Quantum Algorithms
Homework 10 Solutions

Patrick Canny

Due: 2019-04-16

Definition. Let $\mathbb{V}$ be a vector space and let $\mathbb{A}, \mathbb{B} \leq \mathbb{V}$ be subspaces.

- We say that $\mathbb{A}$ is *orthogonal* to $\mathbb{B}$ and write $\mathbb{A} \perp \mathbb{B}$ if for every $|a\rangle \in A$ and $|b\rangle \in B$ we have $\langle a \mid b\rangle = 0$.
- Define the *orthogonal complement* to $\mathbb{A}$ to be $\mathbb{A}^{\perp} = \Big\{ |v\rangle \mid |v\rangle \in V \text{ and } \langle a \mid v\rangle = 0 \text{ for all } |a\rangle \in A \Big\}$.
- Define the *sum* of $\mathbb{A}$ and $\mathbb{B}$ to be $\mathbb{A} + \mathbb{B} = \Big\{ |a\rangle + |b\rangle \mid |a\rangle \in A, |b\rangle \in B \Big\}$.

1. Let $\mathbb{A}$ and $\mathbb{B}$ be subspaces of $\mathbb{V}$.

   (i) Prove that $\mathbb{A}^{\perp}$ is a subspace.

Solution: To prove this, we need to show that $|a\rangle \in \mathbb{A}^{\perp} \in \mathbb{V}$. To do this we need to show that:

- $|a\rangle + |b\rangle \in \mathbb{A}^{\perp} \quad \forall\, |a\rangle, |b\rangle \in \mathbb{A}^{\perp}$.
- $\lambda |a\rangle \in \mathbb{A}^{\perp} \quad \forall\, |a\rangle \in \mathbb{A}^{\perp}, \lambda \in \mathbb{C}$
- $|0\rangle \in \mathbb{A}^{\perp}$

Let's start with addition:

Claim 0.1. $|a\rangle + |b\rangle \in \mathbb{A}^{\perp} \quad \forall\, |a\rangle, |b\rangle \in \mathbb{A}^{\perp}$.

Proof of claim. Take $|a\rangle \in \mathbb{A}^{\perp}$ and $|v\rangle \in \mathbb{V}$. By definition, $\langle a \mid v\rangle = 0$. Now if we take $|b\rangle \in \mathbb{A}^{\perp}$ then $\langle b \mid v\rangle = 0$. This holds for all $|v\rangle \in \mathbb{V}$. So:

$$(|a\rangle + |b\rangle) = |a + b\rangle$$
$$\langle a + b \mid v\rangle = 0$$

○

Next, we can show that $\mathbb{A}^{\perp}$ is closed under scalar multiplication.

Claim 0.2. $\lambda |a\rangle \in \mathbb{A}^{\perp} \quad \forall\, |a\rangle \in \mathbb{A}^{\perp}, \lambda \in \mathbb{C}$

Proof of claim. Take $|a\rangle \in \mathbb{A}^{\perp}$. By definition, $\langle a \mid v\rangle = 0 \quad \forall\, |v\rangle \in \mathbb{V}$. Then:

$$\lambda |a\rangle = |\lambda a\rangle$$
$$\therefore \langle \lambda a \mid v\rangle = \lambda \langle a \mid v\rangle = 0$$

○

Finally, show that $|0\rangle \in \mathbb{A}^{\perp}$

Claim 0.3. $|0\rangle \in \mathbb{A}^{\perp}$

Proof of claim.

$$\langle 0 \mid v\rangle = 0 \quad \forall v \in \mathbb{V}$$
$$\therefore \langle 0 \mid a\rangle = 0 \quad \forall a \in \mathbb{A}^{\perp}$$

So, $|0\rangle \in \mathbb{A}^{\perp}$. ○

(ii) Prove that $\mathbb{A} + \mathbb{B}$ is a subspace.

Solution: To prove this, we need to show that $|a\rangle \in \mathbb{A}^{\perp} \in \mathbb{V}$. To do this we need to show that:

- $|a\rangle + |b\rangle \in \mathbb{A} + \mathbb{B} \quad \forall |a\rangle, |b\rangle \in \mathbb{A} + \mathbb{B}$.
- $\lambda |a\rangle \in \mathbb{A} + \mathbb{B} \quad \forall |a\rangle \in \mathbb{A} + \mathbb{B}, \lambda \in \mathbb{C}$
- $|0\rangle \in \mathbb{A} + \mathbb{B}$

Let's start with addition:

Claim 0.4. $|a\rangle + |b\rangle \in \mathbb{A} + \mathbb{B} \quad \forall |a\rangle, |b\rangle \in \mathbb{A} + \mathbb{B}$.

Proof of claim. Take $|a\rangle \in \mathbb{A} + \mathbb{B}$. It can be written as

$$|x\rangle + |y\rangle$$

Similarly, given $|b\rangle$, it can be written as

$$|x'\rangle + |y'\rangle$$

Then, consider $|a\rangle + |b\rangle$:

$$\begin{aligned} |a\rangle + |b\rangle &= (|x\rangle + |y\rangle) + (|x'\rangle + |y'\rangle) \\ &= (|x\rangle + |x'\rangle) + (|y\rangle + |y'\rangle) \end{aligned}$$

and since $|x\rangle + |x'\rangle \in \mathbb{A}$ by definition (and similarly for $|y\rangle + |y'\rangle \in \mathbb{B}$), it holds that $|a\rangle + |b\rangle \in \mathbb{A} + \mathbb{B}$. ○

Next, we can show that $\mathbb{A} + \mathbb{B}$ is closed under scalar multiplication.

Claim 0.5. $\lambda |a\rangle \in \mathbb{A} + \mathbb{B} \quad \forall |a\rangle \in \mathbb{A} + \mathbb{B}, \lambda \in \mathbb{C}$

Proof of claim. $|a\rangle$, by definition, can be written as $|x\rangle + |y\rangle$.

$$\lambda |a\rangle = \lambda(|x\rangle + |y\rangle) = \lambda |x\rangle + \lambda |y\rangle$$

and since $\mathbb{A}, \mathbb{B}$ are subspaces, they are closed under scalar multiplication, implying that $\lambda |x\rangle \in \mathbb{A}, \lambda |y\rangle \in \mathbb{B}$. Therefore, $\lambda |a\rangle \in \mathbb{A} + \mathbb{B}$ ○

Finally, show that $|0\rangle \in \mathbb{A} + \mathbb{B}$

Claim 0.6. $|0\rangle \in \mathbb{A} + \mathbb{B}$

Proof of claim. $|0\rangle \in \mathbb{A}, \mathbb{B}$ since they are both subspaces. So:

$$|0\rangle + |0\rangle = |0\rangle$$
$$\therefore |0\rangle \in \mathbb{A} + \mathbb{B}$$

○

(iii) Prove that $\dim(\mathbb{A}) + \dim(\mathbb{A}^{\perp}) = \dim(\mathbb{V})$.

Solution: Consider the bases for $\mathbb{A}$ and $\mathbb{A}^{\perp}$. Call them α and β, respectively. We want to show that

$$\alpha \cup \beta = \{v_1, \ldots, v_k, w_1, \ldots, w_l\}$$

is a valid basis for $\mathbb{V}$ given that $v_i \in \alpha$ and $w_j \in \beta$.

Given $v \in \mathbb{V}$, v can be expressed as $v_1 + v_2 \quad v_1 \in \mathbb{A}, v_2 \in \mathbb{A}^{\perp}$. v_1, v_2 can be represented as a linear combination of basis vectors. So:

$$v = v_1 + v_2 = \sum_i \lambda_i |v_i\rangle + \sum_j \gamma_i |w_j\rangle$$

which is an analog to showing that $\alpha \cup \beta$ acts as a basis for $\mathbb{V}$. Is $\alpha \cup \beta$ linearly independant?

2. Let $\mathbb{A}$ be a subspace of $\mathbb{V}$ and let $|v\rangle \in V$.

(i) Show that $\Pi_{\mathbb{A}} |v\rangle \in A$.

Solution: By definition, $\Pi_{\mathbb{A}} = \sum_j |e_j\rangle \langle e_j|$ where e_j runs over an orthonormal basis for $\mathbb{A}$. So, we can re-write the sum as:

$$\begin{aligned}\Pi_{\mathbb{A}} &= \big(\sum_j |e_j\rangle \langle e_j|\big) |v\rangle \\ &= \sum_j \langle e_j \mid v\rangle |e_j\rangle \\ &= \sum_j \lambda |e_j\rangle = \lambda \sum_j |e_j\rangle \\ &= \lambda |a\rangle\end{aligned}$$

Where $|a\rangle \in \mathbb{A}$. This is because, by the sum above, $|a\rangle$ is a linear combination of the basis vectors from $\mathbb{A}$, a.k.a. a vector in $\mathbb{A}$.

(ii) Show that $|v\rangle - \Pi_{\mathbb{A}} |v\rangle \in A^{\perp}$.

Solution: $|v\rangle$ can be represented by $|v_i\rangle + |v_j\rangle$ given that $|v_i\rangle \in \mathbb{A}$ and $|v_j\rangle \in \mathbb{A}^{\perp}$. So, since $\Pi_{\mathbb{A}} |v\rangle \in \mathbb{A}$, an arbitrary $|v\rangle \in \mathbb{V}$ can be expressed as

$$\Pi_{\mathbb{A}} |v\rangle + |v_j\rangle = |v\rangle$$

Therefore, $|v_j\rangle \in \mathbb{A}^{\perp}$.

(iii) Explain why this justifies calling $\Pi_{\mathbb{A}}$ the orthogonal projection onto $\mathbb{A}$.

Solution: $\Pi_{\mathbb{A}}$ effectively extracts the perpendicular component of $|v\rangle$, isolating it to a vector in the $\mathbb{A}$ space.

3. Suppose that $\mathbb{A}$ and $\mathbb{B}$ are orthogonal to each other.

(i) What is $\dim(\mathbb{A} + \mathbb{B})$?

Solution:

$$\dim(\mathbb{A} + \mathbb{B}) = \dim(\mathbb{A}) + \dim(\mathbb{B})$$

This is only possible since $\mathbb{A} \perp \mathbb{B}$. This fact implies that $\mathbb{A} \cap \mathbb{B} = 0$, so their bases are disjoint.

(ii) Show that $\mathbf{P}(|v\rangle, \mathbb{A} + \mathbb{B}) = \mathbf{P}(|v\rangle, \mathbb{A}) + \mathbf{P}(|v\rangle, \mathbb{B})$.

Solution: Since $\mathbb{A} \perp \mathbb{B}$, the two event spaces are independant of one another. In other words, this means that the probabilities of an event occuring in either of the two spaces are independant of each other. Because of this fact,

$$\begin{aligned} \mathbf{P}(|v\rangle, \mathbb{A} + \mathbb{B}) &= \langle v| \Pi_{\mathbb{A}+\mathbb{B}} |v\rangle \\ &= \langle v| \Pi_{\mathbb{A}} + \Pi_{\mathbb{B}} |v\rangle \\ &= \langle v| \Pi_{\mathbb{A}} |v\rangle + \langle v| \Pi_{\mathbb{B}} |v\rangle \\ &= \mathbf{P}(|v\rangle, \mathbb{A}) + \mathbf{P}(|v\rangle, \mathbb{B}) \end{aligned}$$

$$\mathbf{P}(|v\rangle, \mathbb{A} + \mathbb{B}) = \mathbf{P}(|v\rangle, \mathbb{A}) + \mathbf{P}(|v\rangle, \mathbb{B})$$

(iii) Show that $\Pi_{\mathbb{A}}\Pi_{\mathbb{B}} = \Pi_{\mathbb{B}}\Pi_{\mathbb{A}}$.

Solution:

$$\begin{aligned} \Pi_{\mathbb{A}} &= \sum_i |e_i\rangle \langle e_i| \quad e_i \in \mathcal{B}_{\mathbb{A}} \\ \Pi_{\mathbb{B}} &= \sum_j |f_j\rangle \langle f_j| \quad f_j \in \mathcal{B}_{\mathbb{B}} \\ \Pi_{\mathbb{A}}\Pi_{\mathbb{B}} &= \big(\sum_i |e_i\rangle \langle e_i|\big)\big(\sum_j |f_j\rangle \langle f_j|\big) \\ &= \sum_i \sum_j |e_i\rangle \langle e_i \mid f_j\rangle \langle f_j| \end{aligned}$$

Because $\mathbb{A} \perp \mathbb{B}$, $\langle e_i \mid f_j\rangle = 0$, which shows that $\Pi_{\mathbb{A}}\Pi_{\mathbb{B}} = \Pi_{\mathbb{B}}\Pi_{\mathbb{A}}$

4. Suppose that $\mathbb{A} \leq \mathbb{V}$ and $\mathbb{B} \leq \mathbb{W}$ are two subspaces.

(i) Prove that $\Pi_{\mathbb{A}\otimes\mathbb{B}} = \Pi_{\mathbb{A}} \otimes \Pi_{\mathbb{B}}$.

Solution:

$$\begin{aligned}
\Pi_{\mathbb{A}\otimes\mathbb{B}} &= \sum_{i,j} |e_i \otimes f_j\rangle \langle e_i \otimes f_j| \quad e_i \in \mathbb{A}, f_j \in \mathbb{B} \\
&= \sum_{i,j} |e_i\rangle \otimes |f_j\rangle \langle e_i| \otimes \langle f_j| \\
&= \sum_{i,j} |e_i\rangle \langle e_i| \otimes |f_j\rangle \langle f_j| \\
&= \sum_{i} |e_i\rangle \langle e_i| \otimes \sum_{j} |f_j\rangle \langle f_j| \\
&= \Pi_{\mathbb{A}} \otimes \Pi_{\mathbb{B}}
\end{aligned}$$

(ii) Let ρ and τ be density matrices. Prove that $\mathbf{P}(\rho \otimes \tau, \mathbb{A} \otimes \mathbb{B}) = \mathbf{P}(\rho, \mathbb{A})\mathbf{P}(\tau, \mathbb{B})$. You may use the fact that $\mathrm{Tr}(X \otimes Y) = \mathrm{Tr}(X)\mathrm{Tr}(Y)$.

Solution:

$$\begin{aligned}
\mathbf{P}(\rho \otimes \tau, \mathbb{A} \otimes \mathbb{B}) &= \mathrm{Tr}(\rho \otimes \tau, \Pi_{\mathbb{A}\otimes\mathbb{B}}) \\
&= \mathrm{Tr}(\rho \otimes \tau, \Pi_{\mathbb{A}} \otimes \Pi_{\mathbb{B}}) \\
&= \mathrm{Tr}(\rho\Pi_{\mathbb{A}} \otimes \tau\Pi_{\mathbb{B}}) \\
&= \mathrm{Tr}(\rho\Pi_{\mathbb{A}})\mathrm{Tr}(\tau\Pi_{\mathbb{B}}) \\
&= \mathbf{P}(\rho, \mathbb{A})\mathbf{P}(\tau, \mathbb{B})
\end{aligned}$$