MAT 4930: Quantum Algorithms and Complexity **Spring 2021**

Lecture 5: Tensor Product and Multi-Qubit Systems

Lecturer: Jean-François Biasse *TA: Robert Hart*

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

5.1 Basic Definition

Let V and W be complex vector spaces. In the following, $V = \mathbb{C}^m$ and $W = \mathbb{C}^m$. Vectors of V and W can be "multiplied" in a way that we call the *tensor product*. Let $v \in V$, and $w \in W$, we will denote this product by $v \otimes w$. Before giving the formal definition of the tensor product, let us give the essential properties that we want it to possess:

1. $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$.
2. $v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$.
3. $\forall \lambda \in \mathbb{C},\ (\lambda v) \otimes w = v \otimes (\lambda w) = \lambda(v \otimes w)$.

The way to formally define the vector space $V \otimes W$ of tensor products between elements of v and elements of W is to work with $F(v \times W)$ which is the free vector space of formal sums of pairs $(v, w) \in V \times W$. This meas that an element of $F(v \times W)$ has the form

$$x = (v_1, w_1) \oplus (v_2, w_2) \oplus \ldots \oplus (v_k, w_k) \text{ for } k \geq 1,\ v_i \in V, w_j \in W.$$

Here the sum is *formal*, which mean that $(v_1, w_1) \oplus (v_2, w_2)$ is not equal to $(v_1 + v_2, w_1 + w_2)$. However, we can force the natural relations to happen by quotienting $F(V \times W)$ by the right equivalence relation on elements of $F(V \times W)$.

Definition 5.1 (Equivalence relation $\sim$ on $F(V \times W)$) *We define the equivalence relation $\sim$ on $F(V \times W)$ by the following rules:*

1. $\forall (v, w),\ (v, w) \sim (v, w)$.
2. *If* $(v, w) \sim (v', w')$ *then* $(v', w') \sim (v, w)$.
3. *If* $(v, w) \sim (v', w')$ *and* $(v', w') \sim (v'', w'')$ *then* $(v, w) \sim (v'', w'')$.
4. $\forall v, v', w,\ (v, w) \oplus (v', w) \sim (v + v', w)$.
5. $\forall v, w, w'\ (v, w) \oplus (v, w') \sim (v, w + w')$.
6. $\forall \lambda \in \mathbb{C}$, *and* $(v, w) \in V \times W$, $\lambda(v, w) \sim (\lambda v, w)$ *and* $(\lambda v, w) \sim (v, \lambda w)$.

Definition 5.2 (Tensor product space) *Let V and W be complex vector spaces. We define $V \otimes W = F(V \times W)/\sim$ and for each $(v, w) \in V \times W$, $v \otimes w$ is the equivalence class of $(v, w) \in F(V, W)$ under the equivalence relation $\sim$.*

To facilitate explicit calculations, we need to assess the effect of these abstract properties on a concrete basis. Let $|\mathbf{x}_1\rangle, \ldots, |\mathbf{x}_m\rangle$ be a basis of V, and let $|\mathbf{y}_1\rangle, \ldots, |\mathbf{y}_n\rangle$ be a basis of W. Then by following the linearity rules of the tensor product, we have that

$$\left(\sum_{i=1}^{m} v_i|\mathbf{x}_i\rangle\right) \otimes \left(\sum_{j=1}^{n} w_i|\mathbf{y}_i\rangle\right) = \sum_{i=1}^{m}\sum_{j=1}^{n}(v_i w_j)|\mathbf{x}_i\rangle \otimes |\mathbf{y}_j\rangle.$$

Proposition 5.3 *Let $|\boldsymbol{x}_1\rangle, \ldots, |\boldsymbol{x}_m\rangle$ be a basis of V, and let $|\boldsymbol{y}_1\rangle, \ldots, |\boldsymbol{y}_n\rangle$ be a basis of W, then $(|\boldsymbol{x}_i\rangle \otimes |\boldsymbol{y}_j\rangle)_{i,j}$ is a basis of $V \otimes W$ and in particular, $\dim(V \otimes W) = \dim(V) \times \dim(W)$.*

Proof: Let U be a vector space of dimension mn where $m = \dim(V)$ and $n = \dim(W)$. We propose to construct two linear maps

$$\alpha : U \to V \otimes W, \quad \beta : V \otimes W \to U,$$

and to show that they are inverse of each other, thus proving that $U \simeq V \otimes W$. Let $(|\mathbf{u}_{i,j}\rangle)$ be a basis of U for $i \leq m$ and $j \leq m$. We define the map α in the straightforward way by $\alpha(|\mathbf{u}_{i,j}\rangle) := |\mathbf{x}_i\rangle \otimes |\mathbf{y}_j\rangle$. To define β, we first need to build a map $\overline{\beta} : F(V \times W) \to U$ defined by

$$\overline{\beta} : (v, w) \longmapsto \sum_i \sum_j v_i w_j |\mathbf{u}_{i,j}\rangle \text{ where } v = \sum_i v_i|\mathbf{x}_i\rangle,\ w = \sum_j w_j|\mathbf{x}_j\rangle.$$

Now we can see that every time $(v, w) \sim (v', w')$, we have that $\overline{\beta}(v, w) = \overline{\beta}(v', w')$ by inspecting Case 1 to Case 6 of Definition 5.1. This means that $\overline{\beta}$ induces a linear map $\beta : V \otimes W \to U$ given by $\beta(v \otimes w) = \overline{\beta}(v, w)$. We have that $\beta \circ \alpha$ is the identity because

$$\forall i, j,\ \beta(\alpha(|\mathbf{u}_{i,j}\rangle)) = \beta(|\mathbf{x}_i\rangle \otimes |\mathbf{y}_j\rangle) = \overline{\beta}(|\mathbf{x}_i\rangle, |\mathbf{y}_j\rangle) = |\mathbf{u}_{i,j}\rangle$$

To prove that $\alpha \circ \beta$ is the identity as well, we need to show that

$$v \otimes w = \alpha(\beta(v \otimes w)) = \alpha(\overline{\beta}(v, w)) = \alpha\left(\sum_i \sum_j v_i w_j |\mathbf{u}_{i,j}\rangle\right) = \sum_i \sum_j v_i w_j |\mathbf{x}_i\rangle \otimes |\mathbf{y}_j\rangle,$$

which boils down to showing that $(v, w) \sim \sum_i \sum_j v_i w_j (|\mathbf{x}_i\rangle, |\mathbf{y}_j\rangle)$, which can be immediately verified since by Definition 5.1, the equivalence relation $\sim$ was engineered to be bilinear. ■

Therefore, any bases of V and W yield a basis for $V \otimes W$ given by the pairwise tensor products of basis elements of V and W. Note that $|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle$ are in one-to-one correspondance with the outer products $|\mathbf{v}\rangle\langle\mathbf{w}|$.

Definition 5.4 (Bra-ket notation for tensor products) *Let V, W be $\mathbb{C}$-vectors spaces of finite dimension. We define the bra of each tensor of the form $|\boldsymbol{v}\rangle \otimes |\boldsymbol{w}\rangle$ as $\langle\boldsymbol{v}| \otimes \langle\boldsymbol{w}| \in V^* \otimes W^*$ where we identify $\langle\boldsymbol{v}|, \langle\boldsymbol{w}|$ with the linear forms*

$$\langle\boldsymbol{v}|:\ |\boldsymbol{x}\rangle \in V \longmapsto \langle\boldsymbol{v}|\boldsymbol{x}\rangle \in \mathbb{C}$$
$$\langle\boldsymbol{w}|:\ |\boldsymbol{x}\rangle \in W \longmapsto \langle\boldsymbol{w}|\boldsymbol{x}\rangle \in \mathbb{C}.$$

These "bra" are in one-to-one correspondance with linear forms $(V \otimes W)^*$ over $V \otimes W$. This correspondance derives linearly from the map sending tensors of the form $\langle\boldsymbol{v}| \otimes \langle\boldsymbol{w}|$ (which span $V^* \otimes W^*$) to the linear form defined on the generators of $V \otimes W$ by

$$|\boldsymbol{x}\rangle \otimes |\boldsymbol{y}\rangle \in V \otimes W \longmapsto \langle\boldsymbol{v}|\boldsymbol{x}\rangle\langle\boldsymbol{w}|\boldsymbol{y}\rangle.$$

This bra-ket notation corresponds to an inner product on $V \otimes W$ induced by the inner products on V and W respectively. Let $|\mathbf{x}_1\rangle, \ldots, |\mathbf{x}_m\rangle$ be a basis of V, and let $|\mathbf{y}_1\rangle, \ldots, |\mathbf{y}_n\rangle$ be a basis of W. Then by following the linearity rules of the tensor product, we have that

$$\left\langle \left(\sum_{i=1}^{m} v_i \langle \mathbf{x}_i|\right) \otimes \left(\sum_{j=1}^{n} w_i \langle \mathbf{y}_i|\right) \middle| \left(\sum_{k=1}^{m} v_i' |\mathbf{x}_i\rangle\right) \otimes \left(\sum_{l=1}^{n} w_i' |\mathbf{y}_i\rangle\right) \right\rangle = \sum_{i,k \le m} \sum_{j,l \le n} (v_i w_j)(v_k' w_k') \langle \mathbf{x}_i | \mathbf{x}_k \rangle \langle \mathbf{y}_j | \mathbf{y}_l \rangle.$$

This expression is greatly simplified in the case where the $(|\mathbf{x}_i\rangle)_{i\le m}$ and the $(|\mathbf{y}_i\rangle)_{i\le n}$ form orthonormal bases.

Proposition 5.5 *Let $|\boldsymbol{x}_1\rangle, \ldots, |\boldsymbol{x}_m\rangle$ be a an orthonormal basis of V, and let $|\boldsymbol{y}_1\rangle, \ldots, |\boldsymbol{y}_n\rangle$ be an orthonormal basis of W for the inner products on V and W. Then the $(|\boldsymbol{x}_i\rangle \otimes |\boldsymbol{y}_j\rangle)$ is an orthonormal basis of $V \otimes W$ for the inner product of Definition 5.4.*

Proof: This directly follows from our inner product

$$\langle \mathbf{x}_i \otimes \mathbf{y}_j | \mathbf{x}_k \otimes \mathbf{y}_l \rangle = \langle \mathbf{x}_i | \mathbf{x}_k \rangle \langle \mathbf{y}_j | \mathbf{y}_l \rangle = 1 \text{ if } i = k \text{ and } j = l, \; 0 \text{ otherwise.}$$

■

Now assume $|\mathbf{x}_1\rangle, \ldots, |\mathbf{x}_m\rangle$ is an orthonormal basis of V, and $|\mathbf{y}_1\rangle, \ldots, |\mathbf{y}_n\rangle$ is an orthonormal basis of W. Then we have that

$$\left\langle \left(\sum_{i=1}^{m} v_i \langle \mathbf{x}_i|\right) \otimes \left(\sum_{j=1}^{n} w_i \langle \mathbf{y}_i|\right) \middle| \left(\sum_{k=1}^{m} v_i' |\mathbf{x}_i\rangle\right) \otimes \left(\sum_{l=1}^{n} w_i' |\mathbf{y}_i\rangle\right) \right\rangle = \sum_{i=1}^{m} \sum_{j=0}^{n} (v_i v_i')(w_j w_j').$$

Without loss of generality, when $V \simeq \mathbb{C}^m, V \simeq \mathbb{C}^n$, then $V \otimes W \simeq \mathbb{C}^{mn}$ where we map the tensors $|\mathbf{e}_i\rangle \otimes |\mathbf{f}_j\rangle$ for canonical vector basis $|\mathbf{e}_i\rangle \in \mathbb{C}^m$, $|\mathbf{e}_i\rangle \in \mathbb{C}^n$ to the (i, j)-th canonical vector basis of $\mathbb{C}^m n$ (in lexicographic order). Then, the vector representation of the tensor product of

$$|\mathbf{v}\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} \in V, \; |\mathbf{w}\rangle = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in W$$

is given by

$$|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle = |\mathbf{v}, \mathbf{w}\rangle = |\mathbf{vw}\rangle = \begin{pmatrix} v_1 w_1 \\ \vdots \\ v_1 w_n \\ v_2 w_1 \\ \vdots \\ v_m w_n \end{pmatrix}.$$

Example 1 *Here is an example of a tensor product between canonical basis vectors in $\mathbb{C}^2$:*

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |(0,1)\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |1\rangle \in \mathbb{C}^4.$$

Note that $|1\rangle \in \mathbb{C}^4$ is not the same vector as $|1\rangle \in \mathbb{C}^2$ per the definition of the braket notation of canonical basis vectors.

5.2 Linear Operations on Tensor Products

Assume we have a linear operator $\mathbb{C}^n \to \mathbb{C}^m$ represented by the matrix

$$A = \begin{pmatrix} a_{00} & \dots & a_{0n} \\ \vdots & \ddots & \vdots \\ a_{m0} & \dots & a_{mn} \end{pmatrix},$$

and a linear operator $\mathbb{C}^q \to \mathbb{C}^p$ represented by the matrix

$$B = \begin{pmatrix} b_{00} & \dots & b_{0q} \\ \vdots & \ddots & \vdots \\ b_{p0} & \dots & b_{pq} \end{pmatrix},$$

then A and B induce a linear operator $\mathbb{C}^n \otimes \mathbb{C}^q \to \mathbb{C}^m \otimes \mathbb{C}^p$ defined by linearity over the generators of $\mathbb{C}^n \otimes \mathbb{C}^q$ by

$$|\mathbf{v}\rangle \otimes |\mathbf{w}\rangle \longmapsto (A|\mathbf{v}\rangle) \otimes (B|\mathbf{w}\rangle).$$

In turns, this can be represented by the following matrix:

$$A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B \dots & a_{0n}B \\ \vdots & \ddots & \vdots \\ a_{m0}B & a_{m1}B \dots & a_{mn}B \end{pmatrix}.$$

Example 2 *Assume we have a linear operator $\mathbb{C}^2 \to \mathbb{C}^2$ represented by the identity matrix I, and another one by the matrix*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

then these induce a linear operator $\mathbb{C}^4 \to \mathbb{C}^4$ represented by the matrix

$$I \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Definition 5.6 (n-th power tensor product) *Let V be a complex vector space. We denote by $V^{\otimes n}$ the vector space consisting of the tensor product of n copies of V. Every linear operator A on V naturally induces a linear operator on $V^{\otimes n}$ from the above formulae that we denote by $A^{\otimes n}$.*

5.3 Multi-Qubit Systems

We now move to the description of the state of a two-qubit system. In short, if two indenendant qubits are represented by the states $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^2$, then the state of the system made of these two qubits is simply

$$|\psi_1, \psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle.$$

Definition 5.7 (Pure tensor) *Assume V and W are $\mathbb{C}$-vector spaces, a pure tensor is an element of $V \otimes W$ of the form $v \otimes w$ where $v \in V$ and $w \in W$.*

Definition 5.8 (product state) *The product state of the states $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^2$ is the pure tensor $|\psi_1\rangle \otimes |\psi_2\rangle$ it represents the state of a system of two independent qubits in the states $|\psi_1\rangle$, resp. $|\psi_2\rangle$.*

As we know, pure tensors are only a generating set of $V \otimes W$, but certain elements of $V \otimes W$ aren't pure tensors. Likewise, the state of a 2-qubit system may not be in a product state. We call such a state *entangled*.

Definition 5.9 (Entangled state) *A two-qubit system that is not in a product state is said to be in an entangled state.*

Example 3 *Let us look at the state*

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|(0,0)\rangle + |(1,1)\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right) \in \mathbb{C}^4.$$

We can prove that $|\psi\rangle$ is an entangled state. Do do this, assume that $|\psi\rangle$ is in fact a product state. Then let $a_0, a_1, b_0, b_1 \in \mathbb{C}$ such that

$$\begin{aligned} |\psi\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle \\ |\psi_1\rangle &= a_0|0\rangle + a_1|1\rangle \\ |\psi_2\rangle &= b_0|0\rangle + b_1|1\rangle \end{aligned}$$

Then we have

$$|\psi_1\rangle \otimes |\psi_2\rangle = a_0 b_0|0\rangle|0\rangle + a_1 b_1|1\rangle|1\rangle + a_0 b_1|0\rangle|1\rangle + a_1 b_0|1\rangle|0\rangle.$$

This implies that we have the following constraints:

$$\begin{aligned} a_0 b_0 = a_1 b_1 &= \frac{1}{\sqrt{2}} \\ a_0 b_1 = a_1 b_0 &= 0 \end{aligned}$$

This system cannot be solves because the first equalities implie that $a_0, a_1, b_0, b_1 \neq 0$, which is in contradiction with the second equalities. Hence the state is entangled.

Entangled state have a spectacular behavior when one measures only one of the qubits. This is called a partial measurement.

Definition 5.10 (Projective measurement) *Assume that $P_1, \ldots, P_k$ are are the projection operators onto the eigenspaces (representing our observables) with eigenvalues indexed from 1 to k. Then the projective measurement on the state $|\psi\rangle$ returns index m with probability*

$$p(m) = \langle\psi|P_m|\psi\rangle,$$

and leave the system in the state $\frac{P_m|\psi\rangle}{p(m)}$.

Definition 5.11 (Partial measurement) *Let $V \simeq \mathbb{C}^{2^n}$ and $V \simeq \mathbb{C}^{2^m}$, and let $(|\psi_i\rangle)_{i \leq 2^n}$ be an orthonormal basis corresponding to an observable of an n-qubit system. Assume the state $|\psi\rangle \in \mathbb{C}^{2^{n+m}}$ of an $n+m$-qubit state factors as*

$$|\psi\rangle = \sum_{i \leq 2^n} \alpha_i |\psi_i\rangle|\gamma_i\rangle \text{ for some } |\gamma_i\rangle \in \mathbb{C}^{2^m}, \alpha_i \in \mathbb{C},$$

then the measurement of the first n qubits yields the outcome i with probability $|\alpha_i|^2$ and leaves the system in the state $|\psi_i\rangle|\gamma_i\rangle$.

Example 4 *Let us look again at the state*

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|(0,0)\rangle + |(1,1)\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle \in \mathbb{C}^4.$$

If we measure the first qubit, we obtain 0 *with probability* $1/2$*, and the system is left in the state* $|0\rangle|0\rangle$*. Then, a measurement of the second qubit yields* 0 *with probability* 1*.*

On the other hand, if we decide to measure the second qubit first, we obtain 0 *with probability* $1/2$*. This means that the measurement of the first qubit of the system has influenced the subsequent measurements of the second qubit.*

The above example is the basis for the EPR paradox, which can be summarized by the observation that entanglement between the two qubits can continue even after the two systems are done interacting with each other. From a computing standpoint, we sometimes refer to subsets of qubits of the system as *registers*. We then describe a partial measurement as the measurement of a given register.