3. QUANTUM COMPUTING

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

April 16, 2007

3. HILBERT SPACE BASICS

ABSTRACT

Hilbert space is a mathematical framework suitable for describing concepts, principles, processes and laws of quantum mechanics in general; and quantum information processing and communication (QIPC) in particular.

In this chapter those basics of Hilbert space theory are introduced and illustrated that play an important role in QIPC.

QUANTUM SYSTEM = HILBERT SPACE

Hilbert space H_n is n-dimensional complex vector space with

scalar product

$$\langle\psi|\phi\rangle = \sum_{i=1}^{n} \phi_i \psi_i^* \quad \text{of vectors } |\phi\rangle = \begin{vmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{vmatrix}, |\psi\rangle = \begin{vmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{vmatrix},$$

norm of vectors

$$||\phi|| = \sqrt{|\langle\phi|\phi\rangle|}$$

and the **metric**

$$\text{dist}(\phi, \psi) = ||\phi - \psi||.$$

This allows us to introduce on H a metric topology and such concepts as continuity.

All n-dimensional Hilbert spaces are isomorphic. Their vectors of norm 1 are called pure quantum states¿ Their physical counterparts are n-level quantum systems.

BRA-KET NOTATION

Dirac introduced a very handy notation, so called bra-ket notation, to deal with amplitudes, quantum states and linear functionals $f : H \rightarrow \mathbf{C}$.

If $\psi, \phi \in H$, then

$\langle\psi|\phi\rangle$ — **scalar product of ψ and ϕ**
(an amplitude of going from ϕ to ψ).

$|\phi\rangle$ — **ket-vector — an equivalent to ϕ**

$\langle\psi|$ — **bra-vector a linear functional on H**
such that $\langle\psi|(|\phi\rangle) = \langle\psi|\phi\rangle$

Example For states $\phi = (\phi_1, \ldots, \phi_n)$ and $\psi = (\psi_1, \ldots, \psi_n)$ we have

$$|\phi\rangle = \begin{pmatrix} \phi_1 \\ \ldots \\ \phi_n \end{pmatrix}, \langle\phi| = (\phi_1^*, \ldots, \phi_n^*); \langle\phi|\psi\rangle = \sum_{i=1}^{n} \phi_i^* \psi_i; |\phi\rangle\langle\psi| = \begin{pmatrix} \phi_1\psi_1^* & \ldots & \phi_1\psi_n^* \\ \vdots & \ddots & \vdots \\ \phi_n\psi_1^* & \ldots & \phi_n\psi_n^* \end{pmatrix}$$

GENERAL DEFINITION

Definition 0.1 *An* **inner-product space** H *is a complex vector space, equipped with an inner product* $\langle\cdot|\cdot\rangle : H \times H \rightarrow \mathbf{C}$ *satisfying the following axioms for any vectors* ϕ, $\psi, \phi_1, \phi_2 \in H$, *and any* $c_1, c_2 \in \mathbf{C}$.

$$\begin{aligned} \langle\phi|\psi\rangle &= \langle\psi|\phi\rangle^*, \\ \langle\psi|\psi\rangle &\geq 0 \text{ and } \langle\psi|\psi\rangle = 0 \text{ if and only if } \psi = \mathbf{0}, \\ \langle\psi|c_1\phi_1 + c_2\phi_2\rangle &= c_1\langle\psi|\phi_1\rangle + c_2\langle\psi|\phi_2\rangle.^1 \end{aligned}$$

The inner product introduces on H the norm (length)

$$||\psi|| = \sqrt{\langle\psi|\psi\rangle}$$

and the metric (Euclidean distance)

$$\text{dist}(\phi, \psi) = ||\phi - \psi||.$$

This allows us to introduce on H a metric topology and such concepts as continuity.

Some basic properties of the norm:

- $||\phi|| \geq 0$ for all $\phi \in H$ and $||\phi|| = 0$ if and only if $\phi = \mathbf{0}$
- $||\phi + \psi|| \leq ||\phi|| + ||\psi||$ (triangle inequality);
- $||a\phi|| = |a|\ ||\phi||$; (e) $|\langle\phi, \psi\rangle| \leq ||\phi||\ ||\psi||$ (Schwarz inequality).

COMPLETENESS, ISOMORPHISM and DUAL SPACE

Definition 0.2 *An inner-product space H is called* **complete***, if for any sequence*

$$\{\phi_i\}_{i=1}^{\infty},$$

with $\phi_i \in H$, and with the property that

$$\lim_{i,j\to\infty} ||\phi_i - \phi_j|| = 0,$$

there is a unique element $\phi \in H$ such that

$$\lim_{i\to\infty} ||\phi - \phi_i|| = 0.$$

A complete inner-product space is called a **Hilbert space***.*

Two Hilbert spaces H_1 and H_2 are said to be **isomorphic***, notation $H_1 \simeq H_2$, if the underlying vector spaces are isomorphic and their isomorphism preserves the inner product.*

BASIC EXAMPLES of HILBERT SPACES

Let us start with the two most important examples of Hilbert spaces.

Example 0.3 *Hilbert spaces $l_2(D)$ For any countable set D, let $l_2(D)$ be the space of all complex valued functions on D bounded by the so-called l_2-norm, i.e.*

$$l_2(D) = \{x \,|\, x : D \rightarrow \mathbf{C}, \left(\sum_{i \in D} x(i)x^*(i)\right)^{1/2} < \infty\}^2.$$

We say that $l_2(D)$ is a Hilbert space with respect to the **inner product** $\langle \cdot \,|\, \cdot \rangle : l_2(D) \times l_2(D) \rightarrow \mathbf{C}$, *defined by*

$$\langle x_1 | x_2 \rangle = \sum_{i \in D} x_1^*(i) x_2(i).$$

Elements of $l_2(D)$ are usually called vectors (to be indexed by elements of D). The notation $l_2 = l_2(\mathbf{N})$ is usually used in the case $D = \mathbf{N}$.

[2] x^* denotes the conjugate of the com x; i.e., $x^* = a - bi$ if $x = a + bi$, where a, b are real.

Example 0.4 *Hilbert space* L_2[3] *Let* (a, b) *be an interval, with finite or infinite bounds, on the real axis. By* $L_2((a, b))$, *or simply* L_2, *we denote the set of all complex valued functions such that* $\int_a^b |f(x)|^2\,dx$ *exists, equipped with the inner product*

$$\langle f|g\rangle = \int_a^b f^*(t)g(t)\,dt < \infty.$$

If f *and* g *are such that* $|f|^2$ *and* $|g|^2$ *are integrable functions (with respect to Lebesgue measure) on* (a, b), *then so are functions* cf *and* $f + g$, *for any complex number* c, *and therefore* L_2 *is a linear space.*[4]

Surprisingly, for two Hilbert spaces introduced in the last examples it holds

$$l_2 \simeq L_2$$

that is they are isomorphic (so-called Riesz-Fischer Theorem.)

[3] Hilbert studied spaces l_2 and L_2, in his work on linear integral systems, and that is why von Neumann all spaces of such types named as Hilbert spaces.

[4] To be more precise L_2 is to be the set of Lebesgue integrable functions on (a, b) and we do not consider as different a pair of functions that differ only on a set of measure zero. In such a linear space the zero element is a function that is equal to zero almost everywhere on (a, b).

ORTHOGONALITY of STATES

Two vectors $|\phi\rangle$ and $|\psi\rangle$ are called orthogonal vectors if $\langle\phi|\psi\rangle = 0$.

Physically are fully distinguishable only orthogonal vectors (states).

By a basis $\mathcal{B}$ of H_n we will understand any set of n vectors $|b_1\rangle, |b_2\rangle, \ldots, |b_n\rangle$ in $\mathcal{H}_n$ of the norm 1 which are mutually orthogonal.

Given a basis $\mathcal{B}$, any vector $|\psi\rangle$ from H_n can be uniquely expressed in the form

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i |b_i\rangle.$$

A set S of vectors is called orthonormal if all vectors of S have norm 1 and are mutually orthogonal.

DefinitionA subspace G of a Hilbert space H is a subset of H closed under addition and scalar multiplication.

An important property of Hilbert spaces is their decomposability into mutually orthogonal subspaces. It holds:

Theorem **For each closed subspace W of a Hilbert space H there exists a unique subspace $W^\perp$ such that $\langle\phi|\psi\rangle = 0$, whenever $\phi \in W$ and $\psi \in W^\perp$**

and

each $\psi \in H$ can be uniquely expressed in the form $\psi = \phi_1 + \phi_2$, with $\phi_1 \in W$ and $\phi_2 \in W^\perp$. In such a case we write $H = W \oplus W^\perp$ and we say that W and $W^\perp$ form an orthogonal decomposition of H.

In a natural way we can make a generalization of an orthogonal decomposition

$$H = W_1 \oplus W_2 \oplus \ldots \oplus W_n,$$

of H into mutually orthogonal subspaces $W_1, \ldots, W_n$ such that each $\psi \in H$ has a unique representation as $\psi = \phi_1 + \phi_2 + \ldots + \phi_n$, with $\phi_i \in W_i, 1 \leq i \leq n$.

OPERATORS of HILBERT SPACES

A linear operator on a Hilbert space H is a linear mapping $A : H \rightarrow H$.

An application of a linear operator A to a vector $|\psi\rangle$ is denoted $A|\psi\rangle$.

A is also a linear operator of the dual Hilbert space H^*, mapping each linear functional $\langle\phi|$ of the dual space to the linear functional, denoted by $\langle\phi|A$.

A linear operator A is called positive or semi-definite, notation $A \geq 0$, if $\langle\psi|A\psi\rangle \geq 0$ for every $|\psi\rangle \in H$.

The norm $||A||$ of a linear operator A is defined as

$$||A|| = \sup_{||\phi||=1} ||A|\phi\rangle||.$$

A linear operator is called bounded if its norm is finite.

Projections have a special role among linear operators.

If $H = W_1 \oplus W_2$ **is an orthogonal decomposition of a Hilbert space** H **into subspaces** W_1 **and** W_2**, then, as mentioned above, each** $\psi \in H$ **has a unique representation** $\psi = \psi_1 + \psi_2$**, where** $\psi_1 \in W_1$ **and** $\psi_2 \in W_2$**.**

$$P_{W_1}(\psi) = \psi_1 \quad \textbf{and} \quad P_{W_2}(\psi) = \psi_2$$

are called projections onto the subspaces W_1 **and** W_2**, respectively.**

Example If $\phi \in H$ **for** $||\phi|| = 1$ **and a Hilbert space** H**, then the operator defined by** $|\phi\rangle\langle\phi|$ **and defined by**

$$|\phi\rangle\langle\phi|(|\psi\rangle) = \langle\phi|\psi\rangle|\phi\rangle$$

is a projection into the one-dimensional subspace spanned by the vector $|\phi\rangle$**.**

REPRESENTATIONS

If $\beta = \{\theta_i\}_{i=1}^n$ is an orthonormal basis of a Hilbert space $\mathcal{H}$, then any state $|\phi\rangle$ has a unique representation

$$|\phi\rangle = \sum_{i=1}^{n} \langle\theta_i|\phi\rangle|\theta_i\rangle.$$

Each linear operator A of a countable Hilbert space H with a basis $\mathcal{B} = \{|\theta_i\rangle\,|\, i \in I\}$ can be represented by a matrix, in general infinitely dimensional, whose rows and columns are labeled by elements of I and with $\langle\theta_i|A|\theta_j\rangle = \langle\theta_i|A\theta_j\rangle$ in the i-th row and j-th column. Such a matrix is said to be matrix representation of A relative to the basis β.

Each operator A has also so-called outer-product representation:

$$A = \sum_{ij} \langle\theta_i|A|\theta_j\rangle|\theta_i\rangle\langle\theta_j|.$$

(here we use for $\langle\theta_i|A\theta_j\rangle$ Dirac's notation $\langle\theta_i|A|\theta_j\rangle$).

TRACE of OPERATORS

Definition 0.5 *Let $\mathcal{H}$ be an n-dimensional Hilbert space and $\mathcal{B}$ be an orthogonal basis on $\mathcal{H}$. The* **trace (operator)** *of a linear mapping $M : \mathcal{H} \to \mathcal{H}$ is defined by*

$$\mathrm{Tr}(M) = \sum_{\phi \in \mathcal{B}} \langle \phi | M | \phi \rangle.$$

In addition, if A is the matrix representation of M in the basis $\mathcal{B}$. Then

$$\mathrm{Tr}(M) = \mathrm{Tr}(A) = \sum_{i=1}^{n} a_{ii},$$

where a_{ii} is the element of the matrix A at the position (i, i).

Properties of the trace operator:

- Trace of a linear mapping does not depend on the basis chosen.
- $Tr(A + B) = Tr(A) + Tr(B)$.
- $Tr(AB) = Tr(BA)$; $Tr(A \otimes B) = Tr(A)\,Tr(B)$.
- $Tr(\alpha A) = \alpha\, Tr(A)$.
- $Tr(|\psi\rangle\langle\phi|) = \langle\phi|\psi\rangle$.

SELF-ADJOINT OPERATORS

Of special importance are adjoint and self-adjoint operators.

The adjoint operator T^* to a bounded linear operator T is an operator such that for any ϕ and $\psi \in H$,

$$\langle\psi|T\phi\rangle = \langle T^*\psi|\phi\rangle.$$

An operator T is self-adjoint if $T = T^*$.

Instead of $\langle\psi|T\phi\rangle$ notation $\langle\psi|T|\phi\rangle$ is used. Hence

$$\langle T^*\psi|\phi\rangle = \langle\psi|T|\phi\rangle = \langle\psi|T\phi\rangle.$$

SELF-ADJOINT OPERATORS — HERMITIAN MATRICES

To self-adjoint operators correspond Hermitian matrices, i.e., matrices A such that $A = A^*$.

Theorem 0.6 ***Hermitian matrices have the following properties.***

1. ***All eigenvalues of a Hermitian matrix are real.***
2. ***The eigenvectors of an Hermitian matrix corresponding to distinct eigenvalues are orthogonal.***

Proof of property 1: If $A\phi = \lambda\phi$, then

$$\lambda^*\langle\phi|\phi\rangle = \langle\lambda\phi|\phi\rangle = \langle A\phi|\phi\rangle = \langle\phi|A\phi\rangle = \lambda\langle\phi|\phi\rangle.$$

hence $\lambda^* = \lambda$.

Proof of property 2 Assume that $\lambda \neq \lambda'$, $A\phi = \lambda\phi, A\phi' = \lambda'\phi'$. Since λ, λ' are real, it holds

$$\lambda'\langle\phi'|\phi\rangle = \langle A\phi'|\phi\rangle = \langle\phi'|A\phi\rangle = \lambda\langle\phi'|\phi\rangle$$

and therefore $\langle\phi'|\phi\rangle = 0$.

SPECTRAL REPRESENTATION of SELF-ADJOINT OPERATORS

A self-adjoint operator A of a finite dimensional Hilbert space H has the so-called **spectral representation**. If $\lambda_1, \ldots, \lambda_k$ are its distinct eigenvalues, then A can be expressed in the form

$$A = \sum_{i=1}^{k} \lambda_i P_i,$$

where P_i is the projection operator into the subspace of H spanned by the eigenvectors corresponding to λ_i.

In a special case when all eigenvalues are distinct and $|\phi_i\rangle$ is eigenstate corresponding to the eigenvalue λ_i, then

$$A = \sum_{i=1}^{n} \lambda_i |\phi_i\rangle\langle\phi_i|$$

Since $P_i P_j = 0$ for two different projections, it holds for any polynomial

$$p(A) = \sum_{i=1}^{k} p(\lambda_i) P_i.$$

This is generalized to define for ant $f : \mathbf{R} \rightarrow \mathbf{C}$ by

$$f(A) = \sum_{i=1}^{k} f(\lambda_i) P_i.$$

Example Pauli matrix σ_x has eigenvalues 1 and -1 and corresponding eigenvectors are $|0'\rangle$ and $|1'\rangle$. Since

$$|0'\rangle\langle 0'| = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \quad |1'\rangle\langle 1'| = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

and therefore

$$\sqrt{\sigma_x} = \sqrt{1}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} + \sqrt{-1}\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

that is

$$\sqrt{\sigma_x} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}.$$

SPECTRAL REPRESENTATION of UNITARY OPERATORS

Each self-adjoint operator A has spectral decomposition $A = \Sigma_{i=1}\, n\lambda_i|\phi_i\rangle\langle\phi_i|$ and therefore

$$e^{iA} = \sum_{j=1}^{n} e^{i\phi_j}|\phi_j\rangle\langle\phi_j|$$

and therefore

$$(e^{iA})^* = \sum_{j=1}^{n} e^{-i\lambda_j}|\phi_j\rangle\langle\phi_j| = (e^{iA})^{-1}$$

what implies that matrix e^{iA} is unitary.

We show now that each unitary matrix $U = e^{iH}$ for some self-adjoint operator H. Indeed, if U is decomposed into a "real and imaginary" part $U = A + iB$, then A and B are both self-adjoint and have spectral decompositions

$$A = \sum_{i=1}^{n} \lambda_i|\phi_i\rangle\langle\phi_i|$$

$$B = \sum_{i=1}^{n} \mu_i|\phi_i\rangle\langle\phi_i|$$

All eigenvalues of a unitary matrix have eigenvalues with absolute value 1 and self-adjoint matrices have eigenvalues real, for each j an $\theta_j \in [0, 2\pi]$ has to exists such that $\lambda_j + i\mu_j = e^{i\theta_j}$. Hence for

$$H = \sum_{j=1}^{n} \theta_j |\phi_j\rangle\langle\phi_j|$$

we have

$$U = e^{iH}.$$

Example 1 Hadamard transform $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ has as eigenvalues 1 and -1 and corresponding eigenvectors are

$$\phi_1 = \frac{1}{\sqrt{4+2\sqrt{2}}}\begin{pmatrix} 1+\sqrt{2} \\ 1 \end{pmatrix} \quad \phi_{-1} = \frac{1}{\sqrt{4-2\sqrt{2}}}\begin{pmatrix} 1-\sqrt{2} \\ 1 \end{pmatrix}$$

The spectral decomposition of H is then

$$H = 1 \cdot |\phi_1\rangle\langle\phi_1| + (-1)|\phi_{-1}\rangle\langle\phi_{-1}|$$

and therefore $H = e^{iA}$, where

$$A = 0 \cdot |\phi_1\rangle\langle\phi_1| + \pi|\phi_{-1}\rangle\langle\phi_{-1}|$$

Example 2 It holds

$$R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = e^{iA_\theta} \ \ \text{where} A_\theta = \begin{pmatrix} 0 & i\theta \\ -i\theta & 0 \end{pmatrix}.$$

QUANTUM TIME EVOLUTION

It is natural to assume that there is a mapping $U_t : \mathcal{H} \rightarrow \mathcal{H}_n$ that depends on time t that maps the initial state $|\phi_0\rangle$ into the state $|\phi_t\rangle$ in time t, that is that

$$|\phi_t\rangle = U_t|\phi_0\rangle.$$

It is also natural to put the following four requirements on U_t:

1. U_t should map states into states, that is it should preserve norm:

   For each real $t > 0$ and each state $|\phi\rangle$, $||U_t|\phi\rangle|| = ||\phi\rangle||$.

2. U_t should be linear - what means that each basis state should develop independently. Namely: for each basis $\{\beta_i\}_{i=1}^n$,

   $$U_t(\sum_{i=1}^n a_i|\beta_i\rangle) = \sum_{i=1}^n a_i U_t(|\beta_i\rangle)$$

   .

3. U_t should be decomposable. Namely, for all $t_1 > 0, t_2 > 0$

   $$U_{t_1+t_2} = U_{t_1}U_{t_2}.$$

4. Evolution should be smooth. Namely, for each real t_0

$$\lim_{t \to t_0} U_t|\phi_0\rangle = \lim_{t \to t_0} |\phi_t\rangle = |\phi_{t_0}\rangle.$$

Theorem If time evolution U_t satisfies the above four conditions, then U_t has to be unitary and $U_t = e^{-iH}$ for some self-adjoint operator H. Hence

$$\frac{\partial \phi_t}{\partial t} = -iHe^{-itH}\phi_0 = -iH\phi_t$$

what is known as abstract Schrödinger equation.

QUANTUM (PROJECTION) MEASUREMENT - OBSERVABLES

Informally, a quantum state $|\psi\rangle$ is observed (measured) with respect to an **observable** — a Hermitian matrix A which specifies a decomposition of the Hilbert space into orthogonal subspaces (such that each vector can be uniquely represented as a sum of vectors of these subspaces) that are subspaces generated by eigenvectors corresponding to different eigenvalues of the operator A.

There are two outcomes of a projection measurement of a state $|\phi\rangle$:

1. Information into which subspace projection of $|\phi\rangle$ took place.
2. Resulting projection (a new quantum state) $|\phi'\rangle$.

The subspace into which projection is made is chosen **randomly** and the corresponding probability is uniquely determined by the amplitudes at the representation of $|\phi\rangle$ at the basis states of the subspace.

Namely, if

$$A = \sum_{i=1}^{k} \lambda_i P_i$$

where P_i are projections into mutually orthogonal subspaces, then by measuring (observing) a state $|\phi\rangle$ this state collapses into the state

$$P_i|\phi\rangle$$

with probability

$$\langle\phi|P_i\phi\rangle$$

and we also say that with the same probability the value λ_i is observed in the classical world.

Of importance often is also the expected value of A in the state $|\phi\rangle$ defined by

$$E_\phi(A) = \sum_{i=1}^{k} \lambda_i \langle\phi|P_i\phi\rangle = \langle\phi|A\phi\rangle.$$

EXAMPLE

Observable $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has eigenvalues $\{1, -1\}$ and eigenvectors $\{|0'\rangle, |1'\rangle\}$.

A measurement with respect to the observable σ_x is therefore measurement with respect to the dual basis.

Observable $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ has eigenvalues $\{1, -1\}$ and eigenvectors $\{|0\rangle, |1\rangle\}$.

A measurement with respect to the observable σ_x is therefore measurement with respect to the standard (computational) basis.

PROBABILITIES

To the key outcomes of quantum mechanics belong rules for determining probabilities of the outcomes of quantum measurements.

The classical outcome of a measurement of a state $|\psi\rangle$ with respect to an observable A is one of the eigenvalues of A and quantum impact of such a measurement is a "collapse" of $|\psi\rangle$ into a state $|\psi'\rangle$. In the measurement the eigenvalue λ_i is obtained with probability

$$Pr(\lambda_i) = ||P_i|\psi\rangle||^2 = \langle\psi|P_i|\psi\rangle,$$

and the new state $|\psi'\rangle$, into which $|\psi\rangle$ collapses, has the form

$$|\psi'\rangle = \frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}.$$

ANOTHER VIEW of MEASUREMENT

Quantum measurement is described by a finite set $\{P_m\}$ of projectorsacting on the state space of the system being measured and such that $\Sigma_m P_m = I$ - the index m refers to the potentail clasical outcomes of a measurement.

if a state $|\phi\rangle$ is measured with respect to $\{P_m\}$, then the result m occurs with probability

$$\mathbf{Pr}(m) = \langle\phi|P_m|\phi\rangle$$

and if such a resukt occurs the state of the system immediately after measuremnet is

$$\frac{P_m|\phi\rangle}{\sqrt{\langle\phi|P_m|\phi\rangle}} = \frac{P_m|\phi\rangle}{\sqrt{\mathbf{Pr}(m)}}.$$

If α is a real number, we say that states $|\phi\rangle$ and $E^{i\alpha}|\phi\rangle$ are equivalent, or equal up to a phase factor. Two such states give the same measurement statics, what follows from the relations

$$\langle e^{i\alpha}\phi|P_m|e^{i\alpha}\phi\rangle = e^{-i\alpha}e^{i\alpha}\langle\phi|P_m|\phi\rangle = \langle\phi|P_m|\phi\rangle.$$

EXPECTATION VALUE

Let A be self-adjoint operator of a Hilbert space H , with spectral decomposition

$$A = \sum_{i=1}^{k} \lambda_i P_{\lambda_i}.$$

The expectation value of A in the state ψ is defined by

$$\begin{aligned}
\mathrm{exp}_\psi(A) &= \sum_{i=1}^{k} \lambda_i \mathrm{prob}_\psi(\lambda_i) \\
&= \sum_{i=1}^{k} \lambda_i \langle P_{\lambda_i}\psi | P_{\lambda_i}\psi \rangle \\
&= \sum_{i=1}^{k} \lambda_i \langle \psi | P_{\lambda_i}\psi \rangle \\
&= \langle \psi | \sum_{i=1}^{k} \lambda_i P_{\lambda_i} | \psi \rangle \\
&= \langle \psi | A\psi \rangle \\
&= \langle \psi | AP_\psi \psi \rangle = \mathit{Tr}(AP_\psi) = \mathit{Tr}(P_\psi A).
\end{aligned}$$

MIXED STATES — DENSITY MATRICES

Pure states are fundamental objects for quantum mechanics in the sense that the evolution of any closed quantum system can be seen as a unitary evolution of pure states.

However, to deal with unisolated and composed quantum systems the concept of mixed states is of importance.

A probability distribution $\{(p_i, \phi_i) \,|\, 1 \leq i \leq k\}$ on pure states $\{\phi_i\}_{i=1}^k$, with probabilities $0 < p_i \leq 1$, $\Sigma_{i=1}^k p_i = 1$ is called a **mixed state** or **mixture**, and denoted by $[\psi\rangle = \{(p_i, \phi_i) \,|\, 1 \leq i \leq k\}$. For example, a mixed state is created if a source produces pure state $|\phi_i\rangle$ with probability p_i and $\Sigma_{i=1}^k p_i = 1$.

To each mixed state $[\psi\rangle = \{(p_i, \phi_i) \,|\, 1 \leq i \leq k\}$ corresponds a **density operator**

$$\rho_{[\psi\rangle} = \sum_{i=1}^{k} p_i |\phi_i\rangle\langle\phi_i|.$$

Key observation Two mixed states with the same density matrix are physically undistinguishable.

EXAMPLES

The density matrix corresponding to the mixed state

$$(\frac{1}{2}, |0\rangle) \oplus (\frac{1}{2}, |1\rangle)$$

has the form

$$\frac{1}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix}(0,1) + \frac{1}{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}(0,1) = \frac{1}{2}I.$$

For any pure one qubit state $\alpha|0\rangle + \beta|1\rangle$, to the mixed state

$$(\frac{1}{4}, \alpha|0\rangle + \beta|1\rangle) \oplus (\frac{1}{4}, \alpha|0\rangle - \beta|1\rangle) \oplus (\frac{1}{4}, \beta|0\rangle + \alpha|1\rangle) \oplus (\frac{1}{4}, \beta|0\rangle - \alpha|1\rangle)$$

corresponds the density matrix

$$\frac{1}{4}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}(\alpha^*, \beta^*) + \frac{1}{4}\begin{pmatrix} \alpha \\ -\beta \end{pmatrix}(\alpha^*, -\beta^*)$$

$$+\frac{1}{4}\begin{pmatrix} \beta \\ \alpha \end{pmatrix}(\beta^*, \alpha^*) + \frac{1}{4}\begin{pmatrix} \beta \\ -\alpha \end{pmatrix}(\beta^*, -\alpha^*) = \frac{1}{2}I$$

REPRESENTATION of MIXED STATES

If ρ is a density matrix and in a basis $\{\beta_i\}_{i=1}^n$

$$\rho = \{\rho_{i,j}\}_{i,j=1}^n,$$

then

$$\rho = \sum_{i,j=1}^n \rho_{i,j} |\beta_i\rangle\langle\beta_j|.$$

As a consequence

$$\langle\beta_k|\rho|\beta_l\rangle = \rho_{k,l}.$$

PROPERTIES of DENSITY MATRICES

1. **Any density matrix ρ is Hermitian, nonnegative, has only nonnegative eigenvalues and $\boldsymbol{Tr}(\rho) = 1$.**
2. **If ρ_1 and ρ_2 are density matrices on the same Hilbert space, then $p\rho_1 + (1-p)\rho_2$, $0 \leq p \leq 1$ is a density matrix too.**
3. **If ρ is a density matrix, then so is the matrix ρ^T.**
4. **If ρ_1 is a density matrix on a Hilbert space $\mathcal{H}_1$ and ρ_2 is a density matrix on a Hilbert space $\mathcal{H}_2$, then $\rho_1 \otimes \rho_2$ is density matrix on the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$.**
5. **A matrix ρ is a density matrix if it is Hermitian, nonnegative and $\boldsymbol{Tr}\rho = 1$.**

TRACING OUT OPERATION

One of the profound differences between the quantum and classical systems lies in the relation between a system and its subsystems.

As discussed below a state of a Hilbert space $H = H_A \otimes H_B$ cannot be always decomposed into states of its subspaces H_A and H_B. We also cannot define any natural mapping from the space of linear operators on H into the space of linear operators on H_A (or H_B).

However, density operators are much more robust and that is also one reason for their importance. A density operator ρ on H can be "projected" into H_A by the operation of tracing out H_B, to give the density operator (for finite dimensional Hilbert spaces):

$$\rho_{H_A} = Tr_{H_B}(\rho) = \sum_{|\phi\rangle,|\phi'\rangle \in \mathcal{B}_{H_A}} |\phi\rangle \left(\sum_{|\psi\rangle \in \mathcal{B}_{H_B}} \langle \phi, \psi | \rho | \phi', \psi \rangle \right) \langle \phi' |,$$

where $\mathcal{B}_{H_A}$ ($\mathcal{B}_{H_B}$) is an orthonormal basis of the Hilbert space H_A (H_B).

MEANING of TRACING OUT OPERATIONS

If $\boldsymbol{dim}(H_A) = n$, $\boldsymbol{dim}(H_B) = m$, **then** ρ **is an** $nm \times nm$ **matrix which can be seen as an** $n \times n$ **matrix consisting of** $m \times m$ **blocks** ρ_{ij} **as follows:**

$$\rho = \begin{pmatrix} \rho_{11} & \dots & \rho_{1n} \\ \vdots & \ddots & \\ \rho_{n1} & \dots & \rho_{nn} \end{pmatrix}$$

and in such a case

$$\rho_{H_A} = \begin{pmatrix} \boldsymbol{Tr}(\rho_{11}) & \dots & \boldsymbol{Tr}(\rho_{1n}) \\ \vdots & \ddots & \vdots \\ \boldsymbol{Tr}(\rho_{n1}) & \dots & \boldsymbol{tr}(\rho_{nn}) \end{pmatrix}$$

WHY SUCH a TRACING OUT OPERATION?

The following fact is the main mathematical justification that strangely looking tracing out operation has the proper physical meaning:

If $H = \mathcal{H}_A \otimes \mathcal{H}_B$ and ρ is a density matrix of H, then $\rho_A = Tr_B(\rho)$ is the unique density matrix of $\mathcal{H}_A$ such that

$$Tr(\rho_A \cdot O) = Tr(\rho \cdot (O \otimes I))$$

for each observable (Hermitian matrix) O of $\mathcal{H}_A$.

In other words the average value of the measurement of ρ_A on $\mathcal{H}_A$ with respect to the observable $\mathcal{O}$, on $\mathcal{H}_A$, equals the average value of the measurement of ρ on $\mathcal{H}$ with respect to the observable $O \otimes I$ on $\mathcal{H}$.

Informally, one often says that in order to get the density matrix of a subsystem, given the density matrix of the whole system, one should trace over the degrees of freedom of the rest of the system.

TRACING OUT OPERATION

Perhaps the simplest way to introduce tracing out operation is to say that it is a linear operation such that for any bipartite system $A \otimes B$ and any states $|\phi_1\rangle$ and $|\phi_2\rangle$ of A and any states $|\psi_1\rangle$ and $|\psi_2\rangle$ of B

$$\boldsymbol{Tr}_B(|\phi_1\rangle\langle\phi_2| \otimes |\psi_1\rangle\langle\psi_2|) = |\phi_1\rangle\langle\phi_2|\,\boldsymbol{Tr}(|\psi_1\rangle\langle\psi_2|) = \langle\psi_2|\psi_1\rangle|\phi_1\rangle\langle\phi_2|.$$

MEASUREMENT on MIXED STATES

Let A be an observable (self-adjoint operator), Δ an interval on real axis and P_{Δ}^{A} the projection operator into the subspace of all pure states measurement of which, with respect to A, produces with certainty a value from Δ.

The probability that measurement of a mixed state ρ with respect to an observable A produces a value from Δ, that is

$$Pr_{\rho}(A, \Delta)$$

equals

$$Pr_{\rho}(A, \Delta) = \mathit{Tr}(\rho P_{\Delta}^{A})$$

and in the case ρ is a pure state, that is $\rho = |\psi\rangle\langle\psi|$ for a pure state $|\psi\rangle$, then

$$Pr_{\psi}(A, \Delta) = \langle\psi|P_{\Delta}^{P}\psi\rangle.$$

SUPEROPERATORS

- **A superoperator (SO) is a linear transformation on linear operators of a Hilbert space.**
- **A positive superoperator (PSO) is a superoperator that maps density matrices into density matrices.**
- **A completely positive superoperator (CPO) G is a PSO such that, for all positive integer m, $G \otimes I_m$ is also a PSO, where I_m is the identity matrix.**

CPO are exactly the physically allowed transformations on density matrices.

Examples: encoders, decoders, quantum channels, quantum measurements.

SUPEROPERATORS — INFORMAL VIEW

Informally, the best way is to see a superoperator S applied to a state $|\phi\rangle$ of a Hilbert space H as to take first an auxiliary state (called usually ancilla) of another Hilbert space H', then to apply a unitary operator U to the state $|\phi\rangle \otimes |\psi\rangle$ and, finally, to discard the H'-part of the resulting state.

WHAT ARE QUANTUM OPERATIONS?

The main question we deal with in this section is very fundamental. What are physically realizable operations one can perform (at least theoretically) on (mixed) states (to get again (mixed) states)?

In closed quantum systems unitary operations are actually the only quantum operations that are ava ilable. Measurements are actually outside of the closed system framework, an interface from quantum to classical world, but surely they are operations we consider as physically realizable.

Of main importance are quantum operations in open quantum systems. Actually, all actions that are performed in open quantum systems are quantum operations: unitary operations , measurements, channel transmissions, flow of time, noise impacts, ...

The concept of quantum operations is therefore very general and very fundamental.

It is perhaps a bit surprising, but actually nice, useful and natural, that we can actually study and consider open quantum systems in the framework of closed quantum systems. We can consider as the basic setting that our (principal) quantum system and its environment form a closed quantum system in which we operate.

The requirement to consider only physically realizable (at least theoretically) operation is, of course, logical. As we shall see this question has, in a sense and at least theoretically, clear and simple answer. They are, as discussed later, *trace preserving completely positive linear maps*.

THREE APPROACHES

There are basically three main approaches to define what are "physically realizable quantum operations" (superoperators) $\mathcal{E}$.

A physically motivated axiomatic approach says that for a Hilbert space $\mathcal{H}$ we should consider as physically realizable operations maps $\mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$ which are *consistent with the (statistical) interpretation of quantum theory*. That is maps that are *linear* (to preserve superpositions), *positive* and *trace preserving* (to map density operators to density operators) and actually completely positive (to be sure that if a superoperator is applied to a subsystem, then the whole system is again in a quantum state).

A pragmatic approach says that superoperators are those operations that can be combined from unitary operations, adding ancillas, performing (non-selective) projective measurement and discarding subsystems (ancillas), by performing a tracing out operation.

A mathematical approach says that all basic quantum operations: adding and discarding quantum subsystems, unitary operations and non-selective projective measurements have Kraus operator-sum representation

$$\rho \to \sum_{i=1}^{k} E_i \rho E_i^{\dagger},$$

where so called *Kraus operators* $E_i : \mathcal{H} \to \mathcal{H}$ are not necessarily Hermitian operators, but they should be positive and should form a "decomposition of the identity operator", that is, $\sum_{i=1}^{k} E_i^{\dagger} E_i = I_{\mathcal{H}}$ – so called completeness condition.

It is a consequence of the completeness condition, and a property of trace operation, that for any superoperator $\mathcal{E}$ holds

$$\boldsymbol{Tr}(\mathcal{E}(\rho)) = \boldsymbol{Tr}(\sum_i E_i \rho E_i^{\dagger}) = \boldsymbol{Tr}(\sum_i E_i^{\dagger} E_i \rho) = \boldsymbol{Tr}((\sum_i E_i^{\dagger} E_i)\rho) = \boldsymbol{Tr}(\rho) = 1.$$

STINESPRING DILATION THEOREM

So called *Stinespring dilation theorem*, discussed below, says, that each superoperator can be realized in "one big three-stage-step" : adding an ancilla, performing a unitary operation on a composed quantum system and, finally, discarding the ancilla, see Figure 1, or other subsystems.

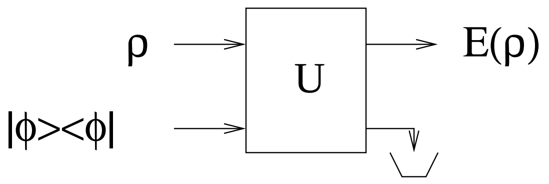

Figure 1: A Stinespring realization of a superoperator. In this view a superoperator $\mathcal{E}$ performs the mapping $\mathcal{E}(\rho) = Tr_a(U(\rho \times \rho_a)U^\dagger)$, where ρ_a is the "initial state", for example $|\phi\rangle\langle\phi|$ of an ancilla subsystem, U is a unitary operation on composed system and, finally, a tracing out operation is performed.