$\hat{Q}\,|B\rangle$**asics** Terms and Definitions Sheet

1 Complex numbers

Complex number - A complex number is any number of the form $a+bi$, where a, b are real numbers and i is the imaginary unit, satisfying $i^2 = -1$. The set of all complex numbers, denoted $\mathbb{C}$, forms a field. This means that any two complex numbers can be added, multiplied, and divided by any other nonzero complex number. Addition is defined by adding together the real and complex parts of each number, e.g. $(a+bi)+(c+di) = (a+c)+i(b+d)$. Multiplication is performed by using the distributive property, e.g.

$$(a+bi)(c+di) = ac + ibc + iad + i^2bd = (ac-bd) + i(bc+ad)$$

Similarly, the reciprocal of any complex number can be put into the form $a+bi$ by multiplying by the complex conjugate, e.g.

$$\frac{1}{a+bi} = \frac{1}{a+bi}\frac{a-bi}{a-bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \left(\frac{a}{a^2+b^2}\right) - i\left(\frac{b}{a^2+b^2}\right)$$

Complex conjugate - If $z = a+bi$ is a complex number, then the complex conjugate of z, denoted by z^*, is defined to be $z^* = a-bi$. Intuitively, if the complex number z is plotted on a 2D plane, where the real component is plotted on the x-axis and the imaginary component is plotted on the y-axis, then the complex conjugate of z is the reflection across the x-axis. The product $z^*z = a^2+b^2$ is always a real number. Importantly, the complex conjugate is a field isomorphism. This means that if $z_1, z_2 \in \mathbb{C}$, then $(z_1+z_2)^* = z_1^* + z_2^*$ and $(z_1z_2)^* = z_1^*z_2^*$. As a consequence, we also have $\left(\frac{1}{z}\right)^* = \frac{1}{z^*}$.

Magnitude - If $z = a+bi$ is a complex number then the magnitude of z, denoted $|z|$ is $\sqrt{a^2+b^2}$. Equivalently, $|z| = \sqrt{z^*z}$. Plotting the complex number z again on a 2D plane, the magnitude of z corresponds to the distance from z to the origin.

Euler's Formula - If θ is a real angle, then $e^{i\theta} = \cos(\theta) + i\sin(\theta)$. One consequence of this formula is that any complex number $z = a+bi$ can be expressed $z = |z|e^{i\arg(z)}$, where $|z|$ is the magnitude of z and $\arg(z)$ is the angle formed between z as a vector in a 2D plane and the x-axis. This formula also shows that multiplying a complex number by $e^{i\theta}$ is like rotating it in the complex plane, because $e^{i\theta}z = |z|e^{i(\arg(z)+\theta)}$, corresponding to a rotation by an angle θ in the complex plane. Lastly, from the trig identity $\sin^2(\theta)+\cos^2(\theta) = 1$, we see that $e^{i\theta}$ is unimodular: $|e^{i\theta}|^2 = \cos^2(\theta)+\sin^2(\theta) = 1$.

2 Linear Algebra

Vector space A set V is said to be a vector space over a field $\mathbb{F}$ if

- Closure under addition: For any two vectors $\vec{v}_1$ and $\vec{v}_2$ in V, the sum $\vec{v}_1+\vec{v}_2$ is also in V.
- Closure under scalar multiplication: For any scalar α in the field $\mathbb{F}$ and vector $\vec{v}$ in V, the product $\alpha\vec{v}$ is also an element of V.

In quantum computing, the focus is directed toward complex vector spaces, which describe quantum states, so we will only talk about vector spaces over the field $\mathbb{F} = \mathbb{C}$ going forward. The most common example of a complex vector space is $\mathbb{C}^d$, which denotes the set of d-component vectors of complex numbers, with addition and multiplication by scalars defined component-wise. There are more interesting vector spaces to consider. For instance, the set of continuous functions that are square-integrable, i.e. $\int_{\mathbb{C}} |f(x)|^2 dx < \infty$, form a vector space. Another example to consider is the set of all linear operators on a complex vector space, which themselves form a vector space.

Linear map A map $T : V \to V$ is said to be linear if V is a vector space and $T(\alpha\vec{v}+\beta\vec{u}) = \alpha T(\vec{v}) + \beta T(\vec{u})$ for any $\vec{u}, \vec{v} \in V$ and complex numbers α, β. Usually the parentheses are dropped and $T(\vec{v})$ is just written $T\vec{v}$. Linear maps can be thought of as a generalization of matrix multiplication. If M is a matrix, then $M(\alpha\vec{u}+\beta\vec{v}) = \alpha M\vec{u} + \beta M\vec{v}$, so the map $\vec{v} \mapsto M\vec{v}$ is an example of a linear map.

Linear combination If V is a complex vector space and $\vec{v}, \vec{u} \in V$, then a linear combination of $\vec{u}$ and $\vec{v}$ is any vector of the form $\alpha\vec{v}+\beta\vec{u}$, where α, β are complex numbers. Oftentimes, linear combinations are written using summations, e.g. $\vec{v} = \sum_{i=1}^{N} \alpha_i\vec{v}_i$.

Span Given a set of vectors $\{\vec{v}_i\}_{i=1}^N$, the span of these vectors is the set of linear combinations, i.e. $\sum_i \alpha_i \vec{v}_i$ for any complex numbers α_i. The span of a set of vectors is itself a vectors space, as closure both under addition and scalar multiplication can be verified. If V is a vector space, the $\{v_i\}_{i=1}^N$ spans V if $\text{span}(\{v_i\}) = V$. Another way of saying this is that any vector in V may be written as a linear combination of $\{\vec{v}_i\}$.

Linearly independent A set of vectors $\{\vec{v}_i\}_{i=1}^N$ is said to be linearly independent if $\sum_{i=1}^N \alpha_i \vec{e}_i = 0$ implies that $\alpha_i = 0$ for all i. This definition is equivalent to the statement that no vector may be in the span of the others. If this were true, then for some complex numbers α_i, we would have $\vec{v}_N = \sum_{i=1}^{N-1} \alpha_i \vec{v}_i$, which implies that $-\vec{v}_N + \sum_{i=1}^{N-1} \alpha_i \vec{v}_i = 0$, and this is a contradiction to linear independence since $-1 \neq 0$. Linear independence implies that if a vector $\vec{v}$ can be written as a linear combination of $\{\vec{v}_i\}_{i=1}^N$, then this linear combination is unique. To see this, suppose $\vec{v} = \sum_{i=1}^N \alpha_i \vec{v}_i$ and $\vec{v} = \sum_{i=1}^N \beta_i \vec{v}_i$, where $\{\alpha_i\}$ and $\{\beta_i\}$ are two possibly unrelated sets of constants. Then we have

$$\sum_{i=1}^N \alpha_i \vec{v}_i = \sum_{i=1}^N \beta_i \vec{v}_i \implies \sum_{i=1}^N (\alpha_i - \beta_i)\vec{v}_i = 0$$

By linear independence, this gives $\alpha_i = \beta_i$ for all i, showing that the expression is unique. This uniqueness gives a motivation for the next definition. One interesting thing to note about linear independence is that a matrix is invertible if and only if its columns are linearly independent.

Basis If V is a complex vector space and $\{v_i\}_{i=1}^N$ is a linearly independent set that spans V, then $\{v_i\}_{i=1}^N$ is said to be a basis for V. This agrees with intuition from a vector space such as $\mathbb{C}^2$. In this vector space, we typically work with the basis $\binom{1}{0}$ and $\binom{0}{1}$, writing any vector as $\binom{\alpha}{\beta} = \alpha\binom{1}{0} + \beta\binom{0}{1}$.

Matrix representation (of vectors) It is important to note that the choice of basis in which to express vectors is not natural, and different choices of basis will lead to different vector representations. For instance, if $\vec{v} = \binom{1}{0}$ is expressed in the basis $\vec{e}_1 = \binom{1}{1}, \vec{e}_2 = \binom{1}{-1}$, then we would write $\vec{v} = \frac{1}{2}\vec{e}_1 + \frac{1}{2}\vec{e}_2$, and the matrix representation would be $\binom{\frac{1}{2}}{\frac{1}{2}}$. We distinguish between the vector $\vec{v}$ which exists independently of the choice of basis, and the vector or matrix representation of $\vec{v}$ that depends on the choice of basis. In general, if $\{\vec{b}_i\}$ is a basis for V, then $\vec{v} = \sum_{i=1}^N \alpha_i \vec{b}_i$ for a unique collection of constants α_i which are called the components of $\vec{v}$, and $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{pmatrix}$ is called the vector or matrix representation of $\vec{v}$.

Matrix representation (of linear operators) If V is a complex vector space, $\{\vec{b}_i\}$ is a basis for V, and T is a linear map, then $T\vec{v}_j = \sum_i \alpha_{ij} \vec{v}_i$ for some complex numbers α_{ij}. These are called the matrix elements of T, and are usually denoted T_{ij}. This agrees with the usual definition of matrix elements as the i^{th} row and j^{th} column of a matrix. For instance, if we consider the matrix $M = \binom{a\ b}{c\ d}$, then

$$M\binom{1}{0} = \binom{a\ b}{c\ d}\binom{1}{0} = \binom{a}{c} = a\binom{1}{0} + c\binom{0}{1} = M_{11}\binom{1}{0} + M_{21}\binom{0}{1} \tag{1}$$

$$M\binom{0}{1} = \binom{a\ b}{c\ d}\binom{0}{1} = \binom{c}{d} = c\binom{1}{0} + d\binom{0}{1} = M_{12}\binom{1}{0} + M_{22}\binom{0}{1} \tag{2}$$

It is important to note that as with vectors, the matrix representation of a linear operator depends on the choice of basis.

Eigenvectors/eigenvalues If T is a linear map and $\vec{v}$ is a vector such that $T\vec{v} = \lambda\vec{v}$ for some complex number λ, then $\vec{v}$ is called an eigenvector of T and λ is called the eigenvalue of $\vec{v}$ or T.

Inner product The inner product between two vectors $\vec{v}, \vec{u}$ is denoted $\langle \vec{v}, \vec{u} \rangle$, and must satisfy the following properties:

- Linearity in the second argument: If $\vec{u}, \vec{v}, \vec{w}$ are vectors and α, β are complex scalars, then $\langle \vec{w}, \alpha\vec{u} + \beta\vec{v} \rangle = \alpha\langle \vec{w}, \vec{u} \rangle + \beta\langle \vec{w}, \vec{v} \rangle$.
- Skew-symmetry: For any vectors $\vec{u}, \vec{v}$, we have $\langle \vec{u}, \vec{v} \rangle = \langle \vec{v}, \vec{u} \rangle^*$.
- Positive-definiteness: For any nonzero vector $\vec{v}$, we have $\langle \vec{v}, \vec{v} \rangle > 0$.

The second two properties, which may seem random at first, are necessary to give the map $\vec{v} \mapsto \langle \vec{v}, \vec{v} \rangle$ the properties of a norm. First, skew-symmetry guarantees that $\langle \vec{v}, \vec{v} \rangle^* = \langle \vec{v}, \vec{v} \rangle$, so this is a real number. Positive-definiteness ensures that this number is positive, and along with linearity, only vanishes if $\vec{v} = 0$. Lastly, the first and second properties also imply sesquilinearity in the first argument, which means that

$$\langle \sum_{i=1}^N \alpha_i \vec{v}_i, \vec{u} \rangle = \left(\langle \vec{u}, \sum_{i=1}^N \alpha_i \vec{v}_i \rangle \right)^* = \left(\sum_{i=1}^N \alpha_i \langle \vec{u}, \vec{v}_i \rangle \right)^* = \sum_{i=1}^N \alpha_i^* \langle \vec{u}, \vec{v}_i \rangle^* = \sum_{i=1}^N \alpha_i^* \langle \vec{v}_i, \vec{u} \rangle$$

This means that in order to pull scalars out of the first argument of the inner product, they must be conjugated.
Orthogonal Two vectors $\vec{v}$ and $\vec{u}$ are called orthogonal if $\langle \vec{v}, \vec{u} \rangle = 0$.
Normalized A vector $\vec{v}$ is called normal if $\langle \vec{v}, \vec{v} \rangle = 1$
Kronecker Delta The kronecker delta is a function of two natural numbers n, m such that

$$\delta_{mn} = \begin{cases} 1 & m = n \\ 0 & m \neq n \end{cases}$$

It is useful to note that this symbol "cancels" out summations. For example, if f is a function and $N > n$, then $\sum_{m=1}^{N} f(m)\delta_{mn} = f(n)$. Since $\delta_{mn} = 1$ only if $m = n$, this is the only term that contributes to the sum.
Orthonormal A set of vectors $\{\vec{e}_i\}$ is called orthonormal if $\langle \vec{e}_i, \vec{e}_j \rangle = \delta_{ij}$ for all i, j.
Orthonormal basis If a collection of vectors $\{\vec{e}_i\}$ is orthonormal, then it is automatically linearly independent. To prove this, suppose that $\sum_{i=1}^{N} \alpha_i \vec{e}_i = 0$. Taking the inner product with $\vec{e}_j$, we have

$$\langle \vec{e}_j, \sum_{i=1}^{N} \alpha_i \vec{e}_i \rangle = \sum_{i=1}^{N} \alpha_i \langle \vec{e}_j, \vec{e}_i \rangle = \sum_{i=1}^{N} \alpha_i \delta_{ij} = \alpha_j = 0$$

This shows that $\alpha_j = 0$ for any j, which is the definition of linear independence. If in addition $\{\vec{e}_i\}$ spans V, then it is called an orthonormal basis of V. With an orthonormal basis, we can express the components of a vector with respect to this basis using an inner product. If $\vec{v} = \sum_i v_i \vec{e}_i$ where α_i are the components of $\vec{v}$, then

$$\langle \vec{e}_j, \sum_{i=1}^{N} v_i \vec{e}_i \rangle = \sum_{i=1}^{N} v_i \langle \vec{e}_j, e_i \rangle = \sum_{i=1}^{N} v_i \delta_{ij} = v_j$$

This shows that $v_j = \langle \vec{e}_j, \vec{v} \rangle$ is the j^{th} component of $\vec{v}$.
Adjoint (of a vector) If $\vec{v}$ is a vector, then the adjoint of $\vec{v}$ is a linear map from vectors to scalars $\vec{u} \mapsto \langle \vec{v}, \vec{u} \rangle$, denoted $\vec{v}^\dagger$. If we fix a basis $\{\vec{b}_i\}$, then

$$\vec{v}^\dagger \vec{b}_j = \langle \vec{v}, b_j \rangle = \langle b_j, \vec{v} \rangle^* = v_j^*$$

This shows that as a matrix, the adjoint of v is a row vector where the elements of the row vector are the complex conjugates of the components of $\vec{v}$. For example, if the matrix representation of $\vec{v}$ is $\vec{v} = \begin{pmatrix} a \\ b \end{pmatrix}$, then the matrix representation of the adjoint is

$$\vec{v}^\dagger = \begin{pmatrix} a^*, b^* \end{pmatrix}$$

This is equivalent to taking the transpose of $\vec{v}$ first and then conjugating each element, often simply called the conjugate transpose. By sesquilinearity,

$$\vec{v}^\dagger \vec{b}_j = \langle \vec{v}, \vec{b}_j \rangle = \langle \vec{v}, \vec{b}_j \rangle = \sum_{i=1}^{N} v_i^* \langle \vec{b}_i, \vec{b}_j \rangle = \sum_{i=1}^{N} v_i^* \vec{b}_i^\dagger \vec{b}_j = \left(\sum_{i=1}^{N} v_i^* \vec{b}_i^\dagger \right) \vec{b}_j$$

This shows that if $\vec{v}$ is written as a linear combination of $\vec{b}_i$ with components v_i, then $\vec{v}^\dagger$ is a linear combination of $\vec{b}_i^\dagger$ with components v_i^*.
Adjoint (of a linear operator) If T is a linear operator, then the adjoint of T, denoted $T^\dagger$, is another linear operator such that $\langle \vec{u}, T\vec{v} \rangle = \langle T^\dagger \vec{u}, \vec{v} \rangle$ for any two vectors $\vec{u}, \vec{v}$. It is sufficient for this property to hold pairwise for any vectors in an orthonormal basis $\{b_i\}$. We can then work out the matrix elements of the operator $T^\dagger$. The matrix elements of T are defined by $T\vec{b}_j = \sum_{i=1}^{N} T_{ij} \vec{b}_i$, so

$$\langle \vec{b}_i, T\vec{b}_j \rangle = \sum_{k=1}^{N} T_{kj} \langle \vec{b}_i, \vec{b}_k \rangle = \sum_{k=1}^{N} T_{kj} \delta_{ik} = T_{ij}$$

This gives a recipe for finding the matrix elements of a linear operator: $T_{ij} = \langle \vec{b}_i, T\vec{b}_j$. Applying this to $T^\dagger$,

$$(T^\dagger)_{ij} = \langle \vec{b}_i, T^\dagger \vec{b}_j \rangle = \langle T^\dagger \vec{b}_j, \vec{b}_i \rangle^* = \langle \vec{b}_j, T\vec{b}_i \rangle^* = T_{ji}^*$$

This shows that $(T^\dagger)_{ij} = T_{ji}^*$. Switching the indices i and j corresponds to taking the transpose, so this operation is again just the conjugate transpose. From this definition, it can also be shown that if A and B are two matrices and α is a scalar, then the following properties hold:

- $(A+B)^\dagger = A^\dagger + B^\dagger$
- $(\alpha A)^\dagger = \alpha^* A^\dagger$
- $(AB)^\dagger = B^\dagger A^\dagger$

Outer product The inner product of two vectors $\vec{v}, \vec{u}$ is defined to be $\vec{v}\vec{u}^\dagger$. If $\{\vec{b}_i\}$ is an orthonormal basis and T is a linear operator, then $T = \sum_{ij} T_{ij}\vec{b}_i\vec{b}_j^\dagger$. To see this, consider

$$T\vec{b}_k =$$

Projection If $\vec{v}$ is normalized, then $\langle \vec{v}, \vec{u} \rangle \vec{v}$ is also called the projection of $\vec{u}$ onto $\vec{v}$.
Unitary: $U^\dagger = U^{-1}$ such that $U^\dagger U = UU^\dagger = I$ (I is the identity matrix)
Hermitian $H^\dagger = H$. Hermitian matrices have real eigenvalues.
Tensor product: The tensor product is represented by $\otimes$. You can get the tensor product of two vectors $\vec{v} \otimes \vec{w}$, or the tensor product of two matrices $A \otimes B$. If A is a matrix that acts on the vector space of $\vec{v}$, and B is a matrix that acts on the vector space of $\vec{w}$, then $(A \otimes B)\vec{v} \otimes \vec{w} = A\vec{v} \otimes B\vec{w}$. In the context of quantum information, we use the tensor product to represent the states of multi-qubit systems.

3 Quantum topics

(Quantum) State: Quantum states describe the full state of the system. They are represented by a 'ket' $|\Psi\rangle$. If these states live in a finite complex vector space (like qubits) they can be represented as column vectors. $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Quantum states must be normalized, which means the column vector representing the state must have a norm $\langle \Psi | \Psi \rangle = 1$.
(Quantum) Operator: Operators are represented as matrices that act on the state (a vector). You can also represent operators/matrices as a sum of outer products. Often, these operators have a 'hat' such as $\hat{I}$ to indicate that these are quantum operators. Operators can evolve the quantum state (if they are Unitary) or represent observables that we measure about the quantum state (if the matrix is hermitian).
Observable An observable is a Hermitian matrix. When we measure an observable, we project the quantum state to an eigenstate of the observable, and we read out the real eigenvalue of that corresponding eigenvector.
Gate A logical gate in quantum computation is a Unitary operation on our quantum state. These gates must be unitary (to preserve the norm of a quantum state
Pauli matrices Pauli matrices span the space of 2×2 complex matrices. They are all Hermitian and Unitary. This means that $\hat{P}^2 = \hat{I}$. The Pauli matrices are $\hat{\sigma_x} = \hat{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\hat{\sigma_z} = \hat{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, and $\hat{\sigma_y} = \hat{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$. Pauli matrices anti-commute with other Pauli matrices. This means that $\hat{X}\hat{Z} = -\hat{Z}\hat{X}$ (and same for every unique combination of $\hat{X}, \hat{Y}, \hat{Z}$).