Quantum Computing

Developed for the Azera Group

By: Joseph D. Fournier B.Sc.E.E., M.Sc.E.E

Why Quantum Computing?

- One of the most important problems in modern hardware design is the limiting factor of the interspatial distances in the Silicon wafers. Quantum computers offer us the theoretical limit of atomic scale.
- One of the most important network problems is the ability to encrypt documents to increase the security of the network. Quantum encryption techniques offer us a theoretical encryption methodology which is beyond computational feasibility.

Review of Fourier Series

- A **Fourier series** is a sum that is created to represents a periodic function as a sum of sine and cosine harmonic waves. The frequency of each wave in the sum, or harmonic, is an integer multiple of the periodic function's fundamental frequency.
- Each harmonic's phase and amplitude can be determined using harmonic analysis. A Fourier series may potentially contain an infinite number of harmonics.
- Summing part of but not all the harmonics in a function's Fourier series produces an approximation to that function.
-

Introduction to Fourier Series

Let $x(t)$ be a periodic signal with period T, *i.e.*,

$$x(t+T) = x(t), \quad \forall t \in \text{R=Reals}$$

Example: the rectangular pulse train

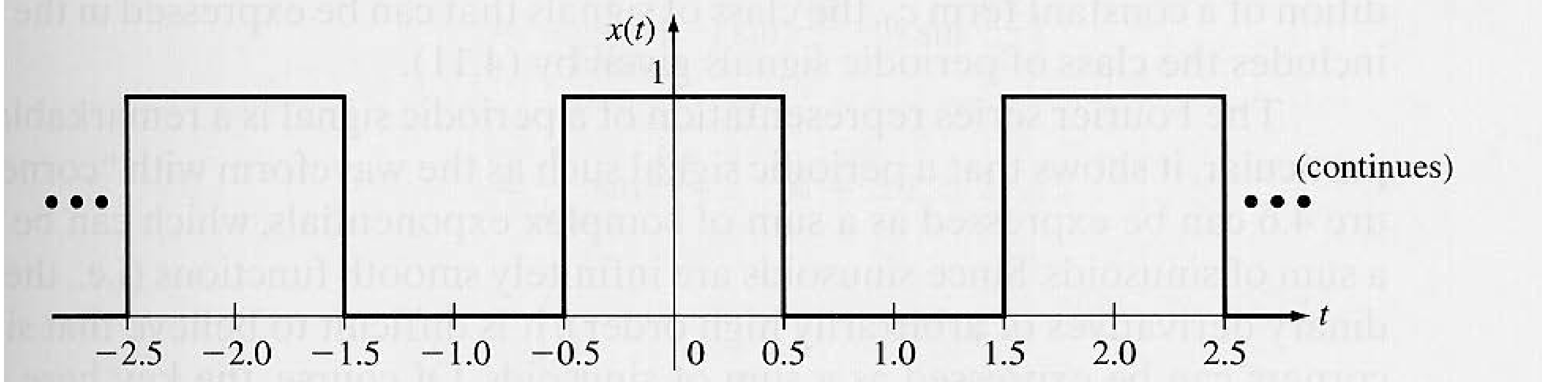


Figure 4.6 Periodic signal with fundamental period $T = 2$.

The Fourier Series

Then, $x(t)$ can be expressed as

$$x(t) = \sum_{k=-\infty}^{\infty} c_k e^{jk\omega_0 t}, \quad t \in \mathrm{R}$$

where $\omega_0 = 2\pi / T$ is the *fundamental frequency* (*rad/sec*) of the signal and

$$c_k = \frac{1}{T} \int_{-T/2}^{T/2} x(t) e^{-jk\omega_o t} dt, \quad k = 0, \pm 1, \pm 2, \ldots$$

c_0 is called the *constant or dc component* of $x(t)$

Convergence Criteria

A periodic signal $x(t)$, has a Fourier series if it satisfies the following conditions:

1. $x(t)$ is absolutely integrable over any period, namely

$$\int_{a}^{a+T} |x(t)|\,dt < \infty, \quad \forall a \in \mathrm{R}$$

2. $x(t)$ has only a finite number of maxima and minima over any period
3. $x(t)$ has only a finite number of discontinuities over any period

Trigonometric Fourier Series

By using Euler's formula, we can rewrite

$$x(t) = \sum_{k=-\infty}^{\infty} c_k e^{jk\omega_0 t}, \quad t \in \mathrm{R}$$

as

$$x(t) = c_0 + \sum_{k=1}^{\infty} 2|c_k|\cos(k\omega_0 t + \angle c_k), \quad t \in \mathrm{R}$$

as long as *x(t)* is real.

This expression is called the trigonometric Fourier series of $x(t)$

Parseval's Theorum

Let $x(t)$ be a periodic signal with period T

The *average power* P of the signal is defined as

$$P = \frac{1}{T}\int_{-T/2}^{T/2} x^2(t)\,dt$$

- Expressing the signal as $x(t) = \sum_{k=-\infty}^{\infty} c_k e^{jk\omega_0 t}, \quad t \in \mathbb{R}$ it is also

$$P = \sum_{k=-\infty}^{\infty} |c_k|^2$$

Fourier Transform: One

- We have seen that periodic signals can be represented with the Fourier series
- Can aperiodic signals be analyzed in terms of frequency components?
- Yes, and the Fourier transform provides the tool for this analysis
- The major difference w.r.t. the line spectra of periodic signals is that the spectra of aperiodic signals are defined for all real values of the frequency variable not just for a discrete set of values

Fourier Transform: Two

- Consider $X(\omega) = \int_{-\infty}^{\infty} x(t) e^{-j\omega t} dt, \quad \omega \in \mathrm{R}$

- Since $X(\omega)$ in general is a complex function, by using Euler's formula

$$X(\omega) = \underbrace{\int_{-\infty}^{\infty} x(t)\cos(\omega t)dt}_{R(\omega)} + j\underbrace{\left(-\int_{-\infty}^{\infty} x(t)\sin(\omega t)dt \right)}_{I(\omega)}$$

$$X(\omega) = R(\omega) + jI(\omega)$$

Inverse Fourier Transform

- Given a signal $x(t)$ with Fourier transform $X(\omega)$, $x(t)$ can be recomputed from $X(\omega)$ by applying the inverse Fourier transform given by

$$x(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} X(\omega) e^{j\omega t} d\omega, \quad t \in \mathrm{R}$$

- Transform pair $\quad x(t) \leftrightarrow X(\omega)$

Properties of Fourier Transform

$$x(t) \leftrightarrow X(\omega) \qquad y(t) \leftrightarrow Y(\omega)$$

- *Linearity:*

$$\alpha x(t) + \beta y(t) \leftrightarrow \alpha X(\omega) + \beta Y(\omega)$$

- *Left or Right Shift in Time:*

$$x(t - t_0) \leftrightarrow X(\omega) e^{-j\omega t_0}$$

- *Time Scaling:*

$$x(at) \leftrightarrow \frac{1}{a} X\left(\frac{\omega}{a}\right)$$

Properties of Fourier Transforms

- *Time Reversal:*

$$x(-t) \leftrightarrow X(-\omega)$$

- *Multiplication by a Power of t:*

$$t^n x(t) \leftrightarrow (j)^n \frac{d^n}{d\omega^n} X(\omega)$$

- *Multiplication by a Complex Exponential:*

$$x(t)e^{j\omega_0 t} \leftrightarrow X(\omega - \omega_0)$$

Properties of Fourier Transforms

- Multiplication by a Sinusoid (Modulation):

$$x(t)\sin(\omega_0 t) \leftrightarrow \frac{j}{2}\left[X(\omega+\omega_0) - X(\omega-\omega_0)\right]$$

$$x(t)\cos(\omega_0 t) \leftrightarrow \frac{1}{2}\left[X(\omega+\omega_0) + X(\omega-\omega_0)\right]$$

- Differentiation in the Time Domain:

$$\frac{d^n}{dt^n}x(t) \leftrightarrow (j\omega)^n X(\omega)$$

Properties of Fourier Transforms

- Integration in the Time Domain:

$$\int_{-\infty}^{t} x(\tau)d\tau \leftrightarrow \frac{1}{j\omega}X(\omega) + \pi X(0)\delta(\omega)$$

- Convolution in the Time Domain:

$$x(t) * y(t) \leftrightarrow X(\omega)Y(\omega)$$

- Multiplication in the Time Domain:

$$x(t)y(t) \leftrightarrow X(\omega) * Y(\omega)$$

Properties of Fourier Transforms

- Parseval's Theorem:

$$\int_{-\infty}^{\infty} x(t)y(t)dt \leftrightarrow \frac{1}{2\pi}\int_{-\infty}^{\infty} X^*(\omega)Y(\omega)d\omega$$

- If $y(t) = x(t)$ $\int_{-\infty}^{\infty} |x(t)|^2 dt \leftrightarrow \frac{1}{2\pi}\int_{-\infty}^{\infty} |X(\omega)|^2 d\omega$
- Duality:

$$X(t) \leftrightarrow 2\pi x(-\omega)$$

Mathematical form of the Fourier Transform

- Given a signal *x*(*t*), its Fourier transform $X(\omega)$ is defined as

$$X(\omega) = \int_{-\infty}^{\infty} x(t)e^{-j\omega t}dt, \quad \omega \in \mathrm{R}$$

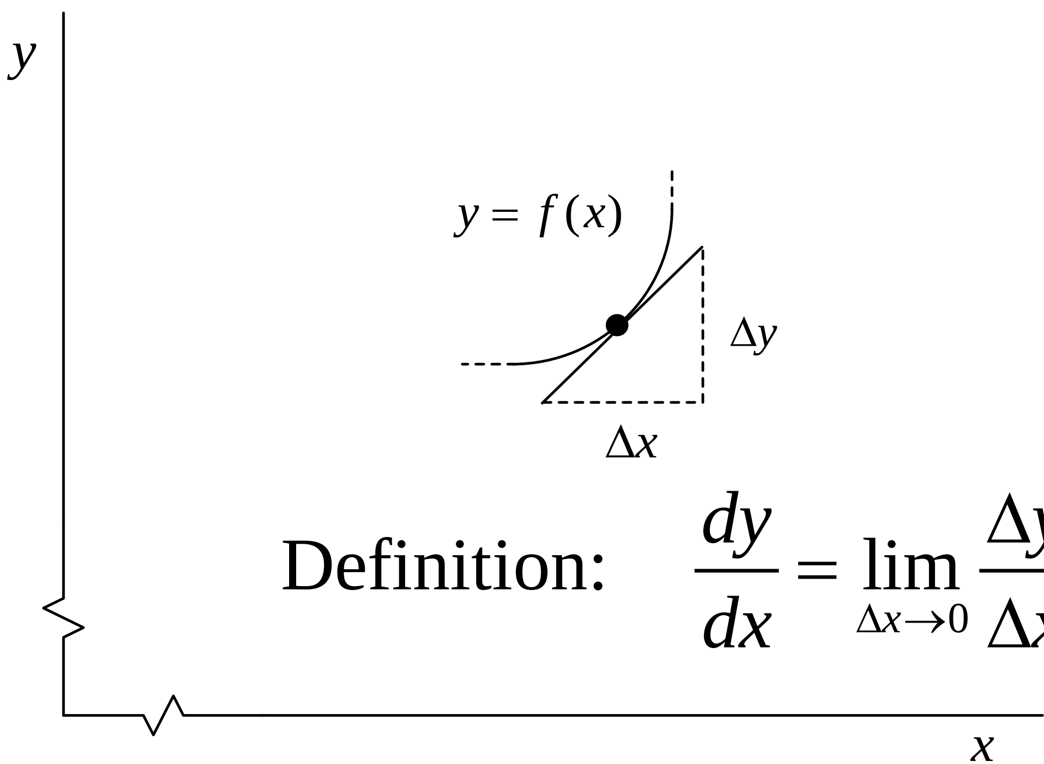
- A signal *x*(*t*) is said to have a *Fourier transform in the ordinary sense* if the above integral converges

Introduction to Differential Calculus

- The study of calculus usually begins with the basic definition of a *derivative*. A derivative is obtained through the process of *differentiation,* and the study of all forms of differentiation is collectively referred to as *differential calculus*.
- If we begin with a function and determine its derivative, we arrive at a new function called the *first derivative*. If we differentiate the *first derivative*, we arrive at a new function called the *second derivative*, and so on.

What is a derivative?

The derivative of a function is the *slope* at a given point.

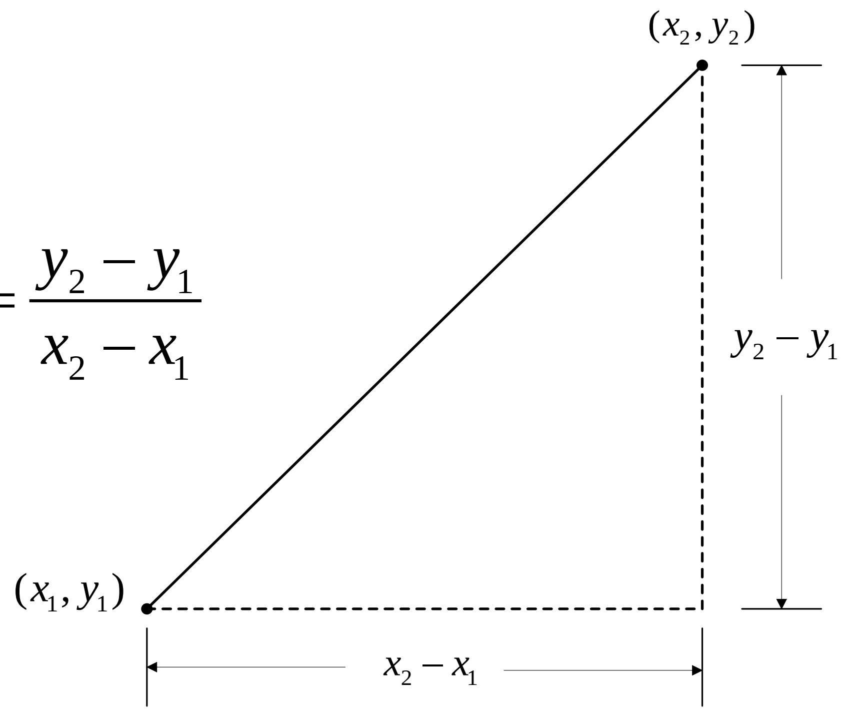


Definition: $$\frac{dy}{dx} = \lim_{\Delta x \to 0} \frac{\Delta y}{\Delta x}$$

Representations of a Derivative

$$\frac{dy}{dx} \quad \text{or} \quad f'(x) \quad \text{or} \quad \frac{df(x)}{dx}$$

$$\frac{dy}{dx} = \text{slope} = \frac{y_2 - y_1}{x_2 - x_1}$$



Introduction to Integral Calculus

Anti-Derivatives

An anti-derivative of a function $f(x)$ is a new function $F(x)$ such that

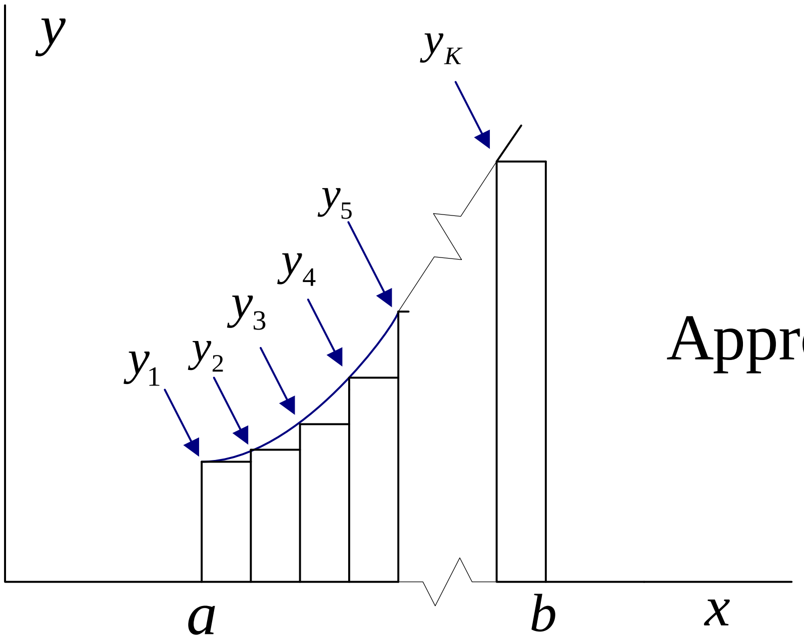
$$\frac{dF(x)}{dx} = f(x)$$

Definite and indefinite Integrals

Indefinite $$\int f(x)dx$$

Definite $$\int_{x_1}^{x_2} f(x)dx$$

Definite Integral as area under a curve



$$\text{Approximate Area} = \sum_k y_k \Delta x$$

Exact Area = $$\int_a^b y\,dx = \lim_{\Delta x \to dx} \sum_k y_k \Delta x$$

Acceleration, velocity and displacement

$$a = a(t) = \text{acceleration in meters/second}^2 \ (\text{m/s}^2)$$

$$v = v(t) = \text{velocity in meters/second (m/s)}$$

$$y = y(t) = \text{displacement in meters } \left(\text{m}\right)$$

$$\frac{dv}{dt} = a(t) \qquad dv = \left(\frac{dv}{dt}\right)dt = a(t)dt$$

$$\int dv = \int a(t)dt \qquad \int dv = v$$

Acceleration, velocity and displacement #2

$$v = \int a(t)dt + C_1$$

$$\frac{dy}{dt} = v(t) \qquad dy = \left(\frac{dy}{dt}\right)dt = v(t)dt$$

$$y = \int v(t)dt + C_2$$

Review of Vector Analysis

Vector analysis is a mathematical tool with which electromagnetic (EM) and Quantum concepts are most conveniently expressed and best comprehended.

A quantity is called a <u>scalar</u> if it has only magnitude (e.g., mass, temperature, electric potential, population).

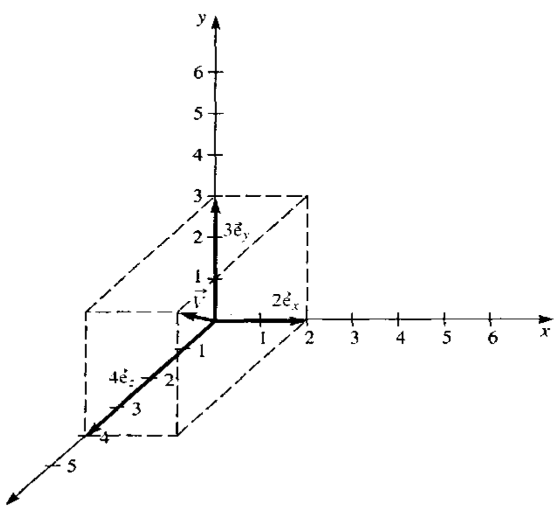
A quantity is called a <u>vector</u> if it has both magnitude and direction (e.g., velocity, force, electric field intensity).

The <u>magnitude</u> of a vector $\overline{A}$ is a scalar written as A or $\left|\overline{A}\right|$

Vectors in Cartesian Co-ordinates

A vector, $\overline{A}$ in Cartesian or rectangular co-ordinates may be represented as:

$$(A_x, A_y, A_z) \quad \text{or} \quad A_x\overline{e}_x + A_y\overline{e}_y + A_z\overline{e}_z$$



Where the vector $\overline{V}$ is given by:

$$\overline{V} = 2\overline{e}_x + 3\overline{e}_y + 4\overline{e}_z$$

Equipotential Surfaces in Cartesian Co-ordinates

Cartesian coordinates (x,y,z) The ranges of the coordinate variables are

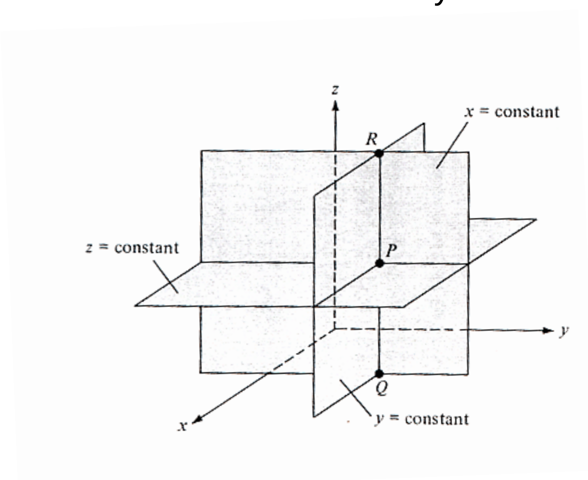
$$-\infty < x < \infty$$

$$-\infty < y < \infty$$

$$-\infty < z < \infty$$

A vector in Cartesian coordinates can be written as

$$(A_x, A_y, A_z) \quad \text{or} \quad A_x\overline{e}_x + A_y\overline{e}_y + A_z\overline{e}_z$$

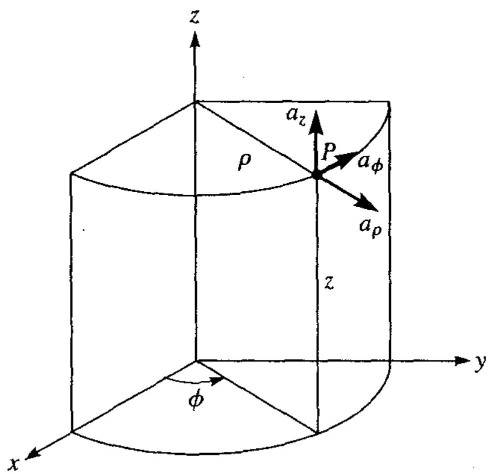


The intersection of three orthogonal infinite planes

(x=const, y= const, and z = const)

defines point P.

Vectors in cylindrical Co-ordinates



Point *P* and unit vectors in the cylindrical coordinate system

$$\overline{e}_\rho \times \overline{e}_\phi = \overline{e}_z$$

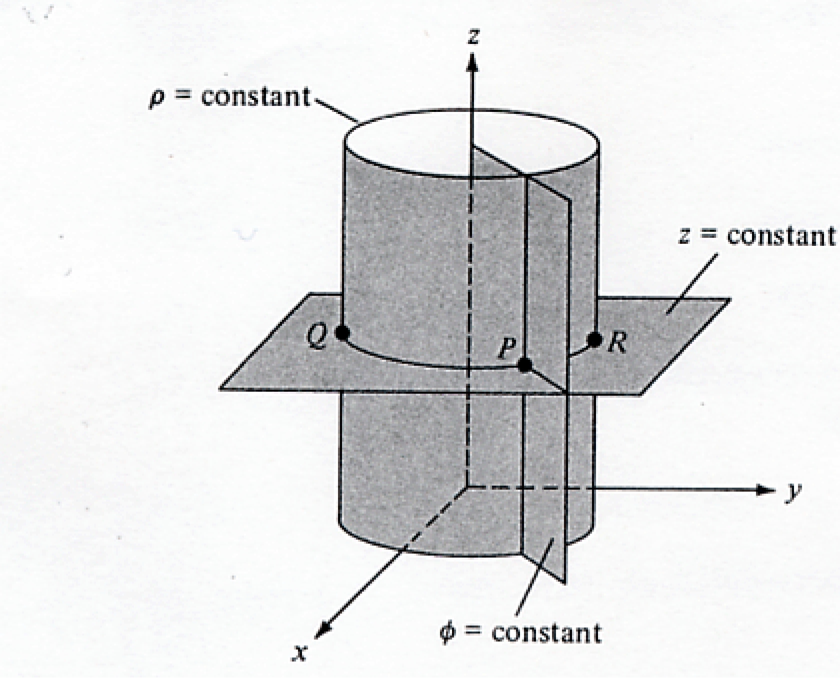
$$\overline{e}_\phi \times \overline{e}_z = \overline{e}_\rho$$

$$\overline{e}_z \times \overline{e}_\rho = \overline{e}_\phi$$

$$\overline{e}_\rho \cdot \overline{e}_\rho = \overline{e}_\phi \cdot \overline{e}_\phi = \overline{e}_z \cdot \overline{e}_z = 1$$

$$\overline{e}_\rho \cdot \overline{e}_\phi = \overline{e}_\phi \cdot \overline{e}_z = \overline{e}_\phi \cdot \overline{e}_\rho = 0$$

Equipotential Surfaces in Cylindrical Co-ordinates



semi-infinite plane with its edge along the z - axis

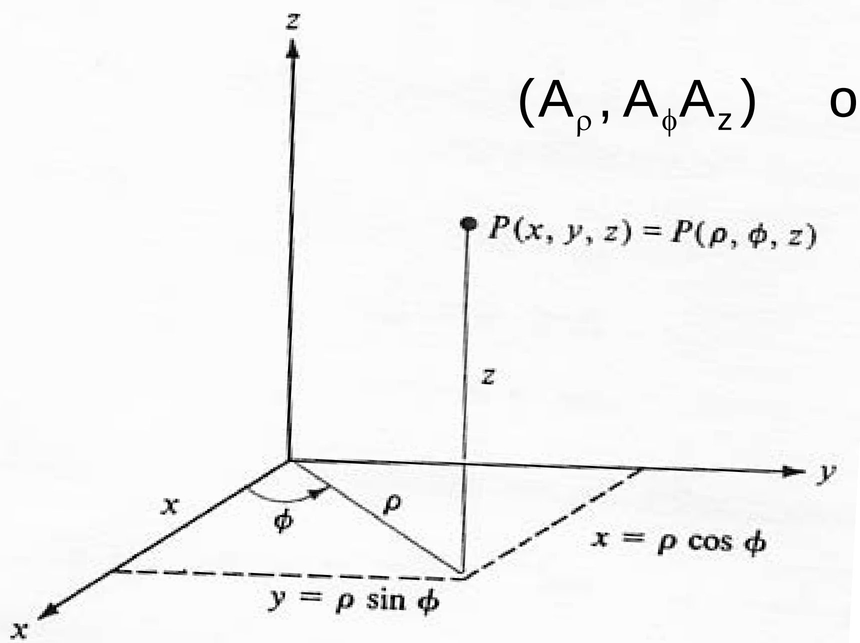
Constant z, ρ, φ surfaces

Cartesian Vectors in Cylindrical Co-ordinates

A vector in cylindrical co-ordinates:

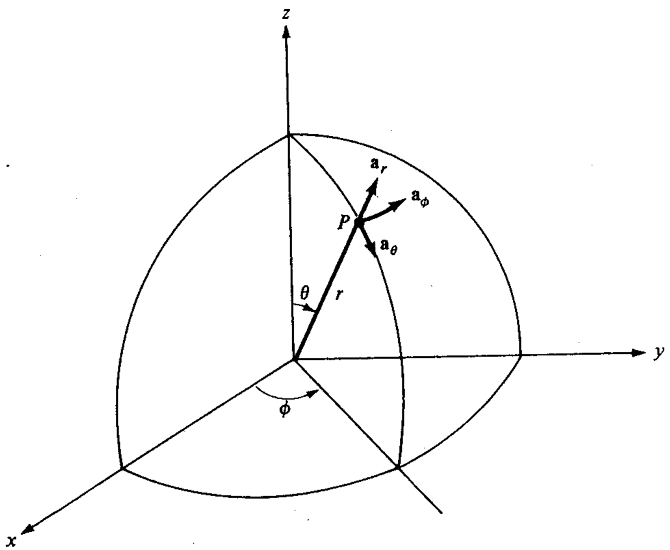
$$(A_\rho, A_\phi A_z) \quad \text{or} \quad A_\rho \overline{e}_\rho + A_\phi \overline{e}_\phi + A_z \overline{e}_z$$

$$\left|\overline{A}\right| = (A_\rho{}^2 + A_\phi{}^2 + A_z{}^2)^{1/2}$$



$$\rho = \sqrt{x^2 + y^2} \qquad \phi = \tan^{-1}\frac{y}{x} \qquad z = z$$

Vectors in Spherical Co-ordinates



$$\overline{e}_r \times \overline{e}_\theta = \overline{e}_\phi$$
$$\overline{e}_\theta \times \overline{e}_\phi = \overline{e}_r$$
$$\overline{e}_\phi \times \overline{e}_r = \overline{e}_\theta$$

$$\overline{e}_r \cdot \overline{e}_r = \overline{e}_\theta \cdot \overline{e}_\theta = \overline{e}_\phi \cdot \overline{e}_\phi = 1$$
$$\overline{e}_r \cdot \overline{e}_\theta = \overline{e}_\theta \cdot \overline{e}_\phi = \overline{e}_\phi \cdot \overline{e}_r = 0$$

A vector A in spherical coordinates may be written as

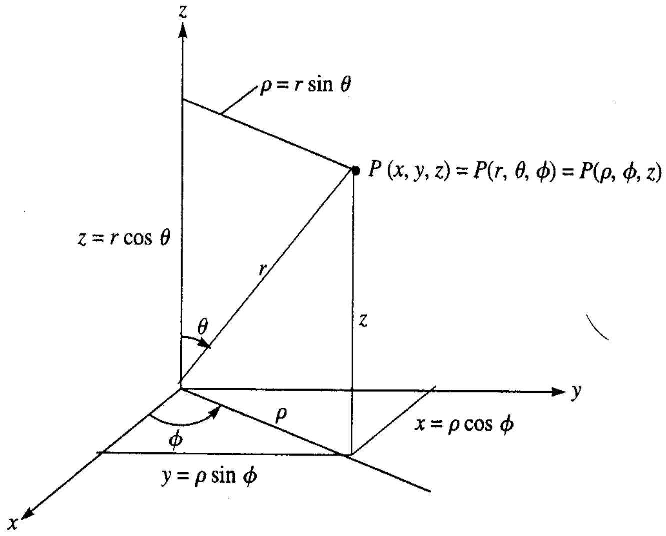
$$(A_r, A_\theta A_\phi) \quad \text{or} \quad A_r\overline{e}_r + A_\theta\overline{e}_\theta + A_\phi\overline{e}_\phi$$

$$\left|\overline{A}\right| = (A_r^{\,2} + A_\theta^{\,2} + A_\phi^{\,2})^{1/2}$$

Cartesian Vectors in Spherical Co-ordinates

$$r = \sqrt{x^2 + y^2 + z^2} \qquad \theta = \tan^{-1}\frac{\sqrt{x^2 + y^2}}{z} \qquad \phi = \tan^{-1}\frac{y}{x} = \cos^{-1}\frac{x}{\sqrt{x^2 + y^2}}$$

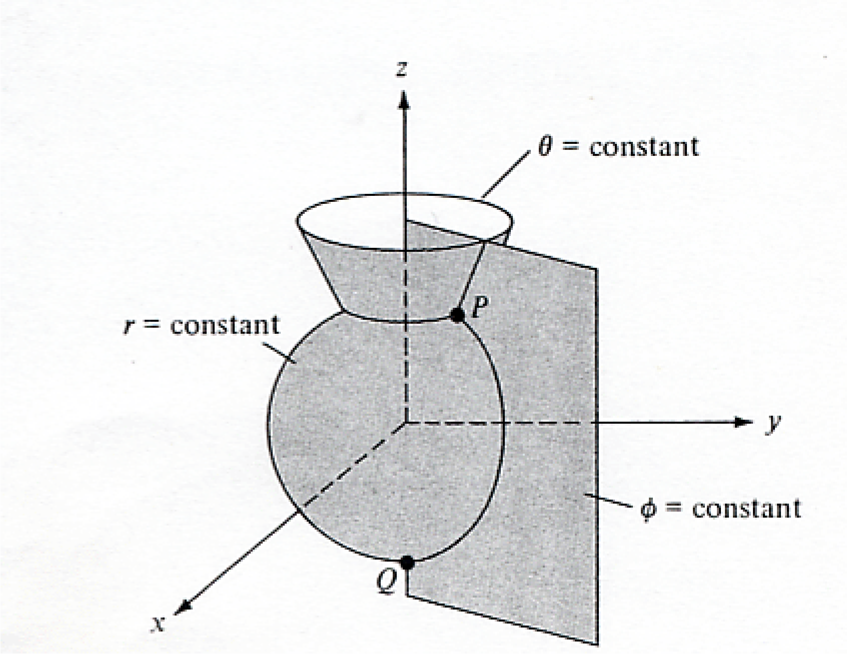
$$\theta = \tan^{-1}\frac{\rho}{z} = \cos^{-1}\frac{z}{r}$$



$$x = r\sin\theta\cos\phi$$
$$y = r\sin\theta\sin\phi$$
$$z = r\cos\theta$$

Relationships between space variables $(x, y, z), (r, \theta, \phi)$, and (ρ, ϕ, z)

Equipotential Surfaces in Spherical Co-ordinates



Constant r , Φ , θ surfaces

Exponential and Sinusoidal Functions

Considering radiations as waves: a periodic function $\Psi(r,t)$ where r is and t is time.
Instead of cosine and sine we will use equivalent exponential expressions:

$$e^{ix} = \cos x + i \sin x \quad \rightarrow \quad \cos x = \frac{e^{ix} + e^{-ix}}{2}$$

$$e^{-ix} = \cos x - i \sin x \quad \rightarrow \quad \sin x = \frac{e^{ix} - e^{-ix}}{2i}$$

Two expressions $\quad \Psi = A\, e^{i(kr-\omega t)} = A\, e^{2\pi i(\frac{r}{\lambda} - \nu t)}$

A is the amplitude

The beam intensity is given by $\Psi^*\Psi = A^2$

which depends neither from k, nor from λ, ν, and ω.

$\boldsymbol{\lambda}$ is the wave length (dimension of a length);

$k = \dfrac{2\pi}{\lambda}$ is the wave number (inverse of a length)

$\boldsymbol{\nu}$ is the frequency; $\omega = 2\pi\nu$ is angular frequency (inverse of time).

Periodicity/Phase Angle/Interference

Ψ is periodic ; $e^{i2\pi} = 1$

Adding 2π to the exponent (either by increasing r, or t), the wave remains unaffected.

Two waves are *in phase* for t=0

- if $\dfrac{r_2}{\lambda_2} - \dfrac{r_1}{\lambda_1} = n$

  Or if $k_2r_2 - k_1r_1 = 2\pi n$

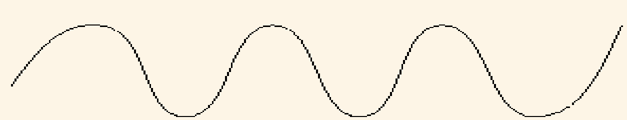
Two waves are *out of phase* at the origin (r=0)

- $\nu_2 t_2 - \nu_1 t_1 = n$

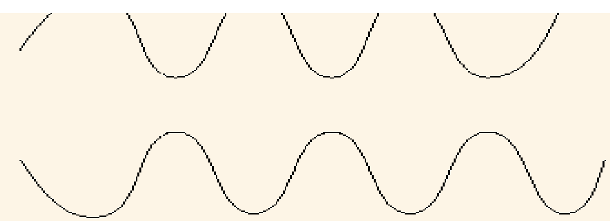
  if $\dfrac{t_2}{T_2} - \dfrac{t_1}{T_1} = n$

  or if $\omega_2 t_2 - \omega_1 t_1 = 2\pi n$ *with n integer*

Constructive Interferences



Destructive Interferences



Phase Velocity

$$(kr_2-\omega t_2) = (kr_1-\omega t_1) \qquad \longrightarrow \qquad k(r_2-r_1) = \omega(t_2-t_1)$$

Where from $v_\varphi = \dfrac{r_2-r_1}{t_2-t_1} = \dfrac{\omega}{k} = \boldsymbol{\lambda\nu}$ et $\nu = \dfrac{v_\varphi}{\lambda}$

Warning, as we will see later

$$\frac{\Delta r}{\Delta t} \textit{ is not equal to } \frac{dr}{dt} \; !$$

$$v_\varphi \textit{ is not equal to } v = \frac{dr}{dt}$$

The velocity, v, will be defined as a derivative :

$v = \dfrac{dr}{dt} = \dfrac{d\omega}{dk}$. $v_\varphi = \dfrac{\Delta r}{\Delta t}$ would be equal to $v = \dfrac{dr}{dt} = \dfrac{\omega}{k}$ only if k vs. ω is a linear expression which is not generally true.

For a photon $v_\varphi = \mathbf{c} = \boldsymbol{\lambda\nu}$ et $\nu = \dfrac{c}{\lambda}$

Introducing new variables

$$\Psi = A\,e^{i(kr-\omega t)} = A\,e^{2\pi i(\frac{r}{\lambda} - \nu t)} = A\,e^{\frac{i}{\hbar}(pr-Et)}$$

At the moment, h is a simple constant

Later on, h will have a dimension and the p and E will be physical quantities

Then

$$p = \hbar\, k = \frac{h}{\lambda} \quad ; \quad E = \hbar\,\omega = h\nu = \frac{h}{T} \quad \text{et} \quad v_\varphi = \frac{E}{p}$$

2 different velocities, v and v_φ

$$v_\varphi = \frac{E}{p}$$

$$E = \frac{mv^2}{2} \text{ and } p = mv \rightarrow v = \frac{2E}{p} = 2v_\varphi$$

v differs from v_φ .

$$p = \hbar k = \frac{h}{\lambda} \quad ; \quad E = \hbar\omega = h\nu = \frac{h}{T} \quad \text{et} \quad v_\varphi = \frac{E}{p}$$

Introduction to Quantum Mechanics

- **Quantum mechanics** is one of the most controversial theories of physics. It portends to provide a description of the physical properties of closed systems at the atomic scale.
- Quantum mechanics differs from classical physics in that energy, momentum, angular momentum, and other quantities of a bound system are restricted to discrete values (quantization)
- Quantum objects have characteristics of both particles and waves.
- Quantum mechanics sets limits to how accurately the value of a physical quantity can be predicted prior to its measurement, given a complete set of initial conditions (the uncertainty principle).

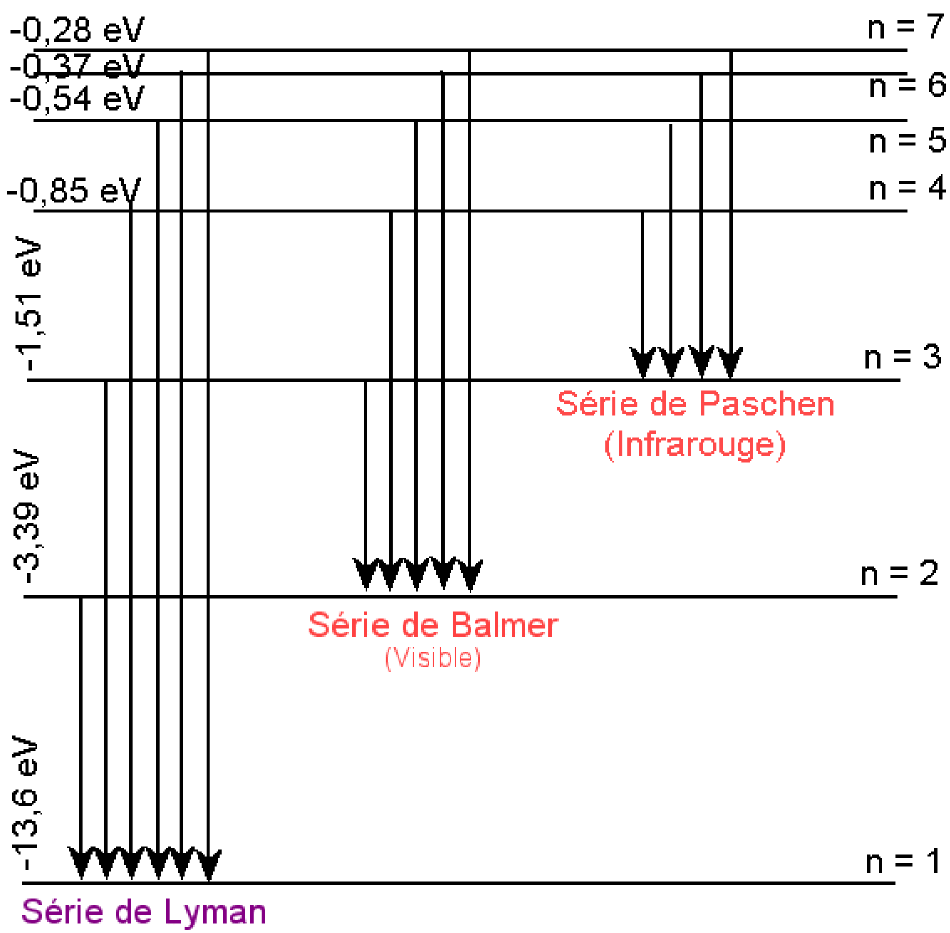
Early problems with classical mechanics

Quantum Mechanics was invented to provide a theoretical basis for atomic phenomena which would correlate with experimental results.

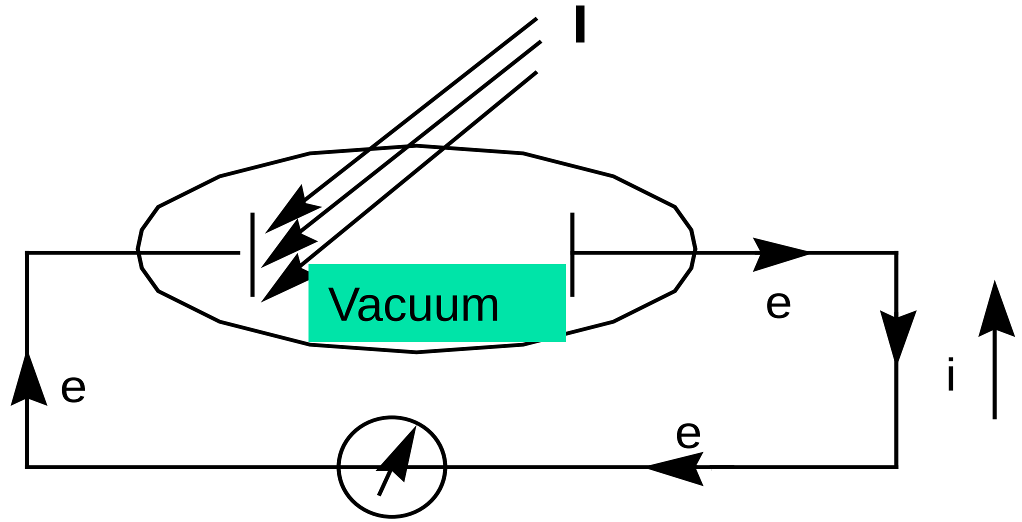
Early experiments on the electronic structure of atoms were centered around the light emitted by atoms of hydrogen under thermal excitation.

Contrary to the predictions of classical electro-magnetic theory these light pulses were very sharp lines.

Atomic Spectroscopy of Hydrogen

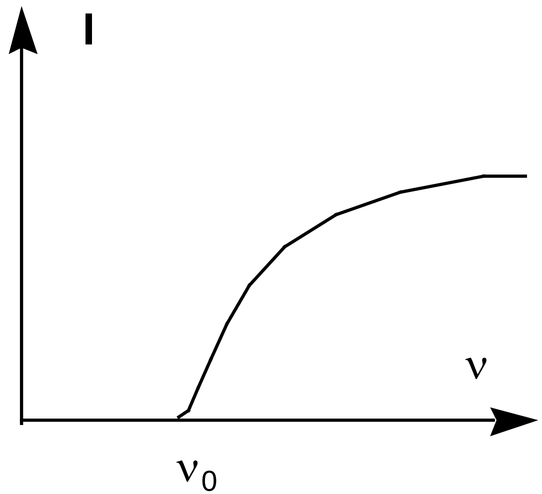


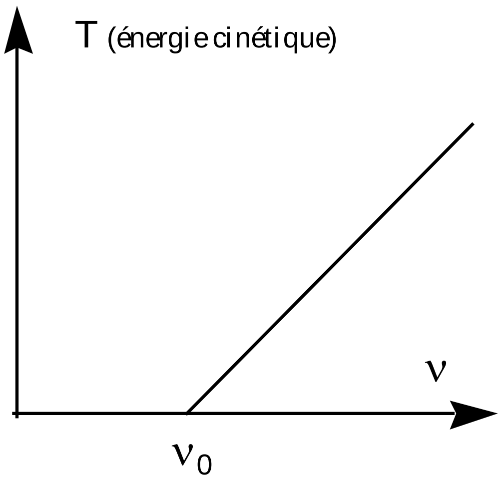
Electron Photoelectric Effect



Every individual photon interacts with the metal surface. This can only be effective if it has the necessary energy E_{min} to wrest the electron of the metal less strongly hold that *has quantified energy level, E_{min}*. The frequency threshold is therefore $\nu_0 = \frac{E_{min}}{h}$. You can not combine the energy from two photons to remove electrons: below $\nu >> \nu_0$ intensity is zero. If the radiation has a frequency $\nu >> \nu_0$, the kinetic energy of the electron ripped off is the excess energy: $E_{kin} = h\nu - E_{min}$. This energy is proportional to ν.

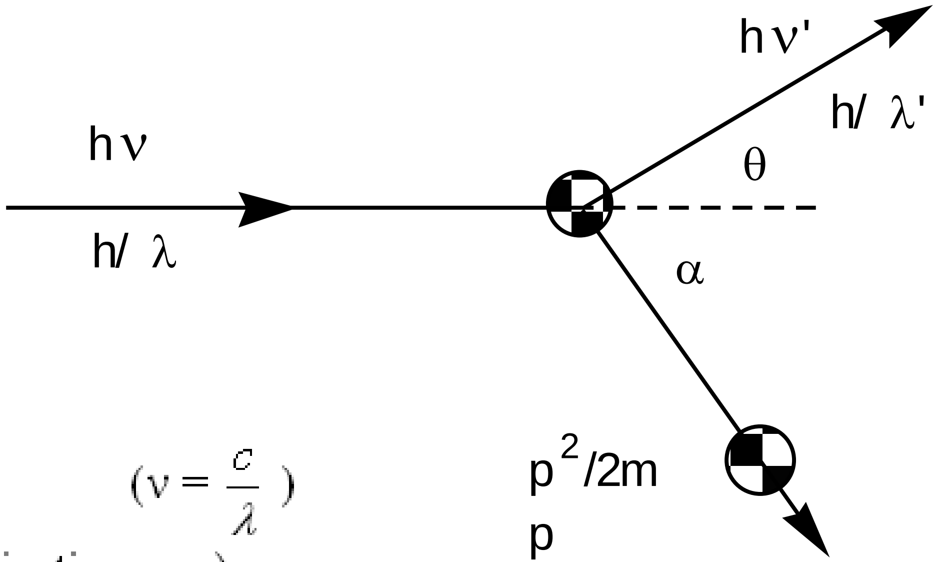
Electron Photoelectric Effect





Every individual photon interacts with the metal surface. This can only be effective if it has the necessary energy E_{min} to wrest the electron of the metal less strongly hold that *has quantified energy level, E_{min}*. The frequency threshold is therefore $\nu_0 = \frac{E_{min}}{h}$. You can not combine the energy from two photons to remove electrons: below $\nu >> \nu_0$ intensity is zero. If the radiation has a frequency $\nu >> \nu_0$, the kinetic energy of the electron ripped off is the excess energy: $E_{kin} = h\nu - E_{min}$. This energy is proportional to ν.

The Compton Effect (Electron Scattering)



Energy Conservation

$$h\frac{c}{\lambda} = h\frac{c}{\lambda'} + \frac{p^2}{2m} \qquad \left(\nu = \frac{c}{\lambda}\right)$$

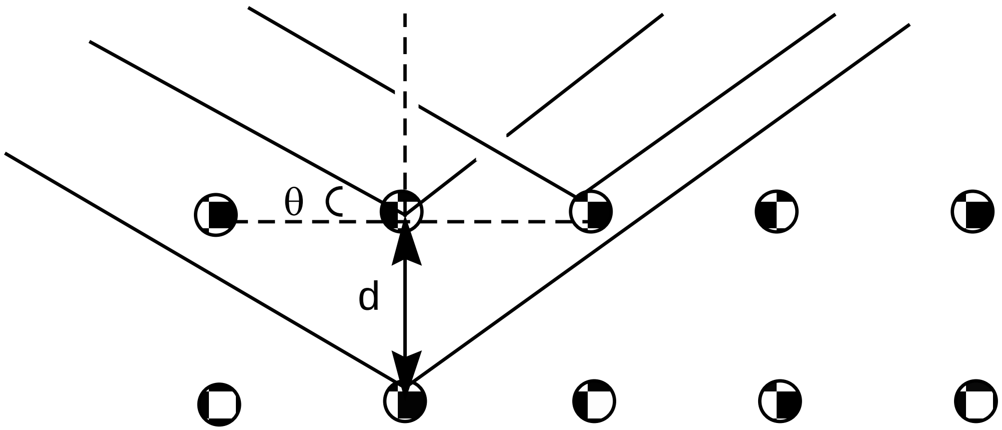
Momentum Conservation (projection on x)

$$\frac{h}{\lambda} = \frac{h}{\lambda'}\cos\theta + p\cos\alpha$$

Momentum Conservation (projection on y)

$$0 = \frac{h}{\lambda'}\sin\theta - p\sin\alpha$$

Davisson and Germer



$$2d \sin \theta = k \lambda$$

Diffraction is similarly observed using a mono-energetic electron beam

Bragg law is verified assuming λ=h/p

Wave-Particle Aspect of Reality

Wave-particle Equivalence.

- Compton Effect (1923).
- Electron Diffraction Davisson and Germer (1925)
- Young's Double Slit Experiment

Wave–particle duality

In physics and chemistry, **wave–particle duality** is the concept that all matter and energy exhibits both wave-like and particle-like properties. A central concept of quantum mechanics, duality, addresses the inadequacy of classical concepts like "particle" and "wave" in fully describing the behavior of small-scale objects. Various interpretations of quantum mechanics attempt to explain this apparent paradox.

Postulates of Quantum Mechanics

Postulate I: For any possible state of a system, there is a function ψ of the coordinates of the parts of the system and time that describes the system.

$$\Psi = \Psi(x, y, z, t)$$

Ψ Is called a **wave function**. For two particles system,

$$\Psi = \Psi(x_1, y_1, z_1, x_2, y_2, z_2, t)$$

The wave function square Ψ^2 is proportional to probability. Since Ψ may be complex, we are interested in $\Psi^*\Psi$, where Ψ^* is the complex conjugate (i → -i) of Ψ. The quantity $\Psi^*\Psi d\tau$ is proportional to the probability of finding the particles of the system in the volume element, dv = dxdydz.

$$\int_{all\_space} \Psi^* \Psi d\tau = 1$$

that is the probability of finding the particle in the universe is 1 ← normalization condition.

Postulate One: Continue

Orthogonal of two wave functions

$$\int \varphi^* \psi d\tau = 0$$

$$\int \psi^* \varphi d\tau = 0$$

Example: sinθ and cosθ are orthogonal functions.

$$\int_0^{\pi} \sin\theta \cos\theta d\theta = 0$$

Fourier series expansion – sin(nθ) and cos(nθ) orthogonal functions

Postulate One: Continue

- In 1924 de Broglie shown that a moving particle has a wave character. This idea was demonstrated in 1927 by Davisson and Gerner when an electron beam was diffracted by a nickel crystal.
- According to the de Broglie relationship, there is a wavelength associate with a moving particle which is given by

$$\lambda = \frac{h}{mv}$$

Postulate Two: Quantum Operators

With every physical observable q there is associated an operator Q, which when operating upon the wavefunction associated with a definite value of that observable will yield that value times the wavefunction Φ, i.e. $Q\Phi = q\Phi$.

$f(x)$	Any function of position, such as x, or potential V(x)	$f(x)$
p_x	x component of momentum (y and z same form)	$\frac{\hbar}{i}\frac{\partial}{\partial x}$
E	Hamiltonian (time independent)	$\frac{p_{op}^2}{2m} + V(x)$
E	Hamiltonian (time dependent)	$i\hbar\frac{\partial}{\partial t}$
KE	Kinetic energy	$\frac{-\hbar^2}{2m}\frac{\partial^2}{\partial x^2}$
L_z	z component of angular momentum	$-i\hbar\frac{\partial}{\partial \phi}$

Quantum Operators: Continue

(1) The operators are **linear**, which means that

$$O(\Psi_1 + \Psi_2) = O\Psi_1 + O\Psi_2$$

- **The linear character** of the operator is related to **the superposition of states and waves** reinforcing each other in the process

(2) The second property of **the operators is that they are Hermitian** (the 19th century French mathematician Charles Hermite).

- Hermitian matrix is defined as the transpose of the complex conjugate (*) of a matrix is equal to itself, i.e. $(M^*)^T = M$

$$M = \begin{pmatrix} a & x+iy \\ x-iy & c \end{pmatrix}$$

$$M^* = \begin{pmatrix} a & x-iy \\ x+iy & c \end{pmatrix}$$

$$(M^*)^T = \begin{pmatrix} a & x+iy \\ x-iy & c \end{pmatrix} = M$$

In QM, the operator *O* is Hermitian if

$$\int \Phi^* O \Psi d\tau = \int \Psi O^* \Phi^* d\tau$$

Postulate Three: Eigenvalues

- The permissible values that a dynamical variable may have are those given by $O\Phi = a\Phi$, where Φ is the eigenfunction of the QM operator (Hermitian) O that corresponds to the observable whose permissible real values are a.
- The is postulate can be stated in the form of an equation as

$$O \quad \Phi \quad = \quad a \quad \Phi$$

operator wave function eignevalue wave function

Eigenvalues: Continue

- Eigenvalues of QM operator must be real !
- Example

$$M = \begin{pmatrix} a & b+ic \\ b-ic & d \end{pmatrix}$$

$$solve \rightarrow Mx = \lambda x$$

$$\Rightarrow (a-\lambda)(d-\lambda)-(b+ic)(b-ic)=0$$

$$\Leftrightarrow \lambda^2 - (a+d)\lambda + ad - b^2 - c^2 = 0$$

The two values for λ are real

Postulate Four: The wave Equation

Postulate IV

- **The state function Ψ is given as a solution of**

$$\hat{H}\Psi = E\Psi \longleftarrow \text{Schrodinger equation}$$

where $\hat{H}$ is the total energy operator, that is the Hamiltonian operator.

- The hamiltonian function is the total energy, T+V, where T is the kinetic energy and V is the potential energy. In operator form

$$\hat{H} = \hat{T} + \hat{V}$$

where $\hat{T}$ is the operator for kinetic energy and $\hat{V}$ is the operator for potential energy. In differential operator form, the time dependent Schrodinger equation is

$$-\frac{h^2}{8m\pi^2}\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} + V(q_i, t)\right)\Psi(q_i, t) = -\frac{h}{2\pi i}\frac{\partial}{\partial t}\Psi(q_i, t)$$

Classical Data Representation

- The basic unit in classical data is a binary digit, called a bit, that can take on the value 0 or 1.
- In classical computing, we represent a datum by a string of bits.
- The letter ‘A’ may be written 0100 0001
- The number 137 can be written   1000 1001

Classical Operations

- All operations in classical computing are based on logic gates.
- For example, the logical AND gate takes in two bits and returns 1 if and only if both inputs are 1.

AND		
Input 1	Input B	Output
0	0	0
0	1	0
1	0	0
1	1	1

OR		
Input 1	Input B	Output
0	0	0
0	1	1
1	0	1
1	1	1

Classical Algorithm

- We define a Classical Algorithm to be any sequence of such classical operations (usually to do something useful).
- A classical computer is any device that can implement a classical algorithm.

Introduction to Logical Gates

- The building blocks used to create digital circuits are **logic gates**
- There are three elementary logic gates and a range of other simple gates
- Each gate has its own **logic symbol** which allows complex functions to be represented by a logic diagram
- The function of each gate can be represented by a **truth table** or using **Boolean notation**

Classical Logic Gates (One)

The AND gate

(a) Circuit symbol

A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

(b) Truth table

$$C = A \cdot B$$

(c) Boolean expression

The OR gate

(a) Circuit symbol

A	B	C
0	0	0
0	1	1
1	0	1
1	1	1

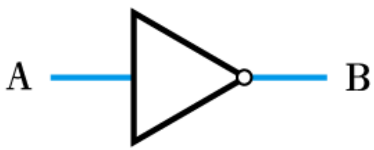
(b) Truth table

$$C = A + B$$

(c) Boolean expression

Classic Logic Gates (Two)

The NOT gate



(a) Circuit symbol

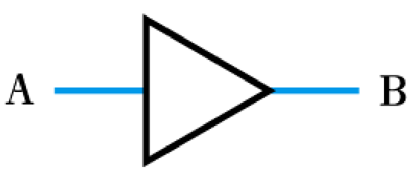
A	B
0	1
1	0

(b) Truth table

$$B = \overline{A}$$

(c) Boolean expression

The Logic Buffer Gate



(a) Circuit symbol

A	B
0	0
1	1

(b) Truth table

$$B = A$$

(c) Boolean expression

Classic Logic Gates (Three)

The NAND gate

(a) Circuit symbol

A	B	C
0	0	1
0	1	1
1	0	1
1	1	0

(b) Truth table

$$C = \overline{A \cdot B}$$

(c) Boolean expression

The NOR gate

(a) Circuit symbol

A	B	C
0	0	1
0	1	0
1	0	0
1	1	0

(b) Truth table

$$C = \overline{A + B}$$

(c) Boolean expression

Classic Logic Gates (Four)

The EXCLUSIVE OR gate

(a) Circuit symbol

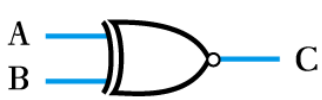
A	B	C
0	0	0
0	1	1
1	0	1
1	1	0

(b) Truth table

$$C = A \oplus B$$

(c) Boolean expression

The EXCLUSIVE OR gate



(a) Circuit symbol

A	B	C
0	0	1
0	1	0
1	0	0
1	1	1

(b) Truth table

$$C = \overline{A \oplus B}$$

(c) Boolean expression

Boolean Algebraic Rules

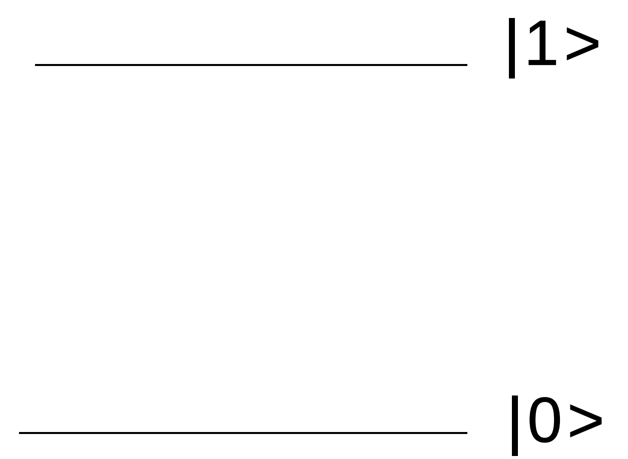
Commutative law $AB = BA$ $A + B = B + A$	**Absorption law** $A + AB = A$ $A(A + B) = A$
Distributive law $A(B + C) = AB + BC$ $A + BC = (A + B)(A + C)$	**De Morgan's law** $\overline{A + B} = \overline{A} \bullet \overline{B}$ $\overline{A \bullet B} = \overline{A} + \overline{B}$
Associative law $A(BC) = (AB)C$ $A + (B + C) = (A + B) + C$	**Note also** $A + \overline{A}B = A + B$ $A(\overline{A} + B) = AB$

Introduction to Quantum Bits

- In quantum computing, a **qubit** or **quantum bit** is a basic unit of quantum information—the quantum version of the classic binary bit physically realized with a two-state device.
- A qubit is a two-state quantum-mechanical system, one of the simplest quantum systems displaying the peculiarity of quantum mechanics.
- In a classical system, a bit would have to be in one state or the other. However, quantum mechanics allows the qubit to be in a coherent superposition of both states simultaneously, a property that is fundamental to quantum mechanics.

Qubits

- A Quantum Bit (Qubit) is a two-level quantum system.
- We can label the states |0> and |1>.
- In principle, this could be any two-level system.



Qubits

- Unlike a classical bit, which is definitely in either state, the state of a Qubit is in general a mix of |0> and |1>.

$$\left|\psi\right\rangle = c_0\left|0\right\rangle + c_1\left|1\right\rangle$$

- We assume a normalized state:

$$\left|c_0\right|^2 + \left|c_1\right|^2 = 1$$

Qubits

- For convenience, we will use the matrix representation

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Quantum Gate

- A Quantum Logic Gate is an operation that we perform on one or more Qubits that yields another set of Qubits.
- We can represent them as linear operators in the Hilbert space of the system.

Quantum NOT Gate

- As in classical computing, the NOT gate returns a 0 if the input is 1 and a 1 if the input is 0.
- The matrix representation is

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Other Quantum Gates

- Other gates include the Hadamard-Walsh matrix:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- And Phase Flip operation:

$$\begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\varphi} \end{pmatrix}$$

Multiple Qubits

- Any useful classical computer has more than one bit. Likewise, a Quantum Computer will consist of multiple qubits.
- A system of n Qubits is called a Quantum Register of length n.
- To represent that Qubit 1 has value b_1, Qubit 2 has value b_2, etc., we will use the notation:

$$\left|b_1\right\rangle_1 \left|b_2\right\rangle_2 \cdots \left|b_n\right\rangle_n$$

Multiple Qubits

- For *n* Qubits, the vector representing the state is a *2n* column vector.
- The operations are then *2n* x *2n* matrices.
- For *n* = 2, we use the representations

$$|0\rangle_1|0\rangle_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |0\rangle_1|1\rangle_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |1\rangle_1|0\rangle_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |1\rangle_1|1\rangle_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Quantum CNOT Gate

- An important Quantum Gate for n = 2 is the conditional not gate.
- The conditional not gate flips the second bit if and only if the first bit is on.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Input		**Output**	
Qubit 1	Qubit 2	Qubit 1	Qubit 2
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Reversibility and No-Cloning

- In Quantum Computing, we use unitary operations ($U^* U = 1$).
- This ensures that all of the operations that we perform are reversible.
- This fact is important, because there is no way to perfectly copy a state in Quantum Computing (No-Cloning Theorem).

No-Cloning Theorem

- That is, the No-Cloning Theorem says that there is no linear operation that copy an arbitrary state to one of the basis states:

$$|\psi\rangle|e_i\rangle \rightarrow |\psi\rangle|\psi\rangle$$

- We can get around this if we are only interested in copying basis vectors, though.

Entanglement

- In Quantum Mechanics, it sometimes occurs that a measurement of one particle will effect the state of another particle, even though classically there is no direct interaction. (This is a controversial interpretation).
- When this happens, the state of the two particles is said to be entangled.

Entanglement: Formalism

- More formally, a two-particle state is entangled if it cannot be written as a product of two one-particle states.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right)$$

- If a state is not entangled, it is decomposable.

$$|\psi\rangle = \frac{1}{2}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|0\rangle_2 + |0\rangle_1|1\rangle_2 + |1\rangle_1|1\rangle_2\right)$$
$$= \frac{1}{\sqrt{2}}\left(|0\rangle_1 + |1\rangle_1\right)\frac{1}{\sqrt{2}}\left(|0\rangle_2 + |1\rangle_2\right)$$

Entanglement: Example

- The state of two spinors is prepared such that the z-component of the spin is zero.
- If we measure $m = +1/2$ for one particle, then the other particle must have $m = -1/2$.
- The measurement performed on one particle resulted in the collapse of the wavefunction of the other particle.

Why Quantum Computing?

- One of the most important problems in modern hardware design is the limiting factor of the interspatial distances in the Silicon wafers. Quantum computers offer us the theoretical limit of atomic scale.
- One of the most important network problems is the ability to encrypt documents to increase the security of the network. Quantum encryption techniques offer us a theoretical encryption methodology which is beyond computational feasibility.

Definitions

- A Quantum Algorithm is any algorithm that requires Quantum Mechanics to implement.
- A Quantum Computer is any device that can implement a Quantum Algorithm.

Universal Gate Sets

- It would be convenient if there was a small set of operations from which all other operations could be produced.
- That is, a set of operators $\{U_1,\ldots,U_n\}$ such that any other operator W could be written $W = U_i U_j \ldots U_k$.
- Such a set of operators in the context of computation is called a universal gate set.

Classical NAND Gate

- One universal set for Classical Computation consists of only the NAND gate which returns 0 only if the two inputs are 1.

NAND		
Input 1	Input B	Output
0	0	1
0	1	1
1	0	1
1	1	0

$$NOT(P) = NAND(P,P)$$

$$AND(P,Q) = NAND(NAND(P,Q), NAND(P,Q))$$

$$OR(P,Q) = NAND(NAND(P,P), NAND(Q,Q))$$

Quantum Universal Gate Set

- There are a few universal sets in Quantum Computing.
- Two convenient sets:
  - CNOT and single Qubit Gates
  - CNOT, Hadamard-Walsh, and Phase Flips
- Having such a set could greatly simplify implementation and design of Quantum Algorithms.

Physical Implementation

- Any physical implementation of a quantum computer must have the following properties to be practical(DiVincenzo)
  - The number of Qubits can be increased
  - Qubits can be arbitrarily initialized
  - A Universal Gate Set must exist
  - Qubits can be easily read
  - Decoherence time is relatively small

Decoherence

- As the number of Qubits increases, the influence of external environment perturbs the system.
- This causes the states in the computer to change in a way that is completely unintended and is unpredictable, rendering the computer useless.
- This is called decoherence.

Shor's Algorithm

- A Quantum Algorithm, due to P. W. Shor (1994) allows for very fast factoring of numbers.
- The algorithm uses other algorithms: the Quantum Fourier Transform, and Euclid's Algorithm.
- It also relies on elements of group theory.
- Because of the unpredictability of Quantum Mechanics, it only gives the correct answer to within a certain probability.
- Multiple runs can be performed to increase the probability that the answer is correct. This increases the complexity to $n^3 \log_2(n)$