Overview of Math Facts & Notations for MTAT.05.118
Quantum Computing I

Assoc. Prof. Dirk Oliver Theis

Version: Fri Dec 20 09:52:14 EET 2019
Compiled: 10:42

1 Why?

This document summarizes the mathematics that’s needed to do quantum computing. The ideal student would only briefly read over it, and remember the properties from her/his linear algebra course. Unfortunately, the ideal student died in an accident in 1973 (car crash — very tragic). All other students should read this document carefully, memorize it, then eat it, for better ingestion.

1.1 References

This document is not meant for learning the topics, but as a reference. If you need a little more time to remember your Linear Algebra, I recommend to do it right away in the context of quantum computing. Here are two textbook chapters easily accessible from the library.

WARNING!! Reading the following chapters may bore you to death!

- Chapter 2 in:
  Kaye, Laflamme, and Mosca, “An Introduction to Quantum Computing”

- Section 2.1 in:
  Nielsen and Cuang, “Quantum Computation and Quantum Information”

The first book (KLM) will be our standard reference for (most of) the quantum algorithms that are discussed in the course.

- If your Linear Algebra course was . . . somehow different, and the stuff below doesn’t make much sense to you: read the Chapter 2 of KLM by Wednesday, and forget about this document.

- If you’re a physicist and have taken a quantum physics course, don’t worry about the math.
2 Notation, terminology, and review of some basic definitions

<table>
<thead>
<tr>
<th>Math Notation</th>
<th>Physics Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complex numbers</td>
<td>$\mathbb{C}$</td>
</tr>
<tr>
<td>Complex conjugate</td>
<td>$\bar{z}$ (won’t be used)</td>
</tr>
<tr>
<td>Hilbert spaces</td>
<td>$H, A, B$</td>
</tr>
<tr>
<td>Vectors</td>
<td>$\psi, \phi, \varphi, \ldots$</td>
</tr>
<tr>
<td>Inner product</td>
<td>(no particular notation)</td>
</tr>
<tr>
<td>Apply operator</td>
<td>$A\psi, B\phi$</td>
</tr>
<tr>
<td>Adjoint operator</td>
<td>$A^\dagger$ (won’t be used) or $A^*$</td>
</tr>
</tbody>
</table>

Note that even in math notation, the inner product is linear in the right argument, and anti-linear in the left one.
We will happily mix math notation and physics notation.

2.1 Some terminology and definitions

From now on, when we say “operator” we mean operator on a Hilbert space which is (unless otherwise stated) finite dimensional.

(Boring, I know. But we want to focus on quantum algorithms.)

1.) $[A, B] := AB - BA$, the commutator.
2.) Operators $A, B$ commute if $[A, B] = 0$.
3.) An operator $A$ is called normal, if it commutes with its adjoint.
4.) An operator $A$ is called self-adjoint or Hermitian, if $A^\dagger = A$.

ONB Orthonormal basis

3 Spectral theorem

We say that a set $\mathcal{A}$ of operators $*$-commutes, if for each $A, B \in \mathcal{A}$, we have $AB = BA$ and $AB^\dagger = B^\dagger A$.

3.1 The spectral theorem, ONB version

Theorem 1. Let $\mathcal{A}$ be a set of operators on a Hilbert space $\mathcal{H}$. The following statements are equivalent.

(a) $\mathcal{A}$ $*$-commutes.
(b) There exists an ONB of $\mathcal{H}$ each of whose elements is an eigenvector for each of the operators in $\mathcal{A}$. I.e., there exists an ONB $(|j\rangle)_{j=1,2,3,\ldots}$ of $\mathcal{H}$, such that for every $A, j$ there is a $\lambda_{A,j} \in \mathbb{C}$ with $A|j\rangle = \lambda_{A,j}|j\rangle$.
(c) There exists an ONB $(|j\rangle)_{j=1,2,3,\ldots}$ of $\mathcal{H}$, such that for each $A \in \mathcal{A}$, the matrix of $A$ wrt that ONB is diagonal ("simultaneous diagonalization").

3.2 Projectors

Proposition 2. Let $P$ be an operator on a Hilbert space $\mathcal{H}$. The following conditions are equivalent:
(i) $P$ is idempotent (i.e., $P^2 = P$) and Hermitian.
(ii) $P$ is normal and has only 0,1 as eigenvalues.
(iii) For every $\psi \in H$, $P\psi$ is the best approximation (in the Hilbert space norm) of $\psi$ by an element of $\text{im } P$, i.e., $\|\psi - P\psi\| = \min_{\phi \in \text{im } P} \|\psi - \phi\|$.
(iv) For every ONB $(\ket{j})_{j=1,2,3,...}$ of $\text{im } P$, we have $P\psi = \sum_j \ket{j}\bra{j}\psi$.

Note that condition (iii) implies that $P = \sum_j \ket{j}\bra{j}$ for every ONB $(\ket{j})_{j=1,2,3,...}$ of $\text{im } P$.

An operator satisfying these conditions is called a projector.

**Proposition 3.** Let $P, Q$ be projectors and $P \neq Q$. The following two statements are equivalent:

(i) $PQ = QP = 0$
(ii) $\text{im } P \perp \text{im } Q$ (i.e., every element in $\text{im } P$ is orthogonal to every element of $\text{im } Q$).

### 3.3 Spectral theorem, projector version

**Theorem 4.**

(a) $A^* -$commutes.

(b) There exists a set $(P_\ell)_{\ell=1,2,3,...}$ of pairwise orthogonal projectors such that for each $A \in A$ there exist $\lambda_\ell$, $\ell = 1,2,3,...$ such that

$$A = \sum_\ell \lambda_\ell P_\ell.$$

(c) There exists an ONB $(\ket{j})_{j=1,2,3,...}$ of $H$ such that for each $A \in A$ there exist $\lambda_j$, $j = 1,2,3,...$ such that

$$A = \sum_j \lambda_j \ket{j}\bra{j}.$$

### 4 Special operators

We have already reviewed normal and Hermitian operators, as well as projectors.

1.) Identity operator: 1 or Id depending on context.
2.) A normal operator $A$ is Hermitian iff all eigenvalues are real.
3.) An operator $U$ is unitary if $UU^\dagger = U^\dagger U = 1$.
   - Immediately from the definition: Unitary operators are invertible.
   - Immediately from the definition: Unitary operators are normal.
   - From the spectral theorem: A normal operator is unitary iff all its eigenvalues have modulus 1.
4.) An operator is called positive is it is normal and all eigenvalues are non-negative positive.
   - From (2) above: positive operators are Hermitian
   - From spectral theorem: A normal is positive iff $\langle \psi | A | \psi \rangle \geq 0$ for all $|\psi\rangle \in H$. (It’s not sufficient to only check a basis.)

### 5 Tensor products

#### 5.1 Review of facts about tensor products of vector spaces

Let $U, V$ be vector spaces over the field $k \in \{R, C\}$.

1.) The tensor product $U \otimes_k V$ is a vector space over $k$. It’s elements are the elementary tensors $u \otimes v$ for $u \in U, v \in V$, and all $k$-linear combinations of them.
2.) The mapping \( U \times V \to U \otimes V \) is \textit{bilinear}, i.e., for all \( \alpha_1, \alpha_2, \beta_1, \beta_2 \in k \) and \( u_1, u_2 \in U \), \( v_1, v_2 \in V \), we have

\[
(\alpha_1 u_1 + \alpha_2 u_2) \otimes (\beta_1 v_1 + \beta_2 v_2) = \alpha_1 \beta_1 (u_1 \otimes v_1) + \alpha_1 \beta_2 (u_1 \otimes v_2) + \alpha_2 \beta_1 (u_2 \otimes v_1) + \alpha_2 \beta_2 (u_2 \otimes v_2)
\]

3.) Universal property of the tensor product: If \( f : U \times V \to W \) is a bilinear mapping, then there exists a unique linear mapping \( F : U \otimes V \to W \) with the property that for all \( u \in U, v \in V \),

\[
F(u \otimes v) = f(u, v).
\]

**Proposition 5.** If \( b_k, k = 1, 2, 3, \ldots \), is a basis of \( U \) and \( c_\ell, \ell = 1, 2, 3, \ldots \), is a basis of \( V \), then \( b_k \otimes c_\ell, k = 1, 2, 3, \ldots; \ell = 1, 2, 3, \ldots \) is a basis of \( U \times V \).

**Proposition 6.** If \( A : U_1 \to U_2 \) and \( B : V_1 \to V_2 \) are linear mappings, then there is a unique linear mapping \( T_{A,B} : U_1 \otimes V_1 \to U_2 \otimes V_2 \) with the property that for all \( u \in U_1, v \in V_1 \), \( T_{A,B}(u \otimes v) = (Au) \otimes (Bv) \).

Confusingly (or not), \( T_{A,B} \) is denoted by \( A \otimes B \).

**5.1.1 More factors**

“Tensor product” is an associative operation: \( (U \otimes V) \otimes W = U \otimes (V \otimes W) =: U \otimes V \otimes W \).

All properties above have obvious corresponding formulations for \( m \) factors. In particular, the universal property is then:

- If \( f : V_1 \times \cdots \times V_m \to W \) is an \( m \)-linear mapping, then there exists a unique linear mapping \( F : V_1 \otimes \cdots \otimes V_m \to W \) with the property that for all \( v_j \in V_j, j = 1, \ldots, m \),

\[
F(v_1 \otimes \cdots \otimes v_m) = f(v_1, \ldots, v_m)
\]

**5.2 Tensor products of Hilbert spaces**

Let \( H_j, j = 1, \ldots, m \) be a family of Hilbert spaces. We define their tensor product \( \bigotimes_{j=1}^m H_j \) first of all as the tensor product of the vector spaces, i.e., the elements are linear combinations of elementary tensors

\[
\psi_1 \otimes \cdots \otimes \psi_m \text{ (math not.)} \quad |\psi_1 \rangle \cdots \langle \psi_m| \text{ (physics not.)}
\]

We define the inner product on \( \bigotimes_{j=1}^m H_j \) as follows:

- For the elementary tensors: For all \( \phi_j, \psi_j \in H_j, j = 1, \ldots, m \), let

\[
(\phi_1 \otimes \cdots \otimes \phi_m | \psi_1 \otimes \cdots \otimes \psi_m) := \prod_{j=1}^m (\phi_j | \psi_j)
\]

\[
|\psi_1 \rangle \cdots \langle \psi_m| (|\psi_1 \rangle \cdots \otimes |\psi_m\rangle) = (\phi_1 | \psi_1 \rangle \cdots \otimes (\phi_m | \psi_m\rangle)
\]

- Since the inner product is required to be sesquilinear, defining it on the elementary tensors defines it on all elements of the vector space.

**Proposition 7.** If \( \{\langle b_\ell \rangle_\ell=1,\ldots,d_j\} \) is an orthonormal basis for \( H_j, j = 1, \ldots, m \), then the vectors

\[
|b_{\ell_1} \rangle \otimes \cdots \otimes |b_{\ell_m} \rangle, \ell \in \prod_{j=1}^m \{1, \ldots, d_j\},
\]

form an ONB for \( \bigotimes_j H_j \).
5.2.1 Operators and tensor products

**Proposition 8.** Let $H_1, \ldots, H_n$ be Hilbert spaces, and let $A_i, B_i$ be operators on $H_i$, for $i = 1, \ldots, n$.

(a) $(B_1 \otimes \cdots \otimes B_n) \circ (A_1 \otimes \cdots \otimes A_n) = (B_1 \circ A_1) \otimes \cdots \otimes (B_n \circ A_n)$.

(b) $(A_1 \otimes \cdots \otimes A_n)^\dagger = A_1^\dagger \otimes \cdots \otimes A_n^\dagger$.

(c) Let the $A_i$ be normal. $A_1 \otimes \cdots \otimes A_n$ is normal, and all its eigenvalues are of the form $\prod_{i=1}^n \alpha_i$, where $\alpha_i$ is an eigenvalue of $A_i$, $i = 1, \ldots, n$. If $|\psi_i\rangle$ is eigenstate to eigenvalue $\alpha_i$ of $A_i$, then $|\alpha_1\rangle \otimes \cdots \otimes |\alpha_n\rangle$ is eigenstate to eigenvalue $\prod_{i=1}^n \alpha_i$ of $A_1 \otimes \cdots \otimes A_n$.

(d) If each of the operators $A_1, \ldots, A_n$ is unitary, then $A_1 \otimes \cdots \otimes A_n$ is unitary.

(e) If each of the operators $A_1, \ldots, A_n$ is a projector, then $A_1 \otimes \cdots \otimes A_n$ is a projector.

E.g., if $A, B$ are normal and $A$ has eigenvalues 1, 2, 3, and $B$ has eigenvalues 4, 16, 64, then $A \otimes B$ has eigenvalues 4, 8, 12, 16, 32, 48, 64, 128, 192.