RWTH AACHEN UNIVERSITY

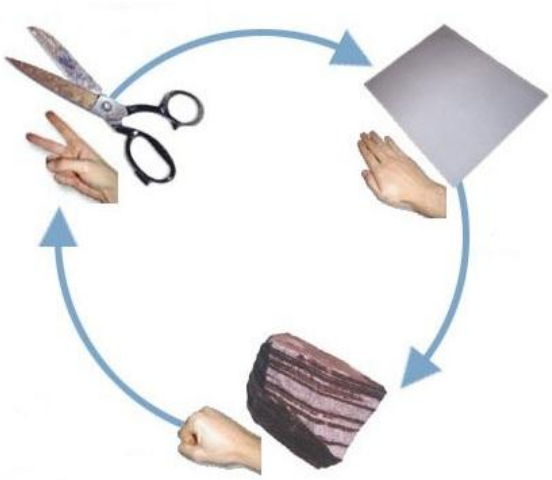
Operational Semantics for a probabilistic guarded command language

Friedrich Gretz

ROCKS meeting in Herrsching am Ammersee

06.10.2011

Motivation



Symmetry breaking,
Leader election...

Scheduling, Routing....

Security

RWTH AACHEN UNIVERSITY

Features:

- parameters
- loops
- inifinite-domain variables
- probabilistic **and** non-deterministic choice

Challenges

- cannot be handled by model checking

➡ use „logical inference“-based methods

A glimpse at denational semantics

- $wp.skip.f = f$
- $wp.abort.f = 0$
- $wp.(x \coloneqq A).f = f[x/A]$
- $wp.(prog_1; prog_2).f = wp.prog_1.(wp.prog_2.f)$
- $wp.(if(G)\ \{prog_1\}\ else\ \{prog_2\}).f =$

  $$[G] \cdot wp.prog_1.f + [\neg G] \cdot wp.prog_2.f$$
- $wp.(prog_1\ [p]\ prog_2).f =$

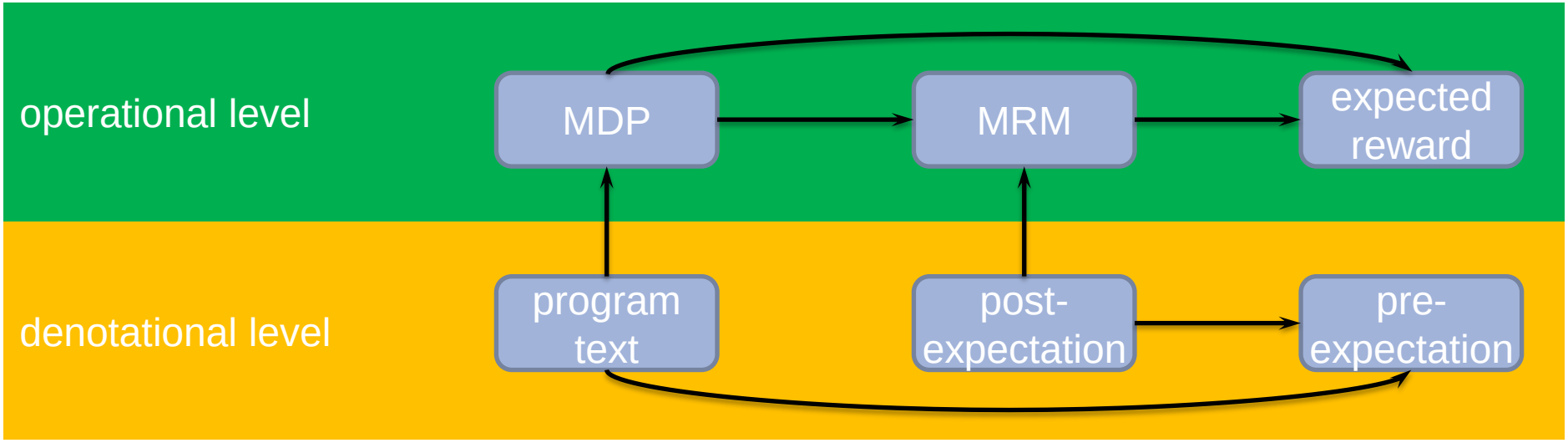
  $$p \cdot wp.prog_1.f + (1-p) \cdot wp.prog_2.f$$
- $wp.(prog_1\ [\,]\ prog_2).f = \min\{wp.prog_1.f,\ wp.prog_2.f\}$
- $wp.(while(G)\ \{prog\}).f =$ least expectation l such that

  $$l = [G] \cdot wp.prog_1.l + [\neg G] \cdot f$$

RWTH AACHEN UNIVERSITY

Questions:

- Howto describe a program‘s execution intuitively?
- What is the underlying σ-Algebra (Ω, A, P)?
- What is the meaning of post- and pre-expectations?



Developing operational semantics

$$\frac{}{\langle \mathbf{skip}, \eta \rangle \to \langle \varepsilon, \eta \rangle}$$

$$\frac{}{\langle x := y(x_1, \ldots, x_n), \eta \rangle \to \langle \varepsilon, \eta[x/y(x_1, \ldots, x_n)] \rangle}$$

$$\frac{}{\langle \mathbf{abort}, \eta \rangle \to \langle \mathbf{abort}, \eta \rangle}$$

$$\frac{}{\langle prog_1 [p] prog_2, \eta \rangle \xrightarrow{p} \langle prog_1, \eta \rangle \quad \langle prog_1 [p] prog_2, \eta \rangle \xrightarrow{1-p} \langle prog_2, \eta \rangle}$$

$$\frac{}{\langle prog_1 [] prog_2, \eta \rangle \xrightarrow{\alpha} \langle prog_1, \eta \rangle \quad \langle prog_1 [] prog_2, \eta \rangle \xrightarrow{\beta} \langle prog_2, \eta \rangle}$$

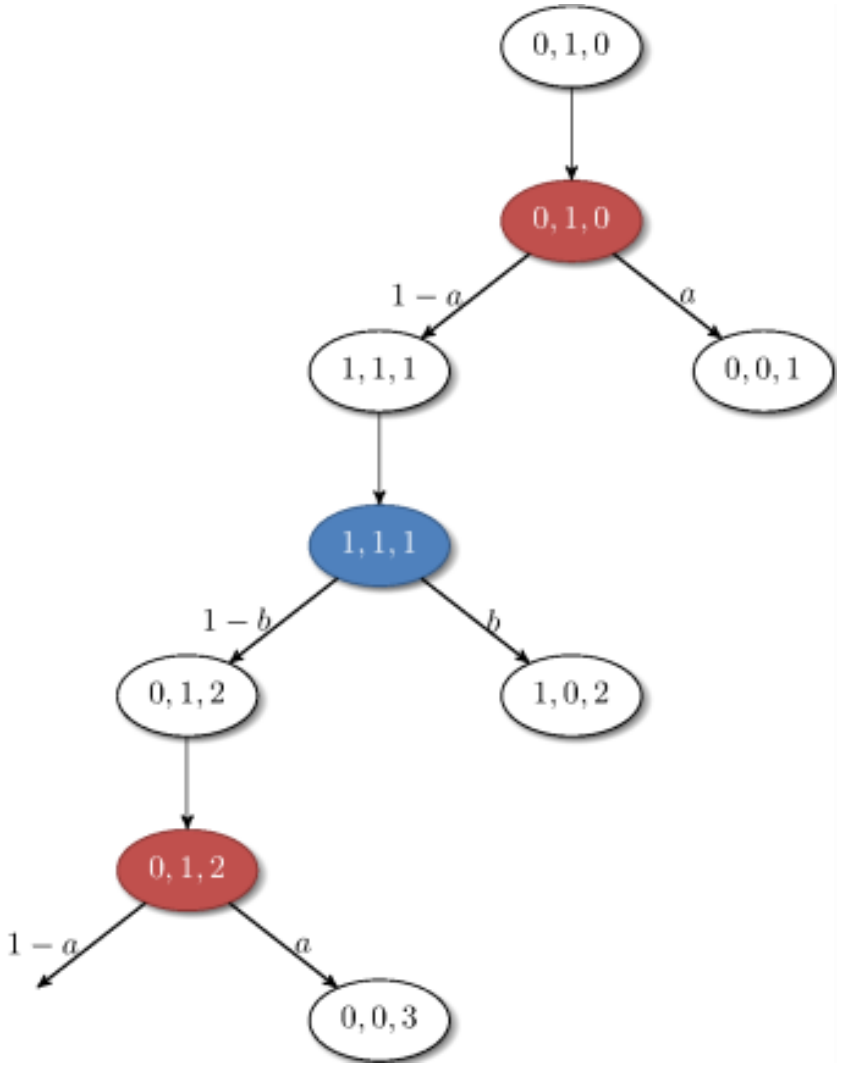
$$\frac{\langle prog_1, \eta \rangle \xrightarrow{\alpha,p} \langle prog_2, \eta' \rangle}{\langle prog_1; prog, \eta \rangle \xrightarrow{\alpha,p} \langle prog_2; prog, \eta' \rangle}$$

$$\frac{\eta \models G}{\langle \mathbf{if}(G)\{prog_1\}\mathbf{else}\{prog_2\}, \eta \rangle \to \langle prog_1, \eta \rangle} \qquad \frac{\eta \not\models G}{\langle \mathbf{if}(G)\{prog_1\}\mathbf{else}\{prog_2\}, \eta \rangle \to \langle prog_2, \eta \rangle}$$

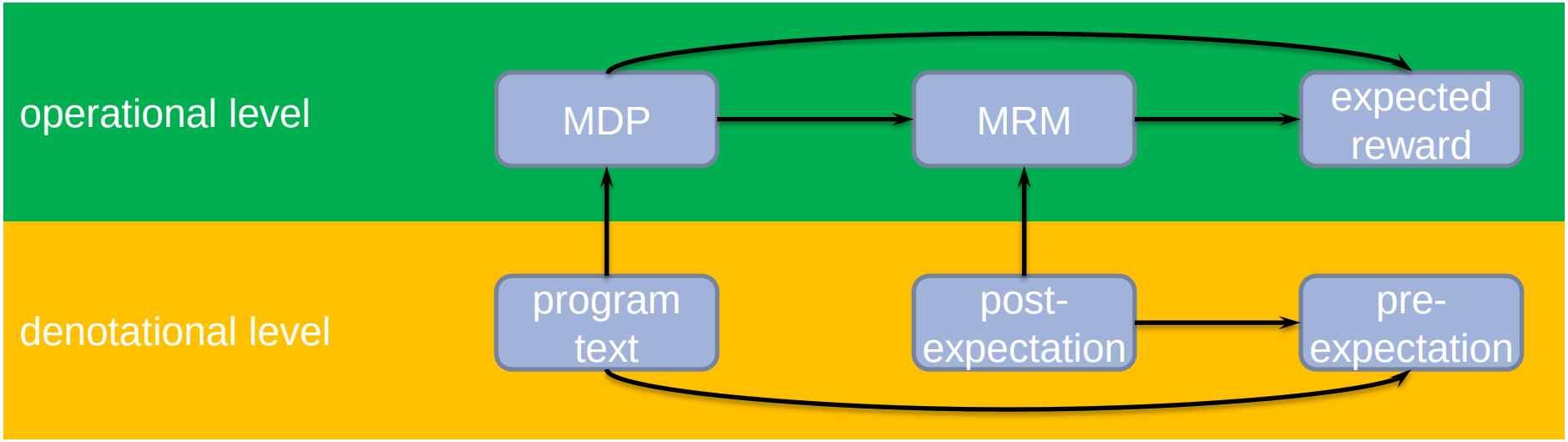
$$\frac{\eta \models G}{\langle \mathbf{while}(G)\{prog\}, \eta \rangle \to \langle prog; \mathbf{while}(G)\{prog\}, \eta \rangle} \qquad \frac{\eta \not\models G}{\langle \mathbf{while}(G)\{prog\}, \eta \rangle \to \langle \varepsilon, \eta \rangle}$$

Duelling cowboys [MM 04]

```
turn := 0;
continue := 1;
counter := 0;

while(continue){
  if(turn = 0){
    (continue := 0 [a] turn := 1);
  } else {
    (continue := 0 [b] turn := 0);
  }
  counter++;
}
```



Developing operational semantics



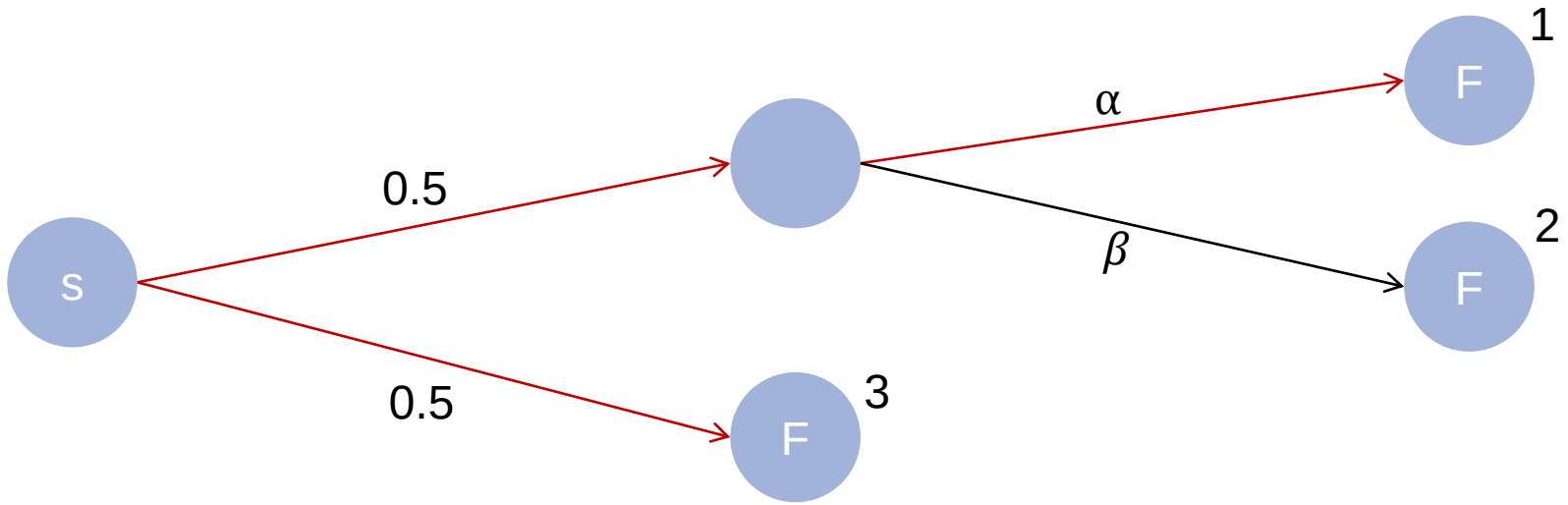
Define (state-)rewards on the MDP

$$rew(\langle prog, \eta \rangle) = \begin{cases} f(\eta) & \text{if } L(\langle prog, \eta \rangle) = \{F\} \\ 0 & \text{else} \end{cases}$$

Definition of Expected Reward on a MRM

$$ER(M, s, \Diamond F) = \min_{\mathfrak{S}} \sum_{r=0}^{\infty} r \cdot Pr\{\pi \in Paths^{\mathfrak{S}}(s) \mid \pi \models \Diamond F \wedge rew(\pi, \Diamond F) = r\}$$

M:

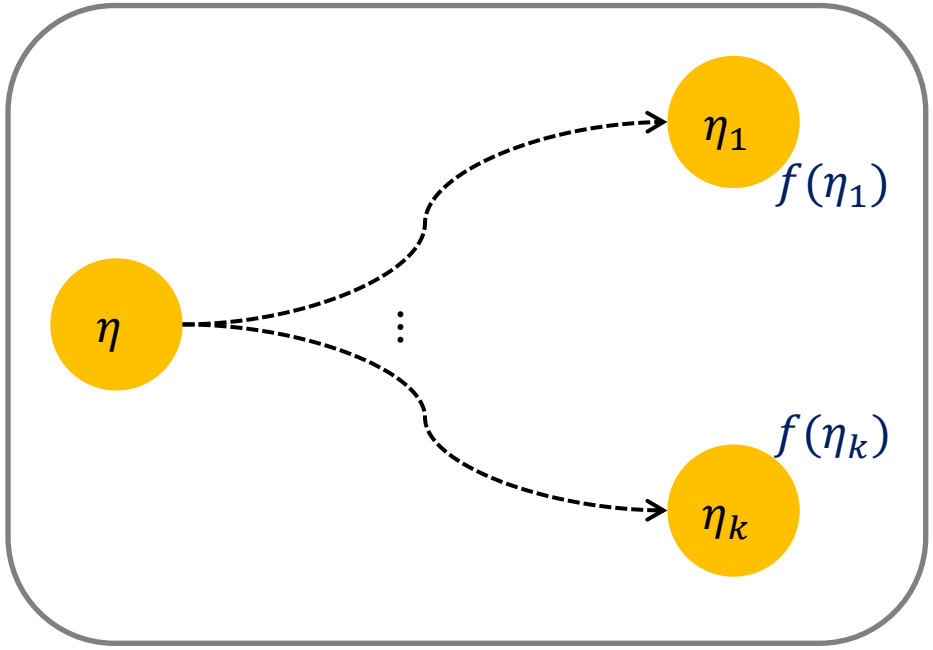


$$ER(M, s, \Diamond F) = 2$$

Equivalence theorem

Theorem (Equivalence)

$$wp.prog.f.\eta$$



$$= ER\left(M_{prog}, \langle prog, \eta \rangle, \Diamond F\right)$$

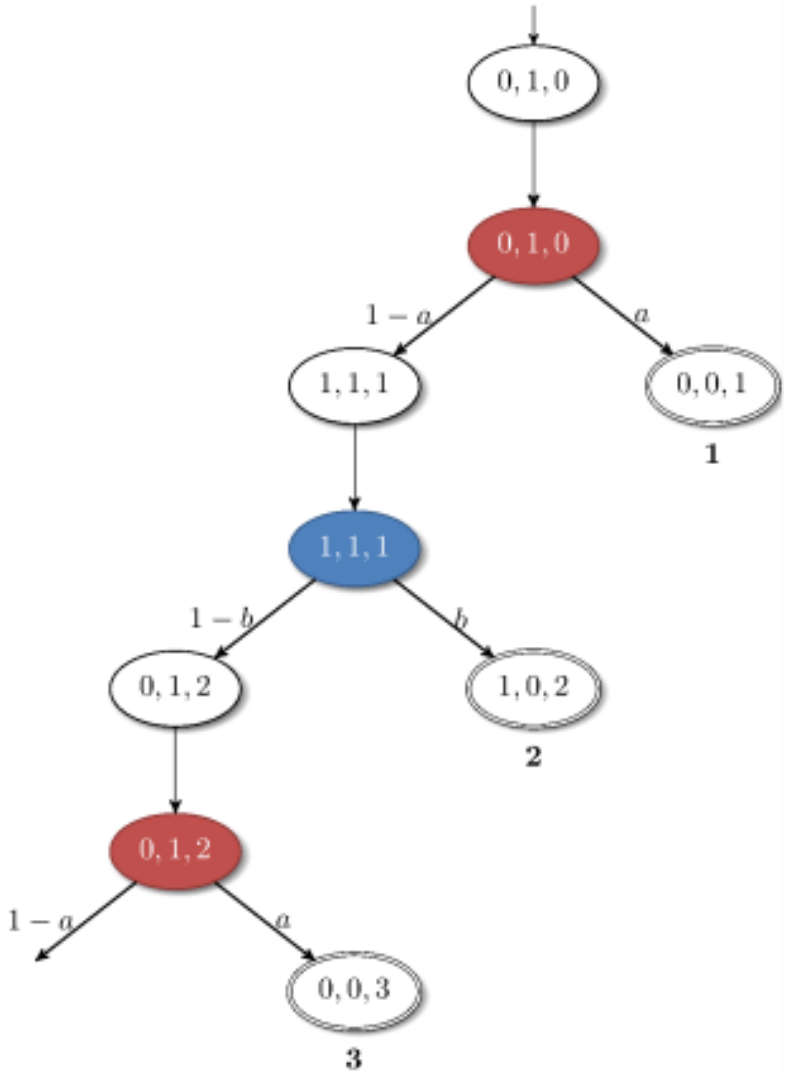
greatest **pre-**expectation *wp*
is a function on the **initial** states,
parameterised by

- a program
- a **post-**expectation (which depends on **final** states)

... corresponds to the *expected reward* gained along executions **from initial** states **to final** states

Duelling cowboys (revisited)

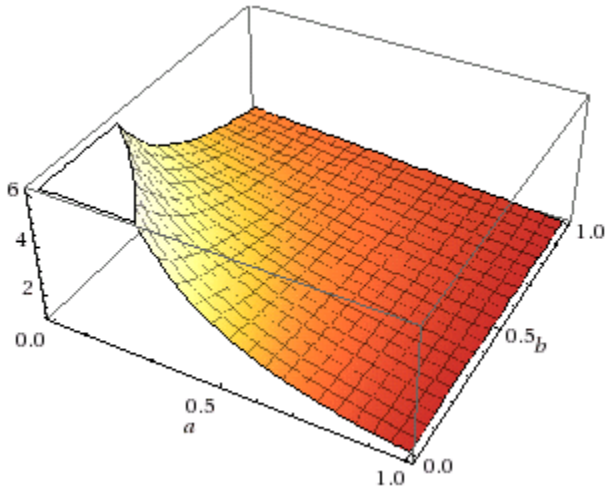
```
turn := 0;
continue := 1;
counter := 0;

while(continue){
  if(turn = 0){
    (continue := 0 [a] turn := 1);
  } else {
    (continue := 0 [b] turn := 0);
  }
  counter++;
}
```

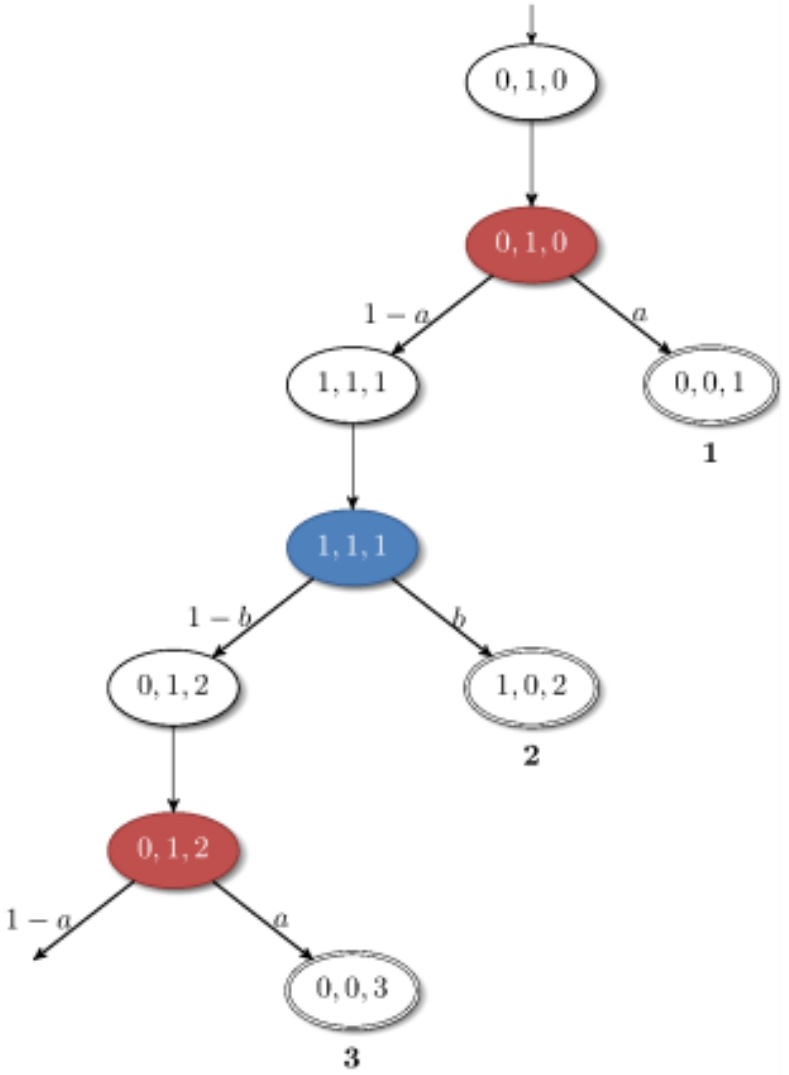


Duelling cowboys (revisited)

What is the expected duration?

$$wp.prog.counter.\langle 0,1,0\rangle$$
$$= ER\left(M_{prog}, \langle 0,1,0\rangle, \Diamond F\right)$$
$$= \ \ldots$$
$$= \frac{a-2}{ab-a-b}$$



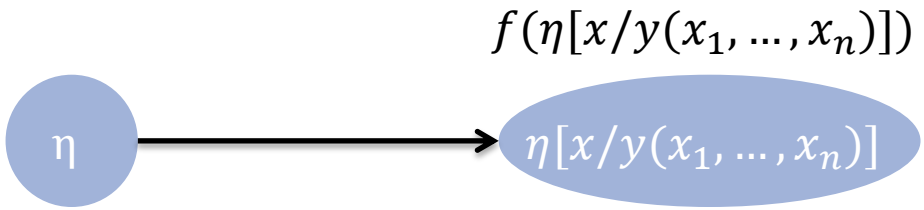


Proof of equivalence

Induction base:

$$wp.(x := y(x_1, \ldots, x_n).f.\eta = f.\eta[x/y(x_1, \ldots, x_n)]$$

$$\begin{aligned}
& ER(M_{x:=y(x_1,\ldots,x_n)}, \langle x := y(x_1, \ldots, x_n), \eta\rangle, \Diamond F) \\
= \quad & \min_{\mathfrak{S}} \sum_{r=0}^{\infty} r \cdot Pr\{\pi \in Paths^{\mathfrak{S}}(\langle x := y(x_1, \ldots, x_n), \eta\rangle) \mid \pi \models \Diamond F \wedge rew(\pi, \Diamond F) = r\} \\
= \quad & \ldots 0 \\
& \quad + f(\eta[x/y(x_1, \ldots, x_n)]) \cdot Pr\{\pi = \langle x := y(x_1, \ldots, x_n), \eta\rangle\langle \varepsilon, \eta[x/y(x_1, \ldots, x_n)]\rangle \models \Diamond F \\
& \qquad \wedge rew(\pi, \Diamond F) = f(\eta[x/y(x_1, \ldots, x_n)])\} \\
& \quad + 0 \ldots \\
= \quad & f(\eta[x/y(x_1, \ldots, x_n)]) \cdot 1 \\
= \quad & f(\eta[x/y(x_1, \ldots, x_n)])
\end{aligned}$$



analogously for **skip** and **abort**

Proof of equivalence

Induction hypothesis: *assume the theorem holds...*

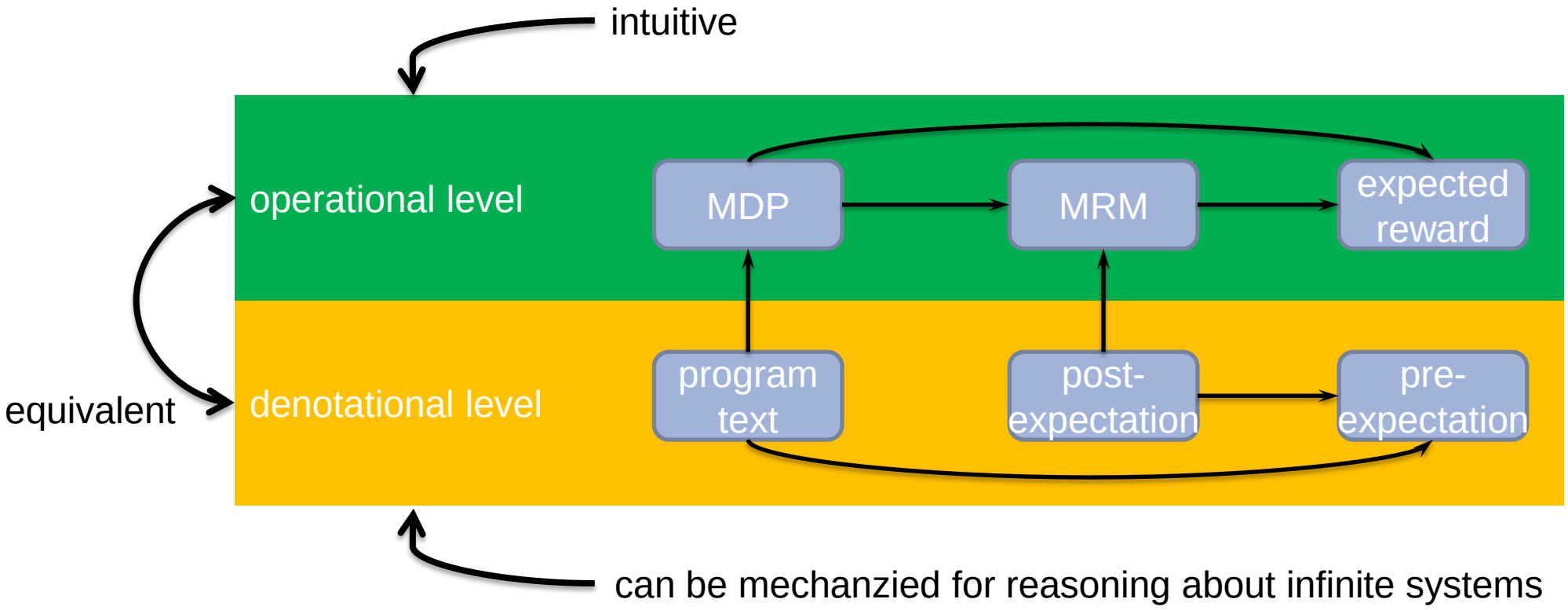
Induction step:

$$wp(prog_1[p]prog_2, f)(\eta) = p \cdot wp(prog_1, f)(\eta) + (1-p) \cdot wp(prog_2, f)(\eta)$$

$$\begin{aligned}
& ER(M_{prog_1[p]prog_2}, \langle prog_1[p]prog_2, \eta\rangle, \Diamond F) \\
= \quad & \min_{\mathfrak{S}} \sum_{r=0}^{\infty} r \cdot Pr\{\pi \in Paths^{\mathfrak{S}}(\langle prog_1[p]prog_2, \eta\rangle) \mid \pi \models \Diamond F \wedge rew(\pi, \Diamond F) = r\} \\
= \quad & \min_{\mathfrak{S}} \sum_{r=0}^{\infty} r \cdot (p \cdot Pr\{\pi \in Paths^{\mathfrak{S}}(\langle prog_1, \eta\rangle) \mid \pi \models \Diamond F \wedge rew(\pi, \Diamond F) = r\} \\
& \quad +(1-p) \cdot Pr\{\pi \in Paths^{\mathfrak{S}}(\langle prog_2, \eta\rangle) \mid \pi \models \Diamond F \wedge rew(\pi, \Diamond F) = r\}) \\
= \quad & p \cdot \min_{\mathfrak{S}_1} \sum_{r=0}^{\infty} r \cdot Pr\{\pi \in Paths^{\mathfrak{S}_1}(\langle prog_1, \eta\rangle) \mid \pi \models \Diamond F \wedge rew(\pi, \Diamond F) = r\} \\
& \quad +(1-p) \cdot \min_{\mathfrak{S}_2} \sum_{r=0}^{\infty} r \cdot Pr\{\pi \in Paths^{\mathfrak{S}_2}(\langle prog_2, \eta\rangle) \mid \pi \models \Diamond F \wedge rew(\pi, \Diamond F) = r\} \\
\overset{I.H.}{=} \quad & p \cdot ER(M_{prog_1}, \langle prog_1, \eta\rangle, \Diamond F) + (1-p) \cdot ER(M_{prog_2}, \langle prog_2, \eta\rangle, \Diamond F)
\end{aligned}$$

analogously for nondeterministic choice, sequential composition, if...then...else, while

Summary



- A similar result can be established between wlp-semantics and conditional expected rewards
- Furthermore we could allow real valued expectations and/or program variables

Outlook

- semantics were just one issue of a broad research field
- we do invariant generation
- contact me if interested ☺