct an example of such states using unextendible product bases (UPB): Construct a regular pentagon on the plane $\mathbb{R}^2$ centered at 0. To the vectors pointing to its vertices let's add a $z$-component of such value that any two vectors pointing to non-neighbouring vertices are orthogonal. We will obtain a set of vectors in $\mathbb{R}^3 \subset \mathbb{C}^3$. Now let us consider a set of 5 vectors in $\mathbb{C}^2 \otimes \mathbb{C}^3 \supset \{\psi_i \otimes \psi_{2i}\}$. Let us observe, that there exists no product vector orthogonal to all of them, hence the orthogonal complement of the subspace spanned by them is a 4-dimensional subspace containing no non-zero product vector $\Rightarrow$ the normalised projector onto this subspace is an entangled state. This state is invariant under the action of partial transposition, hence is a PPT entangled state.

LOCC operations preserve the positivity of the partial transposition. It follows, that from a PPT entangled state no maximally entangled pairs can be distilled. Entanglement of a PPT state is a *bound entanglement*. The following conditions hold:




## Positive maps criterion

The partial transposition criterion is an important, but a special case of positive maps criterion.

If $\Lambda$ is a positive map, then for a product state $\rho \otimes \sigma$, $(I \otimes \Lambda)(\rho \otimes \sigma)$ is a positive operator as well. Hence this property holds for all separable states. We know, that if $\Lambda$ is not completely positive, then $(I \otimes \Lambda)$ is not positive, i.e. acting on a certain state will give a non-positive operator. In this way it detects an entanglement in the state. The Horodecki's theorem says, that for any entangled state there exists a positive map detecting it.

One could detect entanglement in a state if all positive maps were known. It is a hard task. En example of P, not CP map is the transposition. For subsystems dimensions $2 \times 2$ and $2 \times 3$ transposition is (up to composition with a positive map an addition of a CP map) the only positive, not CP map:

$$\Phi : \mathcal{B}(\mathbb{C}^{d_1}) \to \mathcal{B}(\mathbb{C}^{d_1}). \qquad d_1 d_2 \leq 6 \Rightarrow \left( \Phi \in \mathcal{P} \iff \Phi(\rho) = \sum_i A_i \rho^T A_i^\dagger + \sum_i B_i \rho B_i^\dagger \right) \tag{30}$$

An example of a P, not CP map not originating in transposition, is the Choi map, defined in the standart basis:

$$\begin{aligned} CH(|e_i\rangle \langle e_i|) &= |e_i\rangle \langle e_i| + |e_{i+1}\rangle \langle e_{i+1}| \\ CH(|e_i\rangle \langle e_j|) &= -|e_i\rangle \langle e_j|, \text{ dla } i \neq j \end{aligned} \tag{31}$$

This map is able to detect PPT entangled states.

**Exercise 36** *Find the map dual to the Choi map*

## The realignment criterion

Another important entanglement criterion os the realignment or cross-norm criterion. In this criterion we construct a new matrix: $R(\rho)_{ij,kl} = \rho_{ik,jl}$. We calculate the trace norm of this matrix (sum of

its singular values). It cannot exceed 1 for a separable state. Equivalently, we calculate the sum of square roots of eigenvalues of the Gramm matrix of blocks of density matrix.

**Proof:** It is easy to check, that for a pure separable state the norm is equal 1. Norm is a convex functional (triangle inequality), hence for a mixed separable state the norm should be $\leq 1$ $\square$

**Exercise 37** *For two-parameter family of trace-one operators:*

$$\rho = \frac{1}{3(1+a+b)} \left[\begin{array}{ccc|ccc|ccc} 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & a & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \end{array}\right] \tag{32}$$

*Draw on the ab-plane the areas of:*

1. *states*
2. *NPT states*
3. *states detected by the Choi map*
4. *states detected by the map dual to the Choi map*
5. *states detected by the realignment criterion*

We have shown, that if $a < 1$ or $b < 1$, then the state is entangled. In this family we can show, that the remaining states (if $a \geq 1$ and $b \geq 1$) are separable. Let us act on the state $\rho$ with an operation $D \otimes D^*$, where $D$ is a diagonal unitary matrix:

$$D = \left[\begin{array}{ccc} e^{i\phi_0} & \cdot & \cdot \\ \cdot & e^{i\phi_1} & \cdot \\ \cdot & \cdot & e^{i\phi_2} \end{array}\right] \tag{33}$$

and next integrate the above expression over the angles $\phi_0$, $\phi_1$, $\phi_2$. Let us denote such operation on a state $\rho$ as $\Phi$:

$$\Phi(\rho) = \int D \otimes D^* \rho (D \otimes D^*)^\dagger \mathrm{d}\phi_0 \mathrm{d}\phi_1 \mathrm{d}\phi_2 \tag{34}$$

Such a map preserves entries on diagonal and the off-diagonal entries in places where there is 1 in the formula (32), and the rest of the entries are zeroed (hence it is a projector). Moreover, for a separable $\rho$, $\Phi(\rho)$ will be separable. Observe, that the state (32) can be obtained by acting with the map $\Phi$ on the the same state but having all zeros replaced by ones. Such state (being a sum of a diagonal matrix and a projector on a product vector) is separable.

## Entanglement witnesses

To a map $\Lambda : \mathcal{B}(\mathbb{C}^{d_1}) \to \mathcal{B}(\mathbb{C}^{d_2})$ one can prescribe an observable $W \in \mathcal{B}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ by the formula:

$$W = (I_{d_1} \otimes \Lambda) |\Psi\rangle \langle\Psi| , \tag{35}$$

where $\Psi = \frac{1}{\sqrt{d_1}}(\sum_i |ii\rangle)$. This map maps completely positive maps to semi-positive operators, and positive maps to maps semi-positive on product vectors. P but no CP maps are mapped to so-called *entangled witnesses* - observables having non-negative expected value in separable states but negative in certain entangled states. To detect all the states detected by $\Lambda$ one needs the whole orbit (of local unitary group) of entanglement witnesses.

The above map is invertible and is called *Jamiołkowski isomorphism.*

**Exercise 38** *Show, that the CHSH inequality can be reformulated as the condition for positivity of the expected value of an entanglement witness.*

**Exercise 39** *Find witnesses related to the Choi map and the dual Choi map.*

If a map $\Phi$ detects a state $\rho$, then in general the related witness will not detect this state. We find a witness detecting a given entangled state in the following way: if $(I \otimes \Phi)\rho \ngeq 0$, then this matrix possess a negative eigenvalue. Let us take a vector $\phi$ from the related eigensubspace. We have: $\langle\phi| (I \otimes \Phi)\rho |\phi\rangle = \langle P_\phi|(I \otimes \Phi)\rho\rangle_{HS} < 0$. One should take as an entanglement witness the observable $W = I \otimes \Phi^{\#} P_\phi$, where $\Phi^{\#}$ denotes conjugation in the space of operators.

An entanglement witness is an observable acting in the Hilbert space of a system composed of two spatialy separated subsystems. To be measured, it should be decomposed into e sum of tensor products of local observables. Measuring procedure is similar to measuring the CHSH inequality (which is a special case of entanglement witness).

**Exercise 40** *For a witness related to the Choi map find a decomposition into a sum of tensor products of local observables.*

## Set of states in higher dimensions and the Gurvits ball

The set of states of qubit is a ball of a radius $1/\sqrt{2}$ around the maximally mixed state. In arbirtary dimension, a ball circumscribed on the set of states has a radius $\sqrt{(d-1)/d}$, and a ball inscribed has a radius $1/\sqrt{d(d-1)}$. In dimension 2 these balls coincide and the set of states is itself a ball. In higher dimensions its boundary lays between spheres. One can prove, that the ball inscribed in the set of states contains only separable states. This ball is called the *Gurvits ball.* Any ball around the maximally mixed state of a bigger radius will already contain entangled states.

# Quantum algorithms

## Classical Shor algorithm

Let us consider an exponential function $a^x$ from $\mathbb{Z}$ to a number field $\mathbb{Z}_N$. We call a rank of an element $a$ period of this fucntion, i.e. the smallest positive number $r$ such, that:

$$a^r \mod N = 1$$

One of the three possibilities can take place:

- $2 \not| r$
- $2 | r \ \wedge \ a^{r/2} \mod N = -1$
- $2 | r \ \wedge \ a^{r/2} \mod N \neq -1$

We are interested in the last case. Let us introduce a notation $x = a^{r/2}$. While $x^2 \mod N = 1$, hence $x^2 - 1 = (x+1)(x-1) \mod N = 0$, it means that the product is divisible by $N$. None of the factors is divisible by $N$ - the first because $r$ is the rank of $a$, not $r/2$, the second from the assumption that the third case takes place. Hence $N$ is a composite number, and we can find its factor calculating $NWD(x+1, N)$ (algorithm is effective).

Success depend on choice of $a$. It turns out, that the probability of tossing such an $a$ (that the third case in the list holds) is equal to $1 - 2^{-m} \geq 3/4$, where $m$ is the numer of prime factors in the decomposition. Probability of not finding decreases exponentially with the number of tries. It is a probabilistic algorithm. Summarising, its steps go as follows:

1. Toss $a$ randomly from the range $\{1, N-1\}$. If $NWD(a, N) \neq 1$, we have found a factor, otherwise we go further.
2. Determine the rank of $a$
3. If $r$ is odd or $a^{r/2} \mod N = -1$, return to the point 2, otherwise go further
4. factor is $NWD(a^{r/2}, N)$.

## Quantum Shor algorithm

Classical Shor algorithm, despite simple implementation and fast decreasing probability of failure, has no practical meaning. The difficulty is hidden in the time consumption of determining the rank of an element. We improve this step of the algorithm calculating it by a quantum computer.

We need a quantum register in which we are able to write the number $N^2$, hence of the length $K$, where $N^2 < Q = 2^K$. The Hilbert space of the input register has to be at least $N$-dimensional (register of the length $\lceil \log_2 N \rceil$). The initial state of the both registers is $|0\rangle \otimes |0\rangle$.

We perform a discrete Fourier transform on the input register

$$U_F : |q\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{q'=0}^{Q-1} \exp(2\pi i q' q / Q) \, |q'\rangle \, . \tag{36}$$

The input register contains now an equal superposition of all basis states and the output register remains unchanged: $\frac{1}{\sqrt{Q}}\sum_{q=0}^{Q-1}|q\rangle\otimes|0\rangle$ . Now we perform on both registers the function $|q\rangle\otimes|0\rangle\rightarrow|q\rangle\otimes|a^q \mod N\rangle$ and obtain $\frac{1}{\sqrt{Q}}\sum_{q=0}^{Q-1}|q\rangle\otimes|a^q \mod N\rangle$.

Next we perform the Fourier transform on the input register:
$Q^{-1}\sum_{q=0}^{Q-1}\sum_{q'=0}^{Q-1}\exp(2\pi iqq'/Q)|q\rangle\otimes\left|a^{q'} \mod N\right\rangle$ and then a measurement in the standard (computational) basis. The probability of obtaining the result $q_0$ is equal:

$$p(q_0)=\frac{1}{Q^2}\sum_{q}\sum_{q'}\exp(2\pi iq_0q'/Q)\exp(-2\pi iq_0q/Q)\langle f(q)|f(q')\rangle \tag{37}$$

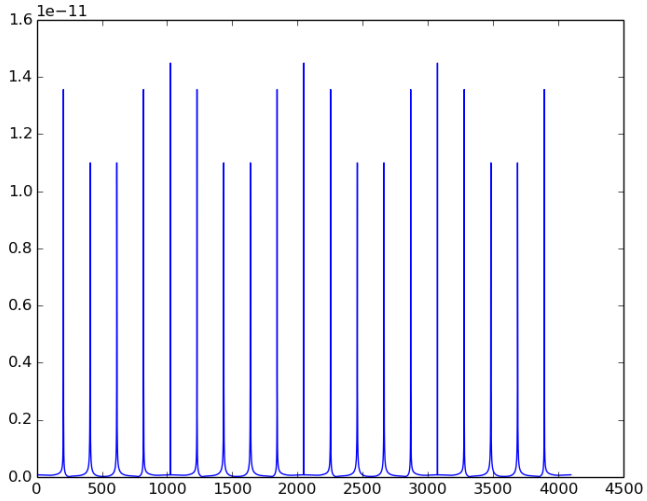
The scalar product is equal to 1 if $q-q'$ is a multiplicity of $r$ and 0 otherwise. Hence we obtain:

$$p(q_0)=\frac{1}{Q^2}\sum_{j=0}^{r-1}\sum_{\mu=0}^{\lfloor\frac{Q-1-j}{r}\rfloor}\sum_{\nu=0}^{\lfloor\frac{Q-1-j}{r}\rfloor}\exp(2\pi iq_0(\mu r+j)/Q)\exp(-2\pi iq_0(\nu r+j)/Q)$$

$$=\frac{1}{Q^2}\sum_{j=0}^{r-1}\left|\sum_{\mu=0}^{\lfloor\frac{Q-1-j}{r}\rfloor}\exp(2\pi iq_0\mu r/Q)\right|^2=$$

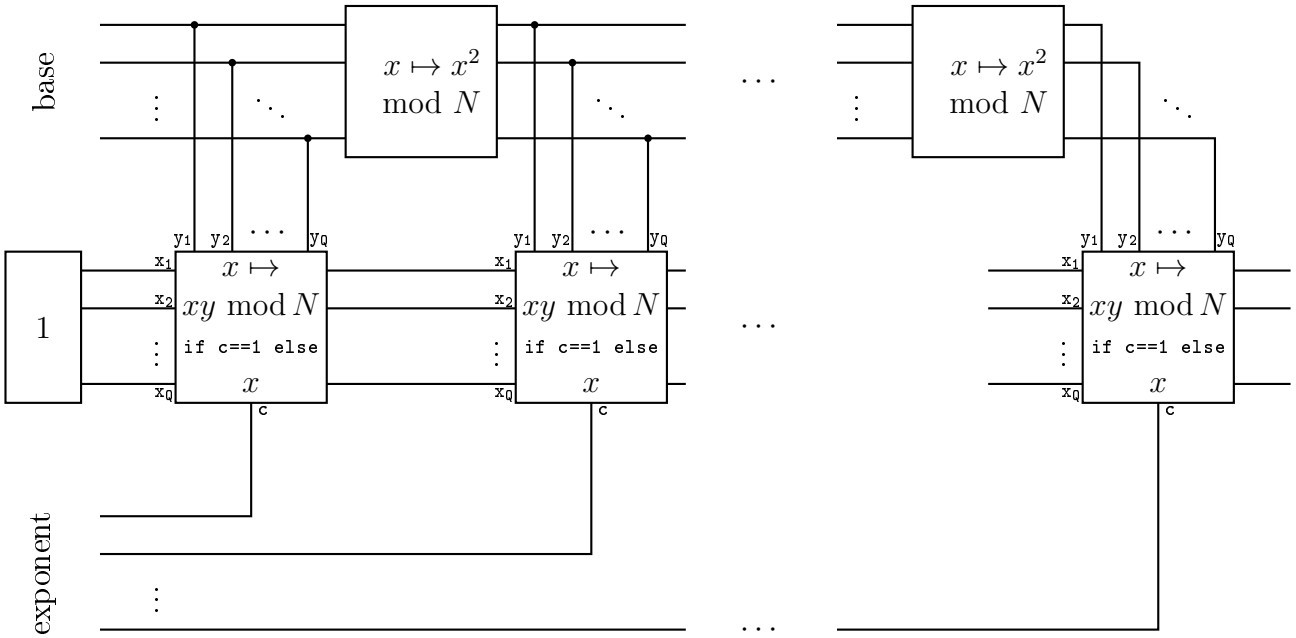
$$\frac{(Q \mod r)\sin^2\left(\pi q_0r\left(\lfloor\frac{Q-1}{r}\rfloor+1\right)/Q\right)+(r-Q \mod r)\sin^2\left(\pi q_0r\lfloor\frac{Q-1}{r}\rfloor/Q\right)}{Q^2\sin\left(\pi q_0r/Q\right)}$$

The function has a peak if $q_0r/Q\in\mathbb{Z}$:




Measuring the first register gives (with high probability) a certain number $y$, such that $y/Q$ is close to a multiplicity of $1/r$. There exists a Istnieje metoda ułamków łańcuchowych, która pozwala z wyniku jednego pomiaru odzyskać $r$.

**Exponential function** One realises an exponential function by power by squaring algorithm:




The circuit is composed of two types of gates. Gates in the upper row realises squaring modulo $N$. Gates in the lower row multiply their input registers (the left and the up) modulo $N$ if the control bit (on the bottom) is set to 1 and release the the left register to the output otherwise. Observe, that there are $2Q-1$ gates, hence the number of operations grows linearly with the bit length of the exponent (logarithmically with its size).

**Fourier transform** Performing the Fourier transform is multiplying the input vector by a matrix of the entries $\exp(2\pi i \cdot kl/Q)/Q$. Observe, that calculating $y_k$ one gets:

$$y_k = \frac{1}{Q}\sum_{l=0}^{Q-1} \exp(2\pi i \cdot kl/Q)\, x_l = \frac{1}{2}\frac{1}{Q/2}\sum_{k=0}^{Q/2-1} \exp(2\pi i \cdot kl/(Q/2))\, x_{2k} + \frac{1}{2}\frac{1}{Q/2}\exp(2\pi i \cdot k/Q)\sum_{k=0}^{Q/2-1} \exp(2\pi i \cdot kl/(Q/2))\, x_{2k+1} \tag{38}$$

- performing one multiplication we reduce the problem to calculation of two Fourier transforms in dimension $Q/2$. (remember, that $Q = 2^K$, hence the above step we will continue till $Q = 1$). In each step we perform $Q$ multiplications, using the results of Fourier transforms from the previous step. There are $K = \log_2 Q$ steps. The whole procedure requires performing $Q \log_2 Q$ multiplications, not $Q^2$, as for a general matrix.

Let us rewrite the formula (36) using the binary representation $k = \sum_l k_l 2^l$ of the number $q'$:

$$\begin{aligned}
|j\rangle \mapsto & 2^{-K/2} \sum_{k_1=0}^{1} \cdots \sum_{k_K=0}^{1} \exp\left(\frac{2\pi i}{2^K} j \sum_{l=0}^{K-1} k_l 2^l\right) |k_{K-1} \dots k_0\rangle \\
= & 2^{-K/2} \sum_{k_1=0}^{1} \cdots \sum_{k_K=0}^{1} \bigotimes_{l=0}^{K-1} \exp\left(2\pi i 2^{l-K} j k_l\right) |k_l\rangle \\
= & 2^{-K/2} \bigotimes_{l=0}^{K-1} \left(\sum_{k_l=0}^{1} \exp\left(2\pi i 2^{l-K} j k_l\right) |k_l\rangle\right) = 2^{-K/2} \bigotimes_{l=0}^{K-1} \left(|0\rangle + \exp\left(2\pi i 2^{l-K} j\right) |1\rangle\right)
\end{aligned} \tag{39}$$

The number $2^{l-K} j$ in the exponent is a rational number, using the binary expansion $j = \sum_{\nu=0}^{K-1} j_\nu 2^\nu$ of $j$ one can rewrite its fractional part (the only relevant part of phase) as $0.j_{K-l-1} \dots j_1$ and finally obtain:

$$\begin{aligned}
|j\rangle \mapsto & \frac{|0\rangle + \exp\left(2\pi i 0.j_{K-1} \dots j_0\right) |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + \exp\left(2\pi i 0.j_{K-2} \dots j_0\right) |1\rangle}{\sqrt{2}} \otimes \cdots \otimes \\
& \frac{|0\rangle + \exp\left(2\pi i 0.j_0\right) |1\rangle}{\sqrt{2}}
\end{aligned} \tag{40}$$

Les us define the qubit gate $R_k$ as

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i 2^{-k}} \end{bmatrix} \tag{41}$$

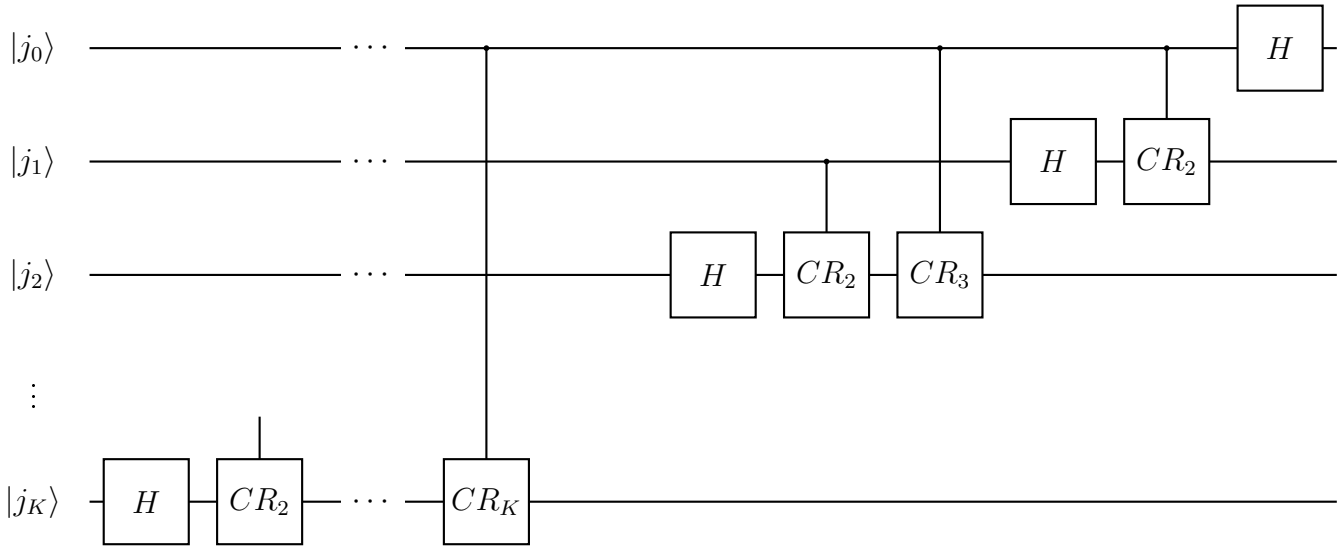
One can define its variant $CR_k$ - two-qubit gate:

$$CR_k = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{2\pi i 2^{-k}} \end{bmatrix} \tag{42}$$

Observe, that the vector $(|0\rangle + \exp(\pi i j_{K-1}) |1\rangle)/\sqrt{2}$ is obtained by acting the Hadamard gate on the vector $|j_{K-1}\rangle$:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{43}$$

Phase shift by a factor $\exp(2\pi i \cdot 0.j_{K-1} j_{K-2} \dots j_0)$ can be written as a sequence of gates $CR_2 \cdot CR_3 \dots CR_K$ controlled by bits from $K-2$-nd do 0-th acting on a vector $(|0\rangle + \exp(\pi i j_{K-1}) |1\rangle)/\sqrt{2}$.



## NMR Computer

One of the implementations of a quantum computer operating on $\lesssim 10$ qubits ai an NMR computer. Qubits are spins 1/2 of atom nuclei in a molecule. Operations are performed on a macroscopic sample of $\sim 10^{20}$ molecules. Because of that the measurements that we perform give us immediately the mean value of an observable in a mixed state. Such measurement does not destroy the state and non-commuting observables can be measured simultaneously.

A sample is placed is a strong magnetic field $\sim 10T$ along the $z$ axis, which orients the nuclear spins. For each nucleus the equation $\hbar\gamma B_0 = \hbar\omega_0$ defines the *Larmor frequency*, depending on the gyromagnetic coefficient $\gamma$, which is different for different nuclei:

| nucleus | H | C | F | P | N |
|---|---|---|---|---|---|
| $\gamma$ [MHz/T] | 42.6 | 10.7 | 40.0 | 17.4 | 3.1 |

Larmor frequencies of nuclei in a molecule can have an additional contribution from chemical shifts - interaction of nuclear spins with electronic angular momentum (if two atoms pass over to each other under an action of the symmetry group of the particle, will have the same value of the chemical shift). For $B_0 \sim 10T$, energy of thermal vibrations is 4-5 orders of magnitude higher than energy of the spin in the magnetic field.

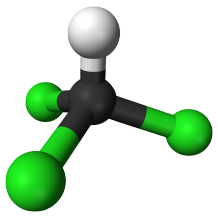
We also apply an alternating magnetic field long the $x$ axis and using it we operate on the states of nuclei. The second coil in the same direction is for reading.

In a molecule as qubits one can treat this nuclei which will be separately addressable by magnetic field pulses, i.e. these, which have their resonant frequencies separated from other nuclear spins frequencies (the more such a frequency is separated, the less time $\tau$ is necessary to perform an operation). In such a way we construct one-qubit operations. many-qubit operations are operations generated by the free evolution Hamiltonian, which depends on the strength $J$ of coupling between nuclei. This time has to be long enough, to treat coupling between nuclei as negligible. It leads to the condition:

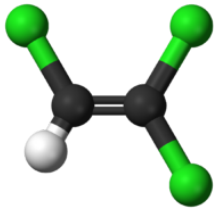
$$\delta\omega_0 \gg \frac{1}{\tau} \gg J/\hbar \tag{44}$$

The decoherence scale has to be greater than $J/\hbar$. It gives some hints, which molecules are appropriate for calculations and how many atoms we can use. Molecules used in calculations include:

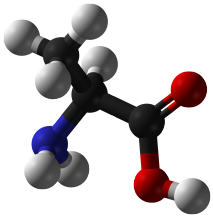
- 2 qubits: chloroform (qubits: H nd C)



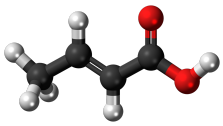
- 3 qubits: trichloroethylene (qubits: H ND C)



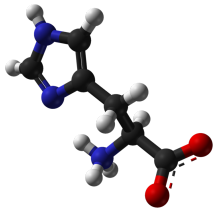
- 4 qubits: alanine (qubits: 1 × H and 3 × C)



- 7 qubits: crotonic acid (qubits: 2 × H, 4 × C, 1 × $H_3$)



- 12 qubits + qutrit: histidine (qubits: 3 × H, 3 × N, 6 × C, two indistinguishable hydrogen atoms establish a singlet and a qutrit)



(carbon $^{12}$C has zero nuclear spin, in all the above molecules we have to have carbon $^{13}$C atoms).

Hamiltonian of nuclear spins in the molecule is

$$H = \frac{\hbar}{2}\sum_i \omega_i \sigma_z^{(i)} + \sum_{i<j} J_{ij} \sum_k \sigma_k^{(i)} \otimes \sigma_k^{(j)}, \tag{45}$$

where $\sigma_k^{(i)}$ denotes $\bigotimes_{i=1}^n I$ z $I$ on the $k$-th place changed to $\sigma_k$.

During the steering impulse of the length $\tau$ and angular velocity $\omega_{rf}$ one qubit is addressed, and at the time the nuclei coupling is negligible. The Hamiltonian of a single spin is of the form:

$$H(t) = -\hbar\omega_z \frac{1}{2}\sigma_z + \hbar\omega_x \cos(\omega_{rf}t - \phi)\frac{1}{2}\sigma_x \tag{46}$$

Lets pass to the interaction picture $\rho(t) \to \rho_R(t) = U_R^\dagger(t)\rho(t)U_R(t)$, gdzie $U_R(t) = \exp(i\omega_z t\frac{1}{2}\sigma_z)$:

$$H_R(t) = U_R^\dagger H U_R - i\hbar U_R^\dagger \dot{U}_R = \hbar/2 \begin{bmatrix} 0 & \omega_x e^{-i\omega_0 t}\cos(\phi - \omega_{rf}t) \\ \omega_x e^{i\omega_0 t}\cos(\phi - \omega_{rf}t) & 0 \end{bmatrix} \tag{47}$$

If a frequency of the steering signal is equal to the Larmor frequency, then the Hamiltonian in the interaction picture is of the form:

$$H_R = \frac{1}{2}\hbar\omega_x(\cos\phi\sigma_x + \sin\phi\sigma_y) \tag{48}$$

Terms oscillating with angular velocity $2\omega_0$ have been omitted, because at the impulse duration they averages to 0 (RWA).

For two non-interacting spins the Hamiltonian is of the form:

$$\begin{aligned} H = &-\hbar\omega_{z1}\frac{1}{2}\sigma_z \otimes I - \hbar\omega_{z2}\frac{1}{2}I \otimes \sigma_z + J_{12}\sum_k \sigma_k \otimes \sigma_k \\ &+B_{x,1}\cos(\omega_{rf1}t - \phi_1)(\gamma_1\frac{1}{2}\sigma_x \otimes I + \gamma_2 I \otimes \frac{1}{2}\sigma_x) \\ &+B_{x,2}\cos(\omega_{rf2}t - \phi_2)(\gamma_1\frac{1}{2}\sigma_x \otimes I + \gamma_2 I \otimes \frac{1}{2}\sigma_x) \end{aligned} \tag{49}$$

we pass to the interaction picture by the transformation $U_R = \exp(i\omega_{z1}t\frac{1}{2}\sigma_z) \otimes \exp(i\omega_{z2}t\frac{1}{2}\sigma_z)$. In the considered time scale ($\Delta\omega_x\tau \gg 1$) terms oscillating with angular velocity $\Delta\omega_x$ averages and the Hamiltonian will take the form:

$$\begin{aligned} H_R = &\frac{1}{4}J_{12}\sigma_z \otimes \sigma_z + \frac{1}{2}\omega_{x,1}(\cos\phi_1\sigma_x \otimes I + \sin\phi_1\sigma_y \otimes I) \\ &+\frac{1}{2}\omega_{x,2}(\cos\phi_2 I \otimes \sigma_x + \sin\phi_2 I \otimes \sigma_y), \end{aligned}$$

where $\omega_{x,i} = \frac{1}{2}\gamma_i B_{x,i}$. For many qubits the Hamiltonian in the interaction picture has the form:

$$H_R = \frac{1}{4}\sum_{i<j} J_{ij}\sigma_z^{(i)} \otimes \sigma_z^{(j)} + \frac{1}{2}\sum_i \omega_{x,i}(\cos\phi_i\sigma_x^{(i)} + \sin\phi_i\sigma_y^{(i)}) \tag{50}$$

**One-qubit gates** We have two-parameter family of operations from SU(2):

$$e^{\frac{i}{2}\theta(\cos\phi\sigma_x + \sin\phi\sigma_y)} = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}e^{-i\phi} \\ -i\sin\frac{\theta}{2}e^{i\phi} & \cos\frac{\theta}{2} \end{bmatrix} \tag{51}$$

We cannot implement in this way a rotation around $z$ axis, but one can obtain it composing the bove operations:

$$e^{-i\alpha\sigma_z/2} = e^{-i\frac{\pi}{4}\sigma_x}e^{-i\alpha\frac{1}{2}\sigma_y}e^{i\frac{\pi}{4}\sigma_x} \tag{52}$$

Choosing phases and duration times of steering impulses one can perform any SU(2) operation on each qubit separately.

**Two-qubit gates** Any many-qubit operation one can perform using CNOT gates. To realise a CNOT gate one has to add to the free evolution the couplings between all pairs of qubits except the one we are interested in. We realise it by the *refocusing* technique. Since now let us assume, that we have one coupling $\sigma_z \otimes \sigma_z$.

**Exercise 41** *Show, that:*

$$\exp\left(-i\frac{\pi}{4}\sigma_z \otimes I\right)\exp\left(i\frac{\pi}{4}I \otimes \sigma_z\right)\exp\left(-i\frac{\pi}{4}I \otimes \sigma_x\right)$$

$$\exp\left(-i\frac{\pi}{4}\sigma_z \otimes \sigma_z\right)\exp\left(-i\frac{\pi}{4}I \otimes \sigma_y\right) = \exp\left(-i\frac{\pi}{4}\right)\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{array}\right] \sim CNOT$$

**Exercise 42** *Show, that:*

$$I \otimes \exp(-i\frac{\pi}{4}\sigma_x) \cdot \exp\left(-i\frac{\pi}{4}\sigma_z \otimes I\right) \exp\left(i\frac{\pi}{4} I \otimes \sigma_z\right) \exp\left(-i\frac{\pi}{2^{k+1}} I \otimes \sigma_x\right) \exp\left(-i\frac{\pi}{4}\sigma_z \otimes \sigma_z\right)$$
$$\exp\left(-i\frac{\pi}{2^{k+1}} I \otimes \sigma_y\right) I \otimes \exp(i\frac{\pi}{4}\sigma_x) = \exp\left(-i\frac{\pi}{4}\right) \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & e^{i\pi/2^k} & 0 \\ 0 & 0 & 0 & e^{-i\pi/2^k} \end{array}\right] \sim CR_k$$

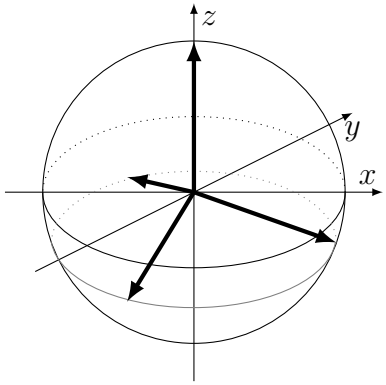
**Effective pure states** As we have mentioned, even for very strong fields and moderately low temperatures, the thermal state of a nuclear spin is close to the maximally mixed state. We do not enhance its purity, but we rewrite it in the form $(1-\epsilon)\rho_{max} + \epsilon|\Psi\rangle\langle\Psi|$. The maximally mixed state is invariant with respect to all operations and gives the equal background level at the measurement.

# Quntum tomography and estimation theory

## SIC POVMs

There exist $d^2$ lines in $\mathbb{C}^d$ where the angles between lines in each pair are equal. It is maximal cardinality of a set of such lines and it is assumed (*Zauner conjecture*), that such a set exists for any $d$. One can provide a construction till dimension 21 and a number of higher dimensions, numerically till 151 and few higher.

Projectors on such vectors sums to $dI_d$, and the HS products of two distinct projectors are always equal. For qubit, the projectors form a regular tetrahedron inscribed in Bloch sphere:




**Exercise 43** *Find matrices of the above projectors*

Answer $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ $\frac{1}{3}\begin{bmatrix} 1 & \sqrt{2} \\ \sqrt{2} & 2 \end{bmatrix}$ $\frac{1}{3}\begin{bmatrix} 1 & \sqrt{2}e^{i\frac{2\pi}{3}} \\ \sqrt{2}e^{i\frac{-2\pi}{3}} & 2 \end{bmatrix}$ $\frac{1}{3}\begin{bmatrix} 1 & \sqrt{2}e^{-i\frac{2\pi}{3}} \\ \sqrt{2}e^{i\frac{2\pi}{3}} & 2 \end{bmatrix}$

Such projectors sums to $2I_2$ ($dI_d$ in general case). Scaling them by a factor $\frac{1}{2}$, we get a POVM called SIC POVM (*symmetric, informationally complete*).

This POVM gives four outcomes, let us denote them oznaczmy je by $0, \ldots, 3$. Measuring a density matrix $\rho = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)$ we get the following probabilities of outcomes:

$$\begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \end{bmatrix} = \frac{1}{4}\mathbb{1} + \frac{1}{12}\begin{bmatrix} 0 & 0 & 3 \\ 2\sqrt{2} & 0 & -1 \\ -\sqrt{2} & \sqrt{6} & -1 \\ -\sqrt{2} & -\sqrt{6} & -1 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} \tag{53}$$

Observe, that the columns of the above matrix are orthogonal to each other. The above formula is an isometric embedding of the Bloch ball into a three-dimensional simplex of four-outcome probability distributions.

**Exercise 44** *Find the formulas for $x, y, z$.*

## Estimation of distribution parameters

A result of a length-$n$ series of $K$-outcome measurements is a $n$-tuple of $K$ numbers, summing to one and denoting probabilities of obtaining the subsequent outcomes. They are estimators of the real

measurements - the parameters of the probability distribution. We would like to know, how well this estimators estimate the probability distribution parameters.

The probability distribution in the simplex of distribution parameters, under the condition that a given series of outcomes has been obtained, where cardinalities of sets of subsequent outcomes are $n_i$, is equal:

$$P(p_1, p_2, \ldots, p_K) \sim \prod_{i=1}^{K} p_i^{n_i} \tag{54}$$

(up to a normalising factor expressed by $\Gamma$ functions) This function attains its maximum, as we expect in the point $\vec{p}_{max} = \frac{1}{n}\vec{n}$, but the expected values of distribution parameters are: $\mathbb{E}(p_i) = \frac{n_i+1}{n+K}$.

The elements of covariance matrix are:

$$Var(p_i) = \frac{(n_i+1)(n+K-n_i-1)}{(n+K)^2(n+K+1)} \tag{55}$$

$$Cov(p_i, p_j) = -\frac{(n_i+1)(n_j+1)}{(n+K)^2(n+K+1)} \tag{56}$$

this distribution is known as the *Dirichlet distribution*. Using the above formulas one can control the covariance matrix of state parameters obtained in the tomography process.