## §2 程序与系统模型

以下是两个进程的互斥协议。系统状态可分成两个部分：进程的指针位置和进程的变量状态。

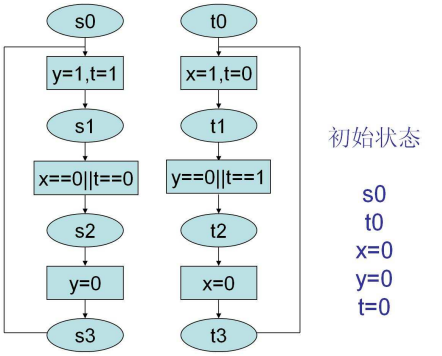


图 1 互斥协议的流程

用 $a$ 和 $b$ 分别表示第一个进程和第二个进程的指针位置。对于进程的初始状态，我们设定进程的指针位置 $(a,b)=(s_0,t_0)$，进程的变量状态 $(x,y,t)=(0,0,0)$。

### §2.3 一阶迁移系统 (FTS)

设 $B=(F,P)$ 和 $V$ 如下：

$$\begin{array}{lcl} F & = & \{0,1,s_0,s_1,s_2,s_3,t_0,t_1,t_2,t_3\} \\ P & = & \{=\} \\ V & = & \{a,b,x,y,t\} \end{array}$$

$I=(Int,I_0)$

$$\begin{array}{lcl} I_0(s_0)=I_0(t_0)=I_0(0) & = & 0 \\ I_0(s_1)=I_0(t_1)=I_0(1) & = & 1 \\ I_0(s_2)=I_0(t_2) & = & 2 \\ I_0(s_3)=I_0(t_3) & = & 3 \\ I_0(=) & = & = \end{array}$$

互斥算法表示为 $(B,V)$ 上的迁移系统 $(T,\Theta)$ 如下：

| | | | |
|---|---|---|---|
| $T$ | $a=s_0$ | $\longrightarrow$ | $(y,t,a):=(1,1,s_1)$ |
| | $a=s_1\wedge(x=0\vee t=0)$ | $\longrightarrow$ | $(a):=(s_2)$ |
| | $a=s_2$ | $\longrightarrow$ | $(y,a):=(0,s_3)$ |
| | $a=s_3$ | $\longrightarrow$ | $(y,t,a):=(1,1,s_1)$ |
| | $b=t_0$ | $\longrightarrow$ | $(x,t,b):=(1,0,t_1)$ |
| | $b=t_1\wedge(y=0\vee t=1)$ | $\longrightarrow$ | $(b):=(t_2)$ |
| | $b=t_2$ | $\longrightarrow$ | $(x,b):=(0,t_3)$ |
| | $b=t_3$ | $\longrightarrow$ | $(x,t,b):=(1,0,t_1)$ |
| $\Theta$ | $(a=s_0\wedge b=t_0\wedge x=0\wedge y=0\wedge t=0)$ | | |

**状态空间**

$\Sigma = \{(a,b,x,y,t)\,|\,a,b \in \{0,1,2,3\}, x,y,t \in \{0,1\}\}$ 。

**初始状态**

系统的初始状态集合为 $\{(s_0,t_0,0,0,0)\}$ 。

**运行**

系统运行为 $\Sigma$ 上的无穷字符串。为阅读方便 $a,b$ 的取值写为 $s_0,t_0$ 等。以下是两个例子。

$$(s_0,t_0,0,0,0)(s_1,t_0,0,1,1)(s_1,t_1,1,1,0)(s_2,t_1,1,1,0)\cdots$$
$$(s_0,t_0,0,0,0)(s_0,t_1,1,0,0)(s_1,t_1,1,1,1)(s_1,t_2,1,1,1)\cdots$$

**状态迁移**

见图 ?? 。

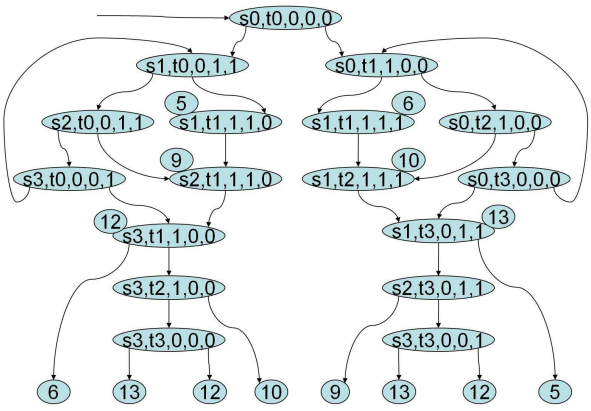


图 2 部分由 $(s_0,t_0,0,0,0)$ 可达的状态的迁移关系

**可达状态**

可达状态有 17 个。可达状态的集合 $rh(\Theta)$ 如下：

| | | |
|---|---|---|
| $(s_0,t_0,0,0,0)$ | $(s_1,t_0,0,1,1)$ | $(s_0,t_1,1,0,0)$ |
| $(s_2,t_0,0,1,1)$ | $(s_1,t_1,1,1,1)$ | $(s_1,t_1,1,1,0)$ |
| $(s_0,t_2,1,0,0)$ | $(s_3,t_0,0,0,1)$ | $(s_2,t_1,1,1,0)$ |
| $(s_1,t_2,1,1,1)$ | $(s_0,t_3,1,0,1)$ | $(s_3,t_1,1,0,0)$ |
| $(s_1,t_3,0,1,1)$ | $(s_3,t_2,1,0,0)$ | $(s_2,t_3,0,1,1)$ |
| $(s_3,t_3,0,0,0)$ | $(s_3,t_3,0,0,1)$ | |

**安全性质**

系统的互斥性质是一种安全性质，表示为

$$\neg(a = s_2 \wedge b = t_2)$$

该系统满足该安全性质，即 $\forall\sigma \in rh(\Theta).\sigma \models_I \varphi$ 。

## §2.4 Kripke 结构和标号 Kripke 结构

### §2.4.1 Kripke 结构 (KS)

状态可以是个抽象的概念, 根据其不同用不同的符号表示。比如互斥协议的 128 个状态可以用 $z_0, z_1, ..., z_{127}$ 表示。对于互斥协议, 假定状态 $z_0, z_1, ..., z_{127}$ 依照 $(a, b, x, y, t)$ 所取的值的字母顺序命名。

#### 状态空间

互斥协议的状态空间可表示为 $S = \{z_0, z_1, ..., z_{127}\}$ 。

#### 初始状态

互斥协议的初始状态集合为 $I = \{z_0\}$ 。

#### 运行

系统运行为 $S$ 上的无穷字符串。以下是两个例子。

$$z_0 z_{35} z_{46} z_{78} \cdots$$
$$z_0 z_{12} z_{47} z_{55} \cdots$$

#### 状态迁移

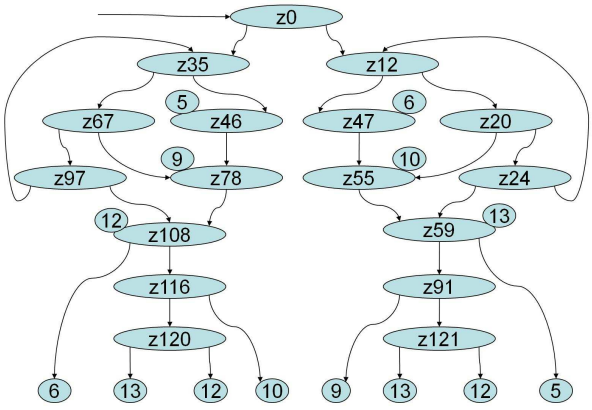


图 3 部分由 $z_0$ 可达的状态的迁移关系

定义 $a(i) = i/32$, $b(i) = (i\%32)/8$, $x(i) = (i\%8)/4$, $y(i) = (i\%4)/2$, $t(i) = (i\%2)$, 互斥协议的一阶迁移系统表示的 8 条迁移分别对应以下迁移集合

$$\{(z_i, z_{35+4\times(i/4)}) \mid a(i) = 0\}$$
$$\{(z_i, z_{i+32)}) \mid a(i) = 1 \wedge (x(i) = 0 \vee t(i) = 0)\}\}$$
$$\{(z_i, z_{i+32-2\times y(i)}) \mid i/32 = 2\}\}$$
$$\{(z_i, z_{i-61-i\%4}) \mid i/32 = 3\}\}$$
$$\{(z_i, z_{i+12}) \mid (i\%32)/8 = 0\}$$
$$\{(z_i, z_{i+32)}) \mid (i\%32)/8 = 1 \wedge i\%4 \neq 2\}\}$$
$$\{(z_i, z_{i+32-2\times(i\%2))}) \mid (i\%32)/8 = 2\}\}$$
$$\{(z_i, z_{i-61-i\%4}) \mid (i\%32)/8 = 3\}\}$$

系统的迁移关系就是上面的集合的并集, 包含以下由可达状态出发的 26 条迁移。

| | | | |
|---|---|---|---|
| $(z_0, z_{35})$ | $(z_0, z_{12})$ | | |
| $(z_{35}, z_{67})$ | $(z_{35}, z_{46})$ | $(z_{12}, z_{47})$ | $(z_{12}, z_{20})$ |
| $(z_{67}, z_{97})$ | $(z_{67}, z_{78})$ | $(z_{46}, z_{78})$ | $(z_{47}, z_{55})$ |
| $(z_{97}, z_{108})$ | $(z_{97}, z_{35})$ | $(z_{78}, z_{108})$ | $(z_{55}, z_{59})$ |
| $(z_{108}, z_{12})$ | $(z_{108}, z_{116})$ | $(z_{59}, z_{83})$ | $(z_{59}, z_{47})$ |
| $(z_{116}, z_{120})$ | $(z_{116}, z_{55})$ | $(z_{83}, z_{121})$ | $(z_{83}, z_{78})$ |
| $(z_{120}, z_{58})$ | $(z_{120}, z_{108})$ | $(z_{121}, z_{59})$ | $(z_{121}, z_{108})$ |

**可达状态**

互斥协议的 17 个可达状态表示如下：

| | | |
|---|---|---|
| $z_0 : (s_0, t_0, 0, 0, 0)$ | $z_{35} : (s_1, t_0, 0, 1, 1)$ | $z_{12} : (s_0, t_1, 1, 0, 0)$ |
| $z_{67} : (s_2, t_0, 0, 1, 1)$ | $z_{47} : (s_1, t_1, 1, 1, 1)$ | $z_{46} : (s_1, t_1, 1, 1, 0)$ |
| $z_{20} : (s_0, t_2, 1, 0, 0)$ | $z_{97} : (s_3, t_0, 0, 0, 1)$ | $z_{78} : (s_2, t_1, 1, 1, 0)$ |
| $z_{55} : (s_1, t_2, 1, 1, 1)$ | $z_{24} : (s_0, t_3, 0, 0, 0)$ | $z_{108} : (s_3, t_1, 1, 0, 0)$ |
| $z_{59} : (s_1, t_3, 0, 1, 1)$ | $z_{116} : (s_3, t_2, 1, 0, 0)$ | $z_{91} : (s_2, t_3, 0, 1, 1)$ |
| $z_{120} : (s_3, t_3, 0, 0, 0)$ | $z_{121} : (s_3, t_3, 0, 0, 1)$ | |

**安全性质**

系统的互斥性质表示为

$$A = \{\sigma_i \mid \frac{i}{32} \neq 2\} \cup \{\sigma_i \mid \frac{i\%32}{8} \neq 2\}$$

该系统满足该安全性质，即 $rh(I) \subseteq A$ 。

**可达性分析算法**

error_state(q) 即 $q \in S - A = \{\sigma_i | \frac{i}{32} = 2\} \cap \{\sigma_i | \frac{i\%32}{8} = 2\} = \{\sigma_i \mid \frac{i}{8} = 10\}$ 。

### §2.4.2 标号 KS

假设我们有以下命题：

| | |
|---|---|
| $p_0 \equiv (x = 0)$ | $p_1 \equiv (x = 1)$ |
| $p_2 \equiv (y = 0)$ | $p_3 \equiv (y = 1)$ |
| $p_4 \equiv (t = 0)$ | $p_5 \equiv (t = 1)$ |
| $p_{6+i} \equiv (a = s_i) \quad i \in \{0, 1, 2, 3\}$ | $p_{10+i} \equiv (b = t_i) \quad i \in \{0, 1, 2, 3\}$ |

互斥算法的例子中，我们有

| | |
|---|---|
| $L(z_0) = \{p_6, p_{10}, p_0, p_2, p_4\}$ | $L(z_{35}) = \{p_7, p_{10}, p_0, p_3, p_5\}$ |
| $L(z_{12}) = \{p_6, p_{11}, p_1, p_2, p_4\}$ | $L(z_{67}) = \{p_8, p_{10}, p_0, p_3, p_5\}$ |
| $L(z_{47}) = \{p_7, p_{11}, p_1, p_3, p_5\}$ | $L(z_{46}) = \{p_7, p_{11}, p_1, p_3, p_4\}$ |
| $L(z_{20}) = \{p_6, p_{12}, p_1, p_2, p_4\}$ | $L(z_{97}) = \{p_9, p_{10}, p_0, p_2, p_5\}$ |
| $L(z_{78}) = \{p_8, p_{11}, p_1, p_3, p_4\}$ | $L(z_{55}) = \{p_7, p_{12}, p_1, p_3, p_5\}$ |
| $L(z_{24}) = \{p_6, p_{13}, p_1, p_2, p_5\}$ | $L(z_{108}) = \{p_9, p_{11}, p_1, p_2, p_4\}$ |
| $L(z_{59}) = \{p_7, p_{13}, p_0, p_3, p_5\}$ | $L(z_{116}) = \{p_9, p_{12}, p_1, p_2, p_4\}$ |
| $L(z_{91}) = \{p_8, p_{13}, p_0, p_3, p_5\}$ | $L(z_{120}) = \{p_9, p_{13}, p_0, p_2, p_4\}$ |
| $L(z_{121}) = \{p_9, p_{13}, p_0, p_2, p_5\}$ | |

除此之外，对于不可达状态也有相应的标号。一般而言，我们有

$$L(z_i) = \{p_{x(i)}, p_{2+y(i)}, p_{4+t(i)}, p_{6+a(i)}, p_{10+b(i)}\}$$

有了 $AP = \{p_0, ..., p_{13}\}$， $S = \{z_0, ..., z_{127}\}$，在这之上定义了 $\Delta$ 、 $I$ 和 $L$，我们就有了一个 $AP$ 上的 Kripke 结构 $\langle S, \Delta, I, L\rangle$ 。

**安全性质**

系统的互斥性质表示为

$$\neg(p_8 \wedge p_{12})$$

该系统满足该安全性质，即

$$\forall s \in rh(I).L(s) \models \neg(p_8 \wedge p_{12})$$

**标号 KS 与一阶迁移系统**

$V = \{a, b, x, y, t\}$
$S = \{(a, b, x, y, t) \mid a, b \in \{0, ..., 3\}, x, y, t \in \{0, 1\}\}$

.

$\Delta$:

$((a_0, b_0, x_0, y_0, t_0), (a_1, b_1, x_1, y_1, t_1)) \in \Delta$ 当且仅当
存在 $p \to a$ 且
$a = a_0, b = b_0, x = x_0, y = y_0, t = t_0 \models p$ 且
$a = a_0, b = b_0, x = x_0, y = y_0, t = t_0, a' = a_1, b' = b_1, x' = x_1, y' = y_1, t' = t_1 \models f(a)$ 。

其中 $f(a)$ 将 $a$ 中左边的变量加 $'$，将赋值改为等式，对每个没有在 $a$ 中出现的变量 $v$ 增加等式 $v' = v$ 。

.

$I = \{(a_0, b_0, x_0, y_0, t_0) \mid a = a_0, b = b_0, x = x_0, y = y_0, t = t_0 \models a = 0 \wedge b = 0 \wedge x = 0 \wedge y = 0 \wedge y = 0\}$

.

我们有以下命题：

| | |
|---|---|
| $p_0 \equiv (x = 0)$ | $p_1 \equiv (x = 1)$ |
| $p_2 \equiv (y = 0)$ | $p_3 \equiv (y = 1)$ |
| $p_4 \equiv (t = 0)$ | $p_5 \equiv (t = 1)$ |
| $p_{6+i} \equiv (a = s_i) \quad i \in \{0, 1, 2, 3\}$ | $p_{10+i} \equiv (b = t_i) \quad i \in \{0, 1, 2, 3\}$ |

$L$ 定义如下：

$p_i \in L((a_0, b_0, x_0, y_0, t_0)) \Leftrightarrow a = a_0, b = b_0, x = x_0, y = y_0, t = t_0 \models p_i$

### 扩展标号 KS

可以表示抽象的系统。比如 $z_{120}$ 和 $z_{121}$ 可以抽象成一个状态，比如命名为 $z_{120121}$ 。

原有 $L(z_{120}) = \{p_9, p_{13}, p_0, p_2, p_4\}$

即 $\bigwedge_{i\in\{0,2,4,9,13\}} p_i \wedge \bigwedge_{i\notin\{0,2,4,9,13\}} \neg p_i$

$L(z_{121}) = \{p_9, p_{13}, p_0, p_2, p_5\}$

即 $\bigwedge_{i\in\{0,2,5,9,13\}} p_i \wedge \bigwedge_{i\notin\{0,2,5,9,13\}} \neg p_i$

现有

$L(z_{120121}) = \bigwedge_{i\in\{0,2,9,13\}} p_i \wedge \bigwedge_{i\notin\{0,2,4,5,9,13\}} \neg p_i$

## §2.5 标号迁移系统与自动机

### 标号迁移系统与 Büchi 自动机

对于互斥协议的 Kripke 结构，我们可以增加信息记载引起迁移发生的进程，获得标号迁移系统 $\langle \Sigma, S, \Delta, I, F\rangle$ 其中

- $\Sigma = \{a, b\}$ 。
- $S = \{z_0, z_1, ..., z_{127}\}$ 。
- $\Delta = \{(z_0, b, z_{12}), (z_0, a, z_{35}), (z_1, a, z_{35}), ...\}$ 。
- $I = \{z_0\}$ 。

我们进一步要求系统的可接受运行必须包含无限多的有 $b$ 进程动作到达的状态，这样的系统表示为 Büchi 自动机 $\langle \Sigma, S, \Delta, I, F\rangle$ 其中

- $\Sigma = \{a, b\}$ 。
- $S = \{z_0, z_1, ..., z_{127}\}$ 。
- $\Delta = \{(z_0, b, z_{12}), (z_0, a, z_{35}), (z_1, a, z_{35}), ...\}$ 。
- $I = \{z_0\}$ 。
- $F = \{z_{20}, z_{120}, z_{116}, z_{12}, z_{47}, z_{55}, z_{59}, z_{24}\}$

从语言上讲，这个自动机所接受的语言为 $(a^*b)^\omega$ 的一个子集。

### 扩展 Büchi 自动机

我们要求系统的可接受运行必须包含无限多的由 $a$ 进程动作到达的状态和限多的由 $b$ 进程动作到达的状态，这样的系统表示为扩展 Büchi 自动机 $\langle \Sigma, S, \Delta, I, F\rangle$ 其中

- $\Sigma = \{a, b\}$ 。
- $S = \{z_0, z_1, ..., z_{127}\}$ 。
- $\Delta = \{(z_0, b, z_{12}), (z_0, a, z_{35}), (z_1, a, z_{35}), ...\}$ 。
- $I = \{z_0\}$ 。
- $F = \{f_1, f_2\}$

其中

$$f_1 = \{z_{20}, z_{120}, z_{116}, z_{12}, z_{47}, z_{55}, z_{59}, z_{24}\}$$

$$f_2 = \{z_{67}, z_{46}, z_{78}, z_{35}, z_{108}, z_{97}, z_{121}, z_{83}\}$$

**公平 Kripke 结构**

我们要求系统的可接受运行必须包含无限多的由 $a$ 进程动作到达的状态和限多的由 $b$ 进程动作到达的状态, 这样的系统表示为公平 Kripke 结构 $\langle S, \Delta, I, F\rangle$ 其中

- $S = \{z_0, z_1, ..., z_{127}\}$ 。
- $\Delta = \{(z_0, z_{12}), (z_0, z_{35}), (z_1, z_{35}), ...\}$ 。
- $I = \{z_0\}$ 。
- $F = \{f_1, f_2\}$

其中

$$f_1 = \{z_{20}, z_{120}, z_{116}, z_{12}, z_{47}, z_{55}, z_{59}, z_{24}\}$$

$$f_2 = \{z_{67}, z_{46}, z_{78}, z_{35}, z_{108}, z_{97}, z_{121}, z_{83}\}$$

**基于迁移的扩展 Büchi 自动机**

互斥算法的基于迁移的扩展 Büchi 自动机可以表示为 $\langle \Sigma, S, \Delta, I, F\rangle$ 其中

- $\Sigma = \{a, b\}$ 。
- $S = \{z_0, z_1, ..., z_{127}\}$ 。
- $\Delta = \{(z_0, b, z_{12}), (z_0, a, z_{35}), (z_1, a, z_{35}), ...\}$ 。
- $I = \{z_0\}$ 。
- $F = \{f_1, f_2\}$

其中

$$f_1 = \{(z, a, z') \mid (z, a, z') \in \Delta\}$$

$$f_2 = \{(z, b, z') \mid (z, b, z') \in \Delta\}$$

## §2.6 交错迁移系统

从 $A$ 的角度描述互斥算法。

设 $\mathcal{B}$ 为 $B$ 进程的可达状态集合。

一个描述互斥算法部分信息的标号交错迁移系统为 $\langle \Sigma, S, \Delta', I\rangle$ ，其中

- $\Sigma = \{a, b\}$ 。
- $S = \{z_0, z_1, ..., z_{127}\}$ 。
- $\Delta' = \{(z_i, a, \{z_j\}), (z_i, a, B) \mid (z_i, a, z_j) \in \Delta\}$ 。
- $I = \{z_0\}$ 。

## §2.7 时间迁移系统

假定我们要求一个进程每次持有资源时间不超过 5 秒。我们用时间迁移系统 $\langle \Sigma, S, C, \Delta, I \rangle$ 表示我们的要求，其中：

- $\Sigma = \{a, b\}$ 。
- $S = \{z_0, z_1, ..., z_{127}\}$ 。
- $C = \{x, y\}$ 。
- $\Delta' =$

$$\begin{aligned}
&\{(z_i, a, \{\}, true, z_j) \mid (z_i, a, z_j) \in \Delta, a(i) \neq 2, a(j) \neq 2\} \cup \\
&\{(z_i, a, \{x\}, true, z_j) \mid (z_i, a, z_j) \in \Delta, a(j) = 2\} \cup \\
&\{(z_i, a, \{\}, x \leq 5, z_j) \mid (z_i, a, z_j) \in \Delta, a(i) = 2\} \cup \\
&\{(z_i, b, \{\}, true, z_j) \mid (z_i, b, z_j) \in \Delta, b(i) \neq 2, b(j) \neq 2\} \cup \\
&\{(z_i, b, \{y\}, true, z_j) \mid (z_i, b, z_j) \in \Delta, b(j) = 2\} \cup \\
&\{(z_i, b, \{\}, y \leq 5, z_j) \mid (z_i, b, z_j) \in \Delta, b(i) = 2\}
\end{aligned}$$

- $I = \{z_0\}$ 。

## §2.8 Petri 网

四元组

$$\langle P, T, F, M_0 \rangle$$

其中

- $P = \{s_0, s_1, s_2, s_3, t_0, t_1, t_2, t_3, ts\}$
- $T = \{u_0, u_1, u_2, u_3, v_0, v_1, v_2, v_3\}$
- $F =$

$$\begin{aligned}
&\{(s_0, u_0), (s_1, u_1), (s_2, u_2), (s_3, u_3), (ts, u_1)\} \cup \\
&\{(t_0, v_0), (t_1, v_1), (t_2, v_2), (t_3, v_3), (ts, v_1)\} \cup \\
&\{(u_0, s_1), (u_1, s_2), (u_2, s_3), (u_2, ts), (u_3, s_1)\} \cup \\
&\{(v_0, t_1), (v_1, t_2), (u_2, t_3), (u_2, ts), (v_3, t_1)\}
\end{aligned}$$

- $M_0(s) = 1$ 若 $s \in \{s_0, t_0, ts\}$ ，否则 $M_0(s) = 0$ 。

## §2.9 通信系统

通信单元 $P$ 是一个四元组

$$\langle Q, M, \Delta, q_0 \rangle$$

其中
$Q_1 = \{s_0, ..., s_3\}$ 为状态集合，
$M = \{ts\}$ 且 $ts \in \langle \{1\}, 1 \rangle$ ，
$\Delta = \{(s_0, \epsilon, s_1\}, (s_1, ts!1, s_2), (s_2, ts?1, s_3), (s_3, \epsilon, s_1)\}$ 。$q_0 = s_0$ 。

通信单元 $P'$ 是一个四元组

$$\langle Q', M', \Delta', q_0' \rangle$$

其中
$Q' = \{t_0, ..., t_3\}$ 为状态集合，
$M' = \{ts\}$ 且 $ts \in \langle \{1\}, 1 \rangle$ ，
$\Delta' = \{(t_0, \epsilon, t_1\}, (t_1, ts!1, t_2), (t_2, ts?1, t_3), (t_3, \epsilon, t_1)\}$ 。 $q_0' = t_0$ 。

那么该通信系统为 $P||P'$ 。