

MAT 3420 : Quantum Computing

Goal of this course.

- understand fundamental frameworks / paradigm behind quantum computation :
quantum mechanics, complex linear algebra, probability
- know some important "quantum" algorithms :
prime factorization, Grover's algorithm, --
- some "quantitative" analysis
information capacity (entropy), error correction
universality of quantum gates ...

Main reference :

Scott Aaronson "Introduction to Quantum Information Science"

Crash course on quantum mechanics

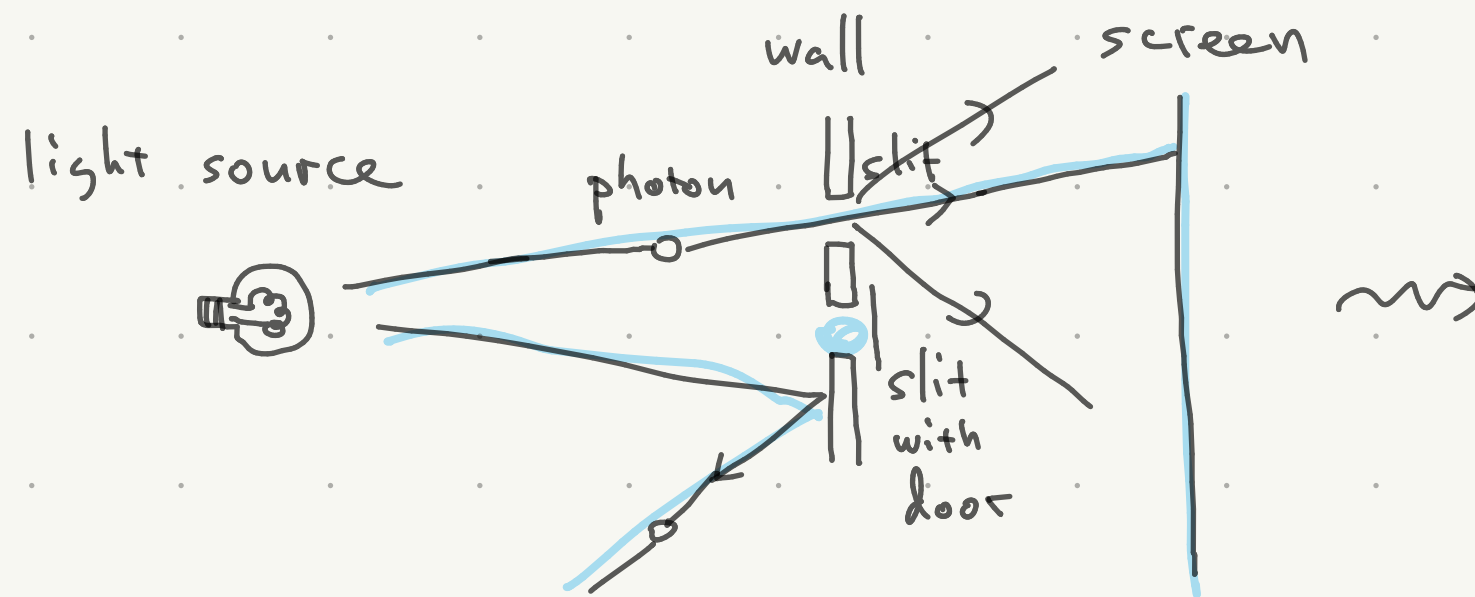
(Lecture 2 in main ref.)

Quantum mechanics is about :

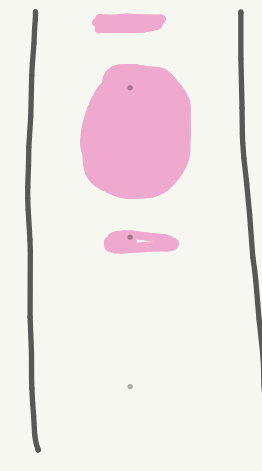
- physical phenomena at small scale (distance, energy, ...)

⇒ we need complex vector-valued functions) and probability to explain these (even to understand single particles)

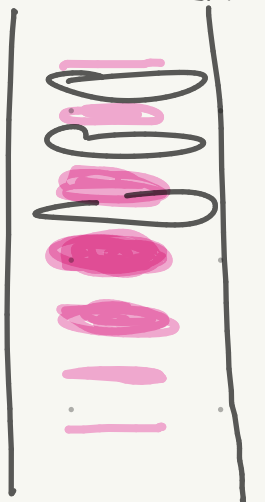
Example : double slit experiment



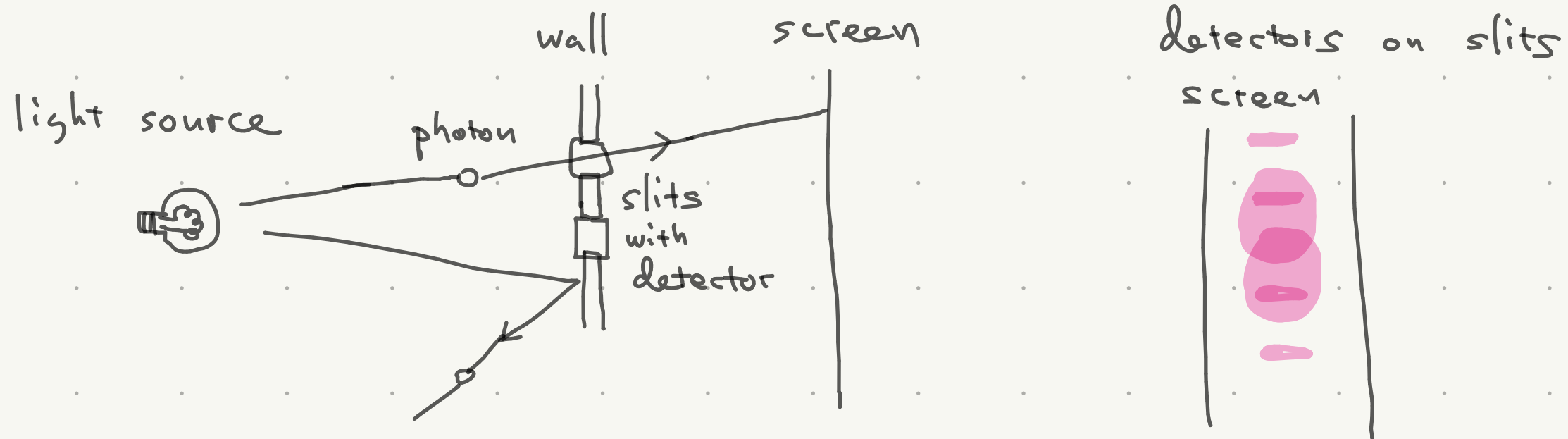
door closed
screen



door open
screen



-- but if we also measure which slit the photon went through



to explain these, we need these paradigms:

- States of particles are described by

"wave functions" $\phi(x, y, \dots)$ complex valued functions.

- probability of finding particle around $x_0, y_0, \dots \sim |\phi(x_0, y_0, \dots)|^2$

- "superposition" of two states $\phi_1 + \phi_2$ Born rule

- measurement of the particle will change its state

another important paradigm:

- at small scale, energy level is discretized

(but we won't use this much)

→ to explain the double slit experiment

pick a region in the screen

$\alpha_1 \in \mathbb{C}$: the amplitude of photon hitting that region
when only one slot open
(slot 1)

$\alpha_2 \in \mathbb{C}$: the amplitude of photon hitting that region
when only one slot open
(slot 2)

→ $(|\alpha_1|^2, |\alpha_2|^2) \geq 0$ probability of photon hitting that
region

two slits open → amplitude $\alpha_1 + \alpha_2$, prob. $|\alpha_1 + \alpha_2|^2$

Transformation of system as matrices

(section 2.1 in main ref.)

think of a system with two possibilities

ex. a coin on a table: "heads up" or "tails up"

the system can be in various different states:

- in each state, we have probability distribution

$$P(\text{heads}) = p, \quad P(\text{tails}) = q \quad (p, q \geq 0; p + q = 1)$$

- transforming the state will change p, q

→ model a state by vector $\begin{bmatrix} p \\ q \end{bmatrix}$

a transform by matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Example "turn the coin over"

change the state from $\begin{bmatrix} p \\ q \end{bmatrix}$ to $\begin{bmatrix} q \\ p \end{bmatrix}$

$$M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad M \begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} q \\ p \end{bmatrix}$$

Example "flip the coin fairly"

change the state from $\begin{bmatrix} p \\ q \end{bmatrix}$ to $\begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix}$

$$M = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}; \quad M \begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \quad \text{by } p + q = 1$$

Consider the conditional probability

$P[a|b]$ = probability of getting "a" given "b"

$P(a|b)$

→ transformation matrix is

$$M = \begin{bmatrix} P[\text{heads} | \text{heads}] & P[\text{heads} | \text{tails}] \\ P[\text{tails} | \text{heads}] & P[\text{tails} | \text{tails}] \end{bmatrix}$$

ex. turning over $P[h|t] = 1$, $P[h|h] = 0$, --

fair flip $P[h|h] = \frac{1}{2}$, $P[h|t] = \frac{1}{2}$, ---

More complicated ex.

$$M = \begin{bmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & 0 \end{bmatrix}$$

if the coin is heads up, do a fair flip
if it is tails up, flip it over

Which matrices do we get as M ?

$$M = \begin{bmatrix} P[\text{heads} | \text{heads}] & P[\text{heads} | \text{tails}] \\ P[\text{tails} | \text{heads}] & P[\text{tails} | \text{tails}] \end{bmatrix}$$

- each entry is a nonnegative number ≤ 1
- sum of each column is 1

$\leadsto$ these are called stochastic matrices

these preserve probability distributions

$$\begin{bmatrix} a \\ b \end{bmatrix} \quad a, b \geq 0, \quad a + b = 1$$

M stoch. mat.

$$\Rightarrow M \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a' \\ b' \end{bmatrix} \quad a', b' \geq 0 \quad a' + b' = 1$$

Combining systems

for simplicity, use "bits" instead of coins

so possibilities are "0" or "1"

and look at a system of two bits

the state of "bit 1" is represented by

$$\begin{bmatrix} a \\ b \end{bmatrix}$$

$$a, b \geq 0, a + b = 1$$

the state of "bit 2" is represented by

$$\begin{bmatrix} c \\ d \end{bmatrix}$$

the entire system is represented by $c, d \geq 0, c + d = 1$

$$\left[\begin{array}{l} P[\text{bit 1} = 0, \text{bit 2} = 0] = ac \\ P[\text{bit 1} = 0, \text{bit 2} = 1] = ad \\ P[\text{bit 1} = 1, \text{bit 2} = 0] = bc \\ P[\text{bit 1} = 1, \text{bit 2} = 1] = bd \end{array} \right] \left. \begin{array}{l} \text{sum} = 1 \\ \text{nonnegative numbers} \end{array} \right\}$$

tensor product (Kronecker product)

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$$

models this combination

Kronecker product of matrices

$[x_{i,j}]_{i,j}$

$[y_{k,e}]_{k,e}$

$$\begin{bmatrix} \begin{array}{ccc} x_{1,1} & y_{1,1} & x_{1,1} y_{1,2} \dots \\ x_{1,1} & y_{2,1} & \dots \\ \vdots & & \end{array} & \begin{array}{ccc} x_{1,2} & y_{1,1} & \dots \\ x_{1,2} & y_{2,1} & \dots \\ \vdots & & \end{array} \\ \hline \begin{array}{ccc} x_{2,1} & y_{1,1} & x_{2,1} y_{1,2} \dots \\ x_{2,1} & y_{2,1} & \dots \\ \vdots & & \end{array} & \begin{array}{ccc} \vdots & & \end{array} \end{bmatrix}$$

manipulating tensor product

$$\left(\begin{array}{l} \underbrace{\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix}} + \underbrace{\begin{bmatrix} a' \\ b' \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix}} = \begin{bmatrix} a+a' \\ b+b' \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} \\ \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} + \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c' \\ d' \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c+c' \\ d+d' \end{bmatrix} \end{array} \right)$$

distributivity

$$(X+Y)Z = XZ + YZ, \dots$$

but

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} \neq \begin{bmatrix} c \\ d \end{bmatrix} \otimes \begin{bmatrix} a \\ b \end{bmatrix}$$

no commutativity

$$XY \neq YX$$

Transformation of this system: 4×4 stochastic matrix

Example: CNOT (controlled NOT)

if bit 1 is 0, do nothing

if bit 1 is 1, flip bit 2

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

transform the state

$$\begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{bmatrix} \quad \text{by CNOT:}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ 0 \\ 0 \\ \frac{1}{2} \end{bmatrix}$$

this is not of the form

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix}$$

distributions of the form $\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} : \underline{\text{uncorrelated}}$ distr.

~ not of the form $\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} : \underline{\text{correlated}}$ distr.

Matrix model of quantum mechanics: