CMPT 476/776: Introduction to Quantum Algorithms
Assignment 0 — Mathematical preliminaries

Not graded.

This is **not** a homework assignment; neither completion nor submission is required. It is only meant to help you review prerequisite concepts and fill in any gaps which we will not otherwise present in the course.

Question 1: Complex numbers

Quantum mechanics, and by extension computation, makes heavy use of complex numbers and arithmetic (though there is no theoretical reason it needs to[1]). For review, we briefly recall some basic facts of complex numbers:

- The **complex numbers** $\mathbb{C}$ are those of the form $z = a + bi$, where $i = \sqrt{-1}$ is the complex unit and $a, b \in \mathbb{R}$ are real numbers.
- $\mathrm{Re}(z) = a$ is the **real** part of $z \in \mathbb{C}$.
- $\mathrm{Im}(z) = b$ is the **imaginary** part of $z \in \mathbb{C}$.
- $z^* = a - bi$ if the **complex conjugate** of z (also written $\overline{z}$).
- $z = re^{i\theta}$ is the **polar form** of z, where $r, \theta \in \mathbb{R}$. $r = |z| = \sqrt{a^2 + b^2}$ is called the **magnitude** of z and θ is the **phase** corresponding to the angle between the x-axis and z when written in the complex plane.
- In polar form, $z^* = (re^{i\theta})^* = re^{-i\theta}$
- (**Euler's formula**) $e^{i\theta} = \cos(\theta) + i\sin(\theta)$.

Exercises:

1. Compute the following in standard form :
   - $(2 + 3i) + (1 - 4i)$
   - $(1 + 2i)(3 - i)$
   - $|4 - 3i|$

[1] T. Hoffreumon, M. Woods, Quantum theory does not need complex numbers.

- $\frac{2+i}{1-3i}$

2. Compute the following in polar form :
   - $4-3i$
   - $(2e^{i\pi/4})(5e^{i\pi/8})$
   - $(3e^{i\pi/4})^2$
   - $\frac{1}{7e^{i3\pi/5}}$
3. Verify that $z+z^* = 2\text{Re}(z)$
4. Verify that $z-z^* = 2i\text{Im}(z)$
5. Verify that $zz^* = |z|^2$

Question 2: Linear algebra

> Everything is linear somewhere
> — *Someone, probably*

As with most mathematics, the most convenient way to work with quantum mechanics is via linear algebra. We briefly review the basics of linear algebra which we will need in this course.

Recall that a vector space V over a field F is a set of vectors $\mathbf{v} \in V$ such that (1) for any $\mathbf{v}, \mathbf{u} \in V$, $\mathbf{v} \pm \mathbf{u}$ is defined (**vector addition**), and (2) for any $\mathbf{v} \in V$ and $a \in F$, av is defined (**scalar multiplication**). Every vector space also has a unique **zero vector** $\mathbf{0} \in V$ with the obvious properties.

Given a set of vectors $B = \{\mathbf{u}_1, \dots, \mathbf{u}_n\} \subset V$, the **linear span** of B, denoted span $B \subseteq V$, is the set of formal F-linear combinations of elements of B — that is, vectors of the form

$$a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_n\mathbf{u}_n \in V$$

where $a_1, \dots, a_n \in F$. We say the set B is **linearly independent** if $a_1\mathbf{u}_1 + a_2\mathbf{u}_2 + \cdots + a_n\mathbf{u}_n = 0$ implies $a_1, \dots, a_n$ are all 0 — that is, no vector in B can be written as a linear combination of other vectors of B. If span $B = V$, then B is a **basis** of V, and the **dimension** of V is $n = \dim V$. **Since we work in finite dimensions, our vector spaces will always have a basis, and we will typically view vectors as linear combinations of basis vectors so understanding bases is very important**.

A **linear transformation** $T : V \to W$ from a vector space V to W is function from V to W which is linear, in that $T(a\mathbf{u} + b\mathbf{v}) = aT(\mathbf{u}) + bT(\mathbf{v})$ for all $a, b \in F$ and $\mathbf{u}, \mathbf{v} \in V$. A linear transformation T is typically represented by a **matrix** A, in which case $T(\mathbf{u}) = A\mathbf{u}$ — that is, T sends a vector $\mathbf{u}$ to the vector $A\mathbf{u}$ defined by matrix-vector multiplication. We say that $\mathbf{u}$ is an **eigenvector** of A if $A\mathbf{u} = \lambda\mathbf{u}$ for some scalar $\lambda \in F$ called an **eigenvalue**. We will review **diagonalization** in class as it's something you may not have previously seen in 232/240.

Recall that the standard **inner product** on real vector spaces is defined as $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^T\mathbf{v} = \sum_i u_i v_i$ — that is, transpose $\mathbf{u}$ to get a row vector and multiply. In complex vector spaces, we similarly define the inner product as $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^\dagger\mathbf{v} = \sum_i u_i^* v_i$ where $\mathbf{u}^\dagger$ is the **conjugate-transpose** as seen in class, obtained by taking the transpose and conjugating each entry. Given an inner product on V, we then define the standard Euclidean **norm** on V as $||\mathbf{v}|| = \sqrt{\langle \mathbf{v}, \mathbf{v} \rangle} = \sqrt{\sum_i |u_i|^2}$.

Exercises:

1. Let $\mathbf{v} = \begin{bmatrix} 1+i \\ 2-i \\ -i \end{bmatrix}$.

   (a) Compute the norm of $\mathbf{v}$.

   (b) Normalize $\mathbf{v}$ to obtain a unit vector.

2. Compute $A\mathbf{v}$ where $A = \begin{bmatrix} 2 & i & 1 \\ -i & 3 & -i \\ 1 & i & 4 \end{bmatrix}$ and $\mathbf{v} = \begin{bmatrix} 1 \\ -i \\ 2 \end{bmatrix}$.

3. Write the matrix $A = \begin{bmatrix} 2 & i & 1 \\ -i & 3 & -i \\ 1 & i & 4 \end{bmatrix}$ in reduced Echelon form via Gaussian elimination.

4. Consider the matrix $B = \begin{bmatrix} 0 & -i & 0 \\ i & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

   (a) Find the eigenvalues of B.

   (b) Find the eigenvectors corresponding to each eigenvalue and normalize them.

5. Let $\mathbf{v}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, $\mathbf{v}_2 = \begin{bmatrix} 1 \\ 1+i \\ 1+i \end{bmatrix}$, and $\mathbf{v}_3 = \begin{bmatrix} 1 \\ 5 \\ 5 \end{bmatrix}$.

   (a) Write each vector as a linear combination over the standard basis of $\mathbb{C}^3$:

   $$\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \mathbf{e}_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

   (b) Does $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ form a basis for $\mathbb{C}^3$?

   (c) What is the dimension of the subspace spanned by $\{\mathbf{v}_2, \mathbf{v}_3\}$? What about just $\{\mathbf{v}_3\}$?

Question 3: Probability theory

As quantum mechanics is inherently probabilistic, probability theory naturally factors into quantum computation. Refresh yourself on some basics of probability theory with the exercises below:

1. A box contains 3 red balls and 2 blue balls. Two balls are drawn at random without replacement.

   (a) What is the probability that the first ball drawn is red?

   (b) Given that the first ball drawn is red, what is the probability that the second ball drawn is also red?

    (c) What is the probability that both balls drawn are red?

2. A discrete random variable X represents the number rolled on a fair six-sided die. Compute the expected value of X.

3. A factory produces items from three machines: Machine A, Machine B, and Machine C.

   - 50% of the items are from Machine A, 30% from Machine B, and 20% from Machine C.
   - The probabilities of a defective item are 2%, 5%, and 10% for Machines A, B, and C, respectively.

   (a) What is the probability that a randomly selected item is defective?

   (b) If an item is found to be defective, what is the probability it was produced by Machine B?

4. A test for a disease has the following characteristics:

   - 99% of people with the disease test positive.
   - 95% of people without the disease test negative.
   - 1% of the population has the disease.

   If a person tests positive, what is the probability they actually have the disease? Use Baye's theorem,

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

Question 4: Discrete math

A few concepts from discrete math which will be helpful to review, notably modular arithmetic and some elementary number theory necessary for Shor's algorithm. These should be trivial and serve only as reminders of the concepts.

1. Compute the following:

   - $27 \mod 5$,
   - $123 \mod 17$,
   - $-11 \mod 7$.

2. Solve $3x \equiv 1 \pmod 5$ for x.

3. Factorize 84 into its prime components.

4. Compute the greatest common divisor (GCD) of 24 and 36

5. Compute the least common multiple (LCM) of 24 and 36