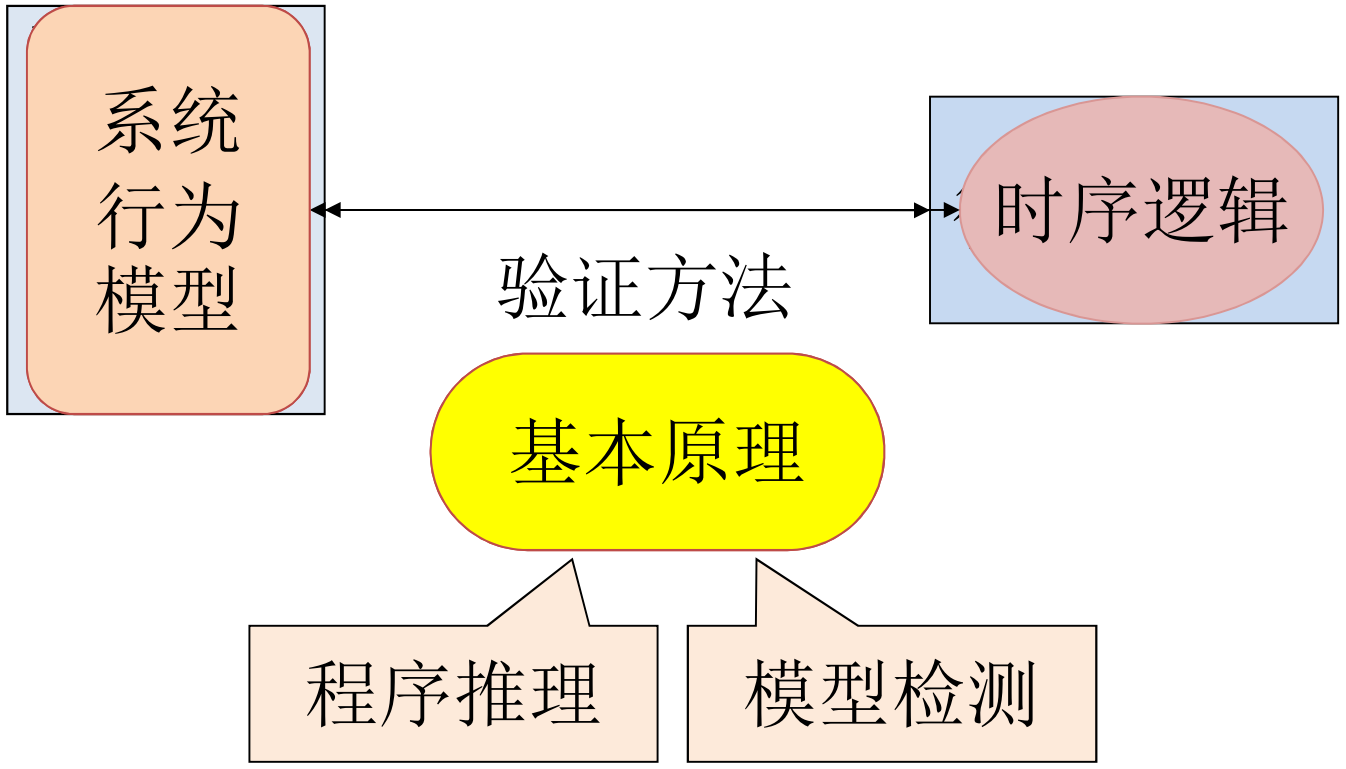
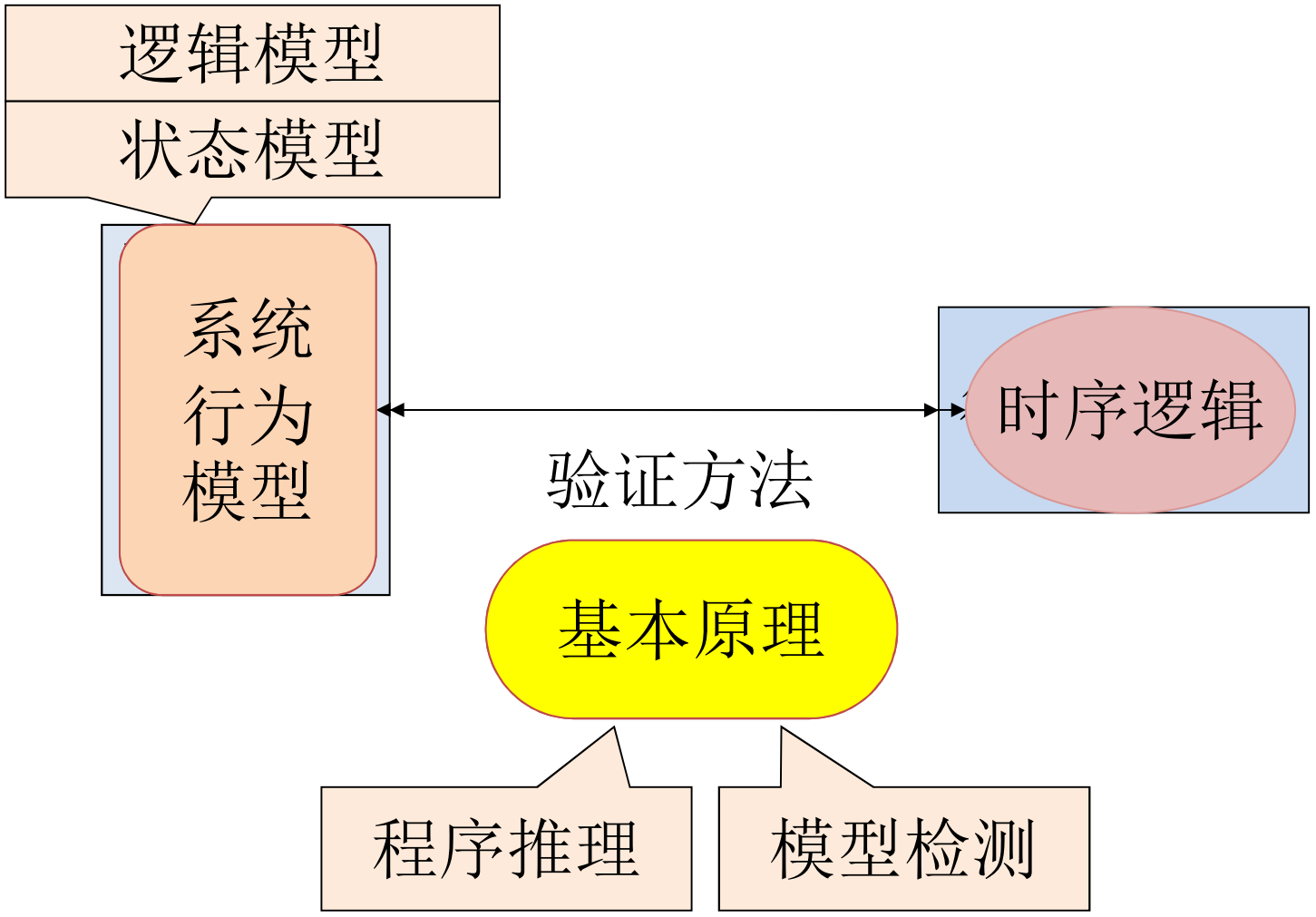
基于迁移标号的迁移系统(II)

中国科学院软件研究所
计算机科学国家重点实验室
张文辉
http://lcs.ios.ac.cn/~zwh/

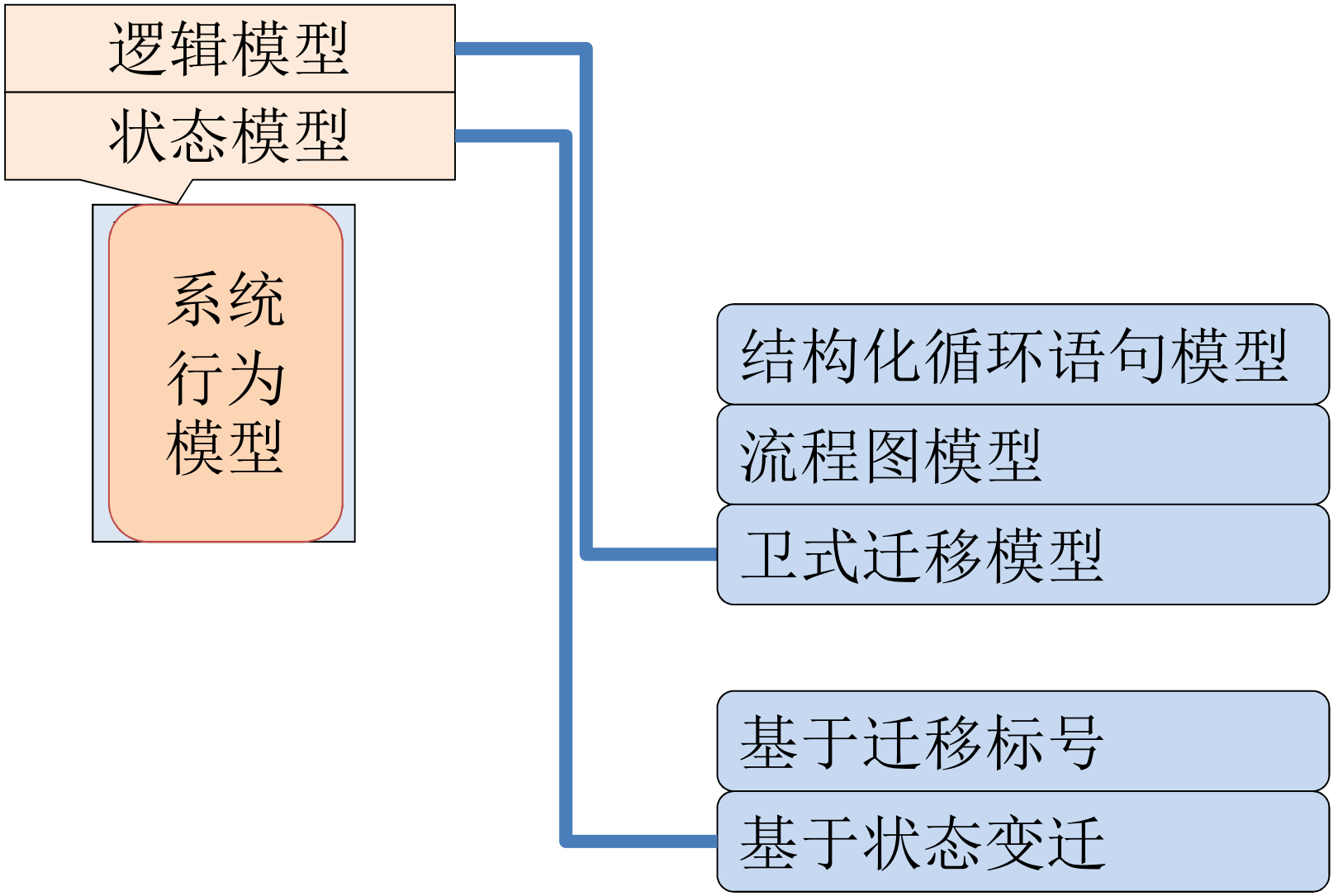
课程内容



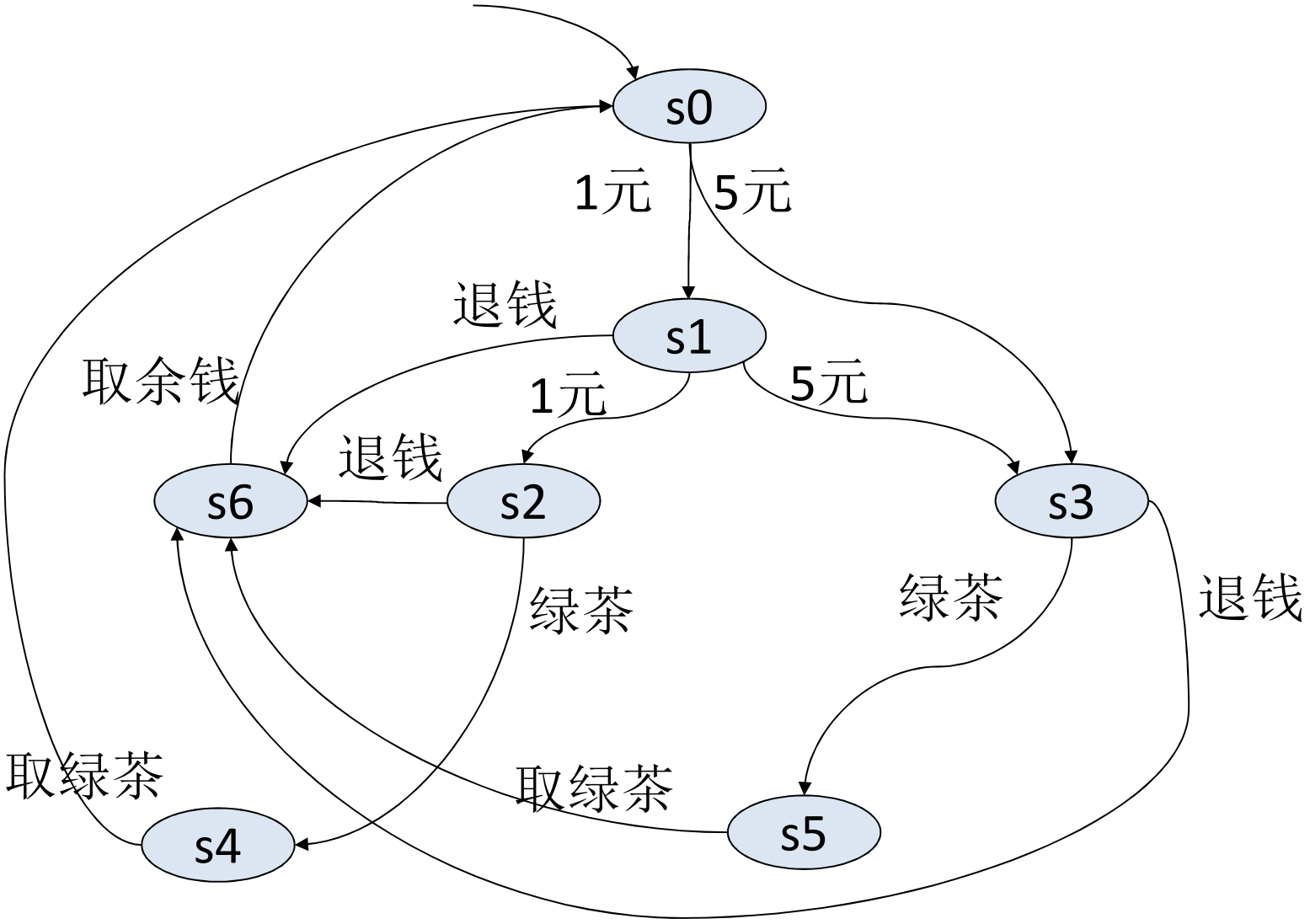
课程内容



课程内容(1)

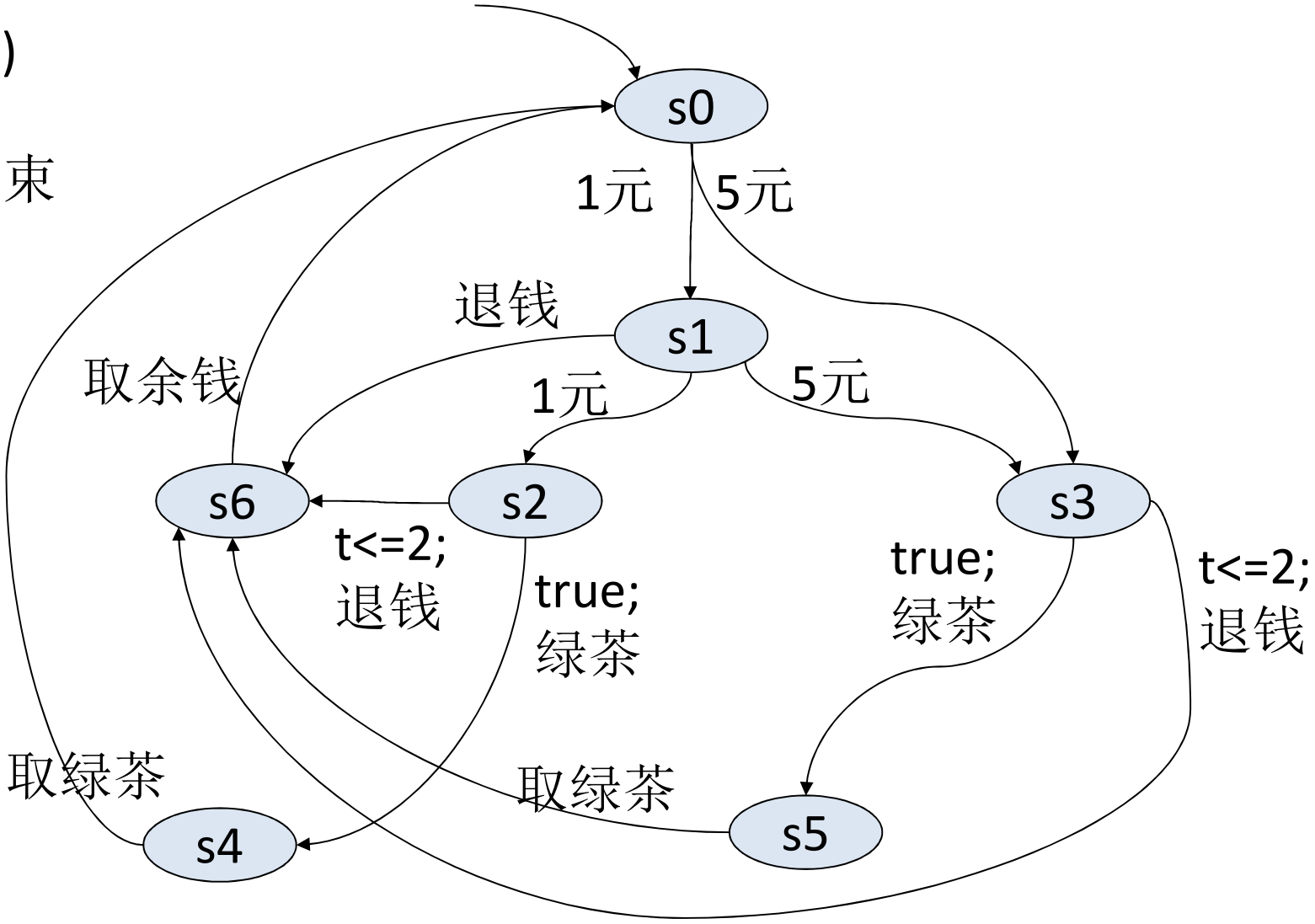


例子：自动售茶机的设计



例子：自动售茶机的设计

(Σ,S,Δ,I)
+
时间约束

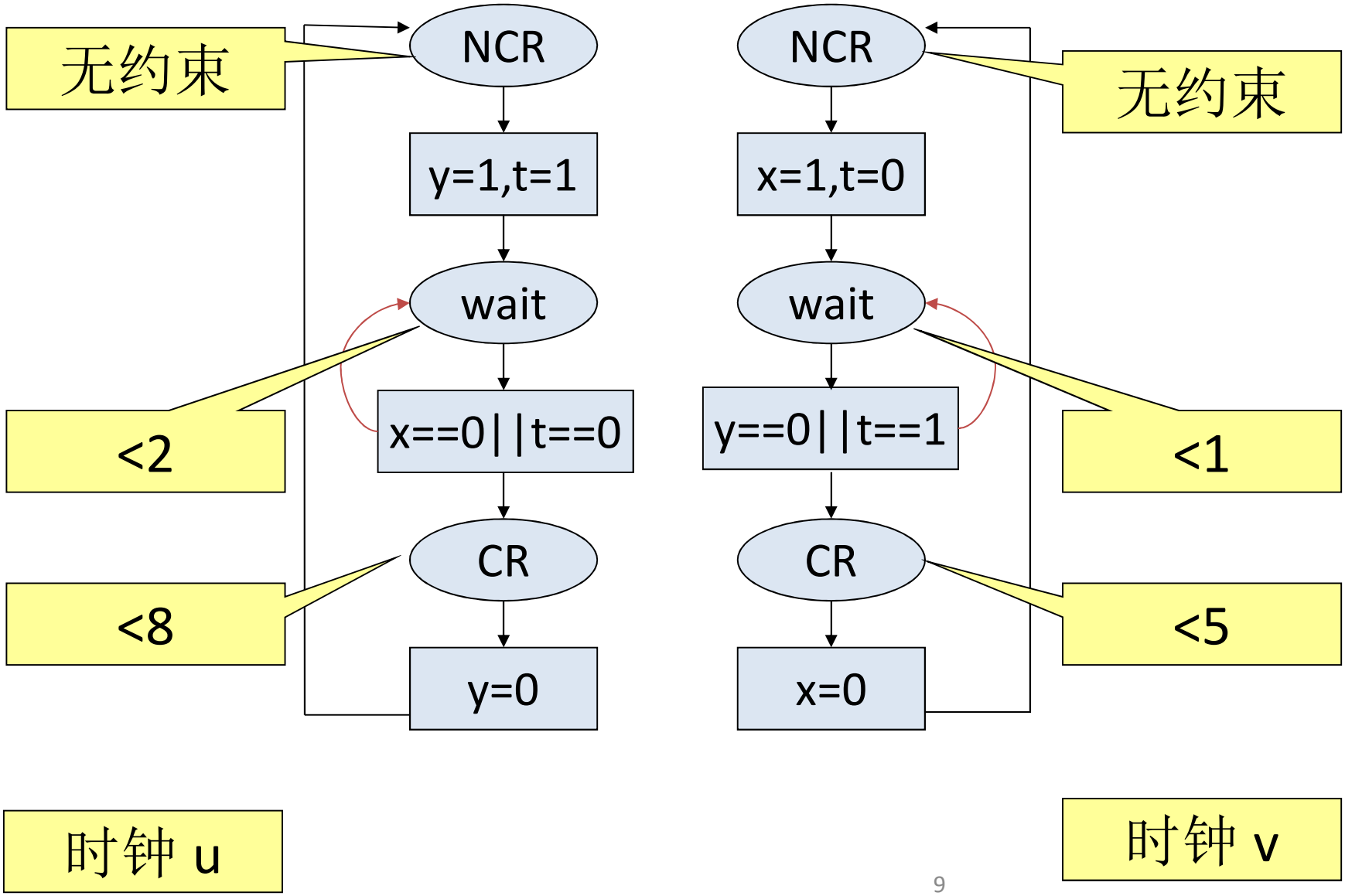


内容：

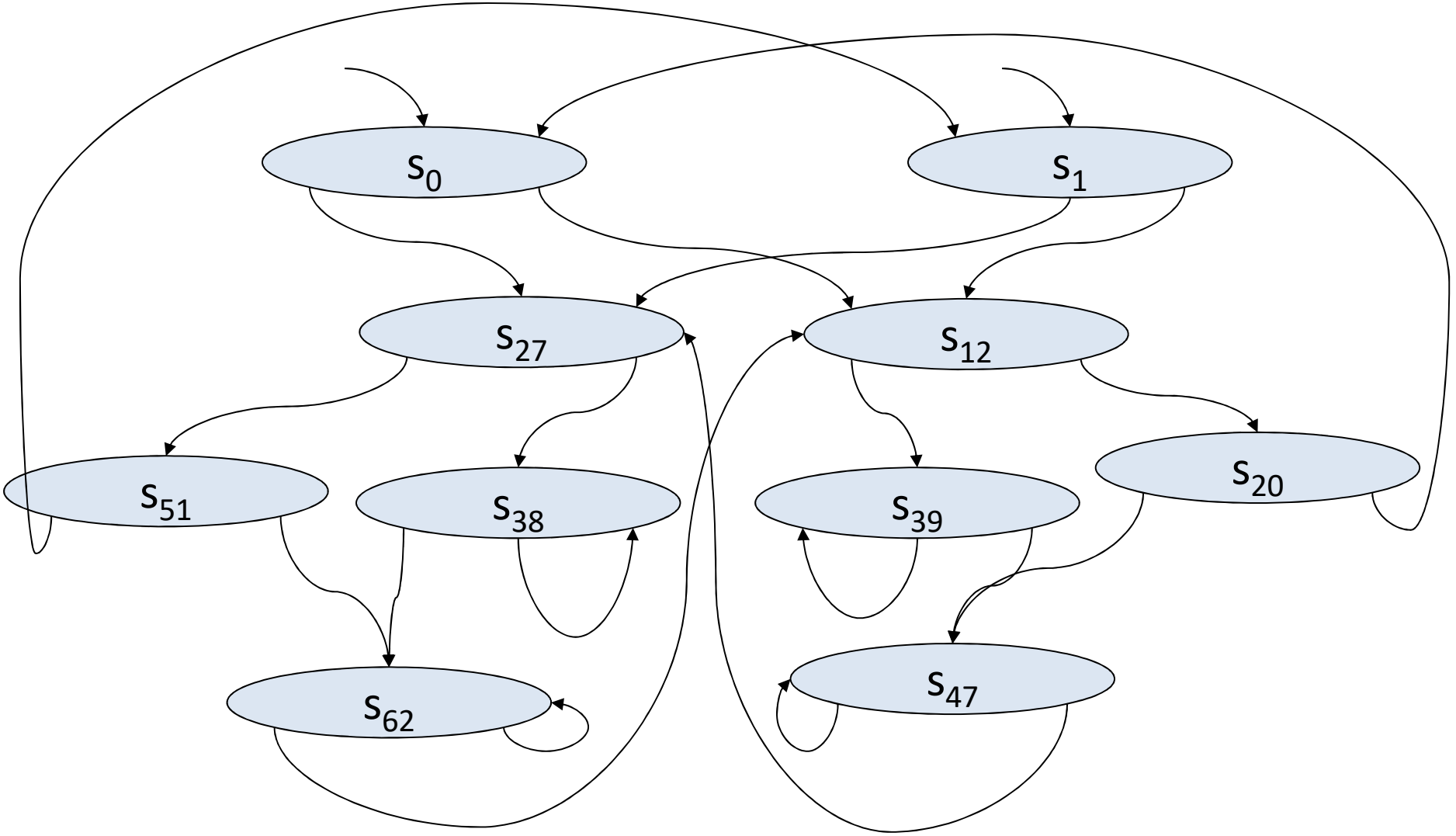
- 时间迁移系统(TTS)与时间自动机(TA)
- 混成迁移系统(Hybrid Systems)与自动机
- Petri-网

(I) Timed Transition Systems and Timed Automata

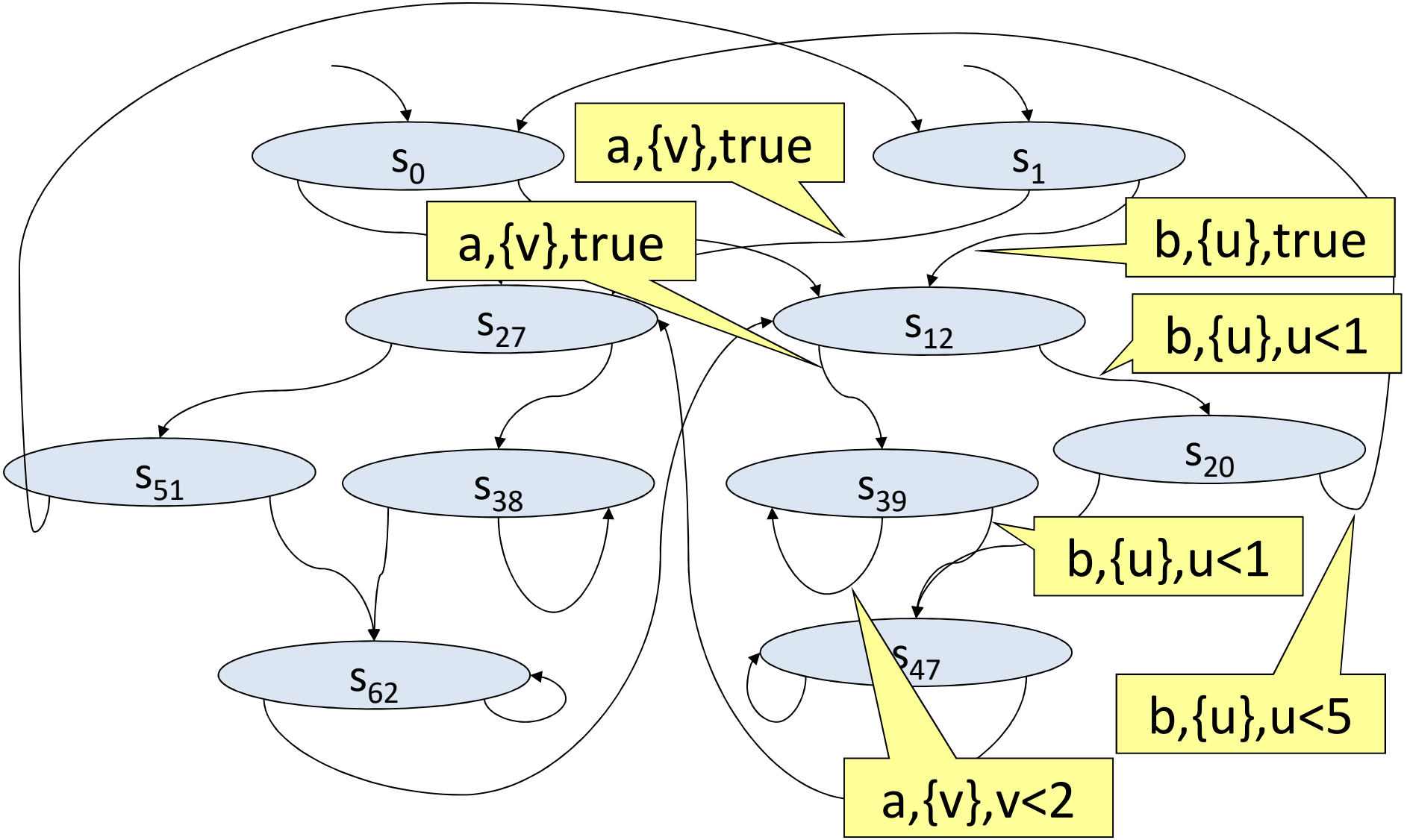
系统运行过程描述：例子


无约束
NCR
y=1,t=1
wait
<2
x==0||t==0
CR
<8
y=0
时钟 u
NCR
x=1,t=0
wait
y==0||t==1
<1
CR
<5
x=0
无约束
时钟 v

例2-互斥：状态迁移图

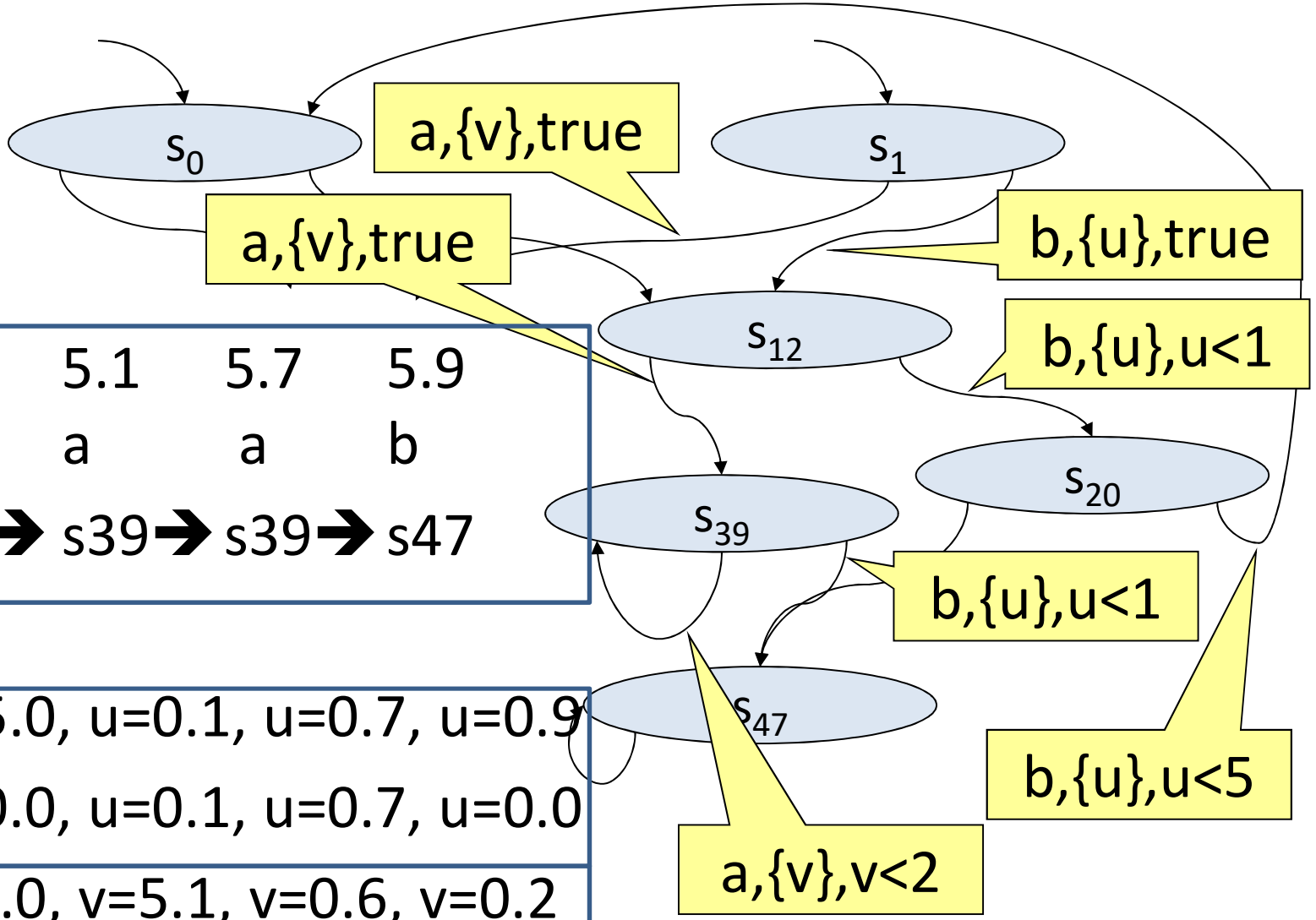


例2-互斥：状态迁移图


s_0
s_1
a,{v},true
a,{v},true
b,{u},true
s_{27}
s_{12}
b,{u},u<1
s_{51}
s_{38}
s_{39}
s_{20}
b,{u},u<1
s_{47}
s_{62}
b,{u},u<5
a,{v},v<2

例2-互斥：状态迁移图

- {u,v}



0.0	5.0	5.1	5.7	5.9
	b	a	a	b
s1 →	s12 →	s39 →	s39 →	s47

u=0.0, u=5.0, u=0.1, u=0.7, u=0.9

u=0.0, u=0.0, u=0.1, u=0.7, u=0.0

v=0.0, v=5.0, v=5.1, v=0.6, v=0.2

v=0.0, v=5.0, v=0.0, v=0.0, v=0.2

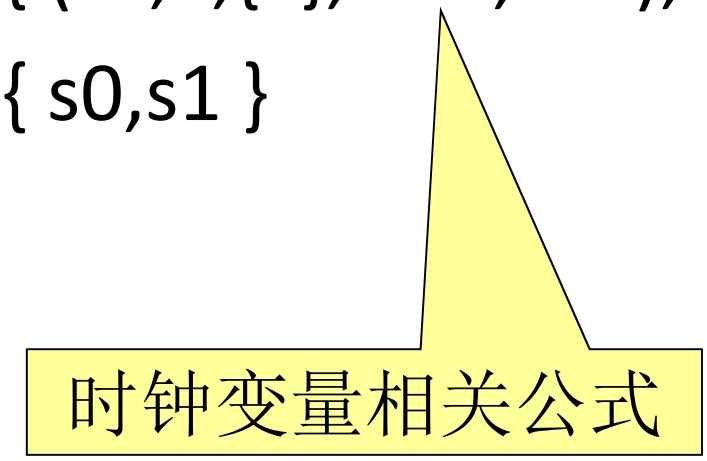
时间迁移系统

- 动作信息　　符号
- 系统状态　　抽象状态
- 时钟变量　　变量集合
- 状态变化　　五元组
- 初始状态　　状态集合

时间迁移系统

时间迁移系统：例子

- 标号集合：　　{ a, b }
- 状态集合：　　{ s0, s1, s2, s3, … }
- 时钟变量集合：　　{ u, v }
- 迁移关系：　　{ (s1,a,{v},true,s12), … }
- 初始状态集：　　{ s0,s1 }



Clocks

X: A set of clock variables

Q: A set of time constants

Let x range over X. Let c range over Q.

The set of clock formulas $\Phi(X)$ is as follows:

$\phi ::= x \leq c \mid c \leq x \mid \neg\phi \mid \phi \wedge \phi$

Valuations

Let R be the set of real numbers.

A valuation is a function $v: X \rightarrow R$.

Notation

v+t denote v' such that $v'(x)=v(x)+t$ for all $x \in X$.

t*v denotev' such that $v'(x)=t*v(x)$ for all $x \in X$.

[Y->t]v denote v' such that:

$v'(x)=t$ for all $x \in Y$, and $v'(x)=v(x)$ for all $x \in X \backslash Y$.

Timed Transition Systems (TTS)

Definition

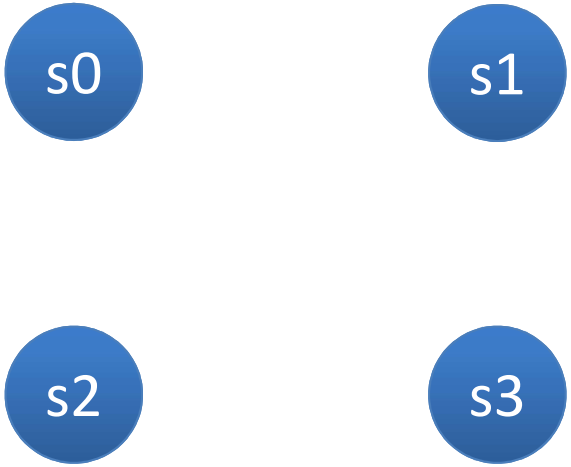
A TTS is a quintuple $<\Sigma,S,X,\Delta,I>$

- Σ : A finite set of symbols
- S : A finite set of states
- X: A finite set of clock variables
- $\Delta \subseteq S \times \Sigma \times 2^X \times \Phi(X) \times S$: A transition relation
- $I \subseteq S$: A set of initial states

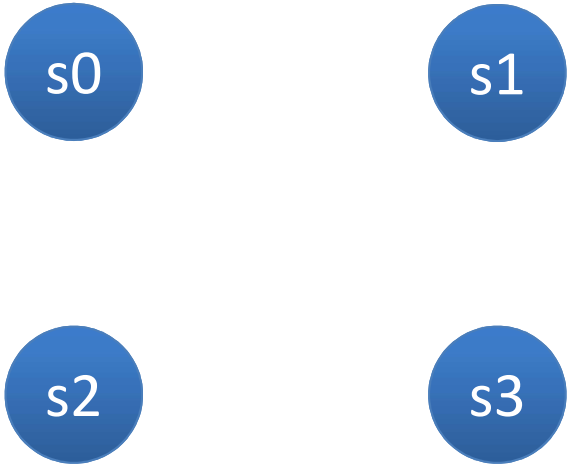
Example: Σ

{a,b,c}

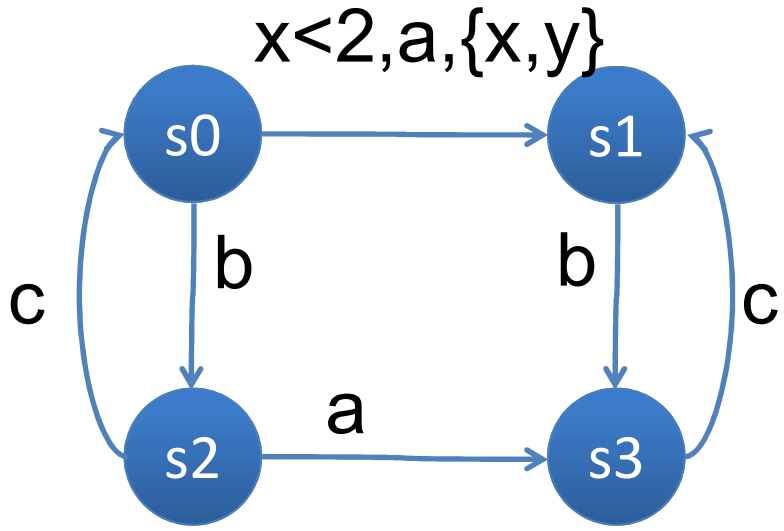
Example: S



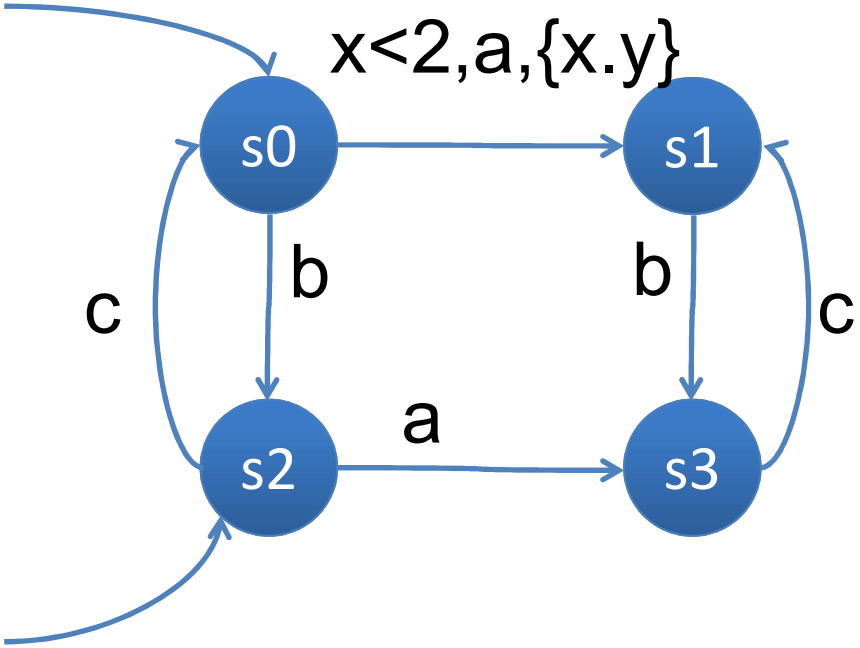
Example: X={x,y,z}



Example: Δ



Example: I



Basic Concepts

States

The set of valuations: $V=X \rightarrow R$.

A state is an element of S x V.

Similar to
Flow Chart
Diagram Models

Timed Words

A timed word is an infinite sequence of Σ x R.

A timed word is denote by $(\sigma,\tau) \in \Sigma^{\omega}$ x R^{ω}.

It is required that $\tau_{i+1} > \tau_i$ (or $\tau_{i+1} \geq \tau_i$) and
for all $t \in R$, there is i such that $\tau_i \geq t$.

Runs

Given $A=<\Sigma,S,X,\Delta,I>$

Definition

Let $(\sigma,\tau) \in \Sigma^{\omega} \times R^{\omega}$.

A **run** of A on (σ,τ) is an infinite sequence $(s_0,v_0)(s_1,v_1)$ .... of S x V such that

$s_0 \in I$, and $v_0 = [X->0]v$;

$\forall i \geq 0, \exists Y \subseteq X, \exists \phi \in \Phi(X), \exists (s_i,\sigma_{i+1},Y,\phi,s_{i+1}) \in \Delta,$

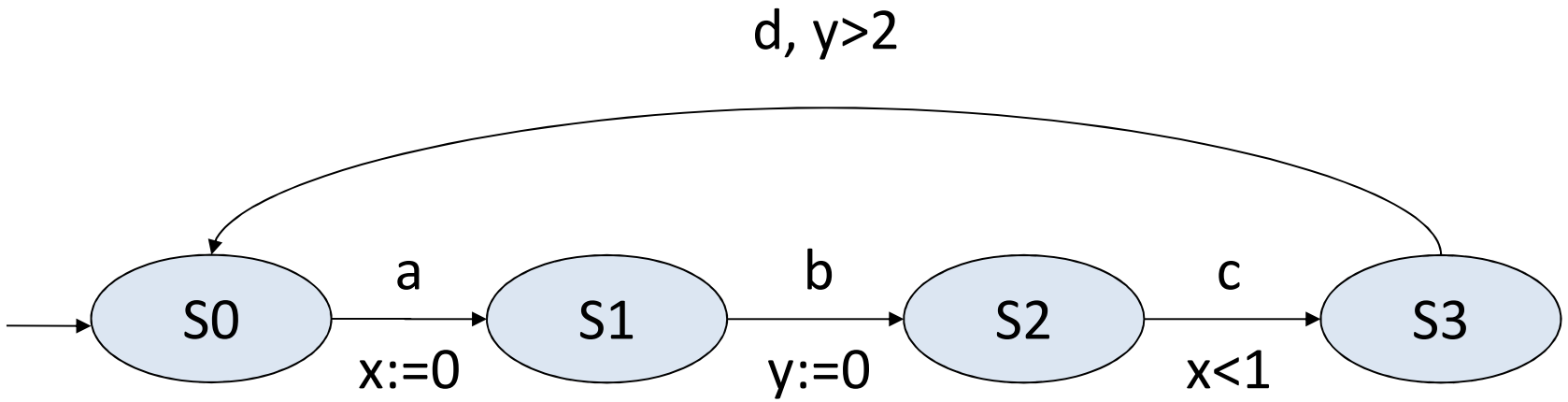
$v_i+\tau_{i+1}-\tau_i \mid = \phi$ and $v_{i+1} = [Y->0](v_i+\tau_{i+1}-\tau_i)$.

Words over Runs

Definition

A **timed word** over a run r of A is an infinite sequence $(\sigma,\tau) \in \Sigma^{\omega} \times R^{\omega}$ such that r is a run on (σ,τ).

时间迁移系统：例子



时间迁移系统：例子

A=<Σ,S,X,Δ,I>其中

Σ={a,b,c,d}

S={s0,s1,s2,s3}

X={x,y}

Δ={

(s0,a,{x},true,s1), (s2,c,{},x<1,s3),

(s1,b,{y},true,s2), (s3,d,{},y>2,s0)

}

I={s0}

时间迁移系统：运行

给定一个时间字符串

$$(a,2) \to (b,2.7) \to (c,2.8) \to (d,5) \cdots\cdots$$

其运行为

$$(s_0,[0,0]) \xrightarrow{a,2}$$
$$(s_1,[0,2]) \xrightarrow{b,2.7}$$
$$(s_2,[0.7,0]) \xrightarrow{c,2.8}$$
$$(s_3,[0.8,0.1]) \xrightarrow{d,5}$$
$$(s_0,[3,2.3]) \cdots\cdots$$

迁移系统的运行集合上的时间字符串为

$$\{((abcd)^\omega,\tau) \mid \forall j.((\tau_{4j+3} < \tau_{4j+1}+1) \wedge (\tau_{4j+4} > \tau_{4j+2}+2))\}$$

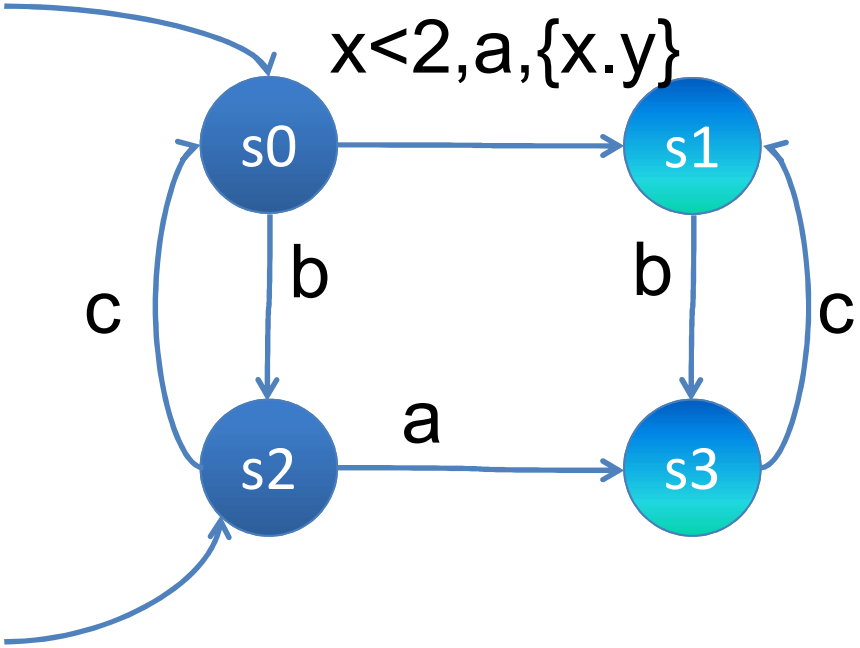
Timed-Automaton

Definition

A timed automaton is a sextuple $<\Sigma,S,X,\Delta,I,F>$

- Σ : A finite set of symbols
- S : A finite set of states
- X: A finite set of clock variables
- $\Delta \subseteq S \times \Sigma \times 2^X \times \Phi(X) \times S$: A transition relation
- $I \subseteq S$: A set of initial states
- $F \subseteq S$: A set of acceptance states

Example: F={s1,s3}



Accepting Runs

Let inf(r) be the set of states
that appear infinitely many times on r.

Definition
An **accepting run** of A is a run r of A
such that $\inf(r) \cap F \neq \emptyset$.

Accepting Words

Definition

An **accepting word** of A is

a word over some accepting run of A.

Language

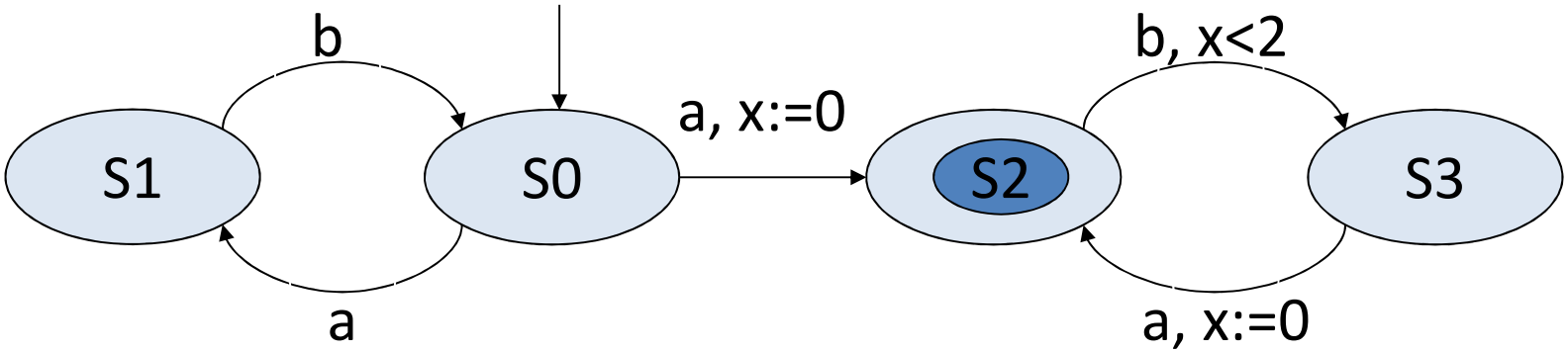
Definition

The language of A is

the set of accepting words of A.

The language of A is denoted L(A).

时间Büchi自动机1



时间Büchi自动机1

A=<Σ,S,X,Δ,I,F> 其中

Σ={a,b}

S={s0,s1,s2,s3}

X={x,y}

Δ={ (s0,a,{},true,s1), (s0,a,{x},true,s2),

(s1,b,{},true,s0), (s2,b,{},x<2,s3),

(s3,a,{x},true,s2)

}

I={s0}

F={s2}

时间Büchi自动机1：运行/语言

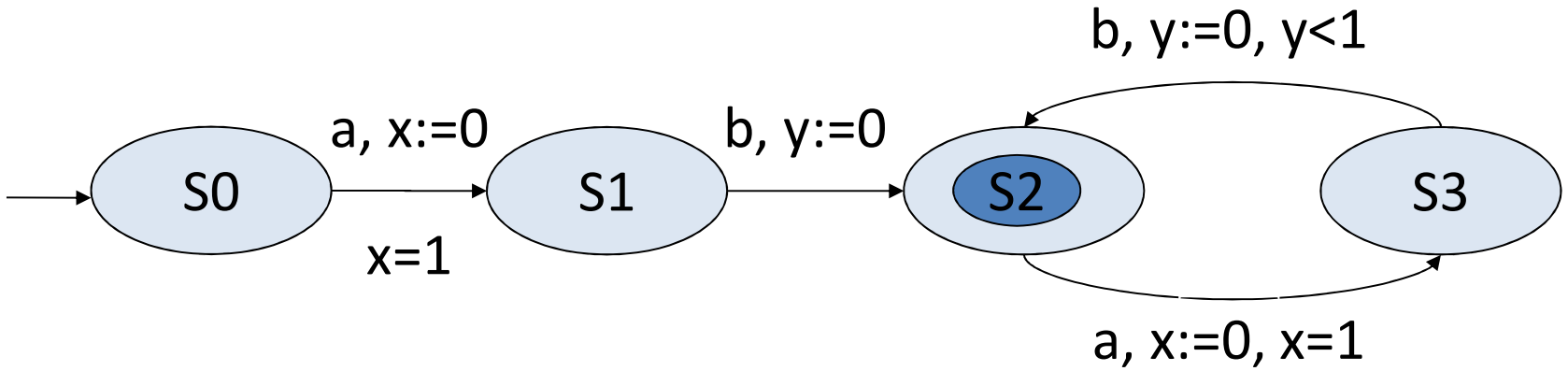
其运行的集合上的时间字符串为

$$\{((ab)^{\omega}, \tau)) \mid \forall j.(\tau_j < \tau_{j+1})\}$$

其语言为

$$\{((ab)^{\omega}, \tau) \mid \exists i. \forall j \geq i.(\tau_{2j} < \tau_{2j-1} + 2)\}$$

时间Büchi自动机2



时间Büchi自动机2

$A = \langle \Sigma, S, \Delta, I, F \rangle$ 其中

$\Sigma = \{a, b\}$ 。

$S = \{s_0, s_1, s_2, s_3\}$ 。

$\Delta = \{$

$(s_0, a, \{x\}, x = 1, s_1),\ (s_2, a, \{x\}, x = 1, s_3),$

$(s_1, b, \{y\}, true, s_2),\quad (s_3, b, \{y\}, y < 1, s_2)$

$\}$ 。

$I = \{s_0\}$ 。

$F = \{s_2\}$ 。

时间Büchi自动机2：运行/语言

其运行的集合上的时间字符串与其语言为

$$\{((ab)^{\omega},\tau)\,|\,\forall j.((\tau_{2j-1}=j)\wedge(\tau_{2j}-\tau_{2j-1}>\tau_{2j+2}-\tau_{2j+1}))\}$$

其一个句子为

$$(a,1)\rightarrow(b,1.5)\rightarrow(a,2)\rightarrow(b,2.25)\rightarrow(a,3)\rightarrow(b,3.125)\rightarrow\cdots$$

其一个性质为

$$\lim_{j\rightarrow\inf}(\tau_{j+2}-\tau_{j})=1$$

Basic Properties

Reachability:

states (locations) + time-constraints

Safety

Inevitability

Operations

Union

Intersection

Not closed under complementation.

Emptiness Problem

Let A be a TA.

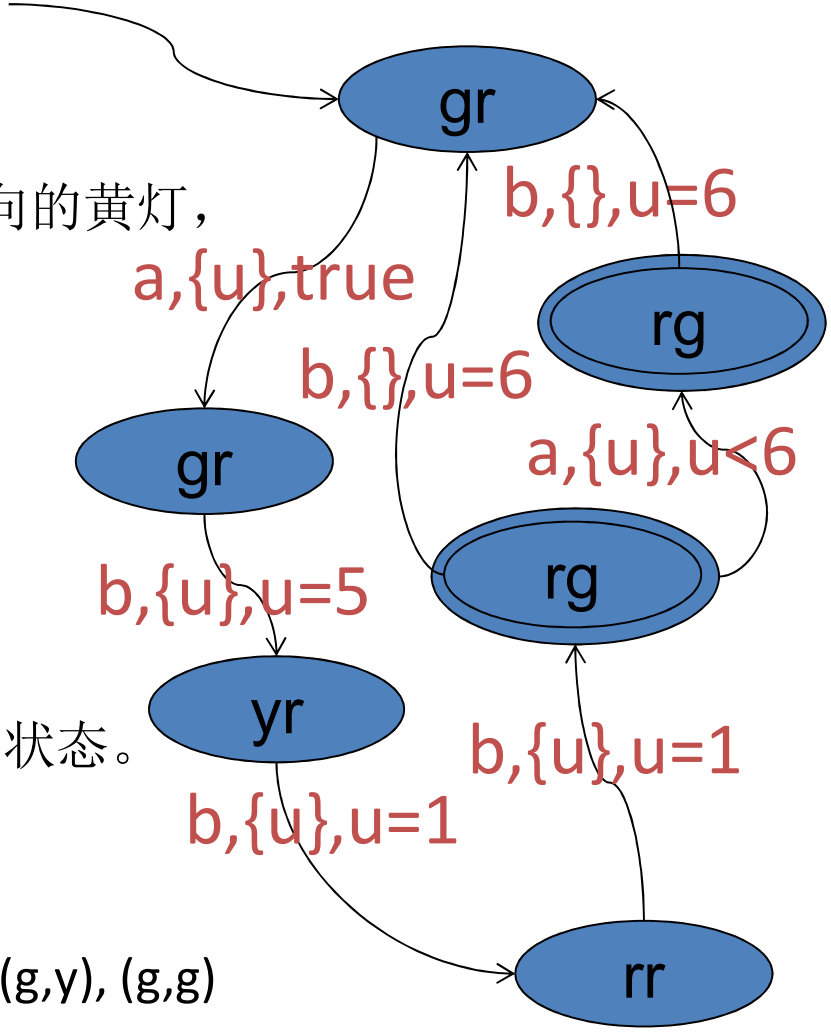
$L(A)=\emptyset$?

PSPACE-complete.

例子

假设在一条街上，有行人过街用的红绿灯。
正常的时候是汽车绿灯和行人红灯。
行人按了绿色按钮之后5个时间单位有汽车方向的黄灯，
然后在1个时间单位后变成红灯，
又1个时间单位后有行人方向的绿灯。
汽车方向的红灯持续6个时间单位后恢复原状。

若在这6个时间单位中有行人按绿灯，
则红灯保持至行人按路灯之后6个时间单位。
系统的有效运行须包括无限次的行人方向绿灯状态。



状态(car,p): (r,r), (r,y), (r,g), (y,r), (y,y), (y,g), (g,r), (g,y), (g,g)
动作: a(按按钮), b(内部动作)

例子

A=<Σ,S,X,Δ,I,F> 其中

Σ={a,b}

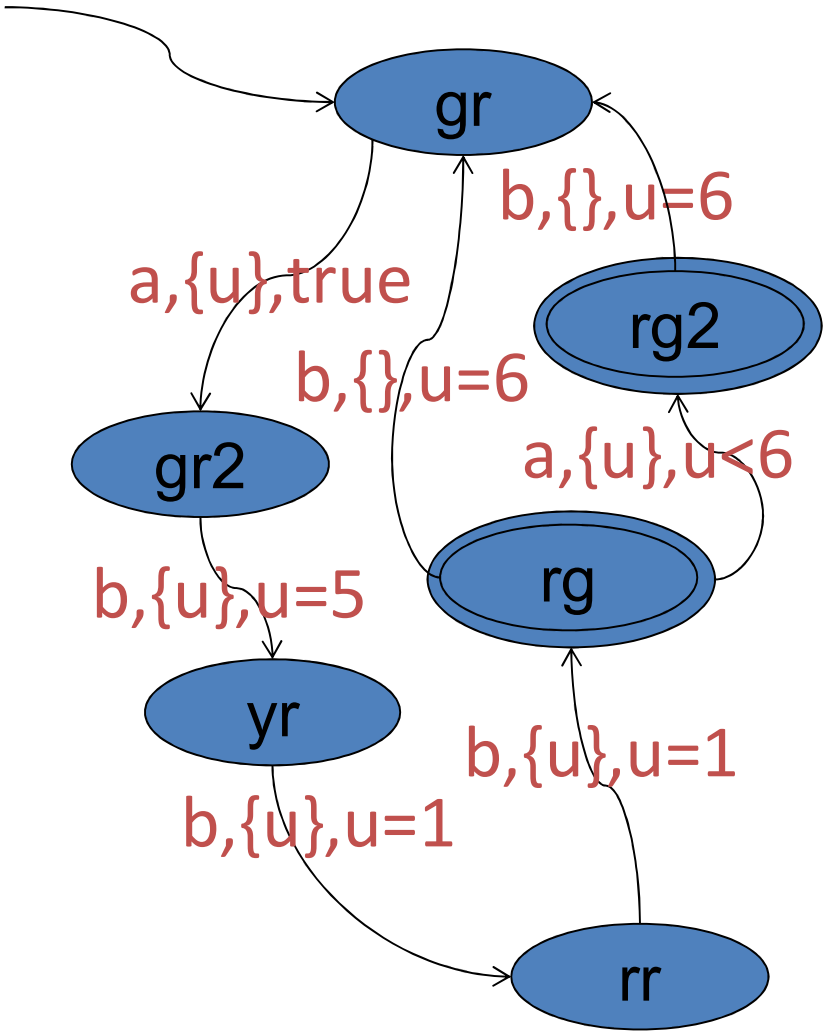
S={gr,gr2,yr,rr,rg,rg2}

X={u}

Δ={ (gr,a,{u},true,gr2),
(gr2,b,{u},u=5,yr),
(yr,b,{u},u=1,rr),
(rr,b,{u},u=1,rg),
(rg,a,{u},u<6,rg2),
(rg,b,{},u=6,gr),
(rg2,b,{},u=6,gr) }

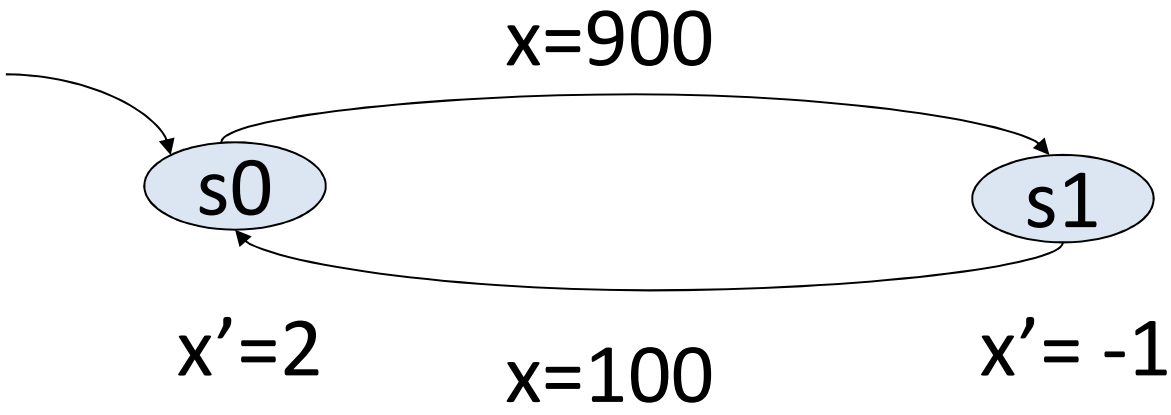
I={gr}

F={rg,rg2}



(II) Hybrid Systems (Hybrid Automata)

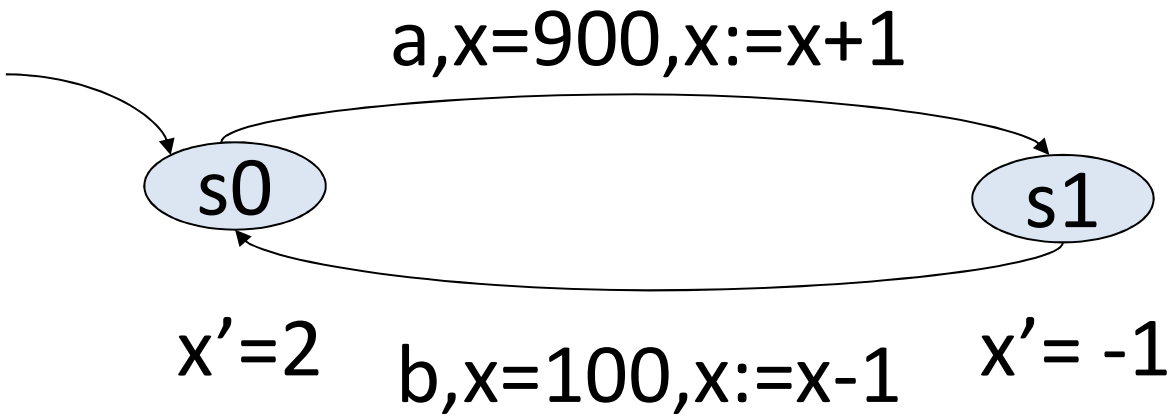
水箱控制



$x=x_0+2t$

$x=x_0-t$

水箱控制



$x=x_0+2t$

$x=x_0-t$

Timed TS (for comparison)

Definition

A timed transition system is a quintuple $<\Sigma,S,X,\Delta,I>$

- Σ : A finite set of symbols
- S : A finite set of states
- X: A finite set of clock variables
- $\Delta \subseteq S \times \Sigma \times 2^X \times \Phi(X) \times S$: A transition relation
- $I \subseteq S$: A set of initial states

Hybrid -Systems

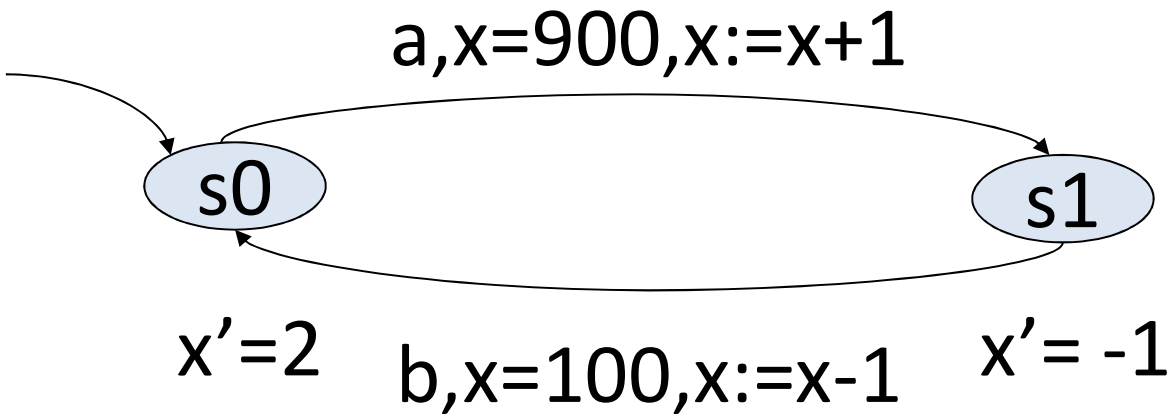
Definition

A hybrid system is a sextuple $<\Sigma,S,X,\Delta,I,flow>$

- Σ : A finite set of symbols
- S : A finite set of states
- X: A set of n real variables
- $\Delta \subseteq S \times \Sigma \times \Phi(X) \times \oplus(X) \times S$: A transition relation
- $I \subseteq S \times (2^R)^n$: A set of initial states
- flow: $S \rightarrow \Phi(X,X')$

$\oplus(X)$: $X \rightarrow (R^n \rightarrow R)$ $\Phi(Z)$: predicates over Z

水箱控制



$x=x_0+2t$

$x=x_0-t$

States

A set of control states: S

A set of variables: X

The set of valuations: $V = X \rightarrow R$.

$v \in V$ denotes:
$(v(x1),\ldots,v(xn)) \in R^n$

A system state is an element of $S \times V$.

Time-Transitions:

$\delta \geq 0$: $(s,v0) \rightarrow^{\delta} (s,v1)$

$\exists f$ such that f is differentiable, and

$f: [0,\delta] \rightarrow R^n$

$f(0) = v0$

$f(\delta) = v1$

$\forall \zeta \in (0,\delta).flow(s)[X/f(\zeta)][X'/f'(\zeta)]=true$

Action-Transitions:

$\sigma \in \Sigma$: (s0,v0) $\rightarrow^{\sigma}$ (s1,v1)

$\exists$ $\lambda \in \oplus(X)$, $\varphi \in \Phi(X)$, $(s0,\sigma,\varphi,\lambda,s1) \in \Delta$,

$\{z1,\ldots,zk\}=dom(\lambda)$,

such that

$v0 \models \varphi$,

$v1 = v0[z1/\lambda(z1)(v0)]\ldots[zk/\lambda(zk)(v0)]$

Runs on Timed-Words

timed-word: $(\sigma,\tau) =$ $(\sigma 1,\tau 1)\,(\sigma 2,\tau 2)\ldots\ldots$

run on (σ,τ): $r=$ $(s0,v0)(s1,v1)\ldots\ldots$

$(s0,v0) \in I$, and

$(s(i),v(i)) \rightarrow^{\tau(i+1)-\tau(i)} (s(i),v^*)$

$(s(i),v^*) \rightarrow^{\sigma(i+1)} (s(i+1),v(i+1))$

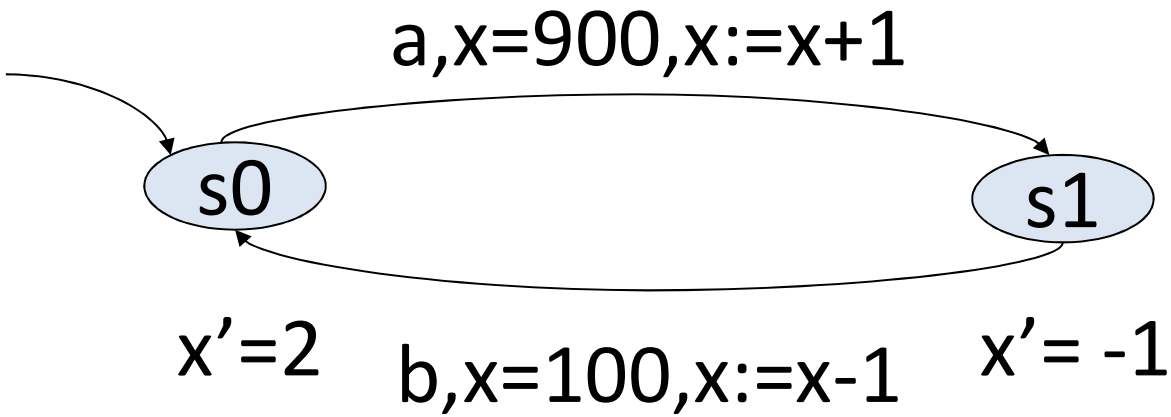
Runs

r is a run, if

there exists a timed word (σ,τ)

such that r is a run on (σ,τ)

水箱控制



$x=x_0+2t$

$x=x_0-t$

水箱控制

A=<Σ,S,X,Δ,I,flow> 其中

Σ={a,b}

S={s0,s1}

X={x}

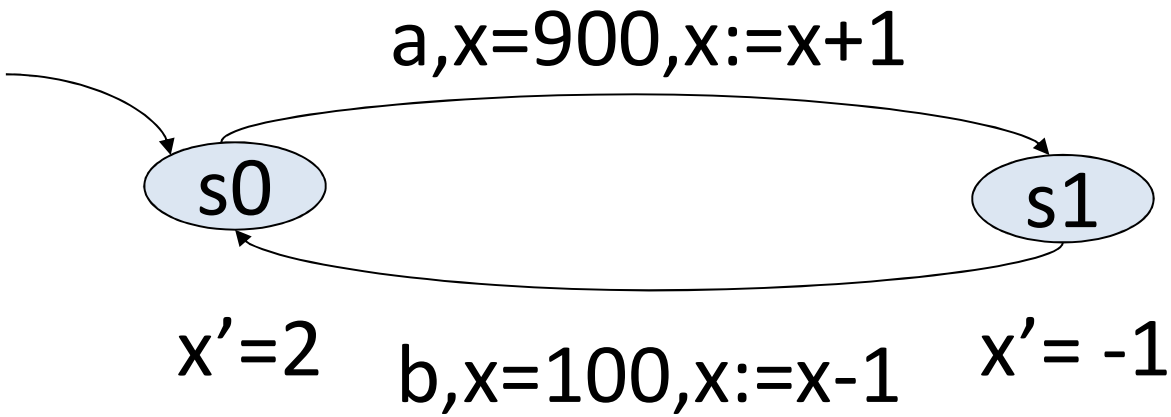
Δ={ (s0,a,λ0,x=900,s1), (s1,b,λ1,x=100,s0) }

I={(s0,[0])}

flow(s0)=(x'=2), flow(s1)=(x'=-1)

λ0(x)=(x+1), λ1(x)=(x-1)

安全性质: x<1000



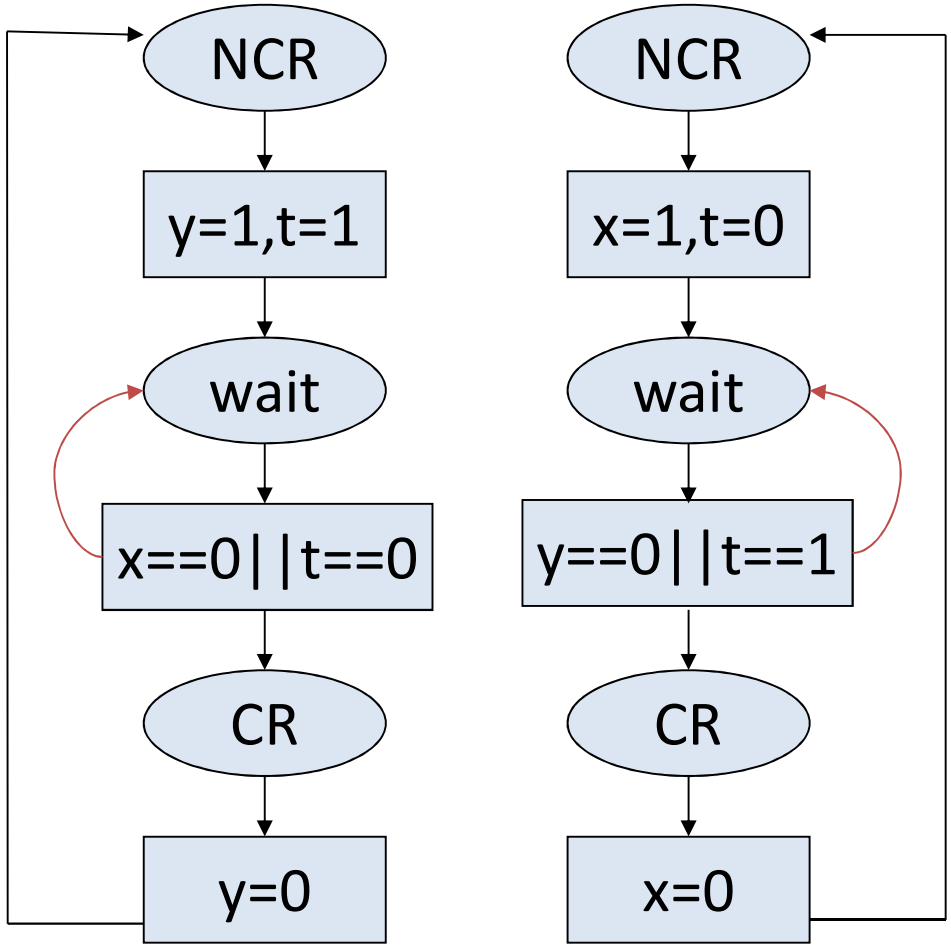
$x=x_0+2t$ $x=x_0-t$

Hybrid Automata

Hybrid System + Acceptance Condition

(III) Petri Nets

系统运行过程描述：例子



初始状态

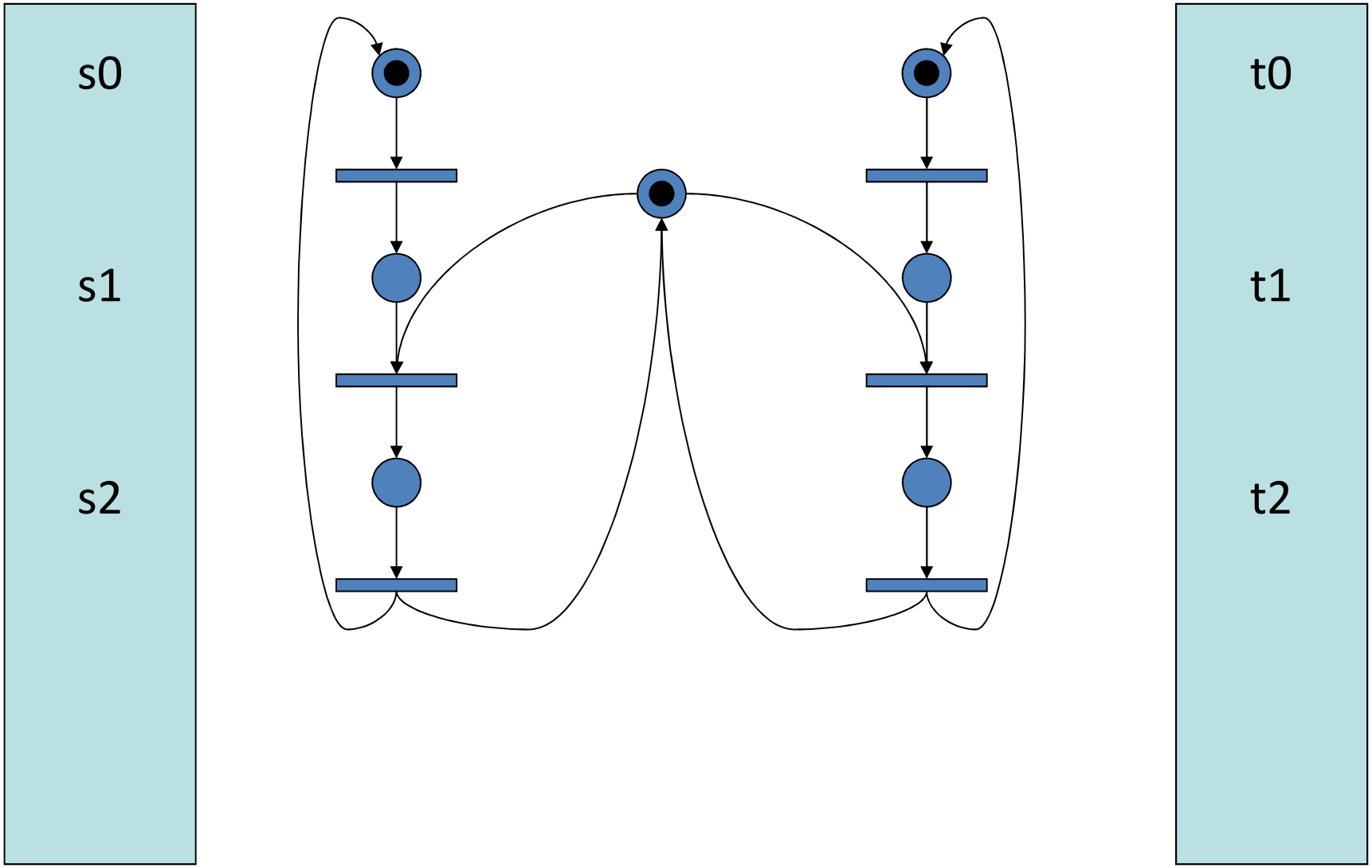
s0

t0

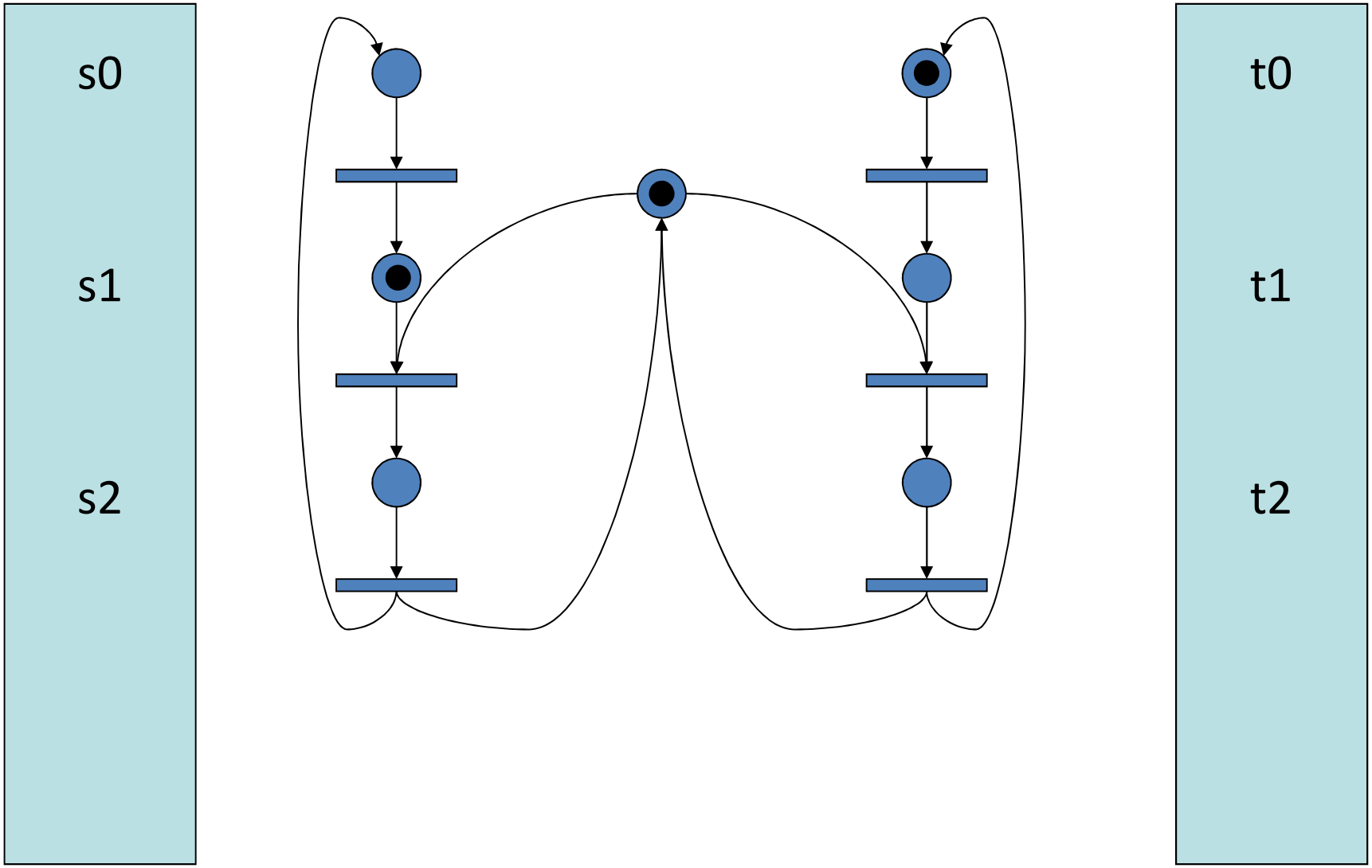
x=0

y=0

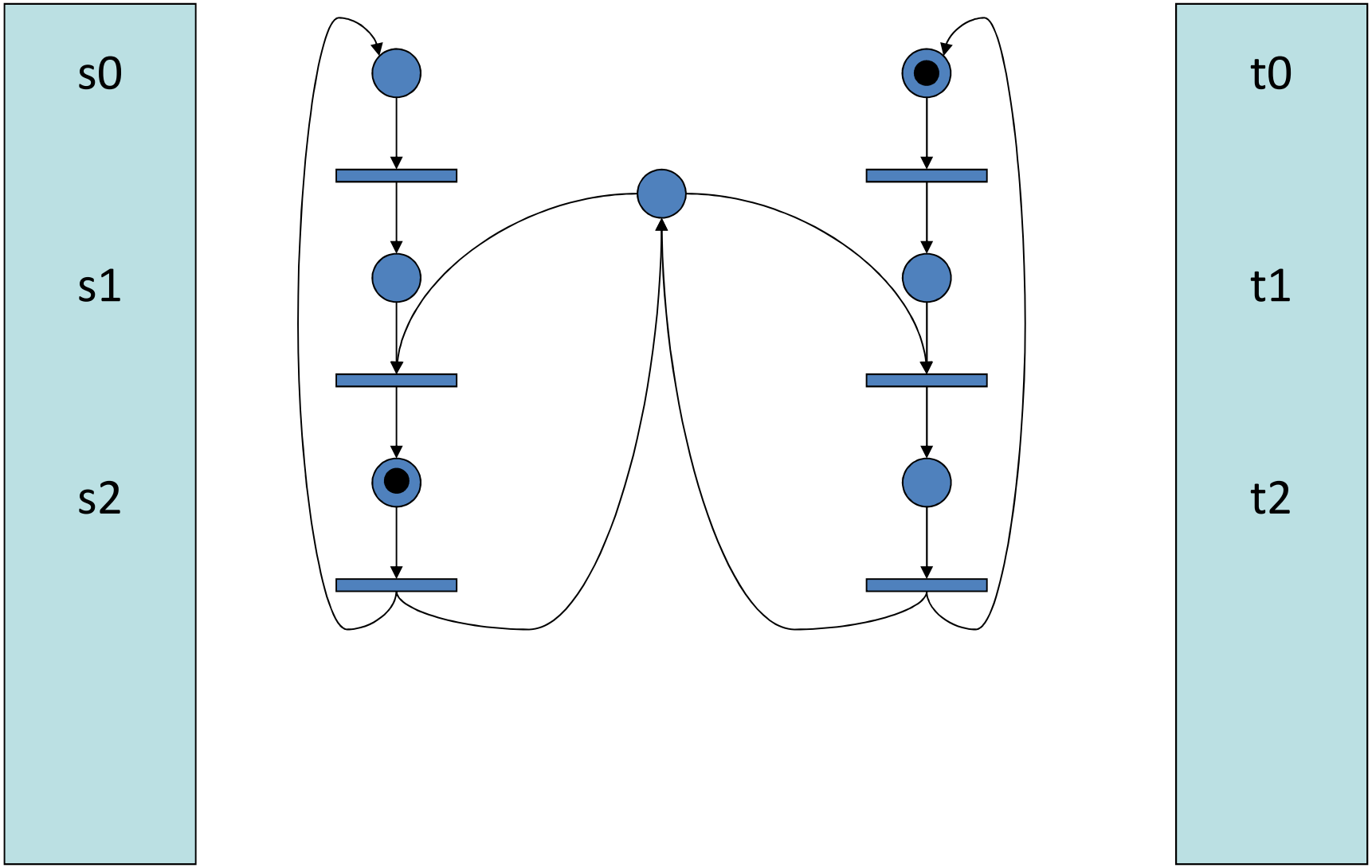
系统资源模型



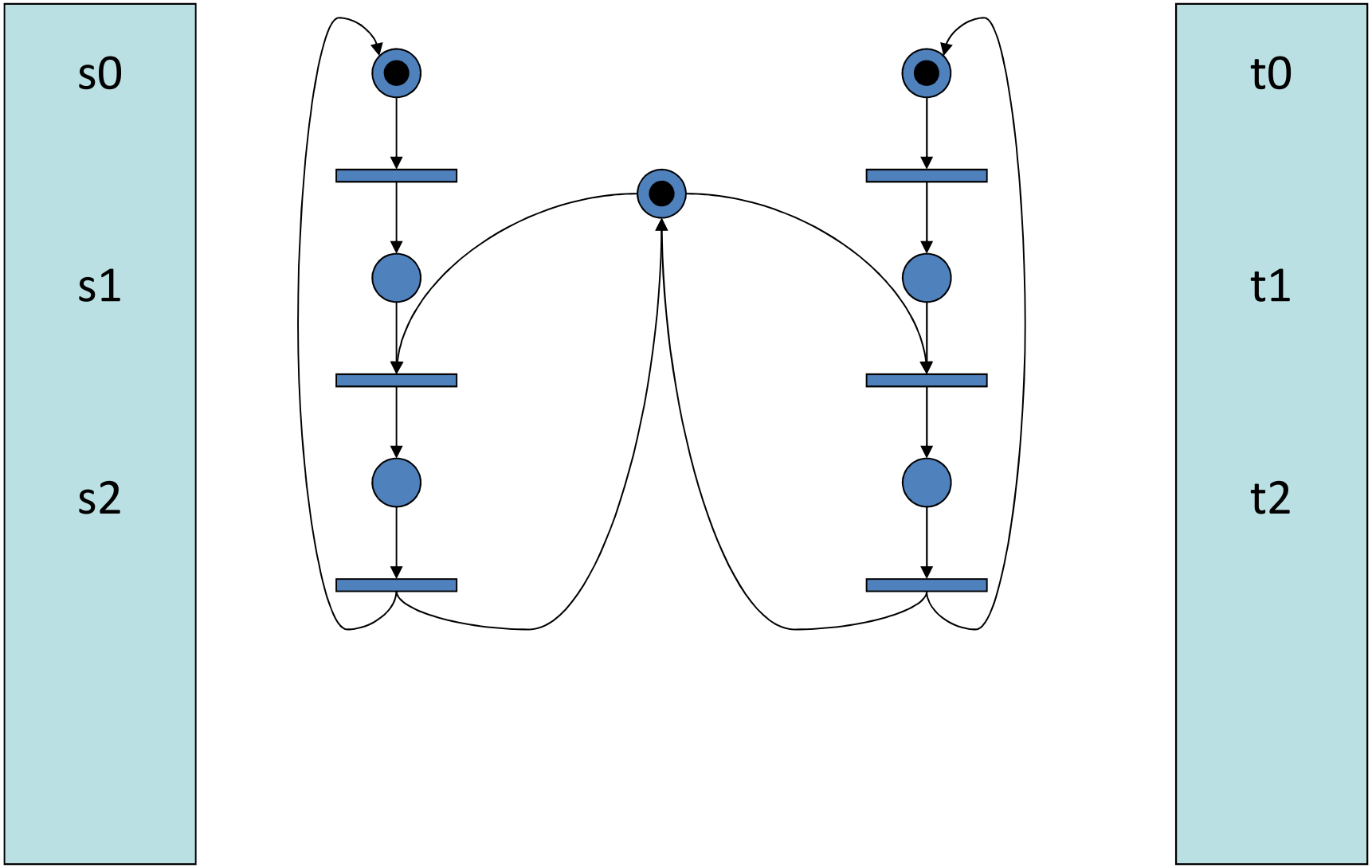
系统资源模型



系统资源模型



系统资源模型

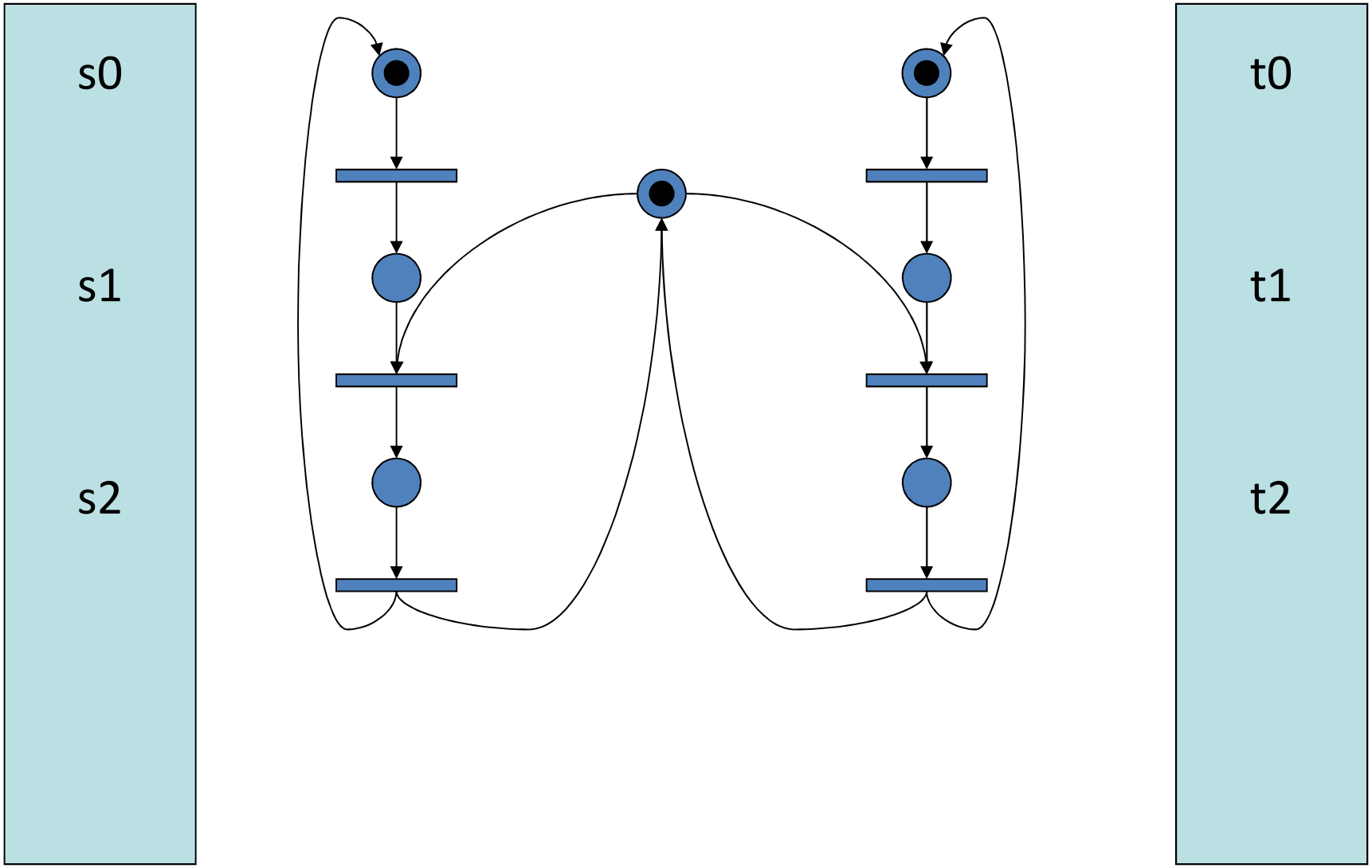


Petri网

- 位置　　抽象元素
- 迁移　　抽象元素
- 状态变化描述　　边（两种）
- 初始状态　　位置标号

Petri网

系统资源模型



Petri网：例子

- 位置集合： { s0,…,s2,t0,…,t2, ts }
- 迁移集合： { u0,…,u2,v0,…,v2 }
- 边的集合： { (s0,u0),(u0,s1),(s1,u1),(ts,u1),…}
- 初始状态： M: M(s0)=1,M(s1)=0,M(s2)=0,…

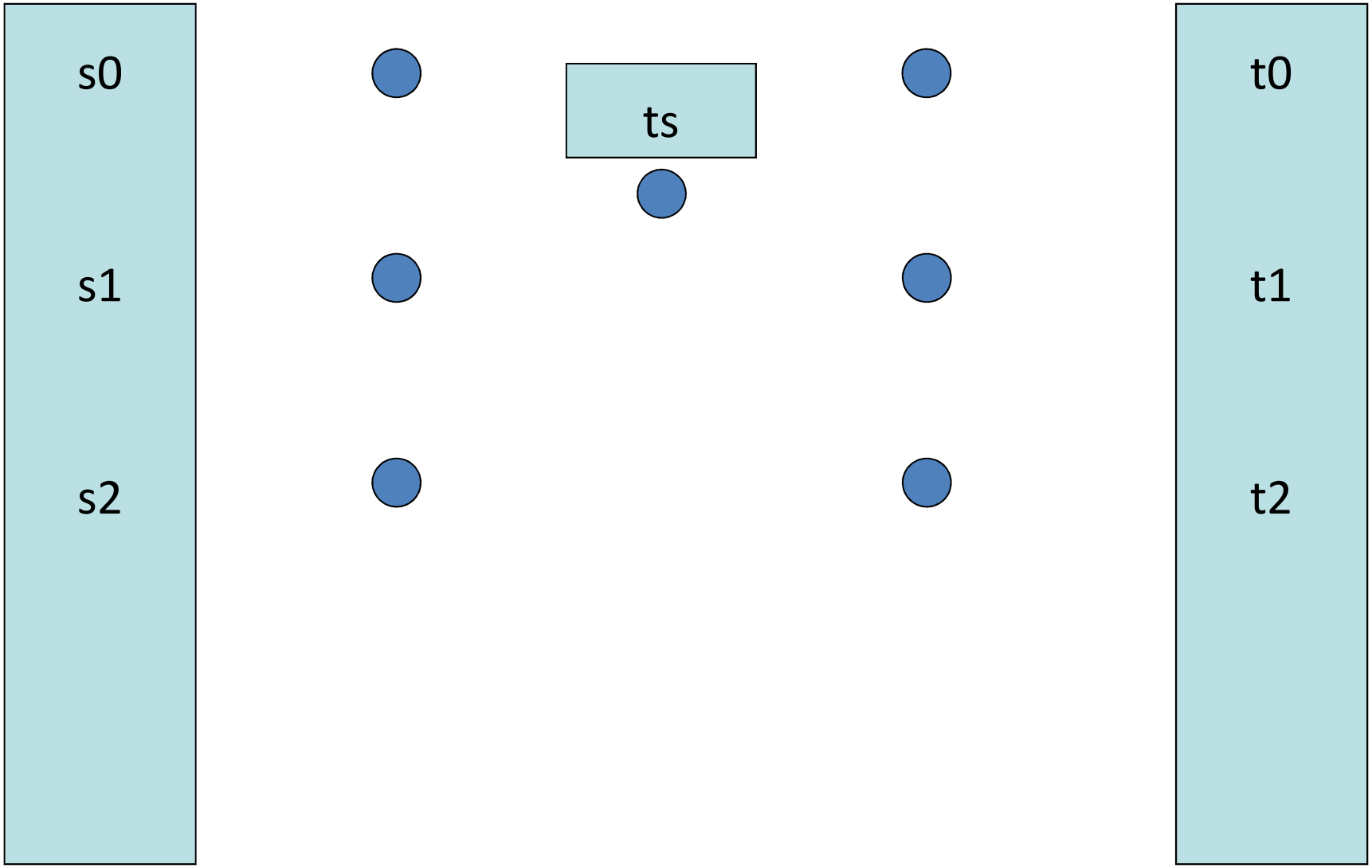
Petri Nets

Definition

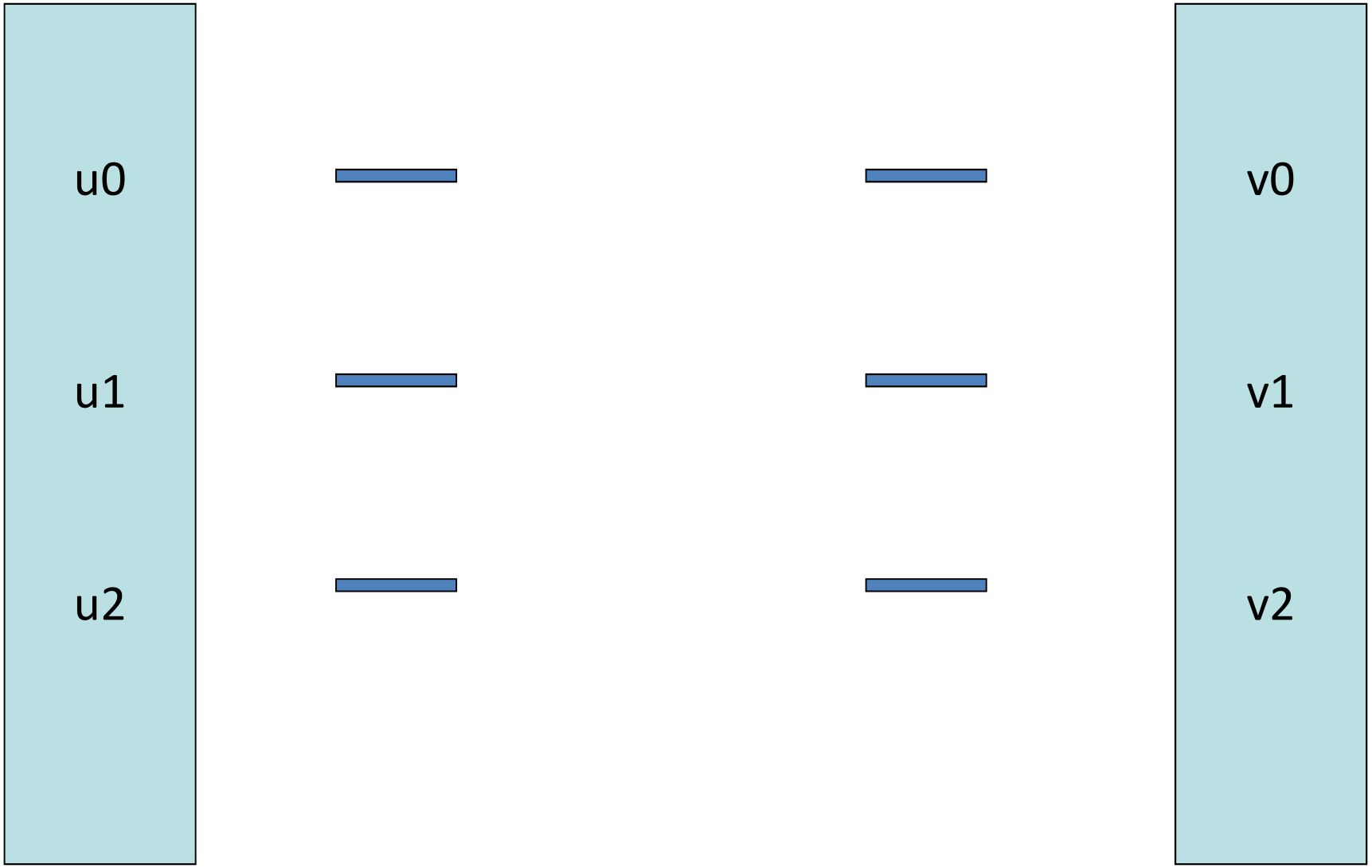
A Petri-net is a quadruple $<P,T,F,M_0>$

- P : A finite set of places
- T : A finite set of transitions
- $F \subseteq (P \times T) \cup (T \times P)$: A set of edges
- M_0: P→N, the initial marking/state

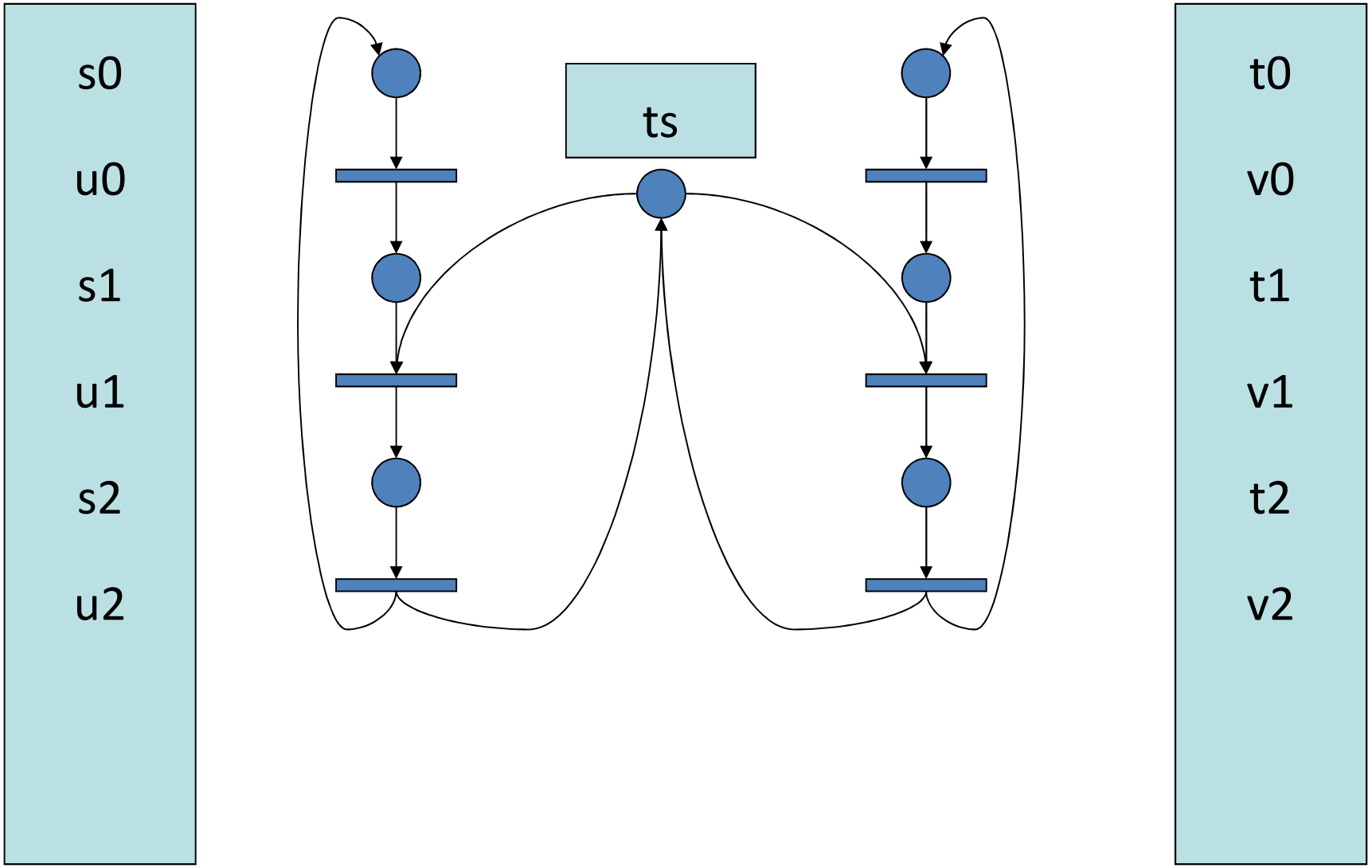
Example: Places



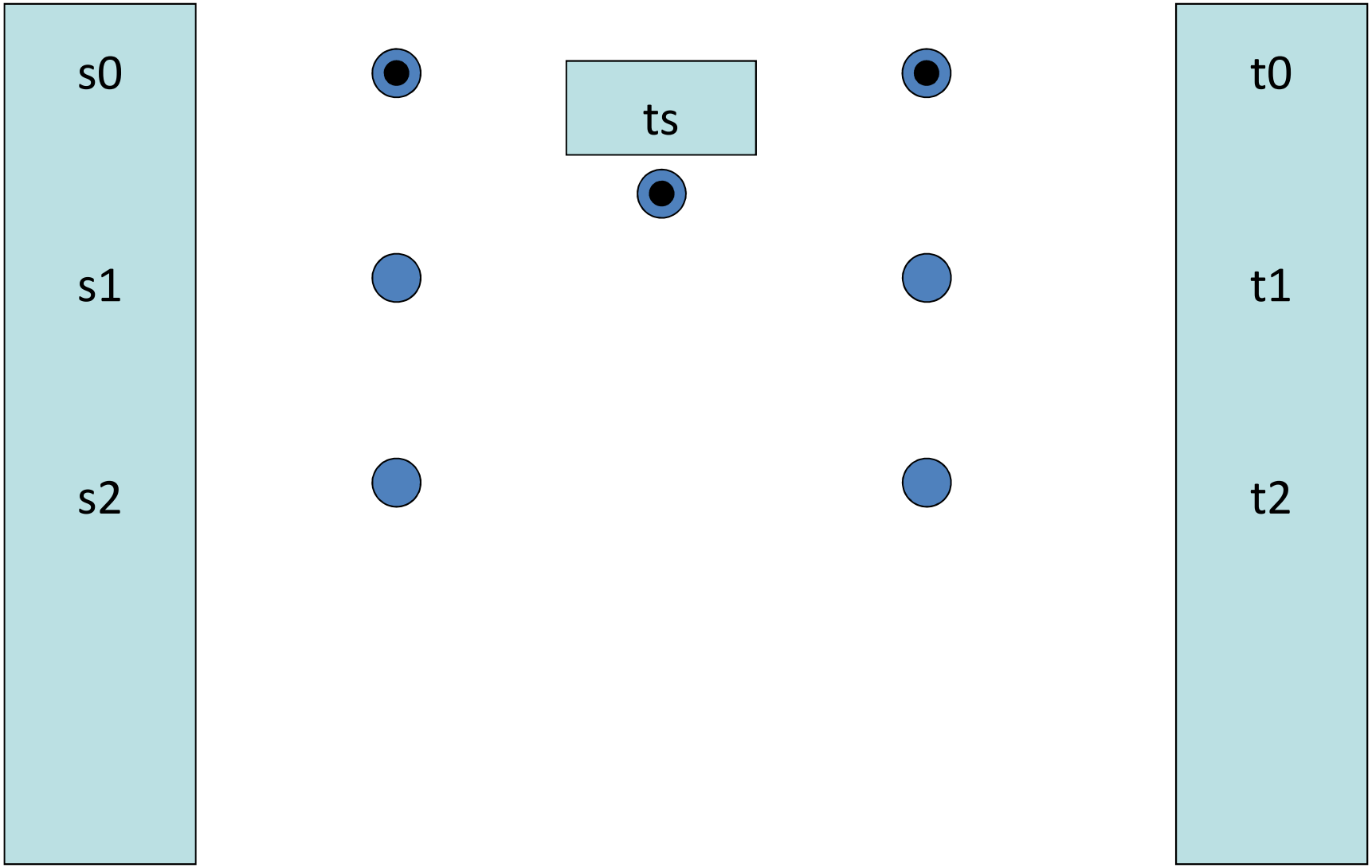
Example: Transitions



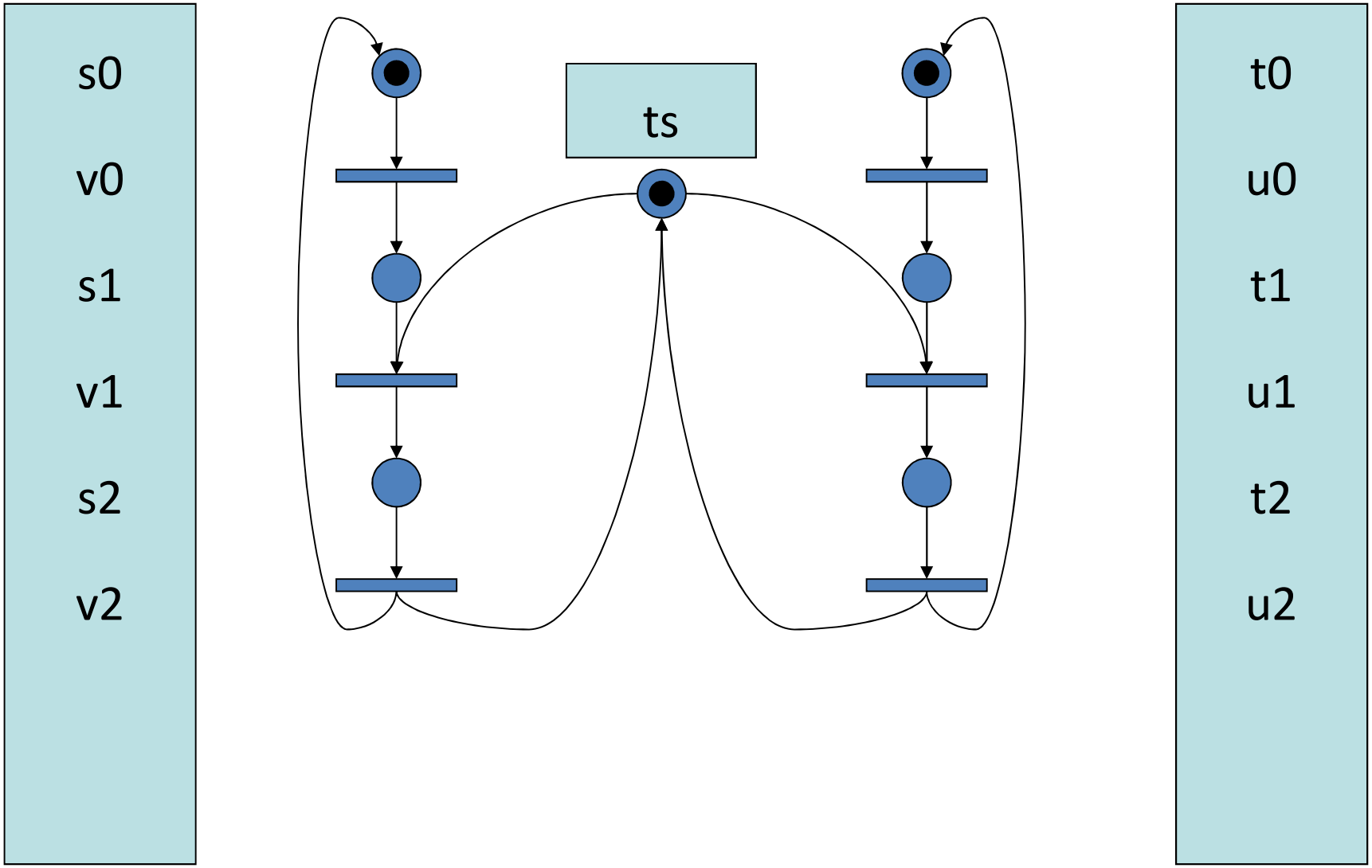
Example: F



Example: M_0



Example: A Compete Model



Basic Concepts

States

Markings

M: P→N

Transitions

$^{o}p(t) = \{ p \in P \mid (p,t) \in F \}$

$p^{o}(t) = \{ p \in P \mid (t,p) \in F \}$

t is executable/fireable at state M,

iff $\forall p \in {}^{o}p(t).M(p) \geq 1$.

$M \rightarrow^{t} M'$ denote t is executable/fireable at M, and

$\forall p.(M'(p)=M(p)-(p \in {}^{o}p(t))+(p \in p^{o}(t))$

$M \rightarrow M'$ iff there is some t such that $M \rightarrow^{t} M'$

or there is no executable t at M and M=M'.

Computations

Definition

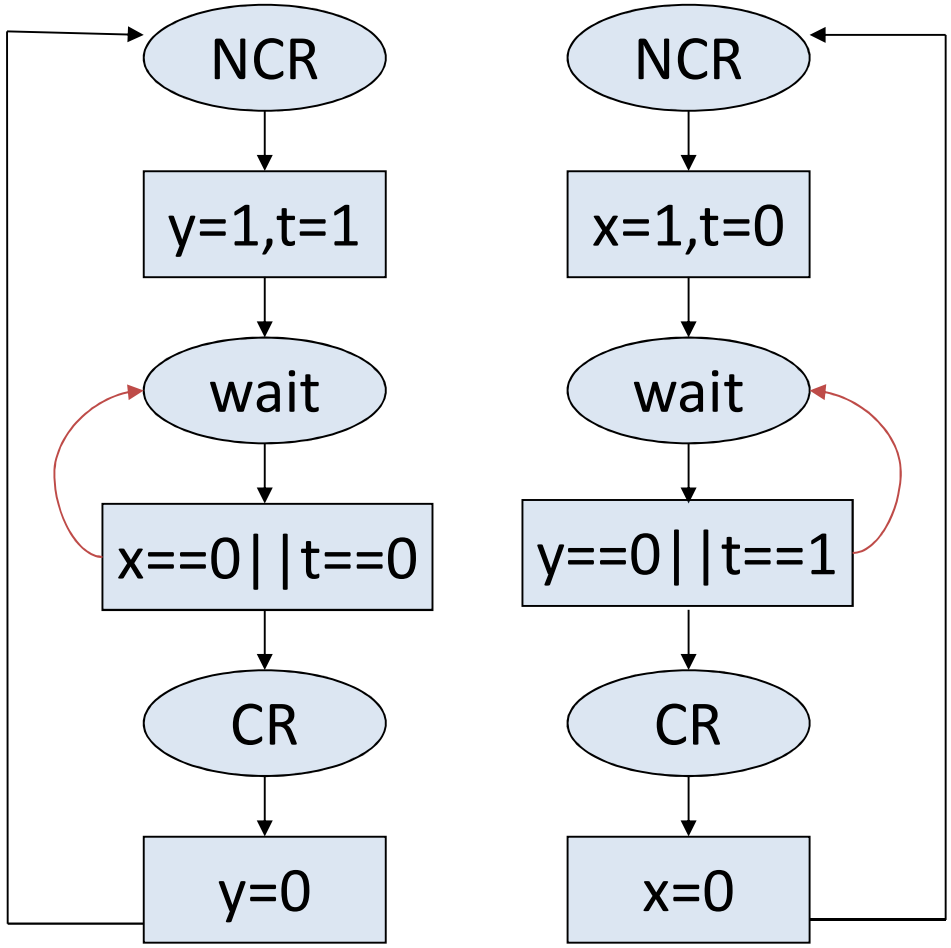
A **computation** of PN=<P,T,F,M_0> is

an infinite sequence of P→N:

$X_0X_1X_2$ ….

such that $X_0 = M_0$, and $X_i \rightarrow X_{i+1}$ for all $i \geq 0$

系统运行过程描述：例子



初始状态

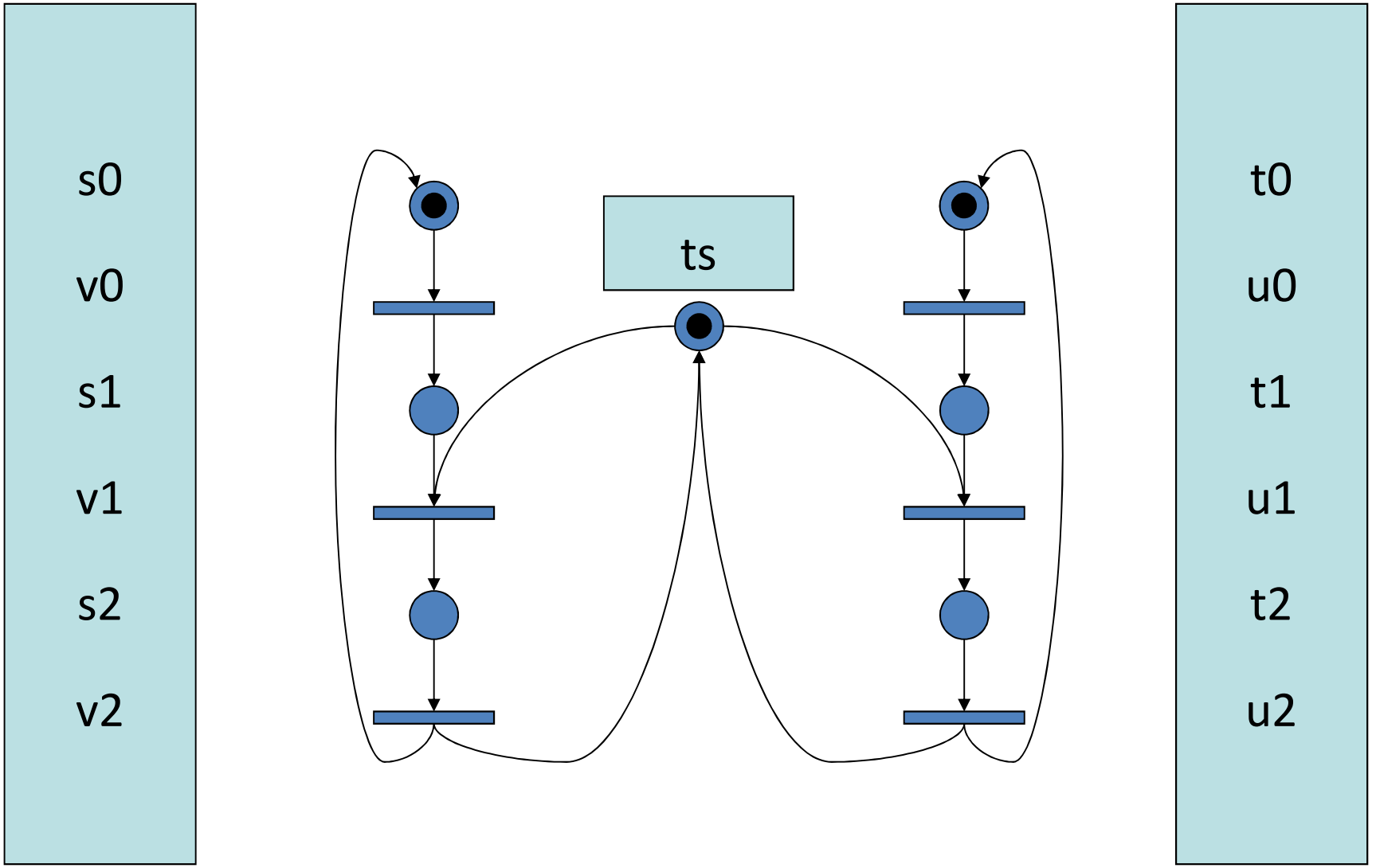
s0

t0

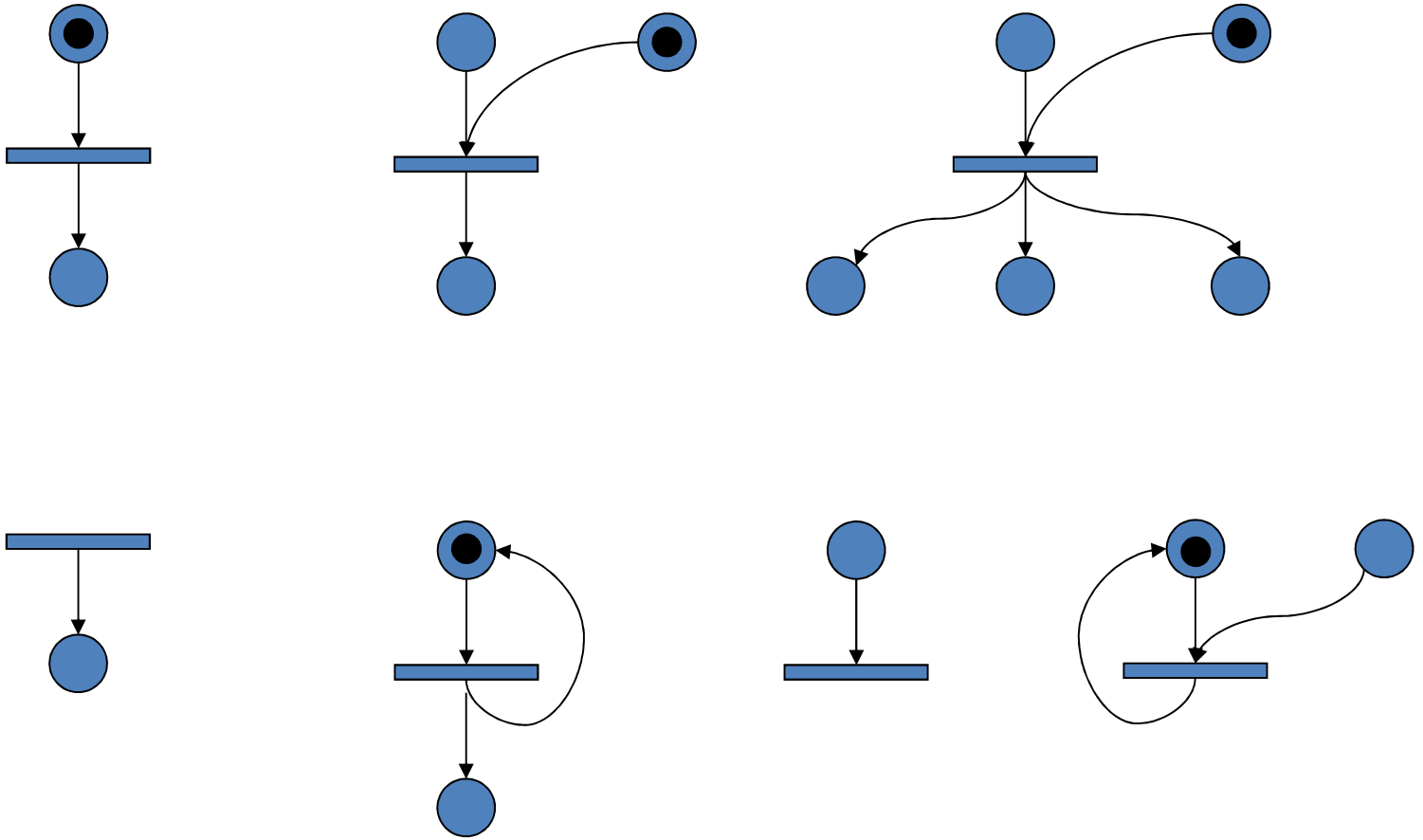
x=0

y=0

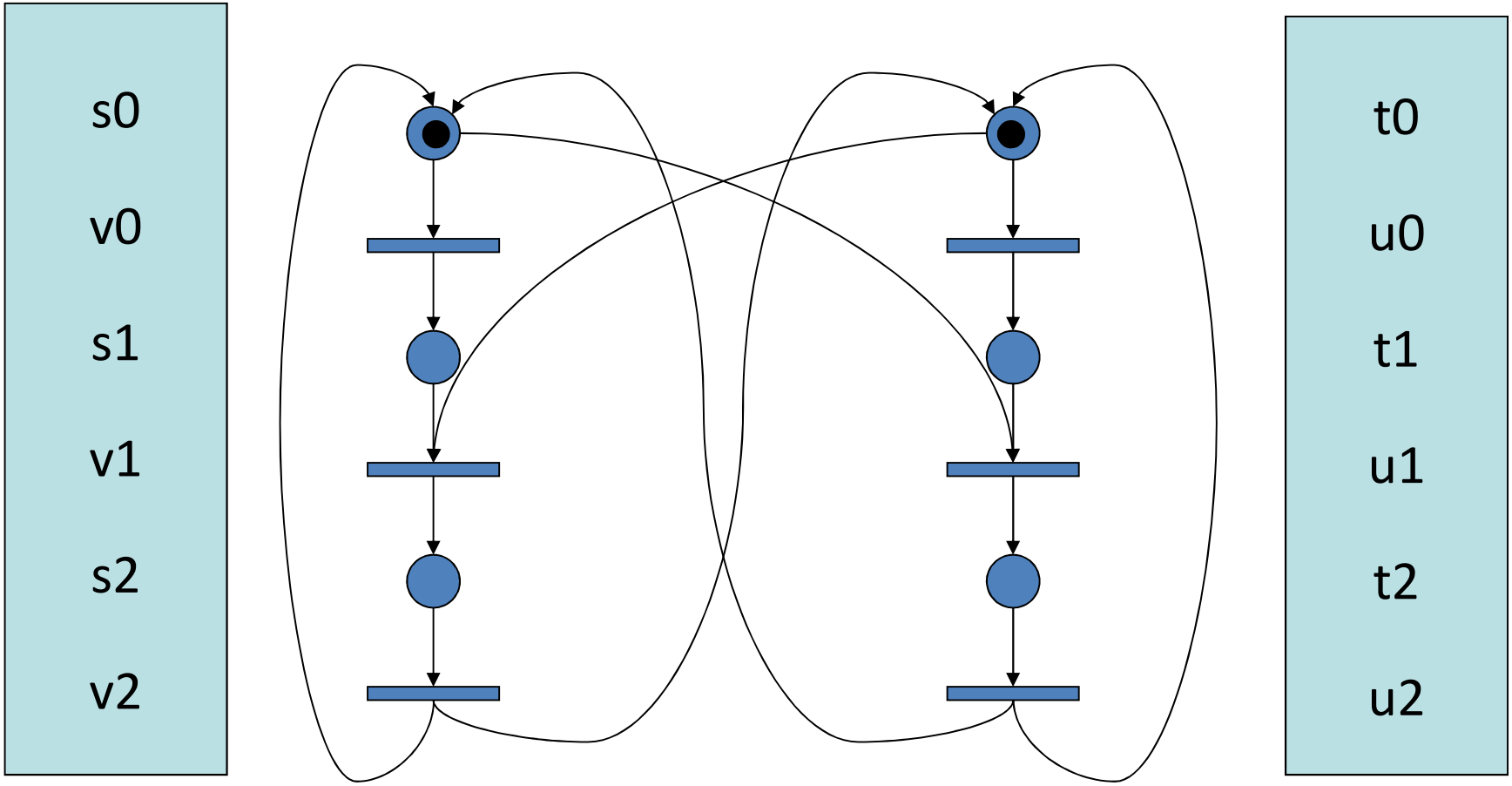
Example:



Example:



Example: 有问题的系统资源模型



Reachability

The set of reachable states $\{ M \mid M_0 \rightarrow^* M \}$

Reachability Problem

Given X: P→N.

Is $X \in \{ M \mid M_0 \rightarrow^* M \}$?

The reachability problem is decidable and is EXPSPACE-hard.

Liveness

Dead

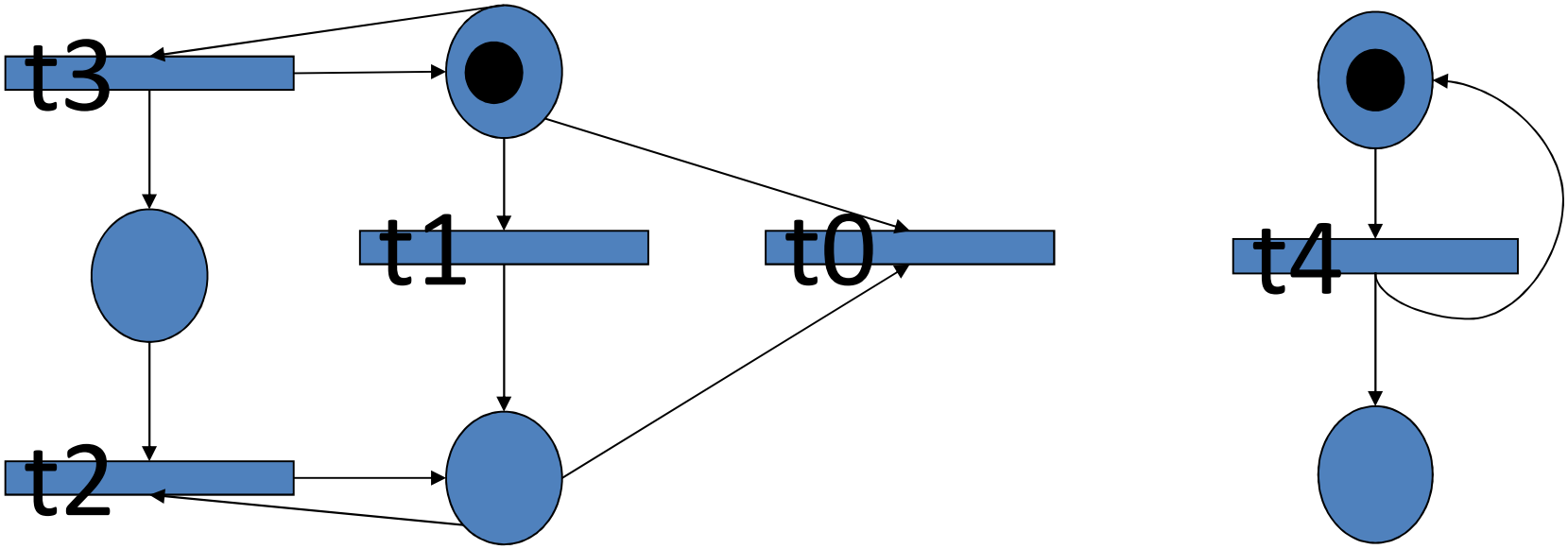
May fire

Can fire arbitrary often

Can fire infinitely often

Can always fire

Example: Liveness



Safe Petri-Nets

A Petri-net is k-bounded, if

$\forall M$ such that $M_0 \rightarrow^* M$, $M(p) \leq k$.

A Petri-net is called safe Petri-nets, if

$\forall M$ such that $M_0 \rightarrow^* M$, $M(p) \leq 1$.

The reachability problem of safe Petri-nets is PSPACE-complete.

(IV) Summary

- Timed Transition Systems and Timed Automata
- Hybrid Systems and Hybrid Automata
- Petri-Nets

练习(1):

用时间自动机描述交通灯的变化。
要求信号灯的周期性变化次序为绿、黄、红，
且黄灯的长度为1，绿灯的长度不小于10，
红灯的长度不小于10，
变化周期绿、黄、红的总长度为30。

思考：能否设计一个模型使得若绿红两灯的长度差别不为零则长度差别逐渐减少？

练习(2):

设有四个生产者A、B、C、D和一个消费者E。
用Petri网描述以下过程。

A不停地生产零件a，
B不停地生产零件b，
C使用a和b生产零件c，
D使用a和c生产产品d，
E不停地消费产品d。