cs467

Austin Xia

April 20, 2021

Contents

List of Figures

List of Tables

1 Course Information

instructor: Ashwin Nayak
Grade: 60% Assignments+15%midterm+20%final

2 April 20, 2021

2.1 quantum phenomena

Experiment:
path 0 denoted by $e_0 := (1,0) \in C^2$
path 1 denoted by $e_1 := (0,1) \in C^2$
a:=b means a is defined to be b
initial state of photon e_0, denoted $| \ 0 >$(a classcial bit being 0)
beam splitter is a linear transform

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

hadamard transformation
after hitting the beam splitter,

$$state = H|0 >= \frac{1}{\sqrt{2}}(1,1)$$

this is called a superposition of state 0 and 1. quantum is simutanously in this state

state on passing through 2nd beam splitter

$$state = H\frac{1}{\sqrt{2}}(1,1) = (1,0) = |0 >$$

1,0 here are probability amplitude probablity of state $|0 >$ being observed $= |its \ amplitude|^2$

2.2 qubit, quantum state, measurement

qubit $\equiv$ quantum bit $\equiv$ register
it is a unit of quantum computation
a register can be consistered as 1 qubit or a collection of qubit
state of a qubit $\equiv$ described by a unit vector in C^2 (Hilbert space)
measurement $\equiv$ experiment
experiment to probing what state the qubit is in, in the simplest case it is a *complete projective measurement* specified by an orthonormal basis $B := \{|u_0 >, |u_1 >\}$
example:

- standard basis $\{|0 >, |1 >\}$, read as capt zero
- Hadamard $\{|+ >, |- >\}$
- $\frac{1}{\sqrt{2}}(|0 > +i|1 >), \frac{1}{\sqrt{2}}(|0 > -i|1 >)$

Definition 2.2.1
"bra" v $\equiv$ dual of vector v $\equiv$ conjugate transpose of v

> **Example 2.2.1**
> question: in lecture you write $< 0| = (1, 0)$, shouldn't it be $bra(|0 >) = (1, 0)$
> $< 0| = (1, 0)$
> $< +| = \frac{1}{\sqrt{2}}(1, 1)$
> $< v_0| = \frac{1}{\sqrt{2}}(1, -i)$

the inner product between two vectors $|u >, |v >\in C$
is denoted as $< u|v >:=< u| * |v >$

> **Example 2.2.2**
> $< 0|+ >= \frac{1}{\sqrt{2}}$
> $< +|v_0 >= (1 + i)/2$, abs value is $\frac{1}{\sqrt{2}}$

Effect of a measurement in $B := \{|u_0 >, |u_1 >\}$ on a qubit in state $|v >$:

- we observe outcome "0" or "1"
- see outcome $b \in \{0, 1\}$, with prob $| < u_b|v > |^2$
- when outcome b is observed, state become $|u_0 >$, the state collapses to $|u_0 >$

> **Example 2.2.3**
> Measure $|+ >$ in basis
>
> - $B := \{|0 >, |1 >\}$ outcomes 0/1, when outcome =b, state = $|b >$
> - $B := \{|v_0 >, |v_1 >\}$, outcome 0 with prob $| < v_0|+ > |^2 = (\frac{1}{\sqrt{2}})^2 = 1/2$ final state = $|v_b >$ when outcome = b

general case is *complete von neumann measurement*

2.3 bit commitment

simple, single mesg. protocol
commit stage:

- Alice has a bit $a \in \{0, 1\}$. She sends a message m (depending on a) to Bob
- Bob receives m stores it

Reveal phase:

- Alice sends bit a, msg r to Bob
- Bob use r to check that m is consistent with a, if so accept

Requirements:

- Hiding property: Bob cannot learn bit 'a' from message m
- Binding property: Alice cannot send bit $\bar{a}$, and some message r s.t. Bob accept

Classically, Bob can learn bit a from m or Alice can cheat
Quantumly, we can have a protocal that solve this
Quantum Protocal

- Alice has a state $a \in \{0,1\}$ Perpares a qubit M in state $|\phi_a >$
- She sends M to Bob. who stores this qubit, this complete the commitment stage

$\theta := \pi/8$
$|\psi_0 > := \alpha|0 > + \beta|1 >$
$\alpha := cos(\pi/8), \beta = sin(\pi/8)$
$|\psi_1 > := \beta|0 > + \alpha|1 >$
Reveal Stage

- Alice send bit a, and no other msg r
- Bob measures qubit M in basis $\{|\psi_a >, |\tilde{\psi_a} >\}$
  He accepts (a) if cutcome = 0, reject o.w.

Proposition: this protocal satisfies the hiding and binding properties in a probablitistic sense:
(a) Given the qubit M, regardless of which measurement Bob makes, P(outcome=a)$\leq \delta$ for some $\delta < 1$
(b) For any state in which Alice prepares M, if she wishes to claim bit b in the reveal stage, P(Bob accepts b)$\leq \delta$ for some $\delta < 1$
Hiding property:
we can show that the optimal measurement $\{|u_0 >, |u_1 >\}$ s.t. Pr(outcome=a — $|\psi_a >$) is maximized is given by $|u_0 > := |0 >, |u_1 > := |1 >$
Concealing property
claim: $|\psi >$ is state that maximizes the

$$min_{a \in \{0,1\}} | < \psi_a | \psi > |^2$$

2.4 multiple qubit

general quantum state is a unit vector in $\mathbf{C}^d$, $d := 2^n$ spanned by $|x\rangle(e_x)$ $|\psi\rangle := \sum_x \alpha_x |x\rangle$ unit vector means $\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$
suppose $|u\rangle \in C^{d_1}$, $|v\rangle \in C^{d2}$ the tensor product $|u\rangle \otimes |v\rangle$ is vector in C^{d1*d2}
suppose we have indexed unit vectors $\{e_i\}, \{f_j\}$ are std basic vectors for C^{d1}, C^{d2}

$$g_{i,j} := (0, 0, 0...1, 0, 0, 0...) \text{ i is the } (i-1)d_1 + j$$

suppose $|u\rangle = \sum u_i e_i \in C^{d1}$ $|v\rangle = \sum v_i f_i \in C^{d2}$

$$|u\rangle \otimes |v\rangle = \sum_{ij} u_i v_j g_{ij}$$

in dirac notation, it is

$$\sum_{ij} u_i v_j |i, j\rangle$$

note $|u\rangle|v\rangle = |u, v\rangle = |uv\rangle$
tensor product is bilinear

$$|\psi_1\rangle$$

$$C^{d1d2} \neq \{|u\rangle \otimes |v\rangle : |u\rangle \in C^d |v\rangle \in C^{d2}\}$$

however

$$C^{d1d2} = span\{|u\rangle \otimes |v\rangle : |u\rangle \in C^d |v\rangle \in C^{d2}\}$$

this span is $C^{d1} \otimes C^{d2}$
product state if can be written as $|a\rangle|b\rangle$
entangled state if cannot

2.4.1 properties of tensor products of operator

- $(\alpha U) \otimes V = \alpha(U \otimes V) = U \otimes (\alpha V)$
- $(U_1 + U_2) \otimes V = U_1 \otimes V + U_2 \otimes V$
- $U \otimes (V_1 + V_2 = U \otimes V_1 + U \otimes V_2)$
- $(U_1 \otimes V_1)(U_2 \otimes V_2) = (U_1 U_2) \otimes (V_1 V_2)$
- $(U \otimes V)^* = U^* \otimes V^*$
- $(U \otimes V)^{-1} = U^{-1} \otimes V^{-1}$
- $\|U \otimes V\| = \|U\| * \|V\|$

2.4.2 inner product

suppose $|u_1 v_1\rangle, |u_2 v_2\rangle \in C^{d1} \otimes C^{d2}$ their inner product=

$$(\langle u_1 v_1|)(|u_2 v_2\rangle) = \langle U_1 u_2\rangle\langle v_1 v_2\rangle$$

suppose $w, w_1, w_2 \in C^{d1} \otimes C^{d2}$

$$E_{ij} = e_i e_j^T = e_i e_j^* = |i\rangle\langle j| U \sum \alpha_{ij} |i\rangle\langle j|$$

2.5 measurement

measurement of multiple qubits
A sequence of qubit (registe) M in state $|\psi\rangle \in C^d$
A complete projective measurement of M is specified by an orthonormal basis

$$B = \{|u_i\rangle : i \in [d]\}$$

2.5.1 transmission of polorized light

photon pass through poloarizing film, with a detector on the other side,

- a photon is either absorbed or passes through
- only $|\rightarrow\rangle$ component pass through
- if state is $\alpha|\rightarrow\rangle + \beta|\uparrow\rangle$ we observe the photon at D with probability $|\alpha|^2$
- if we place a second film fim also oriented horizentally, all light is transmitted

coarser measurment: projective measurement
specified by a sequence of orthogonal projection operation $\{P_i : i \in [k], \sum_{i=1}^{k} = I\}$
On measurement of M in state $|\psi\rangle \in C^d$

- we observe a probablitistic coutcome $i \in [k]$
- $p(outcome = i|...) = \|P_i|\psi\rangle\|^2$
- on outcome i, state of M becomes
$$\frac{P_i|\psi\rangle}{\|P_i|\psi\rangle\|}$$

2.5.2 general measurement in an 0-n basis

$B := \{|u_i\rangle\}$
$P_i := |u_i\rangle\langle u_i|$
P_i is orthogonal proj
the effect of measuring $|\varphi\rangle$ in B or in $\{P_i\}$ is the same

> **Example 2.5.1**
> we want to check if 2 bit of a 2-qubit state is the same
> we apply projection
> $$p_0 = |00\rangle\langle 00| + |11\rangle\langle 11|$$
> $$p_1 = |01\rangle\langle 10| + |10\rangle\langle 01|$$
> when we measure $|+-\rangle$ we have
> $$pob = \|p_0 \,|+-\rangle\|^2 = \||00\rangle\langle 00| \,|+-\rangle + |11\rangle\langle 11| \,|+-\rangle\| = |\langle 00|+-\rangle|^2 + |\langle 11|+-\rangle|^2 = 1/2$$
> state becomes $\frac{p_0|+-\rangle}{1/\sqrt{2}} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

2.5.3 measuring subsystem

we've got register AB, both have several bits, with state space $C^{d1} \otimes C^{d2}$ say state of AB is $|\psi\rangle$ we wish to measure register A with projective measurement
measurement $\{P_i : i \in [k]\}$ This is equivalent to measuring AB according to
$$\{P_i \otimes 1 : i \in [k]\}$$
we can express $|\psi\rangle$ as $|\psi\rangle = \sum_{i=1}^{d_1} \alpha_i \,|u_i\psi_i\rangle$ where $|\psi_i\rangle \in \mathbb{C}^{d_2}, \||\psi_i\rangle\| = 1$, but $\{|\psi_i\rangle\}$ need not be orthogonal
question:how
remark on measurement:
$$|\psi\rangle = \sum_{i=1}^{d} p_i \,|\psi\rangle$$
$$1 = \||\psi\rangle\|^2 = \sum_{i=1}^{d} \|p_i \,|\psi\rangle\|^2$$

2.5.4 general measurement

we will call it a measurement
A general measurement of a resgister M consist of:

prepare another register M' in a fixed state, $|\bar{0}\rangle$
measure MM' with a projective measurement on $C^{d1} \otimes C^{d2}$ where M has state space in C^{d1}, M' in C^{d2}
information content of n qubit:
n-qubit state $|\psi\rangle := \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$
discription: 2^n parameters
However, we may only reliably encode $\theta(n)$ bits into n qubits

Theorem 2.5.2
let $x \in \{0,1\}^m$ be uniformly random. suppose we encode $x \in \{0,1\}^m$ by n-qubit state $|\psi_x\rangle$ Let Y be outcome of any measurement of the state ψ_x
Let y be outcome of any measurement of state $|\psi_x\rangle$ then

$$pr(Y = X) \leq 2^n/2^m$$

Proof
suppose we measure state according to $\{P_y : y \in \{0,1\}^m\}$,where outcome y indicates our guess for the encoded string.
Given state $|\psi_x\rangle$ we append $|\bar{0}\rangle \in \mathbb{C}^{d1}$ and measure according to proj measurement
Note $\sum P_y = 1$ then $\exists$ basis $\{|f_{yi}\rangle\}$ o.n.

$$P_y = \sum_i |f_{yi}\rangle\langle f_{yi}|$$

$pr(y = x) = \frac{1}{2^m} \sum_x Pr(y = x| \, |\psi_x\rangle)$

evolution of quantum bit

- linear
- reversible/invertible
- norm preserving

computation with qubit may be implemented by allowing system to involve or for subsets of qubit to evolve while maintaining the state of the rest.
if subregister A of register AB evolves according to operator U, evolution of AB is given by $U \otimes 1$ Note $U \otimes 1$ unitary $\leftrightarrow$ U unitary
a sophiscated computation may involve sequence of such unitary operators applied to different subregisters
all operations allowed by laws of quantum physics can be expressed as a composition of

- addition of ancilla
- unitary evolution of the entire system
- a projective measurement

2.6 superdense coding

if A and B hold E_1, E_2 respectively, where join state is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
suppose alice has 2 bits. she can apply unitary $U_{ab} = X^a Z^b$ to them
question can we create entangled state
question cheat by entangled

2.7 teleportation

A B connected by classical channel, can send classical bit
A given qubit M in state $\alpha |0\rangle + \beta |1\rangle$ She would help B construct $|\psi\rangle$

Theorem 2.7.1
there is a protocal if Alice and Bob share E_1, E_2
two qbit in state $|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
the protocal:
alice has M E_1, Bob has E_2.
M in $\alpha |0\rangle + \beta |1\rangle$ Bob has $E_2, E_1 E_2$ in state $|\psi_{00}\rangle$
Alice measures qubits ME_1 in Bell basis $\{|\psi_{ab}\rangle\}$ she sends the 2bit outcome to Bob
Bob recieves $ab \in \{0, 1\}$ and applies U_{ab} on E_2
$U_{ab} = X^a Z^b$
where xz are the standard pauli operation
claim: the final satate of E_2 is $|\psi\rangle$

An algorithm/program/cuicuit:
$f\{0,1\}^n \to \{0,1\}^m$

- number of bits in the memory *size*, holding input and workspace
- a string of s bits, to which memory is initialized. the first n to $\{0,1\}^n$ the rest 0
- a sequence of logic gate from a fixed set G
- the index of register that represent the output

3 circuit

time: number of gates
space: number of wire segment

correctness of a random circuit:
let $f : \{0,1\}^n \to \{0,1\}^m$. we say C computes f is $Pr(C(x) = f(x)) \geq 2/3$ for all inputs x

3.1 quantum circuit

- memory consist of qubits
- quantum gates, performing unitary operation
- measurement

it is useful to write quantum gate as CNOT=$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$
we can prepare bell state $|\phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ by:

$$|\phi_{00}\rangle = CNOT^{E_2 E_1}(1 \otimes H) |00\rangle^{E_1 E_2}$$

Note: we use register on which oeprator act AND the register which are in that state
$Z = HXH \quad Y = iXZ \quad HYH = i(HXH)(HZH) = iZX = -Y$

measurement:
we can perform a basis change to unitary, mesaure in unitary, than change it back.

3.2 universality

quantum physics, any unitary operator can occur,
can circuit do it?
we say circuit computes U on n qubits C^{2^n}, if for every state $|\Psi\rangle \in C^d$, final state is $U|\Psi\rangle|0\rangle$ with probability 1

Theorem 3.2.1
for any unitary operation U, there is a quantum circuit that uses only CNOT and single qubit gate and compute U

but how single qubit gate? how irrational number?
can we use small number of gate? can we have not precise gate?

Definition 3.2.1
V approximate U if $\|U - V\| \le \epsilon$
this suffice as $\|V|\phi\rangle - U|\phi\rangle\| \le \|V - U\|$
when output is close, the measurement statistics also close, closeness of probability is measured in l1 distance

$$\|p - q\|_1 := \sum_{k}^{i=1} |p_i - q_i|$$

proposition: when $\||\psi\rangle - |\phi\rangle\| \le \epsilon$

$$\|p - q\|_1 \le 2\epsilon$$

proof:
suppose we measure according to $\{P_i : i \in [k]\}$
$p_i := \|P_i|\psi\rangle\|^2 \quad q_i := \|P_i|\psi\rangle\|^2$

$$\sum |ab| = (\sum a^2)^{1/2}(\sum b^2)^{1/2} \quad Cauchy - Schwarg$$

$$|\|a\| - \|b\||^2 \le \|a - b\|^2$$

3.3 approximating unitary operations

if C computes f with probability 2/3 then if $\|U - V\| \le \epsilon$, then probability $\bar{C}$ compute f with probability $\ge 2/3 - 2\epsilon$
proposision: if pq are probability distribution on [k], E be any event;

$$|p(E) - q(E)| \le \frac{1}{2}\|q\|_1$$

3.4 universality

if $\|U - V\| \le \epsilon$ output state are within ϵ in Euclidean distance, distributions over measurement are within 2ϵ in l_1 distance,

Theorem 3.4.1
For any unitary operation U on $\mathbb{C}^d$, $\epsilon \in (0,1)$ there is a quantum circuit that uses only gates from $\{CNOT, H, T\}$ and computes a unitary operation U
we say the gate set is universal

what is overhead of approximating unitary operation using these 2 gates?

Theorem 3.4.2
for any ϵ and operation $U \in U(2)$ there is a sequence of $O(log\frac{1}{\epsilon})^c$ gates from $\{H, T\}$ which computes V where c is a universal constant

how does the error scale?
Proposition: if $\|U_i - V_i\| \leq \epsilon$, then

$$\|V_t ... V_2 V_1 - U_t ... U_2 U_1\| \leq t\epsilon$$

to get overall error ϵ when approximating m gates, we need only approximate each gate with error ϵ/m, with a sequence of $O(log\frac{m}{\epsilon})$ gates each, total size of new circuit is $O(m(log\frac{m}{\epsilon})^c)$

3.5 implementing measurement

we implement unitary operators $U = \sum |i\rangle\langle u_i|$

3.5.1 projective measurement

how to do projective measurement according to $\{P_i : i \in [k]\}$
recall $P_i = \sum |v_{ij}\rangle\langle V_{ij}|$ we implement basis change operator $U := \sum |i,j\rangle\langle V_{ij}|$

- apply U to get indices in register $A_1 A_2$
- copy A_1 into ancilla B
- Measure B
- apply U* to $A_1 A_2$

3.6 efficiency, complexity classes

the complexity of implementing a measurement is captrued by the basis change operation
if we can efficiently implement basis change operation. we can perform the measurement efficiently
we say a family of cuicuit $\{C_n\}$ where it has n-qubit imput is efficient if its size is $O(n^c)$ for a constant c
the complexity class P consist of all family of boolean functions $\{f_n | f_n : \{0,1\}^n \to \{0,1\}\}$ which has efficient deterministic classical circuits
BPP: bouned error probablitistic polynomial time
BQP: bouned error quantum polynomial time
P: polynomial time

3.7 simulating classcial algorithm

we use toffoli gate to simulate $\{And, Not\}$ given ancilla state $|0\rangle, |1\rangle$

clean simulation: we erase the contents of original output register AND the workspace
we do this by applying unitary transformation, and copying with cnot gate
complexity of clean simulation is efficient

3.8 simulating randomized algrithums, basic algorithm:blackbox, Deutrch-Jozza

for random circuit
Pr(C(x)=y)=pr(h(x,r)=y), where r is uniformly random over $\{0,1\}^k$,
k is number of random bit
using quantum circuit, we apply $H^{\otimes k}$ to $|0\rangle$
$|\psi\rangle = \frac{1}{\sqrt{2^k}} \sum_{r \in \{0,1\}} |r\rangle$
$|\Psi\rangle = U|x\rangle |\psi\rangle |0\rangle = \frac{1}{\sqrt{2^k}} \sum_r |x\rangle |r\rangle |g(x,r)\rangle |h(x,r)\rangle$
$pr(output = y) = \frac{1}{2^k} \sum_r 1(h(x,r) = y) = Pr(h(x,R) = y)$

Definition 3.8.1
blackbox or query model, we have a function $f \to \{0,1\}$ and a circuit that computes it.
classical: x-¿ f(x)
quantum:
$|x\rangle \to |x\rangle$
$|b\rangle \to |b\ CNOT\ f(x)\rangle$
we call this circuit blackbox or oracle for x.

Definition 3.8.2
An assignment $a \in \{0,1\}^h$ of truth values to x satisfies φ if $\varphi(a) = 1$

a classical circuit C or a quantum one O for checking if a given assignment satisfies φ is a blackbox or oracle
given oracle for a function f, we wish to determine if f has some property property like satisfiability
the number of uses of the oracle in an algorithm, the number of queries, is called query complexity

Theorem 3.8.1
$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \otimes_{i=1}^{n} \left(\sum_{y_i \in \{0,1\}} (-1)^{x_i - y_i} |y_i\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{xy} |y\rangle$
Also, $\frac{1}{2^n} \sum_x (-1)^{xy} =$ innerproduct of $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle, \frac{1}{\sqrt{2^n}} \sum_x (-1)^{xy} |x\rangle$
this is innerproduct of $H^{\otimes n}|0^n\rangle, H^{\otimes n}|y\rangle$

xy is scalar product $\sum x_i y_i$
consider a circuit $|xy\rangle \to |x(y \oplus f(x))\rangle$
if $f(x) = 0, |y\rangle = |-\rangle$, second bit become
$U_f = \sqrt{1/2} * |0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = \sqrt{1/2} * (|0\rangle - |1\rangle)$
if $f(x) = 1, |y\rangle = |-\rangle$, second bit become
$U_f = \sqrt{1/2} * |0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = -\sqrt{1/2} * (|0\rangle - |1\rangle)$
this is called phase kickback, where effect of function applying on second qubit becomes a $\pm$ on overall state
most generally,

$$U_f : (\alpha|0\rangle + \alpha_1|1\rangle)(|-\rangle) \to ((-1)^{f(0)}\alpha_0|0\rangle + (-1)^{f(1)}\alpha_1|1\rangle)|-\rangle$$

it can also be written as ,

$$(-1)^{f(0)}(\alpha_0 |0\rangle + (-1)^{f(1)\oplus f(0)}\alpha_1 |1\rangle) |-\rangle$$

we can determine $f(1) \oplus f(0)$ this way

3.9 simon problem

Z_2^n forms a group under mod 2 Z_2
$x + y = (x_1 + y_1, x_2 + y_2 ...)$ $\quad 0x = 0 \quad 1x = x$
there is nonzero element $s \in Z_2^n$ such that $f(x) = f(y)$ iff $y = x + s$ or $x = y$
note $y = x + s, x = y + s, x + y = s$ are the same, we say f hides the string s.
to find s we just need to find f(a)==f(b), b-a=s
$U_f \left(\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |10\rangle \right) = \frac{1}{\sqrt{2}} |0f(0)\rangle + \frac{1}{\sqrt{2}} |1\rangle |0 + f(1)\rangle$

Theorem 3.9.1 (idea of simon algorithm)

$$H^{\otimes n} \frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle) = \frac{1}{\sqrt{2^{n-1}}} \sum_{y \in S^\perp} (-1)^{xy} |y\rangle$$

4 phase estimation

unitary gate $e^{i\psi}$

$$\begin{matrix} 1 & 0 \\ 0 & e^{i\psi} \end{matrix}$$

$Pr(|0\rangle)$ observed at $|0\rangle$ is $cos^2(\psi/2)$ at $|1\rangle$ is $sin^2(\psi/2)$

4.1 textbook

Theorem 4.1.1

$$\frac{1}{\sqrt{2^n}} \sum_{2^n-1}^{1} e^{2\pi i w y} |y\rangle == (\frac{|0\rangle + e^{2\pi i(2^{n-1}w)} |1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle + e^{2\pi i(2^{n-2}w)} |1\rangle}{\sqrt{2}}) \otimes ...(\frac{|0\rangle + e^{2\pi i(2^1 w)} |1\rangle}{\sqrt{2}}) \otimes$$

$$= (\frac{|0\rangle + e^{2\pi i(0.x_n x_{n+1}...)}}{\sqrt{2}}) \otimes ...(\frac{|0\rangle + e^{2\pi i(0.x_1 x_2 ...)}}{\sqrt{2}}) \otimes$$

Theorem 4.1.2
for phase estimation, $p(x) = \frac{sin^2(\pi(2^n w - x))}{2^{2n} sin^2(\pi(w - x/2^n))}$
we also have lemma $|\theta M| < \pi/2$, then $\frac{1}{M^2}\frac{sin^2(M\theta)}{sin^2(\theta)} \geq 4/\pi^2$
this applies to 2 nearest $2^n w$ to x
with probability at least $1 - \frac{1}{2(k-1)}$ phase estimation will ouptut at least $2k$ closest integer multiple of $\frac{1}{2^n}$, $|w - \hat{w}| \leq \frac{k}{2^n}$
final line: phase estimation will output one of the 2k closest integer multiples of $\frac{1}{2^n}$ with probability at least $1 - \frac{1}{2(k-1)}$

4.2

more efficient way of estimating: say $\psi = 2\pi\theta$
$\theta = \theta_1/2 + \theta_2/2^2 ... + \theta_n/2^n$

$$2^m\psi = 2\pi(2^m\theta) = 2\pi(2^{m-1}\theta_1 + 2^{m-2}\theta_2 ... + \theta_m + \frac{\theta_{m+1}}{2} + \frac{\theta_{m+2}}{2^2} ...) = 2\pi(0.\theta_{m+1}...\theta_1)$$

- we can learn θ_{m+1} by repeating experiment O(1) times,
- apply the phase shift twice $2\psi \equiv 2\pi(0.\theta_2\theta_3...)$. and we learn θ_2
- more generally, we can pllay the shift 2^m times and

$$2^m\psi \equiv 2\pi(0.\theta_{m+1}\theta_{m+2}...)$$

U be the unitary gate $e^{i\psi}$

$$U^{2^i} H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(2^i\theta)} |1\rangle)$$

identify a string $y \in \{0,1\}^m$ with corresponding integer $\in \{0, 1..., 2^m - 1\}$
output state of $(U^{2^{m-1}} H \otimes U^{2^{m-2}} H \otimes ...) |000..\rangle$ $|\psi_\theta\rangle = \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^n-1} e^{2\pi i\theta y} |y\rangle$
suppose theta, which we are estimating, is $\theta = a/2^m$ for some $a \in X_{2^m}$
then $e^{2\pi i a y/2^m} = w^{ay}$ where $w = e^{2\pi i/2^m}$ is a constant root of unity
define $|X_x\rangle = \frac{1}{\sqrt{2^m}} \sum_{2^m-1}^{y=0} w^{xy} |y\rangle$
then $\langle x_a | x_b\rangle = 0 | a \neq b$ or $1 | a == b$ due to complex analysis

Definition 4.2.1
$\{|X_x\rangle\, 0 \leq x < 2^m\}$ is then called the fourier basis.

if $\theta = a/2^m$ for some a, then we can measure in fourier basis and determine θ exactly
we has Fourier transform operator

$$F_{2^m} = \sum_{2^{m-1}}^{x=0} |X_x\rangle\langle x|$$

if θ is not integer multiple of $1/2^m$, of we measure in fourier basis , pr(outcome = a) is $|\langle X_a|\psi_\theta\rangle|^2$

4.3 eigenvalue estimation

V is unitary operator on C^d s.t. we can apply V^t geiven

Theorem 4.3.1
note: when c*d is irrational, 1^{c*d} can take infinitely many value, and $1^{c*d} \neq (1^c)^d$

5 error correction

Definition 5.0.1 (Hamming code)
it encodes 1 bit into 3

Definition 5.0.2 (Hamming distance)
the number of bits in which $x, y \in \{0,1\}^n$ differ

Definition 5.0.3
$(n,k,d)_2$ error correction code is a subset $C \in \{0,1\}^n$ of size 2^k st $min\{\delta(x,y)\} : xy \in C, x \neq y = d$
n is block length, k is message length, d is minimum distance of the code c
the elements of the code is called codewords. ratio k/n is information rate
we can recover x if $t \leq (d-1)/2$

Theorem 5.0.1
for any $\epsilon \in [0, 1/4)$, information rate $r < 1 - H(2\epsilon)$ for all n large enough, there are (n,k,d) error correction code with $k := floor(rn)$ and $d \geq 2\epsilon n + 1$

Definition 5.0.4
a linear (n,k,d) code is [n,k,d] code
it has a generator matrix

6 shor code

Theorem 6.0.1 (9-qubit shor code)
1 qubit into 3 for Z error $\alpha |0\rangle + \beta |1\rangle \to \alpha |+++\rangle + \beta |---\rangle$
then encode each of the three qubits into 3 qubits for X error $\to \alpha \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3} + \beta \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3}$

Lemma 6.0.2
if c is [n,k,d] code and $c^\perp$ is $[n, k_2, d_2]$ code with $d_1 d_2 \geq 2t + 1$
$\left|\hat{\psi}\right\rangle = \frac{1}{2^{k/2}} \sum_{x \in c} |x\rangle$ is a code that correct t errors

7 encryption protocal

protocal pi

- alice prepares k bell state $|\psi\rangle^k$ where $|\psi\rangle = |00\rangle + |11\rangle$ in register A_1B_1
- Alice encode state in B_1 using css code C, C has length n, encoded state is B_1'
- alice prepare n bell state $|\psi\rangle^n$ in A_2B_2 with one qubit of each bell state in A_2
- alice premute qubits in B_1' and B_2 uniformly random Afterthis step, all communication is done classically
- bob acknowlodge recepit of 2n qubits
- alice send premutation she used
- bob inverts the premutation and obtain register $B_1'B_2$
- alice selects a unifromly random string $S \in \{0,1\}^n$
- alice measure ith qubit in A_2 in standard basis if $S_i = 0$ in hardarmard basis if $S_i = 1$, send mesasurement to bob
- alice send outcome of measurement to Bob
- Bob measrue ith qubit in B2 in standard basis if $S_i = 0$, or hadamard if 1
- Bob compares outcome with those sent by alice
- let δ_0 be fraction st $S_i = 0$ and different, δ_1 simarly
- if $\delta_0 n \geq (\epsilon - v) * n/2$ ob informs alice, they output fail and stop.
- if both δ_0, δ_1 are small, bob use error correction to decode state in B_1' into B_1
- alice and bob mearue k qubits A_1B_1 instandard basis output pass and outcomes K_AK_B

suppose eve, easedropper apply $P \otimes V$ to qubits sent by alice and private register P, suppose $P = \otimes_{i\in 1:2n} P_i$ where each P_i is 1 X Z XZ
suppose $\geq \epsilon 2n$ of $P_i \in \{X, XZ\}$ then output fail with prob $\geq 1 - 2exp(-cn)$
proof: let $T\{i \in [2n] : P_i \in \{x, xz\}\}$