

# Probabilistic Program Analysis

## Demonstration `pWhile`

Alessandra Di Pierro  
University of Verona, Italy  
[alessandra.dipierro@univr.it](mailto:alessandra.dipierro@univr.it)

Herbert Wiklicky  
Imperial College London, UK  
[herbert@doc.ic.ac.uk](mailto:herbert@doc.ic.ac.uk)

## Structure and Convention of Tool

For an extended version of the probabilistic language `PWHILE` we have a tool which constructs the **DTMC generator**, i.e. `LOS`, for any program in the language.

We also need **declarations** of the finite ranges of each variable (allowing also for arrays) and we have random assignments as well as choices.

**Conventions:** Computational (probabilistic) states (as well as configurations) are represented by **row** vectors/distributions  $\mathbf{p}$ . We use **post**-multiplication  $\mathbf{pT} = \mathbf{p}'$ .

# Randomised Counting

## Example

### Randomised Counting

```

[c := 1]1; [i := 0]2;
while [c > 0]3 do
  [choose]4  $\frac{1}{2} : [i := i + 1]$ 5 or  $\frac{1}{2} : [c := 0]$ 6 ro
od;
[skip]7

```

### Semantics

$$\begin{aligned}
 \llbracket P \rrbracket = \{ & \mathbf{F}_1 \otimes \mathbf{E}(1, 2), \mathbf{F}_2 \otimes \mathbf{E}(2, 3), \\
 & \mathbf{P}(c > 0) \otimes \mathbf{E}(3, 4), \mathbf{P}(c > 0)^\perp \otimes \mathbf{E}(3, 7), \\
 & 0.5 \cdot \mathbf{I} \otimes \mathbf{E}(4, 5), 0.5 \cdot \mathbf{I} \otimes \mathbf{E}(4, 6), \\
 & \mathbf{F}_5 \otimes \mathbf{E}(5, 3), \mathbf{F}_6 \otimes \mathbf{E}(6, 3), \\
 & \mathbf{I} \otimes \mathbf{E}(7, 7) \}
 \end{aligned}$$

### DTMC Generator

$$\mathbf{T}(P) = \mathbf{U}(c := 1) \otimes \mathbf{E}(1, 2) + \mathbf{U}(i := 0) \otimes \mathbf{E}(2, 3) +$$

$$\mathbf{P}(c > 0) \otimes \mathbf{E}(3, 4) + \mathbf{P}(c > 0)^\perp \otimes \mathbf{E}(3, 7) +$$

# Implementation for Finite Loops

```
var
c : {0, 1};
i : {0..10};

begin
c := 1;
i := 0;
while ( ( i < 10 ) && ( c > 0 ) ) do
  choose 1: i := i+1 or 1: c := 0 ro;
od;
stop;
end
```

State Space:  $\mathcal{V}(\{0, 1\}) \otimes \mathcal{V}(\{0, \dots, 10\}) \otimes \mathcal{V}(\{1, \dots, 7\}) = \mathbb{R}^{154}$

## Demo: Counting up to 3

Bounding the counting loop by 3 ...

```
while ( ( i < 3 ) && ( c > 0 ) ) do
  choose 1: i := i+1 or 1: c := 0 ro;
...
```

State Space:  $\mathcal{V}(\{0, 1\}) \otimes \mathcal{V}(\{0, \dots, 3\}) \otimes \mathcal{V}(\{1, \dots, 7\}) = \mathbb{R}^{56}$

Enumeration of states (in tensor product)

1	...	$c \mapsto 0, i \mapsto 0$	5	...	$c \mapsto 1, i \mapsto 0$
2	...	$c \mapsto 0, i \mapsto 1$	6	...	$c \mapsto 1, i \mapsto 1$
3	...	$c \mapsto 0, i \mapsto 2$	7	...	$c \mapsto 1, i \mapsto 2$
4	...	$c \mapsto 0, i \mapsto 3$	8	...	$c \mapsto 1, i \mapsto 3$

# Monty Hall

## Monty Hall – Stick $H_t$

```
var
  d :{0,1,2}; g :{0,1,2}; o :{0,1,2};
begin
  d ?= {0,1,2}; # Pick winning door
  g ?= {0,1,2}; # Pick guessed door
  o ?= {0,1,2}; # Open empty door
  while ((o == g) || (o == d)) do
    o := (o+1)%3; od;
  # Stick with guess
  stop; # looping
end
```

## Monty Hall – Stick $H_t$

```
var
  d :{0,1,2};   g :{0,1,2};   o :{0,1,2};
begin
  [d ?= {0,1,2}]1;
  [g ?= {0,1,2}]2;
  [o ?= {0,1,2}]3;
  while [(o == g) || (o == d)]4 do
    [o := (o+1)%3]5;
  od;
  [stop]6;
end
```

## Monty Hall $H_t$ – Blocks and Flow

$$\begin{aligned} \text{blocks}(H_t) &= \\ &= \{ [d ?= \{0, 1, 2\}]^1, [g ?= \{0, 1, 2\}]^2, \\ &\quad [o ?= \{0, 1, 2\}]^3, [((o == g) || (o == d))]^4, \\ &\quad [o := ((o + 1) \% 3)]^5, [stop]^6 \} \end{aligned}$$

$$\begin{aligned} \text{flow}(H_t) &= \\ &= \{(1, 1, 2), (2, 1, 3), (3, 1, 4), (4, 1, \underline{5}), (5, 1, 4), (4, 1, 6), (6, 1, 6)\} \end{aligned}$$

## Monty Hall – Stick $H_t$

$$\begin{aligned} \mathbf{T}(H_t) = & \frac{1}{3} (\mathbf{U}(d \leftarrow 0) + \mathbf{U}(d \leftarrow 1) + \mathbf{U}(d \leftarrow 2)) \otimes \mathbf{E}(1,2) + \\ & \frac{1}{3} (\mathbf{U}(g \leftarrow 0) + \mathbf{U}(g \leftarrow 1) + \mathbf{U}(g \leftarrow 2)) \otimes \mathbf{E}(2,3) + \\ & \frac{1}{3} (\mathbf{U}(o \leftarrow 0) + \mathbf{U}(o \leftarrow 1) + \mathbf{U}(o \leftarrow 2)) \otimes \mathbf{E}(3,4) + \\ & \mathbf{P}((o == g) || (o == d) = \mathbf{tt}) \otimes \mathbf{E}(4,5) + \\ & \mathbf{P}((o == g) || (o == d) = \mathbf{ff}) \otimes \mathbf{E}(4,6) + \\ & \mathbf{I} \otimes \mathbf{E}(6,6) \end{aligned}$$

## Monty Hall – Switch $H_w$

```
var
  d : {0,1,2}; g : {0,1,2}; o : {0,1,2};
begin
  d := {0,1,2}; # Pick winning door
  g := {0,1,2}; # Pick guessed door
  o := {0,1,2}; # Open empty door
  while ((o == g) || (o == d)) do
    o := (o+1)%3; od;
  g := (g+1)%3; # Switch guess
  while (g == o) do
    g := (g+1)%3; od;
  stop; # looping
end
```

## Monty Hall – Switch $H_w$

```
var
  d :{0,1,2};   g :{0,1,2};   o :{0,1,2};
begin
  [d ?= {0,1,2}]1;
  [g ?= {0,1,2}]2;
  [o ?= {0,1,2}]3;
  while [((o == g) || (o == d))]4 do
    [o := (o+1)%3]5;
  od;
  [g := (g+1)%3]6;
  while [(g == o)]7 do
    [g := (g+1)%3]8;
  od;
  [stop]9;
end
```

## Monty Hall $H_t$ – Blocks and Flow

$$\begin{aligned} \text{blocks}(H_w) &= \\ &= \{ [d ?= \{0, 1, 2\}]^1, [g ?= \{0, 1, 2\}]^2, \\ &\quad [o ?= \{0, 1, 2\}]^3, [((o == g) || (o == d))]^4, \\ &\quad [o := ((o + 1) \% 3)]^5, [g := ((g + 1) \% 3)]^6, \\ &\quad [(g == o)]^7, [g := ((g + 1) \% 3)]^8, [stop]^9 \} \end{aligned}$$

$$\begin{aligned} \text{flow}(H_w) &= \\ &= \{ (1, 1, 2), (2, 1, 3), (3, 1, 4), (4, 1, \underline{5}), (5, 1, 4), (4, 1, 6), \\ &\quad (6, 1, 7), (7, 1, \underline{8}), (8, 1, 7), (7, 1, 9), (9, 1, 9) \} \end{aligned}$$

## Monty Hall – Switch $H_w$

$$\begin{aligned}
 \mathbf{T}(H_w) = & \frac{1}{3} (\mathbf{U}(d \leftarrow 0) + \mathbf{U}(d \leftarrow 1) + \mathbf{U}(d \leftarrow 2)) \otimes \mathbf{E}(1, 2) + \\
 & \frac{1}{3} (\mathbf{U}(g \leftarrow 0) + \mathbf{U}(g \leftarrow 1) + \mathbf{U}(g \leftarrow 2)) \otimes \mathbf{E}(2, 3) + \\
 & \frac{1}{3} (\mathbf{U}(o \leftarrow 0) + \mathbf{U}(o \leftarrow 1) + \mathbf{U}(o \leftarrow 2)) \otimes \mathbf{E}(3, 4) + \\
 & \mathbf{P}((o == g) || (o == d) = \mathbf{tt}) \otimes \mathbf{E}(4, 5) + \\
 & \mathbf{P}((o == g) || (o == d) = \mathbf{ff}) \otimes \mathbf{E}(4, 6) + \\
 & \mathbf{U}(g \leftarrow (g + 1)\%3) \otimes \mathbf{E}(6, 7) + \\
 & \mathbf{P}((g == o) = \mathbf{tt}) \otimes \mathbf{E}(7, 8) + \\
 & \mathbf{P}((g == o) = \mathbf{ff}) \otimes \mathbf{E}(7, 9) + \\
 & \mathbf{U}(g \leftarrow (g + 1)\%3) \otimes \mathbf{E}(6, 7) + \mathbf{I} \otimes \mathbf{E}(9, 9)
 \end{aligned}$$

## Monty Hall – Enumeration

1	...	(d ↦ 0, g ↦ 0, o ↦ 0)	15	...	(d ↦ 1, g ↦ 1, o ↦ 2)
2	...	(d ↦ 0, g ↦ 0, o ↦ 1)	16	...	(d ↦ 1, g ↦ 2, o ↦ 0)
3	...	(d ↦ 0, g ↦ 0, o ↦ 2)	17	...	(d ↦ 1, g ↦ 2, o ↦ 1)
4	...	(d ↦ 0, g ↦ 1, o ↦ 0)	18	...	(d ↦ 1, g ↦ 2, o ↦ 2)
5	...	(d ↦ 0, g ↦ 1, o ↦ 1)	19	...	(d ↦ 2, g ↦ 0, o ↦ 0)
6	...	(d ↦ 0, g ↦ 1, o ↦ 2)	20	...	(d ↦ 2, g ↦ 0, o ↦ 1)
7	...	(d ↦ 0, g ↦ 2, o ↦ 0)	21	...	(d ↦ 2, g ↦ 0, o ↦ 2)
8	...	(d ↦ 0, g ↦ 2, o ↦ 1)	22	...	(d ↦ 2, g ↦ 1, o ↦ 0)
9	...	(d ↦ 0, g ↦ 2, o ↦ 2)	23	...	(d ↦ 2, g ↦ 1, o ↦ 1)
10	...	(d ↦ 1, g ↦ 0, o ↦ 0)	24	...	(d ↦ 2, g ↦ 1, o ↦ 2)
11	...	(d ↦ 1, g ↦ 0, o ↦ 1)	25	...	(d ↦ 2, g ↦ 2, o ↦ 0)
12	...	(d ↦ 1, g ↦ 0, o ↦ 2)	26	...	(d ↦ 2, g ↦ 2, o ↦ 1)
13	...	(d ↦ 1, g ↦ 1, o ↦ 0)	27	...	(d ↦ 2, g ↦ 2, o ↦ 2)
14	...	(d ↦ 1, g ↦ 1, o ↦ 1)			











# Monty Hall – $\mathbf{T}(H_s)$ and $\mathbf{T}(H_s)$

$$\mathbf{T}(H_t) = \mathbf{T}(1,2) + \mathbf{T}(2,3) + \mathbf{T}(3,4) + \mathbf{T}(4,\underline{5}) + \mathbf{T}(5,4) + \mathbf{T}(4,6) + \mathbf{I} \otimes \mathbf{E}(6,6)$$

$$\mathbf{T}(H_w) = \mathbf{T}(1,2) + \mathbf{T}(2,3) + \mathbf{T}(3,4) + \mathbf{T}(4,\underline{5}) + \mathbf{T}(5,4) + \mathbf{T}(4,6) + \mathbf{T}(6,7) + \mathbf{T}(7,\underline{8}) + \mathbf{T}(8,7) + \mathbf{T}(7,9) + \mathbf{I} \otimes \mathbf{E}(9,9)$$

$$\dim(\mathbf{T}(H_t)) = 27 \cdot 5 = 162 \quad \text{and} \quad \dim(\mathbf{T}(H_w)) = 27 \cdot 9 = 243$$

## Abstractions and Analysis: Monty Hall

**Initial configurations** 162 or 243 dimensional (labels dim = 6/9)

$$x_0 = (1 \ 0 \ 0) \otimes (1 \ 0 \ 0) \otimes (1 \ 0 \ 0) \otimes (1 \ 0 \ 0 \ \dots \ 0)$$

**Final configurations** of the same dimension, non-zero entries:

$$\text{for } H_t : \left\{ \begin{array}{l} x_{12} = 0.074074 \\ x_{18} = 0.037037 \\ x_{36} = 0.111111 \\ x_{48} = 0.111111 \\ x_{72} = 0.111111 \\ x_{78} = 0.037037 \\ x_{90} = 0.074074 \\ x_{96} = 0.111111 \\ x_{120} = 0.111111 \\ x_{132} = 0.111111 \\ x_{150} = 0.074074 \\ x_{156} = 0.037037 \end{array} \right. \quad \text{for } H_w : \left\{ \begin{array}{l} x_{18} = 0.111111 \\ x_{27} = 0.111111 \\ x_{54} = 0.037037 \\ x_{72} = 0.074074 \\ x_{108} = 0.074074 \\ x_{117} = 0.111111 \\ x_{135} = 0.111111 \\ x_{144} = 0.037037 \\ x_{180} = 0.037037 \\ x_{198} = 0.074074 \\ x_{225} = 0.111111 \\ x_{234} = 0.111111 \end{array} \right.$$

# Extracting results: Monty Hall

Consider the terminal configurations (with " $\infty = 100$ "):

$$x_t = \lim_{n \rightarrow \infty} (\mathbf{T}(H_t))^n x_0 \quad \text{and} \quad x_w = \lim_{n \rightarrow \infty} (\mathbf{T}(H_w))^n x_0$$

Abstract relevant information with  $\mathbf{A} = \mathbf{I}$  and  $\mathbf{A}_f = (1, 1, \dots, 1)^t$ :

$$\vec{x}_t \cdot (\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{A}_f \otimes \mathbf{A}_f) = ( 0.11 \quad 0.11 \quad 0.11 \quad 0.11 \quad 0.11 \quad 0.11 \quad 0.11 \quad 0.11 \quad 0.11 )$$

$$x_w \cdot (\mathbf{I} \otimes \mathbf{I} \otimes \mathbf{A}_f \otimes \mathbf{A}_f) = ( 0.22 \quad 0.04 \quad 0.07 \quad 0.07 \quad 0.22 \quad 0.04 \quad 0.04 \quad 0.07 \quad 0.22 )$$

## Monty Hall: Optimal Strategy

With further abstraction  $\mathbf{A}_w =$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{matrix} \dots & d \mapsto 0, g \mapsto 0 \\ \dots & d \mapsto 0, g \mapsto 1 \\ \dots & d \mapsto 0, g \mapsto 2 \\ \dots & d \mapsto 1, g \mapsto 0 \\ \dots & d \mapsto 1, g \mapsto 1 \\ \dots & d \mapsto 1, g \mapsto 2 \\ \dots & d \mapsto 2, g \mapsto 0 \\ \dots & d \mapsto 2, g \mapsto 1 \\ \dots & d \mapsto 2, g \mapsto 2 \end{matrix}$$

we get

$$x_t \cdot (\mathbf{A}_w \otimes \mathbf{A}_f \otimes \mathbf{A}_f) = ( 0.33333 \quad 0.66667 )$$

$$x_w \cdot (\mathbf{A}_w \otimes \mathbf{A}_f \otimes \mathbf{A}_f) = ( 0.66667 \quad 0.33333 )$$