# Quantum Automata cannot detect biased coin, even in the limit

Ingyu Baek

# Problem Motivation

- Given an infinite seq of coin tosses (HTHTT⋯) such that each toss is independent event, investigate ability of a finite automaton to distinguish fair coin, or biased ($p = \frac{1}{2} \pm \epsilon$) coin.

# Problem specification

1. Type of (Finite) automaton: Classical or quantum
2. Is $\epsilon$ known? (If Coin is biased, then it is biased by known $\epsilon$)
3. How does the automaton 'outputs' fair or biased?

# Problem specification

## 3. How does the automaton 'outputs' fair or biased?

3-1. Automaton runs forever to output fair, halts to output biased.
-One sided halting

3-2. Every state of (finite) automaton is labelled fair or biased. Consider time-average of automaton spending in biased states vs fair states. Limit the time to infinity, and if automatons spends greater or equal time in fair states on average than $\frac{2}{3}$, automaton output fair.
-Limiting acceptance

# Example

- [Hellman and Cover]

If $\epsilon$ is known, classical finite automaton can detect biased coin by limiting acceptance with $\Omega(1/\epsilon)$ states.

- [Aaronson and Drucker]

(i) If $\epsilon$ is known, a quantum automaton with 2 states can solve the problem by limiting acceptance.

(ii) If $\epsilon$ is unknown, exists no finite quantum automaton with fixed #states that solves the problem by one sided halting.

# Problem specification

1. Type of (Finite) automaton: Classical or quantum
2. Is $\epsilon$ known? (If Coin is biased, then it is biased by known $\epsilon$)
3. How does the automaton 'outputs' fair or biased?

For 48 different versions Aaronson considered, the only unsolved version is as follows:

# Goal

There is no quantum finite automaton that has the following property simultaneously for every $\epsilon \in [-\frac{1}{2}, \frac{1}{2}] \setminus \{0\}$:

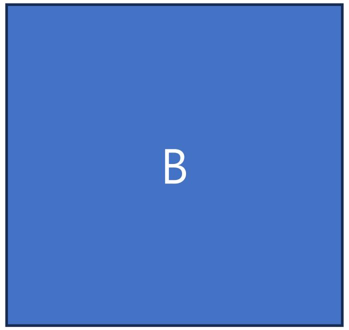
Given access to an infinite sequence of coin tosses, if the coin is $(1/2 + \epsilon)$-biased then the automaton spends at least 2/3 of its time guessing “biased”, and if the coin is fair then the automaton spends at least 2/3 of its time guessing “fair”.

# Mixed State

- Assume two boxes


Outputs $|1\rangle$ with prob ½
Outputs $|0\rangle$ with prob ½

Any way to differentiate two boxes?




Outputs $-\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$ with prob ½
Outputs $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ with prob ½

# Mixed State

- Usually used in two cases
  1. when the preparation of the system is not fully known, and thus one must deal with a statistical ensemble of possible preparations
  2. when one wants to describe a physical system which is entangled with another, without describing their combined state.

  *Ensemble: Idealization consisting large number of virtual copies

  *Like box of above example. (One can pick as many qubits as desired)

# Mixed State

- Density operator is defined as follows:

If pure state $|\psi_i\rangle$ has probability $p_i$, for all $i$, then pure state $\rho \in \mathcal{B}(\mathcal{H})$ is defined as follows to represent all indistinguishable mixed states:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} \frac{3}{4} & -\frac{\sqrt{3}}{4} \\ -\frac{\sqrt{3}}{4} & \frac{1}{4} \end{pmatrix} + \frac{1}{2}\begin{pmatrix} \frac{1}{4} & \frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{3}{4} \end{pmatrix}$$

$$= \frac{1}{2}\left(-\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)\left(-\frac{\sqrt{3}}{2}\langle 0| + \frac{1}{2}\langle 1|\right) + \frac{1}{2}\left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)\left(\frac{1}{2}\langle 0| + \frac{\sqrt{3}}{2}\langle 1|\right)$$

# Mixed State

- Transition of quantum state

From $U|\psi\rangle$, to $\Phi(\rho)$

$\Phi: \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ (Superoperator)

From unitary condition( $U^* = U^{-1}$), quantum channel $\Phi$ should be completely positive and trace-preserving.

Equivalently,

# Mixed State

- Transition of quantum state

Equivalently, exists (not necessarily unique) Kraus operators $K_1, K_2, \ldots, K_r$ with $\sum_{i=1}^{r} K_i^* K_i = I$ such that $\Phi(\rho) = \sum_{i=1}^{r} K_i \rho K_i^*$

- Measurement of quantum state

For pure state $|\psi\rangle$, when measured with standard basis, probability getting result is absolute square value of indices of $|\psi\rangle$. Analogous version for mixed state is as follows:

# Mixed State

- Measurement of quantum state

Defn: POVM(positive operator-valued measure) is a set of Hermitian matrixes $\{F_i\}$ such that $\sum_{i=1}^{n} F_i = I$.

$Prob(i) = \mathrm{tr}(\rho F_i)$ whereas $Prob(i)$ is probability of measuring value related with $i$.

We will denote $Prob(i)$ as $\langle F_i, \rho \rangle$.

# Properties of Quantum Channel

**Cesàro Mean**

Let $\langle a_n \rangle$ be a sequence of complex numbers. Suppose that $\langle a_n \rangle$ converges to $l$ in $\mathbb{C}$ . Then

$$\lim_{n \to \infty} \left( \frac{a_1 + a_2 + \ ... + a_n}{n} \right) = l$$

# Properties of Quantum Channel

## Cesàro Mean

**Proof)** For any fixed integer $n_0$,

$$\left|\frac{a_1 + a_2 + \ \ldots + a_n}{n} - l\right| \leq \frac{(|a_1 - l| + \cdots + |a_n - l|)}{n} \leq n_0 \frac{\sup_{k \leq n_0} |a_k - l|}{n} + \sup_{n_0 < k \leq n} |a_k - l|$$

Apply $n \to \infty$ to both sides. Then,

$$\limsup_{n \to \infty} \left|\frac{a_1 + a_2 + \ \ldots + a_n}{n} - l\right| \leq \sup_{n_0 < k} |a_k - l|$$

Now apply $n_0 \to \infty$. As $a_k$ converge to $l$,

$$\limsup_{n \to \infty} \left|\frac{a_1 + a_2 + \ \ldots + a_n}{n} - l\right| = 0$$

Therefore, $\lim_{n \to \infty} \left(\frac{a_1 + a_2 + \ \ldots + a_n}{n}\right) = l = \lim_{n \to \infty} a_n$ .

# Properties of Quantum Channel

## Cesàro Mean

Similar holds for Quantum channel.

For any quantum channel $\Phi$, let $\widehat{\Phi^{\infty}} := \lim_{N\to\infty} \frac{1}{N} \Sigma_{n=1}^{N} \Phi^{n}$ and $\Phi^{\infty} := \lim_{n\to\infty} \Phi^{\mathrm{n}}$. They both are itself existing quantum channel and they are same.

# Mathematical background

## Invariant subspace

**Def:** Invariant subspace of any linear operator $T$, denoted as $V_1(T)$ , is eigenspace of $T$ with eigenvalue 1.

Why 'invariant'? $T(x) = x$ iff $x \in V_1(T)$. Applying $T$ cannot change $x$.

For any quantum channel $\Phi$,Let $y = \Phi^{\infty}(x)$ for some density operator $x$.

$\Phi(y) = \Phi\left(\Phi^{\infty}(x)\right) = \Phi^{\infty}(x) = y$. Therefore, $y$ is density operator in $V_1(\Phi)$.

(i.e. $\Phi^{\infty}$ is projection onto some fixed points of $V_1(\Phi)$.)

# Mathematical background

## Distance defined between (sub)spaces( Perturbation theory for linear operators, Tosio Kato, 4.2.1)

Let $\mathcal{W}(X, Y)$ be set of all closed operators from $X$ to $Y$. If $T, S \in \mathcal{W}(X, Y)$,their graphs $G(T), G(S)$ are closed linear manifolds in the product space $X \times Y$.

Thus the "distance" between T and S can be measured by the "gap" between the closed linear manifolds: $G(T), G(S)$. For two linear closed manifolds M and N, gap function is denoted $\hat{\delta}$ and defined as follows:

$$\delta(M, N) = \sup_{u \in S_M} dist(u, N) \quad (x \in S_M \ iff \ x \in M \ and \ ||x|| = 1)$$

$$\hat{\delta}(M, N) = \max[\delta(M, N), \delta(N, M)]$$

# Mathematical background

## Invariant subspace

Perturbation theory studies effect of small change of linear operator.

Generally, slight modification of linear operator can change dimension of its invariant space.

## Distance defined between (sub)spaces

(Perturbation theory for linear operators, Tosio Kato, 4.2.2)

Let $M, N$ be a linear manifolds in a Banach space $Z$. If $\dim M > \dim N$ there exists $u \in M$ such that:

$$dist(u, N) = ||u|| > 0$$

# Mathematical background

**Theorem: Given nullity of matrix $\boldsymbol{A(a)}$ is constant(nonzero), its kernel is continuous.**

Pf) By rank- nullity thm, rank of A is also constant:$k$. Say A is of size n.

As it is also known that applying permutation matrix(or any other invertible matrix) to $A$ doesn't change kernel of $A$, one permutate $A$ so that:

$$A(a) = \begin{bmatrix} X(a) & X(a)Y(a) \\ Z(a) & Z(a)Y(a) \end{bmatrix}$$

Where $X(a)$ is invertible matrix of size k.(Thus, rank $k$). Then basis of kernel is

$\left\{\begin{bmatrix} -Y(a)e_1 \\ e_1 \end{bmatrix}, \begin{bmatrix} -Y(a)e_2 \\ e_2 \end{bmatrix} \dots \begin{bmatrix} -Y(a)e_{n-k} \\ e_{n-k} \end{bmatrix}\right\}$, where $e_i$ is standard basis of $\mathbb{R}^{n-k}$.

# Problem Reduction

There is no quantum finite automaton that has the following property simultaneously for every $\epsilon \in [-\frac{1}{2}, \frac{1}{2}] \setminus \{0\}$:

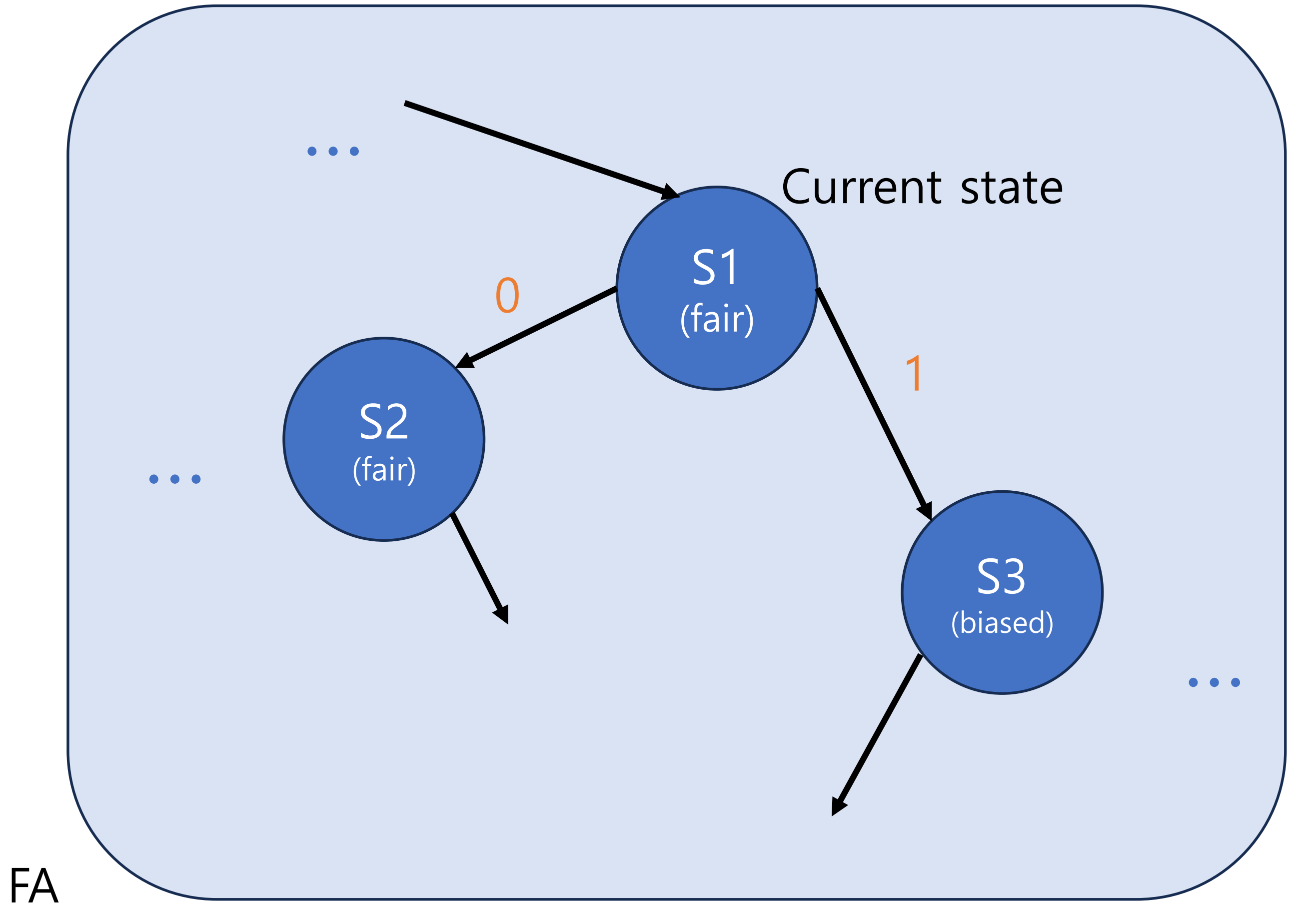
Given access to an infinite sequence of coin tosses, if the coin is $(1/2 + \epsilon)$-biased then the automaton spends at least 2/3 of its time guessing "biased", and if the coin is fair then the automaton spends at least 2/3 of its time guessing "fair".

# Problem Reduction-classic version

There is no finite automaton that has the following property simultaneously for every $\epsilon \in [-\frac{1}{2}, \frac{1}{2}] \setminus \{0\}$:

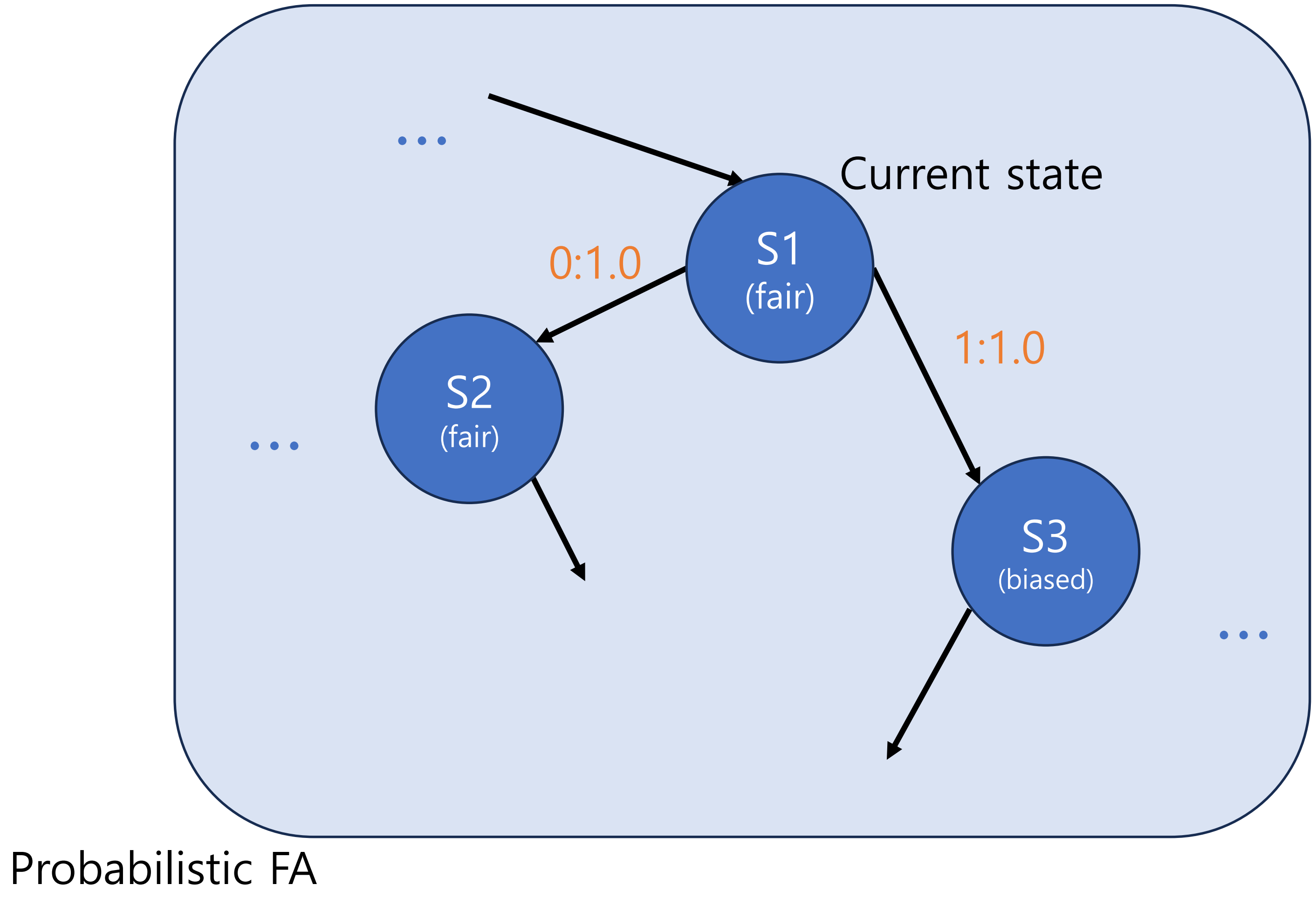
Given access to an infinite sequence of coin tosses, if the coin is $(1/2 + \epsilon)$−biased then the automaton spends at least 2/3 of its time guessing “biased”, and if the coin is fair then the automaton spends at least 2/3 of its time guessing “fair”.

# Problem Reduction-classic version



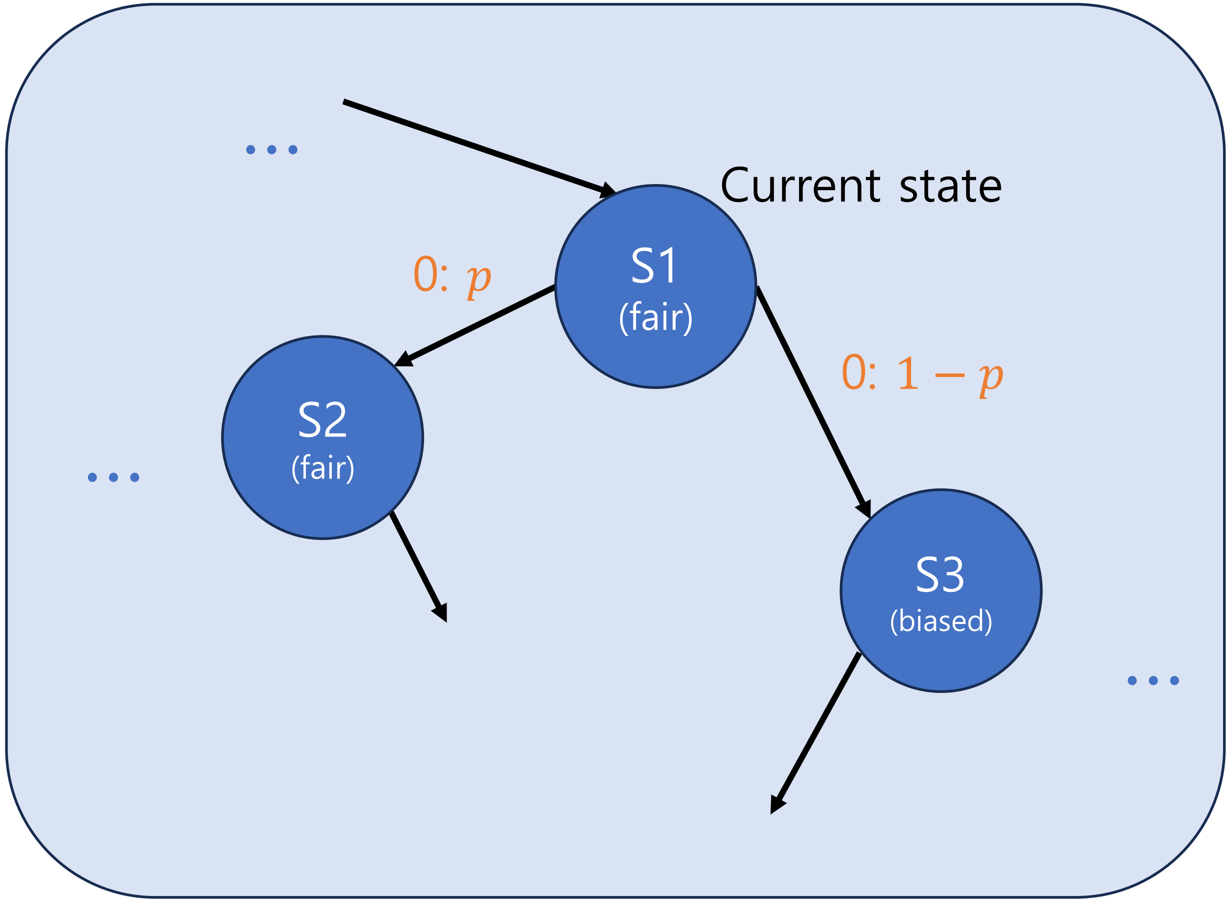

With infinite input string consisted of 0, 1 that is result of coin toss of probability $p$, do there exist FA that detects biased coin?

# Problem Reduction-classic version




With infinite input string consisted of 0, 1 that is result of coin toss of probability $p$, do there exist FA that detects biased coin?

# Problem Reduction-classic version



Probabilistic FA

With infinite input string consisted of just 0, do there exists probabilistic finite automata that detects biased coin?

# Problem Reduction-classic version

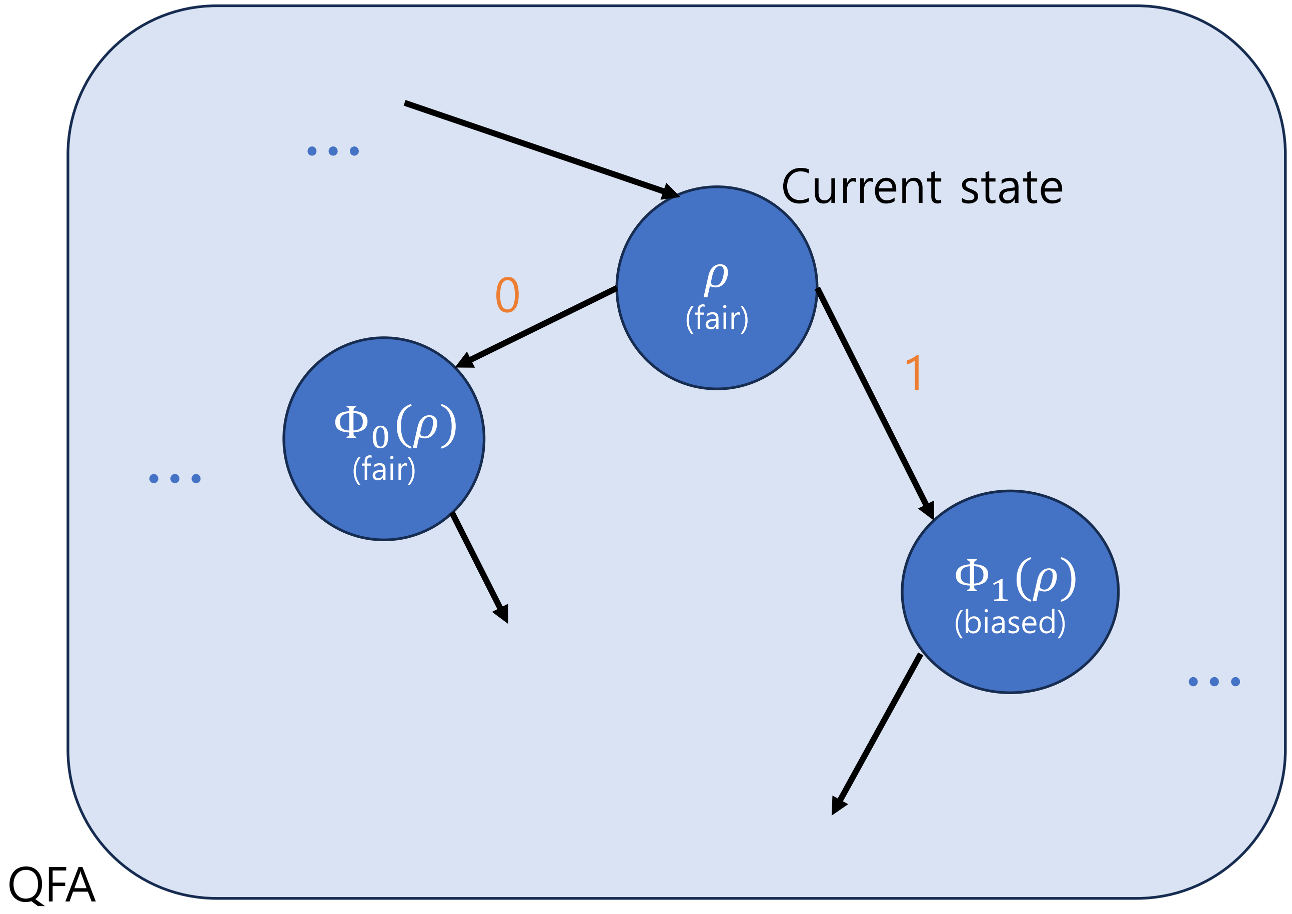
Formally,

Let $S_0, S_1$ be the stochastic matrix, then probabilistic automata applies $S_0$ when current input is 0 and applies $S_1$ when current input is 1.

equivalent with,

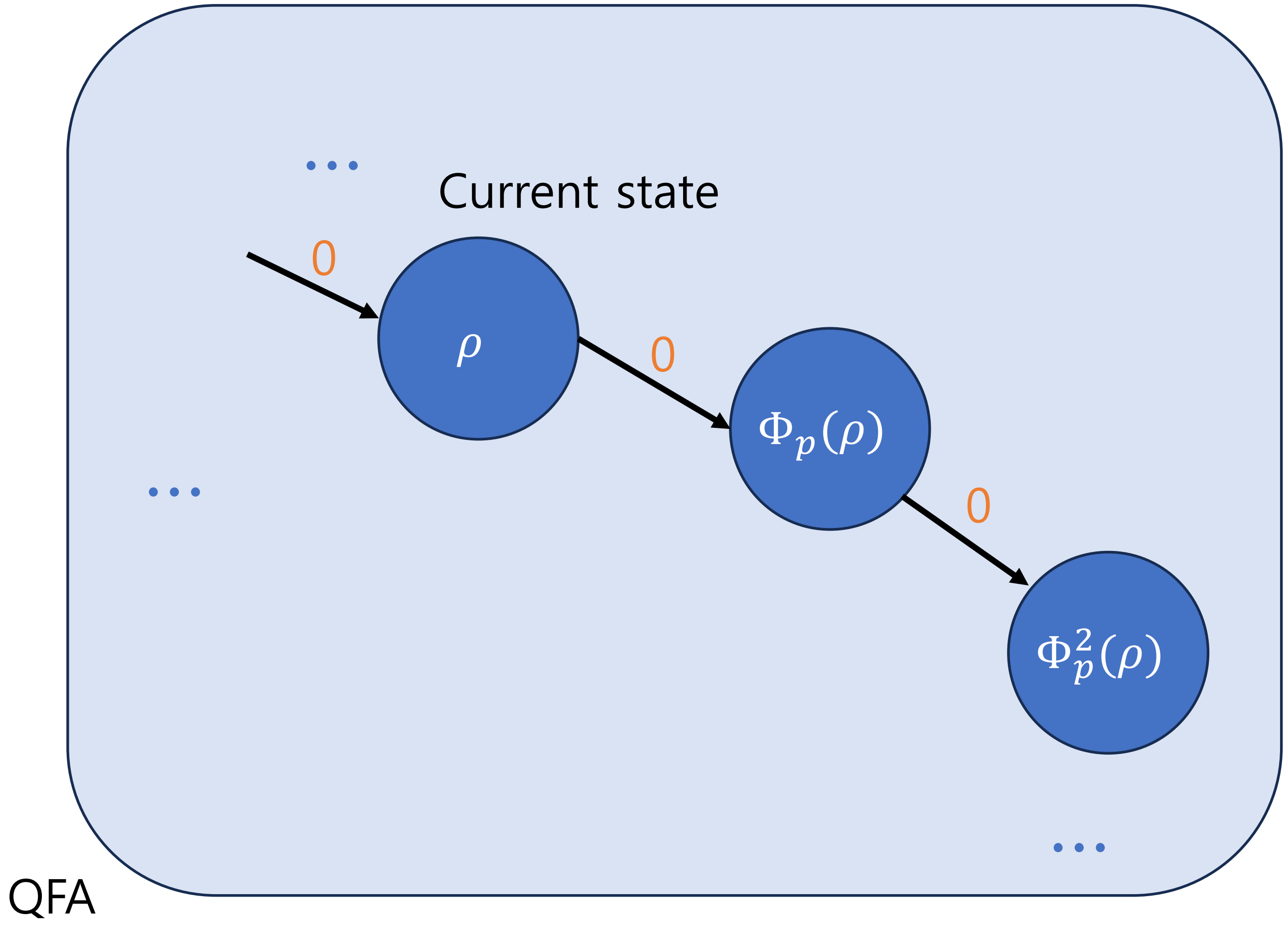
Probabilistic automata applies $S_p := pS_1 + (1-p)S_0$.

# Problem Reduction




With infinite input string consisted of 0, 1 that is result of coin toss of probability $p$, do there exist QFA that detects biased coin?

# Problem Reduction




$$\Phi_p := p\Phi_1 + (1-p)\Phi_0$$

# Problem Reduction

Enough to show:

There exists no quantum finite automaton $Q_p = (\pi_0, S, \Phi_p, \{E_{fair}, I - E_{fair}\})$ where

$S$ is set of quantum (mixed) states,

$\pi_0$ is start state.

$\Phi_p$ is quantum channel that is convex combination of some other quantum channels $\Phi_0, \Phi_1$ i.e. $\Phi_p \coloneqq p\Phi_1 + (1-p)\Phi_0$

$\{E_{fair}, I - E_{fair}\}$ is POVM that probabilistically checks whether state is labelled fair of biased : for $s \in S, \langle E_{fair}, s \rangle$ is probability that automaton may measure state s as fair state

# Problem Reduction

Enough to show:

There exists no quantum finite automaton $Q_p = (\pi_0, S, \Phi_p, \{E_{fair}, I - E_{fair}\})$ such that $Q_p$ 'detects' whether $p$ is ½ or not.

**Defn**

Let $f(p) := \lim_{T\to\infty} \frac{1}{T}\left(\sum_{t=1}^{T} \langle E_{fair}, \Phi_p^t \pi_0 \rangle\right)$

We will say QFA outputs fair for given $p$ if $f(p) \geq \frac{2}{3}$. Otherwise, biased.

# Problem Reduction

## Enough to show:

$f$ is continuous for $p \in (0,1)$.
(∵If f is continuous one can reduce $\epsilon$ as much as needed to 'fool' the QFA.)

## Definition

Let $f(p) := \lim_{T \to \infty} \frac{1}{T} \left( \sum_{t=1}^{T} \langle E_{fair}, \Phi_p^t \pi_0 \rangle \right)$

We will say QFA outputs fair for given $p$ if $f(p) \geq \frac{2}{3}$. Otherwise, biased.

# Problem Reduction

$f(p) := \lim_{T\to\infty} \frac{1}{T} \left( \sum_{t=1}^{T} \left\langle E_{fair}, \Phi_p^t \pi_0 \right\rangle \right) = \left\langle E_{fair}, \widehat{\Phi_p^\infty} \pi_0 \right\rangle = \left\langle E_{fair}, \Phi_p^\infty \pi_0 \right\rangle$ (Cesàro Mean)

Enough to show:

$\Phi_p^\infty$ is continuous.

As $\Phi_p^\infty$ is projection onto $V_1(\Phi_p)$,

one possible obstruction is when dimension of $V_1(\Phi_p)$ changes with small change of p.

# Problem Reduction

Enough to show:

$\Phi_p^\infty$ is continuous.

One possible obstruction: Dimesion of $V_1(\Phi_p)$ changes with small change of p.

Assume $\dim V_1(\Phi_p)$ constant.

Notice, $x \in V_1(\Phi_p)$ iff $\Phi_p(x) = x$ iff $(I - \Phi_p)(x) = 0$ iff $x \in \ker(I - \Phi_p)$ , $V_1(\Phi_p) = \ker(I - \Phi_p)$ .By assumption, nullity of $I - \Phi_p$ also constant.

By previous thm, $\ker(I - \Phi_p)$ continuous, .

# Problem Reduction

Enough to show:

$\dim V_1(\Phi_p)$ is constant for all $p \in (0,1)$. Classical version of solving it?

# Recap Markov chain

Given S as a stochastic matrix, it is known $V_1(S)$ is spanned by a linearly independent set of invariant probabilistic-states.

$\therefore \dim V_1(S)$ is equal to the number of linearly independent invariant distributions

There is one linearly independent invariant distribution per every communication class of the Markov chain.

Communication class: Strongly connected components of the underlying digraph

# Quantum analogous known facts

Given $\Phi$ as a quantum channel, it is known $V_1(\Phi)$ is spanned by a linearly independent set of (quantum) states.

Minimal enclosure is analogous to communicating class.

Enclosure: A closed subspace $V$ is an enclosure for $\Phi$ if, for any state $\rho$, $supp(\rho) \subset V$ implies $supp\,(\Phi(\rho)) \subset V$

$supp(\rho)$: Range of $\rho$. (As it is density operator)

Minimal enclosure: $V$ is nonzero and all subset of $V$ which is also enclosure is rather zero or $V$.

# Quantum analogous known facts

Minimal enclosure is analogous to communicating class.

Known facts:

$V$ is an enclosure for $\Phi$ if and only if $K_i V \subseteq V$ for all Kraus operators of $\Phi$.

Minimal enclosure decomposition (decomposes Hilbert space as direct sum) can be constructed for $\Phi$ (analogous to identifying strongly connected component in digraph)

$\dim V_1(\Phi)$ derives rather directly from minimal enclosure decomposition.

# Problem Reduction

**Definition**

We will say that two channels $\Phi$ and $\widehat{\Phi}$ (with the same Hilbert space $\mathcal{H}$) are combinatorially equivalent if there are Kraus operators $K_1, \ldots, K_r$ for $\Phi$ and $\widehat{K_1}, \ldots, \widehat{K_{\hat{r}}}$ for $\widehat{\Phi}$ such that each $K_i$ is proportional to some $\widehat{K_i}$, and vice versa.

**Theorem . All $\boldsymbol{\Phi_p}$ are combinatorially equivalent.**

Proof can be given by claiming this:

Let $\Phi_0, \Phi_1$ have Kraus operators $\{K_i^{(0)}: i \in [r_0]\}$, $\{K_j^{(1)}: j \in [r_1]\}$ respectively,

the channel $\Phi_p = p\Phi_1 + (1-p)\Phi_0$ has Kraus operators $\left\{\sqrt{1-p}K_i^{(0)}: i \in [r_0]\right\} \cup \left\{\sqrt{p}K_j^{(1)}: j \in [r_1]\right\}$.

# Problem Reduction

**Theorem . All $\mathbf{\Phi_p}$ are combinatorially equivalent.**

Let $\Phi_0, \Phi_1$ have Kraus operators $\{K_i^{(0)}: i \in [r_0]\}$, $\{K_j^{(1)}: j \in [r_1]\}$ respectively,

the channel $\Phi_p = p\Phi_1 + (1-p)\Phi_0$ has Kraus operators $\left\{\sqrt{1-p}K_i^{(0)}: i \in [r_0]\right\} \cup \left\{\sqrt{p}K_j^{(1)}: j \in [r_1]\right\}$.

$$\Phi_p(x) = p\Phi_1(x) + (1-p)\Phi_0(x) = p\Sigma_{i\in[r_0]}K_i^{(0)}xK_i^{(0)^*} + (1-p)\Sigma_{j\in[r_1]}K_j^{(1)}xK_j^{(1)^*}$$

$$= \Sigma_{i\in[r_0]}\sqrt{p}K_i^{(0)}x(\sqrt{p}K_i^{(0)})^* + \Sigma_{j\in[r_1]}\sqrt{1-p}K_j^{(1)}x(\sqrt{1-p}K_j^{(1)})^* \qquad \blacksquare$$

# Proof

Enough to show:

If $\Phi$ and $\widehat{\Phi}$ are combinatorially equivalent, then they have same minimal enclosure decomposition.

This requires rather technical approach, but is fundamentally driven from this fact:

$V$ is an enclosure for $\Phi$ if and only if $K_i V \subseteq V$ for any Kraus operators of $\Phi$.