



MTAT.07.024

Quantum Crypto

Lecture #06

Hilbert Space (complete)

Complex (\mathbb{C}) Hilbert space

- ... is where states of "closed" quantum systems live ("pure" states)
- ... is where the math works out easily.

Real (\mathbb{R}) Hilbert space

- ... is where states of "open" quantum systems live ("mixed" states)
- ... is where calculus is done (gradients, Jacobians, Hessians, ...).
- Not everything works without "escaping" to \mathbb{C} .

Example #1a: \mathbb{R}^n

Set:

- n tuples of real numbers
(usually displayed vertically to make the operations easy to visualize)

Operations:

- Vector addition:
- Zero vector:
- Vector subtraction & additive inverses:
binary minus-operator:
unary minus-operator:
- Scalar multiplication:
- Inner product:
- Norm (length):

$$+(\mathbf{x} :: \mathbb{R}^n, \mathbf{y} :: \mathbb{R}^n) :: \mathbb{R}^n$$

$$0_{\mathbb{R}^n} := (0, \dots, 0)$$

$$-(\mathbf{x} :: \mathbb{R}^n, \mathbf{y} :: \mathbb{R}^n) :: \mathbb{R}^n$$

$$-(\mathbf{x} :: \mathbb{R}^n) :: \mathbb{R}^n$$

$$*(\alpha :: \mathbb{R}, \mathbf{x} :: \mathbb{R}^n) :: \mathbb{R}^n$$

$$\langle \mathbf{x} :: \mathbb{R}^n, \mathbf{y} :: \mathbb{R}^n \rangle :: \mathbb{R}$$

$$\text{norm}(\mathbf{x} :: \mathbb{R}^n) :: \mathbb{R} \quad \text{math notation: } \|x\|_3$$

Example #1a: \mathbb{R}^n

Schaum 1.8

$$x = (x_1, \dots, x_n) \in \mathbb{R}^n, \quad y = (y_1, \dots, y_n) \in \mathbb{R}^n, \quad \alpha \in \mathbb{R}$$

$$x + y := (x_1 + y_1, \dots, x_n + y_n)$$

$$x - y := (x_1 - y_1, \dots, x_n - y_n)$$

$$-x := (-x_1, \dots, -x_n)$$

$$\alpha \cdot x := (\alpha \cdot x_1, \dots, \alpha \cdot x_n)$$

$$\langle x, y \rangle := x_1 \cdot y_1 + \dots + x_n \cdot y_n$$

$$\|x\| := \sqrt{\langle x, x \rangle}$$

Rules & Laws

1. Vector addition is...

- associative & commutative
- zero works, additive inverse/subtraction work

2. Scalar-multiplication is...

- associative: $\forall \alpha, \beta \in \mathbb{R} \forall x \in \mathbb{R}^n: (\alpha \cdot \beta) \cdot x = \alpha \cdot (\beta \cdot x)$
- distributive over vector addition: $\forall \alpha \in \mathbb{R} \forall x, y \in \mathbb{R}^n: \alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$
- distributive over scalar addition: $\forall \alpha, \beta \in \mathbb{R} \forall x \in \mathbb{R}^n: (\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$
- Don't-Bullshit-Me Rule: $1 \cdot x = x$

3. Inner product is...

- \mathbb{R} -linear in the left side: $\forall y: x \mapsto \langle x, y \rangle$ \mathbb{R} -linear
- \mathbb{R} -linear in the right side: $\forall x: y \mapsto \langle x, y \rangle$ \mathbb{R} -linear
- symmetric: $\forall x, y: \langle x, y \rangle = \langle y, x \rangle$
- positive: $\forall x \neq 0_{\mathbb{R}^n}: \langle x, x \rangle > 0.$

Real Hilbert Space

Definition.

A real Hilbert space is a set ("type") for which the operations

- *vector addition (w/ zero, subtraction, unary minus etc)*
- *scalar multiplication with elements of \mathbb{R}*
- *inner product*

are defined and satisfy the laws.

Notes

- inner product is *symmetric* and *bi-linear*
- $\text{norm}(z) = \|x\| := \sqrt{\langle x, x \rangle}$ — no need to mention it

Consequences of the Rules & Laws

Theorem (Cauchy-Schwarz).

For all x, y we have $|\langle x, y \rangle| \leq \|x\| \cdot \|y\|$.

Equality holds if, and only if, x, y are collinear

(i.e., there exist $\alpha, \beta \in \mathbb{R}$, at least one of them non-zero, with $\alpha x = \beta y$).

Theorem (Properties of a "Norm").

1. Triangle leq: For all x, y we have $\|x + y\| \leq \|x\| + \|y\|$.
2. Positive homogeneous: For all x , if $\alpha \in \mathbb{R}$, we have $\|\alpha \cdot x\| = |\alpha| \cdot \|x\|$.
3. Separation: For all x , if $\|x\| = 0$, then $x = 0$.

Example #1: \mathbb{C}^n

Set:

- n tuples of complex numbers
(usually displayed vertically to make the operations easy to visualize)

Operations:

- Vector addition:
- Zero vector:
- Vector subtraction & additive inverses:
binary minus-operator:
unary minus-operator:
- Scalar multiplication:
- Inner product:
- Norm (length):

$$+ (\mathbf{w} :: \mathbb{C}^n, \mathbf{z} :: \mathbb{C}^n) :: \mathbb{C}^n$$

$$0_{\mathbb{C}^n} := (0, \dots, 0)$$

$$- (\mathbf{w} :: \mathbb{C}^n, \mathbf{z} :: \mathbb{C}^n) :: \mathbb{C}^n$$

$$- (\mathbf{w} :: \mathbb{C}^n) :: \mathbb{C}^n$$

$$* (\alpha :: \mathbb{C}, \mathbf{z} :: \mathbb{C}^n) :: \mathbb{C}^n$$

$$(\mathbf{w} :: \mathbb{C}^n \mid \mathbf{z} :: \mathbb{C}^n) :: \mathbb{C}$$

$$\mathbf{norm}(\mathbf{z} :: \mathbb{C}^n) :: \mathbb{R} \quad \text{math notation: } \|z\|_8$$

Example #1: \mathbb{C}^n

Schaum 1.8

$$w = (w_1, \dots, w_n) \in \mathbb{C}^n, \quad z = (z_1, \dots, z_n) \in \mathbb{C}^n, \quad \alpha \in \mathbb{C}$$

$$w + z := (w_1 + z_1, \dots, w_n + z_n)$$

$$w - z := (w_1 - z_1, \dots, w_n - z_n)$$

$$-z := (-z_1, \dots, -z_n)$$

$$\alpha \cdot z := (\alpha \cdot z_1, \dots, \alpha \cdot z_n)$$

$$(w|z) := w_1^* \cdot z_1 + \dots + w_n^* \cdot z_n$$

$$\|z\| := \sqrt{(z|z)}$$

Rules & Laws

1. Vector addition is...

- associative & commutative
- zero works, additive inverse/subtraction work

2. Scalar-multiplication is...

- associative: $\forall \alpha, \beta \in \mathbb{C} \forall z \in \mathbb{C}^n: (\alpha \cdot \beta) \cdot z = \alpha \cdot (\beta \cdot z)$
- distributive over vector addition: $\forall \alpha \in \mathbb{C} \forall w, z \in \mathbb{C}^n: \alpha \cdot (w + z) = \alpha \cdot w + \alpha \cdot z$
- distributive over scalar addition: $\forall \alpha, \beta \in \mathbb{C} \forall z \in \mathbb{C}^n: (\alpha + \beta) \cdot z = \alpha \cdot z + \beta \cdot z$
- Don't Bullshit-Me Rule: $1 \cdot z = z$

3. Inner product is...

- \mathbb{C} -linear in the left side: $\forall z: w \mapsto (w|z)$ anti- \mathbb{C} -linear
- \mathbb{C} -linear in the right side $\forall w: z \mapsto (w|z)$ \mathbb{C} -linear
- anti-symmetric: $\forall w, z: (w|z) = (z|w)^*$
- positive: $\forall z \neq 0_{\mathbb{C}^n}: (z|z) > 0.$

Hilbert Space

Definition.

A (complex) Hilbert space is a set ("type") for which the operations

- *vector addition (w/ zero, subtraction, unary minus etc)*
- *scalar multiplication with elements of \mathbb{C}*
- *inner product*

are defined and satisfy the laws.

Notes

- inner product is *conjugate-symmetric* and *"sesqui"-linear*
- $\text{norm}(z) = \|z\| := \sqrt{(z|z)}$ — no need to mention it

Consequences of the Rules & Laws

Theorem (Cauchy-Schwarz).

For all x, y we have $|(x \mid y)| \leq \|x\| \cdot \|y\|$.

Equality holds if, and only if, x, y are collinear

(i.e., there exist $\alpha, \beta \in \mathbb{C}$, at least one of them non-zero, with $\alpha x = \beta y$).

Theorem (Properties of a "Norm").

1. Triangle leq: For all x, y we have $\|x + y\| \leq \|x\| + \|y\|$.
2. Positive homogeneous: For all x , if $\alpha \in \mathbb{C}$, we have $\|\alpha \cdot x\| = |\alpha| \cdot \|x\|$.
3. Separation: For all x , if $\|x\| = 0$, then $x = 0$.

WARNING

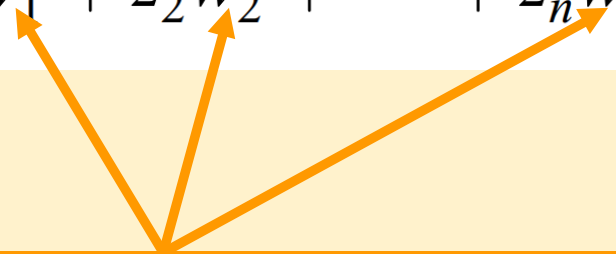
Between math & physics int the \mathbb{C} inner product left and right side are exchanged.

We follow the physics way because that's used in quantum CS.

Schaum 1.8:

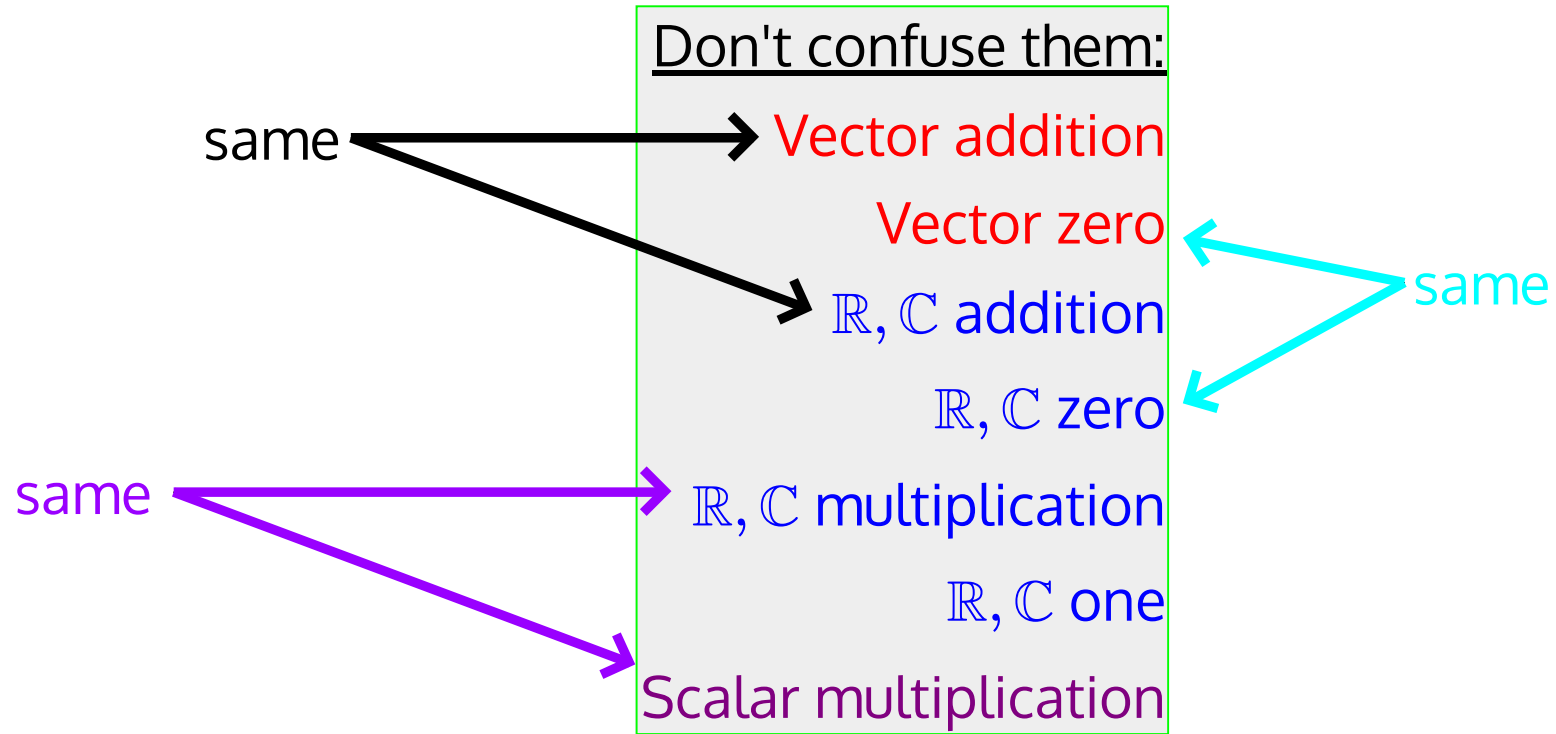
Dot (Inner) Product in \mathbb{C}^n

Consider vectors $u = [z_1, z_2, \dots, z_n]$ and $v = [w_1, w_2, \dots]$ denoted and defined by

$$u \cdot v = z_1 \bar{w}_1 + z_2 \bar{w}_2 + \dots + z_n \bar{w}_n$$


Complex conjugation (overline in Schaum) **should**
be on the left argument z , not w .

Symbols



Some more examples: real HS \mathbb{R} , complex HS \mathbb{C}

- Q:
Is $\mathbb{R}^1 = \mathbb{R}$?
Is $\mathbb{C}^1 = \mathbb{C}$?

- A: Definitely no!
Why?
Take, e.g., Julia



- A: Definitely yes!
Why?
There's an obvious way to convert elements of one into the other and back, and the conversion is compatible with all operations ("isomorphism").

```
julia> x = (3.2,)
(3.2,)
```

```
julia> typeof(x)
Tuple{Float64}
```

```
julia> y = 3.2
3.2
```

```
julia> typeof(y)
Float64
```

```
julia> x == y
false
```


Some more examples: real HS \mathbb{C}

Real Hilbert space:

Set: \mathbb{C}

Operations:

- Vector addition, subtraction, zero:
the usual operations in \mathbb{C}
- Scalar multiplication:
the usual way of multiplying real numbers to complex numbers
 - by considering the real numbers as complex numbers (math speak)
 - by converting the real numbers to complex numbers first (CS speak)
- (Symmetric, bi-linear) inner product: $\langle w, z \rangle := \Re(w^* z)$ (as in homework)

Subspaces

Schaum's 4.4 - 4.6

Subspace — Definition

Replace $\mathbb{K} := \mathbb{R}$ or $\mathbb{K} := \mathbb{C}$

Let V be a Hilbert space, and $U \subseteq V$.

U is called *subspace* of V if U if

- $U \neq \emptyset$
- $\forall u_1, u_2 \in U, \forall \alpha_1, \alpha_2 \in \mathbb{K}: \alpha_1 u_1 + \alpha_2 u_2 \in U$

- 
1. $\forall \alpha \in \mathbb{K}, u \in U: \alpha \cdot u \in U$
 2. $\forall u_1, u_2 \in U: u_1 + u_2 \in U$

That's the same as saying:

- With the same operations, U itself is a Hilbert space

Examples:

Subspaces of the complex Hilbert Space \mathbb{C}^n

1. $\{0\} \subseteq \mathbb{C}^n$
2. $\mathbb{C}^n \subseteq \mathbb{C}^n$
3. $\mathbb{R} \subset \mathbb{C}$
4. $\{z \in \mathbb{C}^n \mid z_1 = 0\} \subseteq \mathbb{C}^n$
5. $\{z \in \mathbb{C}^n \mid z_1 = 1\} \subseteq \mathbb{C}^n$
6. Fix $a \in \mathbb{C}^n$. $\{z \in \mathbb{C}^n \mid \sum_{j=1}^n a_j z_j = 0\} \subseteq \mathbb{C}^n$
7. Fix $a \in \mathbb{C}^n$. $\{z \in \mathbb{C}^n \mid \sum_{j=1}^n a_j z_j = 1\} \subseteq \mathbb{C}^n$
8. Fix $A \in \mathbb{M}_C(m \times n)$. $\{z \in \mathbb{C}^n \mid Az = 0_{\mathbb{C}^m}\} \subseteq \mathbb{C}^n$

Yes: 1,2,4,6,8; No: 3,5,7

Matrix-vector multiplication

$$A = (A_{k,\ell})_{k=1:m,\ell=1:n} \in \mathbb{M}(m \times n)$$

$$x = (x_\ell)_{\ell=1:n}$$

$$(y_k)_{k=1:m} = y := A \cdot x$$

$$y_k = \sum_{\ell=1}^n A_{k,\ell} x_\ell$$

Subspaces through linear mappings

Fix $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$.

Suppose V, W are \mathbb{K} Hilbert spaces ($V = W$ is, of course, allowed)

A mapping (aka function) $f: V_1 \rightarrow V_2$ is called \mathbb{K} -linear if

1. $\forall \alpha \in \mathbb{K}, x \in V: \quad f(\alpha x) = \alpha f(x)$
2. $\forall x_1, x_2 \in V: \quad f(x_1 + x_2) = f(x_1) + f(x_2)$

$$\begin{aligned} &\forall \alpha_1, \alpha_2 \in \mathbb{K}, \forall x_1, x_2 \in V: \\ &f(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 f(x_1) + \alpha_2 f(x_2) \end{aligned}$$

Lemma.

If $f: V_1 \rightarrow V_2$ is a linear mapping, then the set

$$\text{Ker } f := \{x_1 \in V_1 \mid f(x_1) = 0\}$$

is a subspace of V_1 .

Fancy names

In proper math-speak:

- A "**function**" takes values in the real or complex numbers, ...
- ... everything else is a "**mapping**"

For us in this course, we follow the computer science language:

- "Function" = "mapping"

In Hilbert space language:

- "**Operator**" = "linear mapping/function between Hilbert spaces"

#MrsMaisel

Span

Fix $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$; let V be a \mathbb{K} Hilbert space.

We define the **Span** operation:

Input: Subset X of V

Output: Set of all "linear combinations" of elements of X :

$$\text{Span}(X) := \left\{ \sum_{j=1}^m \alpha_j x_j \mid m \in \mathbb{Z}_+, \alpha_1, \dots, \alpha_m \in \mathbb{K}, x_1, \dots, x_m \in X \right\}$$

Lemma. *For every \mathbb{K}, V, X : $\text{Span}(X)$ is a subspace of V .*

Span

1. $\text{Span}(\emptyset) = ??$
2. $\text{Span}(\{0\}) = ??$
3. $\text{Span}(\{x\}) = ??$
4. $\text{Span}(V) = ??$
5. If U is a subspace of V : $\text{Span}(U) = ??$
6. $\text{Span}(\text{Span}(X)) = ??$

Orthogonality & Bases

Schaum's sections 7.5 - 7.7

Orthogonality

1. Two vectors x, y are called *orthogonal* if
 - real Hilbert space: $\langle x, y \rangle = 0$
 - complex Hilbert space: $(x | y) = 0$.
2. Two subspaces U, V of a real/complex Hilbert space \mathcal{H} are called *orthogonal*, if $\forall u \in U \forall v \in V: u, v$ are orthogonal.
3. A set of vectors X is called an *orthogonal system*, if $\forall x, y \in X$ with $x \neq y$: x, y are orthogonal. (The phrase " x_1, \dots, x_d is an orthonormal system" means that (a) the x_i 's are all distinct, and (b) $\{x_1, \dots, x_d\}$ is an orthonormal system.)
4. A set of vectors X is called an *orthonormal system*, if it's an orthogonal system, and every $x \in X$ has norm 1: $\|x\| = 1$.

Orthogonality sanity check

1. If x is orthogonal to y , does that imply that y is orthogonal to x ???
2. Which vector(s) are orthogonal to the zero-vector?
3. Is there any vector that is are orthogonal to itself?
4. Are these two orthogonal? $(i - 1, i, i + 1), (\sqrt{2}e^{i\pi/4}, -1, 3e^{-i\pi/4}/2)$

Useful!!!

Lemma.

Let \mathcal{H} be a (real or complex) Hilbert space.

1. For all $\psi \in \mathcal{H}$:

$\psi = 0$ if and only if $\forall \phi \in \mathcal{H}: (\phi \mid \psi) = 0$.

2. For all $\psi_1, \psi_2 \in \mathcal{H}$:

$\psi_1 = \psi_2$ if and only if $\forall \phi \in \mathcal{H}: (\phi \mid \psi_1) = (\phi \mid \psi_2)$.

P.S.: For real HS, replace $(\cdot \mid \cdot)$ by $\langle \cdot, \cdot \rangle$

Proof. (2) (using (1)). Take ψ_1, ψ_2 , and set $\psi := \psi_1 - \psi_2$. Then $\psi_1 = \psi_2$ iff $\psi = 0$. By (1) this is equivalent to $\forall \phi \in \mathcal{H} \ 0 = (\phi \mid \psi) = (\phi \mid \psi_1 - \psi_2) = (\phi \mid \psi_1) - (\phi \mid \psi_2)$ iff $\forall \phi \in \mathcal{H} \ (\phi \mid \psi_1) = (\phi \mid \psi_2)$.

Fundamental fact

Theorem.

Let x_1, \dots, x_d be an orthonormal system and $y \in \text{Span}(X)$.

1. Whenever $y = \sum_j \alpha_j x_j$ then for all j : $\alpha_j = (x_j \mid y)$.

2. $y = \sum_j x_j \cdot (x_j \mid y)$

Consequence: If $\sum_j \alpha_j x_j = 0$ then, for all j , $\alpha_j = 0$.

ONB (Orthonormal Basis)

If X is an orthonormal system, and $\text{Span}(X) = \mathcal{H}$, then X is called an *orthonormal basis* of \mathcal{H} .

The *dimension* of \mathcal{H} is the number of elements in an ONB.

For this to make sense, we need the following fact:

If X, Y are orthonormal systems with $\text{Span}(X) = \text{Span}(Y)$, then $|X| = |Y|$.

We will prove that using matrices in the chapter 5.

Every orthonormal system is an ONB of its span.

Gram-Schmidt Orthogonalization

You have:

- List of vectors x_1, x_2, \dots, x_m

You want:

- ONB of $\text{Span}(\{x_1, \dots, x_m\})$

Lemma.

*Every time a mark is passed,
the following holds:*

- Y is an orthonormal system
- $\text{Span}(Y) = \text{Span}(\{x_1, \dots, x_j\})$

Gram-Schmidt Algorithm

```
Y := ∅
j=0
# mark
while j < m
  j += 1
  y := xj
  for v in Y
    y -= v • (v | xj)
  end
  if y ≠ 0
    y /= ||y||
    insert y into Y
  end
  # mark
end
return Y
```


Least-squares approximation

A closer look at the basic step

x is replaced by:

- $x - Px$
- with $Px := \sum_{v \in Y} v \cdot (v \mid x)$

The mapping $x \mapsto Px$

- ... is linear
- ... gives the best approximation of x in $U := \text{Span}(Y)$, i.e., the point in U with smallest distance from x

Px is the "least-squares approximation" of x .

Gram-Schmidt Algorithm

```
Y := ∅
j=0
# mark
while j < m
  j += 1
  y := xj
  for v in Y
    y -= v · (v | xj)
  end
  if y ≠ 0
    y /= ||y||
    insert y into Y
  end
# mark
end
return Y
```

Inner products & norms in different bases

Fact.

Let b_1, \dots, b_d be an ONS with span U , and let

- $x = \sum_{j=1}^d \alpha_j b_j \ (\in U),$
- $y = \sum_{j=1}^d \beta_j b_j \ (\in U).$

Then

$$(x \mid y) = \sum_{j=1}^d \alpha_j^* \beta_j$$

and

$$\|x\|^2 = \sum_{j=1}^d |\alpha_j|^2$$

Tensor Products of Hilbert Spaces

One reason for learning Hilbert space shit is because of the first Postulate of quantum mechanics:

For every closed quantum system, there is a (complex) Hilbert space \mathcal{H} such that the states that the quantum system can be in correspond to norm-1 vectors in \mathcal{H} .

Schrödinger's pets



Schrödinger's pets

Schrödinger's cat (in a quantum box)
can be in the following states:

1. Dead ψ_{dead}
2. Alive ψ_{alive}

Physicists tell us that, as these two states can be measured with a single measurement, the two vectors must be orthogonal, i.e., form an ONS.

3. Any superposition $\alpha\psi_{\text{dead}} + \beta\psi_{\text{alive}}$ (with $|\alpha|^2 + |\beta|^2 = 1$) of the two.

→ 2-dim Hilbert space \mathcal{H}_{cat}

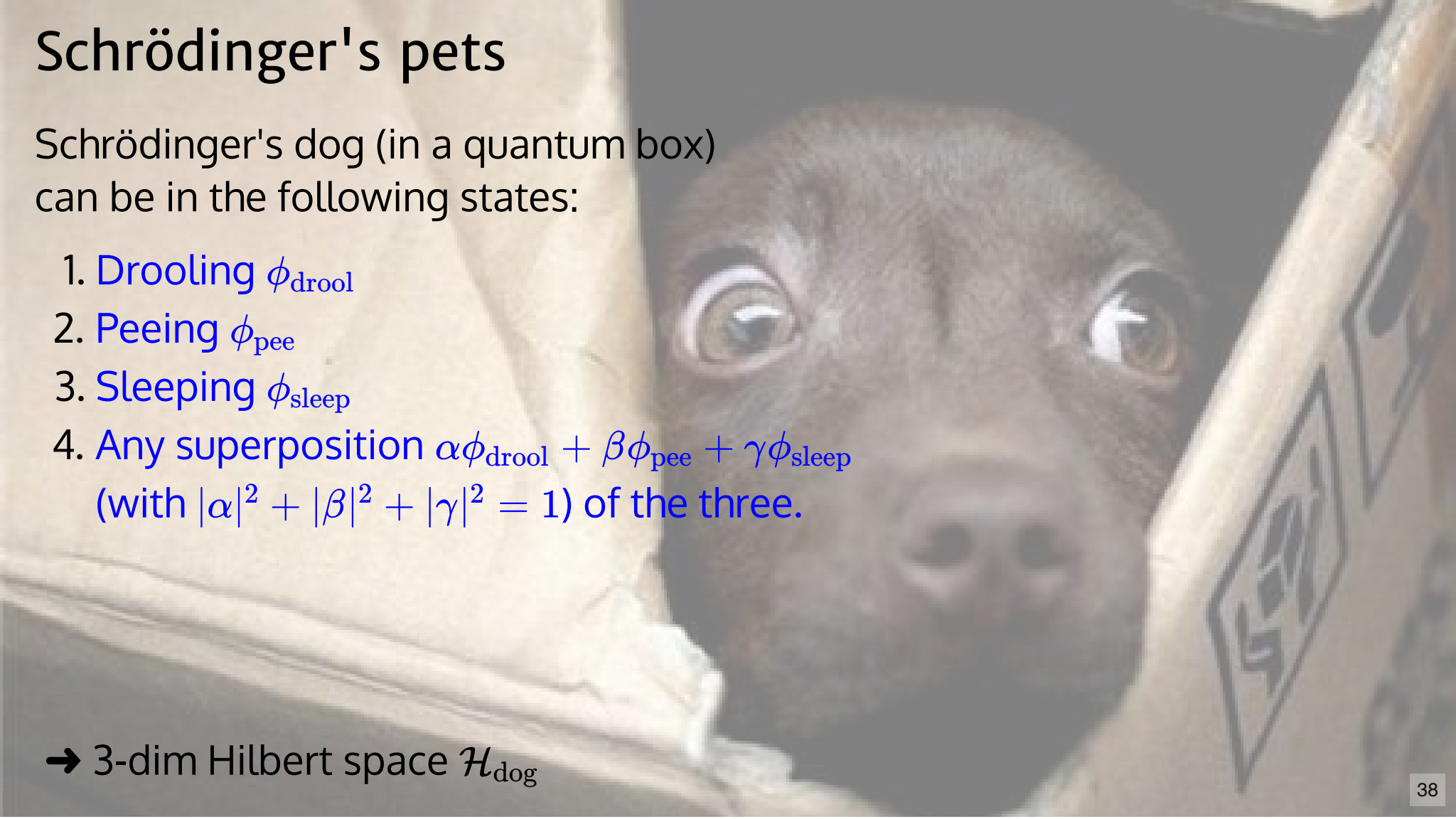
Physics word for linear combination.

Schrödinger's pets

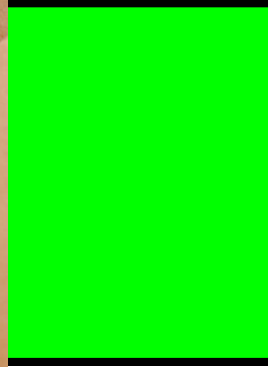
Schrödinger's dog (in a quantum box) can be in the following states:

1. Drooling ϕ_{drool}
2. Peeing ϕ_{pee}
3. Sleeping ϕ_{sleep}
4. Any superposition $\alpha\phi_{\text{drool}} + \beta\phi_{\text{pee}} + \gamma\phi_{\text{sleep}}$
(with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$) of the three.

→ 3-dim Hilbert space \mathcal{H}_{dog}



Schrödinger's pets



The cat and the dog are two separate quantum systems — each with its own Hilbert space. By default, both systems are "closed", i.e., they don't interact with each other (and with nothing else). But we may want to couple them somehow, and consider them together as one bigger system.

What's the Hilbert space of the combined system?

Schrödinger's pets

The combined system can be in the states:

- | | |
|----------------------------|---|
| 1. cat dead, dog drooling | $\psi_{\text{dead}} \otimes \phi_{\text{drool}}$ |
| 2. cat dead, dog peeing | $\psi_{\text{dead}} \otimes \phi_{\text{pee}}$ |
| 3. cat dead, dog sleeping | $\psi_{\text{dead}} \otimes \phi_{\text{sleep}}$ |
| 4. cat alive, dog drooling | $\psi_{\text{alive}} \otimes \phi_{\text{drool}}$ |
| 5. cat alive, dog peeing | $\psi_{\text{alive}} \otimes \phi_{\text{pee}}$ |
| 6. cat alive, dog sleeping | $\psi_{\text{alive}} \otimes \phi_{\text{sleep}}$ |

What about
superpositions?!?

The " \otimes " (tensor product) is a new type of operation, very much like " $*$ " (multiplication), but unlike multiplication, *it is almost always easier to just leave the symbol there* instead of "computing the result".

Schrödinger's pets

Superpositions:

$$\alpha \cdot (\psi_{\text{dead}} \otimes \phi_{\text{drool}}) + \beta \cdot (\psi_{\text{dead}} \otimes \phi_{\text{pee}}) + \gamma \cdot (\psi_{\text{dead}} \otimes \phi_{\text{sleep}}) + \delta \cdot (\psi_{\text{alive}} \otimes \phi_{\text{drool}}) + \epsilon \cdot (\psi_{\text{alive}} \otimes \phi_{\text{pee}}) + \zeta \cdot (\psi_{\text{alive}} \otimes \phi_{\text{sleep}})$$

These (with arbitrary $\alpha, \beta, \gamma, \delta, \epsilon, \zeta \in \mathbb{C}$) are the elements of the Hilbert space that is the "tensor product" of \mathcal{H}_{cat} and \mathcal{H}_{dog}

Confusion warning:

- Tensor product of vectors
- Tensor product of spaces

Definition of tensor product of 2 Hilbert spaces

Definition. Let $\mathcal{H}_1, \mathcal{H}_2$ be \mathbb{K} Hilbert spaces. Their "tensor product" is a \mathbb{K} Hilbert space

- whose elements are $\sum_{j=1}^m \alpha_j \cdot (\psi_j^1 \otimes \psi_j^2)$,
for arbitrary $m \in \mathbb{Z}_+$, $\psi_1^1, \dots, \psi_m^1 \in \mathcal{H}_1$, $\psi_1^2, \dots, \psi_m^2 \in \mathcal{H}_2$, $\alpha_1, \dots, \alpha_m \in \mathbb{K}$
- satisfying the following laws that we know from $*$:
 1. \otimes is bi- \mathbb{K} -linear:
 - $(\alpha\phi^1 + \beta\psi^1) \otimes \phi^2 = \alpha \cdot (\phi^1 \otimes \phi^2) + \beta \cdot (\psi^1 \otimes \phi^2)$
 - $\phi^1 \otimes (\alpha\phi^2 + \beta\psi^2) = \alpha \cdot (\phi^1 \otimes \phi^2) + \beta \cdot (\phi^1 \otimes \psi^2)$
 2. Inner product: $(\phi^1 \otimes \phi^2 \mid \psi^1 \otimes \psi^2) = (\phi^1 \mid \psi^1) \cdot (\phi^2 \mid \psi^2)$

For vector arithmetic:

the \otimes -operator behaves exactly
like multiplication, except:

the left box contains the cat, the right box contains
the dog — so in $\psi \otimes \phi$, you cannot exchange ψ and ϕ ,
because ψ contains information about the cat and ϕ
contains information about the dog.

Definition of tensor product of n Hilbert spaces

Definition. Let $\mathcal{H}_j, j = 1, \dots, r$ be \mathbb{K} Hilbert spaces. Their "tensor product" is a \mathbb{K} Hilbert space

- whose elements are $\sum_{j=1}^m \alpha_j \cdot (\psi_j^1 \otimes \dots \otimes \psi_j^r),$
for arbitrary $m \in \mathbb{Z}_+, \psi_1^1, \dots, \psi_m^1 \in \mathcal{H}_1, \dots, \psi_1^r, \dots, \psi_m^r \in \mathcal{H}_r, \alpha_1, \dots, \alpha_m \in \mathbb{K}$
- satisfying the following laws that we know from $*$:
 1. \otimes is r - \mathbb{K} -linear:
 - $(\alpha\phi^1 + \beta\psi^1) \otimes \phi^2 \otimes \dots \otimes \phi^r = \alpha \cdot (\phi^1 \otimes \phi^2 \otimes \dots \otimes \phi^r) + \beta \cdot (\psi^1 \otimes \phi^2 \otimes \dots \otimes \phi^r)$
 - ...
 - $\phi^1 \otimes \dots \otimes \phi^{r-1} \otimes (\alpha\phi^r + \beta\psi^r) = \alpha \cdot (\phi^1 \otimes \dots \otimes \phi^{r-1} \otimes \phi^r) + \beta \cdot (\phi^1 \otimes \dots \otimes \psi^{r-1} \otimes \psi^r)$
 2. Inner product: $(\phi^1 \otimes \dots \otimes \phi^r \mid \psi^1 \otimes \dots \otimes \psi^r) = \prod_{j=1}^r (\phi^j \mid \psi^j)$

For vector arithmetic:

the \otimes -operator behaves exactly
like multiplication, except:

in $\psi^1 \otimes \psi^2 \otimes \dots \otimes \psi^r$, the ψ^j is information about the
 j th quantum system, so cannot reorder the ψ^* 's.

Back to cats & dogs: ONBs of tensor products

Proposition.

Let $\mathcal{H}_1, \dots, \mathcal{H}_r$ be \mathbb{K} -Hilbert spaces, and for $j = 1, \dots, r$, let $b_1^j, \dots, b_{d_j}^j$ be an ONB of \mathcal{H}_j . Then the following is an ONB of their tensor product:

$$b_{k_1}^1 \otimes \dots \otimes b_{k_r}^r \text{ for } k \in \prod_{j=1}^r \{1, \dots, d_j\}$$

Notation

1. $\psi_1 \in \mathcal{H}_1, \dots, \psi_r \in \mathcal{H}_r$ vectors $\rightarrow \psi_1 \otimes \dots \otimes \psi_r$ a vector
2. $\mathcal{H}_1, \dots, \mathcal{H}_r$ \mathbb{K} -Hilbert spaces $\rightarrow "$ $\mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_r$ " a \mathbb{K} -Hilbert space
3. $"\mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_r" = \text{Span}(\{\psi_1 \otimes \dots \otimes \psi_r \mid \psi_1 \in \mathcal{H}_1, \dots, \psi_r \in \mathcal{H}_r\})$

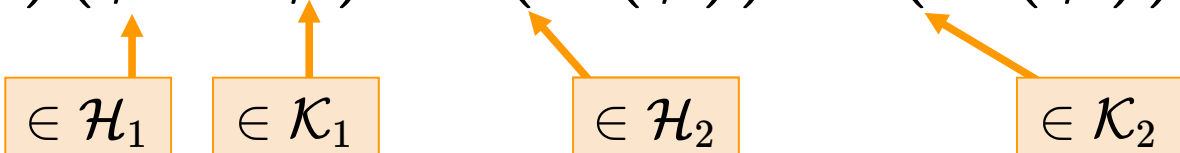
Tensor products of linear operators

We already know what a linear operator (mapping, function) is, but we don't yet have the concept of how the linear operators are *vectors*, i.e., elements of some kind of Hilbert space.

But we treat tensor products of linear operators here anyway.

Let $A: \mathcal{H}_1 \rightarrow \mathcal{H}_2$ and $B: \mathcal{K}_1 \rightarrow \mathcal{K}_2$ be linear operators.

The "vector" (explanation later) $A \otimes B$ can be understood as a linear operator $\mathcal{H}_1 \otimes \mathcal{K}_2 \rightarrow \mathcal{H}_2 \otimes \mathcal{K}_2$ which does this:

$$(A \otimes B)(\phi \otimes \psi) = (A(\phi)) \otimes (B(\psi))$$


$\in \mathcal{H}_1$ $\in \mathcal{K}_1$ $\in \mathcal{H}_2$ $\in \mathcal{K}_2$

Linear operators away from tensor products

Take \mathbb{K} -Hilbert spaces $\mathcal{H}_1, \dots, \mathcal{H}_r$, and consider $\mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_r$. Let \mathcal{G} be a second \mathbb{K} -Hilbert space. There is a simple & convenient way of defining linear operators

$$T: \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_r \rightarrow \mathcal{G}$$

Universal Property.

Let f be a function that takes r arguments of types $\mathcal{H}_1, \dots, \mathcal{H}_r$ and returns values in \mathcal{G} .

If f is r -multi \mathbb{K} -linear, then the following defines a \mathbb{K} -linear mapping $\mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_r \rightarrow \mathcal{G}$:

$$T_f(\psi_1 \otimes \dots \otimes \psi_r) := f(\psi_1, \dots, \psi_r)$$

To apply T_f to linear combinations of elementary tensors, just use the fact that T_f is \mathbb{K} -linear.

Linear operators away from tensor products

Why does f need to be multi-linear?

$$\begin{aligned} & f(\psi_1, \dots, \psi_{j-1}, \alpha\phi_j + \beta\psi_j, \psi_{j+1}, \dots, \psi_r) \\ &= T_f(\psi_1 \otimes \dots \otimes \psi_{j-1} \otimes (\alpha\phi_j + \beta\psi_j) \otimes \psi_{j+1} \otimes \dots \otimes \psi_r) \\ &= T_f\left(\alpha \cdot \psi_1 \otimes \dots \otimes \psi_{j-1} \otimes \phi_j \otimes \psi_{j+1} \otimes \dots \otimes \psi_r \right. \\ &\quad \left. + \beta \cdot \psi_1 \otimes \dots \otimes \psi_{j-1} \otimes \psi_j \otimes \psi_{j+1} \otimes \dots \otimes \psi_r\right) \\ &= \alpha \cdot T_f(\psi_1 \otimes \dots \otimes \psi_{j-1} \otimes \phi_j \otimes \psi_{j+1} \otimes \dots \otimes \psi_r) \\ &\quad + \beta \cdot T_f(\psi_1 \otimes \dots \otimes \psi_{j-1} \otimes \psi_j \otimes \psi_{j+1} \otimes \dots \otimes \psi_r) \\ &= \alpha \cdot f(\psi_1, \dots, \psi_{j-1}, \phi_j, \psi_{j+1}, \dots, \psi_r) \\ &\quad + \beta \cdot f(\psi_1, \dots, \psi_{j-1}, \psi_j, \psi_{j+1}, \dots, \psi_r) \end{aligned}$$

Hilbert space: ☒

