Chapter 1

Mathematical Preliminaries

1.1 Complexity Theory

While this thesis is for the physics department, many of the results require some basic quantum complexity theory. In particular, the computer science idea for classification of computational problems in terms of the requisite resources gives a particularly nice interpretation of why certain physical systems don't equilbriate, and give a simple explanation on why certain systems do not have a known closed form solution.

This is a simple introduction, with a focus designed to make the rest of this thesis comprehensible to those without a background in complexity theory. For a more formal introduction to Complexity Theory, I would recommend [**?**], with a more in depth review found in [**?**]. For a focus on complexity as found in quantum information, I would recommend [**?**].

1.1.1 Languages and promise problems

The main foundation of computational complexity is in the classification of languages based on the requisite number of resources to determine whether some string is in a language. Unfortunately, this requires the definition of many of these terms.

In particular, what exactly is a string? Any person who has taken a basic programming class knows that a string is simply a word, but the mathematical definition is slightly more complicated. In particular, we first need to define an alphabet, and then define a string over a particular alphabet.

Definition 1 (Alphabet)**.** An alphabet is a finite collection of symbols.

Usually, an arbitrary alphabet is denoted by Γ, while the binary alphabet is denoted by $\Sigma = \{0, 1\}$. Usually, the particular alphabet has no impact on a particular complexity result, as any finite alphabet can be represented via the binary alphabet with overhead that is logarithmic in the size of the alphabet (basically, just use a binary encoding of the new alphabet).

With this definition of an alphabet, a string is simply a finite sequence of elements from the alphabet. In particular, we define Γ^n to be all length n sequences of elements from Γ,

and then define

$$\Gamma^* = \bigcup_{n=0}^{\infty} \Gamma^n. \tag{1.1}$$

With this Γ^* is the set of all strings over Γ.

With this, computational complexity then deals with understanding subsets of these strings. In particular, let Π_{yes} be a subset of Γ^*. The language problem related to Π_{yes} is then to understand what resources are necessary to determine whether a given $x \in \Gamma^*$ is also contained in Π_{yes}. This can be trivial, such as for the case of $\Pi_{\text{yes}} = \Gamma^*$, or it can be impossible, such as in the case of the famous Halting Problem.

[**TO DO:** *Find halting problem stuff*]

Related to these language problems are promise problems, in which there are two subsets of Γ^*, namely Π_{yes} and Π_{no}, such that $\Pi_{\text{yes}} \cap \Pi_{\text{no}} = \emptyset$. We are then *promised* that the $x \in \Gamma^*$ that we need to sort is contained either $\Pi_{\text{yes}} \cup \Pi_{\text{no}}$. This generally opens up some more interesting problems, as without this restriction certain complexity classes do not make sense.

1.1.2 Turing machines

Up to this point, we have only discussed various classifications of strings, and stated that we will want to understand the various resources required to sort a given string into one of two different strings, but we have not explained how these resources are defined. There are various ways to do this, depending on the various computational model one is interested in, but at the highest level, we really only need to define a Turing machine.

These are a mathematical construction, that allow for the explicit definition of algorithms. In particular, they consist of a "finite-state machine" and an infinite tape. The finite-state machine is essentially just a small number of internal states, and the infinite state represents the ability to write down and then read an unbounded amount of information. The intuitive idea behind this construction is that the finite-state machine encodes some finite algorithm (which does not depend on the input to the algorithm), while the infinite tape holds the input to the problem, along with a workspace so that the Turing machine can keep track of various pieces of information.

More concretely,

[**TO DO:** *Get turing Machine stuff*]

1.1.2.1 Reductions

Note that up to this point, we have not noticed any relations between different languages.

1.1.3 Useful complexity classes

Once we have an understanding of what defines a relation, and how these are related, we can attempt to classify those languages that require different resources in order to solve.

1.1.3.1 Classical complexity classes

Perhaps the most well known question in computational complexity is the Pvs NPproblem. However, what exactly are these classes. At a most basic level, one can think of Pas those classification problems that have an efficient classical solution, while NPare those that can be checked in an efficient manner.

Definition 2 (P)**.** A promise problem ...

Definition 3 (NP)**.** A promise problem ...

1.1.3.2 Bounded-Error Quantum Polynomial Time

Intuitively, the idea behind Bounded-Error Quantum Polynomial Time (BQP) consists of those problems that can be solved by a quantum computer efficiently.

Definition 4 (BQP)**.** A promise problem $\Pi = (\Pi_{\text{yes}}, \Pi_{\text{no}})$ if there exist polynomials

1.1.3.3 Quantum Merlin-Arthur

In addition to having an understanding of when a quantum computer can solve a particular problem, we will also want an understanding of those problems that most likely cannot be

Definition 5 (QMA)**.** A promise problem $\Pi = (\Pi_{\text{yes}}, \Pi_{\text{no}})$ if there ..

1.2 Various Mathematical Lemmas

In addition to these various complexity results, it will also be useful to have a list of certain mathematical lemmas that will be used several times in the thesis. These lemmas might also be of independent interest.

1.2.1 Truncation Lemma

Perhaps the first such lemma we called the truncation lemma. The idea behind this lemma is to approximate the evolution of a state under some particular Hamiltonian with another, where the differences between the two Hamiltonians only occur far from the support of the given state. One would expect that since the state must evolve "far" in order to reach the differs between the two Hamiltonians, the evolution between the two will be close. This lemma makes this intuition exact.

Lemma 1 (Truncation Lemma)**.** *Let H be a Hamiltonian acting on a Hilbertspace $\mathcal{H}$ and let $|\Phi\rangle \in \mathcal{H}$ be a normalized state. Let $\mathcal{K}$ be a subspace of $\mathcal{H}$, let P be the projector onto $\mathcal{K}$, and let $\tilde{H} = PHP$ be the Hamiltonian within this subspace. Suppose that, for some $T > 0$, $W \in \{H, \tilde{H}\}$, $N_0 \in \natural$, and $\delta > 0$, we have, for all $0 \leq t \leq T$,*

$$e^{-iWt}|\Phi\rangle = |\gamma(t)\rangle + |\epsilon(t)\rangle \text{ with } \||\epsilon(t)\rangle\| \leq \delta$$

and

$$(1-P)H^r|\gamma(t)\rangle = 0 \text{ for all } r \in \{0,1,\ldots,N_0-1\}.$$

Then, for all $0 \le t \le T$,

$$\left\| \left(e^{-iHt} - e^{-i\tilde{H}t}\right)|\Phi\rangle \right\| \le \left(\frac{4e\|H\|t}{N_0} + 2\right)\left(\delta + 2^{-N_0}(1+\delta)\right).$$

Proposition 1. *Let* H *be a Hamiltonian acting on a Hilbert space* $\mathcal{H}$*, and let* $|\Phi\rangle \in \mathcal{H}$ *be a normalized state. Let* $\mathcal{K}$ *be a subspace of* $\mathcal{H}$ *such that there exists an* $N_0 \in \natural$ *so that for all* $|\alpha\rangle \in \mathcal{K}^\perp$ *and for all* $n \in \{0,1,2,\ldots,N_0-1\}$, $\langle\alpha|H^n|\Phi\rangle = 0$*. Let* P *be the projector onto* $\mathcal{K}$ *and let* $\tilde{H} = PHP$ *be the Hamiltonian within this subspace. Then*

$$\|e^{-it\tilde{H}}|\Phi\rangle - e^{-itH}|\Phi\rangle\| \le 2\left(\frac{e\|H\|t}{N_0}\right)^{N_0}.$$

Proof. Define $|\Phi(t)\rangle$ and $|\tilde{\Phi}(t)\rangle$ as

$$|\Phi(t)\rangle = e^{-itH}|\Phi\rangle = \sum_{k=0}^{\infty}\frac{(-it)^k}{k!}H^k|\Phi\rangle \qquad |\tilde{\Phi}(t)\rangle = e^{-it\tilde{H}}|\Phi\rangle = \sum_{k=0}^{\infty}\frac{(-it)^k}{k!}\tilde{H}^k|\Phi\rangle.$$

Note that by assumption, $\tilde{H}^k|\Phi\rangle = H^k|\Phi\rangle$ for all $k < N_0$, and thus the first N_0 terms in the two above sums are equal. Looking at the difference between these two states, we have

$$\begin{aligned}
\||\Phi(t)\rangle - |\tilde{\Phi}(t)\rangle\| &= \left\|\sum_{k=0}^{\infty}\frac{(-it)^k}{k!}\left(H^k - \tilde{H}^k\right)|\Phi\rangle\right\| \\
&= \left\|\sum_{k=0}^{N_0-1}\frac{(-it)^k}{k!}\left(H^k - \tilde{H}^k\right)|\Phi\rangle - \sum_{k=N_0}^{\infty}\frac{(-it)^k}{k!}\left(H^k - \tilde{H}^k\right)|\Phi\rangle\right\| \\
&\le \sum_{k=N_0}^{\infty}\frac{t^k}{k!}\left(\|H\|^k + \|\tilde{H}\|^k\right) \\
&\le 2\sum_{k=N_0}^{\infty}\frac{t^k}{k!}\|H\|^k
\end{aligned}$$

where the last step uses the fact that $\|\tilde{H}\| \le \|P\|\|H\|\|P\| = \|H\|$. Thus for any $c \ge 1$, we have

$$\begin{aligned}
\||\Phi(t)\rangle - |\tilde{\Phi}(t)\rangle\| &\le \frac{2}{c^{N_0}}\sum_{k=N_0}^{\infty}\frac{(ct)^k}{k!}\|H\|^k \\
&\le \frac{2}{c^{N_0}}\exp(ct\|H\|).
\end{aligned}$$

We obtain the best bound by choosing $c = N_0/\|Ht\|$, which gives

$$\||\Phi(t)\rangle - |\tilde{\Phi}(t)\rangle\| \le 2\left(\frac{e\|H\|t}{N_0}\right)^{N_0}$$

as claimed. (If $c < 1$ then the bound is trivial.) □

Proposition 2. *Let $U_1, \ldots, U_n$ and $V_1, \ldots, V_n$ be unitary operators. Then for any $|\psi\rangle$,*

$$\left\| \left(\prod_{i=n}^{1} U_i - \prod_{i=n}^{1} V_i \right) |\psi\rangle \right\| \leq \sum_{j=1}^{n} \left\| (U_j - V_j) \prod_{i=j-1}^{1} U_i |\psi\rangle \right\|. \tag{1.2}$$

Proof. The proof is by induction on n. The case $n = 1$ is obvious. For the induction step, we have

$$\left\| \left(\prod_{i=n}^{1} U_i - \prod_{i=n}^{1} V_i \right) |\psi\rangle \right\| = \left\| \left(\prod_{i=n}^{1} U_i - V_n \prod_{i=n-1}^{1} U_i + V_n \prod_{i=n-1}^{1} U_i - \prod_{i=n}^{1} V_i \right) |\psi\rangle \right\| \tag{1.3}$$

$$\leq \left\| (U_n - V_n) \prod_{i=n-1}^{1} U_i |\psi\rangle \right\| + \left\| \left(\prod_{i=n-1}^{1} U_i - \prod_{i=n-1}^{1} V_i \right) |\psi\rangle \right\| \tag{1.4}$$

$$\leq \sum_{j=1}^{n} \left\| (U_j - V_j) \prod_{i=j-1}^{1} U_i |\psi\rangle \right\| \tag{1.5}$$

where the last step uses the induction hypothesis. □

Proof of Lemma 1. For $M \in \natural$ write

$$\begin{aligned}
\|(e^{-iHt} - e^{-i\tilde{H}t})|\Phi\rangle\| &= \left\| \left(\left(e^{-iH\frac{t}{M}}\right)^M - \left(e^{-i\tilde{H}\frac{t}{M}}\right)^M \right) |\Phi\rangle \right\| \\
&\leq \sum_{j=1}^{M} \left\| \left(e^{-iH\frac{t}{M}} - e^{-i\tilde{H}\frac{t}{M}}\right) e^{-iW(j-1)\frac{t}{M}} |\Phi\rangle \right\| \\
&\leq \sum_{j=1}^{M} \left\| \left(e^{-iH\frac{t}{M}} - e^{-i\tilde{H}\frac{t}{M}}\right) \left(|\gamma(\tfrac{(j-1)t}{M})\rangle + |\epsilon(\tfrac{(j-1)t}{M})\rangle \right) \right\| \\
&\leq 2M\delta + \sum_{j=1}^{M} \left\| \left(e^{-iH\frac{t}{M}} - e^{-i\tilde{H}\frac{t}{M}}\right) \frac{|\gamma(\frac{(j-1)t}{M})\rangle}{\left\||\gamma(\frac{(j-1)t}{M})\rangle\right\|} \right\| \left\| |\gamma(\tfrac{(j-1)t}{M})\rangle \right\| \\
&\leq 2M\delta + 2M \left(\frac{e\|H\|t}{MN_0} \right)^{N_0} (1+\delta)
\end{aligned}$$

where in the second line we have used Proposition **??** and in the last step we have used Proposition **??** and the fact that $\||\gamma(t)\rangle\| \leq 1 + \delta$. Now, for some $\eta > 1$, choose

$$M = \left\lceil \frac{\eta e \|H\| t}{N_0} \right\rceil$$

for $0 < t \leq T$ to get

$$\begin{aligned}
\|(e^{-iHt} - e^{-i\tilde{H}t})|\Phi\rangle\| &\leq 2M \left(\delta + \eta^{-N_0}(1+\delta)\right) \\
&\leq 2 \left(\frac{\eta e \|H\| t}{N_0} + 1 \right) \left(\delta + \eta^{-N_0}(1+\delta)\right).
\end{aligned}$$

The choice $\eta = 2$ gives the stated conclusion. □

Note that it would be slightly better to take a smaller value of η. However, this does not significantly improve the final result; the above bound is simpler and sufficient for our purposes.

1.2.2 Nullspace Projection Lemma

Lemma 2 (Nullspace Projection Lemma)**.** *Let H_A and H_B be positive semi-definite matrices. Suppose that the nullspace, S, of H_A is nonempty, and that*

$$\gamma\big(H_B|_S\big) \geq c > 0 \qquad \textit{and} \qquad \gamma(H_A) \geq d > 0. \tag{1.6}$$

Then,

$$\gamma(H_A + H_B) \geq \frac{cd}{d + \|H_B\|}. \tag{1.7}$$

Proof. Let $|\psi\rangle$ be a normalized state satisfying

$$\langle\psi|H_A + H_B|\psi\rangle = \gamma(H_A + H_B). \tag{1.8}$$

Let Π_S be the projector onto the nullspace of H_A. First suppose that $\Pi_S|\psi\rangle = 0$, in which case

$$\langle\psi|H_A + H_B|\psi\rangle \geq \langle\psi|H_A|\psi\rangle \geq \gamma(H_A) \tag{1.9}$$

and the result follows. On the other hand, if $\Pi_S|\psi\rangle \neq 0$ then we can write

$$|\psi\rangle = \alpha|a\rangle + \beta|a^\perp\rangle \tag{1.10}$$

with $|\alpha|^2 + |\beta|^2 = 1$, $\alpha \neq 0$, and two normalized states $|a\rangle$ and $|a^\perp\rangle$ such that $|a\rangle \in S$ and $|a^\perp\rangle \in S^\perp$. (If $\beta = 0$ then we may choose $|a^\perp\rangle$ to be an arbitrary state in $S^\perp$ but in the following we fix one specific choice for concreteness.) Note that any state $|\phi\rangle$ in the nullspace of $H_A + H_B$ satisfies $H_A|\phi\rangle = 0$ and hence $\langle\phi|a^\perp\rangle = 0$. Since $\langle\phi|\psi\rangle = 0$ and $\alpha \neq 0$ we also see that $\langle\phi|a\rangle = 0$. Hence any state

$$|f(q, r)\rangle = q|a\rangle + r|a^\perp\rangle \tag{1.11}$$

is orthogonal to the nullspace of $H_A + H_B$, and

$$\gamma(H_A + H_B) = \min_{|q|^2+|r|^2=1} \langle f(q, r)|H_A + H_B|f(q, r)\rangle. \tag{1.12}$$

Within the subspace Q spanned by $|\,a\,\rangle$ and $|\,a^\perp\,\rangle$, note that

$$H_A|_Q = \begin{pmatrix} w & v^* \\ v & z \end{pmatrix} \qquad H_B|_Q = \begin{pmatrix} 0 & 0 \\ 0 & y \end{pmatrix} \tag{1.13}$$

where $w = \langle a|H_B|a\rangle$, $v = \langle a^\perp|H_B|a\rangle$, $y = \langle a^\perp|H_A|a^\perp\rangle$, and $z = \langle a^\perp|H_B|a^\perp\rangle$, and that we are interested in the smaller eigenvalue of

$$M = H_A|_Q + H_B|_Q = \begin{pmatrix} w & v^* \\ v & y + z \end{pmatrix}. \tag{1.14}$$

Letting ϵ_+ and ϵ_- be the two eigenvalues of M with $\epsilon_+ \geq \epsilon_-$, note that

$$\epsilon_+ = \|M\| \leq \|H_A|_Q\| + \|H_B|_Q\| \leq y + \|H_B|_Q\| \leq y + \|H_B\|, \tag{1.15}$$

where we have used the Cauchy interlacing theorem to note that $\|H_B|_Q\| \leq \|H_B\|$. Additionally, we have that

$$\epsilon_+\epsilon_- = \det(M) = w(y+z) - |v|^2 \geq wy \tag{1.16}$$

where we used the fact that $H_B|_Q$ is positive-semidefinite. Putting this together, we have that

$$\gamma(H_A + H_B) = \min_{|q|^2+|r|^2=1} \langle f(q,r)|H_A + H_B|f(q,r)\rangle = \epsilon_- \geq \frac{wy}{y + \|H_B\|}. \tag{1.17}$$

As the right hand side increased monotonically with both w and y, and as $w \geq \gamma(H_B|_S) \geq c$ and $y \geq \gamma(H_A) \geq d$, we have

$$\gamma(H_A + H_B) \geq \frac{cd}{d + \|H_B\|} \tag{1.18}$$

as required. □