Exercises

Program Analysis (CO70020)

Sheet 6

Exercise 1 *Consider the following* pWhile *program with* $x \in \{-1, 0, +1\}$*:*

```
x ?= {-1,1};
while (x > 0) || (x < 0) do
  choose 1:  x := (((x+1)+1)%3)-1 or 1:  x := (((x+1)-1)%3)-1 ro
od;
stop
```

By "%" we denote the remainder operation (i.e. $x \bmod 3$*). Describe what this program is doing. Does this program always terminate?*

Label the program and give the probabilistic program flow. Construct the transfer functions/matrices for every block. Give the symbolic construction of the LOS semantics. What is the dimension of the DTMC operator representing the semantics of this program and explicitly write it down and explain what each row/column corresponds to.

For these exercises it is helpful to use tools like `octave`*, Julia or Matlab.*

Solution This is the random walk in one dimension on a "torus" of three elements, i.e. termination when the origin and left and right "borders" (-1 and $+1$) are "neighbours".

The program does not always terminate: A trace $-1, +1, -1, +1, -1, +1 \ldots$ is possible (but has vanishing probability).

```
[x ?= -1, 1]^1;
while [((x > 0) | (x < 0))]^2 do
  [choose]^3
     1: [x := ((((x + 1) + 1) % 3) - 1)]^4
  or
     1: [x := ((((x + 1) - 1) % 3) - 1)]^5
  ro
od;
[stop]^6
```

Probabilistic flow (for tests $\underline{\ell}$ indicates the `true` (`then`) branching, the plane label the `false` (`else`) branch):

$$\{(1,1,2)(2,\underline{1},3)(3,1,4)(3,1,5)(4,1,2)(5,1,2)(2,1,6)(6,1,6)\}$$

or with renormalisation:

$$\{(1,1,2)(2,\underline{1},3)(3,\frac{1}{2},4)(3,\frac{1}{2},5)(4,1,2)(5,1,2)(2,1,6)(6,1,6)\}$$

Transfer Operators for lables $\ell = 1,\ldots,6$:

$$\begin{array}{lcl}
\mathbf{F}_1 & = & \frac{1}{2}\mathbf{U}(x \leftarrow -1) + \frac{1}{2}\mathbf{U}(x \leftarrow +1) \\
\mathbf{P}_2 & = & \mathbf{P}(x <> 0) \\
\mathbf{P}_2^{\perp} & = & \mathbf{P}(x == 0) \\
\mathbf{F}_3 & = & \mathbf{I}_3 \\
\mathbf{F}_4 & = & \mathbf{U}(x \leftarrow ((((x+1)+1)\%3)-1)) \\
\mathbf{F}_5 & = & \mathbf{U}(x \leftarrow ((((x+1)-1)\%3)-1)) \\
\mathbf{F}_6 & = & \mathbf{I}_3
\end{array}$$

Concretely we have:

$$\begin{array}{lcl}
\mathbf{F}_1 & = & \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \\
\mathbf{P}_2 & = & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\mathbf{P}_2^{\perp} & = & \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \\
\mathbf{F}_3 & = & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\mathbf{F}_4 & = & \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \\
\mathbf{F}_5 & = & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\
\mathbf{F}_6 & = & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\end{array}$$

For every (of the eight) control-flow step(s) we have the contribution:

$$\begin{array}{lcl}
\mathbf{T}_1 & = & \mathbf{F}_1 \otimes \mathbf{E}(1,2) \\
\mathbf{T}_2 & = & \mathbf{P}_2 \otimes \mathbf{E}(2,3) \\
\mathbf{T}_3 & = & \frac{1}{2}\mathbf{F}_3 \otimes \mathbf{E}(3,4) \\
\mathbf{T}_4 & = & \frac{1}{2}\mathbf{F}_3 \otimes \mathbf{E}(3,5) \\
\mathbf{T}_5 & = & \mathbf{F}_4 \otimes \mathbf{E}(4,2) \\
\mathbf{T}_6 & = & \mathbf{F}_5 \otimes \mathbf{E}(5,2)
\end{array}$$

$$\begin{aligned}\mathbf{T}_7 &= \mathbf{P}_2^{\perp} \otimes \mathbf{E}(2,6)\\ \mathbf{T}_8 &= \mathbf{F}_6 \otimes \mathbf{E}(6,6)\end{aligned}$$

With this $\mathbf{T} = \sum_{i=1}^{8} \mathbf{T}_i$ gives a $3 \cdot 6 \times 3 \cdot 6 = 18 \times 18$ operator:

$$\mathbf{T} = \begin{pmatrix}
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \\
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 &
\end{pmatrix}$$

The indices refer to the following configurations:

```
 1 ...<x=-1,[x ?= { -1, 1 }]^1>          10 ...<x=0,[x:=((((x+1)+1)%3)-1)]^4>
 2 ...<x=-1,[((x>0)|(x<0))]^2>           11 ...<x=0,[x:=((((x+1)-1)%3)-1)]^5>
 3 ...<x=-1,[choose]^3>                  12 ...<x=0,[skip]^6>
 4 ...<x=-1,[x:=((((x+1)+1)%3)-1)]^4>    13 ...<x=1,[x ?= { -1, 1 }]^1>
 5 ...<x=-1,[x:=((((x+1)-1)%3)-1)]^5>    14 ...<x=1,[((x>0)|(x<0))]^2>
 6 ...<x=-1,[skip]^6>                    15 ...<x=1,[choose]^3>
 7 ...<x=0,[x ?= { -1, 1 }]^1>           16 ...<x=1,[x:=((((x+1)+1)%3)-1)]^4>
 8 ...<x=0,[((x>0)|(x<0))]^2>            17 ...<x=1,[x:=((((x+1)-1)%3)-1)]^5>
 9 ...<x=0,[choose]^3>                   18 ...<x=1,[skip]^6>
```

Exercise 2 *Change the above* pWhile *program such that we have* $x \in \{-3, 0, +3\}$. *Label the program and give the probabilistic program flow.*

Give the symbolic construction of the LOS semantics. What is the dimension of the DTMC operator representing the semantics of this program.

Consider the sign abstraction defined by the extraction function:

$$\eta(n) = \begin{cases} - & \text{if } n < 0 \\ 0 & \text{if } n = 0 \\ + & \text{if } n > 0 \end{cases}$$

Give the (probabilistic) abstraction and concretisation matrices $\mathbf{A}$ *and* $\mathbf{G}$ *for the variable* x*. Describe the corresponding classical abstract interpretation setting (domains,* α*,* γ*, etc.).*

Give the symbolic construction of the abstract semantics of the program using the sign abstraction for variable x*. Give the* **abstract** *transfer functions/matrices for all blocks. What is the dimension of the abstract DTMC generator and construct it explicitly.*

Optionally: Construct the transfer functions/matrices for the **concrete** *semantics for every block.*

Solution The "extended" program is:

```
x ?= {-1,1};
while (x > 0) || (x < 0) do
  choose
        1:  x := (((x+3)+1) % 7)-3
  or
        1:  x := (((x+3)-1) % 7)-3
  ro
od;
stop
```

or labelled:

```
[x ?= -1, 1]^1 ;
while [((x > 0) | (x < 0))]^2 do
[choose]^3
       1: [x := ((((x + 3) + 1) % 7) - 3)]^4
or
       1: [x := ((((x + 3) - 1) % 7) - 3)]^5
ro
od;
[stop]^6
```

Note: One could perhaps also argue for the first statement being:

The probabilistic control flow is identical to the one of the previous program:

$$\{(1,1,2)(2,\underline{1},3)(3,1,4)(3,1,5)(4,1,2)(5,1,2)(2,1,6)(6,1,6)\}$$

$$\{(1,1,2)(2,\underline{1},3)(3,\frac{1}{2},4)(3,\frac{1}{2},5)(4,1,2)(5,1,2)(2,1,6)(6,1,6)\}$$

The concrete transfer operators for labels $\ell = 1,\ldots,6$ are also very similar

$$\begin{array}{lcl}
\mathbf{F}_1 & = & \frac{1}{2}\mathbf{U}(x \leftarrow -1) + \frac{1}{2}\mathbf{U}(x \leftarrow +1) \\
\mathbf{P}_2 & = & \mathbf{P}(x <> 0) \\
\mathbf{P}_2^{\perp} & = & \mathbf{P}(x == 0) \\
\mathbf{F}_3 & = & \mathbf{I}_3 \\
\mathbf{F}_4 & = & \mathbf{U}(x \leftarrow ((((x+3)+1)\%7)-3)) \\
\mathbf{F}_5 & = & \mathbf{U}(x \leftarrow ((((x+3)-1)\%7)-3)) \\
\mathbf{F}_6 & = & \mathbf{I}_3
\end{array}$$

The classical abstractions are given as $\alpha : \mathcal{P}(\mathbb{Z}) \to \mathcal{P}(\{-, 0, +\})$ and $\gamma : \mathcal{P}(\{-, 0, +\}) \to \mathcal{P}(\mathbb{Z})$, or more precisely for the variable x in question:

$$\alpha : \mathcal{P}(\{-3, -2, \ldots, 0, \ldots, 2, 3\}) \to \mathcal{P}(\{-, 0, +\})$$

$$\gamma : \mathcal{P}(\{-, 0, +\}) \to \mathcal{P}(\{-3, -2, \ldots, 0, \ldots, 2, 3\})$$

with

$$\alpha(X) = S \text{ with } S = N \cup Z \cup P$$

where $N = \{-\}$ if $\{-3, -2, -1\} \cap X \neq \emptyset$ otherwise $N = \emptyset$; $Z = \{0\}$ if $0 \in X$ otherwise $Z = \emptyset$; and $P = \{-\}$ if $\{3, 2, 1\} \cap X \neq \emptyset$ otherwise $P = \emptyset$, and

$$\gamma(Y) = \{\sigma(y) \mid y \in Y\}$$

with $\sigma(-) = \{-3, -2, -1\}$; $\sigma(0) = \{0\}$; and $\sigma(+) = \{1, 2, 3\}$.

The abstract transfer functions are constructed as follows:

$$\begin{array}{lcl}
\mathbf{F}_1^{\#} & = & \mathbf{G}(\frac{1}{2}\mathbf{U}(x \leftarrow -1) + \frac{1}{2}\mathbf{U}(x \leftarrow +1))\mathbf{A} \\
\mathbf{P}_2^{\#} & = & \mathbf{GP}(x <> 0)\mathbf{A} \\
\mathbf{P}_2^{\perp\#} & = & \mathbf{GP}(x == 0)\mathbf{A} \\
\mathbf{F}_3^{\#} & = & \mathbf{GI}_3\mathbf{A} \\
\mathbf{F}_4^{\#} & = & \mathbf{GU}(x \leftarrow ((((x + 3) + 1)\%7) - 3))\mathbf{A} \\
\mathbf{F}_5^{\#} & = & \mathbf{GU}(x \leftarrow ((((x + 3) - 1)\%7) - 3))\mathbf{A} \\
\mathbf{F}_6^{\#} & = & \mathbf{GI}_3\mathbf{A}
\end{array}$$

The probabilistic abstraction/concretisation pair is given by:

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \mathbf{G} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

With this we get the abstract transfer functions/matrices as:

$$
\begin{aligned}
\mathbf{F}_1^{\#} &= \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix} \\
\mathbf{P}_2^{\#} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\mathbf{P}_2^{\perp\#} &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \\
\mathbf{F}_3^{\#} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\mathbf{F}_4^{\#} &= \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \\ \frac{1}{3} & 0 & \frac{2}{3} \end{pmatrix} \\
\mathbf{F}_5^{\#} &= \begin{pmatrix} \frac{2}{3} & 0 & 0 \\ 1 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{2}{3} \end{pmatrix} \\
\mathbf{F}_6^{\#} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}
$$

which gives us:

$$
\mathbf{T}^{\#} = \begin{pmatrix}
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{2}{3} & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{2}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\
0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{2}{3} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & \frac{2}{3} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
$$