Quantum Algorithms and Learning Theory

Faris Sbahi

Abstract

In this document, we provide a presentation of the latest results in quantum learning theory alongside theoretical extensions. We also provide experimental analyses of quantum feature maps which can be used for supervised learning.

The first part of our paper is a review: First, we present an overview of quantum computation and information. Next, we present a review of the brief history of quantum machine learning. The subsequent part of our paper is an analysis of recent results in quantum learning theory: (1) information theoretic bounds on quantum computation learning, (2) supervised learning using hybrid quantum-classical circuits, and (3) Tang's [37] idea of least-square sampling providing parallel classical algorithms for quantum machine learning algorithms that solve singular value transformation problems.

The last part of our paper provides new results on quantum feature maps which seek to solve the quantum encoding problem by encoding data inputs into a quantum state that implicitly performs the feature map given by a kernel function. Therefore, if the kernel is sufficiently difficult to evaluate classically, then there may exist a quantum advantage. Hence, we provide a geometric analysis of the properties of a kernel that may provide quantum advantage, and provide experimental results to demonstrate the robustness of particular candidate maps.

Contents

Chapter 1

Introduction

Rough draft readers:

The "Introduction" and "Preliminaries" chapters are in progress. I plan a standard review of the necessary background from quantum information theory (see [30] and [39]) to make the essential chapters of this thesis interpretable to a general Physics audience. Of course, I will primarily restate theorems and provide references in order to keep this portion succinct. For the time being, I've included my personal notes that I've kept since I began working on this project.

Chapter 2

Preliminaries

2.1 Quantum Mechanics

Reference: Chapter 2 of [30]

2.1.1 Postulates of Quantum Mechanics

First, we cover the fundamental postulates of quantum mechanics.

State Space and State Vector

Associated with an isolated physical system is a Hilbert space, $\mathcal{H}$. A Hilbert space is a complete inner-product vector space. Note that completeness holds trivially in a finite-dimensional vector space because we have closure with respect to all sequences (and hence any Cauchy sequence in the vector space must converge to a vector in the same space). Nevertheless, the state space of a physical system may be infinite-dimensional.

A system is completely described by a unit vector $u \in \mathcal{H}$ called the state vector.

For example, consider a system given by a single qubit, which has a two-dimensional state space. Let $|0\rangle$ and $|1\rangle$ be an orthonormal basis for this space. Hence, a state vector in this space is given by

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$.

Evolution

The evolution of a closed quantum system is described by a unitary transformation. Recall that an operator U is unitary iff $U^\dagger U = I = UU^\dagger$ (and hence preserves inner products[1]).

So, let the state of a system at time t_1 be given by $|\psi\rangle$ and $|\psi'\rangle$ at t_2. Hence,

$$|\psi'\rangle = U\,|\psi\rangle$$

[1] and furthermore has a spectral decomposition because it is normal

Evolution in Continuous Time

Schrodinger's equation provides the time evolution of the state of a quantum system

$$i\hbar \frac{d\,|\psi\rangle}{dt} = H\,|\psi\rangle \tag{2.1}$$

where H is the (Hermitian) Hamiltonian of the closed system. Because the Hamiltonian is Hermitian it has spectral decomposition

$$H = \sum_E E\,|E\rangle\,\langle E|$$

where E is the energy eigenvalue corresponding to energy eigenstate $|E\rangle$.

For example, consider the Hamiltonian $H = \hbar\omega X$ (recall that $X = \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ from A.1.1). Hence, we solve for its eigenvalues and eigenvectors

$$\begin{aligned}
\det\left\{\hbar\omega \begin{pmatrix} -\lambda & 1 \\ 1 & -\lambda \end{pmatrix}\right\} &= 0 \\
\lambda^2 - 1^2 &= 0 \\
\lambda &= \pm 1 \\
\Rightarrow E_\pm &= \pm\hbar\omega \\
\hbar\omega \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} |E_+\rangle &= 0 \\
|E_+\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \coloneqq |+\rangle \\
|E_-\rangle &= |-\rangle
\end{aligned}$$

Onwards, notice that we can solve Schrodinger's equation (2.1) and have

$$|\psi(t_2)\rangle = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right] |\psi(t_1)\rangle$$

and equivalently from 2.1.1 we can represent this transformation with unitary operator $U = \exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right]$. This holds in general and so we can consider the two descriptions from 2.1.1 and 2.1.1 interchangeably (the authors prefer the latter).

Quantum Measurement

Quantum measurements are described by a collection of measurements operators $\{M_m\}$ (where the index m refers to the potential measurement outcomes of the experiment) which act on the state space of the system being observed.

Hence, if the pre-measurement state is $|\psi\rangle$, then

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$$

and the post-measurement state is

$$\frac{M_m |\psi\rangle}{\sqrt{p(m)}}$$

Furthermore, $\{M_m\}$ satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = I$$

An important example of a measurement is the measurement of a qubit in the computational basis. This is a measurement of a qubit with two outcomes defined by the measurement operators $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$.

Now, we see an interesting implication. If we seek to distinguish our physical system from a set of orthogonal states, then we can reliably do so by simply defining each measurement operator to be the outer product of our states of interest. We add a final operator defined to be the remaining complement of the identity in order to satisfy the completeness equation.

On the flipside, two non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$ necessarily share a parallel component in their orthogonal decomposition. Hence, a measurement outcome that corresponds to the pre-measurement state being $|\psi_1\rangle$ with probability $p = 1$ has a probability $p' > 0$ of having been in state $|\psi_2\rangle$.

Projective Measurements

There exists a special class of quantum measurements known as projective measurements. These measurements can be described by an observable M, a hermitian operator on the state space being observed. M has spectral decomposition

$$M = \sum_m m P_m$$

where P_m is the projector onto the eigenspace of M with eigenvalues m.

Furthermore, if the pre-measurement state is $|\psi\rangle$, then

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

and the post-measurement state is

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}}$$

This simplifies the formula for the expected value of a measurement

$$\begin{aligned}\langle M\rangle &= \sum_m mp(m)\\ &= \langle\psi|\,(\sum_m mP_m)\,|\psi\rangle\\ &= \langle\psi|\,M\,|\psi\rangle\end{aligned}$$

For example, consider projective measurements on the system given by single qubits with observable Pauli matrix Z. Hence, Z has eigenvalues $+1$ and -1 and eigenstates $|0\rangle$ and $|1\rangle$, respectively. So, consider state $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle \Rightarrow p(+1) = \langle+|0\rangle\langle 0|+\rangle = \frac{1}{2}$. Similarly, $p(-1) = \frac{1}{2}$.

More generally, suppose v is an arbitrary 3-d vector. We can define an observable

$$v\cdot\sigma = v_1\sigma_x + v_2\sigma_y + v_3\sigma_z$$

Example 2.1.1. *Suppose we have a qubit in the state $|0\rangle$, and we measure the observable X. What is the average value of X? What is the standard deviation of X?*

Proof. X has eigenvalues $+1$ and -1 and eigenstates $|+\rangle$ and $|-\rangle$, respectively. Hence,

$$\begin{aligned}\langle X\rangle &= \langle\psi|\,X\,|\psi\rangle\\ &= \langle\psi|\,(|+\rangle\langle+| - |-\rangle\langle-|)\,|\psi\rangle\\ &= \langle 0|+\rangle\langle+|0\rangle - \langle 0|-\rangle\langle-|0\rangle\\ &= \frac{1}{2} - \frac{1}{2} = 0\end{aligned}$$

Furthermore,

$$\begin{aligned}\langle M^2\rangle - \langle M\rangle^2 &= \langle\psi|\,M^2\,|\psi\rangle - 0\\ &= \langle\psi|\,(|+\rangle\langle+| + |-\rangle\langle-|)\,|\psi\rangle\\ &= \frac{1}{2} + \frac{1}{2} = 1\end{aligned}$$

□

Proposition 2.1.2. *$v\cdot\sigma$ has eigenvalues ± 1 and the projectors onto the corresponding eigenspaces are given by $P_\pm = (I \pm v\cdot\sigma)/2$.*

Proof. First, $v\cdot\sigma$ is Hermitian so it's spectral decomposition is given by $v\cdot\sigma = U\Lambda U^\dagger$ for some unitary U, diagonal matrix Λ. Hence, using $(v\cdot\sigma)^2 = I$ we have

$$\begin{aligned}I = (v\cdot\sigma)^2 &= (U\Lambda U^\dagger)^2\\ &= U\Lambda^2 U^\dagger\\ \Rightarrow U^\dagger I U &= \Lambda^2\\ I &= \Lambda^2\end{aligned}$$

Therefore, Λ must have diagonal entries ± 1.

Next, $P_i P_j = \delta_{ij} P_j$ since if $i \neq j$ then $(I+v\cdot\sigma)(I-v\cdot\sigma) = I-(v\cdot\sigma)^2 = I-I = 0$. Furthermore, $P_+ + P_- = (I+v\cdot\sigma)/2 + (I-v\cdot\sigma)/2 = I$.

Finally, $(+1)P_+ + (-1)P_- = (I+v\cdot\sigma)/2 - (I-v\cdot\sigma)/2 = v\cdot\sigma$. □

POVM measurements

POVMs are best viewed as a special case of the general measurement formalism, providing the simplest means to study post-measurement statistics without knowledge of the post measurement state.

From above, $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$ so if we define $E_m \coloneqq M_m^\dagger M_m$ (which is hence positive from A.1.3) then these E_m's are sufficient for the purpose of computing probabilities. We denote $\{E_m\}$ as a POVM. POVMs also satisfy the completeness relation.

Note that projective operators are the special case of being equivalent to their respective POVM element because $E_m = P_m^\dagger P_m = P_m$.

Proposition 2.1.3. *Any measurement where the measurement operators and the POVM elements coincide is a projective measurement*

Proof. We would then have $M_m = E_m = M_m^\dagger M_m$. Furthermore, E_m is a positive operator $\Rightarrow M_m = M_m^\dagger M_m = M_m M_m^\dagger = M_m^\dagger$ so M_m is Hermitian. Hence, $M_m = M_m^2$ so the measurement is projective. □

Nevertheless, the POVM formalism is a useful guide in for our intuition in quantum information. Consider if Alice prepares some state for Bob that is either $|\psi_1\rangle = |0\rangle$ or $|\psi_2\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Recall from 2.1.1, Bob can't determine which state was prepared with full certainty (because of the shared orthogonal component $|0\rangle$). Still, we can define a POVM[2]

$$
\begin{aligned}
E_1 &= \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1| \\
E_2 &= \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} \\
E_3 &= I - E_1 - E_2
\end{aligned}
$$

Now, notice what happens.

$$
\begin{aligned}
\langle\psi_1| E_1 |\psi_1\rangle &= \langle 0| \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1|0\rangle \\
&= 0 \\
\langle\psi_2| E_1 |\psi_2\rangle &= \frac{\langle 0| + \langle 1|}{\sqrt{2}} \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1| \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
&= \frac{\sqrt{2}}{2\sqrt{2}+2} > 0
\end{aligned}
$$

[2] verify that completeness and these being positive operators holds

Hence, if we observe E_1 after the measurement described by $\{E_1, E_2, E_3\}$, then Alice must've prepared $|\psi_2\rangle$. Similarly,

$$\begin{aligned}
\langle\psi_1| E_2 |\psi_1\rangle &= \langle 0| \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} |0\rangle \\
&= \frac{\sqrt{2}}{2\sqrt{2}+2} > 0 \\
\langle\psi_2| E_2 |\psi_2\rangle &= \frac{\langle 0| + \langle 1|}{\sqrt{2}} \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
&= 0
\end{aligned}$$

so if we observe E_2, then Bob concludes that Alice prepared $|\psi_1\rangle$. Our routine is imperfect because we may observe E_3 and hence would infer nothing of the original state. Still, we would never *incorrectly* guess given that we allow ourselves to abstain when we see E_3.

Proposition 2.1.4. *Suppose Bob is given a quantum state chosen from a set $S = |\psi_1\rangle, \cdots, |\psi_m\rangle$ of linearly independent states. Construct a POVM $\{E_1, \cdots, E_{m+1}\}$ such that if outcome E_i occurs, $1 \leq i \leq m$, then Bob knows with certainty that he was given state $|\psi_i\rangle$.*

Proof. To distinguish the states we require $\langle\psi_i| E_j |\psi_i\rangle = p_i \delta_{ij}$ where $p_i > 0$ and $1 \leq i, j \leq m$.

So, we can use the Gram-Schmidt process using S as our linearly independent set. This will give us an orthonormal set $U = |\varphi_1\rangle, \cdots, |\varphi_m\rangle$ that spans the same subspace as S. Next, we can represent each $|\psi_i\rangle$ in this orthonormal basis, U. Finally, for each i we can find a vector $|\psi_i'\rangle$ in the span of U that is orthogonal to all $|\psi_j\rangle, j \neq i$. Hence, we can define $E_i = |\psi_i'\rangle \langle\psi_i'|, 1 \leq i \leq m$. Finally, take $E_{m+1} = I - \sum_m E_i$.

Creating an optimal POVM is much trickier (in the sense of minimizing the probability p_{m+1}). □

From this Proposition, we see that POVMs present a reliable way to distinguish non-orthogonal (but linearly independent) states given that we allow for the slack of an "inconclusive" measurement (E_{m+1}).

Composite Systems

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems.

Interestingly, we can show that a general quantum measurement (as described in 2.1.1) can be implemented as a projective measurement coupled with unitary dynamics.

Consider a quantum system with state space Q and measurements M_m on this system. We can introduce an *ancilla* system M with orthonormal basis $|m\rangle$ which is in one-to-one correspondence with the possible outcomes of the measurement we wish to implement.

So, let $|0\rangle$ be a fixed state of M and define an operator U on $|\psi\rangle |0\rangle$ (with $|\psi\rangle$ as a state of Q) by

$$U |\psi\rangle |0\rangle \coloneqq \sum_m M_m |\psi\rangle |m\rangle$$

Hence,

$$\langle\varphi|\langle 0|U^\dagger U|\psi\rangle|0\rangle = \sum_m \sum_{m'} \langle\varphi| M_m^\dagger M_{m'} |\psi\rangle \langle m|m'\rangle$$

So, because the states $|m\rangle$ are orthonormal

$$= \sum_m \langle\varphi| M_m^\dagger M_m |\psi\rangle$$

and finally by the completeness of M_m

$$= \langle\varphi|\psi\rangle$$

This tells us that U preserves inner products between states of the form $|\psi\rangle|0\rangle$. Furthermore, we can show that U can be extended to a unitary operator on $Q \otimes M$ (exercise).

Hence, consider a projective measurement on the two systems $(U|\psi\rangle|0\rangle)$ given by projectors $P_m \coloneqq I_Q \otimes |m\rangle\langle m|$. So,

$$\begin{aligned} p(m) &= \langle\psi|\langle 0|U^\dagger P_m U|\psi\rangle|0\rangle \\ &= \sum_{m'}\sum_{m''} \langle\psi| M_{m'}^\dagger \langle m'|(I_Q \otimes |m\rangle\langle m|) M_{m''}|\psi\rangle|m''\rangle \\ &= \langle\psi| M_m^\dagger M_m |\psi\rangle \end{aligned}$$

which agrees with the general result from 2.1.1. Similarly, the post-measurement state is as expected. Hence, we've shown that unitary dynamics, projective measurements, and ancillary systems can be used together to describe any general measurement.

A state of a composite system having this property is said to be entangled.

2.1.2 Superdense Coding

Suppose Alice is in possession of two classical bits of information she wishes to transmit to Bob, but is only allowed to send a single qubit to Bob.

Now, suppose that Alice and Bob initially share a pair of qubits in the entangled state from above

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

where Alice is initially holding the first qubit and Bob the second. She can then apply a particular gate to send a bit string. Below shows the corresponding gate and resulting state

Bit String	Applied gate	Resulting state
00	–	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$
01	Z	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$
10	X	$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$
11	iY	$\frac{-\|10\rangle+\|01\rangle}{\sqrt{2}}$

Observe that these are the Bell states (see A.1.2). Furthermore, Bell states form an orthonormal basis and hence can be distinguished (as we've discussed in 2.1.1). Hence, Alice needs only to interact with the single qubit to transmit two classical bits of information to Bob.

2.1.3 The Density Operator

An alternative formulation of quantum mechanics is possible using a tool known as the density operator.

Suppose a quantum system is one of a number of states $|\psi\rangle$ with probability p_i. We call $\{p_i, |\psi_i\rangle\}$ an ensemble of pure states. The density operator is defined

$$\rho \coloneqq \sum_i p_i \, |\psi_i\rangle \, \langle\psi_i|$$

Evolution of the density operator (under a unitary transformation) can be derived readily

$$\sum_i p_i U \, |\psi_i\rangle \, \langle\psi_i| \, U^\dagger = U \rho U^\dagger$$

If we perform a measurement with operator M_m with initial state $|\psi_i\rangle$ then

$$\begin{aligned} p(m \mid i) &= \langle\psi_i| \, M_m^\dagger M_m \, |\psi_i\rangle \\ &= \operatorname{tr}\big(M_m^\dagger M_m \, |\psi_i\rangle \, \langle\psi_i|\big) \end{aligned}$$

using A.1.4.

Hence, summing this conditional probability across all initial states we have

$$\begin{aligned} p(m) &= \sum_i p_i \operatorname{tr}\big(M_m^\dagger M_m \, |\psi_i\rangle \, \langle\psi_i|\big) \\ &= \operatorname{tr}\big(M_m^\dagger M_m \rho\big) \end{aligned}$$

The state after obtaining measurement result m on initial state $|\psi_i\rangle$ is

$$|\psi_i^m\rangle = \frac{M_m \, |\psi_i\rangle}{\sqrt{\langle\psi_i| \, M_m^\dagger M_m \, |\psi_i\rangle}}$$

and so the density operator after result m is given by

$$\begin{aligned} \rho_m &= \sum_i p(i \mid m) \, |\psi_i^m\rangle \, \langle\psi_i^m| \\ &= \sum_i p(i \mid m) \frac{M_m \, |\psi_i\rangle \, \langle\psi_i| \, M_m^\dagger}{\langle\psi_i| \, M_m^\dagger M_m \, |\psi_i\rangle} \end{aligned}$$

Furthermore, from Bayes' rule we have that $p(i \mid m) = \frac{p(m|i)p(i)}{p(m)}$ so we can simplify

$$\begin{aligned}
\rho_m &= \sum_i \frac{p(m \mid i)p(i)}{p(m)} \frac{M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle} \\
&= \sum_i \frac{p(i) \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}{\operatorname{tr}\Big(M_m^\dagger M_m \rho\Big)} \frac{M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle} \\
&= \sum_i \frac{p(i) M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger}{\operatorname{tr}\Big(M_m^\dagger M_m \rho\Big)} \\
&= \frac{M_m \rho M_m^\dagger}{\operatorname{tr}\Big(M_m^\dagger M_m \rho\Big)}
\end{aligned}$$

A quantum state whose state $|\psi\rangle$ is known exactly is said to be in a pure state. In this case the density operator is simply $\rho = |\psi\rangle \langle\psi|$. Otherwise, ρ is in a mixed state.

A pure state satisfies $\operatorname{tr}\big(\rho^2\big) = 1$ and a mixed state $\operatorname{tr}\big(\rho^2\big) < 1$.

Imagine that our record of the result m of a measurement was lost. We would have a quantum system in the state ρ_m with probability $p(m)$ without knowing the actual value of m. Hence, the system would be described as

$$\begin{aligned}
\rho &= \sum_m p(m) \rho_m \\
&= \sum_m M_m \rho M_m^\dagger
\end{aligned}$$

We may wish to move away from the interpretation of the density operator as a means of describing ensembles of quantum states.

Theorem 2.1.5. *An operator ρ is a density operator associated to some ensemble $\{p_i, |\psi_i\rangle\}$ if and only if it satisfies the conditions*

1. *ρ has trace equal to one*
2. *ρ is a positive operator*

Proof. We show one direction (see the text for the other). Let ρ be a density operator. Hence,

$$\begin{aligned}
\operatorname{tr}(\rho) &= \sum_i p_i \operatorname{tr}(|\psi_i\rangle \langle\psi_i|) \\
&= \sum_i p_i = 1
\end{aligned}$$

because $\operatorname{tr}(|\psi_i\rangle \langle\psi_i|) = \psi_{i,11}^2 + \psi_{i,22}^2 + \cdots \psi_{i,nn}^2 = 1$ by normalization.

Furthermore, suppose $|\varphi\rangle$ resides in the vector space

$$\begin{aligned}\langle\varphi|\,\rho\,|\varphi\rangle &= \sum_i p_i \,\langle\varphi|\psi_i\rangle\,\langle\psi_i|\varphi\rangle \\ &= \sum_i p_i |\,\langle\varphi|\psi_i\rangle\,|^2 \geq 0\end{aligned}$$

so we have positivity. □

The use of this theorem is that we can define a density operator to be a positive operator with trace one and hence reformulate the postulates of quantum mechanics without speaking of ensembles.

This reformulation shines when describing quantum systems whose state is not known and when describing subsystems a composite quantum system.

Proposition 2.1.6. *Let ρ be a density operator.* $\operatorname{tr}\left(\rho^2\right) \leq 1$ *with equality iff ρ is a pure state.*

Proof.

$$\begin{aligned}\rho^2 &= \sum_i p_i \,|\psi_i\rangle\,\langle\psi_i| \sum_{i'} p_{i'} \,|\psi_{i'}\rangle\,\langle\psi_{i'}| \\ &= \sum_i p_i^2 \,|\psi_i\rangle\,\langle\psi_i|\end{aligned}$$

by orthonormality. Hence,

$$\operatorname{tr}\rho^2 = \sum_i \sum_j p_i^2 \psi_{i,jj}^2$$

And $\sum_j \psi_{i,jj}^2 = 1$ by normalization

$$= \sum_i p_i^2$$

Now, we have that $\sum_i p_i = 1 \Rightarrow \sum_i p_i^2 = 1 \Leftrightarrow p_i = 1$. If $p_i = 1$, then there is only one index and hence we have a pure state. Otherwise, $\sum_i p_i^2 < 1$ and we have a mixed state. □

Remember that different ensembles of quantum states can give rise to a specific density matrix and hence one must avoid assuming that the eigenvectors and eigenvalues have special significance with regard to the represented ensemble of quantum states.

Nevertheless, there is value in discussing which ensembles give rise to the same density matrix (notably in quantum noise and error correction). Let $\left|\tilde{\psi}_i\right\rangle$ generate ρ i.e. $\rho \coloneqq \sum_i \left|\tilde{\psi}_i\right\rangle\left\langle\tilde{\psi}_i\right|$. Note that $\left|\tilde{\psi}_i\right\rangle = \sqrt{p_i}\,|\psi_i\rangle$ is clearly not necessarily normalized. Now, we have the following theorem.

Theorem 2.1.7. *The sets $\left|\tilde{\psi}_i\right\rangle$ and $|\tilde{\varphi}_j\rangle$ generate the same ρ if and only if*

$$\left|\tilde{\psi}_i\right\rangle = \sum_j u_{ij} \,|\tilde{\varphi}_j\rangle$$

where the matrix with matrix elements u_{ij} is unitary.

Proof. See the text. □

As mentioned above, density operators are powerful tools for describing subsystems of composite systems.

Suppose we have physical systems A and B, whose state is described by ρ^{AB}. The reduced density operator for system A is defined by

$$\rho^A \coloneqq \mathrm{tr}_B(\rho^{AB})$$

where tr_B is a map of operators known as the partial trace over system B which is defined by

$$\begin{aligned}\mathrm{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) &= |a_1\rangle\langle a_2|\,\mathrm{tr}(|b_1\rangle\langle b_2|) \\ &= |a_1\rangle\langle a_2|\langle b_2|b_1\rangle\end{aligned}$$

Hence, consider the Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and the reduced density operator of its first qubit

$$\begin{aligned}\rho &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}\frac{\langle 00| + \langle 11|}{\sqrt{2}} \\ \rho^1 &= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \\ &= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \\ &= \frac{I}{2}\end{aligned}$$

Oddly, $\mathrm{tr}\left(\frac{I^2}{4}\right) = 1/2 < 1$ so the first qubit is in a mixed state despite the system as a whole being in a pure state. This is another hallmark of quantum entanglement.

Example 2.1.8. *For each of the four Bell states, we can find the reduced density operator for each qubit*

First, $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

$$\begin{aligned}\rho &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}\frac{\langle 00| + \langle 11|}{\sqrt{2}} \\ \rho^1 &= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \\ &= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2} \\ \rho^2 &= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \\ &= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2}\end{aligned}$$

The remaining three are similar.

2.1.4 Quantum Teleportation

Quantum teleportation is a procedure for sending quantum information from Alice to Bob, given that Alice and Bob share an EPR pair, and have a classic communications channel. Recall that the need for Alice to communicate her result to Bob prevents faster than light communication.

The state to be teleported is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. We can use the circuit shown in the figure below to perform this telerportation, with inputs $|\psi\rangle|\beta_{00}\rangle$ where $|\beta_{00}\rangle$ is the Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Hence,

$$|\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\Big]$$

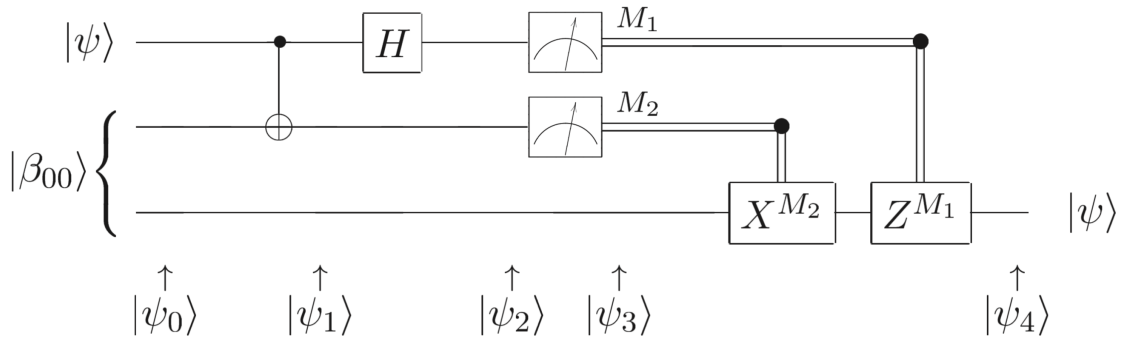


Figure 2.1: Two top lines are Alice's system and bottom is Bob's

Recall the controlled-NOT (CNOT) takes $|a\rangle|b\rangle$ to $|a\rangle|b \oplus a\rangle$. The other gates in the circuit are summarized in the diagram below.

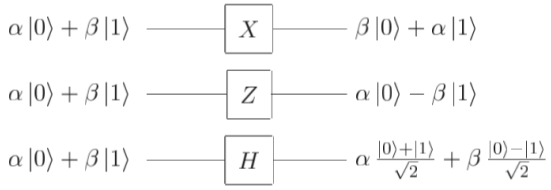


Figure 2.2: Basic gates

So, the first two qubits belong to Alice and the third to Bob. Alice sends her qubits through a CNOT obtaining

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\Big]$$

Then, Alice's first qubit is sent through a Hadamard gate which gives

$$
\begin{aligned}
|\psi_2\rangle &= \frac{1}{2}\Big[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\Big] \\
&= \frac{1}{2}\Big[\,|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)\Big]
\end{aligned}
$$

Now, observe that each grouping in this expression has Alice's bits in a different state ($|00\rangle, |01\rangle, |10\rangle, |11\rangle$), each of which Alice may observe after a measurement. Curiously, each of these groupings has a unique corresponding state for Bob's qubits. Hence, we know the state of Bob's qubits given knowledge of the outcome of Alice's measurement.

Furthermore, note that each of the possible states of Bob's qubits after Alice's measurements can be readily transformed to $|\psi\rangle$. Consider the four cases

1. Alice measures 00. Hence, Bob's state is already $|\psi\rangle$.
2. Alice measures 01. Hence, Bob's state is $\alpha\,|1\rangle + \beta\,|0\rangle$. So, just apply the X gate.
3. Alice measures 10. Hence, Bob's state is $\alpha\,|0\rangle - \beta\,|1\rangle$. So, just apply the Z gate to flip the second sign.
4. Alice measures 11. Hence, Bob's state is $\alpha\,|1\rangle - \beta\,|0\rangle$. So, apply the X gate to flip the bits, then the Z gate to flip the second sign.

So that's what the notation in the circuit above means, we apply X or Z to Bob's qubits to recover $|\psi\rangle$ depending on the outcome of Alice's measurement.

Pretty cool, right? Let's look at this a level deeper using the density operator formalism we've developed. Each of the 4 cases have probability $\frac{1}{4}$ of occurring after the measurement. Hence, the density operator is given by

$$
\begin{aligned}
\rho =& \frac{1}{4}\Big[\,|00\rangle\langle 00|\,(\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) + |01\rangle\langle 01|\,(\alpha\,|1\rangle + \beta\,|0\rangle)(\alpha^*\langle 1| + \beta^*\langle 0|) \\
&+ |10\rangle\langle 10|\,(\alpha\,|0\rangle - \beta\,|1\rangle)(\alpha^*\langle 0| - \beta^*\langle 1|) + |11\rangle\langle 11|\,(\alpha\,|1\rangle - \beta\,|0\rangle)(\alpha^*\langle 1| - \beta^*\langle 0|)\Big]
\end{aligned}
$$

So, the reduced density operator of Bob's system is

$$
\begin{aligned}
\rho^B =& \frac{1}{4}\Big[\,\langle 00|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) + \langle 01|01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle)(\alpha^*\langle 1| + \beta^*\langle 0|) \\
&+ \langle 10|10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle)(\alpha^*\langle 0| - \beta^*\langle 1|) + \langle 11|11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)(\alpha^*\langle 1| - \beta^*\langle 0|)\Big] \\
=& \frac{1}{4}\Big[(\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) + (\alpha\,|1\rangle + \beta\,|0\rangle)(\alpha^*\langle 1| + \beta^*\langle 0|) \\
&+ (\alpha\,|0\rangle - \beta\,|1\rangle)(\alpha^*\langle 0| - \beta^*\langle 1|) + (\alpha\,|1\rangle - \beta\,|0\rangle)(\alpha^*\langle 1| - \beta^*\langle 0|)\Big] \\
=& \frac{1}{4}\Big[2(\alpha^*\alpha + \beta^*\beta)\,|0\rangle\langle 0| + 2(\alpha^*\alpha + \beta^*\beta)\,|1\rangle\langle 1|\Big] \\
=& \frac{I}{2}
\end{aligned}
$$

by $|\alpha|^2 + |\beta|^2 = 1$ and completeness.

Hence, the state of Bob's system after Alice has performed the measurement (but before Bob has learned the measurement result) is $I/2$ which has no dependence upon the state $|\psi\rangle$ being teleported. Therefore, any measurements performed by Bob will contain no information about $|\psi\rangle$, so information being communicated is dependent on the classical communication channel, implying that the speed of light limit is obeyed.

2.1.5 The Schmidt Decomposition and purifications

Schmidt Decomposition theorem says given a pure state $|\psi\rangle$ in a composite system AB, then there are orthonormal states $|i_A\rangle$ and $|i_B\rangle$ in A and B, respectively, such that

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$

where λ_i is nonnegative real and $\sum_i \lambda_i^2 = 1$.

One readily seen implication is that the spectra of ρ^A and ρ^B are the same, given a pure state in composite system AB.

A second technique is purification. Suppose we are given a state ρ^A of system A. We can then introduce another system R and define a pure state $|AR\rangle$ for the joint system AR such that $\rho^A = \mathrm{tr}_R(|AR\rangle \langle AR|)$. R is simply a reference and has no physical significance, the point is that we can associate pure states with mixed states.

2.1.6 EPR and the Bell Inequality

Imagine we perform the following measurement. Charlie prepares a quantum system of two qubits in the state

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

He passes the first bit to Alice and second to Bob. They perform measurements of the following observables

$$\begin{aligned} Q &= Z_1 \\ R &= X_1 \\ S &= \frac{-Z_2 - X_2}{\sqrt{2}} \\ T &= \frac{Z_2 - X_2}{\sqrt{2}} \end{aligned}$$

Alice decides randomly to measure either Q or R once she receives the qubit and similarly Bob decides randomly whether to measure S or T. They perform these measurements at the same time.

Hence, there are 4 combinations of Alice-Bob measurements. We can calculate and show that

$$\langle QS\rangle = \frac{1}{\sqrt{2}}$$
$$\langle RS\rangle = \frac{1}{\sqrt{2}}$$
$$\langle RT\rangle = \frac{1}{\sqrt{2}}$$
$$\langle QT\rangle = \frac{1}{\sqrt{2}}$$

Proof. □

And so $\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2}$. This violates Bell's inequality, derived in the text, which says that this value should never exceed 2.

Bell's inequality requires assuming that Q, R, S, T have definite values before the Alice-Bob measurements (realism). Additionally, we assumed that Alice performing the measurement does not influence the result of Bob's measurement (locality). Hence, at least one of these assumptions must be incorrect, since experimentation confirms this quantum picture.

2.1.7 No-cloning Theorem

It is impossible to copy an unknown quantum state.

Proof. Suppose we have a quantum machine with two slots labelled A and B. Slot A starts out with unknown state $|\psi\rangle$ which is two be copied to B. Assume that B starts out with some pure state $|s\rangle$.

Hence, the initial state of the machine is $|\psi\rangle\,|s\rangle$. So, some unitary evolution U now effects the copying procedure

$$U(|\psi\rangle\,|s\rangle) = |\psi\rangle\,|\psi\rangle$$

Suppose this works for two particular states $|\psi\rangle$ and $|\varphi\rangle$. Hence,

$$U(|\psi\rangle\,|s\rangle) = |\psi\rangle\,|\psi\rangle$$
$$U(|\varphi\rangle\,|s\rangle) = |\varphi\rangle\,|\varphi\rangle$$

Hence, take the inner product of the two equations and

$$(\langle\varphi|\psi\rangle\,\langle s|s\rangle)U^\dagger U = \langle\varphi|\psi\rangle$$
$$\langle\psi|\varphi\rangle\,\langle\psi|\varphi\rangle = |\,\langle\varphi|\psi\rangle\,|^2$$

Hence, either $\langle\varphi|\psi\rangle$ is 0 or 1. Thus, either $|\psi\rangle = |\varphi\rangle$ (a contradiction to assuming they're distinct) or the two states are orthogonal.

Therefore, a cloning device can only clone states which are orthogonal to one another and so a general quantum cloning device is impossible. □

2.2 Quantum Circuits

Reference: Chapter 4 of [30]

2.2.1 Single Qubit Operations

A single qubit in the state $a|0\rangle + b|1\rangle$ can be visualized as a point (θ, φ) on the unit sphere, where $a = \cos(\theta/2), b = e^{i\varphi} sin(\theta/2)$. This is called the Bloch sphere representation and $(\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$ is called the Bloch vector.

Proposition 2.2.1. *Let $x \in \mathbb{R}$ and A be a matrix that satisfies $A^2 = I$. We can show that*

$$\exp(iAx) = \cos(x)I + i\sin(x)A$$

Proof. From the power series definition of e^z, we have that

$$\begin{aligned}
\exp(iAx) &= \sum_{n=0}^{\infty} \frac{(iAx)^n}{n!} \\
&= \sum_{n=0}^{\infty} \frac{(iAx)^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{(iAx)^{2n+1}}{(2n+1)!} \\
\sum_{n=0}^{\infty} \frac{(iAx)^{2n}}{(2n)!} &= \sum_{n=0}^{\infty} \frac{i^{2n}A^{2n}x^{2n}}{(2n)!} \\
&= \sum_{n=0}^{\infty} \frac{(-1)^{2n}Ix^{2n}}{(2n)!} \\
&= I\sum_{n=0}^{\infty} \frac{(-1)^{2n}x^{2n}}{(2n)!} = \cos(x)I \\
\sum_{n=0}^{\infty} \frac{(iAx)^{2n+1}}{(2n+1)!} &= \sum_{n=0}^{\infty} \frac{i^{2n+1}A^{2n+1}x^{2n+1}}{(2n+1)!} \\
&= \sum_{n=0}^{\infty} \frac{i(-1)^{2n+1}Ax^{2n+1}}{(2n+1)!} \\
&= iA\sum_{n=0}^{\infty} \frac{(-1)^{2n+1}x^{2n+1}}{(2n+1)!} = i\sin(x)A
\end{aligned}$$

□

X, Y, Z give rise to three useful classes of unitary matrices when they are exponentiated, the rotation operators about $\hat{x}$, $\hat{y}$, and $\hat{z}$,

$$\begin{aligned}
R_x(\theta) &\equiv e^{-i\theta X/2} \\
R_y(\theta) &\equiv e^{-i\theta Y/2} \\
R_z(\theta) &\equiv e^{-i\theta Z/2}
\end{aligned}$$

We can use the above proposition to write the above equations more conveniently.

Proposition 2.2.2. *$(\hat{n}\cdot\hat{\sigma})^2 = I$, which we can use to conclude that*

$$R_n(\theta) \equiv \exp(-i\theta n\cdot\sigma/2) = \cos(\theta/2)I - i\sin(\theta/2)(n_xX + n_yY + n_zZ)$$

Proof. Evidently, $\hat{n}\cdot\hat{\sigma} = (n_xX+n_yY+n_zZ)$ so, recalling that distinct Pauli matrices anti-commute,

$$\begin{aligned}(n_xX + n_yY + n_zZ)^2 &= n_x^2X^2 + n_xn_yXY + n_xn_zXZ + n_xn_yYX + n_y^2Y^2 + n_yn_zYZ + n_xn_zZX + n_yn_zZY + n_zZ^2\\ &= (n_x^2 + n_y^2 + n_z^2)I + n_xn_z(XZ + ZX) + n_yn_z(YZ + ZY) + n_xn_y(XY + YX)\\ &= (n_x^2 + n_y^2 + n_z^2)I = I\end{aligned}$$

because $\hat{n}$ is a unit vector.
Therefore, using the above proposition, if we let $A = \hat{n}\cdot\hat{\sigma}$, then the result follows directly. □

Lemma 2.2.3. *Suppose U is a unitary operation on a single qubit. Then there exist real numbers $\alpha, \beta, \gamma, \delta$ such that*

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos(\gamma/2) & -e^{i(\alpha-\beta/2+\delta/2)}\sin(\gamma/2) \\ e^{i(\alpha+\beta/2-\delta/2)}\sin(\gamma/2) & e^{i(\alpha+\beta/2+\delta/2)}\cos(\gamma/2)\end{bmatrix}$$

Theorem 2.2.4. *Suppose U is a unitary operation on a single qubit. Then there exist real numbers $\alpha, \beta, \gamma, \delta$ such that*

$$U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta).$$

Corollary 2.2.4.1. *Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha}AXBXC$, where α is some overall phase factor.*

2.3 Quantum Fourier Transform

Reference: Chapter 5 of [30]

2.3.1 Quantum Fourier Transform

The quantum fourier transform on an orthonormal basis $|0\rangle, \cdots, |N-1\rangle$ is defined to be a linear operator with the following action on the basis states,

$$|j\rangle \to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle$$

Example 2.3.1. *We can explicitly compute the Fourier transform of the n qubit state $|00\cdots0\rangle$.*

Proof. $|00\cdots0\rangle$ corresponds to state $|0\rangle$ in the size $N = 2^n$ computational basis. Hence, using the formula above we have

$$\begin{aligned}|0\rangle &\to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle \\ &= \frac{|0\rangle + |1\rangle + \cdots + |N-1\rangle}{\sqrt{N}}\end{aligned}$$

□

We can derive an alternative product representation of the quantum fourier transform. First, represent some state $|j\rangle$ using its binary representation $j = j_1 j_2 \cdots j_n$, $j_i \in \{0, 1\}$. Then,

$$|j_1, \cdots, j_n\rangle \to \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle)}{2^{n/2}}$$

So, define the unitary transformation

$$R_k = \begin{bmatrix}1 & 0\\ 0 & e^{2\pi i/2^k}\end{bmatrix} \tag{2.2}$$

Then, using the circuit below, we can see that this transformation is correctly implemented.

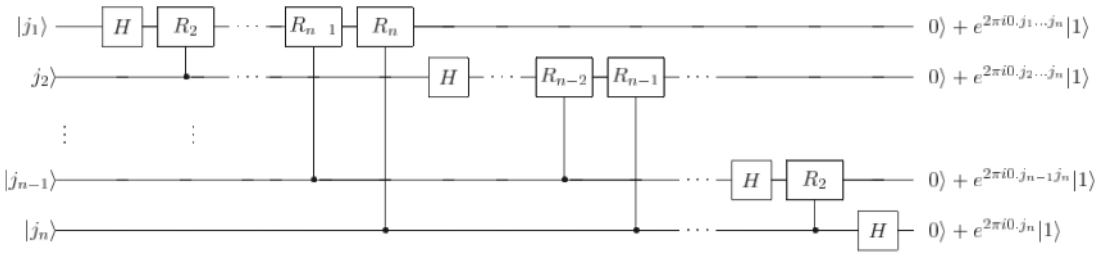


Figure 5.1. Efficient circuit for the quantum Fourier transform. This circuit is easily derived from the product representation (5.4) for the quantum Fourier transform. Not shown are swap gates at the end of the circuit which reverse the order of the qubits, or normalization factors of $1/\sqrt{2}$ in the output.

Furthermore, the gate complexity is $O(n^2)$ as opposed to $O(n2^n)$, classically.

2.3.2 Quantum Phase Estimation Algorithm

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$, where the value of φ is unknown.

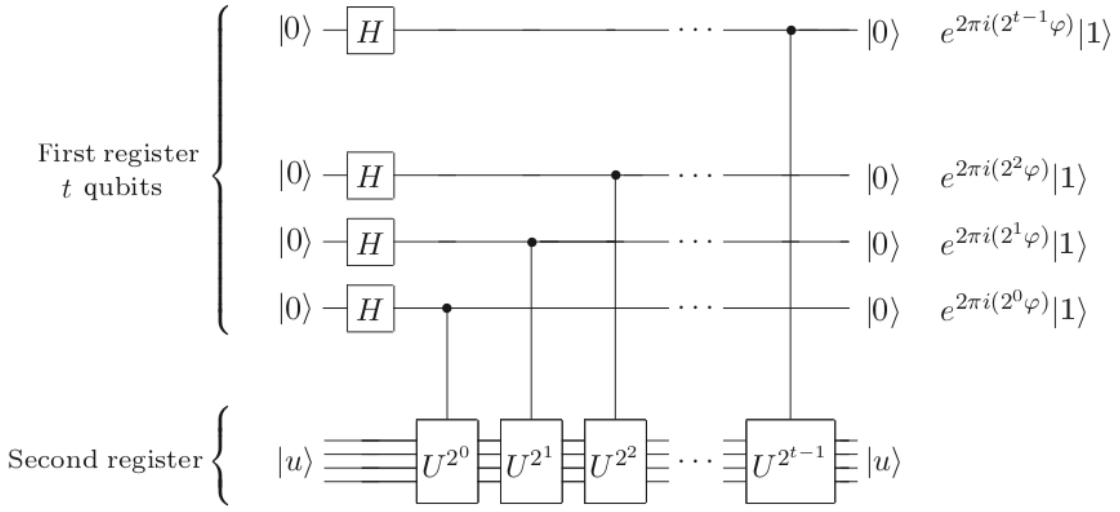


Figure 5.2. The first stage of the phase estimation procedure. Normalization factors of $1/\sqrt{2}$ have been omitted, on the right.

Then, observe that the circuit above gives the state

$$\frac{1}{2^t}(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle)(|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle)\cdots(|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\cdots\varphi_t}|1\rangle)$$

Hence, we can apply the inverse QFT and get the state $|\varphi_1\cdots\varphi_t\rangle$, which is an approximation of φ, whose accuracy is dependent on the size of t.

Therefore, the complexity of this algorithm is essentially that of the inverse Fourier transform, $O(t^2)$. This assumes that each controlled-U^{2^j} operation is given by an oracle, which may not hold in practice. Furthermore, we also assume that we can prepare $|u\rangle$ efficiently, which also may not hold in practice. Hence, we often require workarounds to these problems in our applications of Phase Estimation.

Example 2.3.2. *The effect of the sequence of controlled-U operations like that in the figure is to take the state $|j\rangle|u\rangle$ to $|j\rangle U^j|u\rangle$. (Note that this does not depend on $|u\rangle$ being an eigenstate of U.)*

Proof. Consider an arbitrary j in its binary representation $j_0 j_1 \cdots j_{t-1}$ where $j_i \in \{0,1\}$. Hence, for each $|j_i\rangle$, the control-U acts on $|j_i\rangle|u\rangle$ such that $|j_i\rangle|u\rangle \mapsto |j_i\rangle U^{j_i 2^i}|u\rangle$. Therefore, the final state is given by

$$\begin{aligned}|j_0\rangle\cdots|j_{t-1}\rangle U^{j_0 2^0}\cdots U^{j_{t-1}2^{t-1}}|u\rangle &= |j\rangle U^{j_0 2^0}\cdots U^{j_{t-1}2^{t-1}}|u\rangle \\ &= |j\rangle U^{j_0 2^0 + j_{t-1}2^{t-1}}|u\rangle \\ &= |j\rangle U^j|u\rangle\end{aligned}$$

□

2.4 Quantum Search Algorithms

Reference: Chapter 6 of [30]

2.4.1 Grover's Algorithm and Amplitude Amplification

Suppose we wish to search a space of elements of size N. Clearly this problem is $\Omega(N)$, classically. Rather than searching the elements directly, we can focus on "searching" their indices which are labelled $[0, N-1]$ by using an oracle. So, let $x \in [0, N-1]$ and $|q\rangle$ be an ancillary qubit. Define $f(x) = 1$ if the index is the index of the solution and $f(x) = 0$ otherwise. An oracle is a unitary operation, O, which acts on the computation basis as

$$|x\rangle |q\rangle \rightarrow^{O} |x\rangle |q \oplus f(x)\rangle$$

Hence, if we let $|q\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$, then we can rewrite this transformation as

$$|x\rangle |-\rangle \rightarrow^{O} (-1)^{f(x)} |x\rangle |-\rangle$$

Grover [20] came up with a quantum algorithm that finds a solution with high probability using $O(\sqrt{N})$ oracle queries (which is known to be optimal on a quantum computer [30]).

For $N = 2^n$, the grover iteration can be given by the linear transformation $G = (2 |\psi\rangle \langle\psi| - I)O$ where $|\psi\rangle$ is the equally weighted superposition of states.

So, assuming that the number of solutions $M = 1$, Grover's algorithm essentially prepares N qubits in state $|\psi\rangle |-\rangle$ and then applies G for $\frac{\pi}{4}\sqrt{N}$ iterations.

However, if the number of solutions $M \geq 1$ is unknown, then a variant, known as amplitude amplification [7], can be used to find a solution in the solution subspace with high probability using $O(\sqrt{N/M})$ queries.

2.5 Quantum Information Theory

Reference: Chapter 12 of [30]

Theorem 2.5.1. *Holevo's Theorem*

Let $\{\rho_1, \rho_2, ..., \rho_n\}$ be a set of mixed states and let ρ_X be one of these states drawn according to the probability distribution $P = \{p_1, p_2, \cdots, p_n\}$.

Then, for any measurement described by POVM elements E_Y and performed on $\rho = \sum_X p_X \rho_X$, the amount of accessible information about the variable X knowing the outcome Y of the measurement is bounded from above as follows:

$$I(X:Y) \leq S(\rho) - \sum_i p_i S(\rho_i)$$

where $\rho = \sum_i p_i \rho_i$ and $S(\cdot)$ is the von Neumann entropy.

The quantity on the right hand side of this inequality is called the Holevo information or Holevo χ quantity:

$$\chi := S(\rho) - \sum_i p_i S(\rho_i)$$

2.5.1 Pretty Good Measurement (PGM)

Given a density matrix ensemble $\mathcal{E} = \{p_i, \sigma_i\}$ and a quantum state ρ we are promised that ρ is in state σ_i with probability p_i. In the general case we have $i \in [m]$ and of course $\sum_{i=1}^{m} p_i = 1$. Our goal is then to successfully identify which of the σ_i that our state ρ is actually in. This is known as Quantum Hypothesis Testing.

In some sense, thinking back to Holevo's Theorem (Theorem 2.5.1), this is related to Bob attempting to access information transported from Alice that is given from the distribution above.

Hence, we perform a maximization with respect to both the probabilities on each state as well as with respect to any randomness that our approach employs. We then must choose a Quantum POVM $\{E_i\}$ that carries put a measurement and maximizes our probability of getting the state right.

So say we pick a POVM. Hence, we know that

$$\Pr(Success) = \sum_i p_i \operatorname{Tr}(\sigma_i E_i)$$

So this is the quantity that we seek to maximize.

We've shown above that the trace distance provides the solution for $m = 2$. As it turns out for $m > 2$ this is not an easy problem. However, PGM provides a sound approximation:

Intuitively, it might seem reasonable to simply choose

$$E_i = p_i \sigma_i$$

Unfortunately, then, $\sum_i E_i \neq I$. Well, one case we may think about is if we can guarantee σ_i is a the sum of pure states from an orthonormal basis. In which case, let $S = \sum_i \sigma_i$ and we choose

$$E_i = S^{1/2} \sigma_i S^{1/2}$$

Then we have

$$\operatorname{tr}(E_i \sigma_i) = \operatorname{tr}(\sigma_i) = 1$$

by orthonormality. Inspired by this, define the PGM POVM to be

$$E_i = S^{-1/2} p_i \sigma_i S^{-1/2}$$

for our original problem. Positive semidefiniteness is clear, so it remains to show that we have completeness

$$\begin{aligned} \sum_i E_i &= \sum_i S^{-1/2} p_i \sigma_i S^{-1/2} \\ &= S^{-1/2} \sum_i p_i \sigma_i S^{-1/2} \\ &= S^{-1/2} S S^{-1/2} = I \end{aligned}$$

Theorem 2.5.2. *Let $\Pr_{opt}(\mathcal{E})$ by the optimal success probability for our quantum hypothesis testing problem. Define $\Pr_{PGM}(\mathcal{E})$ to be the average success probability using the PGM POVM. Then,*

$$Pr_{opt}(\mathcal{E})^2 \leq Pr_{PGM}(\mathcal{E}) \leq Pr_{opt}(\mathcal{E})$$

2.5.2 Trace Distance

Definition 2.5.3. *Trace Distance*

The trace distance $T(\cdot,\cdot)$ is a metric on the space of density operators and gives a measure of distinguishability between states. In particular, let ρ,σ be density operators,

$$\begin{aligned} T(\rho,\sigma) &= \frac{1}{2}\operatorname{Tr}\left[\sqrt{(\rho-\sigma)^2}\right] \\ &= \frac{1}{2}\sum_i |\lambda_i| \end{aligned}$$

where λ_i are the eigenvalues of Hermitian $\rho-\sigma$.

Hence, it is simply the trace norm of the positivization of the difference of matrices.

Lemma 2.5.4. *For any states ρ,σ one may write $\rho-\sigma = Q-S$ where Q and S are positive operators with support on orthogonal vector spaces (Exercise 9.7 [30])*

Proof. ρ,σ are p.s.d operators. Hence, $\rho-\sigma$ is Hermitian, so we can write $\rho-\sigma = \sum_i \lambda_i |u_i\rangle\langle u_i|$ where $\{u_i\}$ is an orthonormal basis of the Hilbert space, by spectral theorem. Now, we can decompose the eigenbasis into positive and negative components. Then, $\rho-\sigma = \sum_i \lambda_i^+ |u_i\rangle\langle u_i| + \sum_j \lambda_j^- |u_j\rangle\langle u_j|$ where $\lambda_i^+ > 0, \lambda_j^- < 0$. Since, each component partitions the vector space (other than at the additive identity) by the orthogonality condition, this is a direct sum. □

Lemma 2.5.5. *The maximum probability of distinguishing between two states with an optimal measurement is given by*

$$1/2[1+T(\rho_1,\rho_2)]$$

Proof. Say that we have the ensemble $\{(p_1,\rho_1),(p_2,\rho_2)\}$. We seek to define a POVM $\{E_1,E_2\}$ where E_1 indicates ρ_1 and similarly for ρ_2. hence the probability of success is given by

$$\begin{aligned} \Pr_{\max} &= \max_{E_1,E_2} p_1 \operatorname{Tr}[E_1\rho_1] + p_2\operatorname{Tr}[E_2\rho_2] \\ &= \max_{E_1} p_1\operatorname{Tr}[E_1\rho_1] + p_2\operatorname{Tr}[(I-E_1)\rho_2] && \text{(completeness of POVM)} \\ &= \max_{E_1} p_2\operatorname{Tr}[\rho_2] + \operatorname{Tr}[E_1(p_1\rho_1 - p_2\rho_2)] && \text{(linearity of trace)} \\ &= \max_{E_1}\Big(p_2 + \operatorname{Tr}[E_1(p_1\rho_1-p_2\rho_2)]\Big) && (\operatorname{Tr}(\rho)=1 \text{ for any density operator}) \end{aligned}$$

Therefore, the optimal projection E_1 is onto the positive eigenspace of $(p_1\rho_1 - p_2\rho_2)$. In which case, recalling that ρ_i are p.s.d, $E_1(p_1\rho_1-p_2\rho_2)] = p_1\rho_1$ and so

$$= \Big(p_2 + \operatorname{Tr}[p_1\rho_1]\Big)$$

We did implicitly assume that $E_1+E_2 = I$ where we could've had an additional indeterminate E_3. However, the proof would still follow in any case ([30]). □

Corollary 2.5.5.1. *Consider attempting to distinguish two pure states* $|\psi_0\rangle, |\psi_1\rangle$*. Then, we will distinguish correctly with probability at most* $1/2[1+\sqrt{1-|\langle\psi_0|\psi_1\rangle|^2}]$*.*

Equivalently, if we can distinguish between the two states w.p. $1-\delta$*, then* $|\langle\psi_0|\psi_1\rangle| \leq 2\sqrt{\delta(1-\delta)}$*.*

Proof. Applying the previous Lemma, we have maximum probability

$$1/2[1+T(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|)]$$

So, write $|\psi_1\rangle = \cos(\theta)|\psi_0\rangle + e^{i\varphi}\sin(\theta)|\psi_0^\perp\rangle$. Hence,

$$|\psi_1\rangle\langle\psi_1| = \cos^2(\theta)|\psi_0\rangle\langle\psi_0| + \sin^2(\theta)|\psi_0^\perp\rangle\langle\psi_0^\perp|$$
$$+e^{i\varphi}\cos(\theta)\sin(\theta)|\psi_0^\perp\rangle\langle\psi_0| + e^{-i\varphi}\cos(\theta)\sin(\theta)|\psi_0\rangle\langle\psi_0^\perp|$$

Since trace is basis-independent, we can write $|\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1|$ in the above used orthogonal basis. This gives us characteristic polynomial

$$\begin{aligned}
0 &= (1-\cos^2(\theta)-\lambda)(-\sin^2(\theta)-\lambda) - \cos^2(\theta)\sin^2(\theta) \\
&= (\sin^2(\theta)-\lambda)(-\sin^2(\theta)-\lambda) - \cos^2(\theta)\sin^2(\theta) \\
&= -\sin^4(\theta) + \lambda^2 - \cos^2(\theta)\sin^2(\theta) \\
&= -\sin^2(\theta) + \lambda^2
\end{aligned}$$

So, $\lambda = \pm|\sin(\theta)|$. Therefore, since the trace distance is the absolute sum of the eigenvalues of this difference,

$$T(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) = 2|\sin(\theta)| sam$$

and indeed

$$|\langle\psi_0|\psi_1\rangle|^2 = |\cos(\theta)|^2 \Rightarrow \sqrt{1-|\langle\psi_0|\psi_1\rangle|^2} = |\sin(\theta)|$$

as desired. □

Lemma 2.5.6. *Let* A, B, C *by symmetric* $d \times d$ *matrices satisfying* $A \succeq 0$ *and* $B \preceq C$*. Hence,* $\mathrm{Tr}(AB) \leq \mathrm{Tr}(AC)$

Proof. Write A in its spectral decomposition $A = \sum \lambda_i |i\rangle\langle i|$, invoking Spectral Theorem (A.1.5). Hence,

$$\begin{aligned}
\mathrm{Tr}(AB) &= \mathrm{Tr}\Big(\sum \lambda_i |i\rangle\langle i| B\Big) \\
&= \sum \lambda_i \mathrm{Tr}(|i\rangle\langle i| B) && \text{(linearity of trace)} \\
&= \sum \lambda_i \mathrm{Tr}(\langle i| B |i\rangle) && \text{(cyclic property of trace)} \\
&\leq \sum \lambda_i \mathrm{Tr}(\langle i| C |i\rangle) \\
&= \sum \lambda_i \mathrm{Tr}(|i\rangle\langle i| C) = \mathrm{Tr}\Big(\sum \lambda_i |i\rangle\langle i| C\Big) = \mathrm{Tr}(AC)
\end{aligned}$$

□

Corollary 2.5.6.1. *If* $A, B \succeq 0$, *then* $\operatorname{Tr}(AB) \leq \|B\|_2 \operatorname{Tr}(A)$

Proof. Note that the singular values of B coincide with the eigenvalues of B since $B^\dagger B = B^2$ and $B \succeq 0 \Rightarrow \lambda_i(B) \geq 0, \forall i$. So, let $C = \|B\|_2 I$ which then trivially satisfies $\lambda_i(C) = \lambda_{\max}(B), \forall i$ since C is the diagonal matrix with diagonal values all equal to $\lambda_{\max}(B)$. Therefore, $B \preceq C$. So, we can simply apply 2.5.6 above,

$$\begin{aligned}\operatorname{Tr}(AB) &\leq \operatorname{Tr}(AC) \\ &= \operatorname{Tr}\left(A\|B\|_2 I\right) \\ &= \|B\|_2 \operatorname{Tr}(A)\end{aligned}$$

□

Chapter 3

Learning Theory and Mathematical Methods

Machine learning explores the study and construction of algorithms that are capable of finding patterns in data. Hence, this entails studying the ability of learning models to capture these patterns and generalize, as one would in statistical learning theory, in addition to studying model efficiency, enabled by computational complexity theory.

It is often natural to describe these patterns as unknown functions, as one does in computational learning theory. For example, if we are learning a classification function (say handwritten digit classification), then our function acts on some space of examples (say the handwriting in terms of pixels) and returns a label (the corresponding digit). Hence, the first two sections of this chapter are dedicated to tools and formalism for this view of machine learning.

On the other hand, many of the widely used supervised and unsupervised machine learning algorithms amount to linear algebraic data analysis techniques. For example, consider that ordinary least squares regression and ridge regression can be given in terms of a closed-form product of matrices and matrix inverses. Similarly, principal component analysis on a feature matrix A is essentially solving for the largest-eigenvalue eigenvectors of its singular matrix $A^\dagger A$. For some machine learning algorithms, such as SVM, the most computationally expensive steps involve solving linear and nonlinear convex programs. Nevertheless, we often rely on linear algebraic subroutines to solve these optimization problems.

We will show in Section 4.7 that it is reasonable to compare quantum algorithms with quantum state preparation to classical algorithms with sample and query access to input. Hence, we survey ideas from randomized linear algebra that rely on this sort of sample and query access. Then, in Section 4.7 we will use these concepts to show that many quantum machine-learning algorithms that solve linear algebra problems in low-dimensional spaces have a classical, randomized analog.

3.1 Boolean Fourier Analysis

A boolean function is a function

$$f : \{0,1\}^n \to \{0,1\}$$

or by relabeling

$$f : \{-1, +1\}^n \to \{-1, +1\}$$

The domain of a boolean function is the "Hamming cube", $\mathbb{B}^n$.

Definition 3.1.1. *Let $S \subseteq [n]$ with $n \in \mathbb{Z}$. Then,*

$$\chi_S(x) := \prod_{i \in S} x_i \qquad \text{(with } x^{\emptyset} = 1 \text{ by convention)}$$

Hence, it is clear that we can view $\chi_S(x) : \{-1, +1\}^n \to \{-1, +1\}$ as computing the parity of x over the set S.

Theorem 3.1.2. *Every function $f : \{-1, +1\} \to \mathbb{R}$ can be uniquely expressed as a multilinear polynomial,*

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S)\chi_S(x)$$

We denote this expansion as the Fourier expansion of f, and term the real coefficent $\hat{f}(S)$ the Fourier coefficient of f on S.

Definition 3.1.3. *Define an inner product $\langle \cdot, \cdot \rangle$ on $f, g : \{-1, +1\} \to \mathbb{R}$ by*

$$\begin{aligned} \langle f, g \rangle &= 2^{-n} \sum_{x \in \{-1,+1\}^n} f(x)g(x) \\ &= E_{x \sim \{-1,+1\}^n}[f(x)g(x)] \end{aligned}$$

where $x \sim \{-1, +1\}^n$ denotes that x is chosen uniformly at random from $\{-1, +1\}^n$.

Theorem 3.1.4. *The set of all functions $f : \{-1, +1\}^n \to \mathbb{R}$ forms a vector space V such that $\dim V = 2^n$. The $\{\chi_S\}, S \subseteq [n]$ form an orthonormal basis for V.*

Proof. Let f, g both map $\{-1, +1\}^n$ to $\mathbb{R}$. Clearly, by Theorem 3.1.2, $h = \alpha f + g$ for $\alpha \in \mathbb{R}$ is also a boolean function $h : \{-1, +1\}^n \to \mathbb{R}$. Hence, we have a vector space V of boolean functions and $\dim V = 2^n$ because we can describe a function by how it acts on each point of the Hamming cube. So, we can canonically identify $V \cong \mathbb{R}^{2^n}$. Because the number of parity functions is 2^n and they are independent, we conclude that the χ_S form a basis of V.

If this basis is indeed orthonormal, then the Definition above requires

$$\langle \chi_S, \chi_T \rangle = \begin{cases} 1, S = T \\ 0, S \neq T \end{cases}$$

So, observe that

$$\begin{aligned}\chi_S(x)\chi_T(x) &= \prod_{i\in S}\prod_{j\in T} x_i x_j \\ &= \prod_{i\in S\cap T} x_i^2 \prod_{j\in S\Delta T} x_i \\ &= \chi_{S\Delta T}(X)\end{aligned}$$

where $S\Delta T$ is the symmetric difference $(S\cup T)\setminus(S\cap T)$.

Now, we claim that $E[\chi_{S\Delta T}] = 1$ iff $S\Delta T = \emptyset$ and 0 otherwise. Indeed, we've defined that $\chi_\emptyset = 1$ so $E[\chi_\emptyset] = 1$. Otherwise,

$$E[\prod_{i\in S\Delta T} x_i] = \prod_{i\in S\Delta T} E[x_i]$$

by independence of the $\{x_i\}$. But each $E[x_i] = (1/2)(+1) + (1/2)(-1) = 0$. □

Proposition 3.1.5. *For $f : \{-1,+1\}^n \to \mathbb{R}$ and $S \subseteq [n]$, the Fourier coefficient of f on S is given by*

$$\hat{f}(S) = \langle f, \chi_S\rangle = E_{x\sim\{-1,+1\}^n}[f(x)\chi_S(x)]$$

Theorem 3.1.6. *For any $f, g : \{-1,+1\} \to \mathbb{R}$,*

$$\langle f, g\rangle = E_{x\sim\{-1,+1\}^n}[f(x)g(x)] = \sum_{S\in[n]} \hat{f}(S)\hat{g}(S) \qquad \text{(Parseval's Theorem)}$$

Hence,

$$\langle f, f\rangle = \sum_{S\in[n]} \hat{f}(S)\hat{f}(S) = 1 \qquad \text{(Plancherel's Theorem)}$$

3.2 Computational Learning Theory

Computational learning theory addresses the following task: Given a source of "examples" $(x, f(x))$ from an unknown function f, compute a "hypothesis" function h that is good at predicting $f(y)$ on future inputs y.

Definition 3.2.1. *In the PAC ("probably approximately correct") model learning under the uniform distribution on $\{-1,+1\}^n$, a learning problem is identified with a concept class $\mathcal{C}$, which is just a collection of functions $f : \{-1,+1\}^n \to \{-1,+1\}$. A learning algorithm $\mathcal{A}$ for $\mathcal{C}$ is a randomized algorithm which has limited access to an unknown target function $f \in \mathcal{C}$. These two access models, in increasing order of strength are:*

- *"random examples", meaning $\mathcal{A}$ can draw pairs $(x, f(x))$ where $x \in \{-1,+1\}^n$ is uniformly random*

- *"queries", meaning $\mathcal{A}$ can request the value $f(x)$ for any $x \in \{-1,+1\}^n$ of its choice.*

In addition $\mathcal{A}$ is given an accuracy parameter $\epsilon \in [0, 1/2]$ and failure parameter δ. The output of $\mathcal{A}$ is required to be a hypothesis function $h : \{-1,+1\} \to \{-1,+1\}$. We say that A learns $\mathcal{C}$ with error ϵ if for any $f \in \mathcal{C}$, $\mathcal{A}$ outputs an h which is ϵ-close to f, i.e.

$$dist(f,h) \leq \epsilon$$

with probability $\geq 1 - \delta$.

Note that dist is the relative Hamming distance more generally defined as total variation distance 3.3.1.

Clearly, we can learn any such f in $O(2^n)$ time for $\epsilon = 0$ (there are only 2^n hypotheses). If $\mathcal{C}$ is complex, then exponential running time may be the best we can do. Nevertheless, if $\mathcal{C}$ contains relatively "simple" functions then improved bounds are possible. A common way of doing so is discovering "most of" a function's Fourier spectrum.

Definition 3.2.2. *Let $\mathfrak{F}$ be a collection of subsets $S \subseteq [n]$. We say that the Fourier spectrum of $f : \{-1,+1\}^n \to \mathbb{R}$ is ϵ-concentrated on $\mathfrak{F}$ if*

$$\sum_{S \subseteq [n], S \notin \mathfrak{F}} \hat{f}(S)^2 \leq \epsilon$$

Using the notation of the previous section, we can equivalently write

$$Pr_{S \sim S_f}[S \notin \mathfrak{F}] \leq \epsilon$$

where $S \sim S_f$ implies sampling S with probability $\hat{f}(S)^2$.

Proposition 3.2.3. *Given access to random examples from $f : \{-1,+1\}^n \to \{-1,+1\}$, there is a randomized algorithm which takes as input $S \subseteq [n], 0 < \delta, \epsilon \leq 1/2$, and outputs an estimate $\tilde{f}(S)$ for $\tilde{f}(S)$ that satisfies*

$$|\tilde{f}(S) - \hat{f}(S)| \leq \epsilon$$

with probability $\geq 1 - \delta$ in running time $poly(n, 1/\epsilon) \cdot \log(1/\delta)$.

Proof. First, we know that $\hat{f}(S) = \langle f(x), \chi_S(x) \rangle$, recalling that this is an expectation across all $x \in \{-1,+1\}^n$ from the previous section. Hence, given an example $(x_1, f(x_1))$, we can compute $f(x_1)\chi_S(x_1) \in \{-1,+1\}$ to empirically estimate $\hat{f}(S)$. From here, we simply apply a Chernoff bound (Corollary 3.3.4.1) to determine the number of samples required to satisfy our claim.

Say we are given random samples $x_1, \cdots, x_s$. Then, write random variable $X_i = f(x_i)\chi_S(x_i)$ and $X := \sum_i X_i$. Then,

$$\Pr(X - E[X] \geq \epsilon) \leq 2e^{-\frac{s\epsilon^2}{2}}$$

Hence, in order to satisfy that this probability is $\leq \delta$, we require $s = O(\frac{1}{\epsilon^2} \log(1/\delta))$ □

Proposition 3.2.4. *Suppose that $f : \{-1,+1\}^n \to \{-1,+1\}$ and $g : \{-1,+1\}^n \to \mathbb{R}$ satisfy $\|f-g\|_2^2 \leq \epsilon$. Let $h : \{-1,+1\}^n \to \{-1,+1\}$ be defined by $h(x) = sgn(g(x))$. Then,*

$$dist(f,h) \leq \epsilon$$

Proof. Since $|f(x)-g(x)|^2 \geq 1$ whenever $f(x) \neq sgn(g(x))$, we conclude

$$\begin{aligned} dist(f,h) &= Pr_x[f(x) \neq h(x)] \\ &= E_x[1_{f(x)\neq sgn(g(x))}] \\ &\leq E_x[|f(x)-g(x)|^2] = \|f-g\|_2^2 \end{aligned}$$

□

Theorem 3.2.5. *Assume learning algorithm $\mathcal{A}$ has (at least) random sample access to target $f : \{-1,+1\}^n \to \{-1,+1\}$. Suppose that $\mathcal{A}$ can identify a collection $\mathfrak{F}$ of subsets on which f's Fourier spectrum is $\epsilon/2$-concentrated. Then using $poly(|\mathfrak{F}|, n, 1/\epsilon)$ additional time, $\mathcal{A}$ can with high probability output a hypothesis h that is ϵ-close to f*

Proof. For each $S \in \mathfrak{F}$ the algorithm uses Proposition 3.2.3 to produce an estimate $\tilde{f}(S)$ for $\hat{f}(S)$ which satisfies $|\hat{f}(S)-\tilde{f}(S)| \leq \frac{\sqrt{\epsilon}}{2\sqrt{|\mathfrak{F}|}}$ except with probability at most $1/(10|\mathfrak{F}|)$. Overall this requires $poly(|\mathfrak{F}|, n, 1/\epsilon)$ time and all $|\mathfrak{F}|$ estimates have the desired accuracy with probability $\geq 9/10$.

Now, $\mathcal{A}$ forms the real-valued function $g = \sum_{S\in\mathfrak{F}} \tilde{f}(S)\chi_S$ and outputs hypothesis $h = sgn(g)$. By Proposition 3.2.4, it suffices to show that $\|f-g\|_2^2 \leq \epsilon$. Indeed,

$$\begin{aligned} \|f-g\|_2^2 &= \sum_{S\subseteq[n]} \widehat{f-g}(S)^2 && \text{(Parseval's Theorem)} \\ &= \sum_{S\in\mathfrak{F}} (\hat{f}(S)-\tilde{f}(S))^2 + \sum_{S\notin\mathfrak{F}} \hat{f}(S)^2 \\ &\leq \sum_{S\in\mathfrak{F}} (\frac{\sqrt{\epsilon}}{2\sqrt{|\mathfrak{F}|}})^2 + \epsilon/2 && \text{(concentration assumption)} \\ &= \epsilon/4 + \epsilon/2 \leq \epsilon \end{aligned}$$

as desired. This theorem essentially reduces the algorithmic task of learning f to the algorithmic task of identifying a collection $\mathfrak{F}$ on which f's Fourier spectrum is concentrated. □

We've seen that the Fourier spectrum concentration provides a useful notion of the complexity of a *function*. In a more general sense, we can describe the complexity of a *concept class* in terms of a combinatorial parameter known as the VC dimension.

Definition 3.2.6. *(VC Dimension) The VC dimension of $\mathcal{C}$ is the size of the biggest $S \subseteq \{0,1\}^n$ that can be labelled all $2^{|S|}$ ways by concepts from $\mathcal{C}$: for each sequence of $|S|$ binary labels for the elements of S, there is a $c \in \mathcal{C}$ that has that labeling (such an S is said to be shattered by $\mathcal{C}$)*

Example 3.2.7. *The VC dimension of halfspaces in p dimensions is $p+1$*

3.3 Randomized Linear Algebra

3.3.1 Probability Bounds

Definition 3.3.1. *Total Variation Distance.*

Let P and Q be distinct probability measures on a σ-algebra $\mathcal{F}$ of subsets of the sample space Ω. Then, the total variation distance is given by

$$\delta(P, Q) = \sup_{A \in \mathcal{F}} |P(A) - Q(A)|$$

Proposition 3.3.2. *(Markov's Inequality) Let X be a nonnegative random variable. Then,*

$$Pr(X \geq t) \leq \frac{1}{t} E[X]$$

for all $t \geq 0$.

Proposition 3.3.3. *(Chebyshev's Inequality) Let X be a random variable with finite variance $Var(X)$. Then,*

$$Pr(|X - E[X]| \geq t) \leq \frac{1}{t^2} Var[X]$$

for all $t \geq 0.x$

Proposition 3.3.4. *(Hoeffding–Chernoff Inequality)*

Let $X_1, X_2, \cdots, X_s$ be i.i.d real random variables. For any positive, real numbers a, t we have that, from Markov's inequality,

$$\begin{aligned} \Pr\left(\sum_{i=1}^{s} X_i \geq a\right) &\leq e^{-ta} E\left[\prod_{i=1}^{s} e^{tX_i}\right] \\ &= e^{-ta} \prod_{i=1}^{s} E\left[e^{tX_i}\right] \end{aligned}$$

by independence.

Corollary 3.3.4.1. *(Chernoff Bounds) Let $X_1, X_2, \cdots, X_s$ be i.i.d real random variables such that $X_i \in [a_i, b_i]$ with probability 1. Define $X := \sum_{i=1}^{s} X_i$. Then,*

$$\Pr(|X - E[X]| \geq t) \leq 2e^{-\frac{2t^2}{\sum_{i=1}^{n}(b_i - a_i)^2}}$$

Theorem 3.3.5. *(Hoeffding–Chernoff Inequality for matrix-valued random variables) [22]*

Let X be a random variable taking values which are real symmetric $d \times d$ matrices. Suppose $X_1, X_2, \cdots, X_s$ are i.i.d. draws of X. For any positive real numbers a, t, we have

$$\Pr\left(\lambda_{\max}\Big(\sum_{i=1}^{s} X_i\Big) \geq a\right) \leq de^{-ta}\|E[e^{tX}]\|_2^s \tag{3.1}$$

$$\Pr\left(\Big\|\Big(\sum_{i=1}^{s} X_i\Big)\Big\|_2 \geq a\right) \leq de^{-ta}(\|E[e^{tX}]\|_2^s + \|E[e^{-tX}]\|_2^s) \tag{3.2}$$

where $\lambda_{\max}$ is the largest eigenvalue.

Proof. First, we can show that (3.1) $\Rightarrow$ (3.2). By definition of the 2-norm of a matrix,

$$\|\sum_i X_i\|_2 = \max\Big(\lambda_{\max}\Big(\sum_i X_i\Big), \lambda_{\max}\Big(\sum_i (-X_i)\Big)\Big)$$

since it is the square root of the maximum eigenvalue of $(\sum_i X_i^T)\sum_i X_i = (\sum_i X_i)\sum_i X_i$ and hence, equivalently, the maximum absolute value of an eigenvalue of X_i. Therefore, we can simply apply (3.1) to both X_i and $-X_i$ and we get (3.2).

So, we can focus our attention on (3.2). Let $S = \sum_i^s X_i$. Hence,

$$\lambda_{\max}(S) \geq a \Leftrightarrow \lambda_{\max}(tS) \geq ta$$

Furthermore, by considering the power series definition of the exponential,

$$\begin{aligned} &\Leftrightarrow \lambda_{\max}(e^{tS}) \geq e^{ta} \\ &\Rightarrow \mathrm{Tr}\big(e^{tS}\big) \geq e^{ta} \end{aligned}$$

since the trace is the sum of the matrix's eigenvalues. Since $\mathrm{Tr}\big(e^{tS}\big) \geq 0$, we can apply Markov's inequality

$$\Pr\big(\mathrm{Tr}\big(e^{tS}\big) \geq e^{ta}\big) \leq \frac{E[\mathrm{Tr}\big(e^{tS}\big)]}{e^{ta}}$$

Now, we use the following lemma

Lemma 3.3.6. *Golden-Thompson Inequality*
If A and B are Hermitian matrices, then

$$\mathrm{Tr}\big(e^{A+B}\big) \leq \mathrm{Tr}\big(e^A e^B\big)$$

□

Hence, we can let $A = t(\sum_i^{s-1} X_i)$ and $B = tX_s$. Then,

$$E_X\Big[\mathrm{Tr}\big(e^{tS}\big)\Big] \leq E_X\Big[\mathrm{Tr}\Big(e^{t\left(\sum_i^{s-1} X_i\right)} e^{tX_s}\Big)\Big]$$

Since the expectation operator commutes with the summation of the trace by linearity of trace,

$$\begin{aligned}
&= \operatorname{Tr}\left(E_X\left[e^{t\left(\sum_i^{s-1} X_i\right)} e^{tX_s}\right]\right) \\
&= \operatorname{Tr}\left(E_{X_1,X_2,\cdots,X_{s-1}}\left[e^{t\left(\sum_i^{s-1} X_i\right)}\right] E_{X_s}\left[e^{tX_s}\right]\right) \qquad \text{(by independence)}
\end{aligned}$$

Now, we can apply Corollary (2.5.6.1), which gives

$$\begin{aligned}
&\leq \operatorname{Tr}\left(E_{X_1,X_2,\cdots,X_{s-1}}\left[e^{t\left(\sum_i^{s-1} X_i\right)}\right]\right)\left\|E_{X_s}\left[e^{tX_s}\right]\right\|_2 \\
&= \operatorname{Tr}\left(E_X\left[e^{t\left(\sum_i^{s-1} X_i\right)}\right]\right)\left\|E_X\left[e^{tX}\right]\right\|_2 \\
&= E_X\left[\operatorname{Tr}\left(e^{t\left(\sum_i^{s-1} X_i\right)}\right)\right]\left\|E_X\left[e^{tX}\right]\right\|_2
\end{aligned}$$

So we can repeat this process iteratively, peeling an X_i each time from the left term. For clarity, the next step gives,

$$\begin{aligned}
E_X\left[\operatorname{Tr}\left(e^{t\left(\sum_i^{s-1} X_i\right)}\right)\right] &\leq E_X\left[\operatorname{Tr}\left(e^{t\left(\sum_i^{s-2} X_i\right)} e^{tX_{s-1}}\right)\right] \\
&\leq E_X\left[\operatorname{Tr}\left(e^{t\left(\sum_i^{s-2} X_i\right)}\right)\right]\left\|E_X\left[e^{tX}\right]\right\|_2 \qquad \text{(applying (2.5.6.1) again)}
\end{aligned}$$

Therefore, after peeling all terms but the last X_i, we have

$$E_X\left[\operatorname{Tr}(e^{tS})\right] \leq E_X\left[\operatorname{Tr}\left(e^{tX}\right)\right]\left\|E_X\left[e^{tX}\right]\right\|_2^{s-1}$$

Hence, since the trace is the sum of eigenvalues, $\operatorname{Tr}\left(e^{tX}\right) \leq d\lambda_{\max}(e^{tX})$ i.e. the worst case of all d eigenvalues being the max

$$\leq d\left\|E_X\left[e^{tX}\right]\right\|_2^s$$

as desired. □

Lemma 3.3.7. *If $B \in \mathbb{C}^{d\times d}$ is a hermitian matrix for which $\|B\|_2 \leq 1$, then $e^B \leq I + B + B^2$*

Proof. We know that $e^{\lambda_i} \leq 1 + \lambda_i + \lambda_i^2$, $|\lambda_i|^2 \leq 1$. Hence,

$$e^{\lambda_i} |v_i\rangle \langle v_i| \leq (1 + \lambda_i + \lambda_i^2) |v_i\rangle \langle v_i|$$

where $|v_i\rangle$ is the corresponding eigenvector. This then implies

$$\begin{aligned}
e^B &= \sum_{i=1}^{d} e^{\lambda_i} |v_i\rangle \langle v_i| \preceq \sum_{i=1}^{d} (1 + \lambda_i + \lambda_i^2) |v_i\rangle \langle v_i| \\
&= I + B + B^2
\end{aligned}$$

□

3.3.2 Computing Approximate Singular Vectors

Definition 3.3.8. *We have "query access" to $x \in \mathbb{C}^n$ if, given $i \in [n]$, we can efficiently compute x_i. We say that $x \in \mathcal{Q}$.*

Definition 3.3.9. *We have sample **and** query access to $x \in \mathbb{C}^n$ if*

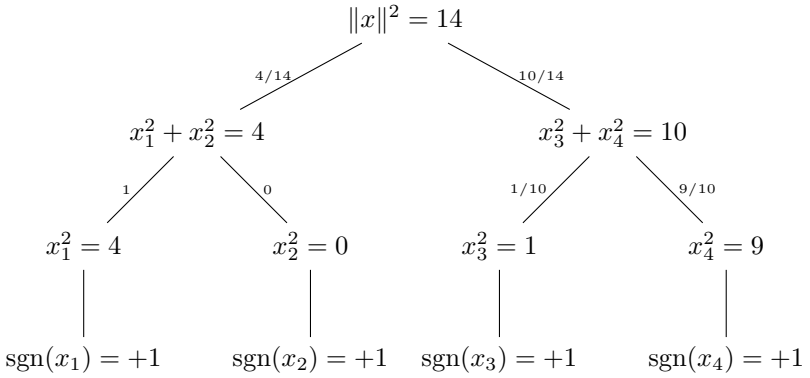
1. *We have query access to x i.e. $x \in \mathcal{Q}$ ($\Rightarrow \mathcal{SQ} \subset \mathcal{Q}$)*
2. *We can produce independent random samples $i \in [n]$ where we sample i with probability $|x_i|^2/\|x\|^2$ and can query for $\|x\|$.*

We say that $x \in \mathcal{SQ}$.

Definition 3.3.10. *For $A \in \mathbb{C}^{m\times n}$, $A \in \mathcal{SQ}$ (by abuse in notation) if*

1. *$A_i \in \mathcal{SQ}$ where A_i is the ith row of A*
2. *$\tilde{A} \in \mathcal{SQ}$ for $\tilde{A}$ the vector of row norms (so $\tilde{A}_i = \|A_i\|$).*

Example 3.3.11. *Say we have the vector $\vec{x} = (2, 0, 1, 3)$ and $\vec{x} \in \mathcal{SQ}$. Consider the following binary tree data structure.*



So, consider if we have length-square sampling access to the original matrix $A \in \mathbb{C}^{m\times n}$ i.e. $A \in \mathcal{SQ}$. Suppose we want to draw s rows in s i.i.d. trials. Then, pick row index i of A with probability

$$p_i = \frac{\|A_{(i,\cdot)}\|^2}{\|A\|_F^2} \tag{3.3}$$

and output random row

$$\begin{aligned} Y &= \frac{1}{\sqrt{sp_i}} \left\langle A_{(i,\cdot)} \right| \\ &= \frac{1}{\sqrt{s}} \frac{\|A\|_F}{\|A_{(i,\cdot)}\|} \left\langle A_{(i,\cdot)} \right| \end{aligned}$$

which is just a scaling of the ith row of A[1]. In other words,

$$\Pr\left(Y = \frac{1}{\sqrt{sp_i}} \langle A_{(i,\cdot)}|\right) = p_i$$

After sampling s rows, we implicitly define matrix R to be the concatenation of the outputted random rows. Therefore,

$$R = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_s \end{bmatrix} \in \mathbb{C}^{s \times n} \tag{3.4}$$

Note that $\langle Y_k|$ denotes the random row outputted by the procedure on the kth i.i.d. draw.

Lemma 3.3.12. *Let $X = Y^\dagger Y - E[Y^\dagger Y]$ which evidently satisfies $E[X] = 0$. Then,*

$$E[X^2] \preceq E[(Y^\dagger Y)^2] \tag{3.5}$$

$$= A^\dagger A \|A\|_F^2 \frac{1}{s^2} \tag{3.6}$$

and so

$$\|E[X^2]\|_2 \leq \frac{1}{s^2}\|A\|_2^2\|A\|_F^2 \tag{3.7}$$

Furthermore,

$$\|X\|_2 = \frac{1}{s}\|A\|_F^2 \tag{3.8}$$

Proof. First, observe that $E[X^2]$ is the element-wise variance of $Y^\dagger Y$ and $E[(Y^\dagger Y)^2]$ is the corresponding second moment. Hence, the relation $E[X^2] \leq E[(Y^\dagger Y)^2]$ holds element-wise which implies that the matrix relation $E[X^2] \preceq E[(Y^\dagger Y)^2]$ holds as well.

Furthermore,

$$\begin{aligned}
E[(Y^\dagger Y)^2] &= \frac{1}{s^2}\sum_{i=1}^m \frac{p_i}{p_i^2} |A_{(i,\cdot)}\rangle \langle A_{(i,\cdot)}|A_{(i,\cdot)}\rangle \langle A_{(i,\cdot)}| \\
&= \frac{1}{s^2}\sum_{i=1}^m \frac{\|A\|_F^2}{\langle A_{(i,\cdot)}|A_{(i,\cdot)}\rangle} |A_{(i,\cdot)}\rangle \langle A_{(i,\cdot)}|A_{(i,\cdot)}\rangle \langle A_{(i,\cdot)}| \qquad \text{(using (3.3))} \\
&= \frac{1}{s^2}\sum_{i=1}^m \|A\|_F^2 |A_{(i,\cdot)}\rangle \langle A_{(i,\cdot)}| = \frac{\|A\|_F^2}{s^2}\sum_{i=1}^m |A_{(i,\cdot)}\rangle \langle A_{(i,\cdot)}| \\
&= A^\dagger A \|A\|_F^2 \frac{1}{s^2}
\end{aligned}$$

[1]The reason that we scale by s is so that the expectations of $A^\dagger A$ and $R^\dagger R$ coincide in the theorem that follows. The reason that we scale by p_i is so that the norms of all rows are equivalent—a fact which we'll utilize when we sample R column-wise.

Recall that $E[R^\dagger R] = \frac{1}{s}A^\dagger A$. So, observe that

$$\begin{aligned}
\|X\|_2 &= \|Y^\dagger Y - E[Y^\dagger Y]\|_2 \\
&= \frac{1}{s}\left\| \frac{1}{p_i} |A_{(i,\cdot)}\rangle \langle A_{(i,\cdot)}| - A^\dagger A \right\|_2 \\
&\leq \frac{1}{s} \max\left\{ \left\| \frac{1}{p_i} |A_{(i,\cdot)}\rangle \langle A_{(i,\cdot)}| \right\|_2, \left\| A^\dagger A \right\|_2 \right\} \\
&\leq \frac{1}{s} \max\left\{ \frac{\|A\|_F^2}{\| |A_{(i,\cdot)}\rangle \|_2^2} \left\| |A_{(i,\cdot)}\rangle \langle A_{(i,\cdot)}| \right\|_2, \|A^\dagger A\|_F^2 \right\}
\end{aligned}$$

using $\|A^\dagger A\|_2 = \|A\|_2^2 \leq \|A\|_F^2$ and plugging in (3.3).

$$= \frac{1}{s}\|A\|_F^2$$

□

Proposition 3.3.13. *If $t > 0, t \in \mathbb{C}$ satisfies $\|tX\|_2 \leq 1$ for all possible values of X, then*

$$\begin{aligned}
\|E[e^{\pm tX}]\|_2 &\leq 1 + \frac{t^2}{s^2}\|A\|_2^2\|A\|_F^2 \\
&\leq e^{t^2\|A\|_2^2\|A\|_F^2/s^2}
\end{aligned} \tag{3.9}$$

Proof. First, from (3.3.7) we know that $E[e^{tX}] \preceq E[I + X + X^2] = I + E[X^2]$ since $E[X] = 0$. Hence, we have the proposition by (3.7). □

Theorem 3.3.14. *Let $A \in \mathbb{C}^{m\times n}$ and $R \in \mathbb{C}^{r\times n}$ be constructed by the length-square sampling and scaling so that $E[R^\dagger R] = E[A^\dagger A]$ (requirements that are met by R defined in (3.4)). Then, for all $\epsilon \in [0, \|A\|/\|A\|_F]$[2], we have*

$$\Pr\left(\|R^\dagger R - A^\dagger A\| \geq \|A\|\|A\|_F\right) \leq 2ne^{\frac{-\epsilon^2 s}{4}}$$

Hence, for $s \geq (4\ln\frac{2n}{\eta})/\epsilon^2$, with probability at least $(1-\eta)$ we have

$$\|R^\dagger R - A^\dagger A\| \leq \epsilon\|A\|\|A\|_F$$

Proof. From our definition above, we have that

[2] If $\epsilon \geq \|A\|/\|A\|_F$, then we can simply use $\hat{0}$ to approximate $A^\dagger A$

$$R^\dagger R = \begin{bmatrix} Y_1^\dagger & Y_2^\dagger & \dots & Y_s^\dagger \end{bmatrix} \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_s \end{bmatrix}$$
$$= \sum_{k=1}^{s} |Y_k\rangle \langle Y_k|$$

Let i_k give the index of the row sampled from A on the kth draw. Hence,

$$= \frac{1}{s} \sum_{k=1}^{s} \frac{1}{p_{i_k}} \left|A_{(i_k,\cdot)}\right\rangle \left\langle A_{(i_k,\cdot)}\right|$$

Furthermore,

$$E[R^\dagger R] = \frac{1}{s} \sum_{k=1}^{s} \sum_{i_k=1}^{m} \frac{p_{i_k}}{p_{i_k}} \left|A_{(i_k,\cdot)}\right\rangle \left\langle A_{(i_k,\cdot)}\right|$$
$$= \frac{1}{s} \sum_{k=1}^{s} A^\dagger A$$
$$= A^\dagger A$$

Note that similarly $E[Y^\dagger Y] = \frac{1}{s} A^\dagger A$.

So, we can define $X_i = |Y_k\rangle \langle Y_k| - E\Big[\, |Y_k\rangle \langle Y_k| \,\Big]$ which is evidently an i.i.d. copy of X as we've defined previously. Hence,

$$\sum_{i=1}^{s} X_i = R^\dagger R - E[R^\dagger R]$$
$$= R^\dagger R - A^\dagger A$$

Now, we can first apply Theorem 3.1 with $a = \epsilon \|A\|_2 \|A\|_F$,

$$\Pr\left(\left\| \Big(\sum_{i=1}^{s} X_i \Big) \right\|_2 \geq \epsilon \|A\|_2 \|A\|_F \right)$$
$$\leq n e^{-t\epsilon \|A\|_2 \|A\|_F} (\|E[e^{tX}]\|_2^s + \|E[e^{-tX}]\|_2^s)$$

for any $t > 0$. Hence, we can apply Proposition 3.3.13 which then gives us

$$\leq 2n e^{-t\epsilon \|A\|_2 \|A\|_F} e^{t^2 \|A\|_2^2 \|A\|_F^2 / s^2}$$

for $t \leq s/\|A\|_F^2$. Hence, we can set $t = \frac{\epsilon s}{2\|A\|_F\|A\|_2}$ (which is indeed less than $s/\|A\|_F^2$) and finally,

$$\leq 2ne^{-\epsilon^2 s/4}$$

Therefore, if we require that $s \geq (4 \ln \frac{2n}{\eta})/\epsilon^2$ we then have

$$\Pr\left(\left\|\left(\sum_{i=1}^{s} X_i\right)\right\|_2 \geq \epsilon\|A\|_2\|A\|_F\right) \leq 2ne^{-\frac{\epsilon^2}{4}\frac{4\ln\frac{2n}{\eta}}{\epsilon^2}}$$
$$= 2ne^{-\ln\frac{2n}{\eta}} = \eta$$

□

FKV Algorithm

Given $A \in \mathbb{C}^{m\times n}$ such that $A \in \mathcal{SQ}$ and some threshold k, we can output a description of a low-rank approximation of A with poly(k) queries. Specifically, we output two matrices $S, \hat{U} \in \mathcal{SQ}$ where $S \in \mathbb{C}^{\ell\times n}$, $\hat{U} \in \mathbb{C}^{\ell\times k}$ ($\ell = \text{poly}(k, \frac{1}{\epsilon})$). This implicitly describes the low-rank approximation to A by the following theorem

Theorem 3.3.15. *Define*

$$D := A(S^\dagger\hat{U})(S^\dagger\hat{U})^\dagger \qquad (\text{rank}(D) \leq k)$$
$$\sigma := \sqrt{2/k}\|A\|_F$$
$$A_\sigma := \sum_{\sigma_i \geq \sigma} \sigma_i |u_i\rangle\langle v_i| \qquad (\text{using SVD})$$

Then,

$$\|A - D\|_F^2 \leq \|A - A_\sigma\|_F^2 + \epsilon^2\|A\|_F^2$$

with probability $\geq 1 - \delta$.

Proof. Sketch. Theorem 3.3.14 says that $\|S^\dagger S - A^\dagger A\| \leq \epsilon\|A\|_F^2$ with high probability ($\|A\|_2 \leq \|A\|_F$ in general). Similarly, by performing the sampling process on $S^\dagger$ to get $T \in \mathbb{C}^{\ell\times k}$, we have an analogous bound on $SS^\dagger - TT^\dagger$. Since T is a constant-sized matrix, we can compute $\hat{U}$, the large left singular vectors of T, which approximate the large left singular vectors of T. Then, $S^\dagger\hat{U}$ translates these large left singular vectors to their corresponding right singular vectors, which are the approximate singular vectors of A as desired. □

For more intuition, write SVDs

$$A = \sum_i |u_i\rangle\langle v_i|$$
$$S = \sum_i |w_i\rangle\langle\tilde{v}_i|$$
$$U = \sum_i |\tilde{w}_i\rangle\langle z_i|$$

where $\tilde{v_i}$ denotes that the right singular vectors of S well-approximate the right singular vectors of A and similarly for $\tilde{w_i}$. Hence,

$$\begin{aligned} UU^\dagger &= \sum_i |\tilde{w_i}\rangle \langle \tilde{w_i}| \\ S^\dagger(UU^\dagger)S &\approx \sum_i |\tilde{v_i}\rangle \langle \tilde{v_i}| \\ A(S^\dagger UU^\dagger S) &\approx \sum_i |u_i\rangle \langle \tilde{v_i}| \end{aligned}$$

To visualize the projection,

$$\begin{bmatrix} \cdots A \cdots \end{bmatrix} \begin{bmatrix} S^\dagger \end{bmatrix} \begin{bmatrix} \hat{U} \end{bmatrix} \begin{bmatrix} \hat{U^\dagger} \end{bmatrix} \begin{bmatrix} \cdots S \cdots \end{bmatrix}$$

Chapter 4

A Review of Quantum Machine Learning

4.1 Introduction

Since its conception, quantum computation and quantum information has taught us to "think physically about computation" [30]. Well, if quantum mechanics tells us that physical states are mathematically linear algebraic objects (vectors in a Hilbert space), then perhaps this lesson says that the type of computation best suited for quantum physical reality are linear algebraic problems, such as the machine learning ones noted above. This somewhat naive intuition turns out to have value, as we will show in this review.

Hence, this leads us to the idea of quantum machine learning which uses quantum algorithms as part of a larger implementation to outperform the corresponding classical learning algorithms.

Nevertheless, past linear algebraic analysis techniques, there exist other classes of machine learning algorithms such as deep learning built on artificial neural networks and reinforcement learning which models an environment as a Markov decision process [36]. Successes have been achieved in terms of (potential) quantum speedups in these arenas [13], but we won't explore these alternative machine learning routes further in our review.

In this chapter, we will cover the main theoretical results in terms of quantum algorithms relevant to quantum machine learning. Then, we'll describe specific learning problems that have achieved quantum speedups using these results. Finally, we'll discuss important limitations to these results which may pose substantive challenges to the future of quantum learning theory.

Our goal is to provide a birds-eye view of these concepts and refer the reader to appropriate references where they desire greater detail.

4.2 Comparing Machine Learning Performance

If we are to claim that some machine learning algorithms perform better on a quantum computer, we first must decide on a notion of "outperforming".

This is currently characterized by the advantage in runtime obtained by a quantum algorithm over the classical methods for the same task. We quantify the runtime with the asymptotic scaling

of the number of elementary operations used by the algorithm with respect to the size of the input, as one does in complexity theory.

The definition of an elementary operation is dependent on the choice of measure of complexity. Query complexity measures the number of queries to the information source for the classical or quantum algorithm. Hence, a quantum speedup results if the number of queries needed to solve a problem is lower for the quantum than for the classical algorithm [6].

4.3 Speedup Techniques

4.3.1 Solving Systems of Linear Equations

Solving linear systems of equations is a ubiquitous problem in machine learning. As we will discuss, many learning problems, such as least-squares regression and least-squares SVMs, require the inversion of a matrix. Hence, we will describe two common quantum algorithms which lead up to the recent HHL algorithm, named after the algorithm's authors, Harrow, Hassidim, and LLoyd.

HHL Algorithm

One such application of Phase Estimation (Section 2.3.2) is with respect to solving linear systems of equations. This is the so-called HHL algorithm [24]. Here, we will cover the essential details of the algorithm.

The general problem statement of a linear system is if we are given matrix A and unit vector $\vec{b}$, then find $\vec{x}$ satisfying,

$$A\vec{x} = \vec{b}$$

However, assume that instead of solving for x itself, we instead solve for an expectation value $x^T Mx$ for some linear operator M. The original description of the algorithm provides runtime bound of $\tilde{O}(\log(N)\kappa^2 s^2/\epsilon)$, where s is sparsity measured by the maximum number of non-zero elements in a row and column of A, κ is the condition number, and ϵ is the approximation precision. Hence, we can only achieve speedup if the linear system is sparse and has a low condition number κ. Ambainis [3] and Childs [10] improved this depency on κ and s to linear and ϵ to poly-logarithmic.

This compares well considering that the best classical algorithm has a runtime of $O(N^{2.373})$ [12]. However, due to the large amount of pre-processing required, the algorithm is not used in practice. Standard methods, for example, based on QR-factorization take $O(N^3)$ steps [19].

So, assume that A in our linear system is an $N \times N$ Hermitian matrix. Notice that this is an "unrestrictive" constraint on A because we can always take non-Hermitian matrix A' and linear system $A'\vec{x} = \vec{b}$ and instead solve $\begin{bmatrix} 0 & A' \\ A'^\dagger & 0 \end{bmatrix} \begin{bmatrix} 0 \\ x \end{bmatrix} = \begin{bmatrix} b \\ 0 \end{bmatrix}$. Hence, we we will assume that A is Hermitian from here on.

Recall that because A is hermitian, then we can perform quantum phase estimation using e^{-iAt} as the unitary transformation. This can be done efficiently if A is sparse.

So, we first prepare $|b\rangle = \sum_i b_i |i\rangle$ (the representation of $\vec{b}$). We assume that this can be done efficiently or that $|b\rangle$ is supplied as an input.

Denote by $|\psi_j\rangle$ the eigenvectors of A with associated eigenvalues λ_j. Hence, we can express $|b\rangle$ as $|b\rangle = \sum_j \beta_j |\psi_j\rangle$. So, we initialize a first register to state $\sum_j \beta_j |\psi_j\rangle$ and second register to state $|0\rangle$. After applying phase estimation, we then have the joint state $\sum_j \beta_j |\psi_j\rangle \left|\widetilde{\lambda}_j\right\rangle$, where $\widetilde{\lambda}_j$ is an

approximation of λ_j. We'll assume that this approximation is perfect from here on, for the sake of demonstration.

Next we add an ancilla qubit and perform a rotation conditional on the first register which now holds $|\lambda_j\rangle$. The rotation transforms the system to

$$\sum_j \beta_j |\psi_j\rangle |\lambda_j\rangle \left(\sqrt{1 - \frac{C^2}{\lambda_j^2}} |0\rangle + \frac{C}{\lambda_j} |1\rangle\right)$$

for some small constant $C \in \mathbb{R}$ that is $O(1/\kappa)$.

Hence, we can undo phase estimation to restore the second register to $|0\rangle$.

Now, if we measure the ancillary qubit in the computational basis, we'll evidently collapse the state to $|1\rangle$ with some probability. We'd then have

$$\sum_j \frac{C}{\lambda_j} \beta_j |\psi_j\rangle |\lambda_j\rangle |1\rangle = C(A^{-1} |b\rangle)$$

In particular, the probability of getting this result is

$$\begin{aligned}
p(-1) &= \left(\sum_j \beta_j \langle\psi_j| \langle\lambda_j| \left(\sqrt{1 - \frac{C^2}{\lambda_j^2}} \langle 0| + \frac{C}{\lambda_j} \langle 1|\right)\right) |1\rangle \langle 1| \left(\sum_j \beta_j |\psi_j\rangle |\lambda_j\rangle \left(\sqrt{1 - \frac{C^2}{\lambda_j^2}} |0\rangle + \frac{C}{\lambda_j} |1\rangle\right)\right) \\
&= \sum_j \beta_j \langle\psi_j| \langle\lambda_j| \left(\sqrt{1 - \frac{C^2}{\lambda_j^2}} \langle 0| + \frac{C}{\lambda_j} \langle 1|\right) |1\rangle \langle 1| \beta_j |\psi_j\rangle |\lambda_j\rangle \left(\sqrt{1 - \frac{C^2}{\lambda_j^2}} |0\rangle + \frac{C}{\lambda_j} |1\rangle\right) \\
&= \sum_j \beta_j \langle\psi_j| \langle\lambda_j| \frac{C}{\lambda_j} \langle 1|1\rangle \langle 1| \beta_j |\psi_j\rangle |\lambda_j\rangle \frac{C}{\lambda_j} |1\rangle \\
&= \sum_j \beta_j^2 \frac{C^2}{\lambda_j^2} \\
&= \|A^{-1} |b\rangle\|^2 C^2 = \Omega(1/\kappa^2)
\end{aligned}$$

However, using amplitude amplification (Section 2.4) this can be upper-bounded to $O(1/\kappa)$.

Finally, we can make a measurement M whose expectation value $\langle x| M |x\rangle$ corresponds to the feature of x we wish to evaluate.

The concessions we noted along the way clearly limit the algorithm's applicability to practical problems. We have three essential caveats to achieving exponential speedup: (1) A must be sparse and have a condition number that scales at most sublinearly with N, (2) $|b\rangle$ must be loaded in quantum superposition in $\log(N)$ time, and (3) $|x\rangle$ isn't actually be read out, but instead an expectation is computed.

Limitation (1) has been partially resolved by the work of [40] to achieve a quadratic speedup for dense matrices.

Limitation (2) may be solved by quantum RAM, which then has its own limitations discussed in the next section.

Limitation (3) is a general issue with regards to reading out classical information from a quantum state at the conclusion of a quantum algorithm because we would need at least N measurements to retrieve this classical data. Hence, this would eliminate the potential for exponential speed-up.

Hence, after observing these limitations we may wonder if there can exist a classical algorithm with the same caveats that can achieve the same runtime. Importantly, in the original paper the authors showed that HHL is universal for quantum computation. Hence, we can encode any quantum algorithm e.g. Shor's algorithm into a system of roughly 2^n linear equations in 2^n unknowns, and then use HHL to solve the system (i.e., simulate the algorithm) in polynomial time. Thus, provided we believe any quantum algorithm achieves an exponential speedup over the best possible classical algorithm, HHL can theoretically achieve such a speedup as well [1].

To conclude, HHL is a logarithmic time quantum algorithm for matrix inversion, a task arising in many learning problems. However, a number of caveats that include the requirement of a logarithmic access time to the memory and the impossibility of retrieving the solution vector with one measurement lead to the question of whether classical or parallel algorithms that make use of the same assumptions obtain similar, or better, runtimes in practice. Hence, we will need empirical data to further address this question.

4.3.2 Quantum Random Access Memory

The essence of machine learning is analyzing a vast amount of data. Hence, we must address the question of how classical data is encoded in quantum superposition, a concern brought up in our previous discussion of the matrix inversion algorithm.

So, assume that we have an classical vectors $\{v_1, \cdots, v_n : v_1 \in \mathbb{R}^m\}$ that need to be encoded for use as part of a quantum algorithm. Quantum random access memory (qRAM) can encode these classical vectors in superposition into $\log(nm)$ qubits in $\log(nm)$ time using its "bucket-brigade architecture"[18]. The basic idea is to use a three-level tree structure where the nm qubit "leaves" contain the entries of the n vectors in $\mathbb{R}^m$.

One of the central limitations of qRAM is that the number of resources scales as $O(nm)$ i.e. exponentially in the binary representation of n, m. There have been open questions of the viability of this model of memory, in practice. In particular, if each of the qubits must be error-corrected, then it seems entirely impractical for general use. Some of this concern has been answered by proponents who have showed that, given a certain error model, algorithms that require to query the memory a polynomial number of times (e.g. the HLL algorithm above) might not require fault-tolerant components. Still, the amplitude amplification algorithm above does require this error correction.

Furthermore, it may be only fair to compare qRAM to a parallel classical architecture, given that we are allowing resources to scale exponentially.

Considerable, too, is the fact that data must be distribute fairly uniformly over the quantum register or else qRAM is no longer efficient [1].

In conclusion, qRAM comes with a significant number of considerations in itself and hence should be subjected to empirical investigation to determine its genuine quantum speed-up in practice.

4.4 Applications

4.4.1 Principal Component Analysis

First, we consider the ubiquitous principal component analysis (PCA) algorithm. PCA reduces the dimensionality of data by transforming the features to uncorrelated weightings of the original features ("principal components"). This requires simply finding the eigenvalues and eigenvectors of the data covariance matrix.

Hence, let $v_j \in V$ where V is a d-dimensional vector space such that $d = 2^n = N$ and assume that $|v_j| = 1$ for simplicity. Hence, the covariance matrix of the data is given by $C = \sum_j v_j v_j^T$ whose eigenvalues and eigenvectors we seek to discover. So, suppose we can prepare quantum state $v_j \to |v_j\rangle$, choosing classical data vector v_j uniformly at random. For example, we can use qRAM, discussed above. Then, because of our random selection, the resulting quantum state has density matrix $\rho = \frac{1}{N} \sum_j |v_j\rangle \langle v_j|$ which we observe to be the covariance matrix, up to an overall factor.

Then, as Lloyd, Mohseni and Rebentrost describe [27], one way to perform quantum PCA use that given n copies of ρ we have the ability to apply the unitary operator $e^{-i\rho t}$ to any state σ with accuracy $O(t^2/n)$. This can be done by using repeated infinitesmal applications of the SWAP operator on $\rho \otimes \sigma$.

Hence, using $e^{-i\rho t}$, we can perform phase estimation on rho. So, let $|\psi_i\rangle$ be the eigenvectors of ρ with associated eigenvalues λ_i and so $\rho = \sum_j \lambda_j |\psi_j\rangle \langle \psi_j|$. Therefore, phase estimation gives u

$$\sum_j \lambda_j |\psi_j\rangle \langle \psi_j| \otimes \left|\tilde{\lambda_j}\right\rangle \left\langle\tilde{\lambda_j}\right|$$

where $\tilde{\lambda_j}$ is an approximation of λ_j. Hence, if we measure the second register and repeat this procedure several times, the most frequent outcome is the first principal component $|\psi_{max}\rangle$, and so on.

The algorithm works best when a small number of principal components have significantly greater eigenvalues than the rest. Hence, ρ is well represented by the subspace spanned by the principal components. In particular, let $m << d$ be the dimension of the subspace of principal components which represent ρ within some bound. Then, the algorithm has runtime $O(m \log n)$.

Hence, this gives a limitation: if the eigenvalues of the covariance are roughly equal and of size $O(1/d)$, then the algorithm reduces to scaling in time $O(d)$ (as does the classical algorithm). Furthermore, we evidently inherit the limitations of qRAM, if we use it for the state preparation above.

4.4.2 Support Vector Machines

Support vector machines seek to find an optimal (maximum margin) separating hyperplane between two classes of data in a dataset. Hence, if the training data is linearly separable, each class can be found on only one side of the hyperplane. In particular, let $\{x_1, \cdots, x_n\}$ be a set of observations where x_i is a d-dimensional vector with associated labels $y_i \in \{0, 1\}$. Hence, we seek a linear function $f(x) = \vec{w} \cdot \vec{x} - \vec{b}$ where $\vec{w}$ is a weight vector and $\vec{b}$ is a bias vector s.t. $y_i f(x_i) > 0, \forall i$. Furthermore, we seek to maximize the minimum $y_i f(x_i)$, across all i.

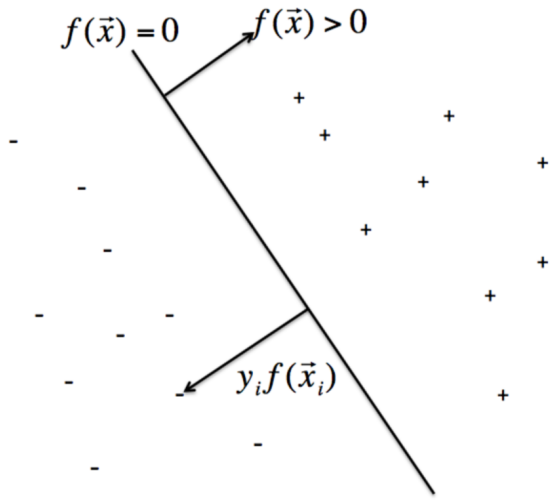


Figure 4.1: Visualization of a separating hyperplane and its associated margin taken from [33].

Much of the appeal of SVM is in its generalization to nonlinear hypersurfaces by replacing the constituent inner products with a kernel that implicitly maps the observations to another high dimensional space [33].

Solving SVM generally is performed by optimization of the dual problem which is a quadratic optimization problem. Hence, in [32], the authors show that quantum evaluation of inner products leads to exponential speed-ups in terms of d.

Full exponential improvements, however, can be achieved (with respect to d and n) in the case of least-squares SVMs [32]. In this case, finding a solution requires optimizing a least squares minimization. Hence, this type of minimization reduces to solving a set of linear equations. So, after data has been inputted efficiently (perhaps using qRAM), a modified version of the matrix inversion algorithm above can be used, incorporating methods from the PCA algorithm above to prepare the linear system.

The key point is, all the operations required to construct the maximum-margin separating hyperplane and to test whether a vector's classification can be performed in time that is polynomial in $\log n$.

4.4.3 Gaussian Processes

In [43], the authors demonstrate an application of HHL algorithm with respect to Gaussian process regression (GPR), another supervised learning method. In effect, GPR is a stochastic generalization of ordinary regression. In particular, let $\{x_1, \cdots, x_n\}$ be a set of observations where x_i is a d-dimensional vector with associated scalar targets y_i. In GPR, we consider the distribution over latent functions $f(x)$ which can return the correct labelling, y, given an inputted data-point. However, we further assume that this labelling is subject to Gaussian noise i.e. $f(x) = y + \epsilon$, where ϵ is the Gaussian noise. Hence, GPR uses Bayesian inference to return this distribution of latent functions such that they are consistent with the observed data.

Now, given this distribution and some test input x', we can predict its output by computing (1) a linear predictor known as the predictive mean and (2) the variance of the predictor with respect to x'. These values then give the distribution the y' that is consistent with training data. Hence, the quantum speedup comes from the fact that both of these values can be computed using a modification of the HHL algorithm, as described in [43]. Furthermore, the size of the output is independent from the size of the dataset which the authors use to show that, combined with the efficiency of HHL, can given exponential speedups in terms of d. Again, we require that the data can be loaded in efficiently initially e.g. using qRAM.

4.4.4 Optimization

Unsurprisingly, optimization methods are fundamental to many machine learning algorithms. Again, we can apply our quantum set of tools to several important optimization problems, including semi-definite programs (with potential super-polynomial speedups) and constraint satisfiability programs. Even easier to see, we can directly use our demonstrated results to solve quadratic programming problems which reduce to a linear system. If $N \times N$ matrices that define the linear system are sparse and low rank, we can use HHL and yield a solution in $\log N$ time–an exponential speedup.

Furthermore, iterative optimization, such as by means of gradient descent can be implemented by modifying PCA. In this case, several copies of a quantum state representing the solution are used to iteratively improve the solution. We may expect improvements in this type of optimization to lead to improvement in training neural networks on a quantum computer.

Interestingly, the quantum optimization algorithm finds approximate solutions for combinatorial optimization by "alternating qubit rotations with the application of the problem's penalty function" [6].

4.4.5 Topological Data Analysis

By now, we've seen that the presented algorithms suffer from a common limitation: the classical data must be loaded into a quantum superposition efficiently given that the speedups come from performing the computational steps after data is loaded in. However, this issue can be avoided in cases where the data points can be computed efficiently individually, as opposed to loading all of a large dataset in. In terms of machine learning, this can happen when the computation component of the algorithm requires exploring a comparatively small subset of the original dataset. In other words, if we can explore a subset of the input data to determine the distribution and other descriptive features of the overall data, we can then have the quantum algorithm generate the combinatorially larger space in quantum parallel, thereby computing the quantum dataset efficiently. This idea was used in the context of topological data analysis in [25].

Topological features, in particular, seem promising for this goal given that they are independent of the metric of choice and hence capture essential features of the data. In a discrete set, topological features are given by features that persist across spatial resolutions. These persistent features, formalized through persistent homology, are less likely to be artifacts of noise or parameterization. For example, the holes, voids, or connected components are examples of such features. The number of these types of features are defined for simplical complex (roughly a closed set of simplexes) as "Betti numbers".

In the paper, the authors show how to generate quantum states to encode the simplexes using logarithmically fewer qubits. Furthermore, they show that the Betti numbers can be efficiently represented using this representation. Important assumptions were made, in particular such that

the quantum state encoding the simplexes can be generated efficiently. One satisfying condition is if the number of simplexes in the complex are exponentially large. Hence, in at least some cases, we may extract exponential speed-ups in this type of topological analysis.

4.5 Challenges

The first obvious challenge to quantum machine learning is that the execution of quantum algorithms requires quantum hardware that does not exist at present.

Aside from this, as we've seen by now, many of the quantum algorithms which are used to potentially give quantum speedups come with several caveats and limitations to their use. As noted in [6], implicitly in [1], and repeatedly elsewhere, we can condense the general caveats into a few fundamental problems:

(1) The Input State Preparation Problem. The cost of reading in the input can in some cases dominate the cost of quantum algorithms. In many cases, we hoped qRAM would solve this problem. Understanding this factor is an important ongoing challenge.

(2) The Readout problem. Retrieving the solution in terms of classical information after performing quantum algorithms requires learning an exponential number of bits through repeated trials. We've shown that learning an expectation value of a linear operator can be a sound alternative (e.g. in the case of matrix inversion).

(3) The true cost problem. We require empirical study to show the number of gates or elementary operations to carry out a quantum algorithm, in practice. For example, we encountered this issue in the fundamental phase estimation algorithm (i.e. is it fair to assume that a U^{2^j} gate is an elementary operation?). Nevertheless, our query complexity bounds seem to indicate great advantages in specific cases, as we've noted.

Throughout this review, we've considered learning classical data which introduces problems (1) and (2), given that we have to interface between classical and quantum states. Hence, we may consider the case of applying quantum algorithms to quantum data. This is covered in detail in [2].

4.6 Supervised learning with quantum feature Hilbert spaces

[21]

One classical method is using so-called Support Vector Machines (SVM), which construct a separating hyperplane such that the distance to the nearest training observation (minimum margin) is maximized. Much of the popularity of SVMs can be attributed to its association with the "kernel trick" which maps the data to a higher dimensional space so that it is separable or approximately separable.

Here, we suppose that the data is given classically and we seek to show that, in some cases, we can obtain a quantum advantage by either generating the separating hyperplane in quantum feature space or simply estimating the kernel function.

4.6.1 Feature Map

Consider the feature vector kernel $K(x, z) = |\langle \Phi(x) | \Phi(z) \rangle|^2$

4.6.2 Quantum Variational Classification

4.6.3 Quantum Kernel Estimation

4.6.4 Non-Trivial Feature Map with Entanglement

4.6.5 Geometric Analysis of Candidate Feature Maps

4.6.6 Experimental Simulation of Candidate Feature Maps

4.7 Quantum-Inspired Length-Square Sampling

As we've seen, most well-known QML algorithms convert input quantum states to a desired output state or value. Thus, they do not provide a routine to get necessary copies of these input states (a state preparation routine) and a strategy to extract information from an output state. Both are essential to making the algorithm useful.

We've also seen that that many of the initial "practical" quantum algorithms attempted to workaround this difficulty by considering low-rank linear algebraic problems (poly-logarithmic in matrix dimension). For example, the data fitting algorithm [38] allows one to compute $A^+ |b\rangle = |x_{LS}\rangle$ in $\tilde{O}(log(N)(s^3\kappa^6)/\epsilon)$ time (query complexity) by using the HHL algorithm and matrix multiplication. Hence, we require that A is sparse with low condition number κ as well.

Nevertheless, these low-rank quantum algorithms still have substantial help from an assumed input state preparation routine which has been shown to be at least $\Omega(\sqrt{n})$ in vector input size ([37]). Hence, a natural question to ask is whether there's a similar classical data structure which takes time polynomial in quantum state preparation which can offer machine learning algorithms with similar guarantees. In particular, we compare quantum algorithms with quantum state preparation to classical algorithms with sample and query access to input.

Definitions

We remain consistent with the definitions of Section 3.3.2.

Low-Rank Estimation

Low-rank estimation is given by the FKV algorithm detailed in Section 3.3.2.

Trace Inner Product Estimation

- For $x, y \in \mathbb{C}^n$, if we are given that $x \in \mathcal{SQ}$ and $y \in \mathcal{Q}$, then we can estimate $\langle x, y\rangle$ with probability $\geq 1 - \delta$ and error $\epsilon\|x\|\|y\|$
- Quantum analog: SWAP test

Fact 4.7.1. *For $\{X_{i,j}\}$ i.i.d random variables with mean μ and variance σ^2, let*

$$Y := \underset{j\in[\log 1/\delta]}{\text{median}} \underset{i\in[1/\epsilon^2]}{\text{mean}} X_{i,j}$$

Then $|Y - \mu| \leq \epsilon\sigma$ with probability $\geq 1 - \delta$, using only $O(\frac{1}{\epsilon^2}\log\frac{1}{\delta})$ samples.

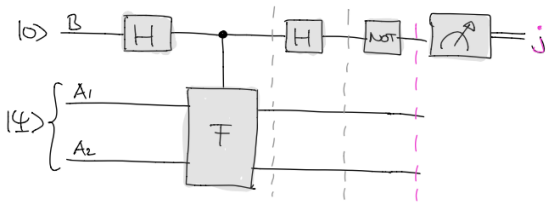


Figure 4.2: Swap test

- In words: We may create a mean estimator from $1/\epsilon^2$ samples of X. We compute the median of $\log 1/\delta$ such estimators
- Catoni (2012) shows that Chebyshev's inequality is the best guarantee one can provide when considering pure empirical mean estimators for an unknown distribution (and finite μ, σ)
- "Median of means" provides an exponential improvement in probability of success $(1-\delta)$ guarantee

Corollary 4.7.1.1. *For $x, y \in \mathbb{C}^n$, given $x \in \mathcal{SQ}$ and $y \in \mathcal{Q}$, we can estimate $\langle x, y\rangle$ to $\epsilon\|x\|\|y\|$ error with probability $\geq 1-\delta$ with query complexity $O(\frac{1}{\epsilon^2}\log\frac{1}{\delta})$*

Proof. Sample an **index** s from x. Then, define $Z := x_s y_s \frac{\|y\|^2}{|y_s|^2}$. Apply the Fact with $X_{i,j}$ being independent samples Z. □

Least-Square Sample Generation

- For $V \in \mathbb{C}^{n\times k}, w \in \mathbb{C}^k$, given $V^\dagger \in \mathcal{SQ}$ (*column*-wise sampling of V) and $w \in \mathcal{Q}$, we can simulate $Vw \in \mathcal{SQ}$ with poly(k) queries
- In words: if we can least-square sample the columns of matrix V and query the entries of vector w, then
  1. We can query entries of their multiplication (Vw)
  2. We can least-square sample from a distribution that emulates their multiplication
- Hence, as long as $k \ll n$, we can perform each using a number of steps polynomial in the number of columns of V.

Definition 4.7.2. *Rejection sampling*

Algorithm 4.7.3. *Input: Samples from distribution P*
Output: Samples from distribution Q

- *Sample s from P*
- *Compute $r_s = \frac{1}{N}\frac{Q(s)}{P(s)}$, for fixed constant N*
- *Output s with probability r_s and restart otherwise*

Fact 4.7.4. *Fact. If $r_i \leq 1, \forall i$, then the above procedure is well-defined and outputs a sample from Q in N iterations in expectation.*

Proposition 4.7.5. *For $V \in \mathbb{R}^{n\times k}$ and $w \in \mathbb{R}^k$, given $V^\dagger \in \mathcal{SQ}$ and $w \in \mathcal{Q}$, we can simulate $Vw \in \mathcal{SQ}$ with expected query complexity $\tilde{O}((\frac{1}{\epsilon^2}\log\frac{1}{\delta}))$*

We can compute entries $(Vw)_i$ with $O(k)$ queries.

We can sample using rejection sampling:

- *P is the distribution formed by sampling from $V_{(\cdot,j)}$.*
- *Q is the target Vw.*
- *Hence, compute r_s to be a constant factor of Q/P*

$$r_i = \frac{\|w^T V_{\cdot,i}\|^2}{\|w\|^2\|V_{\cdot,i}\|^2}$$

- Notice that we can compute these r_i's (in fact, despite that we cannot compute probabilities from the target distribution), and that the rejection sampling guarantee is satisfied (via Cauchy-Schwarz).
- Since the probability of success is $\|Vw\|^2/\|w\|^2$, it suffices to estimate the probability of success of this rejection sampling process to estimate this norm.
- Through a Chernoff bound, we see that the average of $O(\|w\|^2(\frac{1}{\epsilon^2}\log\frac{1}{\delta}))$ "coin flips" is in $[(1-\epsilon)\|Vw\|, (1+\epsilon)\|Vw\|]$ with probability $\geq 1-\delta$.

Application: Stochastic Regression

For a low-rank matrix $A \in \mathbb{R}^{m\times n}$ and a vector $b \in \mathbb{R}^n$, given $b, A \in \mathcal{SQ}$, (approximately) simulate $A^+b \in \mathcal{SQ}$.

Algorithm 4.7.6.

- *Low-rank approximation (3) gives us $S, \hat{U} \in \mathcal{SQ}$.*
- *Applying thin-matrix vector (2), we get $\hat{V} \in \mathcal{SQ}$, where $\hat{V} := S^T\hat{U}$; we can show that the columns of $\hat{V}$ behave like the right singular vectors of A.*
- *Let $\hat{U}$ have columns $\{\hat{u}_i\}$. Hence, $\hat{V}$ has columns $\{S\hat{u}_i\}$. Write its ith column as $\hat{v}_i := S\hat{u}_i$.*
- *Low-rank approximation (3) also outputs the approximate singular values $\hat{\sigma}_i$ of A*

Now, we can write the approximate vector we wish to sample in terms of these approximations:

$$A^+b = (A^TA)^+A^Tb \approx \sum_{i=1}^{k} \frac{1}{\hat{\sigma}_i^2}\hat{v}_i\hat{v}_i^TA^Tb$$

- We approximate $\hat{v}_i^TA^Tb$ to additive error for all by noticing that $\hat{v}_i^TA^Tb = \mathrm{tr}\big(A^Tb\hat{v}_i^T\big)$ is an inner product of A^T and $b\hat{v}_i^T$.
- Thus, we can apply (1), since being given $A \in \mathcal{SQ}$ implies $A^T \in \mathcal{SQ}$ for A^T viewed as a long vector.

- Define the approximation of $\hat{v}_i^T A^T b$ to be $\hat{\lambda}_i$. At this point we have (recalling that $\hat{v}_i := S\hat{u}_i$)

$$A^+ b \approx \sum_{i=1}^{k} \frac{1}{\hat{\sigma}_i^2} \hat{v}_i \hat{\lambda}_i = S \sum_{i=1}^{k} \frac{1}{\hat{\sigma}_i^2} \hat{u}_i \hat{\lambda}_i$$

- Finally, using (2) to provide sample access to each $S\hat{u}_i$, we are done ! $\tilde{O}(\kappa^{16} k^6 \|A\|_F^6 / \epsilon^6)$ complexity.

Definitions and Assumptions

Let $b \in \mathbb{C}^m$ and $A \in \mathbb{C}^{m \times n}$ s.t. $\|A\| \leq 1$ where $\|\cdot\|$ signifies the operator norm (or spectral norm). Furthermore, require that $\text{rank}(A) = k$ and $\|A^+\| \leq \kappa$ where A^+ is the pseudoinverse of A. Hence, observe that $\|A\| \leq 1$ is equivalent to A having maximum singular value 1[1]. Similarly, A^+ has inverted singular values from A and so $\|A^+\|$ is equal to the reciprocal of the minimum nonzero singular value. Therefore, the condition number of A is given by $\|A\|\|A^+\| \leq \kappa$.

So, define x to be the least-squares solution to the linear system $Ax = b$ i.e. $x = A^+ b$. Then, in terms of these definitions, we define two primary goals:

1. Query a vector $\tilde{x}$ s.t. $\|\tilde{x} - x\| \leq \epsilon \|x\|$
2. Sample from a distribution that approximates $\frac{|x_j|^2}{\|x\|^2}$ within total variation distance (Theorem 3.3.1) 2ϵ.

In order to do this, we simply assume that we have length-square sampling access to A. In other words, we are able to sample row indices of A from the distribution $\frac{\|A_{(i,\cdot)}\|^2}{\|A\|_F^2}$

Sequence of Approximations

First, we'll summarize the sequence of approximations that we'll perform using length-squared sampling techniques. We'll describe these steps in depth in the following sections.

Of course, we know that the least squares solution of the linear system is given by the orthogonal projection

$$(A^\dagger A)^+ A^\dagger = A^+ b$$

So, we first approximate $A^\dagger A$ by $R^\dagger R$ where $R \in \mathbb{C}^{r \times n}$, $r \ll m$ is constructed from length-square sampling r rows of A. Now, denote the spectral decomposition

$$A^\dagger A \approx R^\dagger R = \sum_{l=1}^{k} \frac{1}{\sigma_l^2} \left| v^{(l)} \right\rangle \left\langle v^{(l)} \right|$$

where of course σ_i and $\left| v^{(i)} \right\rangle \in \mathbb{C}^n$ are the singular values and right singular vectors of R, respectively.

[1] To see this, simply consider Spectral Theorem applied to Hermitian matrix $A^\dagger A$

We see that computing these right singular vectors of R can still be computationally prohibitive given the dimension n. Hence, we can use length-square sampling again, this time on the columns of R to give a matrix $C \in \mathbb{C}^{r\times c}$, $c \ll n$. Now, the left singular vectors of C which we denote as $\left|w^{(i)}\right\rangle \in \mathbb{C}^r$ can be efficiently computed via standard SVD methods. So,

$$RR^\dagger \approx CC^\dagger = \sum_{l=1}^{k} \frac{1}{\sigma_l^2} \left|w^{(l)}\right\rangle \left\langle w^{(l)}\right|$$

We can then show that ()

$$\left|\tilde{v}^{(i)}\right\rangle := R^\dagger \left|w^{(l)}\right\rangle / \tilde{\sigma}_l \tag{4.1}$$

provides a good approximation of $\left|v^{(i)}\right\rangle$. Note that $\tilde{\sigma}_l$ are the singular values of C which then approximate the singular values of R which similarly approximate the singular values of A. This follows from $A^\dagger A \approx R^\dagger R$ and $RR^\dagger \approx CC^\dagger$ by the Hoffman–Wielandt inequality detailed in Lemma 2.7 of [22] and stated without proof below.

Lemma 4.7.7. *Hoffman–Wielandt inequality*
If P, Q are two real, symmetric $n\times n$ matrices and $\lambda_1, \cdots \lambda_n$ denote eigenvalues in non-decreasing order, then

$$\sum_{t=1}^{n} (\lambda_t(P) - \lambda_t(Q))^2 \leq \|P - Q\|_F^2$$

At this point, it seems like we haven't made much progress since computing $R^\dagger \left|w^{(l)}\right\rangle$ is still expensive. However, it turns out that all we need to enable query access to $\tilde{x}$ is the ability to efficiently estimate the trace inner product $\mathrm{tr}\big(U^\dagger V\big)$ where U and V are operators such that U can be the length-square sampled and V can be queried. To see this, we write our solution, $\tilde{x}$, in terms of the approximations thus far

$$\begin{aligned}
\tilde{x} &\approx A^+ |b\rangle \\
&\approx (R^\dagger R)^+ A^\dagger |b\rangle \\
&\approx \sum_{l=1}^{k} \frac{1}{\tilde{\sigma}_l^2} \left|\tilde{v}^{(l)}\right\rangle \left\langle \tilde{v}^{(l)}\right| A^\dagger |b\rangle
\end{aligned}$$

Hence, define $U := A$, $V := |b\rangle \left\langle \tilde{v}^{(l)}\right|$ in which case

$$\begin{aligned}
\mathrm{tr}\big(U^\dagger V\big) &= \mathrm{tr}\Big(A^\dagger |b\rangle \left\langle \tilde{v}^{(l)}\right|\Big) \\
&= \mathrm{tr}\Big(\left\langle \tilde{v}^{(l)}\right| A^\dagger |b\rangle\Big) \\
&= \left\langle \tilde{v}^{(l)}\right| A^\dagger |b\rangle
\end{aligned}$$

since $\langle \tilde{v}^{(l)} | A^\dagger |b\rangle$ is a scalar. Therefore, say that

$$\tilde{\lambda}_l \approx \mathrm{tr}\Big(A^\dagger |b\rangle \left\langle \tilde{v}^{(l)} \right|\Big)$$

and assume that we can compute and memoize these scalars $\tilde{\lambda}_i$ efficiently. In which case,

$$\tilde{x} \approx \sum_{l=1}^{k} \frac{1}{\tilde{\sigma}_l^2} \left|\tilde{v}^{(l)}\right\rangle \tilde{\lambda}_l$$

Recalling the definition of $\left|\tilde{v}^{(i)}\right\rangle$ (4.1),

$$= \sum_{l=1}^{k} \frac{1}{\tilde{\sigma}_l^3} R^\dagger \left|w^{(l)}\right\rangle \tilde{\lambda}_l$$
$$= R^\dagger \sum_{l=1}^{k} \frac{1}{\tilde{\sigma}_l^3} \left|w^{(l)}\right\rangle \tilde{\lambda}_l$$

and so defining $z := \sum_{l=1}^{k} \frac{1}{\tilde{\sigma}_l^3} \left|w^{(l)}\right\rangle \tilde{\lambda}_l$,

$$= R^\dagger z$$

We see that we can compute z efficiently (and memoize it for future queries) because it is a k-linear combination of left singular vectors in $\mathbb{C}^r$. So, say that we wish to query an element $\tilde{x}_j$. We can simply query column $R_{\cdot,j} \in \mathbb{C}^r$ (or equivalently row $R^\dagger_{j,\cdot}$) and compute $R_{\cdot,j} \cdot z$. Hence, we've achieved our first goal.

In order to achieve our second goal, enabling sample access to a distribution that approximates $\frac{|x_j|^2}{\|x\|^2}$, we require one more trick: rejection sampling which we detail in Section ().

All in all, we've performed the chain of approximations,

$$\begin{aligned}
|x\rangle = A^+ |b\rangle &= (A^\dagger A)^+ A^\dagger |b\rangle \\
&\approx (R^\dagger R)^+ A^\dagger |b\rangle = \sum_{l=1}^{k} \frac{1}{\tilde{\sigma}_l^2} \left|v^{(l)}\right\rangle \left\langle v^{(l)}\right| A^\dagger |b\rangle \\
&\approx \sum_{l=1}^{k} \frac{1}{\tilde{\sigma}_l^2} \left|\tilde{v}^{(l)}\right\rangle \left\langle \tilde{v}^{(l)}\right| A^\dagger |b\rangle \\
&\approx \sum_{l=1}^{k} \frac{1}{\tilde{\sigma}_l^2} \left|\tilde{v}^{(l)}\right\rangle \tilde{\lambda}_l = R^\dagger \sum_{l=1}^{k} \frac{1}{\tilde{\sigma}_l^3} \left|w^{(l)}\right\rangle \tilde{\lambda}_l = R^\dagger z
\end{aligned}$$

Now that we've sketched the steps of this process, we detail each approximation and show that we can achieve the claimed correctness and complexity bounds.

4.7.1 Conclusions

- Claim (Tang): For machine learning problems, $\mathcal{SQ}$ assumptions are more reasonable than state preparation assumptions.
- We discussed pseudo-inverse which inverts singular values, but in principle we could have applied any function to the singular values
- Gilyen et. al (2018) show that many quantum machine learning algorithms indeed apply polynomial functions to singular values
- Our discussion suggests that exponential quantum speedups are tightly related to problems where high-rank matrices play a crucial role (e.g. Hamiltonian simulation or QFT)

4.8 Optimal Quantum Sample Complexity

It is well known that one can tightly bound the number of samples from an unknown distribution required to PAC-learn (Section **??**) an unknown concept in terms of its VC dimension (Section **??**). Hence, a natural question to ask is whether "quantum samples" are more powerful in the sense of requiring less examples to achieve this goal.

Here we will explore the techniques of Arunachalam and de Wolf [5] in order to address this question. The authors show that the ideas of quantum state discrimination discussed in Section **??** offer an intuitive analysis, despite resulting in a suboptimal lower bound. However, Boolean Fourier analysis (Section 3.1) applied to the Pretty Good Measurement (Section 2.5.1) gives an optimal bound showing that there is no quantum advantage in terms of sample complexity when restricting to PAC learning and quantum samples as specified in the model introduced by Bshouty and Jackson [8].

4.8.1 Definitions

Quantum Learning Models: PAC Setting

A quantum example oracle $QPEX(c, D)$ acts on $|0\rangle^{\otimes n} |0\rangle$ and produces a quantum example

$$\sum_{x \in \{0,1\}^n} D(x) |x, c(x)\rangle \tag{4.2}$$

A quantum learner is given access to some copies of the state generated by $QPEX(c, D)$ and performs a POVM where each outcome is associated with a hypothesis.

A learning algorithm $\mathcal{A}$ is an (ϵ, δ)-PAC quantum learner for C if for every $c \in \mathcal{C}$ and distribution D, given access to the $QPEX(c, D)$ oracle, $\mathcal{A}$ outputs an h such that

$$err_D(h, c) \leq \epsilon \tag{4.3}$$

with probability at least $1 - \delta$.

The sample complexity of $\mathcal{A}$ is the maximum number invocations of the $QPEX(c, D)$ oracle, maximized over all $c \in \mathcal{C}$, distributions D, and the learners internal randomness. The (ϵ, δ)-PAC quantum sample complexity of a concept class $\mathcal{C}$ is the minimum sample complexity over all (ϵ, δ)-PAC quantum learners for $\mathcal{C}$.

Quantum Learning Models: Agnostic Setting

For a joint distribution $D : \{0,1\}^{n+1} \to [0,1]$ over the set of examples, the learner has access to an $QAEX(D)$ oracle which acts on $|0\rangle^{\otimes n} |0\rangle$ and produces a quantum example

$$\sum_{(x,b)\in\{0,1\}^{n+1}} D(x,b) |x,b\rangle \tag{4.4}$$

A $\mathcal{A}$ is an (ϵ,δ)-agnostic quantum learner for $\mathcal{C}$ if for every distribution D, given access to the $QAEX(D)$ oracle, $\mathcal{A}$ outputs an $h \in \mathcal{C}$ such that

$$err_D(h) \leq opt_D(h) + \epsilon \tag{4.5}$$

with probability at least $1 - \delta$.

The sample complexity of $\mathcal{A}$ is the maximum number invocations of the $QAEX(D)$ oracle over all distributions D and over the learners internal randomness. The (ϵ,δ)-agnostic quantum sample complexity of a concept class $\mathcal{C}$ is the minimum sample complexity over all (ϵ,δ)-agnostic quantum learners for $\mathcal{C}$.

4.8.2 Goals

We seek to show that quantum examples are not actually more powerful than classical labeled examples in the PAC model and in the agnostic model when the underlying data distribution is arbitrary. We emphasize this point on the data distribution because we plan to later detail advantages that can be reaped if the example distribution is e.g. uniform (hint: think about the Bernstein-Vazirani algorithm and a linear classifier).

In the classical case, the sample complexity of concept class $\mathcal{C}$ with VC dimension d in the PAC setting is

$$\Theta(\frac{d}{\epsilon} + \frac{\log(1/\delta)}{\epsilon})$$

where ϵ is the approximation coefficient and δ is the probability of success, as usual.

In the agnostic case, the optimal sample complexity of such agnostic learners is tightly determined by the VC dimension of $\mathcal{C}$

$$\Theta(\frac{d}{\epsilon^2} + \frac{\log(1/\delta)}{\epsilon^2})$$

The authors indeed show that, using the quantum learning models above, the bounds are the same in the quantum case. This requires a state identification argument which uses Fourier Analysis to analyze the performance of a Pretty Good Measurement 2.5.1. However, we can get close by instead using simple concepts from quantum information theory.xs

Of course, we know that the upper bounds in sample complexity are the same as the classical case since we can always implement a classical algorithm on a quantum computer. Hence, we seek lower bounds instead.

4.8.3 Information Theoretic Lower Bounds on Sample Complexity

VC-independent lower bounds

Lemma 4.8.1. *Let $\mathcal{C}$ be a non-trivial concept class. For every $\delta \in (0, 1/2), \epsilon \in (0, 1/4)$, a (ϵ, δ)-PAC quantum learner for $\mathcal{C}$ has sample complexity $\Omega(\frac{1}{\epsilon} \log \frac{1}{\delta})$*

Proof. Since $\mathcal{C}$ is non-trivial, we may assume there are two concepts $c_1, c_2 \in C$ defined on two inputs $\{x_1, x_2\}$ as follows:

$$c_1(x_1) = c_2(x_1) = 0$$
$$c_1(x_2) = 0, c_2(x_2) = 1$$

Consider the distribution D such that

$$D(x_1) = 1 - \epsilon$$
$$D(x_2) = \epsilon$$

For $i \in \{1, 2\}$, the state of the algorithm after T queries to $QPEX(c_i, D)$ is

$$|\psi_i\rangle = (\sqrt{1-\epsilon}\,|x_1, 0\rangle + \sqrt{\epsilon}\,|x_2, c_i(x_2)\rangle)^{\otimes T}$$

Therefore, $\langle\psi_1|\psi_2\rangle = (1-\epsilon)^T$. Since the success probability of an (ϵ, δ)-PAC quantum learner is $\geq 1 - \delta$, Corollary 2.5.5.1 implies $\langle\psi_1|\psi_2\rangle \leq 2\sqrt{\delta(1-\delta)}$.
$\therefore T = \Omega(\frac{1}{\epsilon} \log \frac{1}{\delta})$ □

Lemma 4.8.2. *Let $\mathcal{C}$ be a non-trivial concept class. For every $\delta \in (0, 1/2), \epsilon \in (0, 1/4)$, a (ϵ, δ)-agnostic quantum learner for $\mathcal{C}$ has sample complexity $\Omega(\frac{1}{\epsilon^2} \log \frac{1}{\delta})$*

Proof. Since $\mathcal{C}$ is non-trivial, we may assume there are two concepts $c_1, c_2 \in C$ defined on two inputs $\{x_1, x_2\}$ such that $c_1(x) \neq c_2(x)$.
Consider the two distributions $D_\pm$ s.t.

$$D_\pm(x, c_1(x)) = (1 \pm \epsilon)/2$$
$$D_\pm(x, c_2(x)) = (1 \mp \epsilon)/2$$

The state of the algorithm after T queries to $QAEX(D_\pm)$ is then

$$|\psi_\pm\rangle = ((\sqrt{(1 \pm \epsilon)/2})\,|x, c_1(x)\rangle + (\sqrt{(1 \mp \epsilon)/2})\,|x, c_2(x)\rangle)^{\otimes T}$$

Therefore, $\langle\psi_+|\psi_-\rangle = (1 - \epsilon^2)^{T/2}$. Since the success probability of an (ϵ, δ)-agnostic quantum learner is $\geq 1 - \delta$, Corollary 2.5.5.1 implies $\langle\psi_+|\psi_-\rangle \leq 2\sqrt{\delta(1-\delta)}$.
$\therefore T = \Omega(\frac{1}{\epsilon^2} \log \frac{1}{\delta})$ □

Corollary 4.8.2.1.

VC-dependent lower bounds

Theorem 4.8.3. *Let C be a concept class with $VC-dim(\mathcal{C}) = d+1$. Then for every $\delta \in (0, 1/2)$ and $\epsilon \in (0, 1/4)$, every (ϵ, δ)-PAC learner for $\mathcal{C}$ has sample complexity $\Omega(\frac{d}{\epsilon} + \frac{\log(1/\delta)}{\epsilon})$.*

Proof. Consider an (ϵ, δ)-PAC learner for $\mathcal{C}$ that uses T examples. The d-independent part of the lower bound, $T = \Omega(\frac{1}{\epsilon^2} \log \frac{1}{\delta})$, was proven in Lemma 4.8.1. Hence it remains to prove $T = \Omega(d/\epsilon)$.

It suffices to show this for a specific distribution D, defined as follows. Let $S = \{s_0, s_1, \cdots, s_d\} \subseteq \{0,1\}^n$ be some $(d+1)$-element set shattered by $\mathcal{C}$. Define

$$D(s_0) = 1 - 4\epsilon \tag{4.6}$$

$$D(s_i) = 4\epsilon/d \tag{4.7}$$

for all $i \in [d]$.

Because S is shattered by $\mathcal{C}$, for each string $a \in \{0,1\}^d$, there exists a concept $c_a\mathcal{C}$ such that $c_a(s_0) = 0$ and $c_a(s_i) = a_i$ for all $i \in [d]$. We define two correlated random variables A and B corresponding to the concept and to the examples, respectively. Let A be a random variable that is uniformly distributed over $\{0,1\}^d$; if $A = a$, let $B = B_1 \cdots B_T$ correspond to T i.i.d. samples from c_a distributed as D.

We give the following three-step analysis of these random variables:

1. $I(A:B) \geq (1-\delta)(1-H(1/4))dH(\delta) = \Omega(d)$.

   Proof. Let random variable h(B) 0, 1d be the hypothesis that the learner produces (given the examples in B) restricted to the elements s1,...,sd. Note that the error of the hypothesis □

□

VC-dependent bound for quantum agnostic learning

4.8.4 Optimal lower bounds by state identification

4.9 Online Learning of Quantum States

4.9.1 Goals

We will prove that

Theorem 4.9.1. *Let $E_1, E_2, \cdots$ be a sequence of two-outcome measurements on an n-qubit state presented to the learner, and $l_1, l_2, \cdots$ be the corresponding loss functions revealed in successive iterations in the regret minimization model. Suppose l_t is convex and L-lipschitz; in particular for every $x \in \mathbb{R}$, there is a subderivative $l'_t(x)$ such that $|l'_t(x)| \leq L$. Then there is an explicit learning strategy that guarantees regret $R_T = O(L\sqrt{Tn})$ for all T. This is so even assuming the measurement E_t and loss function l_t are chosen adaptively, in response to the learner's previous behavior.*

Specifically, the algorithm applies to L_1 loss and L_2 loss, and achieves regret $O(\sqrt{Tn})$ for both.

4.9.2 Online Learning and Regret

In progress...

Appendix A

Appendix

A.1 Quantum Mechanics

Definition A.1.1. *Pauli Matrices*

$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$
$$\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Definition A.1.2. *Bell States*

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$\frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$\frac{|10\rangle + |01\rangle}{\sqrt{2}}$$
$$\frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Definition A.1.3. *Positive Operators*

Let A be a bounded[1] linear operator on complex Hilbert space $\mathcal{H}$. The following conditions are equivalent to A being positive

1. *$A = S^\dagger S$ for some bounded operator S on $\mathcal{H}$*
2. *A is hermitian and $\langle x| A |x\rangle \geq 0$ for every $|x\rangle \in \mathcal{H}$*

[1] $\|Av\| \leq M\|v\|$ for some $M > 0$ and all $v \in \mathcal{H}$

3. the spectrum of A is non-negative

Definition A.1.4. *Trace of an Operator*
Let $\{|i\rangle\}$ be an orthonormal basis for A and so

$$\begin{aligned}\mathrm{tr}(A) &= \sum_i A_{ii} \\ &= \sum_i \langle i| A |i\rangle\end{aligned}$$

Hence, if we extend $|\psi\rangle$ to the orthonormal basis $\{|i\rangle\}$ which includes $|\psi\rangle$ as the first element (for example via the Gram-Schmidt procedure) then

$$\begin{aligned}\mathrm{tr}(A |\psi\rangle \langle\psi|) &= \sum_i \langle i| A |\psi\rangle \langle\psi|i\rangle \\ &= \langle\psi| A |\psi\rangle\end{aligned}$$

by orthonormality.

Theorem A.1.5. *Spectral Theorem*
Suppose A is a compact[2] hermitian operator (compactness ensures A has eigenvectors) on complex Hilbert space $\mathcal{H}$. Hence, there is an orthonormal basis of $\mathcal{H}$ consisting of eigenvectors of A. Each eigenvalue is in $\mathbb{R}$.

[2]the image under A acting on any bounded subset of $\mathcal{H}$ is a compact subset of $\mathcal{H}$

Bibliography

[1] Scott Aaronson. "Read the fine print". In: *Nature Physics* 11.4 (2015), p. 291.

[2] Scott Aaronson. "The learnability of quantum states". In: *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. Vol. 463. 2088. The Royal Society. 2007, pp. 3089–3114.

[3] Andris Ambainis. "Variable time amplitude amplification and quantum algorithms for linear algebra problems". In: *STACS'12 (29th Symposium on Theoretical Aspects of Computer Science)*. Vol. 14. LIPIcs. 2012, pp. 636–647.

[4] Srinivasan Arunachalam and Ronald de Wolf. "Guest column: a survey of quantum learning theory". In: *ACM SIGACT News* 48.2 (2017), pp. 41–67.

[5] Srinivasan Arunachalam and Ronald de Wolf. "Optimal quantum sample complexity of learning algorithms". In: *arXiv preprint arXiv:1607.00932* (2016).

[6] Jacob Biamonte et al. "Quantum machine learning". In: *Nature* 549.7671 (2017), p. 195.

[7] Gilles Brassard et al. "Quantum amplitude amplification and estimation". In: *Contemporary Mathematics* 305 (2002), pp. 53–74.

[8] Nader H Bshouty and Jeffrey C Jackson. "Learning DNF over the uniform distribution using a quantum example oracle". In: *SIAM Journal on Computing* 28.3 (1998), pp. 1136–1153.

[9] Yudong Cao et al. "Quantum Circuit Design for Solving Linear Systems of Equations". In: 110 (Oct. 2011).

[10] Andrew M Childs, Robin Kothari, and Rolando D Somma. "Quantum linear systems algorithm with exponentially improved dependence on precision". In: *arXiv preprint arXiv:1511.02306* (2015).

[11] Carlo Ciliberto et al. "Quantum machine learning: a classical perspective". In: *Proc. R. Soc. A* 474.2209 (2018), p. 20170551.

[12] Don Coppersmith and Shmuel Winograd. "Matrix multiplication via arithmetic progressions". In: *Proceedings of the nineteenth annual ACM symposium on Theory of computing*. ACM. 1987, pp. 1–6.

[13] Daoyi Dong et al. "Quantum reinforcement learning". In: *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)* 38.5 (2008), pp. 1207–1220.

[14] Vedran Dunjko and Hans J Briegel. "Machine learning & artificial intelligence in the quantum domain: a review of recent progress". In: *Reports on Progress in Physics* (2018). URL: http://iopscience.iop.org/10.1088/1361-6633/aab406.

[15] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. "A quantum approximate optimization algorithm". In: *arXiv preprint arXiv:1411.4028* (2014).

[16] Jerome Friedman, Trevor Hastie, and Robert Tibshirani. *The elements of statistical learning*. Vol. 1. Springer series in statistics New York, 2001.

[17] András Gilyén, Seth Lloyd, and Ewin Tang. "Quantum-inspired low-rank stochastic regression with logarithmic dependence on the dimension". In: *arXiv preprint arXiv:1811.04909* (2018).

[18] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. "Quantum random access memory". In: *Physical review letters* 100.16 (2008), p. 160501.

[19] Gene H Golub and Charles F Van Loan. *Matrix computations*. Vol. 3. JHU Press, 2012.

[20] Lov K Grover. "A fast quantum mechanical algorithm for database search". In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. ACM. 1996, pp. 212–219.

[21] Vojtech Havlicek et al. "Supervised learning with quantum enhanced feature spaces". In: *arXiv preprint arXiv:1804.11326* (2018).

[22] Ravindran Kannan and Santosh Vempala. "Randomized algorithms in numerical linear algebra". In: *Acta Numerica* 26 (2017), pp. 95–135.

[23] Iordanis Kerenidis and Anupam Prakash. "Quantum recommendation systems". In: *arXiv preprint arXiv:1603.08675* (2016).

[24] Seth Lloyd. "Quantum algorithm for solving linear systems of equations". In: *APS March Meeting Abstracts*. 2010.

[25] Seth Lloyd, Silvano Garnerone, and Paolo Zanardi. "Quantum algorithms for topological and geometric analysis of data". In: *Nature communications* 7 (2016), p. 10138.

[26] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. "Quantum algorithms for supervised and unsupervised machine learning". In: *arXiv preprint arXiv:1307.0411* (2013).

[27] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. "Quantum principal component analysis". In: *Nature Physics* 10.9 (2014), p. 631.

[28] Seth Lloyd and Christian Weedbrook. "Quantum generative adversarial learning". In: *arXiv preprint arXiv:1804.09139* (2018).

[29] Kosuke Mitarai et al. "Quantum Circuit Learning: Framework for Machine Learning with Quantum Enhanced Feature Space." In: ().

[30] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[31] Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014.

[32] Patrick Rebentrost, Masoud Mohseni, and Seth Lloyd. "Quantum support vector machine for big data classification". In: *Physical review letters* 113.13 (2014), p. 130503.

[33] Cynthia Rudin. "Support Vector Machines". In: *Duke Course Notes* ().

[34] Maria Schuld, Ilya Sinayskiy, and Francesco Petruccione. "Prediction by linear regression on a quantum computer". In: *Physical Review A* 94.2 (2016), p. 022342.

[35] Changpeng Shao. "Reconsider HHL algorithm and its related quantum machine learning algorithms". In: *arXiv preprint arXiv:1803.01486* (2018).

[36] Richard S Sutton and Andrew G Barto. *Reinforcement learning: An introduction*. Vol. 1. 1. MIT press Cambridge, 1998.

[37] Ewin Tang. "Quantum-inspired classical algorithms for principal component analysis and supervised clustering". In: *arXiv preprint arXiv:1811.00414* (2018).

[38] Nathan Wiebe, Daniel Braun, and Seth Lloyd. "Quantum algorithm for data fitting". In: *Physical review letters* 109.5 (2012), p. 050505.

[39] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[40] Leonard Wossnig, Zhikuan Zhao, and Anupam Prakash. "Quantum linear system algorithm for dense matrices". In: *Physical review letters* 120.5 (2018), p. 050502.

[41] VU Thi Xuan. "CR04 Report: Solving linear equations on a quantum computer". In: (2016).

[42] Zhikuan Zhao et al. "A note on state preparation for quantum machine learning". In: *arXiv preprint arXiv:1804.00281* (2018).

[43] Zhikuan Zhao et al. "Quantum algorithms for training Gaussian Processes". In: *arXiv preprint arXiv:1803.10520* (2018).

[44] Yarui Zheng et al. "Solving systems of linear equations with a superconducting quantum processor". In: *Physical review letters* 118.21 (2017), p. 210504.