Approximately correct quantum algorithms

(sections 5.1 & 5.2 in the main ref.)

Coin problem

($\varepsilon > 0$ fixed) we want to distinguish two coins:

- fair coin
- biased coin ; $P[\text{heads}] = \frac{1}{2} + \varepsilon$, $P[\text{tails}] = \frac{1}{2} - \varepsilon$

Classically : we choose one of the coins, flip it $N \gg 1$ times, record the number of times we got heads up

estimate $P[\text{heads}]$

↳ how should we choose N ?

to model this:

consider a string of length n, consisting of randomly generated 0's (tails) with prob. $\frac{1}{2}-\varepsilon$ and 1's (heads) with prob. $\frac{1}{2}+\varepsilon$

$\rightsquigarrow$ want to know the likelihood of $\#(1\text{'s}) = m$ for different m's

more formally

X_i $\quad 0 \le i < n$ independent random variables,

each satisfying $P[X_i = 0] = \frac{1}{2}-\varepsilon$, $P[X_i = 1] = \frac{1}{2}+\varepsilon$

what is the probability distribution of $Y_n = \sum_{0 \le i < n} X_i$?

the <u>central</u> <u>limit</u> <u>theorem</u>

$$\lim_{n\to\infty} \sqrt{n}\ \frac{\frac{1}{n}Y_n - \mu}{\sigma^2}$$

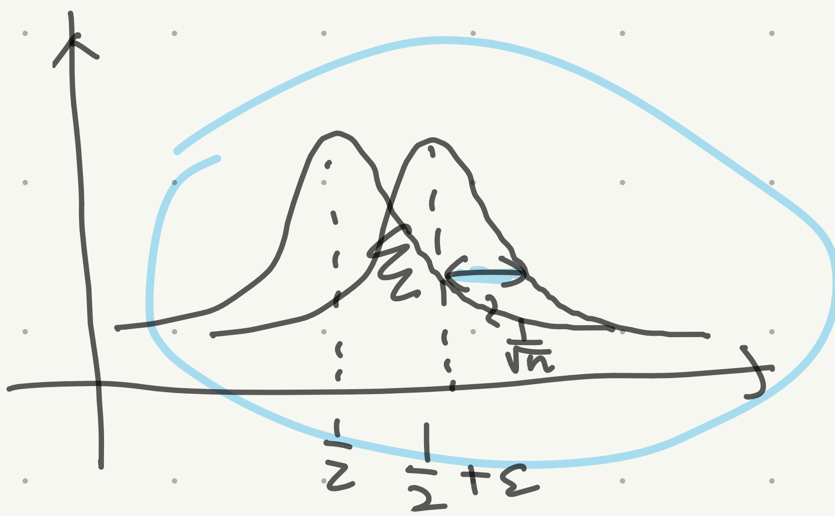
μ: expected value of X_i

σ^2: variance of X_i

is the standard normal distribution

so $\frac{1}{n} Y_n \sim N\left(\text{avg} = \frac{1}{2} + \varepsilon,\ \text{var} = \frac{\left(\frac{1}{4} - \varepsilon^2\right)}{n}\right)$ ← var. of X_i

error scales like $\sqrt{\text{var}} \sim \frac{1}{\sqrt{n}}$



$\frac{1}{n} \sum_{0 \le i < n} X_i$

$\sqrt{n}\, \frac{Y_n - \mu}{\sigma^2} \sim N(0, 1)$

$\Leftrightarrow \frac{Y_n - \mu}{\sigma^2} \sim N\left(0, \frac{1}{n}\right)$

so we need n s.t. $\boxed{\frac{1}{\sqrt{n}} = C\,\varepsilon}$ to achieve a predetermined certainty

$N \sim \frac{1}{\varepsilon^2}$

bits to count such experiment

$\underbrace{* \cdots *}_{m \text{ bits}}$ counts up to $2^m - 1$ ⇝ need $\sim \log \frac{1}{\varepsilon^2}$ bits

$\log_2 N$ bits to count (up to) N flips

An almost quantum algorithm

- prepare the state $|0\rangle \in \mathbb{C}^2$, fix a coin
- repeat:

  controls the # of flips

  - with prob. $\frac{1}{N}$ stop the experiment and measure the state for $|0\rangle, |1\rangle$ basis
  - else, flip the coin, if we get heads up, apply $R_\varepsilon = \begin{bmatrix} \cos\varepsilon & -\sin\varepsilon \\ \sin\varepsilon & \cos\varepsilon \end{bmatrix}$ to the state otherwise apply $R_{-\varepsilon} = R_\varepsilon^{-1}$ then continue to the next step.

expected number of flips: N

how many times do we apply R_ε & $R_{-\varepsilon}$?

(cont.) if the coin is fair, $\frac{N}{2}$ times

⇝ overall apply $R_\varepsilon^{\frac{N}{2}} R_{-\varepsilon}^{\frac{N}{2}} = \mathrm{Id}$ to our state

⇝ we observe $|0\rangle$ with high probability
(if $\varepsilon \ll 1$)

if the coin is biased,

typically we apply $R_\varepsilon^{N(\frac{1}{2}+\varepsilon)} R_{-\varepsilon}^{N(\frac{1}{2}-\varepsilon)} = R_\varepsilon^{2N\varepsilon} = R_{2N\varepsilon^2}$

⇝ setting $N = \frac{\pi}{4\varepsilon^2}$, we are typically applying $R_{\frac{\pi}{2}}$

⇝ initial state is moved to $|1\rangle$

⇝ we observe $|1\rangle$ with high probability

We only need one qubit to record the result of coin flips ⇝ very space efficient

Distinguishing quantum states

Suppose we want to decide if our state is either

$|v\rangle \in \mathbb{C}^N$ or $|w\rangle \in \mathbb{C}^N$

reduction to $N=2$:

choose an orthonormal basis $|u_i\rangle$ $(0 \leq i < N)$

s.t. $|u_i\rangle \perp |v\rangle$, $|u_i\rangle \perp |w\rangle$ for $i \geq 2$

so span of $|v\rangle$ and $|w\rangle$ = span of $|u_0\rangle$ and $|u_1\rangle$

to set up an experiment : choose an orthonormal basis

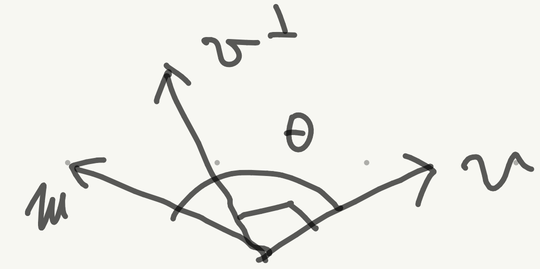
$|u'_0\rangle$, $|u'_1\rangle$ from this space,

$\rightsquigarrow$ $|u'_0\rangle, |u'_1\rangle, |u_2\rangle, |u_3\rangle, \ldots, |u_{N-1}\rangle$ ONB of $\mathbb{C}^N$

we can also work with the <u>real</u> vector space

spanned by $|v\rangle$ and $|w\rangle$

if we do measurement for $|v\rangle$, $|v^\perp\rangle$



if the state was $|v\rangle$: observe $|v\rangle$ surely

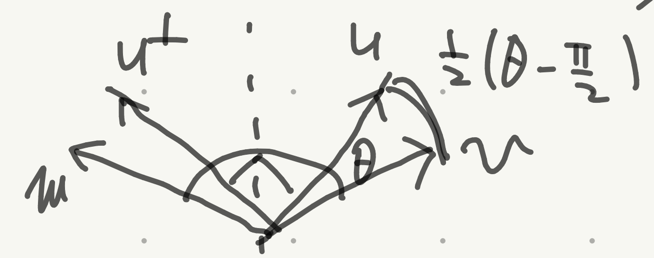
if the state was $|w\rangle$:

observe $|v\rangle$ with prob. $|\langle v | w \rangle|^2 = \boxed{\cos^2\theta}$

observe $|v^\perp\rangle$ with prob. $1 - |\langle v | w \rangle|^2 = \sin^2\theta$

if we do measurement for $|u\rangle$, $|u^\perp\rangle$ s.t.

$|u\rangle + |u^\perp\rangle$ points to the bisector of $|v\rangle$ and $|w\rangle$



if the state was $|v\rangle$

observe $|u\rangle$ with $\cos^2 \frac{1}{2}\left(\frac{\pi}{2} - \theta\right) = \frac{\sin\theta + 1}{2}$ ⇝ guess that we had $|v\rangle$

$|u^\perp\rangle$ with $\boxed{\frac{1 - \sin\theta}{2}}$ ⇝ guess that we had $|w\rangle$

similar for $|w\rangle$

prob. for wrong guess

Partial measurement (section 5.3)

Suppose we have a two-qubit system $\mathbb{C}^2 \otimes \mathbb{C}^2$

generic state vector $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

$\leftarrow |0\rangle\otimes|0\rangle$ $\qquad$ $\leftarrow |0\rangle\otimes|1\rangle$

$(|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1)$

the two qubits can be separated: so two parties can observe each bit separately

do measurement of first bit in basis $|0\rangle, |1\rangle$

if we get $|0\rangle$, the state is

$$|0\rangle \otimes \frac{\alpha|0\rangle + \beta|1\rangle}{\sqrt{|\alpha|^2+|\beta|^2}} \rightsquigarrow \text{second bit is } \begin{cases} |0\rangle \text{ with prob. } \dfrac{|\alpha|^2}{|\alpha|^2+|\beta|^2} \\ |1\rangle \text{ with prob. } \dfrac{|\beta|^2}{|\alpha|^2+|\beta|^2} \end{cases}$$

orthogonal proj. of $|\psi\rangle$ to the span of $|0*\rangle$, then normalized

Maximally entangled state : $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

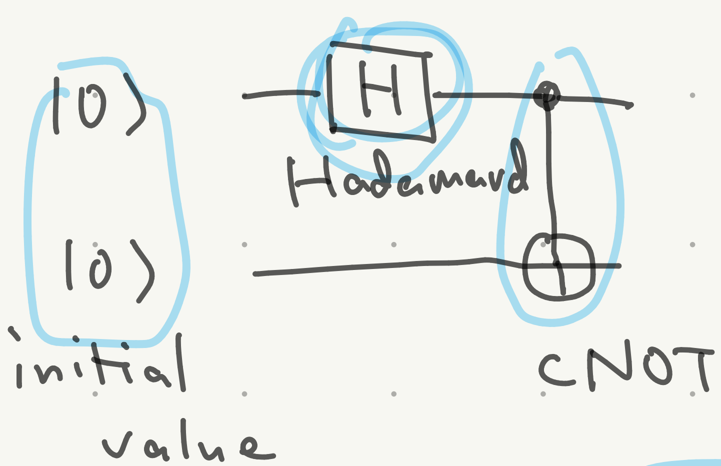
if the measurement for first qubit is $|0\rangle$,

we know that the measurement of second qubit is $|0\rangle$

same with $|1\rangle$

To create interesting states ...

start with $|00\rangle$ and apply gates :

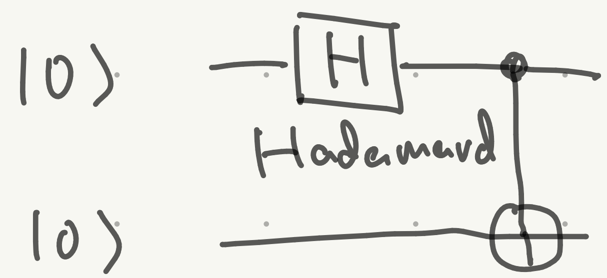


i.e. $\underbrace{\begin{array}{c} \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix} \end{array}}_{\text{CNOT}} \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} (H \otimes I_2)\,|00\rangle$

$H|0\rangle = |+\rangle = \boxed{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}$

$\Rightarrow (H \otimes I_2)\,|00\rangle = H|0\rangle \otimes |0\rangle = \boxed{\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)}$ corresp. to $\begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}$

(cont.) so



represents $\boxed{\begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}} = \underline{\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)}$

Def. an <u>entangled</u> state in $\mathbb{C}^2 \otimes \mathbb{C}^2$ is a state not of the form $|\psi\rangle \otimes |\varphi\rangle$ for $|\varphi\rangle, |\psi\rangle \in \mathbb{C}^2$

(<u>separable</u> or <u>product</u> state)

Ex. <u>singlet</u> / <u>Bell</u> <u>pair</u> / <u>EPR</u> <u>pair</u> :

Einstein-Podolski-Rosen

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

maximally entangled state.