Why Probability and Nondeterminism?
Concurrency Theory

• Nondeterminism
  - Scheduling within parallel composition
  - Unknown behavior of the environment
  - Underspecification

• Probability
  - Environment may be stochastic
  - Processes may flip coins
Automata

\[ A = (Q, q_0, E, H, D) \]

- **Transition relation**
  \[ D \subseteq Q \times (E \cup H) \times Q \]

- **Internal (hidden) actions**

- **External actions**:
  \[ E \cap H = \emptyset \]

- **Initial state**:
  \[ q_0 \in Q \]

- **States**
Example: Automata

\[ A = (Q, q_0, E, H, D) \]

Execution: \[ q_0 \ n \ q_1 \ n \ q_2 \ ch \ q_3 \ coffee \ q_5 \]

Trace: \[ n \ n \ coffee \]
Probabilistic Automata

\[ PA = (Q, q_0, E, H, D) \]

Transition relation
\[ D \subseteq Q \times (E \cup H) \times \text{Disc}(Q) \]

Internal (hidden) actions

External actions: \( E \cap H = \emptyset \)

Initial state: \( q_0 \in Q \)

States
Example: Probabilistic Automata

\[ q_0 \xrightarrow{\text{fair}} q_1 \xrightarrow{\text{flip} \ 1/2} q_3 \xrightarrow{\text{beep}} q_5 \]

\[ q_0 \xrightarrow{\text{unfair}} q_2 \xrightarrow{\text{flip} \ 2/3} q_3 \]

\[ q_2 \xrightarrow{\text{flip} \ 1/2} q_4 \xrightarrow{\text{flip} \ 1/3} q_5 \]
Example: Probabilistic Automata

\[ q_0 \xrightarrow{\text{flip}} q_h \xrightarrow{1/2} q_p \]

\[ q_0 \xrightarrow{\text{flip}} q_t \xrightarrow{2/3} q_p \]

\[ q_0 \xrightarrow{1/3} q_p \]
Example: Probabilistic Automata

What is the probability of beeping?
Example: Probabilistic Executions

\[ q_0 \xrightarrow{\text{fair}} q_1 \xrightarrow{\text{flip} \ 1/2} q_3 \xrightarrow{\text{beep}} q_5 \]

\[ \mu(\text{beep}) = 1/2 \]

\[ q_0 \xrightarrow{\text{unfair}} q_2 \xrightarrow{\text{flip} \ 1/3} q_4 \xrightarrow{\text{beep} \ 2/3} q_5 \]

\[ \mu(\text{beep}) = 2/3 \]
Example: Probabilistic Executions

\[
\begin{align*}
q_0 & \xrightarrow{\text{fair}} q_1 \\
q_0 & \xrightarrow{\text{unfair}} q_2 \\
q_1 & \xrightarrow{\text{flip}} q_3 \\
q_2 & \xrightarrow{\text{flip}} q_3 \\
q_3 & \xrightarrow{\text{beep}} q_5 \\
q_4 & \xrightarrow{\text{beep}} q_5 \\
q_5 & \xrightarrow{1/4} \text{fair} \\
q_5 & \xrightarrow{7/12} \text{unfair} \\
q_5 & \xrightarrow{2/6} \text{flip}
\end{align*}
\]
Measure Theory

- **Sample set**
  - Set of objects $\Omega$

- **Sigma-field ($\sigma$-field)**
  - Subset $F$ of $2^{\Omega}$ satisfying
    - Inclusion of $\Omega$
    - Closure under complement
    - Closure under countable union
    - Closure under countable intersection

- **Measure on $(\Omega,F)$**
  - Function $\mu$ from $F$ to $\mathbb{R}_{\geq 0}$
    - For each countable collection $\{X_i\}$ of pairwise disjoint sets of $F$, $\mu(\bigcup I X_i) = \Sigma \mu(X_i)$

- **(Sub-)probability measure**
  - Measure $\mu$ such that $\mu(\Omega) = 1$ ($\mu(\Omega) \leq 1$)

- **Sigma-field generated by $C \subseteq 2^{\Omega}$**
  - Smallest $\sigma$-field that includes $C$
Measure Theory

Why not \( F = 2^\Omega \)?

Flip a fair coin infinitely many times

\( \Omega = \{h,t\}^\infty \)

\( \mu(\omega) = 0 \) for each \( \omega \in \Omega \)

\( \mu(\text{first coin } h) = 1/2 \)

Theorem: there is no probability measure on \( 2^\Omega \) such that \( \mu(\omega) = 0 \) for each \( \omega \in \Omega \).
Cones and Measures

• **Cone of** $\alpha$
  - Set of executions with prefix $\alpha$
  - Represent event “$\alpha$ occurs”

• **Measure of a cone**
  - Product edges of $\alpha$

---

**Theorem**

A measure on cones extends uniquely to a measure on the $\sigma$-field generated by cones.
Examples of Events

• Eventually action $a$ occurs
  - Union of cones where action $a$ occurs once

• Action $a$ occurs at least $n$ times
  - Union of cones where action $a$ occurs $n$ times

• Action $a$ occurs at most $n$ times
  - Complement of action $a$ occurs at least $n+1$ times

• Action $a$ occurs exactly $n$ times
  - Intersection of previous two events

• Action $a$ occurs infinitely many times
  - Intersection of action $a$ occurs at least $n$ times for all $n$

• Execution $\alpha$ occurs and nothing is scheduled after
  - Set consisting of $\alpha$ only
  - $C_\alpha$ intersected complement of cones that extend $\alpha$
Scheduler - Resolution of nondeterminism

**Scheduler**

**Function**

\[ \sigma : \text{exec}^*(A) \rightarrow Q \times (E \cup H) \times \text{Disc}(Q) \]

\[
\text{if } \sigma(\alpha) = (q,a,\nu) \text{ then } q = \text{lstate}(\alpha)
\]

**Probabilistic execution**

**generated by** \( \sigma \) **from state** \( r \)

**Measure**

\[
\mu_{\sigma,r}(C_s) = 0 \quad \text{if} \quad r \neq s
\]

\[
\mu_{\sigma,r}(C_r) = 1
\]

\[
\mu_{\sigma,r}(C_{\alpha aq}) = \mu_{\sigma,r}(C_{\alpha}) \cdot \nu(q) \quad \text{if} \quad \sigma(\alpha) = (q,a,\nu)
\]
Probabilistic CCS

\[ P :: = 0 \mid P|P \mid \alpha.P \mid P + P \mid (\nu \alpha) P \]

\[ \mid X \mid \text{let } X = P \text{ in } X \mid P\oplus_p P \]

**Prefix**

\[ \alpha.P \xrightarrow{\alpha} \delta(P) \]

**Nondeterministic process**

\[ P \xrightarrow{\alpha} \mu \]

\[ P + Q \xrightarrow{\alpha} \mu \]

**Probabilistic processes**

\[ P_1 \oplus_p P_2 \xrightarrow{\tau} p\mu_1 + (1-p)\mu_2 \]
Probabilistic CCS

Interleaving

\[ \frac{P \xrightarrow{\alpha} \mu}{P|Q \xrightarrow{\alpha} \mu|Q} \]

Hiding

\[ \frac{P \xrightarrow{\alpha} \mu}{(va) \ \mu} \quad \alpha \neq a, \hat{a} \]

Communication

\[ \frac{P_1 \xrightarrow{a} \delta(P'_2) \quad P_2 \xrightarrow{\hat{a}} \delta(P'_2)}{P_1|P_2 \xrightarrow{\tau} \delta(P'_2 | P'_2)} \]

Recursion

\[ \frac{P \xrightarrow{[ \text{let } X = P \text{ in } X / X ] \ x} \mu}{\text{let } X = P \text{ in } X \xrightarrow{\alpha} \mu} \]
Bisimulation Relations

We have the following objectives

• They should extend the corresponding relations in the non probabilistic case

• Keep definitions simple

• Where are the key differences?
Strong Bisimulation on Automata

Strong bisimulation between $A_1$ and $A_2$

Relation $R \subseteq Q \times Q$, $Q = Q_1 \cup Q_2$, such that

$\forall q, s, a, q' \exists s'$

$R$
Strong Bisimulation on Probabilistic Automata

Strong bisimulation between $A_1$ and $A_2$

Relation $R \subseteq Q \times Q$, $Q = Q_1 \cup Q_2$, such that

$\forall C \in Q/R$. $\mu(C) = \mu'(C)$

[LS89]
Probabilistic Bisimulations

- These two Probabilistic Automata are not bisimilar

- Yet they satisfy the same formulas of a logic PCTL
  - The logic observes probability bounds on reachability properties
- Bisimilar if we match transitions with convex combinations of transitions
Weak Bisimulation on Automata

Weak bisimulation between $A_1$ and $A_2$

Relation $R \subseteq Q \times Q$, $Q=Q_1 \cup Q_2$, such that

\[
\forall q, s, a, q' \exists s' \ni \forall q, s, a, q' \exists s' \ni q \xrightarrow{a} q' \quad R \quad s \xrightarrow{a} s' \quad R
\]

\[
s \Rightarrow^a s' \quad \iff \quad \exists \alpha: \text{trace}(\alpha)=a, \text{fstate}(\alpha)=s, \text{lstate}(\alpha)=s'
\]
Weak bisimulation between $A_1$ and $A_2$

Relation $R \subseteq Q \times Q$, $Q = Q_1 \cup Q_2$, such that

\[ \forall q, s, a, \mu \exists \mu' \]

\[ \mu R \mu' \quad \text{[LS89]} \]

\[ \forall C \in Q/R. \mu(C) = \mu'(C) \]
Weak Transition

There is a probabilistic execution $\mu$ such that

- $\mu(\text{exec}^*) = 1$ (it is finite)
- $\text{trace}(\mu) = \delta(a)$ (its trace is $a$)
- $\text{fstate}(\mu) = \delta(q)$ (it starts from $q$)
- $\text{lstate}(\mu) = \rho$ (it leads to $\rho$)

$q \xrightarrow{a} s \iff \exists \alpha: \text{trace}(\alpha) = a, \text{fstate}(\alpha) = q, \text{lstate}(\alpha) = s$
Exercises

• Prove that the probabilistic CCS is an extension of CCS (to define what this means is part of the exercise)
• Prove that probabilistic bisimulation is an extension of bisimulation
• Write the Lehmann-Rabin algorithm in probabilistic CCS (without using guarded choice)