**Introductory Linear Algebra for Quantum Computing**

**Vectors and Vector Spaces**

Formally, a vector is defined as an element of a set known as a vector space. More intuitively and geometrically, a vector defines a mathematical object with both a magnitude and a direction.

A vector space V over a field F is defined as a set of objects known as vectors, such that the following properties always hold:

Vector addition of any two vectors yields a third vector:

Scalar multiplication yields a vector:

For example, the set over is a vector space. *Proof:*

In quantum computing, most of the vectors are **state vectors**, which point to a specific point in space which corresponds to a specific quantum state. For example, any vector pointing to a point on the Bloch sphere describes a quantum state, and the surface of the Bloch sphere is the state space, wherein it describes all areas where the vector can point.

**Matrices and Matrix Operations**

Matrices are mathematical objects that transform vectors into other vectors

Generally, matrices are written as an array of numbers, such as:

Multiplication of matrices is done row by row and column by column. The first matrix uses its rows, and the second matrix uses its columns.

Matrix multiplication is used to apply a matrix to a vector. Quantum gates manipulate qubits by applying a matrix to the qubit’s vector. For example, the Pauli-X gate is represented by the following matrix:

Consider the two basis states, written as column vectors:

Applying the Pauli-X gate to each of the basis states, we see the following:

A matrix’s conjugate transpose flips the signs of the imaginary components, then reflects it across the main diagonal. For example, consider the Pauli-Y gate.

The Pauli-Y gate happens to be a **Hermitian matrix,** or a matrix that is equal to its conjugate transpose.

The identity matrix, often denoted , “acts trivially” on any other matrix, meaning it has no effect.

Consider the following matrix.

A matrix’s inverse, denoted , is a matrix such that the following holds.

Calculating inverse matrices is sufficiently difficult such that computers are generally used for any matrix larger than 2x2. For a 2x2 matrix, the inverse is defined as:

where is the determinant of the matrix. In the 2x2 case, .

A unitary matrix is a matrix such that its inverse is equal to its conjugate transpose. For example, consider the Pauli-Y gate again. Since the Pauli-Y gate is Hermitian, meaning it’s equal to its conjugate transpose. Thus, if the conjugate transpose of the Pauli-Y gate equals the inverse of the Pauli-Y gate, it must be its own inverse. We can multiply the matrix by its conjugate transpose to see if this is the case.

Unitary matrices will become more important in the section concerning Hilbert spaces, however the general idea is that the evolution of a quantum state through the application of a unitary matrix preserves the norm (magnitude) of the quantum state.

**Spanning Sets, Linear Dependence, and Bases**

Consider some vector space . Some set of vectors is said to span a subspace if every vector in the subspace can be written as a **linear combination** of the vectors in the spanning set.

A linear combination of some collection of vectors in some vector space over a field is defined as an arbitrary sum of these vectors (which itself must be a vector by definition of a vector space):

If a set of vectors spans a space, we’re saying any other vector in this space can be written as a linear combination of these vectors.

A set of vectors is said to be **linearly dependent** if there exist corresponding coefficients for each vector with at least one value of being nonzero, such that the following holds.

This means that the set of vectors can be expressed as linear combinations of each other. Consider some with .

In this case, some vector and coefficient have been pulled out of the series describing the linear combination, and the equation has been rearranged to show that is equal to a linear combination of vectors within the original set.

Notably, if is the only nonzero coefficient, must be the null vector.

For example, consider the vector space over , and the following vectors.

Therefore, the vectors are a linearly dependent combination.

A set of vectors is said to be **linearly independent** if there is no vector in the set that can be expressed as a linear combination of the others. A **basis** of a vector space is simply the smallest possible linearly independent set of vectors that spans the entire space. For example, in quantum computing the basis is the set , since all other vectors can be created out of them.

The basis and linearly dependent sets allow us to consider a small number of vectors instead of an entire set, and form conclusions that can be generalized to the entire vector space.

**Hilbert Spaces, Orthonormality, and the Inner Product**

Hilbert Spaces are one of the most important mathematical constructs in all of quantum mechanics and can be thought of as the vector space in which all quantum state vectors live. The main difference between a Hilbert space and any other vector space is that a Hilbert space is equipped with an operation known as the **inner product**, which is an operation that can be performed between two vectors, returning a scalar.

In the context of quantum mechanics and quantum computation, the inner product between two state vectors returns a scalar quantity representing the amount to which the first vector lies on the second vector. This allows for probabilities of measurement in certain states to be calculated.

For two vectors and in a Hilbert space, the inner product is denoted as , for . Thus, the inner product of two vectors in a Hilbert space looks something like:

One of the most important conditions for a Hilbert space representing a quantum system is the normalization condition, stating the inner product of a vector with itself equals 1: . This means the length of each vector squared must be equal to 1. This means the length of a vector in a particular direction is representative of the probability amplitude of the quantum system in that particular state. The probability of the quantum system being measured in that state must be equal to 1, just as the sum of all the probabilities must be equal to 1.

**Outer Products and Tensor Products**

The **outer product** is an operation performed between two vectors which returns a matrix. For the vectors and in a Hilbert space, this is denoted for . Thus:

Outer products allow us to represent quantum gates as bras and kets, instead of as matrices. For example, take the Pauli-X gate.

We can represent this as . *Proof:*

Outer products are a specific example of the more general **tensor product** used to multiply vector spaces together. Generally, the tensor product describes the shared state of two or more qubits. The tensor product involves multiplying two kets together, so it does not involve conjugate transposes. The tensor product of vectors and , written as or , equals:

If we want to act on the new tensor product , we need the tensor product of the operators. For matrices and , we have:

**Eigenvalues and Eigenvectors**

Consider the relationship:

where is some number. Given some matrix , the vectors and numbers that satisfy this relationship are known as **eigenvectors** and **eigenvalues**, respectively. We exploit an interesting trick to find the eigenvectors and their corresponding eigenvalues. Rearrange the equation as the following:

If we multiply both sides of the equation by the inverse matrix , we find , which is considered an extraneous solution, as we don’t allow eigenvectors to be the null vector. Allowing this would allow any vector or value to satisfy the relationship. To find the allowed eigenvectors and eigenvalues, we must assume the matrix is **non-invertible**. Given some matrix and some variation of the matrix , we recall that the inverse of a matrix is given by:

If the determinate of M is 0, then the resulting inverse is undefined. Thus, it follows that:

We can determine from this, and then plug each value back into the original equation to find . For example, consider the Pauli-Z gate:

It follows that:

When solving the determinant, the resulting equation in terms of is called the characteristic polynomial.

We can plug back in our eigenvalues to find our eigenvectors for the Pauli-Z matrix.

Suppose

This relationship is satisfied for any value of , and . Thus, the basis vector is .

Suppose

This time can be any number, and must be 0. Thus, the basis vector is .

The following properties are very important for gate model of quantum computation, where we deal with finite dimensional vector spaces:

* Hermitian matrices have linearly independent eigenvectors, which form the basis of the vector space.
* The eigenvectors of a unitary matrix form the orthonormal basis of the vector space.

**Matrix Exponentials**

We often see unitary transformations in the form:

where is some real number, and is some Hermitian matrix. All matrices of this form are unitary. This can be trivially proven.

The reason a matrix in an exponential can still be considered a matrix becomes clearer when the function’s Taylor series is considered.

For , we can consider the Mclauren series:

Thus, it follows that:

Therefore, the exponential of a matrix is a matrix.

An **involuntary matrix** is a matrix such that the matrix satisfies . For any matrix , then:

Notice that we can split our power series into an imaginary component and a real component, based on whether n is odd or even.

Recall the Mclauren series for sin and cos:

For , these series are the exact same as our previous series.

Recall that . For any , we have:

Substituting this new information, we find the following:

This relationship is extremely important for quantum computing. Consider the 3 Pauli matrices:

These matrices are among the fundamental gates used to manipulate qubits. These operations are unitary, Hermitian, and involuntary. This means a matrix of the form is not only a valid unitary matrix that can act on a qubit, but can be expressed through the sine-cosine relationship just shown.

One last important note about exponentials: for some matrix with eigenvectors and corresponding eigenvalues , then:

This one is more straightforward to prove. *Proof:*

This is very useful for creating quantum circuits that simulate a certain Hamiltonian.