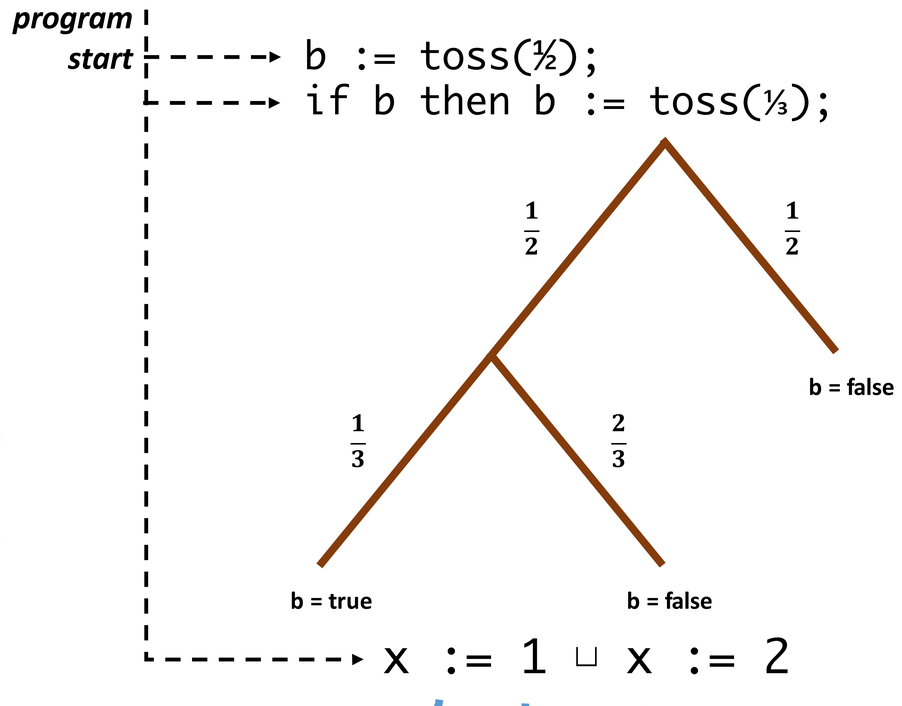
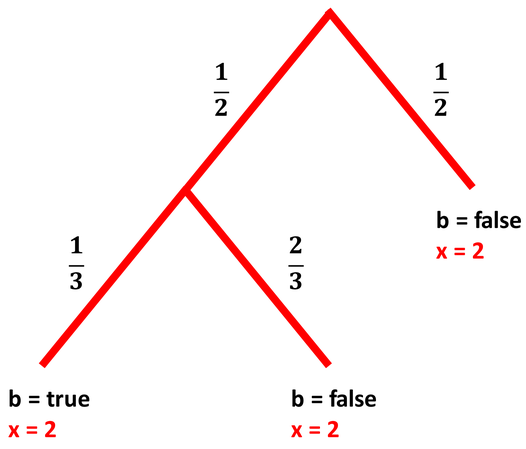
Verifying Probabilistic Programs in the Presence of an Adversary

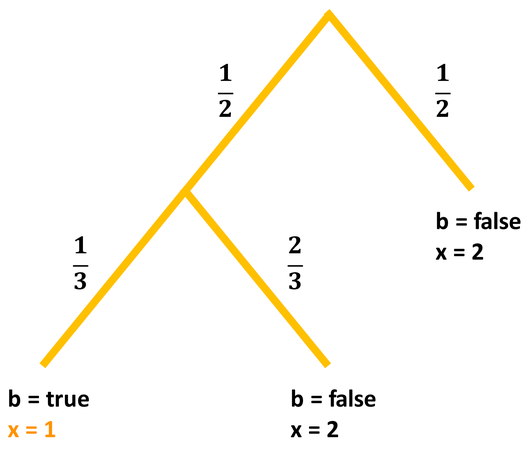
Robert Rand
University of Pennsylvania

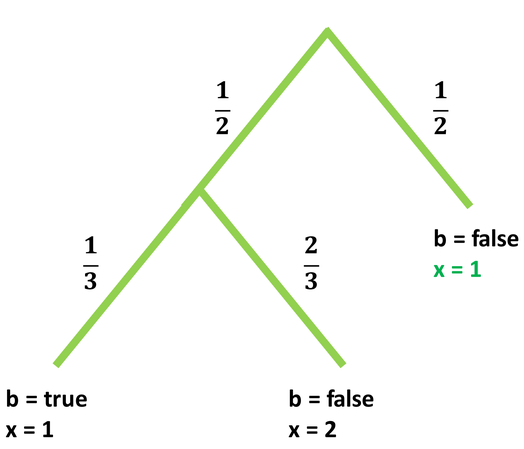
Adversary Strength

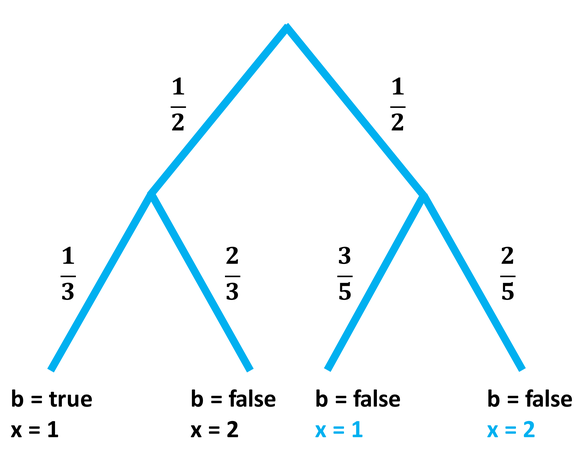
1. Adversary knows the program structure
2. Adversary knows the current program state
3. Adversary knows the program history
4. Adversary knows the full program execution (single source of random bits)
5. Adversary knows the full program execution (command specific bits)












```
if b then c else c
↛
c
```

```
x := toss(½); y := 1 ⊔ 2
↛
y := 1 ⊔ 2; x := toss(½)
```

```
x := toss(½); x = true
↛
x = true
```

```
x, y := toss(½)
↛
y, x := toss(½)
```
4

```
c ⊔ c
↛
c
```
5

Hoare Rules

$$\frac{\{P\}\ c_1\ \{Q_1\} \qquad \{P\}\ c_2\ \{Q_2\}}{\{P\}\ \ c_1 \sqcup c_2\ \ \{Q_1 \vee Q_2\}}\ 1$$

$$\frac{\{P\}\ c_1\ \{Q\}\ \begin{matrix} NP\ P \\ ND\ Q \end{matrix}\ \{P\}\ c_2\ \{Q\}}{\{P\}\ c_1 \sqcup c_2\ \{Q\}}\ 2\ 3$$

$$\frac{\{P\}\ c_1\ \{Q\}\ \ Det\ Q\ \ \{P\}\ c_2\ \{Q\}}{\{P\}\ c_1 \sqcup c_2\ \{Q\}}\ 4\ 5$$

* NP = Non-probabilistic. ND = Non-disjunctive. Det = NP and ND