# Exercise 6

## Generalized Stochastic Petri Nets (GSPNS)
## Introduction to Laboratory Class 2
## Problems 3.10, 3.4

Fault-Tolerant Computer Systems

2011

# Elements of GSPNs

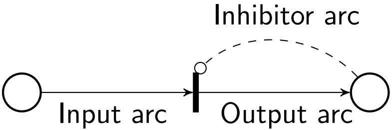
- *Places* – Hold tokens.


- *Timed transitions* – Fires at a random point in time when enabled.

- *Immediate transitions* – Fires immediate when enabled.



- *Input and output arcs* – Connect places with transitions
- *Inhibitor arcs* – Blocks the firing of a transition.

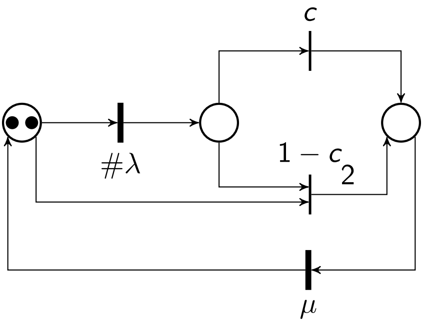


# Hot stand-by system

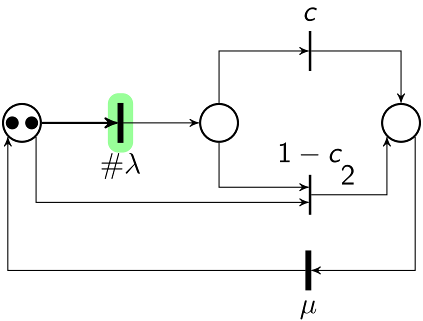
A fault-tolerant computer system consists of two modules working in active redundancy. The failure rate of the computer modules is $\lambda$ and the repair rate is $\mu$. The coverage for reconfigurations is $c$.

Define a Petri net model of the system.

# Hot stand-by system

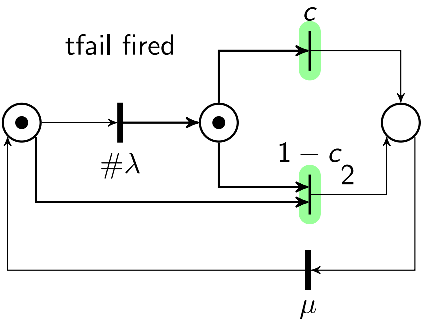


# Hot stand-by system



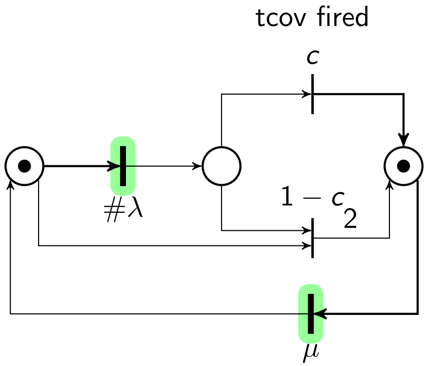

| | Marking | Comment |
|---|---|---|
| ⇒ | $\{2,0,0\}$ | Initial marking |

# Hot stand-by system



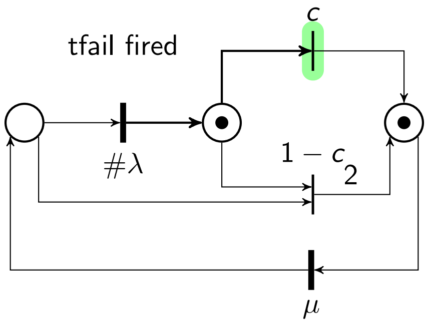

| | Marking | Comment |
|---|---|---|
| | $\{2,0,0\}$ | Initial marking |
| $\Rightarrow$ | $\{1,1,0\}$ | One module failed (vanishing marking) |

# Hot stand-by system



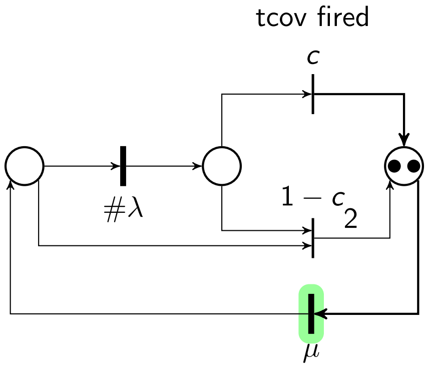

| | Marking | Comment |
|---|---|---|
| | $\{2, 0, 0\}$ | Initial marking |
| | $\{1, 1, 0\}$ | One module failed (vanishing marking) |
| $\Rightarrow$ | $\{1, 0, 1\}$ | One module failed |

# Hot stand-by system



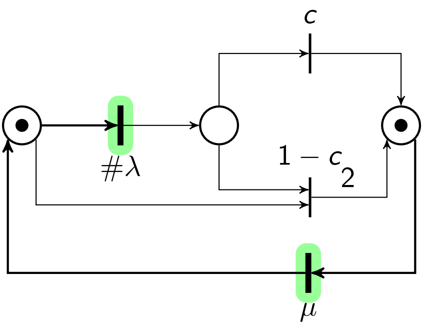

| | Marking | Comment |
|---|---|---|
| | $\{2,0,0\}$ | Initial marking |
| | $\{1,1,0\}$ | One module failed (vanishing marking) |
| | $\{1,0,1\}$ | One module failed |
| $\Rightarrow$ | $\{0,1,1\}$ | Two modules failed (vanishing marking) |

# Hot stand-by system




| | Marking | Comment |
|---|---|---|
| | $\{2, 0, 0\}$ | Initial marking |
| | $\{1, 1, 0\}$ | One module failed (vanishing marking) |
| | $\{1, 0, 1\}$ | One module failed |
| | $\{0, 1, 1\}$ | Two modules failed (vanishing marking) |
| $\Rightarrow$ | $\{0, 0, 2\}$ | Two modules failed |

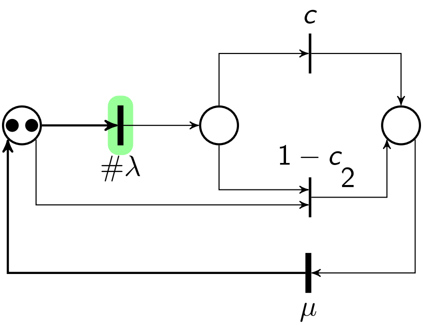
# Hot stand-by system




trepair fired

| | Marking | Comment |
|---|---|---|
| | $\{2, 0, 0\}$ | Initial marking |
| | $\{1, 1, 0\}$ | One module failed (vanishing marking) |
| $\Rightarrow$ | $\{1, 0, 1\}$ | One module failed |
| | $\{0, 1, 1\}$ | Two modules failed (vanishing marking) |
| | $\{0, 0, 2\}$ | Two modules failed |

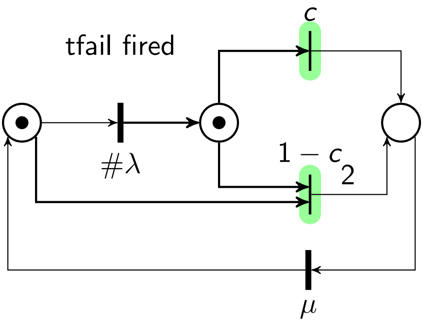
# Hot stand-by system




trepair fired

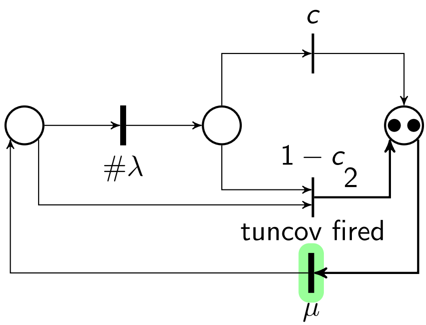
| | Marking | Comment |
|---|---|---|
| ⇒ | $\{2, 0, 0\}$ | Initial marking |
| | $\{1, 1, 0\}$ | One module failed (vanishing marking) |
| | $\{1, 0, 1\}$ | One module failed |
| | $\{0, 1, 1\}$ | Two modules failed (vanishing marking) |
| | $\{0, 0, 2\}$ | Two modules failed |

# Hot stand-by system




| | Marking | Comment |
|---|---|---|
| | $\{2,0,0\}$ | Initial marking |
| ⇒ | $\{1,1,0\}$ | One module failed (vanishing marking) |
| | $\{1,0,1\}$ | One module failed |
| | $\{0,1,1\}$ | Two modules failed (vanishing marking) |
| | $\{0,0,2\}$ | Two modules failed |

# Hot stand-by system



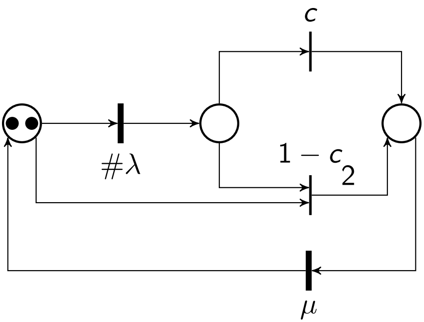

| Marking | Comment |
|---|---|
| $\{2, 0, 0\}$ | Initial marking |
| $\{1, 1, 0\}$ | One module failed (vanishing marking) |
| $\{1, 0, 1\}$ | One module failed |
| $\{0, 1, 1\}$ | Two modules failed (vanishing marking) |
| ⇒ $\{0, 0, 2\}$ | Two modules failed |

# GSPN Analysis

- Reachability graphs show possible firing sequences of GSPNs.
- An extended reachability graph contains
  - Tangible markings – Only timed transitions are enabled.
  - Vanishing markings – At least one immediate transition is enabled.
- A reduced reachability graph is created by transforming the extended reachability graph.
  - Transition rates are modified so that they account for the effects of tangible markings.

# Hot stand-by system

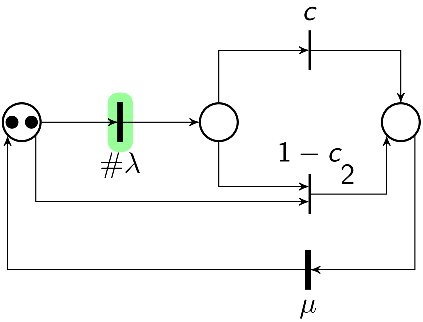
## Extended reachability graph

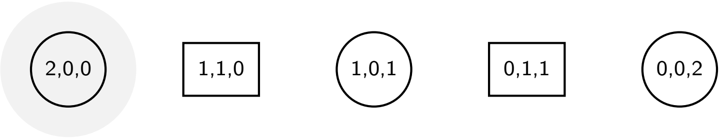



| Marking | Comment |
|---|---|
| $\{2, 0, 0\}$ | Initial marking |
| $\{1, 1, 0\}$ | One module failed (vanishing marking) |
| $\{1, 0, 1\}$ | One module failed |
| $\{0, 1, 1\}$ | Two modules failed (vanishing marking) |
| $\{0, 0, 2\}$ | Two modules failed |

# Hot stand-by system

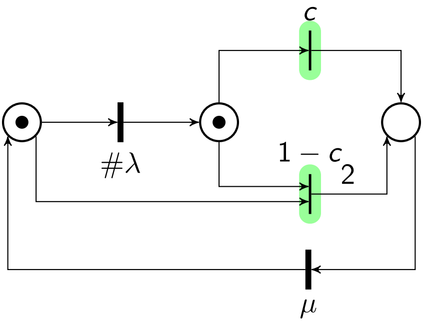
## Extended reachability graph



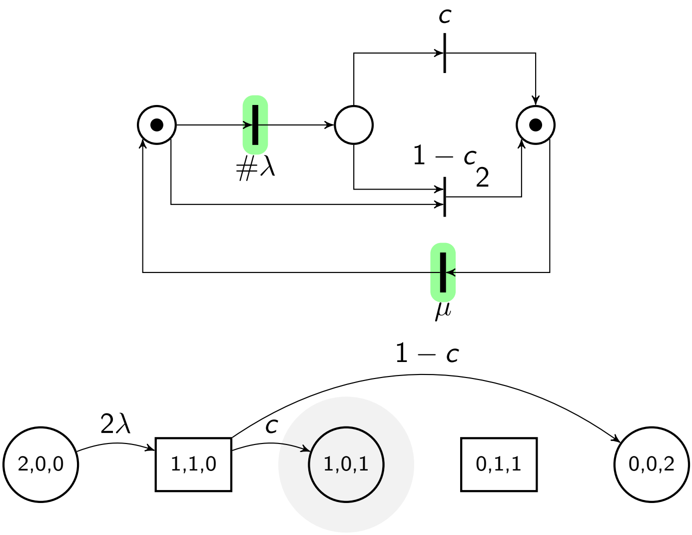
# Hot stand-by system

## Extended reachability graph



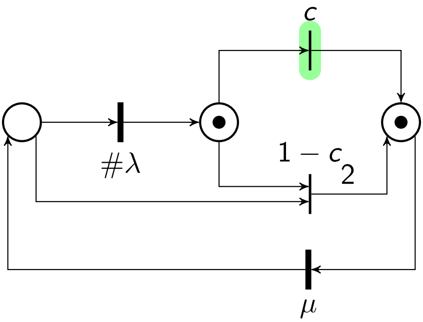

# Hot stand-by system

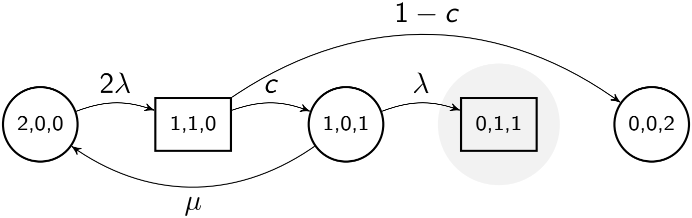
## Extended reachability graph



# Hot stand-by system

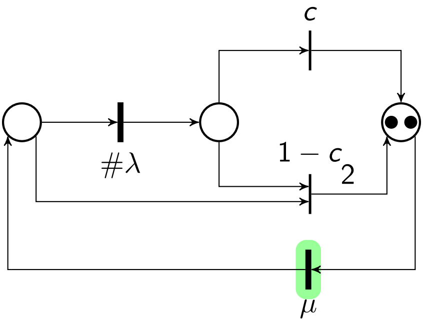
## Extended reachability graph

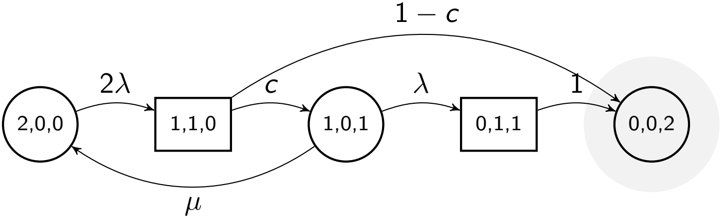


# Hot stand-by system

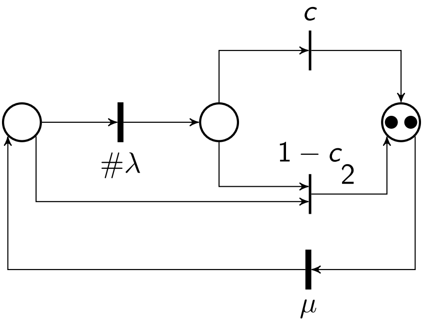
## Extended reachability graph

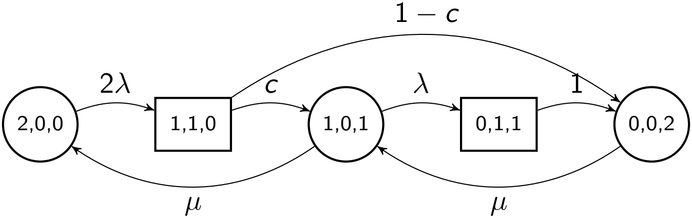


# Hot stand-by system

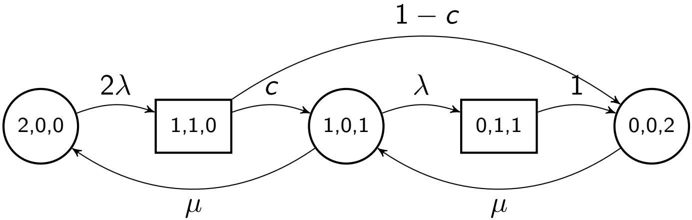
## Extended reachability graph



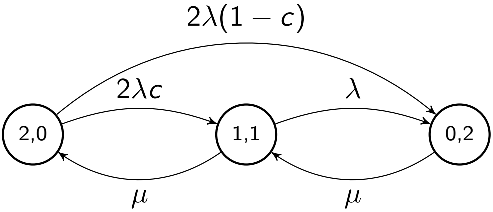



# Hot stand-by system

Extended reachability graph:




Reduced reachability graph:



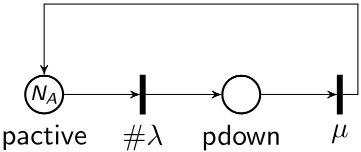
# Cold stand-by system

A fault-tolerant computer system from start consists of $N_A$ active modules and $N_S$ spare modules. The failure rate for an active module is $\lambda$ and the failure rate of the spare modules is negligible. The coverage for all reconfigurations is assumed to be ideal.

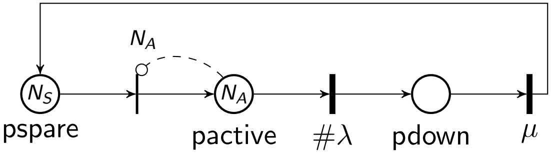
Define a GSPN model of the system.

# Cold stand-by system

Hint: A hot stand-by system can be modelled with the following GSPN model:



# Cold stand-by system



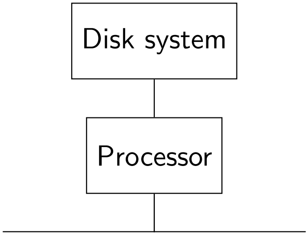
# Laboratory class 2

Study the impact of repair on the availability.

- Evaluate two different file server configurations: a simplex and a duplex server.
- Use Markov models and GPSN models to calculate the steady-state availability.

# Laboratory class 2

## Simplex server

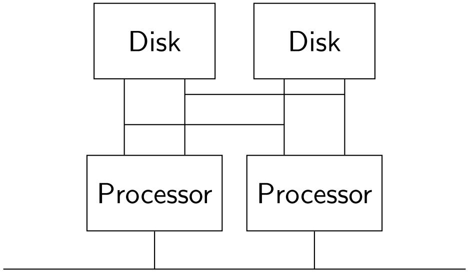



Repair policies:

1. Each unit has its own repair facility. The units fail independently of each other.
2. The units share one repair facility. The units fail independently of each other. Repairs are made using a *first-come first-served policy*. (Repairs are not preempted.)

# Laboratory class 2

## Duplex server



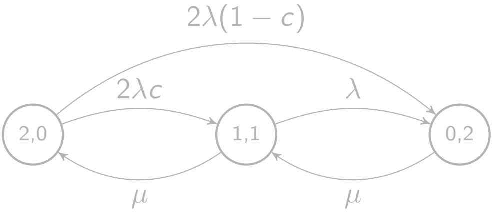
# Laboratory class 2

## Duplex server – Repair policies

1. One repair facility handles one processor or disk at a time.
   - Processor/disk failures do not occur if the system is down.
   - Processor repairs always are given priority over disk repairs.
2. One repair facility handles one processor or disk at a time.
   - Processor/disk failures may occur when the system is down
   - Processor repairs are given priority over disk repairs except when both disks have failed and one processor is working.
   - In that case, one disk is repaired first.
3. One repair facility for the processors and one for the disks.

# SHARPE

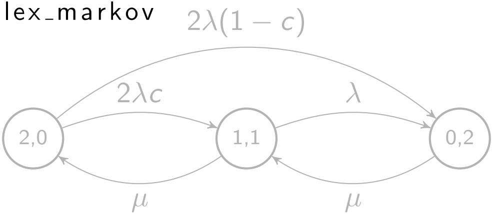
## Markov chains



# SHARPE

## Markov chains

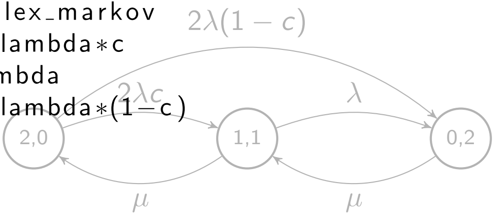
**markov** duplex_markov



# SHARPE

## Markov chains

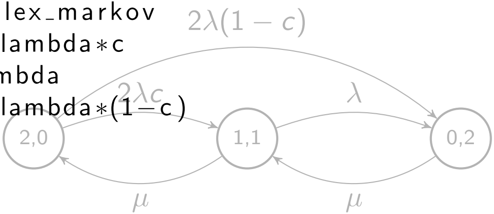
```
markov duplex_markov
s20 s11 2*lambda*c
s11 s02 lambda
s20 s02 2*lambda*(1-c)
s11 s20 mu
s02 s11 mu
end
```



# SHARPE

## Markov chains

```
markov duplex_markov
s20 s11 2*lambda*c
s11 s02 lambda
s20 s02 2*lambda*(1-c)
s11 s20 mu
s02 s11 mu
end
s20 1.0
end
```



# SHARPE

## Markov chains

```
markov name { (param_list) }
* Transitions and transition rates
<name name expression>
end
* Initial state probabilities
<name expression>
end
```

# SHARPE

## Steady-state probability for Markov models

- Calculate $\lim_{t \to \infty} A(t)$ for a state in a Markov model with

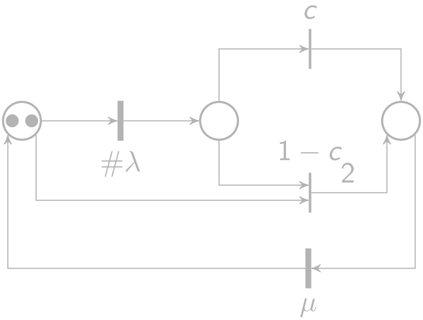
  ```
  prob (system_name, state_eword {;arg_list})
  ```

- Example: steady-state availability for the duplex system

  ```
  func ss_avail_duplex_markov () \
  prob(duplex_markov, s20) + prob(duplex_markov, s11)

  expr ss_avail_duplex_markov ()
  ```

# SHARPE

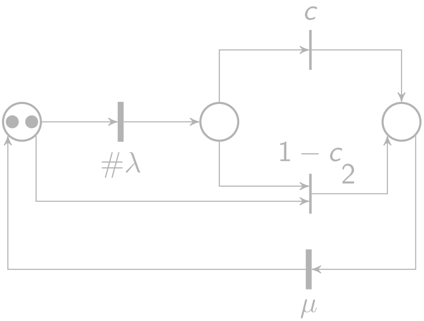
## GSPNs



# SHARPE

## GSPNs

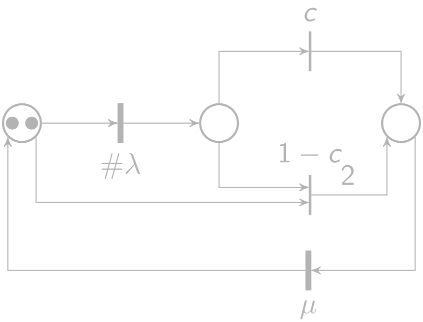
```
gspn duplex_petri
```



# SHARPE

## GSPNs

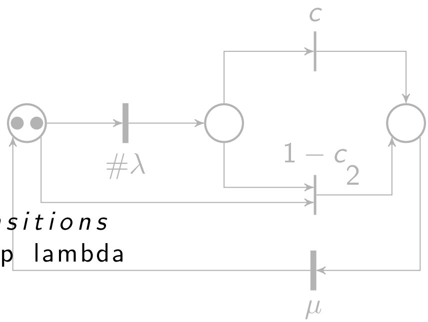
```
gspn duplex_petri

* places
pup 2
pdown 0
pdownim 0
end
```



# SHARPE

## GSPNs

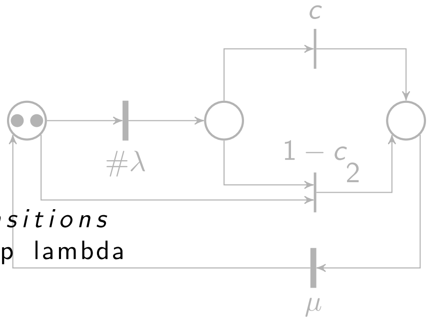
```
gspn duplex_petri

* places
pup 2
pdown 0
pdownim 0
end

* timed transitions
tfail dep pup lambda
trep ind mu
end
```



# SHARPE

## GSPNs

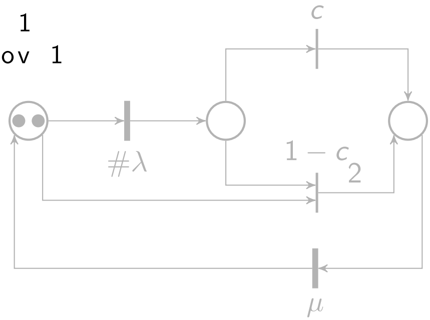
```
gspn duplex_petri

* places
pup 2
pdown 0
pdownim 0
end

* timed transitions
tfail dep pup lambda
trep ind mu
end

* immediate transitions
tcov ind c
tuncov ind (1-c)
end
```



# SHARPE

## GSPNs

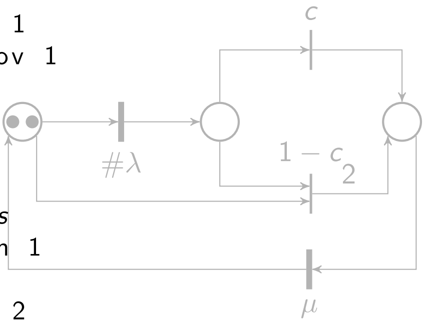
```
* input arcs
pup tfail 1
pdownim tcov 1
pdownim tuncov 1
pup tuncov 1
pdown trep 1
end
```



# SHARPE

## GSPNs

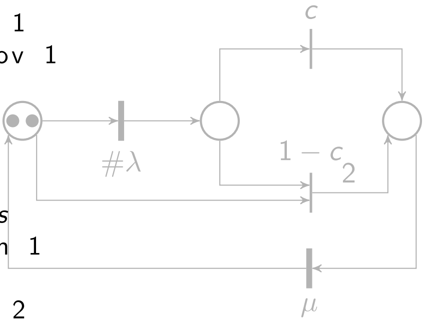
```
* input arcs
pup tfail 1
pdownim tcov 1
pdownim tuncov 1
pup tuncov 1
pdown trep 1
end

* output arcs
tfail pdownim 1
tcov pdown 1
tuncov pdown 2
trep pup 1
end
```



# SHARPE

## GSPNs

```
* input arcs
pup tfail 1
pdownim tcov 1
pdownim tuncov 1
pup tuncov 1
pdown trep 1
end

* output arcs
tfail pdownim 1
tcov pdown 1
tuncov pdown 2
trep pup 1
end

* inhibitor arcs
end
```



# SHARPE

## GSPNs

```
gspn name (param_list)
* section 1: places and initial numbers of tokens
<place_name expression>
end
* section 2: timed transition names, types and rates
<transition_name ind expression>
<transition_name dep place_name expression>
end
* section 3: immediate transition names and weights
<transition_name ind expression>
<transition_name dep place_name expression>
end
* section 4: place-to-transition arcs and multiplicity
<place name_transition_name expression>
end
* section 5: transition-to-place arcs and multiplicity
<transition_name place_name expression>
end
* section 6: inhibitor arcs and multiplicity
<place_name transition_name expression>
end
```

# SHARPE

## Steady-state probability for GSPNs

- Calculate the steady-state probability that a given state is empty using

```
prempty (system_name, place_eword {;arg_list})
```

- Example: steady-state availability for the duplex system

```
func ss_avail_duplex () \
1 - prempty(duplex_petri, pup)

expr ss_avail_duplex ()
```

# Laboratory class 2

Preparations for the lab

- Read the lab pm.
- Draw Markov models and GSPN models for the different repair policies.

### 3.10

Consider a hot stand-by system that from system start has one active and two spare modules. The system is shut down when one module remains operational. Assume that the shut-down time is exponentially distributed with the expected value $1/\mu$. A catastrophic failure occurs if the last remaining module fails before the shut-down is completed. The fault coverage is $c$ ($c < 1$) for an active module and ideal for a spare module. The occurrence of a non-covered fault in the active module leads to a catastrophic failure.

Draw a state diagram for a Markov model of the system and derive an expression for the steady-state safety of the system. Hint: the steady-state safety can be directly derived from the transition intensities in the Markov model.

#### Solution

*Failure rates are missing! Assume that the failure rate for active and spare modules are $\lambda$.*

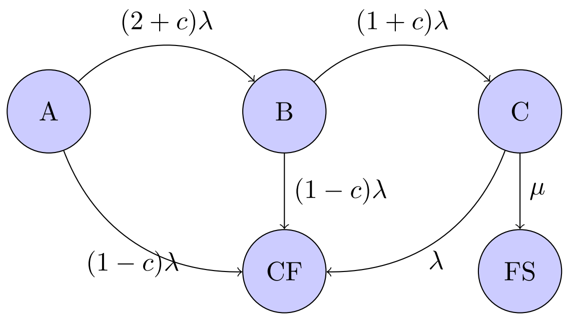



Figure 4: Markov chain

Steady-state safety is obtained directly from the figure:

$$A(\infty) = \frac{(2+c)\lambda}{3\lambda} \cdot \frac{(1+c)\lambda}{2\lambda} \cdot \frac{\mu}{\lambda+\mu}$$

# Solution

## 3.4

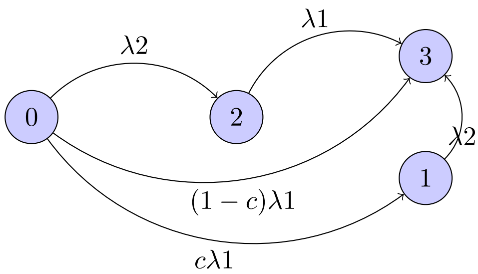



Figure 1: Markov chain

| State | Description |
|---|---|
| 0 | M1 and M2 working |
| 1 | M2 working |
| 2 | M1 working |
| 3 | Failure |

$$Q = \begin{bmatrix} -(\lambda_1+\lambda_2) & \lambda_1 c & \lambda_2 & \lambda_1(1-c) \\ 0 & -\lambda_2 & 0 & \lambda_2 \\ 0 & 0 & -\lambda_1 & \lambda_1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{aligned} P'(t) &= P(t)Q \\ P(0) &= \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \end{aligned}$$

Laplace transform:

$$\mathcal{L}\{P'(t) = P(t)Q\} \Rightarrow sP(s) - P(0) = P(s)Q$$

$$\begin{cases} sP_0 - 1 &= -(\lambda_1+\lambda_2)P_0 \\ sP_1 &= \lambda_1 c P_0 - \lambda_2 P_1 \\ sP_2 &= \lambda_2 P_0 - \lambda_1 P_2 \\ sP_3 &= \ldots \end{cases}$$

$$\begin{aligned} P_0 &= \frac{1}{s+(\lambda_1+\lambda_2)} \\ P_1 &= \frac{\lambda_1 c}{s+\lambda_2}P_0 = \frac{\lambda_1 c}{s+\lambda_2}\frac{1}{s+(\lambda_1+\lambda_2)} = c\left(\frac{1}{s+\lambda_2} - \frac{1}{s+(\lambda_1+\lambda_2)}\right) \\ P_2 &= \frac{\lambda_2}{s+\lambda_1}P_0 = \frac{\lambda_2}{s+\lambda_1}\frac{1}{s+(\lambda_1+\lambda_2)} = \frac{1}{s+\lambda_1} - \frac{1}{s+(\lambda_1+\lambda_2)} \end{aligned}$$

$$
\begin{aligned}
P_0(t) &= e^{-(\lambda_1+\lambda_2)t} \\
P_1(t) &= c\left(e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t}\right) \\
P_2(t) &= e^{-\lambda_1 t} - e^{-(\lambda_1+\lambda_2)t} \\
R(t) &= P_0(t) + P_1(t) + P_2(t) \\
&= e^{-(\lambda_1+\lambda_2)t} + c\left(e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t}\right) + e^{-\lambda_1 t} - e^{-(\lambda_1+\lambda_2)t} \\
&= e^{-\lambda_1 t} + c\left(e^{-\lambda_2 t} + e^{-(\lambda_1+\lambda_2)t}\right)
\end{aligned}
$$