MTAT.07.024

Quantum Crypto

Lecture #0a

Hilbert Space Basics

Example #1: $\mathbb{C}^n$

Set:

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

Operations:

`typedef` $\mathbb{C}$`<<42>>` $\mathscr{H}$`;`

- Vector addition: $\mathscr{H}$ `operator +(`$\mathscr{H}$ ϕ`,` $\mathscr{H}$ ψ`);`
- Zero vector: $0_{\mathbb{C}^n} := (0, \ldots, 0)$
- Vector subtraction & additive inverses:
  binary minus-operator: $\mathscr{H}$ `operator -(`$\mathscr{H}$ ψ`);`
  unary minus-operator: $\mathscr{H}$ `operator +(`$\mathscr{H}$ ϕ`,` $\mathscr{H}$ ψ`);`
- Scalar multiplication: $\mathscr{H}$ `operator *(`$\mathbb{C}$ α`,` $\mathscr{H}$ ψ`);`
- Inner product: `complex operator |(`$\mathscr{H}$ ϕ`,` $\mathscr{H}$ ψ`);`
- Norm (length, ||…||): `double norm(`$\mathscr{H}$ ϕ`);`

Example #1: $\mathbb{C}^n$

Schaum 1.8

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

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

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

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

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

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

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

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...
   - $\mathbb{C}$-anti-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*
- $\mathtt{norm}(z) = \|z\| := \sqrt{(z|z)}$ — 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, in 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 $\mathbf{C}^n$

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

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

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

Symbols

same

Don't confuse them:

Vector addition

Vector zero

same

$\mathbb{C}$ addition

$\mathbb{C}$ zero

same

$\mathbb{C}$ multiplication

$\mathbb{C}$ one

Scalar multiplication

Matrix-vector multiplication

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

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

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

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

Linear mappings

Suppose V, W are Hilbert spaces ($V = W$ is, of course, allowed)

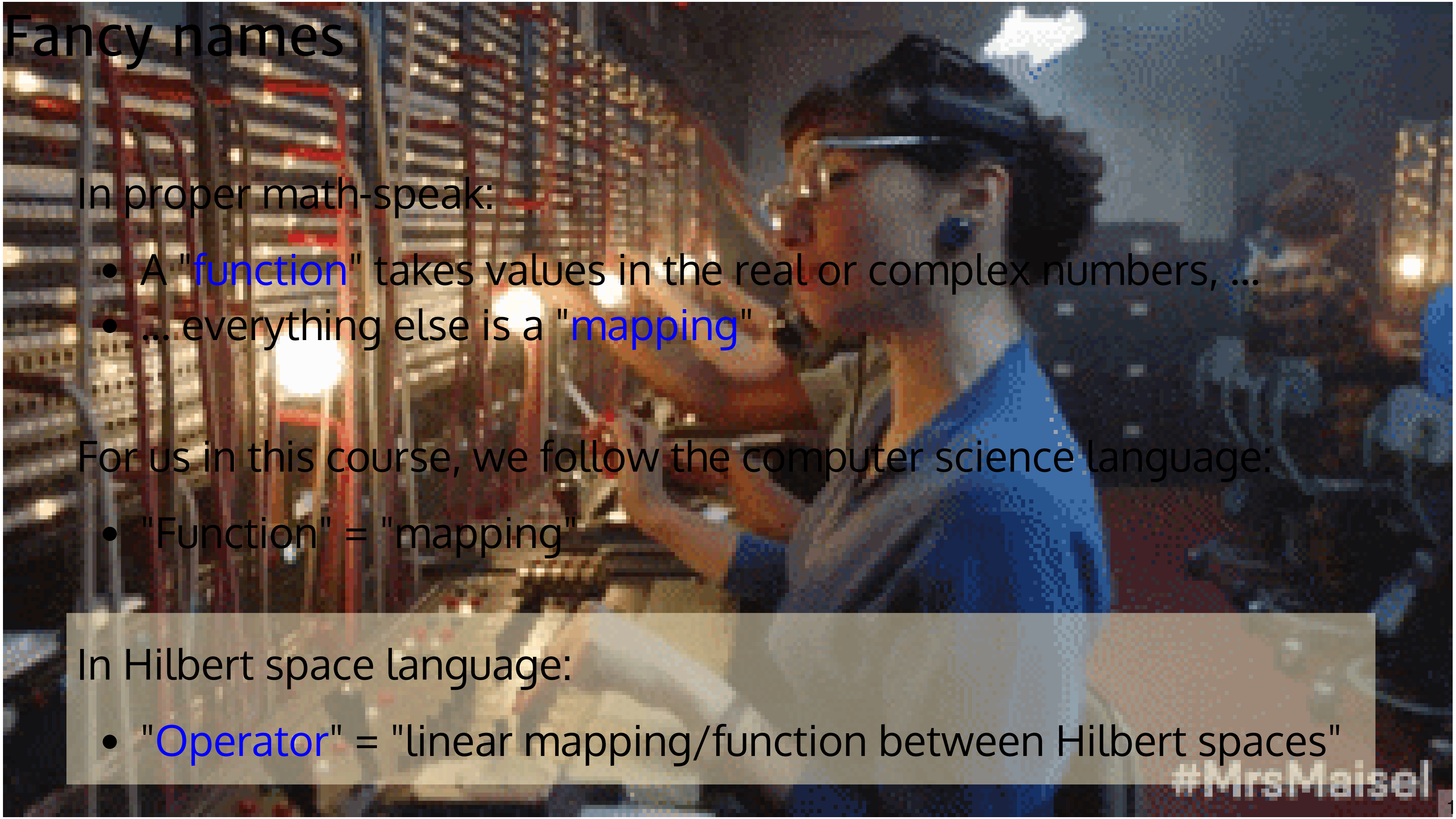
A mapping (aka function) $f: V \to W$ is called *linear* if

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

$\forall \alpha_1, \alpha_2 \in \mathbb{C}, \forall x_1, x_2 \in V:$

$f(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 f(x_1) + \alpha_2 f(x_2)$

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"

Span

Let V be a Hilbert space.

We define the $\texttt{Span}$ operation:

Input: Subset X of V

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

$$\texttt{Span}(X) := \left\{ \sum_{j=1}^{m} \alpha_j x_j \;\middle|\; m \in \mathbb{Z}_+,\ \alpha_1, \ldots, \alpha_m \in \mathbb{C},\ x_1, \ldots, x_m \in X \right\}$$

Facts. (Check them!!)

- $\texttt{Span}(X) \subseteq V$
- $X \subseteq \texttt{Span}(X)$
- *If* $X \subseteq Y$ *then* $\texttt{Span}(X) \subseteq \texttt{Span}(Y)$

Quiz

1. $\texttt{Span}(\emptyset) = ??$
2. $\texttt{Span}(\{0\}) = ??$
3. $\texttt{Span}(\{x\}) = ??$
4. $\texttt{Span}(V) = ??$
5. $\texttt{Span}(\texttt{Span}(X)) = ??$

Orthogonality & Bases

Schaum's sections 7.5 - 7.7

Orthogonality

1. Two vectors x, y are called *orthogonal* if $(x \mid y) = 0$.

2. Two subspaces U, V of a 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 "$x_1, \ldots, x_d$ is an orthonormal system" means that (a) the $x_\cdot$'s are all distinct, and (b) $\{x_1, \ldots, x_d\}$ is an orthonormal system.)

4. A set of vectors X is called an *ortho<u>normal</u> 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? $(i-1, i, i+1)$, $(\sqrt{2}e^{i\pi/4}, -1, 3e^{-i\pi/4}/2)$

Fundamental fact

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

1. *Whenever $y = \sum_j \alpha_j x_j$ then for all j:* $\quad \alpha_j = (x_j \mid y)$.
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 $\mathtt{Span}(X) = \mathcal{H}$, 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 $\mathtt{Span}(X) = \mathtt{Span}(Y)$, then $|X| = |Y|$.

We will not prove that.

Every orthonormal system is an ONB of its span.

Inner products & norms in different bases

Fact.

Let $b_1, \ldots, b_d$ 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

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

Hilbert space: ☑

Show that the vectors $u=(1,1,0)$, $v=(1,3,2)$, $w=(4,9,5)$ are linearly dependent or independent.

Show that the vectors $u=(1,2,3)$, $v=(2,5,7)$, $w=(1,3,5)$ are linearly dependent or independent.

Suppose z=2+3i, w=5−2i)

Calculate the absolute value of the complex numbers.

Suppose u=[2+3i, 4−i, 5−2i), v=[3−4i, 5i, 4−2i]

Calculate the norm of the vectors.