CSE 190 / Math 152 - Introduction to Quantum Computing
Homework 1
Due **Tuesday, April 9th, 1:30pm**

Instructions: There may be opportunities to work in groups for future assignments, but since this assignment is the basis for all future work in this class, it is important that it is completed individually.

It is highly recommended (though not required) that you type your answers. It is your responsibility to make any handwriting clear and legible for grading. A LaTeX template for the homework is provided on Canvas.

For many of the problems below, I ask you to "prove" some fact. In general in this class, there is no specific structure of a proof that I am looking for. Most of the proofs of the identities below can be shown by just computing two quantities and showing that they are evidently the same.

We will only be grading some of the problems below for correctness. However, because all of the concepts are important, we will not reveal which problems are being graded for correctness until after the assignment has been submitted. The remaining problems will be graded for completeness (i.e., does it look like there was a good-faith effort to solve the problem?).

Problems:

1. **Complex numbers fundamentals**

Quantum mechnical systems are described by vectors of complex numbers. Therefore, it is important to review some important properties of complex numbers. We will use the symbol $\mathbb{R}$ to denote the set of all real numbers and the symbol $\mathbb{C}$ to denote the set of all complex numbers. That is,

$$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R} \text{ and } i^2 = -1\}$$

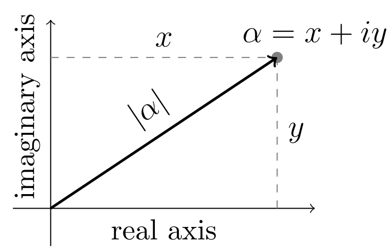
For complex number $\alpha = x + iy$, we say that x is the *real part* of α and y is the *imaginary part* of α.

(a) **Complex conjugate**: for every complex number $\alpha = x+iy$, we define its *complex conjugate* as $\alpha^* := x - iy$. As a note of warning, we will mostly write the complex conjugate as α^*, but it is also common to see it written as $\overline{\alpha}$. Let $\alpha, \beta \in \mathbb{C}$ be any two complex numbers. Prove the following two identities:

i. $(\alpha\beta)^* = \alpha^*\beta^*$

ii. $(\alpha + \beta)^* = \alpha^* + \beta^*$

(b) **Magnitude**: As shown on the right, we can think of a complex number $\alpha = x + iy$ as a vector in 2-dimensional space, where the real and imaginary parts are the two components. The *absolute value* or *magnitude* of α, which we denote by $|\alpha|$, is just the length of this vector. That is, $|\alpha| = \sqrt{x^2 + y^2}$.



Once again, let $\alpha, \beta \in \mathbb{C}$ be arbitrary complex numbers. Prove the following facts:

i. $|\alpha| = \sqrt{\alpha\alpha^*}$.

ii. $|\alpha\beta| = |\alpha| \cdot |\beta|$. In other words, the magnitude of the product of two complex numbers is the product of their magnitudes.

iii. $\alpha = 0$ if and only if $|\alpha| = 0$. In other words, the magnitude of a complex number is 0 exactly when the complex number is 0.

2. **Linear algebra fundamentals**

The following problems are intended to be a review of what you've learned in a previous linear algebra class (Math 18 or similar). At some level, quantum computation consists entirely of multiplying a vector by a matrix. Therefore, these concepts need to become second nature.

A complex matrix $A \in \mathbb{C}^{n \times m}$ is a rectangular array of complex numbers with n rows and m columns. We denote by $A_{i,j}$ the entry at row i and column j.

(a) **Matrix multiplication**: Let $A \in \mathbb{C}^{n \times m}$ and $B \in \mathbb{C}^{m \times p}$ be complex matrices. We define the product of these two matrices AB to be the $n \times p$ matrix such that (i, j)th entry is $(AB)_{i,j} = \sum_{k=1}^{m} A_{i,k} B_{k,j}$. We can extend matrix multiplication to complex vectors $v \in \mathbb{C}^n$ by thinking of v as a $n \times 1$ matrix.

i. Prove that matrix multiplication is not commutative. Namely, give an example of 2×2 matrices A and B such that $AB \neq BA$.

ii. Prove that matrix multiplication *is* distributive. That is, you should show that $A(B+C) = AB+AC$ for any matrices $A \in \mathbb{C}^{n \times m}$, $B \in \mathbb{C}^{m \times p}$, $C \in \mathbb{C}^{m \times p}$.

(b) **Matrix inverse**: The inverse of a matrix $A \in \mathbb{C}^{n \times n}$ (if it exists) is the unique matrix A^{-1} such that $AA^{-1} = A^{-1}A = I$. Here, I is the $n \times n$ identity matrix, which has 1's along the diagonal and 0's everywhere else. If matrix A has an inverse, we say that it is *invertible*.

i. Not all matrices are invertible. For example, the matrix which is 0 everywhere can't have an inverse. Give an example of a 2×2 matrix A such that A is not the all-zeros matrix and yet A still doesn't have an inverse.

ii. True/False: If $A^2 = A$, then A is invertible. Give a short explanation.

iii. True/False: If $A^2 = I$, then A is invertible. Give a short explanation.

(c) **Conjugate transpose**: Given any $n \times m$ matrix A, we define its transpose A^T to be the $m \times n$ matrix where the rows and columns have been swapped. Formally, $(A^T)_{i,j} = A_{j,i}$. We define its conjguate A^* to be the $n \times m$ matrix where we take the complex conjugate of each entry, that is, $(A^*)_{i,j} = A^*_{i,j}$. We define its conugate transpose $A^\dagger$ to be the $m \times n$ matrix where we have taken both the tranpose and the conjugate of A, that is, $A^\dagger = (A^*)^T = (A^T)^*$. Once again, we can extend these operations to complex vectors $v \in \mathbb{C}^n$ by thinking of v as $n \times 1$ matrix. That is, v is a column vector, but $v^\dagger$ is a row vector.

i. Let $A \in \mathbb{C}^{n \times m}$ be a matrix and $v \in \mathbb{C}^n$ and $w \in \mathbb{C}^m$ be vectors. Which of the following are valid linear-algebraic products: vA, $v^\dagger A$, $w^T A$, Aw, $Av^\dagger$?

ii. Prove that $(AB)^\dagger = B^\dagger A^\dagger$ for any matrices $A, B \in \mathbb{C}^{n \times n}$.

iii. Prove that if $A \in \mathbb{C}^{n \times n}$ is invertible, then $A^\dagger$ is invertible.