Lecture 1

Sep 24, 2025

The two faces of quantum computation

1. The theoretical model of q. computation
   - what we will explore in this class
   - idealized, consistent, plausible description of reality
   - "implementation agnostic"
   - testbed for algorithm design and proving impossibility results.

2. Implementations of q. computation
   - Ion traps, photonic, Neutral atoms etc
   - Models in which we hope to simulate idealized q.c.
   - Not what we will explore but pertinent to q.c. implementations

Lecture 1 plan:

1. Representation and manipulation of q. information
2. An example of q. computing advantage.

Notation

We express vectors over $\mathbb{C}^d$ as follows:

$$|v\rangle = \begin{pmatrix} v(0) \\ v(1) \\ \vdots \\ v(d-1) \end{pmatrix}$$

For $j \in \{0, \dots d-1\}$

$$|j\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \end{pmatrix} \begin{array}{l} \leftarrow 0^{th} \text{ pos.} \\ \leftarrow j^{th} \text{ pos.} \\ \leftarrow d-1^{th} \text{ pos.} \end{array}$$

and because of its prevalance, we write

$$\langle v| = \left(v(0)^* \quad v(1)^* \quad \dots \quad v(d)^* \right)$$

complex conjugate.

Questions for class: (see pset 0 for length explanation).

① What is $\langle v| \cdot |v\rangle$?

we use short form $\langle v|v\rangle$ for this.

② Let $M = |w\rangle \cdot \langle v|$ (short form $|w\rangle\langle v|$)

for unit vectors $|w\rangle, |v\rangle$. What is $M|v\rangle$?

Axioms of Q.C.

Axiom 1 [State description]

The state of exclusively one qubit can be expressed as a vector in $\mathbb{C}^2$ of unit norm.

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad \text{s.t.} \quad |\alpha|^2 + |\beta|^2 = 1.$$

Not. Define $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Note: $|0\rangle \neq 0$.

These form a orthonormal basis for $\mathbb{C}^2$ and are possible states for a qubit. If the state of a qubit is either $|0\rangle$ or $|1\rangle$, we call it "classical".

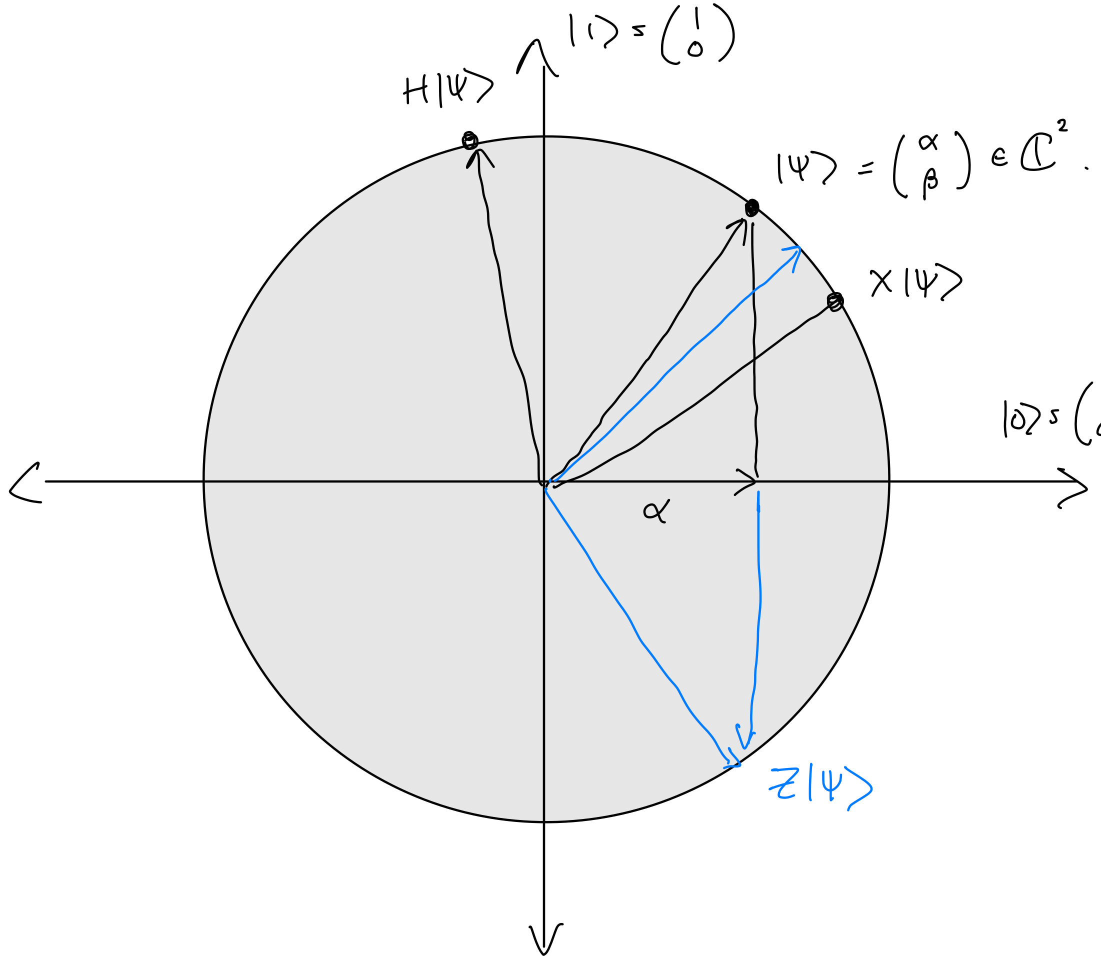
Ex. $\frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] = \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

is a non-classical – i.e. "quantum" – possible state.

Axiom 2 Transformation of a qubit

Let $\mathcal{U}$ be a unitary matrix $\in \mathbb{C}^{2\times 2}$.

We can transform the state $|\psi\rangle$ to $\mathcal{U}|\psi\rangle$.



$|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
$H|\psi\rangle$
$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2.$
$X|\psi\rangle$
$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
α
$Z|\psi\rangle$

Recall $\mathcal{U}$ is a unitary if (equivalently)

① $\mathcal{U}|\psi\rangle$ is unit iff $|\psi\rangle$ is unit.

② $\mathcal{U}^\dagger \mathcal{U} = \mathbb{1}$.

Ex. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ "bit flip"

$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ "phase flip"

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

Axiom 3 (Measurement / Born's Rule)

Given a quantum state $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, we can "measure" the quantum state meaning with

pr $|\langle 0|\psi\rangle|^2 = |\alpha|^2$, the state is now $|0\rangle$

pr $|\langle 1|\psi\rangle|^2 = |\beta|^2$, the $\underbrace{\text{state is now}}_{\text{"collapses"}}$ $|1\rangle$.

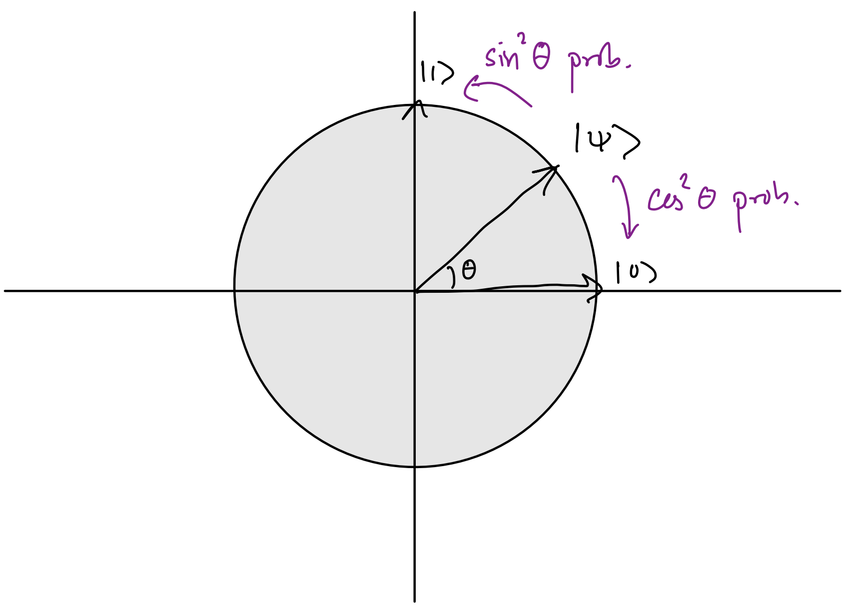
Plus, the classical value "0" or "1" is output.

What does measuring twice in a row do?

If state is $|0\rangle$ or $|1\rangle$ measurement does not change the state.

Hence, why $|0\rangle$ or $|1\rangle$ are classical values

like classical objects, measurement/observations do not change the state.



<u>Remark</u> $\theta \in [0, 2\pi)$, the states $e^{i\theta}|\psi\rangle$ and $|\psi\rangle$ cannot be distinguished by measurement.

<u>Pf</u>: $\Pr[e^{i\theta}|\psi\rangle$ collapsing to $j]$

$$= |\langle j | e^{i\theta} |\psi\rangle|^2$$

$$= \langle \psi | e^{-i\theta} | j\rangle\langle j | e^{i\theta} |\psi\rangle$$

$$= e^{-i\theta} e^{i\theta} \langle \psi | j\rangle\langle j|\psi\rangle$$

$$= \Pr[|\psi\rangle \text{ collapsing to } j].$$

$e^{i\theta}$ is defined as the "global phase".

Quantum states form an equivalence class for $|\psi\rangle \sim e^{i\theta}|\psi\rangle$ and set of states is $\mathbb{C}^2/\sim$.

Axiom 4 (Initialization)

We can initialize a qubit as $|0\rangle$.

These axioms already imply a perfect random number generator.

① Initialize qubit as $|\psi_0\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

② Apply H transform:

$$|\psi_1\rangle = H|\psi_0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}.$$

③ Measure the qubit.

w pr $|\langle 0|\psi_1\rangle|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$ collapses to $|0\rangle$.

w pr $|\langle 1|\psi_1\rangle|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$ collapses to $|1\rangle$.

Multiple qubits

Recall the notion of tensor products

$$A \in \mathbb{C}^{m_1 \times n_1} \qquad B \in \mathbb{C}^{m_2 \times n_2}$$

$$\begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n_1} \\ A_{21} & A_{22} & & A_{2n_1} \\ \vdots & & \ddots & \\ A_{m_1 1} & & & A_{m_1 n_1} \end{pmatrix} \qquad \begin{pmatrix} B_{11} & \cdots & B_{1n_2} \\ \vdots & & \vdots \\ B_{m_2 1} & & B_{m_2 n_2} \end{pmatrix}$$

$$A \otimes B \in \mathbb{C}^{m_1 m_2 \times n_1 n_2}$$

$$\begin{pmatrix} A_{11} \cdot B & A_{12} \cdot B & \cdots & A_{1n_1} \cdot B \\ \vdots & & \ddots & \\ A_{m_1 1} \cdot B & & & A_{m_1 n_1} \cdot B \end{pmatrix}$$

$$\begin{pmatrix} \begin{pmatrix} A_{11}B_{11} & \cdots & A_{11}B_{1n_2} \\ \vdots & & \vdots \\ A_{11}B_{m_2 1} & & A_{11}B_{m_2 n_2} \end{pmatrix} & \cdots & \begin{pmatrix} \; \end{pmatrix} \\ \vdots & & \vdots \\ \begin{pmatrix} \; \end{pmatrix} & & \begin{pmatrix} \; \end{pmatrix} \end{pmatrix}$$

Properties of the tensor product (hw 1):

$A \in \mathbb{C}^{l_1 \times m_1}$ $\quad B \in \mathbb{C}^{l_2 \times m_2}$

note: vectors are matrices too!

$C \in \mathbb{C}^{m_1 \times n_1}$ $\quad D \in \mathbb{C}^{m_2 \times n_2}$

so $AC \in \mathbb{C}^{l_1 \times n_1}$ $\quad BD \in \mathbb{C}^{l_2 \times n_2}$

① $(A \otimes B)(C \otimes D) = AC \otimes BD$.

② linearity. ex. $(A \otimes B)\left(\sum_i C_1 \otimes D_i\right) = \sum_i AC_i \otimes BD_i$.

② $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$

③ $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$ when invertible.

We can also take tensor products of vectors as vectors are 1-D matrices.

Exercises

① What is $|0\rangle \otimes |1\rangle \otimes |0\rangle$?

② What is $|0\rangle \otimes |1\rangle \otimes |1\rangle$?

Notation $\quad |0\rangle \otimes |1\rangle \otimes |0\rangle = |0\rangle|1\rangle|0\rangle = |0,1,0\rangle$

Remark $\quad |x_1, x_2, \ldots, x_n\rangle$ for $x_i \in \{0, 1\}$ is the x^{th} basis vector when $x = x_1 \ldots x_n$ is interpreted in binary.

Better notation: $|0\rangle \otimes |1\rangle \otimes |0\rangle = |010\rangle$

So for $j \in \{0, \ldots, 2^n - 1\}$ we write

$$|j\rangle = |j_1 j_2 \ldots j_n\rangle = |j_1\rangle \otimes \ldots \otimes |j_n\rangle$$

where $j_1 \ldots j_n$ is binary value of j.

Note: orthogonality.

Additionally, when considering vectors in $\mathbb{C}^d$, we use

$$|j\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{array}{l} \leftarrow 0^{th} \text{ location} \\ \\ \\ \leftarrow j^{th} \text{ location} \\ \\ \\ \leftarrow d\text{-}1^{th} \text{ location} \end{array} \qquad \text{for } j \in \{0, \ldots d-1\}$$

This matches the binary description of the vector.

<u>Bringing multiple qubits together</u>

If we have qubit A in state $|\psi_A\rangle$ and qubit B in state $|\psi_B\rangle$,

We need a way to describe the state of the 2 qubits.

$$|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\varphi\rangle_B .$$

We need axioms to describe the composite system

① If qubits don't interact, should reproduce statistics of 1 qubit.

(2) A method for entangling the qubits.

i.e. for any vector $|\varphi\rangle \in (\mathbb{C}^2)^{\otimes 2}$

there exists a method of generating said state.

Updated Axioms for n qubits:

(1) The state of a n qubit system is a unit vec in

$$\underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_{n \text{ times}} = (\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n} =: \underbrace{\mathcal{H}}_{\text{Hilbert space.}}$$

Every quantum state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is a unit vec.

$$\begin{pmatrix} \psi(0\dots0) \\ \psi(0\dots1) \\ \psi(0\dots10) \\ \vdots \\ \psi(1\dots\dots1) \end{pmatrix} = \begin{pmatrix} \psi(0) \\ \psi(1) \\ \vdots \\ \psi(2^n-1) \end{pmatrix}$$

$$|\psi\rangle = \sum_{x=0}^{2^n-1} \underbrace{\psi(x_1 x_2 \dots x_n)}_{\text{amplitude}} \, |x_1, \dots, x_n\rangle = \sum \psi(x) \, |x\rangle$$

$|\psi\rangle$ is classical if all amplitudes are 0 except 1.

$|\psi\rangle$ is in superposition if there are multiple non-zero amplitudes.

② For any unitary $U \in \mathbb{C}^{4 \times 4}$, we can transform the state $|\psi\rangle$ to

$$\Big[\underbrace{\mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_2}_{l_1} \otimes U \otimes \underbrace{\mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_2}_{l_2} \Big] |\psi\rangle$$

$l_1 + 2 + l_2 = n$

this only allows action between adjacent qubits but this turns out to be sufficient (hw 1).

Then,

$$\left(\mathbb{1}_2 \otimes \cdots \otimes \mathbb{1}_2 \otimes \mathcal{U} \otimes \mathbb{1}_2 \cdots \otimes \mathbb{1}_2\right) |x_1 \ldots x_n\rangle$$

$$= \left(|x_1\rangle |x_2\rangle \cdots |x_{i-1}\rangle\right) \otimes \mathcal{U} |x_i, x_{i+1}\rangle \otimes \left(|x_{i+2}\rangle \cdots |x_n\rangle\right)$$

$$= \left(|x_1\rangle |x_2\rangle \cdots |x_{i-1}\rangle\right) \otimes \sum_{k_1, k_2} \mathcal{U}_{(k_1,k_2)(x_i, x_{i+1})} |k_1, k_2\rangle \otimes \left(|x_{i+2}\rangle \cdots |x_n\rangle\right)$$

By linearity we can compute

$$\left(\mathbb{1}_2 \otimes \cdots \otimes \mathbb{1}_2 \otimes \mathcal{U} \otimes \mathbb{1}_2 \cdots \otimes \mathbb{1}_2\right) |\Psi\rangle$$

for any $|\Psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ by expressing

$$|\Psi\rangle = \sum_{x_1 \ldots x_n} \underbrace{\Psi(x_1 \ldots x_n)}_{\text{amplitude.}} |x_1, \ldots, x_n\rangle$$

A unitary $\mathcal{U} \in \mathbb{C}^{2^k \times 2^k}$ is also called a k-qubit unitary. In particular, $\mathcal{U} \in \mathbb{C}^{2\times 2}$ is a single-qubit unitary and $\mathcal{U} \in \mathbb{C}^{4\times 4}$ is a 2-qubit unitary.

$$\underset{\substack{\uparrow \\ \text{acting on} \\ \text{qubit } 1}}{\mathbb{1}_2} \otimes \cdots \otimes \mathbb{1}_2 \otimes \underset{\substack{\uparrow \\ \text{acting on} \\ \text{qubits } i \,\&\, i+1}}{\mathcal{U}} \otimes \mathbb{1}_2 \cdots \otimes \underset{\substack{\uparrow \\ \text{acting on} \\ \text{qubit } n}}{\mathbb{1}_2}$$

is a general q.c. unitary transform.

say
$$\mathcal{U} = \begin{pmatrix} \mathcal{U}_{(0,0),(0,0)} & \mathcal{U}_{(0,0),(0,1)} & \cdots & \mathcal{U}_{(0,0),(1,1)} \\ \vdots & & & \\ \mathcal{U}_{(1,1),(0,0)} & \cdots & & \mathcal{U}_{(1,1),(1,1)} \end{pmatrix}$$

i.e.
$$\mathcal{U} = \sum_{k_1 k_2 j_1 j_2 \in \{0,1\}} \mathcal{U}_{(k_1,k_2)(j_1,j_2)} \, |k_1,k_2\rangle\langle j_1,j_2|$$

③ Measurement of all qubits. (n-qubit Born's rule)

For $j \in \{0, \dots 2^n - 1\}$,

w pr $|\langle j|\psi\rangle|^2$ collapse to $|j\rangle$ and output "j".

problem set 1 will introduce how to measure arbitrary single qubits.

③' measurement of the 1^{st} qubit.

$|\psi\rangle = |0\rangle \otimes |\psi_0\rangle + |1\rangle \otimes |\psi_1\rangle.$

$$|\psi\rangle = \begin{pmatrix} \begin{pmatrix} |\psi_0\rangle \end{pmatrix} \\ \begin{pmatrix} |\psi_1\rangle \end{pmatrix} \end{pmatrix}$$

w pr $\||\psi_0\rangle\|^2$ collapse to $|0\rangle \otimes \frac{|\psi_0\rangle}{\||\psi_0\rangle\|}$.

w pr $\||\psi_1\rangle\|^2$ collapse to $|1\rangle \otimes \frac{|\psi_1\rangle}{\||\psi_1\rangle\|}$.

④ Given n-qubit state $|\psi\rangle$, we can initialize a "fresh" qubit as $|0\rangle$, generating state $|\psi\rangle \otimes |0\rangle$ (unentangled) on $(n+1)$-qubits.

More generally, we can join q. systems

$|\psi\rangle_A \otimes |\varphi_B\rangle$ from $|\psi_A\rangle$ and $|\varphi_B\rangle$.

And we can separate unentangled systems.

These are not axioms as we can derive them from the axioms.

Why does this def satisfy uninteracting qubit statistics.

$$|\Psi\rangle = \underbrace{|\psi\rangle}_{1\text{ qubit}} \otimes \underbrace{|\varphi\rangle}_{\text{multiple qubits}}$$

If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Then $|\Psi\rangle = \alpha|0\rangle|\varphi\rangle + \beta|1\rangle|\varphi\rangle$.

$$= |0\rangle\alpha|\varphi\rangle + |1\rangle\beta|\varphi\rangle.$$

So, pr $\| \alpha|\varphi\rangle \|^2 = |\alpha|^2$ collapses to $\dfrac{\alpha|\varphi\rangle}{|\alpha|}$

pr $|\beta|^2$ collapses to $\dfrac{\beta|\psi\rangle}{|\beta|}$.

So remaining state remains $\propto |\psi\rangle$.

Matches our intuition for what should happen.

Important math review: Prob. Theory.

Let $X \geq 0$ be a pos. random variable.

(1)

Markov's Ineq. $\Pr[X \geq a] \leq \dfrac{\mathbb{E}X}{a}$ for all $a > 0$.

Pf. $$\mathbb{E}X = \underbrace{\mathbb{E}[X \mid X \geq a]}_{a} \cdot \Pr[X \geq a] + \underbrace{\mathbb{E}[X \mid X < a]}_{0} \underbrace{\Pr[X < a]}_{0}$$
$$\geq a \quad \Pr[X \geq a] + 0 \cdot 0$$

(2)

Let X be a r.v. with $\mathrm{Var}\, X = \sigma^2$ finite and $\mathbb{E}X = \mu$.

Chebyshev's Ineq. $\forall\, k > 0$,

$$\Pr\Big[\, |X - \mu| \geq k\sigma \,\Big] \leq \frac{1}{k^2}.$$

Pf. Apply Markov for $Y = (X-\mu)^2$ and $a = k^2\sigma^2$.

$$\Pr\left[\,|X-\mu| \geq k\sigma\right] = \Pr\left[(X-\mu)^2 \geq k^2\sigma^2\right]$$

$$= \Pr\left[Y \geq k^2\sigma^2\right]$$

$$\leq \frac{\mathbb{E}Y}{k^2\sigma^2} = \frac{\sigma^2}{k^2\sigma^2} = \frac{1}{k^2}.$$

③ Chernoff bounds:

$$\Pr\left[X \geq a\right] = \Pr\left[e^{tX} \geq e^{ta}\right]$$

$$\leq \frac{\mathbb{E}\left[e^{tX}\right]}{e^{ta}} \qquad \text{(Markov's)}$$

So, $\Pr\left[X \geq a\right] \leq \inf\limits_{t>0} \dfrac{\mathbb{E}\left[e^{tX}\right]}{e^{ta}}$.

If $X = X_1 + \dots + X_n$, then

$$\Pr\left[X \geq a\right] = \inf_{t>0} e^{-ta} \prod_{i=1}^{n} \mathbb{E}\left[e^{tX_i}\right].$$

If $X_i \in \{0,1\}$ then $e^{tX_i} = \begin{cases} e^t & \text{pr } p_i := \mathbb{E}X_i \\ 1 & \text{pr } 1-p_i \end{cases}$

$$\mathbb{E}\, e^{tX_i} = (e^t - 1)\, p_i + 1 \le e^{p_i(e^t-1)}.$$

So, $$\prod_i \mathbb{E}\, e^{tX_i} \le e^{(p_1+\dots+p_n)(e^t-1)}.$$
$$= e^{\mu(e^t-1)} \qquad \mu = \mathbb{E}X = p_1+\dots+p_n.$$

Let $a = (1+\delta)\mu$.

$$\inf_{t>0} e^{-ta} \prod_i \mathbb{E}[e^{tX_i}]$$
$$\le \inf_{t>0} e^{-t(1+\delta)\mu} e^{\mu(e^t-1)}$$
$$\le \inf_{t\ge 0} \left(e^{\left(\frac{e^t-1}{(1+\delta)t}\right)} \right)^{\mu}.$$

<u>Ex.</u> inf at $t = \ln(1+\delta)$.

$$= \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}} \right)^{\mu} \underbrace{\le}_{\text{exercise.}} e^{-\delta^2\mu/(2+\delta)}.$$

Chernoff bounds: $X_1, \ldots X_n \in \{0,1\}$. $X = \sum X_i$, $\mu = \mathbb{E} X$,

$$\Pr[X \geq (1+\delta)\mu] \leq e^{-\delta^2 \mu/(2+\delta)}$$

$$\Pr[X \leq (1-\delta)\mu] \leq e^{-\delta^2 \mu/2}$$

$$\Pr[|X-\mu| \geq \delta\mu] \leq 2e^{-\delta^2 \mu/3}$$