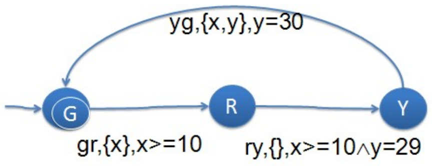
第六次课：

(1)

习题第一部分参考以下写法及图示表示。

$A=<\Sigma,S,X,\Delta,I,F>$ 其中

- $\Sigma = \{ gr, ry, yg \}$ 代表从绿变红、红变黄、黄变绿
- $S = \{ G, R, Y \}$ 代表状态绿、红、黄
- $X = \{ x, y \}$ (这一部分的描述其实用一个时钟变量就够了)
- $\Delta = \{ (G,gr,\{x\},x>=10,R), (R,ry,\{\},x>=10 \wedge y=29,Y), (Y,yg,\{x,y\},y=30,G) \}$
- $I = \{ G \}$ (定义一个初始状态)
- $F = \{ G \}$ (定义一个接受状态)



其中 G 代表绿，gr 代表由绿变红的动作，其余类推。这里的 G 同时为自动机的接受状态。

习题第二部分（略）

(2)

参考以下写法及图示解释。

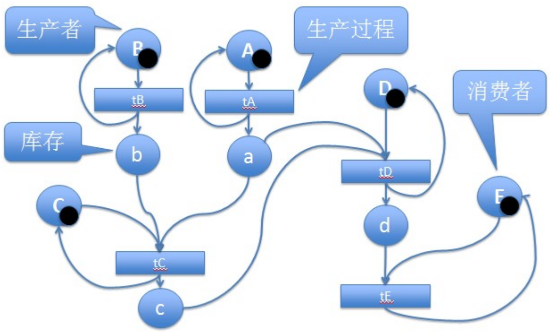
$PN=<P,T,F,M_0>$ 其中

$P=\{A,B,C,D,E,a,b,c,d\}$

$T=\{tA,tB,tC,tD,tE\}$

$F=\{(tB,b),(tB,B),(tA,a),(tA,A),(tC,c), (tC,C),(tD,d),(tD,D),(tE,E),$
$(A,tA),(B,tB),(C,tC),(D,tD),(E,tE),(a,tB),(b,tB),(a,tD),(c,tD),(d,tE)\}$

$M_0=(1,1,1,1,1,0,0,0,0)$ 即 $M_0(A)=1, M_0(B)=1, \ldots, M_0(E)=1, M_0(a)=0, \ldots, M_0(d)=0$



第七次课：

7.1

a.1)

证明 $G(p\to Xp)\to(p\to Gp)$，

即证明对所有<S, ζ,L> ,我们有 $\zeta \models G(p\to Xp)\to(p\to Gp)$

假定(1) $\zeta \models G(p\to Xp)$ 且 (2) $\zeta \models p$

需要证明 $\zeta \models Gp$，即对所有 $k\geq 0, \zeta^k \models p$

由(1) 可得对所有 $k\geq 0, \zeta^k \models p$ 则 $\zeta^{k+1} \models p$

由(2) 可得 $\zeta^0 \models p$，由归纳法可得对所有 $k\geq 0, \zeta^k \models p$，因而命题得证。

a.2)

证明$(p\to Gp) \to G(p\to Xp)$不成立，只需举一个反例。

需要证明存在<S, ζ,L> ,我们有 $\zeta \not\models (p\to Gp) \to G(p\to Xp)$

即 $\zeta \models (p\to Gp)$成立且 $\zeta \models G(p\to Xp)$不成立

选取<S, ζ,L>使得 $L(\zeta_0)=\{\}, L(\zeta_1)=\{p\}, L(\zeta_2)=\{\}$,

则有 $\zeta \models (p\to Gp)$成立且 $\zeta \models G(p\to Xp)$不成立,

因此$(p\to Gp) \to G(p\to Xp)$不成立.

b)

应用推理系统证明 $X(p\vee q) \leftrightarrow (Xp\vee Xq)$，每一步需要有根据。

先证明 $X(p\vee q) \to (Xp\vee Xq)$

- 1。$X(p\vee q)$ AS
- 2。$p\vee q\to\neg p\to q$ AX
- 3。$G(p\vee q\to\neg p\to q)$ 2+G
- 4。$X(p\vee q\to\neg p\to q)$ 3+A4+MP
- 5。$X(p\vee q)\to X(\neg p\to q)$ 4+A8+MP
- 6。$X(\neg p\to q)$ 1+5+MP
- 7。$X\neg p\to Xq$ 6+A8+MP
- 8。$X\neg p\leftrightarrow \neg Xp$ A7
- 9。$(X\neg p\leftrightarrow \neg Xp)\to(X\neg p\to Xq)\to (Xp\vee Xq)$ AX
- 10。$Xp\vee Xq$ 9+8+7+MP

所以我们有 $X(p\vee q) \to (Xp\vee Xq)$。

类似地，可以证明$(Xp\vee Xq)\to X(p\vee q)$ 。

7.2

用命题 yellow,red,green 分别表示交通灯的黄红绿色。

所述规范为以下公式的合取。

green

$G(\neg(yellow\wedge green)) \wedge G(\neg(green\wedge red)) \wedge G(\neg(red\wedge yellow))$

$G(green\to(green\ U\ yellow)) \wedge G(yellow \to X\ red) \wedge G(red \to (red\ U\ green))$

这三个组成部分分别表示初始状态、不同灯的两两互斥、灯的变化规律。

第八次课：

8.1

a) $M \models ((a=NCR \vee a=wait)\ U\ a=CR)$

考虑问题的思路:

首先从图上查找一条能够说明 $M \models ((a=NCR \vee a=wait)\ U\ a=CR)$不成立的路径。

如：

(NCR,NCR,0,0,0)

(NCR,wait,1,0,0)

(NCR,NCR,1,0,0)

(NCR,NCR,0,0,0) -- （重复第一个状态）

因此有一条无穷路径不满足$(a=NCR \vee a=wait)\ U\ a=CR)$。

然后应用限界语义证明如下:

$M \models ((a=NCR \vee a=wait)\ U\ a=CR)$不成立，当且仅当

$M \models^E \neg((a=NCR \vee a=wait)\ U\ a=CR)$成立，当且仅当

存在 k 和以初始状态为起点 k 路径 π 使得 $M, \pi \models_k \neg((a=NCR \vee a=wait)\ U\ a=CR)$，即

$M, \pi \models_k (\neg(a=NCR \vee a=wait)\ R\ a\neq CR)$，即

$M, \pi \models_k G(a\neq CR) \vee (a\neq CR\ U\ (a\neq CR \wedge \neg(a=NCR \vee a=wait)))$

1. k=0.
   检查所有以初始状态为起点的 0-路径
   (NCR,NCR,0,0,0),….
   不存在以初始状态为起点的 0 路径 π 使得
   $M, \pi \models_k G(a\neq CR) \vee (a\neq CR\ U\ (a\neq CR \wedge \neg(a=NCR \vee a=wait)))$
2. k=1.
   检查所有以初始状态为起点的 1-路径
   (NCR,NCR,0,0,0)(wait,NCR,0,1,1),….
   不存在以初始状态为起点的 1-路径 π 使得
   $M, \pi \models_k G(a\neq CR) \vee (a\neq CR\ U\ (a\neq CR \wedge \neg(a=NCR \vee a=wait)))$
3. k=2.
   检查所有以初始状态为起点的 2-路径
   (NCR,NCR,0,0,0)(wait,NCR,0,1,1) (wait, wait,1,1,0),….
   找到了如下一条能说明问题的。
   设 π=(NCR,NCR,0,0,0)(NCR,wait,1,0,0)(NCR,CR,1,0,0)。
   则根据限界语义我们有 $M, \pi \models_k G(a\neq CR) \vee (a\neq CR\ U\ (a\neq CR \wedge \neg(a=NCR \vee a=wait)))$
   因而证明了 $M \models ((a=NCR \vee a=wait)\ U\ a=CR)$不成立

b) $M \models ((a=NCR \vee a=wait)\ U\ (a=CR \vee b=CR))$

从图上看这个是成立的。因而没法找到反例。作为限界语义的应用，可以说明如下：

设 ϕ = (a=NCR $\vee$a=wait) U (a=CR $\vee$ b=CR)。

M |= ϕ
当且仅当
对所有 k 和以初始状态为起点 k 路径π都没有 M, π $|=_k$ $\neg$ ((a=NCR $\vee$a=wait) U (a=CR $\vee$ b=CR))
当且仅当
对所有k<=|M|x2$^{|\phi|}$和以初始状态为起点k路径π都没有M, π $|=_k$ $\neg$ ((a=NCR $\vee$a=wait) U (a=CR $\vee$ b=CR))。

应用限界语义和对 k 路径的枚举可证明
对所有 k=0，1，2，。。。， |M|x2$^{|\phi|}$和
以初始状态为起点 k 路径π都没有 M, π $|=_k$ $\neg$ ((a=NCR $\vee$a=wait) U (a=CR $\vee$ b=CR))。
因而 M |= ((a=NCR $\vee$a=wait) U (a=CR $\vee$ b=CR))。

8.2

习题第一部分：公式 (p ∨ (q U r))等价的 GBA。（略）

习题第二部分：公式 Xp∧(q R r)等价的 GBA 构造如下。

用 FIN 标识最后要保留的节点。

1	e	Xp ∧ (qRr)		
1	e	Xp , (qRr)	Xp ∧ (qRr)	
1	e	(qRr)	Xp ∧ (qRr), Xp	p
11	e	q,r	Xp ∧ (qRr), Xp, (qRr)	p
12	e	r	Xp ∧ (qRr), Xp, (qRr)	p, (qRr)
11	e	FIN	Xp ∧ (qRr), Xp, (qRr),q,r	p
12	e	FIN	Xp ∧ (qRr), Xp, (qRr),r	p, (qRr)

2	11	p		
3	12	p, (qRr)		
2	11	FIN	p	
3	12	(qRr)	p	
31	12	q,r	p,(qRr)	
32	12	r	P,(qRr)	(qRr)
31	12	FIN	P,(qRr),q,r	
32	12	FIN	P,(qRr),r	(qRr)

4	2	FIN		
5=4	31			
6	32	(qRr)		

61	32	q,r	(qRr)	
62	32	r	(qRr)	(qRr)
61	32	FIN	(qRr),q,r	
62	32	FIN	(qRr),r	(qRr)

7=4	4			
8=4	61			
9=6	62	(qRr)		

最后保留的节点

11	e	FIN	Xp ∧ (qRr), Xp, (qRr),q,r	p
12	e	FIN	Xp ∧ (qRr), Xp, (qRr),r	p, (qRr)
2	11	FIN	p	
31	12	FIN	p,(qRr),q,r	
32	12	FIN	p,(qRr),r	(qRr)
4	2,31,4,61	FIN		
61	32,62	FIN	(qRr),q,r	
62	32,62	FIN	(qRr),r	(qRr)

构造的 GBA 为 A=<Σ,S,Δ,I,F>如下图。其中

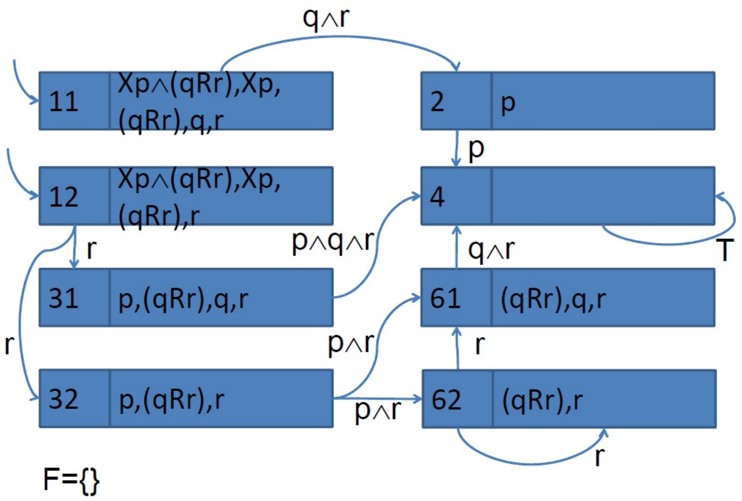
- $\Sigma = 2^{\{p,q,r\}}$
- S = { 11,12,31,32,2,4,61,62 }
- Δ = {

  (11,{q,r},2), (11,{p,q,r},2),

  (12,{r},31), (12,{p,r},31), (12,{q,r},31), (12,{p,q,r},31),

  ……

  }
- I = { 11,12 }
- F={ }



根据构造，我们有<S,ζ,L> |= Xp∧(q R r) iff L(ζ)∈ *L*(A)

第九次课：

9 .1

a) 对照 A(q0 U q2)与¬ A(q0 U q2)，即 E(¬q0 R ¬q2)，看是否前一个在模型中满足或后一个在模型中的某个初始状态满足。

1) k=0
   M,s0 $|=_0$ A(q0 U q2) 不满足，M,s0 $|=_0$ E(¬q0 R ¬q2) 不满足
2) k=1
   M,s0 $|=_1$ A(q0 U q2) 不满足，M,s0 $|=_1$ E(¬q0 R ¬q2) 不满足
3) k=2
   M,s0 $|=_2$ A(q0 U q2) 不满足，
   M,s0 $|=_2$ E(¬q0 R ¬q2) 满足（因为有 M,s0s2s4 $|=_2$ ¬q0 R ¬q2）
   因而 M,s0 |= E¬q0 R ¬q2，因而 M,s0 不满足 A(q0 U q2)，因而 M 不满足 A(q0 U q2)。
   且根据前面计算知 k=2 是最小可确定 A(q0 U q2)是否满足的限界模型。

b）和上题类似，EG(q0 ∨ q2)与 AF(¬q0 ∧ ¬q2)对照着看。

对于不同的 k 考虑如下路径。
k=0: s0
k=1: s0s1,s0s2
k=2: s0s1s3,s0s1s5,s0s2s5,s0s2s4
k=3: s0s1s3s4,s0s1s3s5,s0s1s5s0,...;
...

由于 $M, s0s1s5s0 |=_3 G(q_0 \vee q_2)$

因此，M_3满足$EG(q_0 \vee q_2)$，因此M满足$EG(q_0 \vee q_2)$

由于M_0时不满足$EG(q_0 \vee q_2)$，M_1时不满足$EG(q_0 \vee q_2)$，M_2时不满足$EG(q_0 \vee q_2)$，

故 k=3 是最小可确定$EG(q_0 \vee q_2)$是否满足的界。

9.2

a）
根据基于不动点的算法[[A(q0 U q2)]] = μZ.([[q2]] ∪ ([[q0]] ∩ [[AX(Z)]]))。
为方便起见，可将公式直接解释为满足公式的状态集合，布尔运算符号解释为集合运算，直接写为 A(q0 U q2) = μZ.(q2 ∨ (q0 ∧ AX(Z)))。
依照计算最小不动点的方法进行计算。

A(q0Uq2) = μZ.(q2∨(q0∧AX Z))

- S0=false={} 空集

- $S1=q2 = \{s5\}$
- $S2=\{s5\}\cup(\{s0,\ldots,s3\}\cap\{s4\}) = \{s5\}$

即 $f(Z) = [[q2]] \cup ([[q0]] \cap [[AX(Z)]])$的最小不动点为$\{s5\}$
即只有 s5 满足 A(q0 U q2)。

由于模型的初始状态 s0 不满足 A(q0 U q2)，该模型不满足 A(q0Uq2)

b）

类似地 $EG(q0\vee q2) = \nu Z.((q0\vee q2) \wedge EX\ Z)$，计算最大不动点如下：

- $S0=true=\{s0,\ldots,s5\}$ 全集
- $S1=q0\vee q2 = \{s0,s1,s2,s3,s5\}$
- $S2=\{s0,s1,s2,s3,s5\}\cap\{s0,s1,s2,s3,s4,s5\} =\{s0,s1,s2,s3,s5\}$

由于模型的初始状态 s0 满足 $EG(q0\vee q2)$，因而该模型满足 $EG(q0\vee q2)$。

第十次课：

1．计算最弱宽松前断言 wlp(T,a=s4)即[T](a=s4) 并证明 $(a=s3)\rightarrow X(a=s4)$。

$$
\begin{aligned}
&[T](a=s4)\\
&= (a=s3 \rightarrow s4=s4) \wedge\\
&\quad (a=s1\wedge\neg(x<n) \rightarrow s3=s4) \wedge\\
&\quad (a=s2 \rightarrow s1=s4) \wedge\\
&\quad (a=s1\wedge(x<n) \rightarrow s2=s4) \wedge\\
&\quad (a=s0 \rightarrow s1=s4)\\
&= \neg(a=s1\wedge\neg(x<n)) \wedge \neg(a=s2) \wedge \neg(a=s1\wedge(x<n)) \wedge \neg(a=s0\ )\\
&= \neg(a=s1) \wedge \neg(a=s2) \wedge \neg(a=s0\ )
\end{aligned}
$$

$$
\begin{aligned}
&(a=s3)\rightarrow X(a=s4)\\
&\text{IFF } (a=s3)\rightarrow[T+](a=s4)\\
&\text{IFF } (a=s3)\rightarrow[T](a=s4) \text{ and } (a=s3)\rightarrow(E(T)\vee a=s4)\\
&\text{IFF } (a=s3)\rightarrow[T](a=s4)\\
&\text{IFF } (a=s3)\rightarrow \neg(a=s1) \wedge \neg(a=s2) \wedge \neg(a=s0\ )\\
&\text{IFF true}
\end{aligned}
$$

2(a)
我们有 $(T,\Theta) \models_I a=s0$。只需证明：$(T,\Theta) \models_I (a=s0 \wedge n>=0) \quad => \quad G(a=s4 \rightarrow y=n*n*n-n)$

使用推理规则

$$
\begin{aligned}
&\phi \Rightarrow \varphi'\\
&\varphi' \Rightarrow [T]\ \varphi'
\end{aligned}
$$

$$\varphi' \Rightarrow \varphi$$

$$\phi \Rightarrow G\varphi$$

设

ϕ= (a=s0 ∧n>=0)

φ= (a=s4 → y=n*n*n-n)

φ'= (a=s0 ∧ n>=0) ∨ (a=s1 ∧y=(x*x*x-x)/3 ∧ x<=n) ∨ (a=s2 ∧y=(x*x*x-x)/3 ∧ x<n) ∨ (a=s3 ∧3y=n*n*n-n) ∨ (a=s4 ∧ y=n*n*n-n)

通过计算和推理，我们有

$$\phi \Rightarrow \varphi'$$
$$\varphi' \Rightarrow [T]\, \varphi'$$
$$\varphi' \Rightarrow \varphi$$

根据推理规则，我们有(a=s0 ∧n>=0) => G(a=s4 → y=n*n*n-n)

因而(T,Θ) $|=_I$ n>=0→ G(a=s4 → y=n*n*n-n)

2(b).

我们有 (T,Θ) $|=_I$ a=s0。只需证明：(T,Θ) $|=_I$ (a=s0 ∧n>=0) => F(a=s4)

使用推理规则

$$\phi \Rightarrow (\psi \vee \varphi)$$
$$\varphi \Rightarrow (w(t/x) \wedge (E(T) \vee \psi)$$
$$(\varphi \wedge t=v) \Rightarrow [T](\psi \vee (\varphi \wedge t<v))$$

$$\phi \Rightarrow F\psi$$

设 f(a,n,x) 为具有以下性质的函数（项）。

I(f(s0,n,x)) (σ) = I(2n+3)(σ)

I(f(s1,n,x)) (σ) = I(2(n-x)+2)(σ)

I(f(s2,n,x)) (σ) = I(2(n-x)+1)(σ)

I(f(s3,n,x)) (σ) = 0

I(f(s4,n,x)) (σ) = 0

设

w= (w>=0)

W= NAT

t= f(a,n,x)

ϕ= (a=s0 ∧n>=0)

ψ= (a=s4)

φ= (a=s0 ∧ n>=0) ∨ (a=s1 ∧ 0<=x<=n) ∨ (a=s2 ∧0<= x<n) ∨ (a=s3∧0<=x=n)

假定 φ ⇒ ((E(T) ∨ψ) 已根据证明安全性质的方法证明。

通过计算和推理，我们有

$$\phi \Rightarrow (\psi \vee \varphi)$$
$$\varphi \Rightarrow w(t/x)$$
$$(\varphi \wedge t=v) \Rightarrow [T](\psi \vee (\varphi \wedge t<v))$$

其中第三个条件的验证如下。

$(\varphi \wedge t=v)$ 为$(a=s0 \wedge n>=0) \vee (a=s1 \wedge 0<=x<=n) \vee (a=s2 \wedge 0<= x<n) \vee (a=s3 \wedge 0<=x=n) \wedge f(a,n,x)=v$

五条迁移分别验证如下

$(\varphi \wedge t=v) \rightarrow [t1]\ (\psi \vee (\varphi \wedge t<v))$ iff $(\varphi) \rightarrow (a=s0 \rightarrow (0<=n) \wedge f(s1,n,0)< f(s0,n,x))$ iff true

$(\varphi \wedge t=v) \rightarrow [t2]\ (\psi \vee (\varphi \wedge t<v))$ iff $(\varphi) \rightarrow ((a=s1 \wedge x<n) \rightarrow (0<=x<n) \wedge f(s2,n,x)< f(s1,n,x))$ iff true

$(\varphi \wedge t=v) \rightarrow [t3]\ (\psi \vee (\varphi \wedge t<v))$ iff $(\varphi) \rightarrow ((a=s2) \rightarrow (0<=x<n) \wedge f(s1,n,x+1)< f(s2,n,x))$ iff true

$(\varphi \wedge t=v) \rightarrow [t4]\ (\psi \vee (\varphi \wedge t<v))$ iff $(\varphi) \rightarrow ((a=s1 \wedge \neg\, x<n) \rightarrow (0<=x=n) \wedge f(s3,n,x)< f(s1,n,x))$ iff true

$(\varphi \wedge t=v) \rightarrow [t5]\ (\psi \vee (\varphi \wedge t<v))$ iff $(\varphi \wedge t=v) \rightarrow ((a=s3) \rightarrow (s4=s4 \vee (f(s4,n,x)< f(s3,n,x)))$ iff true

根据推理规则，我们有$(a=s0 \wedge n>=0)$ => $F(a=s4)$

因而$(T,\Theta) \models_I n>=0 \rightarrow F(a=s4)$

<u>第十一次课：</u>

1.计算最弱宽松前断言[l1,l3,end](y=n*n*n-n),

并证明 $\{(x<=n) \wedge 3y=x*x*x-x\}(l1,l3,end)\{(y=n*n*n-n)\}$

[l1,l3,end](y=n*n*n-n)

=[l1,l3] (3y=n*n*n-n)

$=\neg(x<n) \rightarrow (3y=n*n*n-n)$

$\{x<=n \wedge 3y=x*x*x-x\}(l1,l3,end)\{(y=n*n*n-n)\}$

IFF $(x<=n \wedge 3y=x*x*x-x) \rightarrow$ [l1,l3] (3y=n*n*n-n)

IFF $(x<=n \wedge 3y=x*x*x-x) \rightarrow (\neg(x<n) \rightarrow (3y=n*n*n-n))$

IFF true

2(a).

选择 C={beg,l1,end}

选择 q_beg = (n>=0)

q_l1 = $(0<=x<=n) \wedge (3y=x*x*x-x)$

q_end = (y=n*n*n-n)

枚举相关路径如下：

(beg,l1), (l1,l2,l1), (l1,l3,end)

证明路径正确性如下：

$\{0 <=n \}(beg,l1)\{(0<=x<=n)\wedge(3y=x*x*x-x)\}$
IFF $(0 <=n)[beg,l1]((0<=x<=n)\wedge(3y=x*x*x-x))$
IFF $(0<=n\rightarrow 0<=n\wedge 0=0)$
IFF true

$\{0<=x<=n \wedge 3y=x*x*x-x \}(l1,l2,l1) \{0<=x<=n \wedge 3y=x*x*x-x \}$
IFF $(0<=x<=n \wedge 3y=x*x*x-x)\rightarrow[l1,l2,l1)](0<=x<=n \wedge 3y=x*x*x-x)$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow [l1,l2] (0<=x+1<=n \wedge 3(y+x*(x+1)=(x+1)*(x+1)*(x+1)-x-1)$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow (x<n\rightarrow (0<=x+1<=n \wedge 3(y+x*(x+1)=(x+1)*(x+1)*(x+1)-x-1))$
IFF true

$\{0<=x<=n \wedge 3y=x*x*x-x \}(l1,l3,end)\{(y=n*n*n-n)\}$
IFF $(0<=x<=n \wedge 3y=x*x*x-x)[l1,l3,end](y=n*n*n-n)$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow [l1,l3] (3y=n*n*n-n)$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow(\neg(x<n)\rightarrow(3y=n*n*n-n))$
IFF true

2(b)

选择 C={beg,l1}
选择 q_beg = (n>=0)
q_l1 = $(0<=x<=n)\wedge(3y=x*x*x-x)$

枚举相关路径如下：
(beg,l1),
(l1,l2,l1)

证明路径正确性如下：

$\{0 <=n \}(beg,l1)\{(0<=x<=n)\wedge(3y=x*x*x-x)\}$
IFF $(0 <=n)[beg,l1]((0<=x<=n)\wedge(3y=x*x*x-x))$
IFF $(0<=n\rightarrow 0<=n\wedge 0=0)$
IFF true

$\{0<=x<=n \wedge 3y=x*x*x-x \}(l1,l2,l1) \{0<=x<=n \wedge 3y=x*x*x-x \}$
IFF $(0<=x<=n \wedge 3y=x*x*x-x)\rightarrow[l1,l2,l1)](0<=x<=n \wedge 3y=x*x*x-x)$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow [l1,l2] (0<=x+1<=n \wedge 3(y+x*(x+1)=(x+1)*(x+1)*(x+1)-x-1)$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow (x<n\rightarrow (0<=x+1<=n \wedge 3(y+x*(x+1)=(x+1)*(x+1)*(x+1)-x-1))$
IFF true

选择 C’={l1}
选择 W=NAT, w=(x>=0).

我们有 W={σ(x) | I(w)(σ)=true }

选择 t_l1 = (n-x)

我们有 q_l1 → (n-x)>=0.

枚举相关路径如下：(l1,l2,l1)

证明路径正确性如下：

vc(0<=x<=n∧(n-x=v), (l1,l2,l1),(n-x<v))
IFF (0<=x<=n∧(n-x=v))→ (x<n→ (n-x-1<v)
IFF true.

<u>第十二次课：</u>

1.
记以下程序片段为 T:
if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j;
a.计算最弱宽松前断言[T] (x=i*a+j*b)，
b.并证明{ y=k*a+l*b ∧(x=i*a+j*b) } T { x=i*a+j*b}。

a.
我们有
[T] (x=i*a+j*b)=
((x>y)→ (x-y=(i-k)*a+(j-l)*b)) ∧ (¬(x>y)→ (x=i*a+j*b))

b.
我们有
y=k*a+l*b ∧(x=i*a+j*b)→ ((x>y)→ (x-y=(i-k)*a+(j-l)*b)) ∧ (¬(x>y)→ (x=i*a+j*b))
因而{ y=k*a+l*b ∧(x=i*a+j*b) } T { x=i*a+j*b}。

2(a)

设φ为 gcd(x,y)=gcd(a,b) ∧(y=k*a+l*b) ∧(x=i*a+j*b)

我们有
{φ∧ ¬(x=y)}   if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j { φ }
且
φ∧ (x=y)→ x=gcd(a,b) ∧ (x=i*a+j*b)

根据推理规则，我们有
{φ}
while (¬(x=y)) do   if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j od

$\{\ x=gcd(a,b) \wedge (x=i*a+j*b)\ \}$

我们有

$\{x=a \wedge y=b \wedge a>=0 \wedge b>=0\}$ i:=1; j:=0; k:=0; l:=1 $\{\varphi\}$

根据推理规则，我们有

$\{x=a \wedge y=b \wedge a>=0 \wedge b>=0\}$

i:=1; j:=0; k:=0; l:=1;

while (¬(x=y)) do if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j od

$\{\ x=gcd(a,b) \wedge (x=i*a+j*b)\ \}$

因此我们有 $\{x=a \wedge y=b \wedge a>=0 \wedge b>=0\} T \{\ x=gcd(a,b) \wedge (x=i*a+j*b)\ \}$

2(b)

设 W=NAT, w=(x>=0). 我们有 W={σ(x) | I(w)(σ)=true }

设 t= (x+y)

设φ为 $gcd(x,y)=gcd(a,b) \wedge (y=k*a+l*b) \wedge (x=i*a+j*b) \wedge x>0 \wedge y>0$

我们有

$\varphi \wedge \neg(x=y) \rightarrow t>=0$

且

$[\varphi \wedge \neg(x=y) \wedge t=v]$ if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j $[\ \varphi \wedge t<v]$

且

$\varphi \wedge (x=y) \rightarrow x=gcd(a,b) \wedge (x=i*a+j*b)$

根据推理规则，我们有

$[\varphi]$

while (¬(x=y)) do if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j od

$[\ x=gcd(a,b) \wedge (x=i*a+j*b)\ ]$

我们有

$[x=a \wedge y=b \wedge a>0 \wedge b>0]$ i:=1; j:=0; k:=0; l:=1 $[\varphi]$

根据推理规则，我们有

$[x=a \wedge y=b \wedge a>0 \wedge b>0]$

i:=1; j:=0; k:=0; l:=1;

while (¬(x=y)) do if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j od

$[x=gcd(a,b) \wedge (x=i*a+j*b)\ ]$

因此我们有 $[x=a \wedge y=b \wedge a>0 \wedge b>0] T [\ x=gcd(a,b) \wedge (x=i*a+j*b)\ ]$

第十三次课：

1.

定义 $V=\{v1,v2\}$。定义 f 如下。

$f(s\_0) = \neg v1\wedge \neg v2$；$f(s\_1) = \neg v1\wedge v2$；$f(s\_2) = v1\wedge \neg v2$；$f(s\_3) = v1\wedge v2$。

模型中的 6 条迁移记为 t1,t2,t3,t4,t5,t6。这些在符号模型中的表示分别为

$f(s0)\wedge(f(s1))' = \neg v1\wedge \neg v2\wedge\neg v1'\wedge v2'$

$f(s0)\wedge(f(s2))' = \neg v1\wedge \neg v2\wedge v1'\wedge\neg v2'$

$f(s1)\wedge(f(s3))' = \neg v1\wedge v2\wedge v1'\wedge v2'$

$f(s2)\wedge(f(s0))' = v1\wedge \neg v2\wedge\neg v1\wedge \neg v2'$

$f(s2)\wedge(f(s3))' = v1\wedge \neg v2\wedge v1'\wedge v2'$

$f(s3)\wedge(f(s1))' = v1\wedge v2\wedge\neg v1'\wedge v2'$

定义ρ为以上公式的析取。化简后得：$\rho =$

$(\neg v1\wedge\neg v2\wedge(v1'\leftrightarrow \neg v2'))\vee(\neg v1\wedge v2\wedge(v1'\wedge v2'))\vee$

$(v1\wedge\neg v2\wedge(v1'\leftrightarrow v2'))\vee(v1\wedge v2\wedge(\neg v1'\wedge v2'))$。

模型的初始状态集为相关状态公式的析取，即 $f(s0)\vee f(s2)$。化简后得：$\Theta = \neg v1$。

定义 N 如下：

N(p)为满足 p 的状态公式的析取，化简后得：$N(p) = v1$。

N(q)为满足 q 的状态公式的析取，化简后得：$N(q) = v2$。

(V,ρ,Θ,N)为标号 Kripke 模型的基于 f 的符号模型。

（2）

$[[EG(p\vee q)]] = \nu Z.([[p\vee q]]\wedge ex(Z))$。设 $g(Z) = [[p\vee q]]\wedge ex(Z)$。

g(TRUE)

$= ([[p\vee q]]\wedge ex(TRUE))$

$= (v1\vee v2)\wedge\exists v1',\ldots,vn'.(\rho\wedge TRUE) = (v1\vee v2)$

g(g(TRUE))

$= ([[p\vee q]]\wedge ex(v1\vee v2))$

$= (v1\vee v2)\wedge\exists v1',\ldots,vn'.(\rho\wedge(v1\vee v2)) = (v1\vee v2)$

因此 $[[EG(p\vee q)]] = (v1\vee v2)$

模型满足 $EG(p\vee q)$当且仅当 $\Theta\rightarrow[[EG(p\vee q)]]$当且仅当 $\neg v1\rightarrow(v1\vee v2)$。

由于 $\neg v1\rightarrow(v1\vee v2)$不成立，模型不满足 $EG(p\vee q)$。