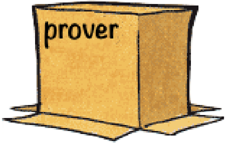
Models for Probabilistic Programs with an Adversary

Robert Rand, Steve Zdancewic

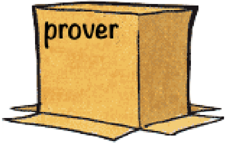
University of Pennsylvania

Probabilistic Programming Semantics 2016

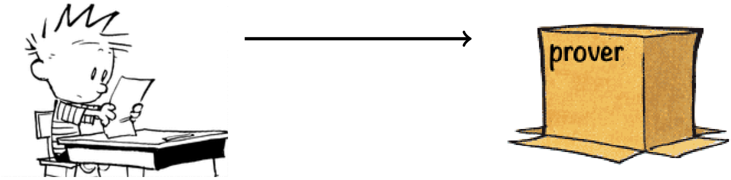
Interactive Proofs



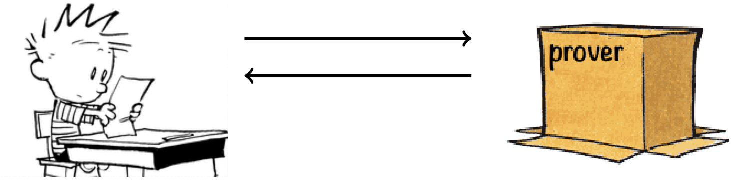
Interactive Proofs



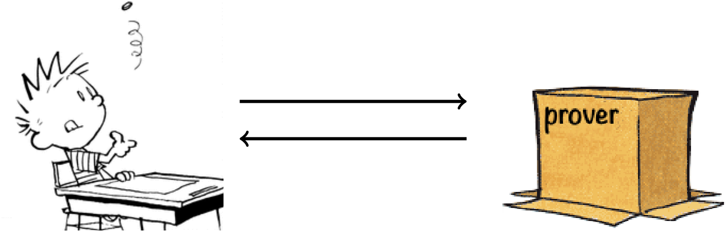
Interactive Proofs



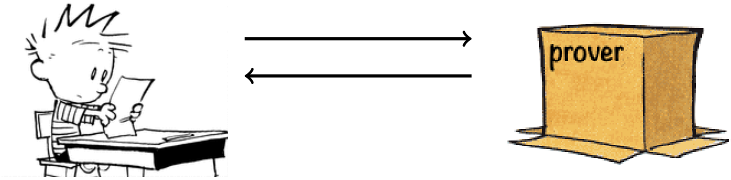
Interactive Proofs



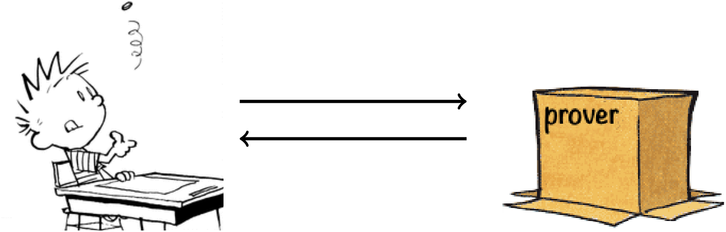
Interactive Proofs



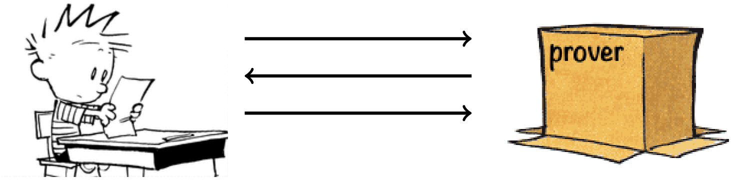
Interactive Proofs



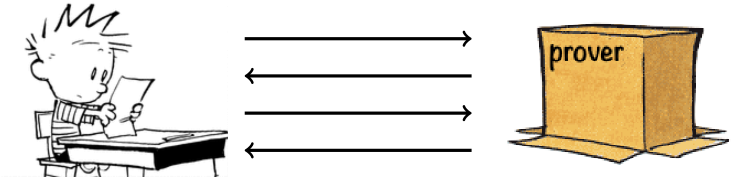
Interactive Proofs



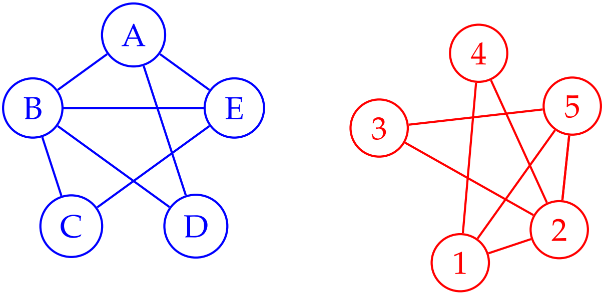
Interactive Proofs



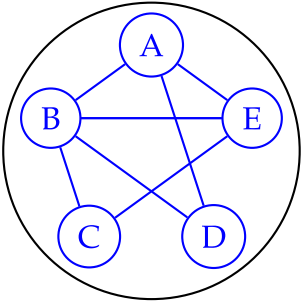
Interactive Proofs

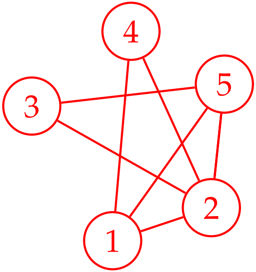


Graph Non-Isomorphism

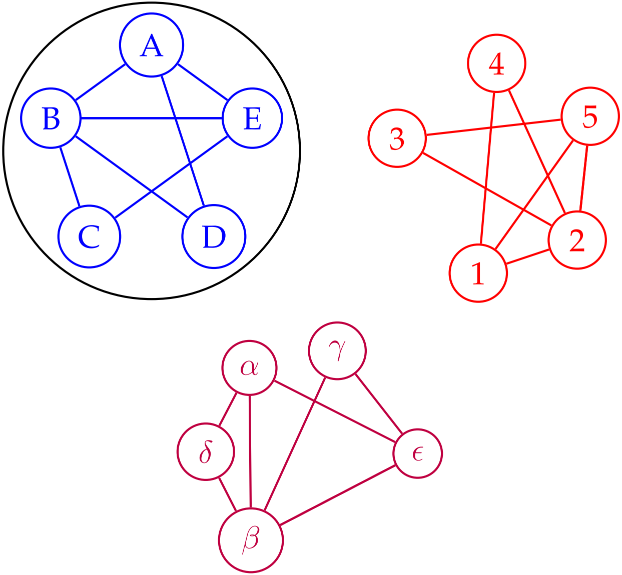


Graph Non-Isomorphism

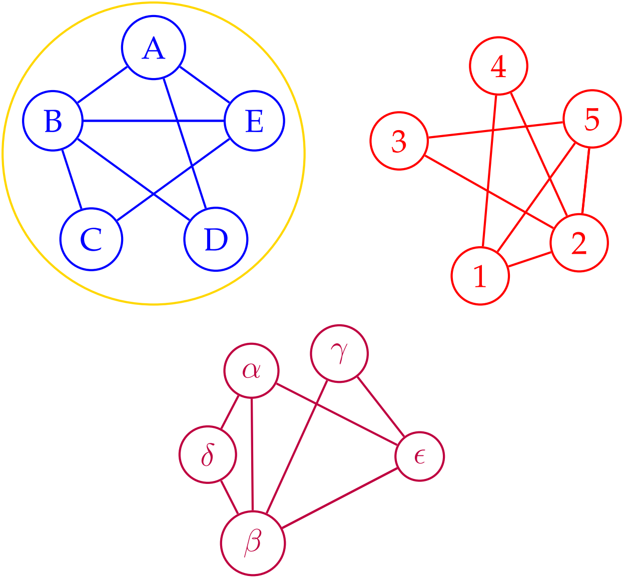




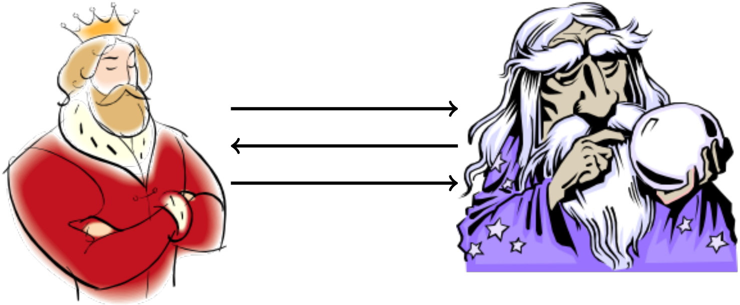
Graph Non-Isomorphism



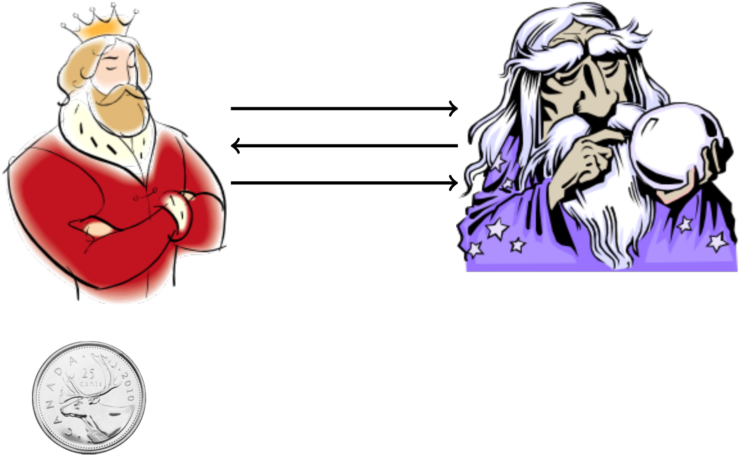
Graph Non-Isomorphism



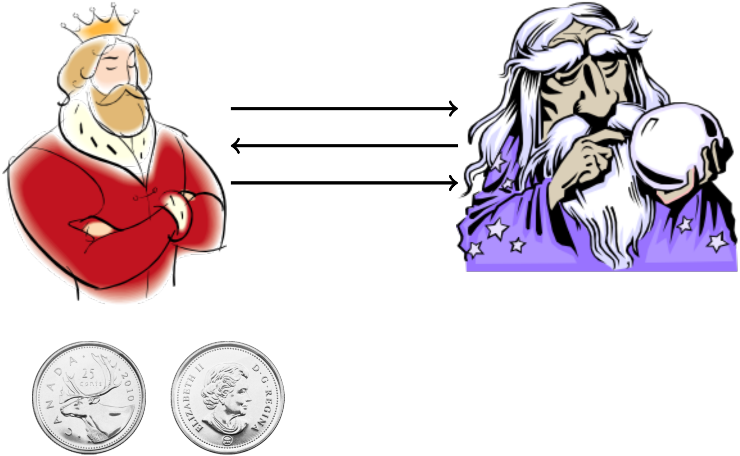
Arthur Merlin Games



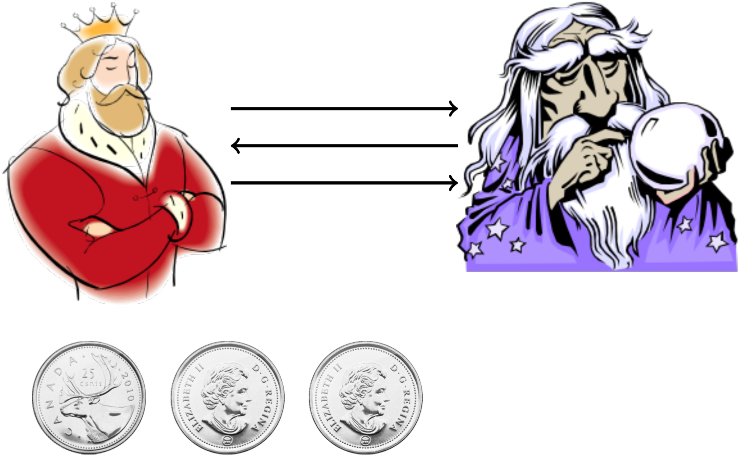
Arthur Merlin Games



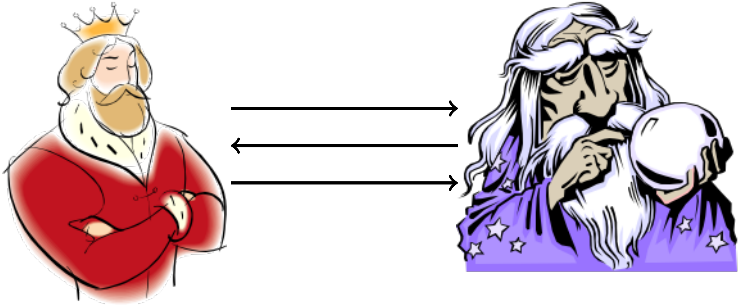
Arthur Merlin Games



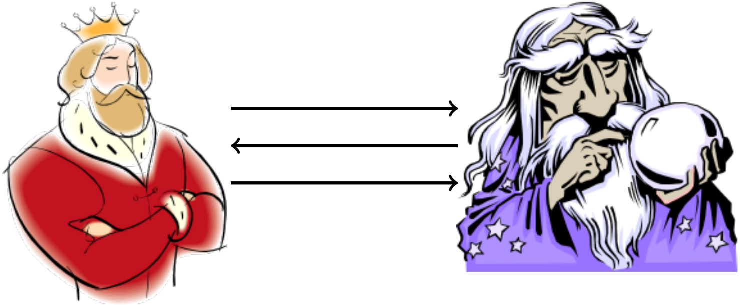
Arthur Merlin Games



Arthur Merlin Games



Arthur Merlin Games



Why Should We Care?

- Mixing probability and nondeterminism is powerful.
- Private vs. public coins matter.

Let's Start with a Deterministic Semantics...

$$\frac{}{\texttt{skip} \ / \ \sigma \Downarrow \sigma} \qquad \frac{\sigma(a) = n}{x \ \texttt{:=} \ a \ / \ \sigma \Downarrow \sigma[x \mapsto n]}$$

$$\frac{c_1 \ / \ \sigma \Downarrow \sigma' \qquad c_2 \ / \ \sigma' \Downarrow \sigma''}{c_1; c_2 \ / \ \sigma \Downarrow \sigma''}$$

$$\frac{\sigma(b) = \texttt{T} \qquad c_1 \ / \ \sigma \Downarrow \sigma'}{\texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2 \ / \ \sigma \Downarrow \sigma'}$$

For Point Distributions

$$\boxed{\Theta ::= [\sigma] \mid \Theta \oplus_p \Theta}$$

$$\frac{}{\texttt{skip} \;/\; [\sigma] \Downarrow [\sigma]} \qquad \frac{[\sigma](a) = n}{x \texttt{ := } a \;/\; [\sigma] \Downarrow [\sigma[x \mapsto n]]}$$

$$\frac{c_1 \;/\; [\sigma] \Downarrow \Theta \qquad c_2 \;/\; \Theta \Downarrow \Theta'}{c_1; c_2 \;/\; [\sigma] \Downarrow \Theta'}$$

$$\frac{\sigma(b) = \texttt{T} \qquad c_1 \;/\; [\sigma] \Downarrow \Theta}{\texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \;/\; [\sigma] \Downarrow \Theta}$$

Toss in Some Probability

$$\boxed{\Theta ::= [\sigma] \mid \Theta \oplus_p \Theta}$$

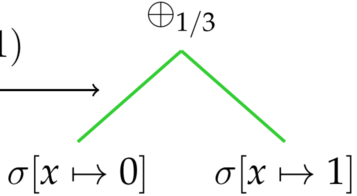
$$\frac{c_1 \ / \ [\sigma] \Downarrow \Theta_1 \qquad c_2 \ / \ [\sigma] \Downarrow \Theta_2}{(c_1 \ \oplus_p \ c_2) \ / \ [\sigma] \Downarrow \Theta_1 \oplus_p \Theta_2}$$

Toss in Some Probability

$$\boxed{\Theta ::= [\sigma] \mid \Theta \oplus_p \Theta}$$

$$\frac{c_1 \;/\; [\sigma] \Downarrow \Theta_1 \qquad c_2 \;/\; [\sigma] \Downarrow \Theta_2}{(c_1 \;\oplus_p\; c_2) \;/\; [\sigma] \Downarrow \Theta_1 \oplus_p \Theta_2}$$

$$[\sigma] \xrightarrow{\quad (x \;:=\; 0 \;\oplus_{\frac{1}{3}}\; x \;:=\; 1) \quad}$$

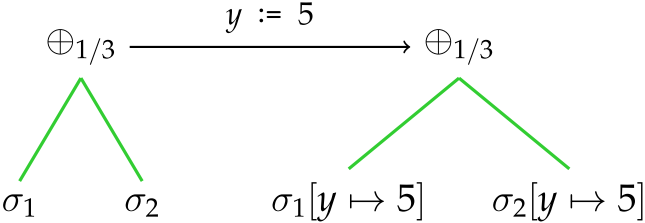


And Lift!

$$\frac{c \;/\; \Theta_1 \Downarrow \Theta_1' \qquad c \;/\; \Theta_2 \Downarrow \Theta_2'}{c \;/\; \Theta_1 \oplus_p \Theta_2 \Downarrow \Theta_1' \oplus_p \Theta_2'}$$

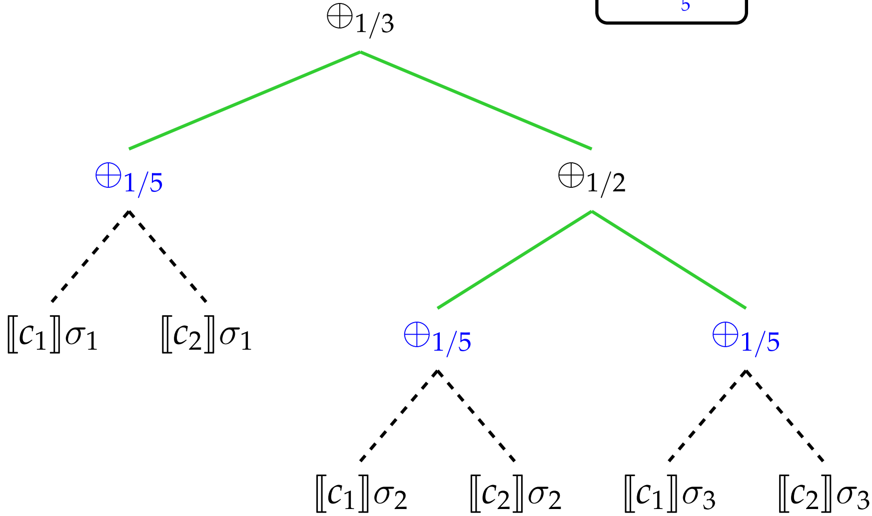
And Lift!

$$\frac{c \;/\; \Theta_1 \Downarrow \Theta_1' \qquad c \;/\; \Theta_2 \Downarrow \Theta_2'}{c \;/\; \Theta_1 \oplus_p \Theta_2 \Downarrow \Theta_1' \oplus_p \Theta_2'}$$

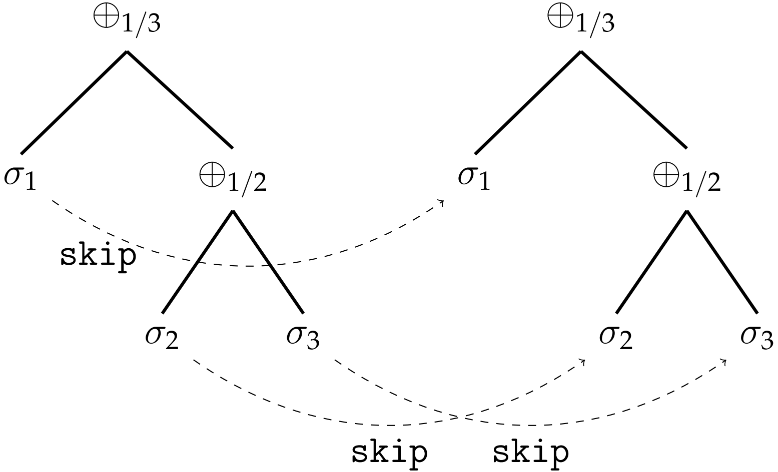


The Toss Command

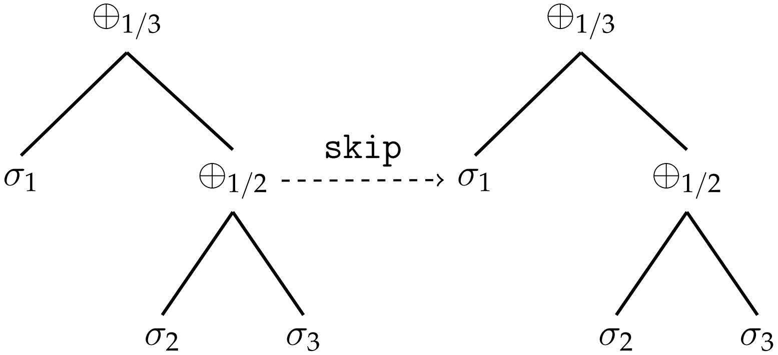
$$\boxed{c_1 \oplus_{\frac{1}{5}} c_2}$$



The Skip Command



More Direct



$\oplus_{1/3}$
σ_1
$\oplus_{1/2}$
σ_2
σ_3
skip
$\oplus_{1/3}$
σ_1
$\oplus_{1/2}$
σ_2
σ_3

Direct Semantics

$$\frac{}{\texttt{skip} \;/\; \Theta \Downarrow \Theta} \qquad \frac{\sigma(a) = n}{x \;\texttt{:=}\; a \;/\; \Theta \Downarrow \Theta[\sigma_i(x) \mapsto n]}$$

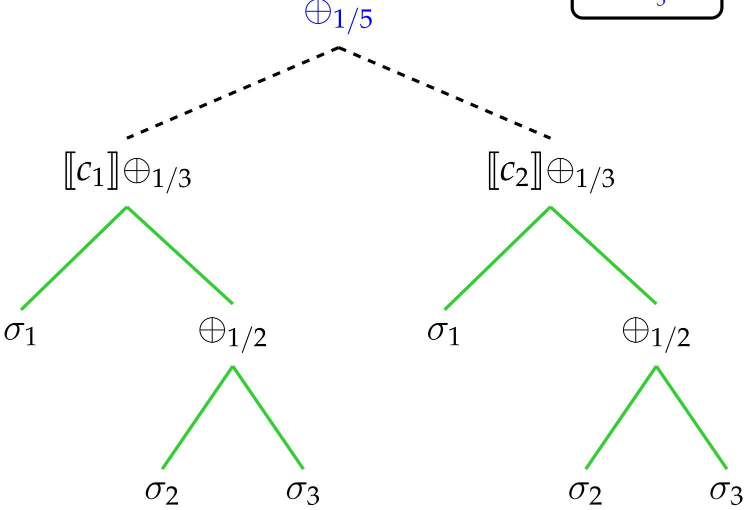
$$\frac{c_1 \;/\; \Theta \Downarrow \Theta' \qquad c_2 \;/\; \Theta' \Downarrow \Theta''}{c_1; c_2 \;/\; \Theta \Downarrow \Theta''}$$

$$\frac{Pr_b(\Theta_1) = 1 \quad c_1 \;/\; \Theta_1 \Downarrow \Theta_1' \qquad c_2 \;/\; \Theta_0 \Downarrow \Theta_0' \quad Pr_b(\Theta_0) = 0}{\texttt{if}\; b \;\texttt{then}\; c_1 \;\texttt{else}\; c_2 \;/\; \Theta_1 \oplus_p \Theta_0 \Downarrow \Theta_1' \oplus_p \Theta_0'}$$

$$\frac{c_1 \;/\; \Theta \Downarrow \Theta_1 \qquad c_2 \;/\; \Theta \Downarrow \Theta_2}{(c_1 \;\oplus_p\; c_2) \;/\; \Theta \Downarrow \Theta_1 \oplus_p \Theta_2}$$

Direct Toss

$\boxed{c_1 \oplus_{\frac{1}{5}} c_2}$



The Distinction

Recursive

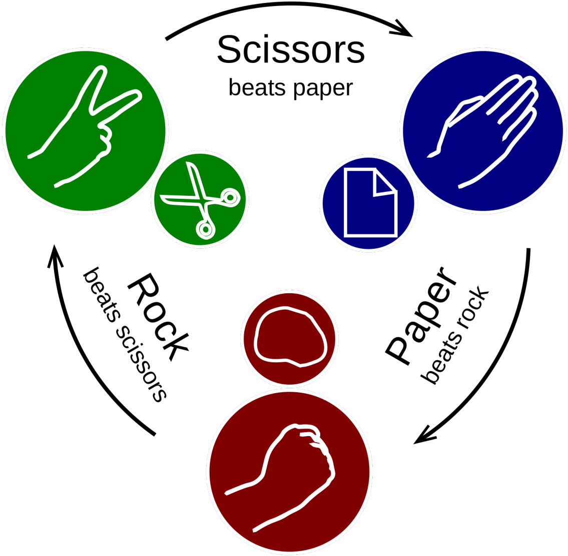
$$\frac{c_1 \;/\; [\sigma] \Downarrow \Theta_1}{(c_1 \;\sqcup\; c_2) \;/\; [\sigma] \Downarrow \Theta_1} \qquad \frac{c_2 \;/\; [\sigma] \Downarrow \Theta_2}{(c_1 \;\sqcup\; c_2) \;/\; [\sigma] \Downarrow \Theta_2}$$

vs.

$$\frac{c_1 \;/\; \Theta \Downarrow \Theta_1}{(c_1 \;\sqcup\; c_2) \;/\; \Theta \Downarrow \Theta_1} \qquad \frac{c_2 \;/\; \Theta \Downarrow \Theta_2}{(c_1 \;\sqcup\; c_2) \;/\; \Theta \Downarrow \Theta_2}$$

Direct

Let's Play a Game!



Let's Play a Game!

$P :=$  $\oplus_{\frac{1}{3}}$ $\big($  $\oplus_{\frac{1}{2}}$  $\big)$

$O :=$  $\sqcup$  $\sqcup$ 

Let's Play a Game!

c_1 $\quad P :=$  $\oplus_{\frac{1}{3}}$ ( $\oplus_{\frac{1}{2}}$ )

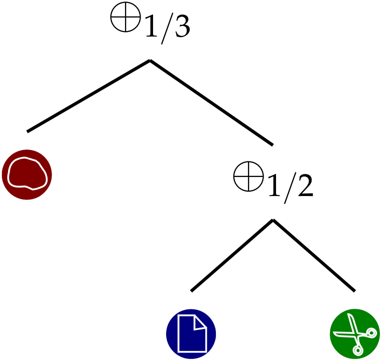
c_2 $\quad O :=$  $\sqcup$  $\sqcup$ 

Direct Play

c_1 : $P :=$  $\oplus_{\frac{1}{3}}$ ( $\oplus_{\frac{1}{2}}$ )

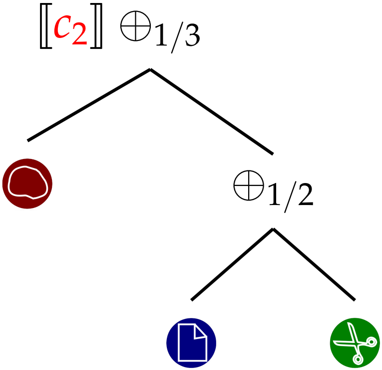
Direct Play

$c_1 : P :=$  $\oplus_{\frac{1}{3}}$ ( $\oplus_{\frac{1}{2}}$ )



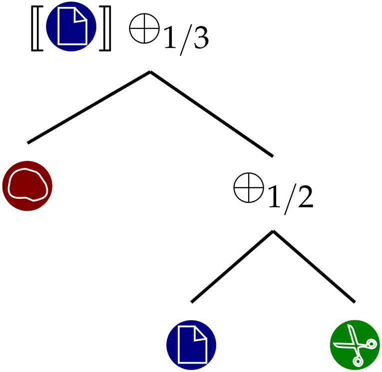
Direct Play

$c_2 : O :=$ 



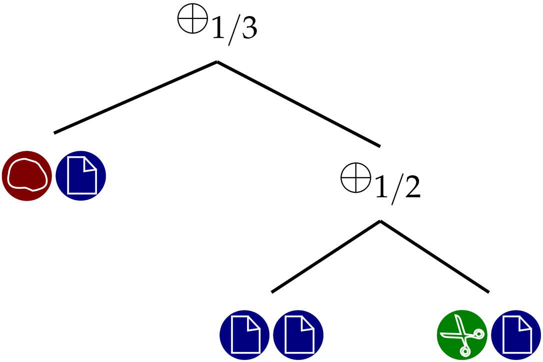
Direct Play

$c_2 : O :=$ 



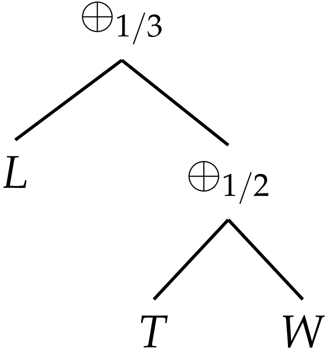
Direct Play

$c_2 : O :=$ 
$\sqcup$
$\sqcup$



Direct Play

$c_2 : O :=$  $\sqcup$  $\sqcup$ 

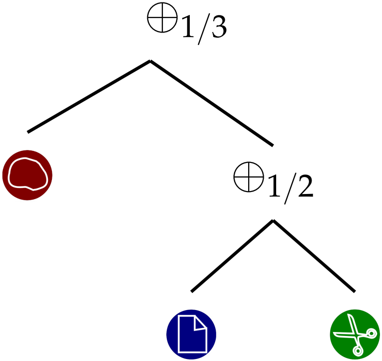


Recursive Play

c_1 : P:=  $\oplus_{\frac{1}{3}}$ ( $\oplus_{\frac{1}{2}}$ )

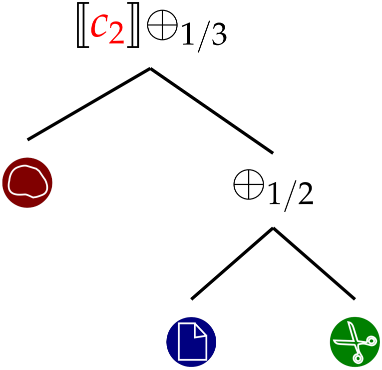
Recursive Play

c_1 : $P :=$  $\oplus_{\frac{1}{3}}$ ( $\oplus_{\frac{1}{2}}$ )



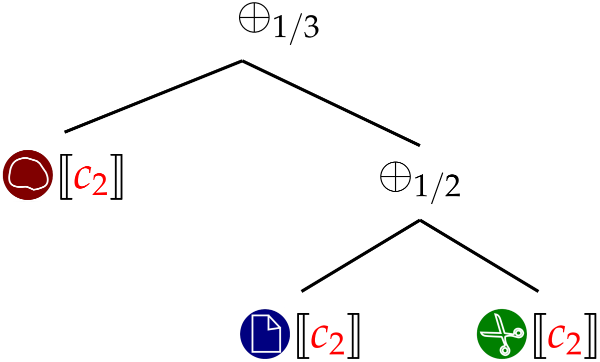
Recursive Play

$c_2 : O :=$ 



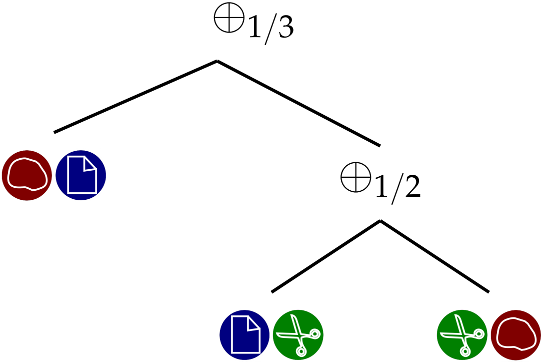
Recursive Play

$c_2 : O :=$ ⊔ ⊔



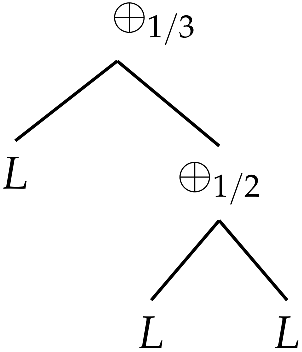
Recursive Play

$c_2 : O :=$ 



Recursive Play

$c_2 : O :=$ ⊔ ⊔



Knowledge

The two levels of operational semantics reflect whether the adversary knows the outcome of coin flips.

Levels of Knowledge

1. Adversary is blind to probabilistic outcomes.
   - Single choice in $((c_1 \sqcup c_2) \oplus (c_1 \sqcup c_2))$
   - Distinct choices in $((c_1 \sqcup c_2) \oplus (c_1 \sqcup c_2))$ (Direct)
2. Adversary can see current program state
3. Adversary recalls program history (Recursive)
4. Adversary can foresee all outcomes.
   - Single coin flip in $((c_1 \oplus c_2) \sqcup (c_1 \oplus c_2))$
   - Distinct coin flips in $((c_1 \oplus c_2) \sqcup (c_1 \oplus c_2))$

Levels of Knowledge

1. Adversary is blind to probabilistic outcomes.
   - Single choice in $((c_1 \sqcup c_2) \oplus (c_1 \sqcup c_2))$
   - Distinct choices in $((c_1 \sqcup c_2) \oplus (c_1 \sqcup c_2))$ (Direct)
2. Adversary can see current program state
3. Adversary recalls program history (Recursive)
4. Adversary can foresee all outcomes.
   - Single coin flip in $((c_1 \oplus c_2) \sqcup (c_1 \oplus c_2))$
   - Distinct coin flips in $((c_1 \oplus c_2) \sqcup (c_1 \oplus c_2))$

Levels of Knowledge

1. Adversary is blind to probabilistic outcomes.
   - Single choice in $((c_1 \sqcup c_2) \oplus (c_1 \sqcup c_2))$
   - Distinct choices in $((c_1 \sqcup c_2) \oplus (c_1 \sqcup c_2))$ (Direct)
2. Adversary can see current program state
3. Adversary recalls program history (Recursive)
4. Adversary can foresee all outcomes.
   - Single coin flip in $((c_1 \oplus c_2) \sqcup (c_1 \oplus c_2))$
   - Distinct coin flips in $((c_1 \oplus c_2) \sqcup (c_1 \oplus c_2))$

Levels of Knowledge

1. Adversary is blind to probabilistic outcomes.
   - Single choice in $((c_1 \sqcup c_2) \oplus (c_1 \sqcup c_2))$
   - Distinct choices in $((c_1 \sqcup c_2) \oplus (c_1 \sqcup c_2))$ (Direct)
2. Adversary can see current program state
3. Adversary recalls program history (Recursive)
4. Adversary can foresee all outcomes.
   - Single coin flip in $((c_1 \oplus c_2) \sqcup (c_1 \oplus c_2))$
   - Distinct coin flips in $((c_1 \oplus c_2) \sqcup (c_1 \oplus c_2))$

So...

What can we verify?

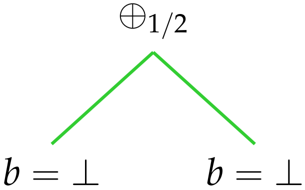
Verification: Direct

$$\frac{\{P\}\ c_1\ \{Q\} \qquad \{P\}\ c_2\ \{Q\}}{\{P\}\ (c_1 \sqcup c_2)\ \{Q\}}$$

Verification: Recursive

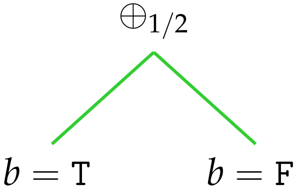
$$\frac{\{True\}\ b\ \mathtt{:=}\ \mathtt{T}\ \{Pr(b) = 1\} \qquad \{True\}\ b\ \mathtt{:=}\ \mathtt{F}\ \{Pr(b) = 0\}}{\{True\}\ (b\ \mathtt{:=}\ \mathtt{T} \sqcup b\ \mathtt{:=}\ \mathtt{F})\ \{Pr(b) = 1 \vee Pr(b) = 0\}}$$

Verification: Recursive



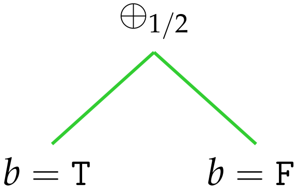
$$\frac{\{True\}\ b\ \texttt{:=}\ \texttt{T}\ \{Pr(b) = 1\} \qquad \{True\}\ b\ \texttt{:=}\ \texttt{F}\ \{Pr(b) = 0\}}{\{True\}\ (b\ \texttt{:=}\ \texttt{T} \sqcup b\ \texttt{:=}\ \texttt{F})\ \{Pr(b) = 1 \vee Pr(b) = 0\}}$$

Verification: Recursive



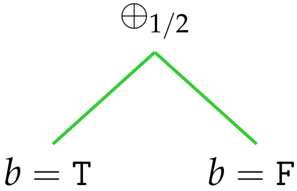
$$\frac{\{True\}\ b \ \mathtt{:=}\ \mathtt{T}\ \{Pr(b) = 1\} \qquad \{True\}\ b \ \mathtt{:=}\ \mathtt{F}\ \{Pr(b) = 0\}}{\{True\}\ (b \ \mathtt{:=}\ \mathtt{T} \sqcup b \ \mathtt{:=}\ \mathtt{F})\ \{Pr(b) = 1 \vee Pr(b) = 0\}}$$

Verification: Recursive



$$\frac{\{True\}\ b\ \mathtt{:=}\ \mathtt{T}\ \{Pr(b) = 1\} \qquad \{True\}\ b\ \mathtt{:=}\ \mathtt{F}\ \{Pr(b) = 0\}}{\{True\}\ (b\ \mathtt{:=}\ \mathtt{T} \sqcup b\ \mathtt{:=}\ \mathtt{F})\ \{\color{red}{Pr(b) = 1 \vee Pr(b) = 0}\}}$$

Verification: Recursive



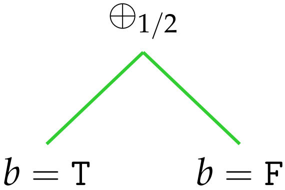
$$\frac{\{True\}\ b\ \mathtt{:=}\ \mathtt{T}\ \{Pr(b) = 1\} \qquad \{True\}\ b\ \mathtt{:=}\ \mathtt{F}\ \{Pr(b) = 0\}}{\{True\}\ (b\ \mathtt{:=}\ \mathtt{T} \sqcup b\ \mathtt{:=}\ \mathtt{F})\ \{\color{red}{Pr(b) = 1 \vee Pr(b) = 0}\}}$$

Q cannot include disjunctions

Verification: Recursive

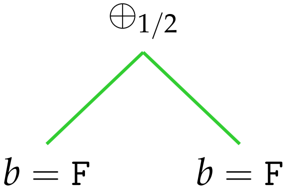
$$\frac{\{Pr(b) = \frac{1}{2}\}\ \texttt{skip}\ \{Pr(b) = \frac{1}{2}\} \qquad \{Pr(b) = \frac{1}{2}\}\ b\ \texttt{:=}\ \neg b\ \{Pr(b) = \frac{1}{2}\}}{\{Pr(b) = \frac{1}{2}\}\ (\texttt{skip} \sqcup b\ \texttt{:=}\ \neg b)\ \{Pr(b) = \frac{1}{2}\}}$$

Verification: Recursive



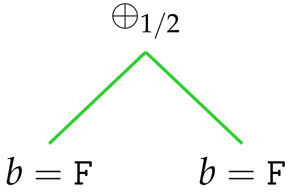
$$\frac{\{Pr(b) = \tfrac{1}{2}\}\ \mathtt{skip}\ \{Pr(b) = \tfrac{1}{2}\} \qquad \{Pr(b) = \tfrac{1}{2}\}\ b\ \mathtt{:=}\ \neg b\ \{Pr(b) = \tfrac{1}{2}\}}{\{Pr(b) = \tfrac{1}{2}\}\ (\mathtt{skip}\ \sqcup\ b\ \mathtt{:=}\ \neg b)\ \{Pr(b) = \tfrac{1}{2}\}}$$

Verification: Recursive



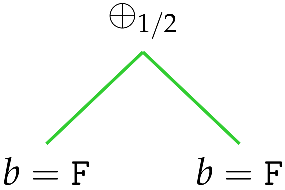
$$\frac{\{Pr(b) = \frac{1}{2}\}\ \mathtt{skip}\ \{Pr(b) = \frac{1}{2}\} \qquad \{Pr(b) = \frac{1}{2}\}\ b\ \mathtt{:=}\ \neg b\ \{Pr(b) = \frac{1}{2}\}}{\{Pr(b) = \frac{1}{2}\}\ (\mathtt{skip} \sqcup b\ \mathtt{:=}\ \neg b)\ \{Pr(b) = \frac{1}{2}\}}$$

Verification: Recursive



$$\frac{\{Pr(b) = \tfrac{1}{2}\}\ \mathtt{skip}\ \{Pr(b) = \tfrac{1}{2}\} \qquad \{Pr(b) = \tfrac{1}{2}\}\ b \mathrel{\mathtt{:=}} \neg b\ \{Pr(b) = \tfrac{1}{2}\}}{\{Pr(b) = \tfrac{1}{2}\}\ (\mathtt{skip} \sqcup b \mathrel{\mathtt{:=}} \neg b)\ \{Pr(b) = \tfrac{1}{2}\}}$$

Verification: Recursive



$$\frac{\{Pr(b) = \frac{1}{2}\}\ \mathtt{skip}\ \{Pr(b) = \frac{1}{2}\} \qquad \{Pr(b) = \frac{1}{2}\}\ b\ \mathtt{:=}\ \neg b\ \{Pr(b) = \frac{1}{2}\}}{\{{\color{red}Pr(b) = \frac{1}{2}}\}\ (\mathtt{skip} \sqcup b\ \mathtt{:=}\ \neg b)\ \{Pr(b) = \frac{1}{2}\}}$$

P cannot include probabilities in $(0, 1)$

Verification: Recursive

$$\frac{\{P\}\ c_1\ \{Q\} \qquad \begin{array}{c}\text{non-probabilistic } P \\ \text{non-disjunctive } Q\end{array} \qquad \{P\}\ c_2\ \{Q\}}{\{P\}\ (c_1 \sqcup c_2)\ \{Q\}}$$

Compositionality

$$(c_1 \;\sqcup\; c_2); (c_3 \;\sqcup\; c_4)$$

Compositionality

$$\{P\}\ (c_1 \ \sqcup \ c_2); (c_3 \ \sqcup \ c_4)\ \{R\}$$

Compositionality

$$\{P\}\ (c_1 \ \sqcup\ c_2)\ \{Q\}\ (c_3 \ \sqcup\ c_4)\ \{R\}$$

Compositionality

$$\{P\}\ (c_1 \ \sqcup \ c_2)\ \{Q\}\ (c_3 \ \sqcup \ c_4)\ \{R\}$$

Compositionality

non-probabilistic P
non-disjunctive Q

$$\{P\}\ (c_1 \sqcup c_2)\ \{Q\}\ (c_3 \sqcup c_4)\ \{R\}$$

Compositionality

non-probabilistic P
non-disjunctive Q

$$\{P\}\ (c_1\ \sqcup\ c_2)\ \{Q\}\ (c_3\ \sqcup\ c_4)\ \{R\}$$

Compositionality

non-probabilistic P non-probabilistic Q
non-disjunctive Q non-disjunctive R

$$\{P\}\ (c_1 \ \sqcup \ c_2)\ \{Q\}\ (c_3 \ \sqcup \ c_4)\ \{R\}$$

Compositionality

non-probabilistic P non-probabilistic Q

non-disjunctive Q non-disjunctive R

$$\{P\}\ (c_1 \sqcup c_2)\ \{Q\}\ (c_3 \sqcup c_4)\ \{R\}$$

Are private coins applicable?

Theorem (Minimax Theorem)

For every two-person, zero-sum game with finitely many strategies, there exists a value V *and a mixed strategy for each player, such that*

1. Given player 2's strategy, the best payoff possible for player 1 is V*, and*

2. Given player 1's strategy, the best payoff possible for player 2 is $-V$*.*

Game Theory

- game $\Longleftrightarrow$ program with nondeterminism

Game Theory

- game $\iff$ program with nondeterminism
- zero sum $\iff$ returns a single value

Game Theory

- game $\iff$ program with nondeterminism
- zero sum $\iff$ returns a single value
- finitely many strategies $\iff$ no unbounded loops

Game Theory

- game $\iff$ program with nondeterminism
- zero sum $\iff$ returns a single value
- finitely many strategies $\iff$ no unbounded loops
- mixed strategy $\iff$ choice of p, q, r annotating the $\oplus$s

Game Theory

Theorem (Minimax Theorem Restated)

Any finite program combining probability and nondeterminism with a single output value has a dual program with the probabilistic and nondeterministic choices inverted, that returns the same value in the worst case.

Game Theory Questions

- Can we use this to find and prove Nash Equilibria in games?
- Does this yield useful generalizations of Nash Equilibrium?
- Can we discover useful compositionality results from this formulation?

More Open Questions

- How does a semantics using infinite bit streams compare to our distribution semantics?
- Can we enumerate the possible interactions between probability and nondeterminism via algebraic equivalences?
  - Can we extend KAT to probabilistic-nondeterministic programs?
- Can we translate between Direct and Recursive Semantics?

Questions?

Thank You

Questions?
Answers?

Questions?
Answers?
Rebuttals?