Birth of a Qubit

$$\boxed{\{\mathbf{0},\mathbf{1}\} = \mathbb{B} \text{ versus } \boldsymbol{a}\,|0\rangle + \boldsymbol{b}\,|1\rangle \in \mathbb{C}^{\mathbf{2}}}$$

I believe $\cdots$

Quantum Physics is not a prerequisite of quantum computing unless one wants to build a quantum computer.
Nevertheless we start with an experiment of Physics to show that the Nature supports qubit.

Stern-Gerlach Experiment

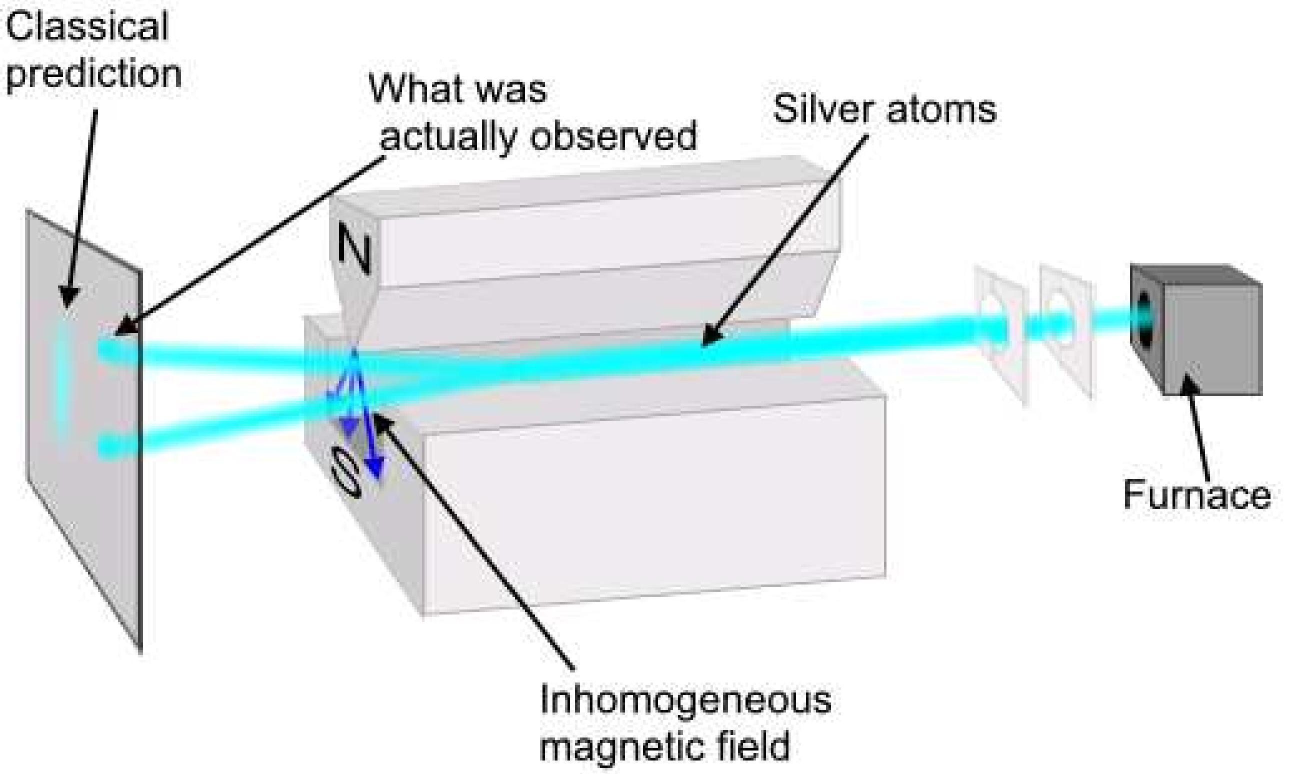


Image Source: `https://upload.wikimedia.org/wikipedia/commons/2/29/Stern-Gerlach_experiment.PNG`

The result of Stern-Gerlach experiment (1921-22) indicates the requirement of a radical change not only from classical mechanics (space quantization) but also from old quantum theory of Bohr and Sommerfeld (intrinsic spin etc.).

- The physics of the experiment is not of much relevance for our purpose.
- But it shows the existence of a 2-state quantum mechanical system, the spin of an electron.
- This cannot be modelled by a bit. And it is necessary to introduce a mathematical object called quantum bit (qubit).

A Brief Description

- A narrow beam of silver atom is passed through a strong non-uniform magnetic field with a gradient along the z-axis. Finally the beam hits the screen.
- A silver atom has 47 electrons. In the accepted view the inner 46 electrons are forming a sphere of electron cloud with no magnetic moment. [Electron configuration of Ag: 2, 8, 18, 18, 1].

- The magnetic moment of the atom is due to the intrinsic spin of the 47^{th} outer electron.
- The experiment measures the z-component of the magnetic moment of the atom, which is proportional to the spin of the 47^{th} electron.

Note

The concept of spin (intrinsic angular momentum) of an electron was not known when Stern and Gerlach performed the experiment. So people tried to explain the outcome of the experiment using the classical electrodynamics or using Bohr-Sommerfeld model of atom (quantized orbital angular momentum of electrons).

You may Read

Stern and Gerlach: How a Bad Cigar Helped Reorient Atomic Physics

https://physlab.lums.edu.pk/images/c/c4/Cigar.pdf

Classical Prediction

- Silver atoms come out of the furnace with random orientations of their magnetic moments with a random distribution of their z-components.
- So the image on the screen should have a continuous band of silver atoms.

Prediction of Bohr-Sommerfeld Model

According to Bohr-Sommerfeld model, orbits of electron should assume certain discrete spacial orientations under the influence of an external magnetic field. If one assumes a circular orbit, there are two possibilities of the projection of orbital angular momentum. And in a strong non-uniform magnetic field the silver beam can be split in two parts.

Actual Image and Interpretation

Stern and Gerlach could manage to split the bean and get two localised spots of silver. They incorrectly interpreted it as an outcome of Bohr-Sommerfeld space quantization.

Actual Image and Interpretation

- The correct interpretation had to wait until the discovery of the intrinsic spin of an electron by George Uhlenbeck and Samuel Goudsmit (studying spectral lines of anomalous Zeeman effect).
- We shall see that the postulates of quantum mechanics are also required for proper explanation of the experiment.

Two State System

The Stern-Gerlach experiment was performed on may other elements including hydrogen atom. Now it is known that the splitting of the beam in two parts is due to two orientations (up and down) of the intrinsic spin of the outermost single electron (the 47^{th} electron in case silver), along the z-axis. The inner core of 46-electrons has zero angular momentum.

Simplified Physics

$\mu \propto \mathrm{S}$, where μ is the magnetic moment of the atom and S is the electron spin. If B is the magnetic field, the force along the z-direction is $F_z = \frac{\partial}{\partial z}(\mu \cdot \mathrm{S}) = \mu_z \frac{\partial B_z}{\partial z}$.

The field must be non-uniform to make $\frac{\partial B_z}{\partial z}$ non-zero (potential energy must change in the z-direction).

Two State System

- Let us call the two spin states of an electron along z-axis as S_{z+} and S_{z-}. It is an example of a 2-state (observable) quantum mechanical system.
- There is nothing special about the z-axis. We can orient the magnetic field along x or y-axis and split the beam coming from the furness in $\{S_{x+}, S_{x-}\}$ or $\{S_{y+}, S_{y-}\}$ respectively.

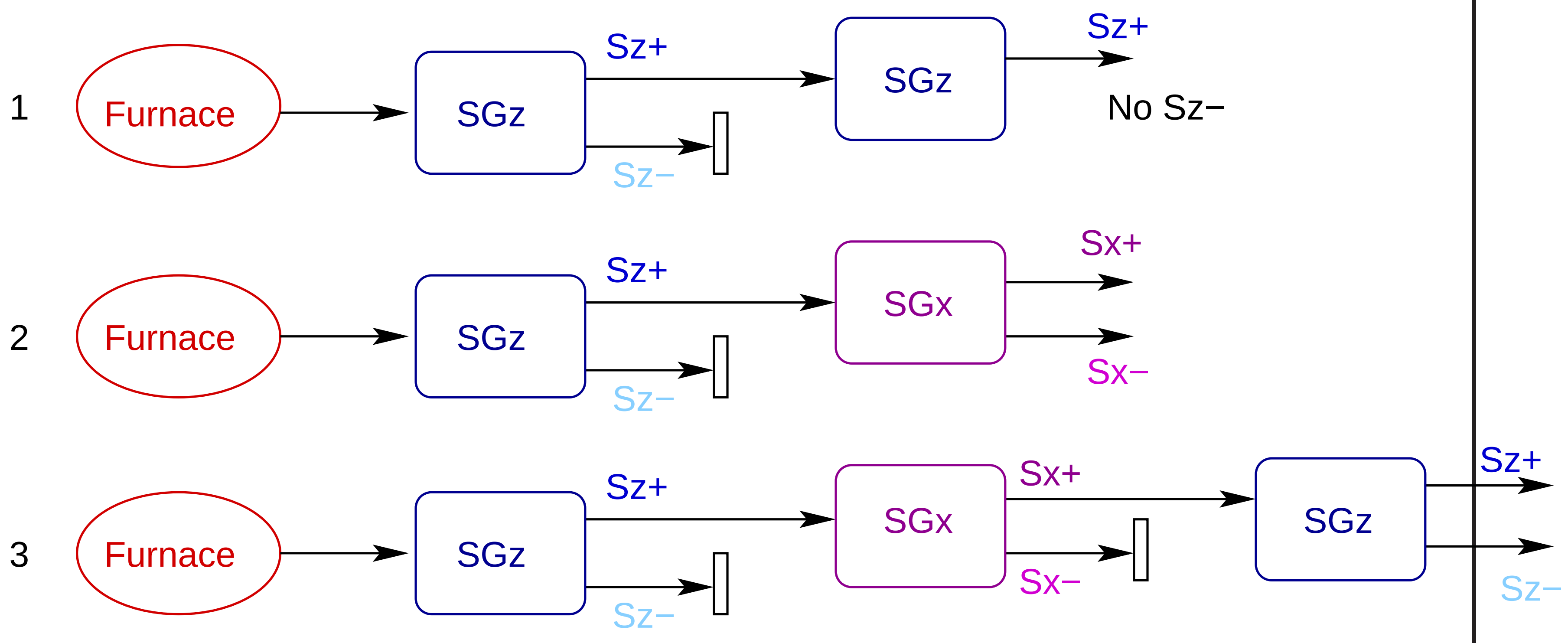
Other SG Apparatus

Let SGz be the Stern-Gerlach apparatus with magnetic field oriented along the z-axis. Similarly the field of SGx is along the x-axis.

Apparatus in Cascade

Gedankenexperiment with Stern-Gerlach apparatus in cascade.

1. The S_{z+} beam coming out of SGz apparatus is passed through another SGz apparatus.
2. The S_{z+} beam of SGz apparatus is passed through an SGx apparatus.
3. The S_{x+} beam of the previous experiment is passed through another SGz apparatus.


1
Furnace
SGz
Sz+
Sz−
SGz
Sz+
No Sz−
2
Furnace
SGz
Sz+
Sz−
SGx
Sx+
Sx−
3
Furnace
SGz
Sz+
Sz−
SGx
Sx+
Sx−
SGz
Sz+
Sz−

Experiment 1

In the first experiment, the S_{z+} beam is passed through another Stern-Gerlach apparatus with the magnetic field along the z-axis. The final output is a S_{z+} beam.
A simple-minded interpretation may be the absence of any S_{z-} atom in the incoming S_{z+} beam.

Experiment 2

In the second experiment, the S_{z+} beam is passed through a Stern-Gerlach apparatus where the non-uniform magnetic field is along the x-axis. The incoming S_{z+} beam is split into two beams S_{x+} and S_{x-} of equal intensity.

Note

According to classical physics the S_{z+} silver atoms does not have any magnetic moment in x or y directions. So experiment 2 should have produced one spot.

One may think that the incoming S_{z+} beam is a mixture of $S_{z+} + S_{x+}$ and $S_{z+} + S_{x-}$ in equal proportion (due to some reason).

Experiment 3

In the third experiment, the S_{x+} beam of the experiment 2 is passed through a Stern-Gerlach apparatus where the no-uniform magnetic field is again oriented along the z-axis. The final outcome is two beams of S_{z+} and S_{z-} of equal intensity.
None of the interpretations of the previous two experiments can explain this result.

A Qubit

- The spin state of an electron cannot be modelled as a binary digits (bit) with two discrete states.
- It is modelled as a quantum bit (qubit), a unit vector of a 2-dimensional vector space over a complex field (for some purpose real subfield may be used). This is simply an element of $\mathbb{C}^2$ with norm 1.

A Qubit

- Two basis states of a qubit are denoted by $|0\rangle$ and $|1\rangle$ - ket 0 and ket 1.
- A qubit is a linear combination or superposition of the basis states: $a\,|0\rangle + b\,|1\rangle$, where in general $a, b \in \mathbb{C}$, and $|a|^2 + |b|^2 = 1$. A qubit has uncountably many states,

Measurement

In a measurement of a qubit, we can only observe the basis states characteristic of the device. If $|0\rangle$ and $|1\rangle$ are the basis states of a measurement and the state of a qubit is $a\,|0\rangle + b\,|1\rangle$, then we observe $|0\rangle$ with the probability $|a|^2$ or $|1\rangle$ with the probability $|b|^2$. This explains the requirement of $|a|^2 + |b|^2 = 1$.

Stern-Gerlach and Qubit

Let the state of a silver atom in S_{z+} be $|0\rangle$ and the state of S_{z-} be $|1\rangle$.
Note that there is nothing special about the z-direction. Only requirement is that $|0\rangle$ and $|1\rangle$ should be orthonormal (orthogonal and unit length).

Experiment 2

We take the state of a silver atom in S_{x+} as a superposition $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and that of a silver atom in S_{x-} as the $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Note that these two are basis states w.r.t. SGx apparatus.

We get $\frac{|S_{x+}\rangle}{\sqrt{2}} + \frac{|S_{x-}\rangle}{\sqrt{2}} = |0\rangle = |S_{z+}\rangle$.

So the probability of an S_{z+} qubit to be in state S_{x+} or in state S_{x-} are both $(1/\sqrt{2})^2 = 1/2$.

Experiment 3

As $|S_{x+}\rangle = \frac{|0\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}$, the output of the 3^{rd} experiment is as we have observed - the $|S_{x+}\rangle$ beam is split in two beams, $|S_{z+}\rangle$ and $|S_{z+}\rangle$, as they are equally probable.

Note

Following assignments also give the same result:

$$\begin{aligned}|S_{x+}\rangle &\leftarrow |0\rangle\\ |S_{x-}\rangle &\leftarrow |1\rangle\\ |S_{z+}\rangle &\leftarrow \frac{|0\rangle}{\sqrt{2}}+\frac{|1\rangle}{\sqrt{2}}\\ |S_{z-}\rangle &\leftarrow \frac{|0\rangle}{\sqrt{2}}-\frac{|1\rangle}{\sqrt{2}}\end{aligned}$$

Conclusion

This funny vector qubit captures the spin state of an electron and explains the outcome of Stern-Gerlach experiment - on the other hand we know how to implement a qubit!

Probabilistic Bit and Qubit

- In a probabilistic model a bit may have a value 0 with a probability p or a value 1 with a probability $1 - p$. We associate a vector $(p, 1 - p)$, $p \in [0, 1]$ with the bit.
- When a qbit $a\,|0\rangle + b\,|1\rangle$ is measured, then the probability of getting $|0\rangle$ is $|a|^2$ and the probability of getting $|1\rangle$ is $|b|^2$. Here we associate a vector $(a, b) \in \mathbb{C}^2$, so that $|a|^2 + |b|^2 = 1$.

Vector Space

A vector space V over a field F satisfies a set of axioms.
As an example any point on a 2-dimensional Euclidean plane may be viewed as a vector (position vector). The collection of these vectors form a vector space over the field of reals$(\mathbb{R})$.

Note

Euclidean vectors are usually taken as a column vectors. A column vector will be written as,

$$\overrightarrow{v} = \begin{bmatrix} v_1 \\ \cdots \\ v_n \end{bmatrix} = (v_1, \cdots, v_n)$$

A row vector will be written as
$\overleftarrow{u} = [u_1, u_2, \cdots, u_n]$.

Vector Space

- In the space $\mathbb{R}^n$ the origin is the null vector $(0, \cdots, 0)$.
- Two vectors can be added and addition satisfies usual properties e.g. associativity, commutativity, inverse etc.
- The null vector is the identity element of addition.

Vector Space

- A vector can be multiplied by an element of the field, known as scalar.
- In case of Euclidean vectors, a scalar multiplication scales the Euclidean norm or length of the vector.
  $k(v_1, \cdots, v_n) = (kv_1, \cdots, kv_n)$, where $k \in \mathbb{R}$, and $|k(v_1, \cdots, v_n)| = k|(v_1, \cdots, v_n)|$.

Vector Space

- Standard basis of an n-dimensional Euclidean vector space is a set n unit vectors along n axes. But any set of n orthogonal unit vectors may form a basis.
- The whole n-dimensional vector space can be generated by linear combination of the basis vectors - for $n = 3$, any vector $\overrightarrow{v} = a\vec{i} + b\vec{j} + c\vec{k}$, where $a, b, c \in \mathbb{R}$.

Vector Space

It is easy to visualise this 2 or 3-dimensional vector space over reals. But the visualisation of the space of qubits which is a 2-dimensional vector space over complex is difficult.

Dirac Vectors

Traditionally a quantum state is represented by a ket vector $|x\rangle$, where x is any name. We shall us this Dirac notation of ket vectors for all our subsequent definitions. But most of them are general enough for any vector space with inner product.

Linear Combination

Given a set of vectors $\{\vec{v_1}, \cdots, \vec{v_n}\}$ over a field F, and a set of scalars $a_1, \cdots, a_n \in F$, a linear combination or superposition is a vector $\vec{v}$ defined as

$$\vec{v} = a_1\vec{v_1} + \cdots + a_n\vec{v_n}.$$

Span

Given a set of vectors S over a field F, the collection of all possible F-vectors V that can be generated by linear combinations of elements of S is called the span of S.

Linearly Dependent and Independent

A set $S = \{\vec{v_1}, \cdots, \vec{v_n}\}$ vectors over F is linearly dependent if there are n scalars $a_1, \cdots, a_n \in F$, not all zeros, such that

$$a_1\vec{v_1} + \cdots + a_n\vec{v_n} = \vec{0},$$

where $\vec{0}$ is the null vector. If no such set of scalars is there, then S is called linearly dependent.

Linearly Dependent and Independent

In 2 or 3-dimensional vector space over reals,

1. $\{(0,0),(a,b)\}$ is a linearly dependent set.
2. $\{(1,2,2),(1,1,2),(2,-1,4)\}$ is a linearly dependent set as $3(1,2,2)+(-5)(1,1,2)+(2,-1,4) = (0,0,0)$.
3. $\{(1,0),(0,1)\}$ is linearly independent.
4. $\{(1,1,3),(3,1,5),(2,1,6)\}$ is also linearly independent.

Basis

If S is a set of linearly independent vectors and V is the span of S, then the set S is called a basis of V.

Basis

The standard basis for 2-dimensional Euclidean space is $\{(1,0),(0,1)\}$. Another basis may be $\{(1/\sqrt{2},1/\sqrt{2}),(-1/\sqrt{2},1/\sqrt{2})\}$.

Consider a vector $(1,2)$, we can write

- $1\cdot(1,0)+2\cdot(0,1)=(1,2)$, and
- $3/\sqrt{2}\cdot(1/\sqrt{2},1/\sqrt{2})+1/\sqrt{2}(-1/\sqrt{2},1/\sqrt{2})=(1,2)$.

Inner Product

Given two n-dimensional Euclidean vectors $\overrightarrow{u} = (u_1, \cdots, u_n)$ and $\overrightarrow{v} = (v_1, \cdots, v_n)$ we define a map from $\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ called an inner product or dot product. Its value is $\sum_{i=1}^{n} u_i v_i$ and is written as $\overrightarrow{u} \cdot \overrightarrow{v}$.
As a matrix product it may be viewed as the product of a row and a column vector.

Inner Product of Ket Vector

Given two ket vectors $|u\rangle$ and $|v\rangle$, the inner product of them is a map from $V \times V \rightarrow \mathbb{C}$, where V is the inner product space where the ket vectors live. It is written as $\langle u|v\rangle$, which is a complex number.

People use bra vector $\langle u|$ as the dual vector of $|u\rangle$. If $|u\rangle = (a + ib, c + id)$ then $[a - ib, c - id]$ the adjoint $|u\rangle$.

Properties of Inner Product of Ket

- $\langle u|u\rangle \geq 0$ (non-negative real). It is 0 if and only if $|u\rangle$ is null.
- $\langle u|v\rangle = \overline{\langle v|u\rangle}$, where $\overline{\langle v|u\rangle}$ is the complex conjugate of $\langle u|v\rangle$.
- $\langle u|(a\,|v\rangle + b\,|w\rangle)\rangle = a\,\langle u|v\rangle + b\,\langle u|w\rangle$ - it is linear on its second argument.

Properties of Inner Product of Ket

Let $|u\rangle = (a + ib, c + id)$.
$\langle u|u\rangle = [a - ib, c - id](a + ib, c + id) = (a^2 + b^2 + c^2 + d^2)$. This is a real number. It is zero if and only if $a = b = c = d = 0$.

Properties of Inner Product of Ket

Let $|u\rangle = (a+ib, c+id)$ and $|v\rangle = (p+iq, r+is)$.

$$\begin{aligned}
\langle u|v\rangle &= [a-ib, c-id](p+iq, r+is) \\
&= (a-ib)(p+iq)+(c-id)(r+is) \\
&= \overline{\overline{(a-ib)(p+iq)+(c-id)(r+is)}} \\
&= \overline{(a+ib)(p-iq)+(c+id)(r-is)} \\
&= \overline{\langle v|u\rangle}.
\end{aligned}$$

Properties of Inner Product of Ket

Let $|u\rangle = (a+ib, c+id)$, $|v\rangle = (p+iq, r+is)$, $|w\rangle = (e+if, g+ih)$ and $\alpha, \beta \in \mathbb{C}$.

$$\begin{aligned} & \langle u|(\alpha\,|v\rangle + \beta\,|w\rangle)\rangle \\ = \;& \langle u|(\alpha\,|v\rangle)\rangle + \langle u|(\beta\,|w\rangle)\rangle \\ = \;& [a-ib, c-id](\alpha(p+iq, r+is) + \beta(e+if, g+ih)) \\ = \;& \alpha\,\langle u|v\rangle + \beta\,\langle u|w\rangle \end{aligned}$$

Linear on the second component.

Properties of Inner Product of Ket

Let $|u\rangle = (a+ib, c+id)$, $|v\rangle = (p+iq, r+is)$, $|w\rangle = (e+if, g+ih)$ and $\alpha, \beta \in \mathbb{C}$.

$$\begin{aligned}
& \langle (\alpha u + \beta v)| \, |w\rangle) \rangle \\
= \ & \langle (\alpha u)|w\rangle + \langle (\beta v)|w\rangle \\
= \ & \overline{\alpha}[a-ib, c-id](e+if, h+ih) + \\
& \overline{\beta}[p-iq, r-is](e+if, h+ih) \\
= \ & \overline{\alpha}\, \langle u|w\rangle + \overline{\beta}\, \langle v|w\rangle \, .
\end{aligned}$$

Anti-linear on the first component.

Note

- Inner product of a Euclidean vector $\vec{v} \in \mathbb{R}^n$ with itself gives the square of its length, $|\vec{v}| = \sqrt{\vec{v} \cdot \vec{v}}$. It is 0 if and only if $\vec{v} = (0, \cdots, 0)$, the null vector.
- The the inner product of Euclidean vector is commutative i.e. $\vec{u} \cdot \vec{v} = \vec{v} \cdot \vec{u}$.
- But the inner product of ket vectors is non-commutative.

Note

In case of complex vector space, $\mathbb{C}^n$, the inner product of two vectors $\vec{u} = (u_1, \cdots, u_n)$ and $\vec{v} = (v_1, \cdots, v_n)$, where $u_i, v_i \in \mathbb{C}$ is defined as $\vec{u} \cdot \vec{v} = \sum_{i=1}^{n} \overline{u_i} v_i$, where $\overline{u_i}$ is the complex conjugate of u_i.

The definition of inner product of ket vectors satisfies the properties of inner product of complex vector space.

Note

So we get

- $\vec{u} \cdot \vec{u} = \sum_{i=1}^{n} \overline{u_i} u_i = \sum_{i=1}^{n} |u_i|^2$.
- $\vec{v} \cdot \vec{u} = \sum_{i=1}^{n} \overline{v_i} u_i = \sum_{i=1}^{n} \overline{v_i \overline{u_i}}$
  $= \overline{\sum_{i=1}^{n} v_i \overline{u_i}} = \overline{\vec{u} \cdot \vec{v}}$.

Orthogonal Vectors

Two vectors $\vec{u}$ and $\vec{v}$ are said to be orthogonal if $\vec{u} \cdot \vec{v} = 0$. In ket notation $\langle u|v\rangle = 0$.
A set of vectors are said to be orthogonal if they are pairwise orthogonal.

Orthonormal Vectors

The natural length or norm of a vector $\vec{v}$ in an inner product space is $\sqrt{\vec{u}\cdot\vec{u}}$. For ket vector $|u\rangle$ it is $\sqrt{\langle u|u\rangle}$.

A set of ket vectors $\{|u_1\rangle, \cdots, |u_n\rangle\}$ is said to be orthonormal if they are orthogonal and lengths of each u_i is one i.e $\langle u_i|u_j\rangle = \delta_{ij}$, where

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Representation of Qubit

The basis of the state space of a qubit is a pair of 2-dimensional complex vectors that are orthonormal and spans $\mathbb{C}^2$.

We may view

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ or } (1, 0) \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ or } (0, 1)$$

Representation of Qubit

It is clear that they are orthonormal -

$$[1,0]\cdot(1,0) = 1 + 0 = 1 = [0,1]\cdot(0,1),$$

$$[1,0]\cdot(0,1) = 0 + 0 = 0 = [0,1]\cdot(1,0),$$

And linear combination of them generates any element of $\mathbb{C}^2$.

$$a\,|0\rangle + b\,|1\rangle = (a,0) + (0,b) = (a,b),$$

where $a, b \in \mathbb{C}$.

Basis is not Unique

As it is well known, the set of orthonormal basis is not unique. We may take any $\{(\cos\theta, \sin\theta), (-\sin\theta, \cos\theta)\}$ as an orthonormal basis for $\mathbb{C}^2$.
Two examples are -
$\{(1/2, \sqrt{3}/2), (-\sqrt{3}/2, 1/2))\}$ and
$\{(1/\sqrt{2}, 1/\sqrt{2}), (-1/\sqrt{2}, 1/\sqrt{2})\}$,

Measurement Axiom

- Interaction of silver atoms with a Stern-Gerlach apparatus is viewed as a measurement on a 2-state quantum system.
- A particular set of basis vectors (two elements) of the qubit space is associated with a measuring device.

Measurement Axiom

- A measurement transforms a qubit state to one of the basis states of the device with appropriate probability.
- If $\{|0\rangle, |1\rangle\}$ are the orthonormal basis vectors associated with a measurement, and a qubit state $|u\rangle = a|0\rangle + b|1\rangle$, then after the measurement the qubit will be in $|0\rangle$ or $|1\rangle$ with probabilities $|a|^2$ and $|b|^2$ respectively.

Measurement Axiom and SG-Device

Let us associate the basis vectors $\{(1,0),(0,1)\}$ with the SG$_z$ device and the basis vectors $\{(1/\sqrt{2},-1/\sqrt{2}),(1/\sqrt{2},1/\sqrt{2})\}$ with the SG$_x$ device.

- State of a silver atom entering a SG$_z$ device may be viewed as $1/\sqrt{2}(1,0)+1/\sqrt{2}(0,1)=(1/\sqrt{2},1/\sqrt{2})$ So each atom will either be in $|0\rangle=(1,0)$ or in $|1\rangle=(0,1)$ with equal probability.

Measurement Axiom and SG-Device

In experiment-2, when a silver atom in state $|0\rangle = (1, 0)$ enters the SG$_x$ device, its state is a superposition of $\{(1/\sqrt{2}, -1/\sqrt{2}), (1/\sqrt{2}, 1/\sqrt{2})\}$ i.e. $|0\rangle = (1, 0) =$ $1/\sqrt{2}(1/\sqrt{2}, -1/\sqrt{2}) + 1/\sqrt{2}(1/\sqrt{2}, 1/\sqrt{2})$. So the incoming atoms will either be in $(1/\sqrt{2}, -1/\sqrt{2})$ or in $(1/\sqrt{2}, 1/\sqrt{2})$ with equal probability.

Measurement Axiom and SG-Device

Finally in experiment-3 when atom in state $(1/\sqrt{2}, -1/\sqrt{2})$ enters the SG$_z$ device, its state is a superposition of $\{(1,0),(0,1)\}$ i.e. $(1/\sqrt{2}, -1/\sqrt{2}) = 1/\sqrt{2}(1,0) - 1/\sqrt{2}(0,1)$. It explains the result of the experiment.

Redundancy

- Every distinct unit vectors of $\mathbb{C}^2$ is not a distinct qubit state.
- $|u\rangle = a|0\rangle + b|1\rangle$ and $|v\rangle = c|0\rangle + d|1\rangle$ represent the same qubit state if $|v\rangle = \alpha|u\rangle$, where $\alpha \in \mathbb{C}$ and $|\alpha| = 1$.
  So $a|0\rangle + b|1\rangle$ and $e^{i\theta}(a|0\rangle + b|1\rangle)$ represents the same qubit state.

Global Phase

A multiplier of the form $\alpha = \cos\theta + i\sin\theta = e^{i\theta}$ is known as global phase of the state and cannot be detected by any measurement.

Let $|a\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|b\rangle = e^{i\theta}(\alpha\,|0\rangle + \beta\,|1\rangle)$, where $|\alpha|^2 + |\beta|^2 = 1$. Let the orthonormal basis for a measurement M be $B = \{|x\rangle\,, |y\rangle\}$.

Global Phase

After the measurement we have $|a\rangle = (\alpha, \beta) = p\,|x\rangle + q\,|y\rangle$ so that the qubit will be in state $|x\rangle$ with a probability $|p|^2$ or in state $|y\rangle$ with a probability $|q|^2$.

If the same measurement is performed on $|b\rangle = (e^{i\theta}\alpha, e^{i\theta}\beta) = e^{i\theta}p\,|x\rangle + e^{i\theta}q\,|y\rangle$, the probabilities of outcomes remain unchanged as $|e^{i\theta}p|^2 = |e^{i\theta}|^2|p|^2 = |p|^2$.

Global Phase

- The equality $|a\rangle = e^{i\theta}|a\rangle = |b\rangle$ induces an equivalence relation $|a\rangle \sim |b\rangle$ over vectors of $\mathbb{C}^2$.
- The quotient space is called complex projective space of dimension one (CP^1). The state of a qubit has one to one correspondence with CP^1

Relative Phase

- Let $|u\rangle = a\,|0\rangle + b\,|1\rangle$, where $a = r_1 e^{i\theta_1}$ and $b = r_2 e^{i\theta_2}$, so that $\frac{a}{b} = \frac{r_1}{r_2} e^{i(\theta_1 - \theta_2)}$.
- $e^{i(\theta_1 - \theta_2)}$ is called the relative phase of the amplitudes a and b.

Relative Phase

- Two superpositions $|u\rangle = a|0\rangle + b|1\rangle$ and $|v\rangle = c|0\rangle + d|1\rangle$ with same magnitudes of amplitudes ($|a| = |c|$, $|b| = |d|$) but different relative phases, represents different states.
- So $a|0\rangle + b|1\rangle$ and $a|0\rangle + e^{i\theta}b|1\rangle$ may represent different states, though $|b| = |e^{i\theta}b|$. A simple example is $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ where $\theta = \pi$.

Relative Phase

Consider $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. If the basis for the measurement be $\{|+\rangle, |-\rangle\}$, then the states can be detected.

A Few Important States

$$\begin{aligned}
|+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
|-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
|\boldsymbol{i}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + \boldsymbol{i}\,|1\rangle) \\
|-\boldsymbol{i}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - \boldsymbol{i}\,|1\rangle)
\end{aligned}$$

$\{|+\rangle, |-\rangle\}$ is known as Hadamard basis.

Qubit Visualisation

A qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ can be represented as $r_a e^{i\theta_a}|0\rangle + r_b e^{i\theta_b}|1\rangle$, where $a = r_a e^{i\theta_a},\ b = r_b e^{i\theta_b}$ and $r_a^2 + r_b^2 = 1$.
Let $r_a = \cos(\theta/2),\ r_b = \sin(\theta/2)$ and
$\theta_b - \theta_a = \phi$.
We get $|\psi\rangle = e^{i\theta_a}(\cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle)$.

On Bloch Sphere

We have already argued that the global phase is not observable, so we can ignore it and get

$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle.$

We keep $0 \leq \theta \leq \pi$ and $-\pi \leq \phi \leq \pi$. and identify every qubit as a point on the surface of a 3-dimensional unit sphere known as Bloch sphere.

Note that the coefficient of $|0\rangle$ is positive real.

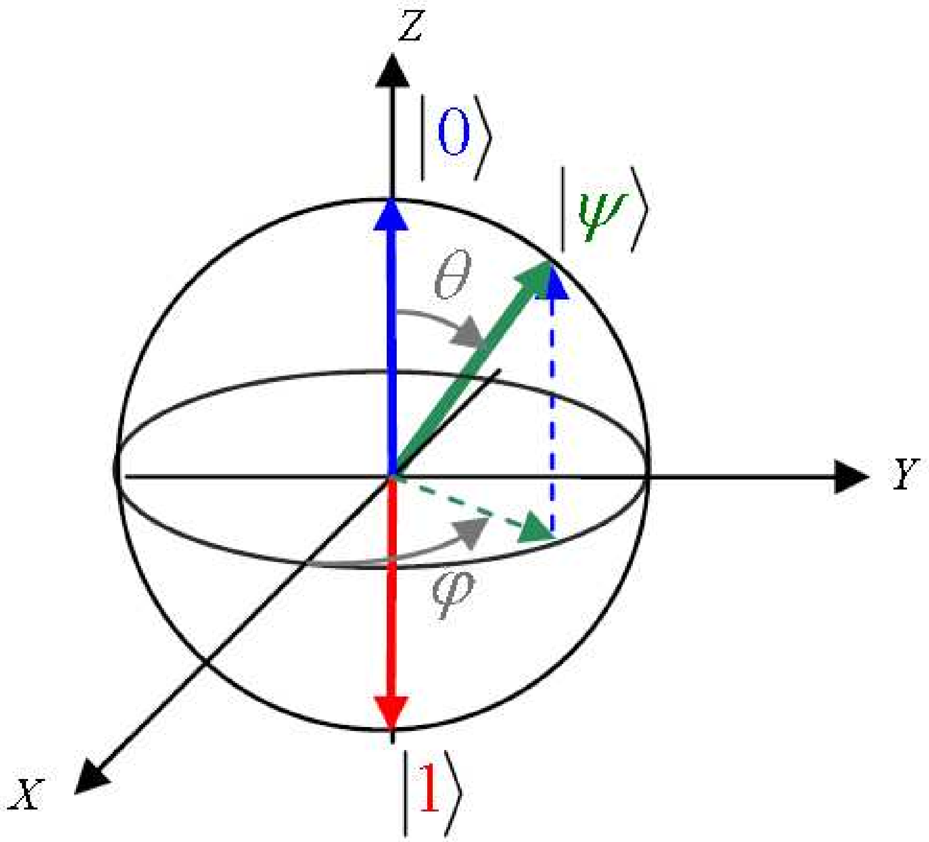


Image Source: https://commons.wikimedia.org/wiki/File:Sphere_bloch.jpg

Note

Given the angles the position of $|0\rangle$ is the north pole of the sphere (where the z_+-axis meets the sphere). So $\theta = 0$. And $|1\rangle$ is at the south pole. Other axial points on the sphere are the following :

Other Axial Points

- x_+: $\theta = \pi/2, \phi = 0$, vector: $\frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle$
- x_-: $\theta = \pi/2, \phi = \pi$, vector: $\frac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle$
- y_+: $\theta = \pi/2, \phi = \pi/2$, vector: $\frac{|0\rangle+i|1\rangle}{\sqrt{2}} = |i\rangle$
- y_-: $\theta = \pi/2, \phi = -\pi/2$, vector: $\frac{|0\rangle-i|1\rangle}{\sqrt{2}} = |-i\rangle$

Bloch Vector

The point corresponding to the qubit state $\cos\theta/2\,|0\rangle + e^{i\phi}\sin\theta/2\,|1\rangle$ has the Cartesian coordinates $(\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ on the Bloch sphere.

$\mathbb{C} \cup \{\infty\}$

There is a bijection between the qubit space and $\mathbb{C} \cup \{\infty\}$. The map is

$$\begin{aligned} |1\rangle &\mapsto \infty \\ |u\rangle = a\,|0\rangle + b\,|1\rangle &\mapsto \frac{b}{a},\ a \neq 0, \end{aligned}$$

$\mathbb{C} \cup \{\infty\}$

If we consider the Bloch sphere representation of a qubit state, then $|u\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$ is mapped to $\frac{e^{i\phi}\sin\left(\frac{\theta}{2}\right)}{\cos\left(\frac{\theta}{2}\right)} = e^{i\phi}\tan\left(\frac{\theta}{2}\right)$, except for $\theta = \pi$. This mapping is clearly one-to-one. This is also surjective as $\tan\left(\frac{\theta}{2}\right) \in [0, \infty)$ when $\theta \in [0, \pi)$ - every complex number can be written as $re^{i\phi}$ where $r \in [0, \infty)$ and $\phi \in [0, 2\pi]$.

$\mathbb{C} \cup \{\infty\}$

The inverse mapping is

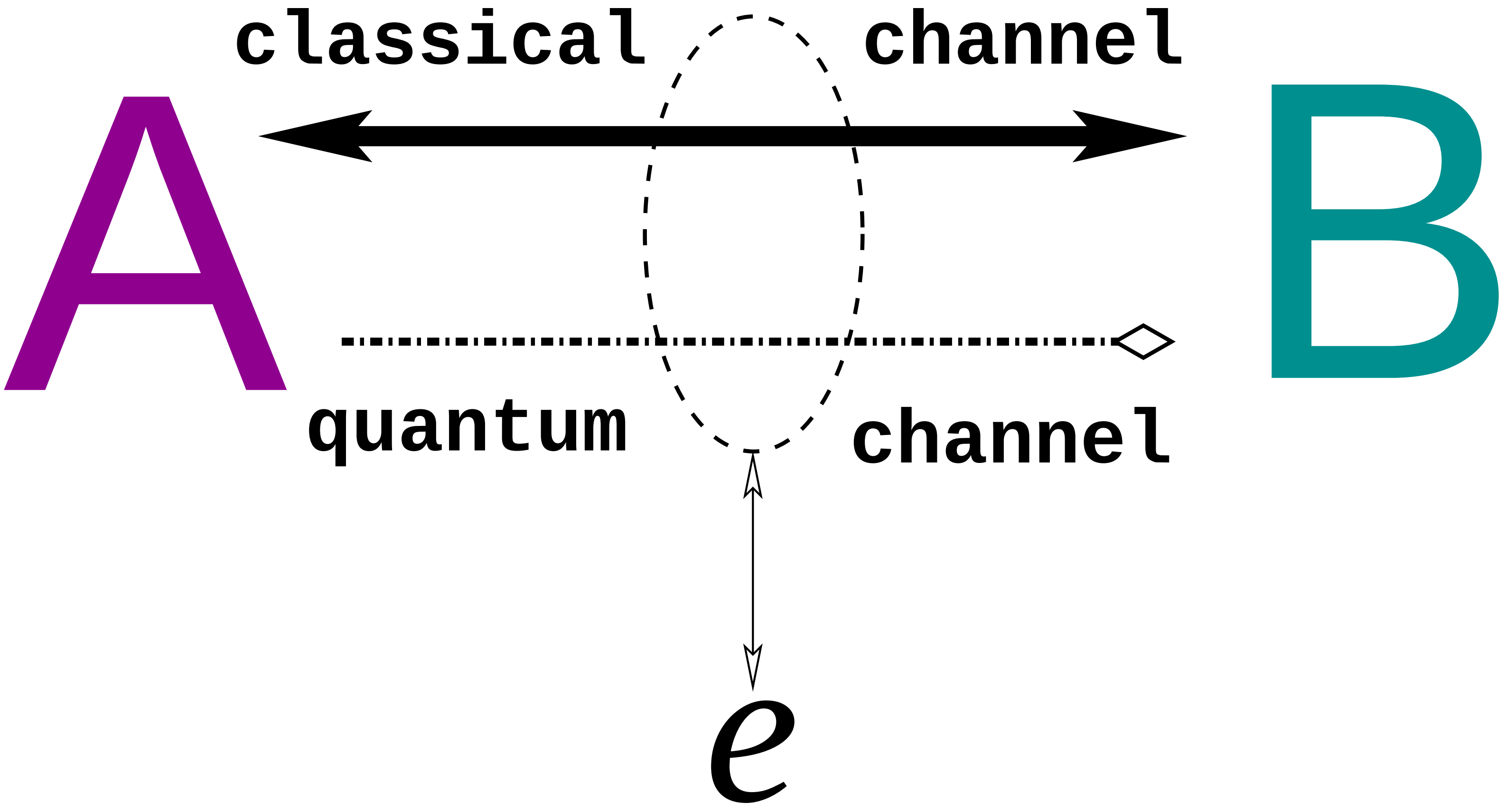
$$z \mapsto \frac{1}{\sqrt{1+|z|^2}} |0\rangle + \frac{z}{\sqrt{1+|z|^2}} |1\rangle .$$

BB84

An early quantum protocol for symmetric key sharing between two parties Alice and Bob is due to Charles Bennett and Gilles Brassard proposed in 1984.

BB84

The goal of the protocol is to generate a shared key, a random sequence of bits, known only to Alice and Bob. The protocol uses properties of qubit and ensures that, if Alice and Bob cannot detect any problem of eavesdropping, then with high probability, the key is secret. But it does not guarantee about the success in key sharing.


classical
channel
A
B
quantum
channel
e

BB84

Alice and Bob are connected by two communication channels - a bidirectional classical channel to transmit bits and an Alice → Bob quantum channel to transmit qubits. An eavesdropper may listen to both the channels.

BB84 Protocols

1. Alice generates a random sequence of bits.
2. She encodes each bit to a qubit by randomly selecting one of the two different agreed upon bases of qubit space e.g.
   $B_1 : \{0 \mapsto |0\rangle, 1 \mapsto |1\rangle\}$ or
   $B_2 : \{0 \mapsto |+\rangle, 1 \mapsto |-\rangle\}$.
   She sends the qubit to Bob through the quantum channel.

BB84 Protocols

3. Bob measures the state of the received qubit by choosing a base at random.

   - If the base chosen by Bob is identical to the encoding base used by Alice, the measured value of the bit is correct.
   - Otherwise, the probability that Bob gets the correct bit is $\frac{1}{2}$.

BB84 Protocols

4. Bob sends an acknowledgement on classical channel after receiving each qubit.
5. Once the transfer of one qubit is ensured, both Alice and Bob exchanges on classical channel the bases they used to encode and decode.
6. They retains the bit if the corresponding bases are identical, otherwise it is discarded.

BB84 Protocols

7. To detect any eavesdropping, they compare a fraction of accepted bits over the classical channel. These bits are also discarded and if they are convinced about no eavesdropping, remaining accepted bits are used as the key.

Eve Listening CC

Alice and Bob exchanges acknowledgement, base information and a fraction of bits finally discarded, on the classical channel. So Eve cannot get the values of the key by listening to classical channel.

Eve Listening QC

When Eve gets the qubit, she has no clue about the base of encoding and she picks up a base at random. So she will pickup a correct (incorrect) base with a probability $\frac{1}{2}$.
The probability that both Eve and Bob choose the correct base for measurement of a qubit is $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. So the probability that Eve gets access to n bit secret key without being detected by Alice and Bob is $\frac{1}{4^n}$.

Wrong Base by Eve

The probability that Eve chooses the wrong base for a qubit she measures is $\frac{1}{2}$. Eve eventually can detect that the base was incorrect, but importantly she has changed the state of the qubit sent to Bob.

Wrong Base by Eve

Now even if Bob chooses the correct base, he may get a wrong bit value with the probability $\frac{1}{2}$.
So in presence of Eve, $\frac{1}{4}$ of the bits retained by Alice and Bob should have mismatch. This they can detect by comparing sufficient number of bits over the classical channel.

No-Cloning Principle

There is no method consistent with the permissible transformations (unitary) of quantum mechanics, that can create two separate copies of an input.
So Eve cannot store a qubit and also pass a copy to Bob without knowing its base.

Man-in-the-Middle-Attack

The protocol is vulnerable if Eve pretends to Alice as Bob and as Alice to Bob.

References

[ERWP] Quantum Computing: A Gentle Introduction by Eleanor Rieffel & Wolfgang Polak, Pub. MIT Press, 2011, ISBN 978-0-262-52667-8.

[MNIC] Quantum Computation and Quantum Information by Michael A Nielsen & Isaac L Chuang, Pub. Cambridge University Press, 2002, ISBN 81-7596-092-2.

[SA] Quantum Computing Since Democritus by Scott Aaronson, Pub. Cambridge University Press, 2013, ISBN 978-0-521-19956-8.

[AAM] Classical and Quantum Computation by A Yu Kitaev, A H Shen & M N Vyalyi, Pub. American Mathematical Society (GSM vol 47) 2002, ISBN 978-1-4704-0927-2.

References

[PRM] An Introduction to Quantum Computing by Phillip Kaye, Raymond Laflamme & Michele Mosca, Pub. Oxford University Press, 2007, ISBN 978-0-19-923677-0.