Appendix B

Formal Definition of a Vector Space

In classical physics and engineering, we generally work with simple three-component position, velocity and acceleration vectors consisting of a triple of real numbers. The concept of a vector space is however much more general than this. Strictly speaking, we should refer to a 'vector space over a field.' Here are the properties:

We need a field S (e.g., a set of objects like the real numbers or the complex numbers on which two operations, multiplication and addition are defined). The elements of the field are called scalars.

The vectors are a set of objects $\{V\}$ with two operations:

- addition, so that for $\vec{v}_1, \vec{v}_2 \in \{V\}$, $\vec{v}_1 + \vec{v}_2$ is also in $\{V\}$ (*closure under addition*).

- multiplication by a scalar. If $s \in S$ then $s\vec{v}_1 \in \{V\}$ (*closure under scalar multiplication*).

The following eight properties must be satsified:

1. $(\vec{v}_1 + \vec{v}_2) + \vec{v}_3 = \vec{v}_1 + (\vec{v}_2 + \vec{v}_3)$ (addition is associative)

2. $\vec{v}_1 + \vec{v}_2 = \vec{v}_2 + \vec{v}_1$ (addition is commutative)

3. $\exists\, \vec{0} \in \{V\}$ such that $\vec{0} + \vec{v} = \vec{v}$ (additive identity exists)

4. $\forall\, \vec{v} \in \{V\}, \exists\, -\vec{v} \in \{V\}$ such that $\vec{v} + (-\vec{v}) = \vec{0}$. (additive inverse exists)

5. $s(\vec{v}_1 + \vec{v}_2) = s\vec{v}_1 + s\vec{v}_2$ (1st distribution law)
6. $(s_1 + s_2)\vec{v} = s_1\vec{v} + s_2\vec{v}$ (2nd distribution law)
7. $s_1(s_2\vec{v}) = (s_1 s_2)\vec{v}$
8. $1(\vec{v}) = \vec{v}$ (where 1 is the multiplicative identity of the scalar field)

B.1 Basis Vectors and the Dimension of a Vector Space

The *dimension* D of a vector space is the maximum number[1] of linearly independent vectors. Suppose that we have a set of vectors $Q = \{B_1, B_2, \ldots, B_N\}$ and we consider the function

$$F(s_1, s_2, \ldots, s_N) = \sum_{j=1}^{N} s_j B_j. \tag{B.1}$$

The set Q of vectors is by definition *linearly independent* if the only solution to the equation $F(s_1, s_2, \ldots, s_N) = 0$ is that all of its arguments vanish $(s_1, s_2, \ldots, s_N) = (0, 0, \ldots, 0)$. If $N > D$ there are too many vectors to all be pointing in orthogonal directions and some of the vectors are redundant in the sense that they can be expressed as linear combinations of other vectors. In this case $F = 0$ has solutions for non-zero arguments of F.

A *basis* for a vector space of dimension D is a set of vectors $Q = \{B_1, B_2, \ldots, B_D\}$ which *span* the space. That is every vector V in the space can be written as a (unique) linear combination of the basis vectors

$$V = \sum_{j=1}^{D} b_j B_j \tag{B.2}$$

by choosing appropriate values for the set of scalars (coefficients) $(b_1, b_2, \ldots, b_D)$. This list of coefficients constitutes a representation of the abstract vector V in this basis B.

[1] We consider here only the case where the Hilbert space dimension is finite (or at least countable).

As a familiar example, the unit vectors

$$\hat{i} = (1,0,0) \tag{B.3}$$
$$\hat{j} = (0,1,0) \tag{B.4}$$
$$\hat{k} = (0,0,1) \tag{B.5}$$

can be used to form any position vector in ordinary three-dimensional space

$$\vec{r} = (x,y,z) = x\hat{i} + y\hat{j} + z\hat{k}. \tag{B.6}$$

These Cartesian coordinate basis vectors happen to be orthogonal (formally defined below) because they are perpendicular in the usual geometric sense. However a basis set is not required to be orthogonal, only complete.

B.2 Inner Products and Norms

For the ordinary vectors like positions and displacements (differences of position vectors) that we are used to the concept of the length (or 'norm') of a vector defined in terms of Pythagorean theorem. If

$$\vec{A} = (A_x, A_y, A_z), \tag{B.7}$$

then the norm is

$$|\vec{A}| = \sqrt{A_x^2 + A_y^2 + A_z^2}. \tag{B.8}$$

The general definition of a norm for a vector space is (more or less) any mapping from the vectors to the non-negative real numbers satisfying the triangle inequality $|\vec{A}+\vec{B}| \leq |\vec{A}| + |\vec{B}|$. It is important to note that a given vector space need not have a norm defined.

For ordinary vectors we are used to the dot product

$$\vec{A}\cdot\vec{B} = a_xB_x + A_yB_y + A_zB_z = |\vec{A}||\vec{B}|\cos\theta_{AB}, \tag{B.9}$$

where θ_{AB} is the angle between the two vectors. The dot product is a specific example of the general concept of an *inner product*. An inner product of two abstract vectors V_1 and V_2 is a mapping onto a scalar s, often denoted

$$(V_1, V_2) = s. \tag{B.10}$$

For the case where the vector space is defined over the field of complex numbers, an inner product satisfies the following requirements:

- Linearity in the second argument

$$
\begin{aligned}
(V_1, aV_2) &= as, && \text{(B.11)}\\
(V_1, V_2 + V_3) &= (V_1, V_2) + (V_1, V_3), && \text{(B.12)}
\end{aligned}
$$

- Anti-linearity (conjugate linearity) in the first argument

$$
\begin{aligned}
(aV_1, V_2) &= a^*(V_1, V_2), && \text{(B.13)}\\
(V_1, V_2) &= (V_2, V_1)^*, && \text{(B.14)}
\end{aligned}
$$

- Positive semi-definite

$$(V_1, V_1) \geq 0 \tag{B.15}$$

and

$$(V_1, V_1) = 0 \implies V_1 = \vec{0}. \tag{B.16}$$

[Note the first zero above is the scalar zero and the arrow is placed on the second zero to make clear that this is the null vector (additive zero vector) not the scalar zero.]

Two vectors are defined to be *orthogonal* if their inner product vanishes.

Exercise B.1. Prove that the usual dot product for real three-dimensional vectors satisfies the definition of an inner product.

The Pythagorean norm defined above for ordinary real vectors is thus related to the inner product of the vector with itself

$$|\vec{A}| = \sqrt{\vec{A} \cdot \vec{A}}. \tag{B.17}$$

Exercise B.2. Prove that for a general complex vector space, $\sqrt{(V, V)}$ satisfies the definition of a norm.

In describing qubit states we will deal with two component complex valued vectors of the form

$$
\begin{aligned}
\Psi_1 &= (\alpha_1, \beta_1), && \text{(B.18)}\\
\Psi_2 &= (\alpha_2, \beta_2). && \text{(B.19)}
\end{aligned}
$$

The standard inner product and norm for such vectors are defined in Ex. B.3.

Exercise B.3. Prove that the following generalization of the dot product to complex vectors satisfies the definition of an inner product

$$(\Psi_1, \Psi_2) = \alpha_1^* \alpha_2 + \beta_1^* \beta_2. \tag{B.20}$$

and prove that

$$\sqrt{(\Psi_1, \Psi_1)} = \sqrt{\alpha_1^* \alpha_1 + \beta_1^* \beta_1}. \tag{B.21}$$

satisfies the definition of a norm.

B.3 Dirac Notation, Outer Products and Operators for Single and Multiple Qubits

Physicists generally use a notation for complex state vectors and their inner products that was developed by Paul Adrian Maurice Dirac. In this notation the complex vector in Eq. (B.18) is represented as column vector instead of a row vector using the 'bracket' notation

$$|\Psi_1\rangle = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}, \tag{B.22}$$

where $|\Psi_1\rangle$ is referred to as a 'ket' vector and the inner product is represented by

$$(\Psi_1, \Psi_2) = \langle\Psi_1|\Psi_2\rangle, \tag{B.23}$$

where the 'dual vector'

$$\langle\Psi_1| = (\alpha_1^*, \beta_1^*)\,, \tag{B.24}$$

is a row vector representing the conjugate transpose of the column vector. In this notation, the inner product is computed using the rules of matrix multiplication

$$\langle\Psi_1|\Psi_2\rangle = (\alpha_1^*, \beta_1^*) \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \alpha_1^* \alpha_2 + \beta_1^* \beta_2. \tag{B.25}$$

The Dirac notation is also very convenient for defining the *outer product* of two vectors which, as described in Chapter 3 is a linear operator that maps the vector space back onto itself (i.e. maps vectors onto other vectors)

$$\mathcal{O} = |\Psi_2\rangle\langle\Psi_1|. \tag{B.26}$$

Applying this operator to a vector $|\Psi_3\rangle$ yields

$$\mathcal{O}|\Psi_3\rangle = (|\Psi_2\rangle\langle\Psi_1|)\,|\Psi_3\rangle = |\Psi_2\rangle\langle\Psi_1|\Psi_3\rangle = |\Psi_2\rangle\,(\langle\Psi_1|\Psi_3\rangle) = s_{13}|\Psi_2\rangle, \tag{B.27}$$

where the scalar s_{13} is given by the inner product (also known in quantum parlance as the 'overlap')

$$s_{13} = \langle\Psi_1|\Psi_3\rangle. \tag{B.28}$$

Subsituting the definitions of of the bra and ket vectors in Eq. (B.26) we see that the abstract operator can be represented as a matrix

$$\mathcal{O} = \left(\begin{array}{c} \alpha_2 \\ \beta_2 \end{array}\right) (\alpha_1^*, \beta_1^*) = \left(\begin{array}{cc} \alpha_2\alpha_1^* & \alpha_2\beta_1^* \\ \beta_2\alpha_1^* & \beta_2\beta_1^* \end{array}\right). \tag{B.29}$$

By simply switching the order of the row and column vector from that in Eq. (B.25), the rules of matrix multiplication give us a matrix instead of a scalar!

Exercise B.4. Use the matrix representation of $\mathcal{O}$ in Eq. (B.29) and apply it to the column vector representation of $|\Psi_3\rangle$

$$|\Psi_3\rangle = \left(\begin{array}{c} \gamma \\ \delta \end{array}\right)$$

to verify the last equality in Eq. (B.27.)

Recall that the adjoint of the product of two matrices is the product of the adjoints in reverse order

$$(AB)^\dagger = B^\dagger A^\dagger. \tag{B.30}$$

It works the same way in the Dirac notation for the outer product of two vectors that forms an operator. Thus the adjoint of the operator in Eq. (B.26) is simply

$$\mathcal{O}^\dagger = |\Psi_1\rangle\langle\Psi_2|. \tag{B.31}$$

To see that this is true, it is best to work with the representation in Eq. (B.29)

$$\begin{aligned}
\mathcal{O}^\dagger &= \left[\begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} (\alpha_1^*, \beta_1^*)\right]^\dagger = \left[\begin{pmatrix} \alpha_2\alpha_1^* & \alpha_2\beta_1^* \\ \beta_2\alpha_1^* & \beta_2\beta_1^* \end{pmatrix}\right]^\dagger, && \text{(B.32)}\\
&= \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} (\alpha_2^*, \beta_2^*) = \begin{pmatrix} \alpha_1\alpha_2^* & \alpha_1\beta_2^* \\ \beta_1\alpha_2^* & \beta_1\beta_2^* \end{pmatrix}, && \text{(B.33)}\\
&= |\Psi_1\rangle\langle\Psi_2|. && \text{(B.34)}
\end{aligned}$$

Tensor Products and Multiqubit States

The so-called tensor product of a pair of 2×2 matrices produces a 4×4 matrix

$$\begin{aligned}
A \otimes B &= \begin{pmatrix} A_{11}[B] & A_{12}[B] \\ A_{21}[B] & A_{22}[B] \end{pmatrix} && \text{(B.35)}\\
&= \begin{pmatrix} A_{11}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} & A_{12}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \\ A_{21}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} & A_{22}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \end{pmatrix}. && \text{(B.36)}
\end{aligned}$$

Such tensor products appear when dealing with the Hilbert space of two qubits where the operator A acts on one qubit and operator B acts on the other. This Hilbert space has dimension four and the states are represented by column vectors of length four

$$|\psi\rangle = \begin{pmatrix} \psi_0 \\ \psi_1 \\ \psi_2 \\ \psi_3 \end{pmatrix}. \tag{B.37}$$

For the Hilbert space of n qubits, we will use the following Dirac notation for state vectors and their duals in the computational basis

$$\begin{aligned}
|\psi\rangle &= |b_{n-1}\dots b_2 b_1 b_0\rangle && \text{(B.38)}\\
\langle\psi| &= \langle b_{n-1}\dots b_2 b_1 b_0| && \text{(B.39)}
\end{aligned}$$

in which the qubits are numbered from 0 to $n-1$ and their values $b_j \in \{0, 1\}$ are ordered from right to left. (Note that we maintain this same label ordering in the dual vector.) The computational basis is simply the tensor product of the computational basis of the individual qubits (illustrated here for the case of two qubits)

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{B.40}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{B.41}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{B.42}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{B.43}$$

Notice that if we label the ordinal positions in the column vector starting with 0 at the top and ending with 3 as in Eq. (B.37), then the binary representation of the position of the entry containing 1 gives the state of the two qubits in the computational basis. For example $|11\rangle$ corresponds to the binary representation of the number 3 which in turn corresponds to the location of the entry 1 being at the bottom of the column vector in Eq. (B.43)

We can also write the dual vectors associated with the above two-qubit state vectors. For example the dual of the vector in Eq. (B.41) is

$$\langle 01| = \langle 0| \otimes \langle 1| = \begin{pmatrix} 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}. \tag{B.44}$$

Recall from Eq. (B.30) for ordinary products of matrices we need to reverse the order of the matrices when forming the transpose. However in forming the dual of the tensor product $|0\rangle \otimes |1\rangle$, we do *not* reverse the order of the two terms in the tensor product. This is because of our convention of keeping the bit order the same when writing the dual of $|01\rangle$ as $\langle 01|$ rather than $\langle 10|$.

As examples of operators acting on this Hilbert space consider the joint

Pauli operators

$$Z \otimes X = \begin{pmatrix} 0 & +1 & 0 & 0 \\ +1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \tag{B.45}$$

and

$$X \otimes Z = \begin{pmatrix} 0 & 0 & +1 & 0 \\ 0 & 0 & 0 & -1 \\ +1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}. \tag{B.46}$$

It is straightforward to verify that (for example)

$$(Z \otimes X)|10\rangle = \begin{pmatrix} 0 & +1 & 0 & 0 \\ +1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = - \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{B.47}$$

is equivalent to (i.e., correctly represents)

$$\begin{aligned} (Z \otimes X)|10\rangle &= (Z|1\rangle) \otimes (X|0\rangle) && \text{(B.48)} \\ &= (-|1\rangle) \otimes (|1\rangle) && \text{(B.49)} \\ &= -|11\rangle. && \text{(B.50)} \end{aligned}$$

Similarly

$$(X \otimes Z)|10\rangle = \begin{pmatrix} 0 & 0 & +1 & 0 \\ 0 & 0 & 0 & -1 \\ +1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \tag{B.51}$$

is equivalent to

$$\begin{aligned} (X \otimes Z)|10\rangle &= (X|1\rangle) \otimes (Z|0\rangle) && \text{(B.52)} \\ &= (|0\rangle) \otimes (+|0\rangle) && \text{(B.53)} \\ &= +|00\rangle. && \text{(B.54)} \end{aligned}$$

The above examples show us that the tensor product of two operators is represented by a 4×4 matrix that can act on the column vector representing the tensor product of two single qubit states. But we also see that this is exactly equivalent to each operator acting separately on their respective qubits and then taking the tensor product of the resulting state vectors. If we want an operator that acts on only qubit q_0 we simply tensor it with the identity acting on q_1. For example,

$$X_0 = I \otimes X = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{B.55}$$

whereas if we want the operator to act only on q_1 we should use

$$X_0 = X \otimes I = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{B.56}$$

It is important to note that the tensor product of two Pauli matrices is not the most general form of two-qubit operator. For example, the CNOT gate shown in Eq. (4.19) is a sum of four different products of Pauli operators.

B.4 The Vector Space of Bit Strings

Computer and information science deals with bit strings and it turns out that these form a vector space over a field. To see this, consider the set of all possible bit strings $\vec{x} = (x_{n-1}x_{n-2}\dots x_2x_1x_0)$ of length n. Since every element in the vector is a bit whose only allowed values are 0 and 1, we define addition via

$$\vec{x} \oplus \vec{y} \equiv \vec{x} + \vec{y} \mod 2, \tag{B.57}$$

where the mod 2 operation is performed bitwise. Strangely, this means that every vector is its own additive inverse

$$\vec{x} \oplus \vec{x} = \vec{0}. \tag{B.58}$$

Similarly the only allowed scalars are $s = 0, 1$ because only for these values are vectors of the form $s\vec{x}$ in the space of bit strings. The set of scalars $\{0, 1\}$

together with the operations of ordinary multiplication and addition mod 2, constitute a field. This binary field is traditionally denoted $\mathbb{F}_2$. Given these facts, it is straightforward to verify that the criteria required for the set of bit strings of length n to be a vector space over a field are all satisfied.

We can define an inner product on this vector space

$$\vec{x}.\vec{y} = \left(\sum_{j=0}^{n-1} x_j y_j\right) \mod 2 = (\vec{x}\cdot\vec{y}) \mod 2, \tag{B.59}$$

where $\vec{x}\cdot\vec{y}$ is the ordinary Euclidean dot product. (The inner product has to be a scalar and there are only two allowed scalars which is why the mod 2 arithmetic is required in the inner product.) The 'length' of a vector $L^2 = L = \vec{x}.\vec{x}$ is thus the parity of the number non-zero bits in the string. $L = 0$ if the vector contains an even number of 1's and $L = 1$ if the vector contains an odd number of 1's.

This notion of 'length' does not give a very complete notion of the distance between two vectors. To remedy this one can define the notion of the *Hamming distance* between two vectors

$$d_{\mathrm{H}}(\vec{x},\vec{y}) = \sum_{j=0}^{n-1}(x_j \oplus y_j). \tag{B.60}$$

Because $x_j \oplus y_j$ is zero if the two bits agree and one if they differ, the Hamming distance is the total number of instances where the bit strings differ. Equivalently it is the total number of bits in $\vec{x}$ that would need to be flipped to convert $\vec{x}$ into $\vec{y}$.

The notion of Hamming distance is very important in classical error correction, because the Hamming distance between a code word (a bit string in the code space) and a word that has been corrupted by errors (bit flips) is equal to the number of bitflip errors. These various notions of length and distance are not to be confused with the 'length' n of a bit string in the ordinary sense of the number of bits in the bit string vectors, which is the dimension of the vector space.

Appendix C

Handy Mathematical Identities

Useful Information about the Mathematical Representation of Qubit States and Operations

Standard basis states:

$$
\begin{aligned}
|0\rangle = |\uparrow\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
|1\rangle = |\downarrow\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}.
\end{aligned}
$$

The representation of the basis states in the $\hat{n}$ basis in terms of the standard basis states is

$$
\begin{aligned}
|+\hat{n}\rangle &= \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \\
|-\hat{n}\rangle &= \sin\left(\frac{\theta}{2}\right)|0\rangle - e^{i\varphi}\cos\left(\frac{\theta}{2}\right)|1\rangle
\end{aligned}
$$

Standard basis states:

$$
\begin{aligned}
|0\rangle = |\uparrow\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
|1\rangle = |\downarrow\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}.
\end{aligned}
$$

The representation of the basis states in the $\hat{n}$ basis in terms of the standard basis states is

$$\begin{aligned} |+\hat{n}\rangle &= \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \\ |-\hat{n}\rangle &= \sin\left(\frac{\theta}{2}\right)|0\rangle - e^{i\varphi}\cos\left(\frac{\theta}{2}\right)|1\rangle \end{aligned}$$

where $\hat{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$.

Pauli matrices:

$$\begin{aligned} X = \sigma^x &= \begin{pmatrix} 0 & +1 \\ +1 & 0 \end{pmatrix} \\ Y = \sigma^y &= \begin{pmatrix} 0 & -i \\ +i & 0 \end{pmatrix} \\ Z = \sigma^z &= \begin{pmatrix} +1 & 0 \\ 0 & -1 \end{pmatrix} \\ I = \sigma_0 &= \begin{pmatrix} +1 & 0 \\ 0 & +1 \end{pmatrix}. \end{aligned}$$

Trace of Pauli matrices

$$\begin{aligned} \mathrm{Tr}\, X = \mathrm{Tr}\, Y = \mathrm{Tr}\, Z = 0 \\ \mathrm{Tr} I = 2. \end{aligned}$$

Products of Pauli Matrices

$$\begin{aligned} X^2 &= Y^2 = Z^2 = I \\ XY &= -YX = iZ \\ YZ &= -ZY = iX \\ ZX &= -XZ = iY \\ XYZ &= iI. \end{aligned}$$

Commutators of Pauli matrices:

$$\begin{aligned} [X, Y] = XY - YX = 2iZ \\ [Y, Z] = YZ - ZY = 2iX \\ [Z, X] = ZX - XZ = 2iY. \end{aligned}$$

Anticommutators of Pauli matrices

$$\begin{aligned}\{X,Y\} &= XY + YX = 0\\ \{Y,Z\} &= YZ + ZY = 0\\ \{Z,X\} &= ZX + XZ = 0.\end{aligned}$$

Eigenstates of σ^x:

$$|\pm\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle \pm |1\rangle\right].$$

Eigenstates of σ^y:

$$|\pm i\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle \pm i|1\rangle\right].$$

Euler-Pauli Identity: If A^2 is the identity operator I (for any dimension Hilbert space) then for real θ, $e^{i\theta A} = [\cos\theta]I + [i\sin\theta]A$.

Rotation of qubit on Bloch sphere by an angle χ around the $\hat{\omega}$ axis (recall the right-hand rule)

$$R_{\hat{\omega}}(\chi) = e^{-i\frac{\chi}{2}\hat{\omega}\cdot\vec{\sigma}} = \cos(\chi/2)\,\hat{I} - i\sin(\chi/2)\,\hat{\omega}\cdot\vec{\sigma}.$$

Standard right-to-left ordering of multi-qubit states in the computational basis $|q_{n-1}, q_{n-2}, \ldots, q_2, q_1, q_0\rangle$. Generic two-qubit state is:

$$|\Psi\rangle = \psi_{00}|00\rangle + \psi_{01}|01\rangle + \psi_{10}|10\rangle + \psi_{11}|11\rangle = \begin{pmatrix}\psi_{00}\\ \psi_{01}\\ \psi_{10}\\ \psi_{11}\end{pmatrix}.$$

In addition to the standard orthonormal computational basis states for two qubits, $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, another commonly used orthonormal basis for two qubits are the so-called Bell states:

$$\begin{aligned}|B_0\rangle &= \frac{1}{\sqrt{2}}\left[|01\rangle - |10\rangle\right]\\ |B_1\rangle &= \frac{1}{\sqrt{2}}\left[|01\rangle + |10\rangle\right]\\ |B_2\rangle &= \frac{1}{\sqrt{2}}\left[|00\rangle - |11\rangle\right]\\ |B_3\rangle &= \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right].\end{aligned}$$

Handy trig identities:

$$\begin{aligned}
\cos(\xi) &= \cos^2\left(\frac{\xi}{2}\right) - \sin^2\left(\frac{\xi}{2}\right) \\
\sin(\xi) &= 2\sin\left(\frac{\xi}{2}\right)\cos\left(\frac{\xi}{2}\right) \\
\sin\left(\frac{\xi}{2}\right) &= -\sin\left(\frac{\xi}{2}\right)\cos(\xi) + \cos\left(\frac{\xi}{2}\right)\sin(\xi) \\
\cos\left(\frac{\xi}{2}\right) &= \sin\left(\frac{\xi}{2}\right)\sin(\xi) + \cos\left(\frac{\xi}{2}\right)\cos(\xi) \\
\sin(\pi/4) &= \cos(\pi/4) = 1/\sqrt{2}.
\end{aligned}$$