Propositional Hoare Logicの拡張について

東京工業大学　情報理工学研究科　数理・計算科学専攻
鹿島研究室M1　　中村　誠希

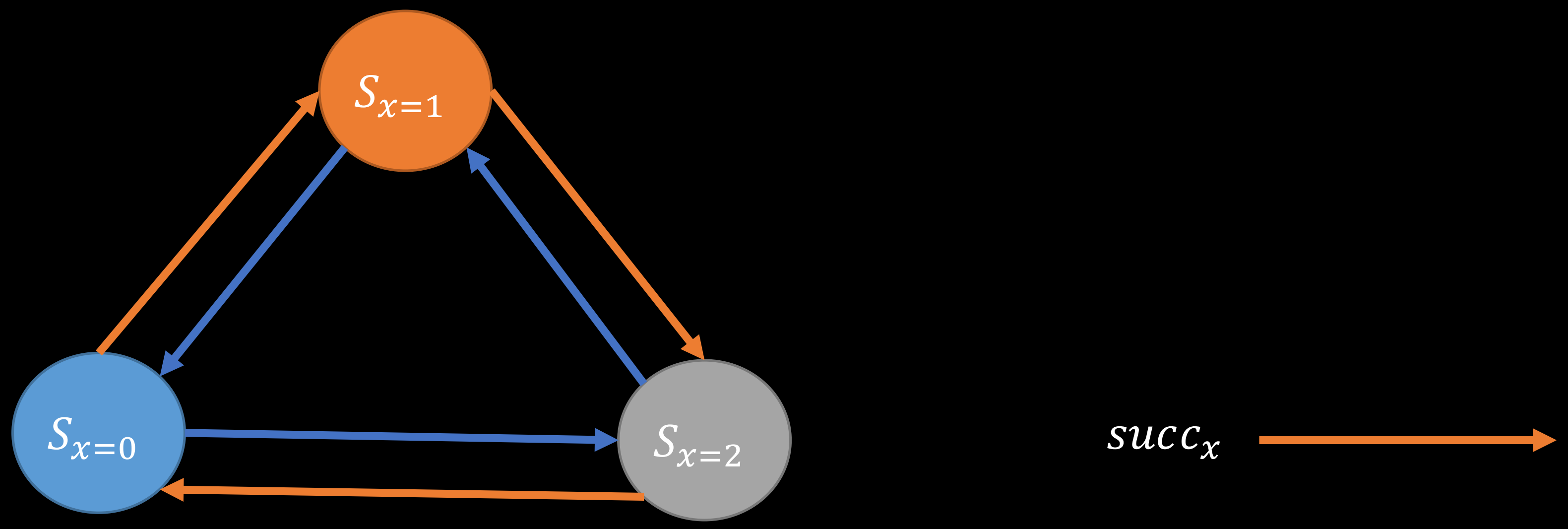
発表内容

- t^* unfolding : IPDLのモデルをdagモデルへ変換
- IPHLの有限モデル性

	PHL	PDL	IPHL	IPDL
ツリーモデル性	○	○	×	×
有限モデル性	○	○	○	×

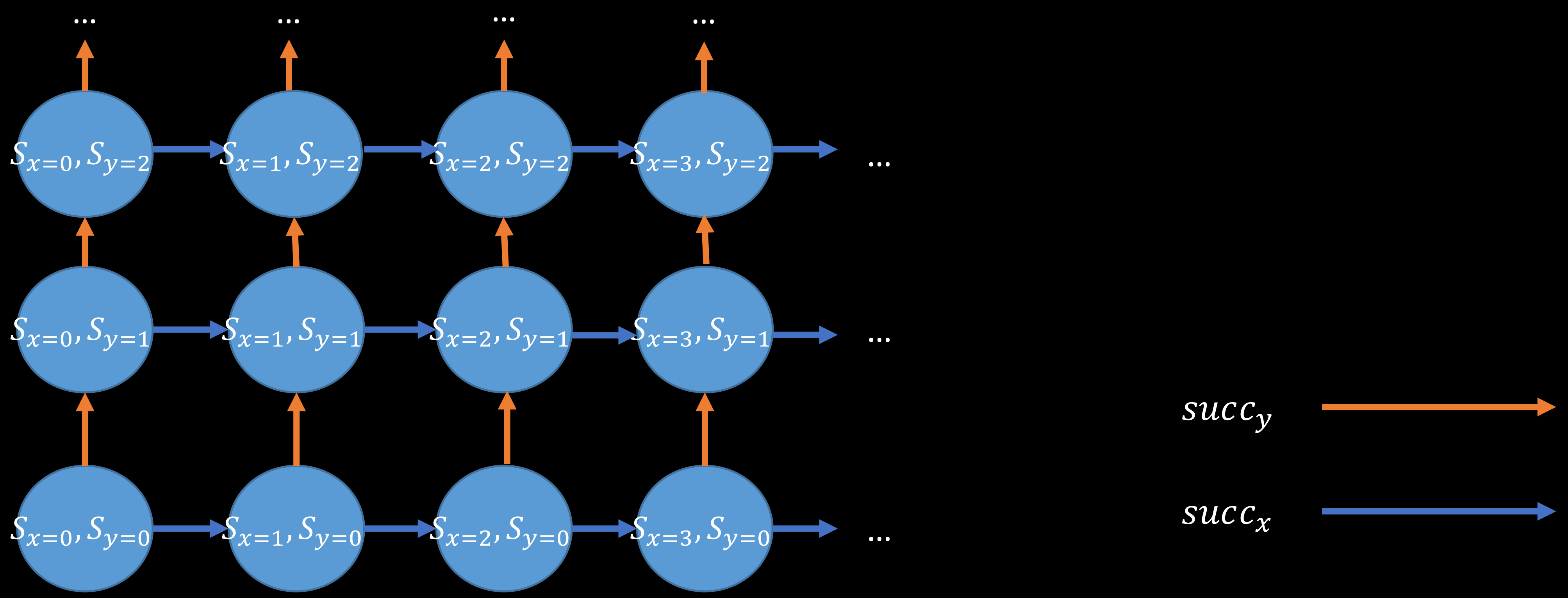
LTS : Labeled Transition System

- プログラム・アクションの実行に伴う状態遷移のモデル
  - ex1 : mod 3のインクリメント・デクリメント



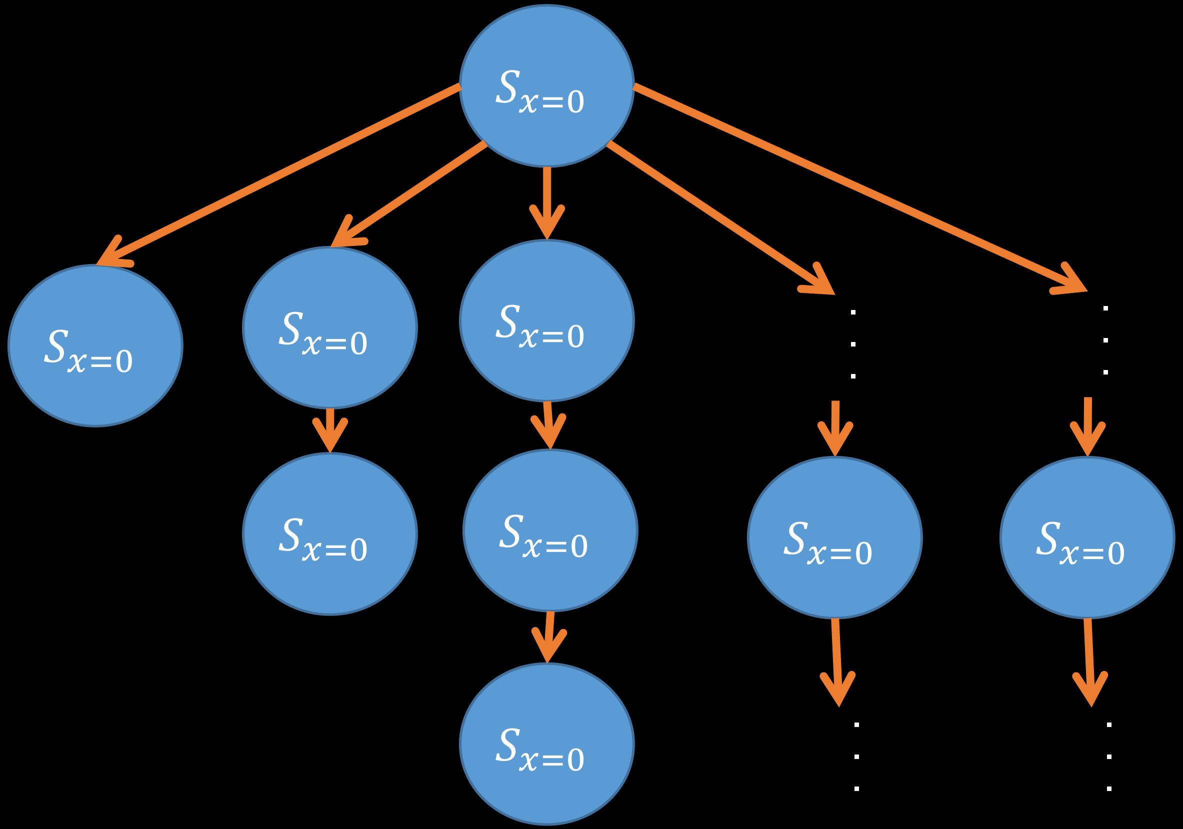
LTS : Labeled Transition System

- プログラム・アクションの実行に伴う状態遷移のモデル
  - ex2 : 無限の状態

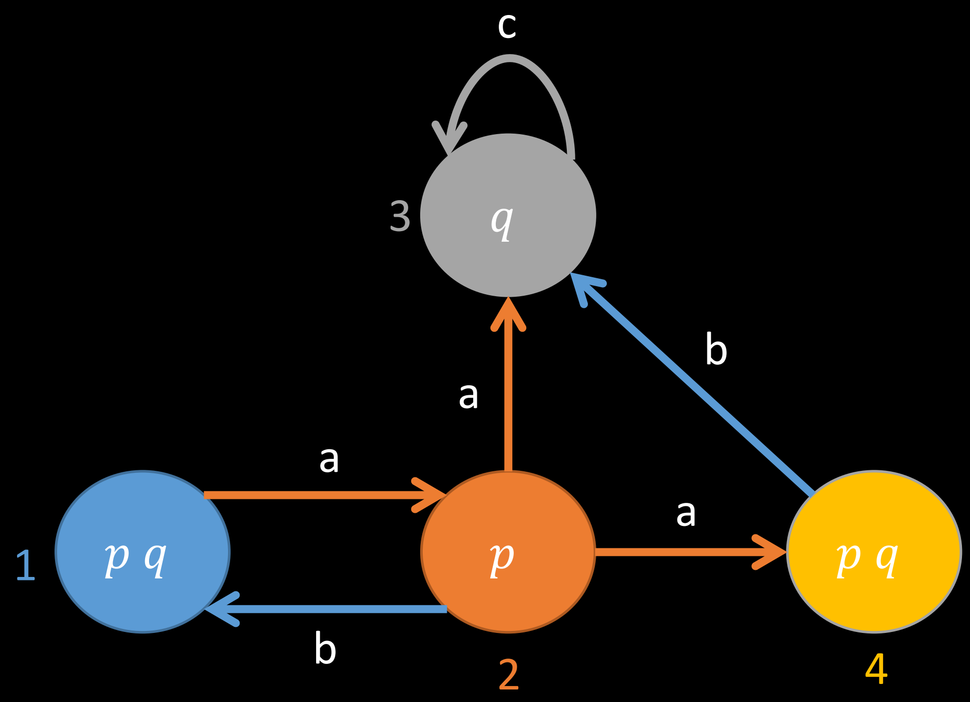


LTS : Labeled Transition System

- プログラム･アクションの実行に伴う状態遷移のモデル
  - ex3 : 無限の分岐



PDL : Propositional Dynamic Logic



LTSの頂点に命題変数を割り当てる

LTSモデル $M = (S, R, V)$

$S = \{1,2,3,4\}$

$R(a) = \{(1,2),(2,3),(2,4)\}$

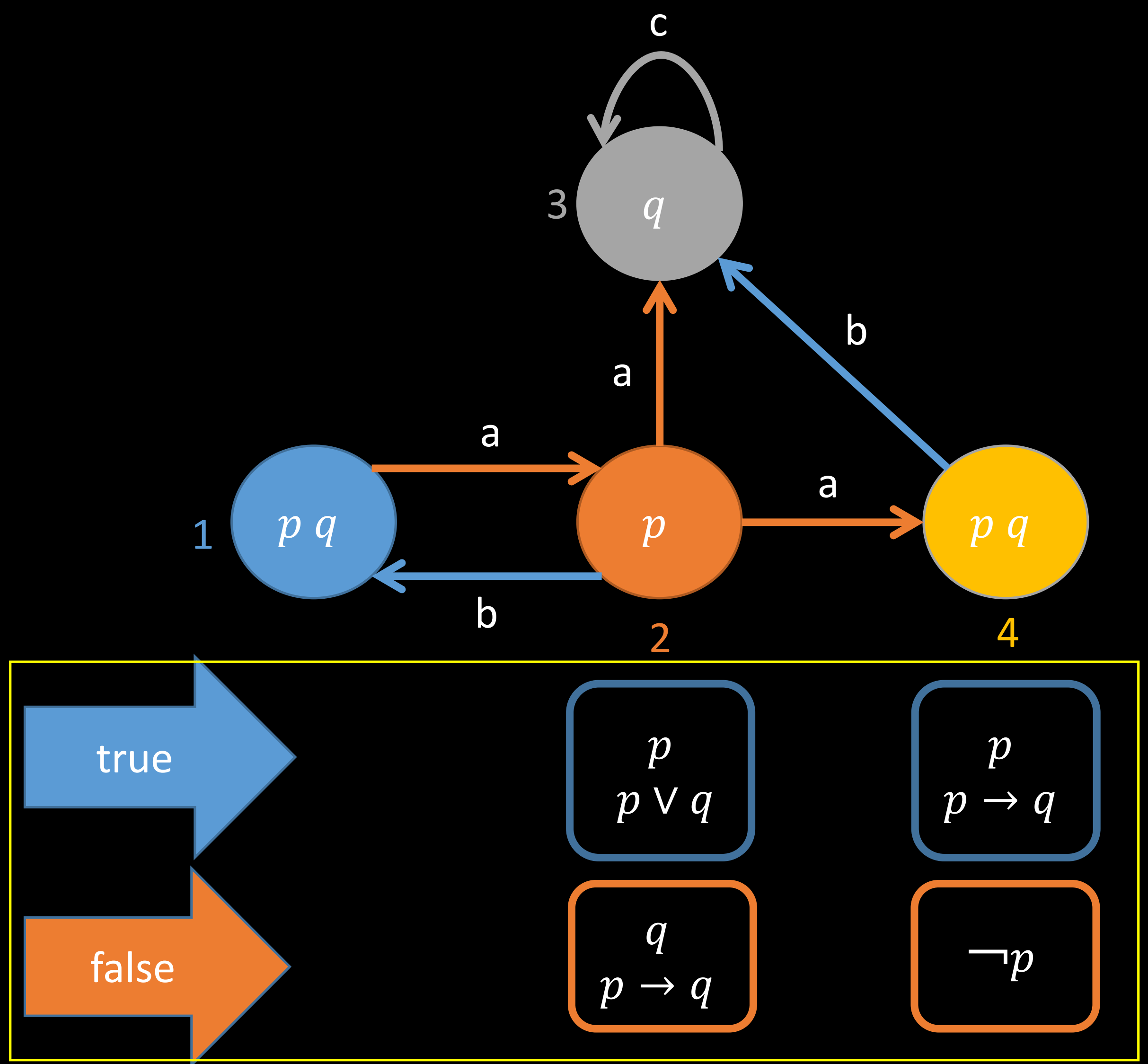
$R(b) = \{(2,1),(4,3)\}$

$R(c) = \{(3,3)\}$

$V(p) = \{1,2,4\}$

$V(q) = \{3,4\}$

PDL : Propositional Dynamic Logic



LTSの頂点に命題変数を割り当てる

LTSモデル $M = (S, R, V)$

$S = \{1,2,3,4\}$

$R(a) = \{(1,2),(2,3),(2,4)\}$

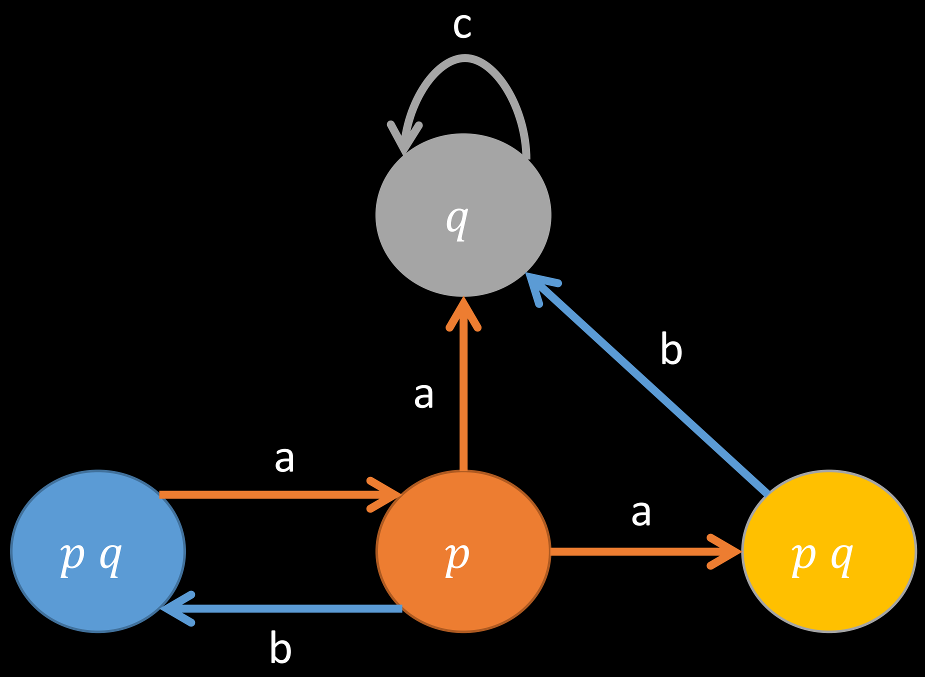
$R(b) = \{(2,1),(4,3)\}$

$R(c) = \{(3,3)\}$

$V(p) = \{1,2,4\}$

$V(q) = \{3,4\}$

PDL : Propositional Dynamic Logic



注: $\neg, \wedge, \vee$

$\neg A \overset{def}{\Longleftrightarrow} A \to 0$

$A \vee B \overset{def}{\Longleftrightarrow} \neg A \to B$

$A \wedge B \overset{def}{\Longleftrightarrow} \neg(\neg A \vee \neg B)$

$[\alpha]A$ … α の遷移先の全ての点で A が真

$\langle\alpha\rangle A$ … α の遷移先のある点で A が真

PDL 論理式

$$A ::= p \text{ (命題変数)}$$
$$\mid 0 \ (\perp)$$
$$\mid A_1 \to A_2$$
$$\mid [\alpha]A_1$$
$$(\langle\alpha\rangle A \overset{def}{\Longleftrightarrow} \neg[\alpha]\neg A)$$

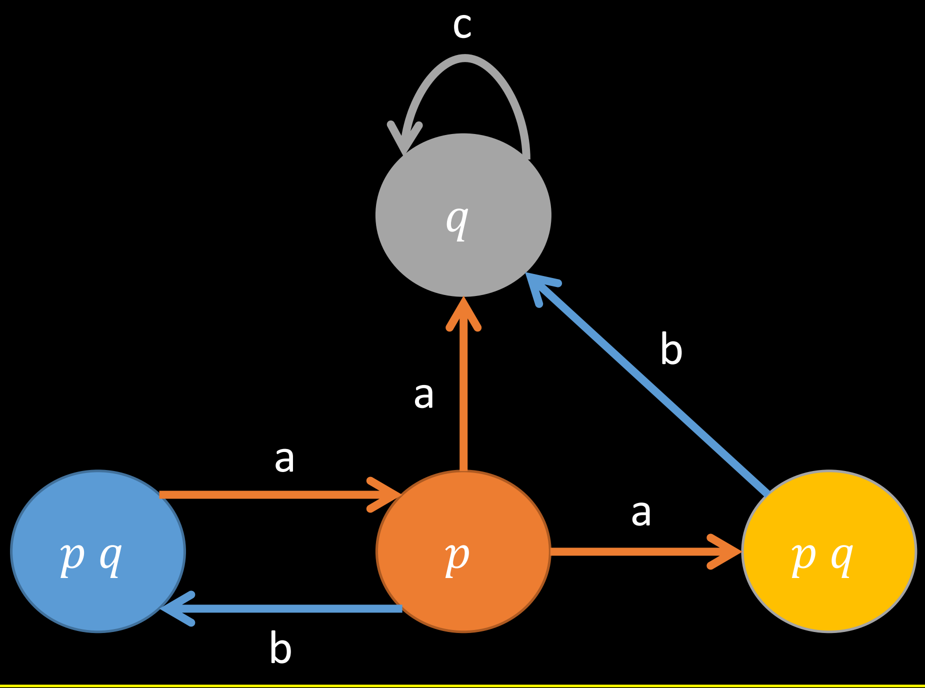
PDL : Propositional Dynamic Logic

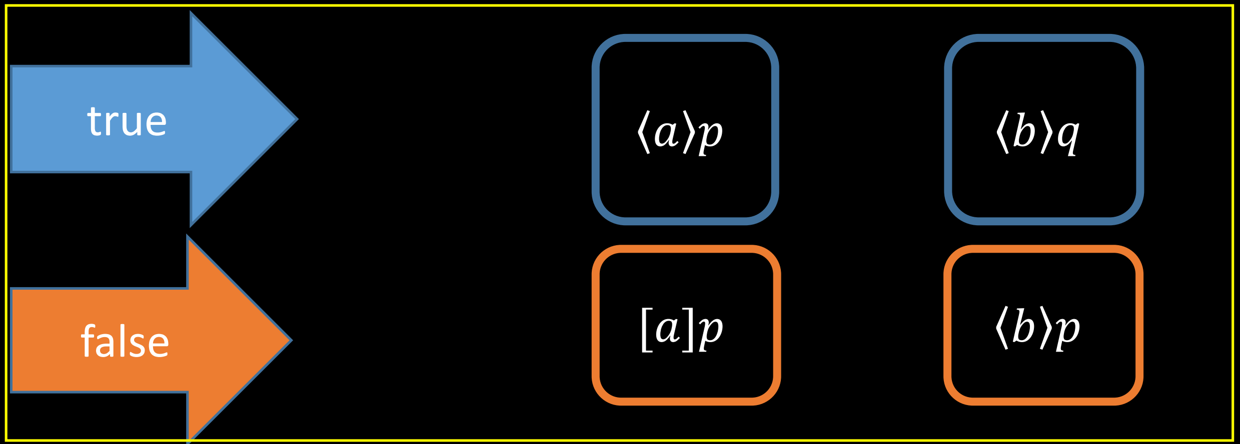
注: $\neg, \wedge, \vee$

$\neg A \overset{def}{\Longleftrightarrow} A \to 0$

$A \vee B \overset{def}{\Longleftrightarrow} \neg A \to B$

$A \wedge B \overset{def}{\Longleftrightarrow} \neg(\neg A \vee \neg B)$





$[\alpha]A$ … α の遷移先の全ての点で A が真

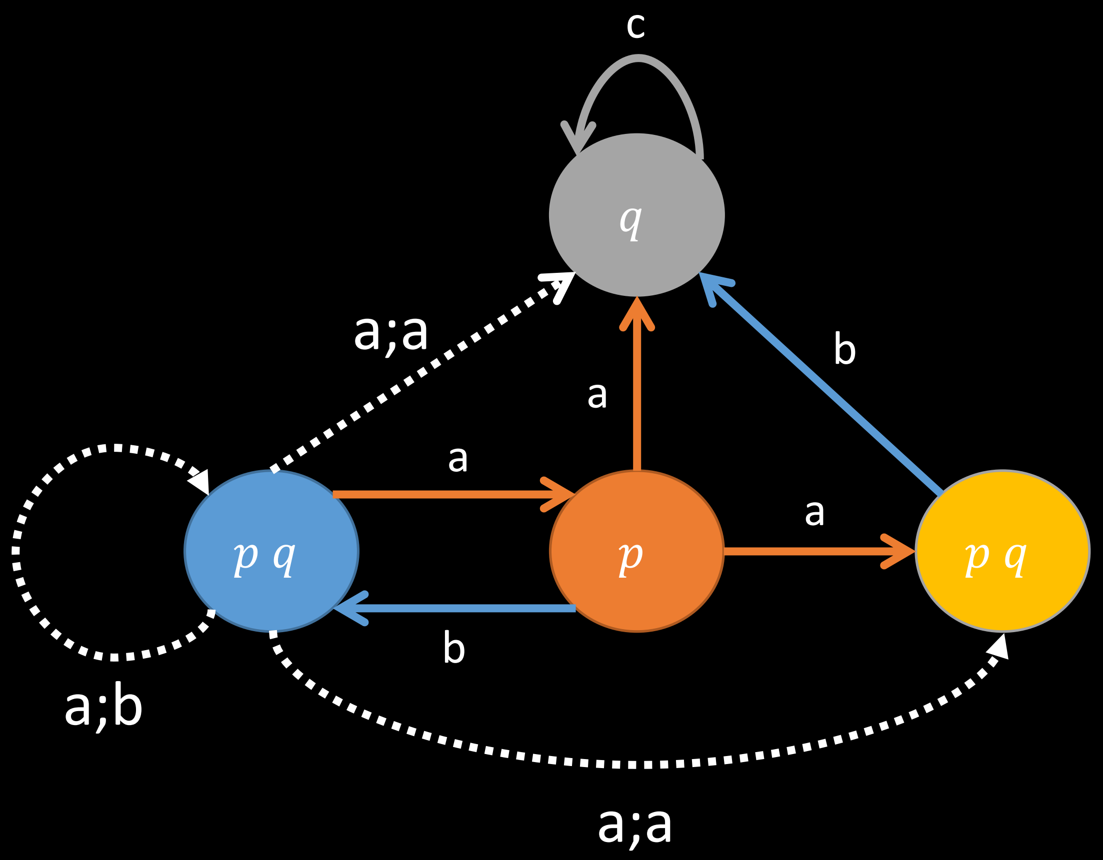
$\langle\alpha\rangle A$ … α の遷移先のある点で A が真

PDL 論理式

$$A ::= p \ (\text{命題変数}) \mid 0 \ (\bot) \mid A_1 \to A_2 \mid [\alpha]A_1$$

$$(\langle\alpha\rangle A \overset{def}{\Longleftrightarrow} \neg[\alpha]\neg A)$$

PDL : Propositional Dynamic Logic



PDL 論理式

$$A \;::=\; p \mid 0 \mid A_1 \to A_2 \mid [\alpha]A_1$$

プログラム

α ::= a (ベースプログラム)

$|\alpha_1 ; \alpha_2$ (結合)

$|\alpha_1 \cup \alpha_2$ (非決定的選択)

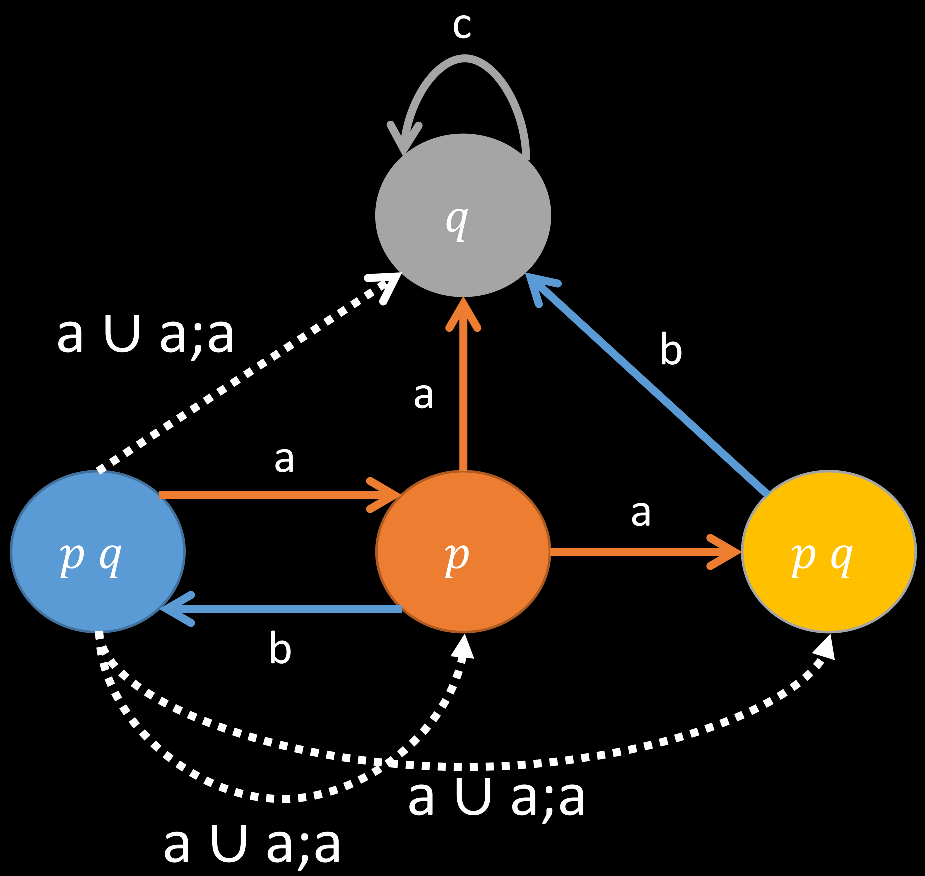
$|\alpha_1^*$ (非決定的繰り返し)

$|\varphi?$ (テスト)

テスト

$$\varphi ::= p \mid 0 \mid \varphi_1 \to \varphi_2$$

PDL : Propositional Dynamic Logic



PDL 論理式

$$A \ ::= \ p \mid 0 \mid A_1 \rightarrow A_2 \mid [\alpha]A_1$$

プログラム

α ::= a (ベースプログラム)

$|\alpha_1 \,;\, \alpha_2$ (結合)

$|\alpha_1 \cup \alpha_2$ (非決定的選択)

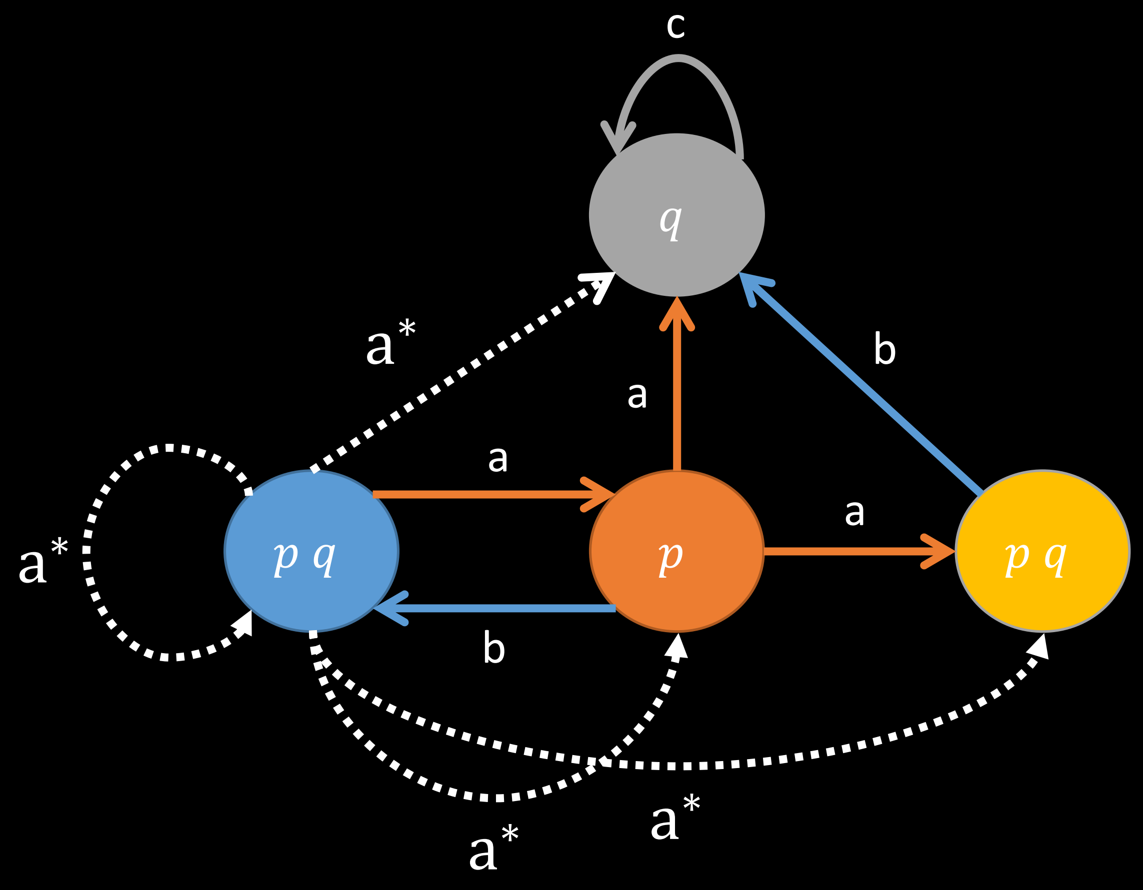
$|\alpha_1^*$ (非決定的繰り返し)

$|\varphi?$ (テスト)

テスト

$$\varphi ::= \ p \mid 0 \mid \varphi_1 \rightarrow \ \varphi_2$$

PDL : Propositional Dynamic Logic



PDL 論理式

$$A \ ::= \ p \mid 0 \mid A_1 \rightarrow A_2 \mid [\alpha]A_1$$

プログラム

α ::= a (ベースプログラム)

$|\alpha_1 \,;\, \alpha_2$ (結合)

$|\alpha_1 \cup \alpha_2$ (非決定的選択)

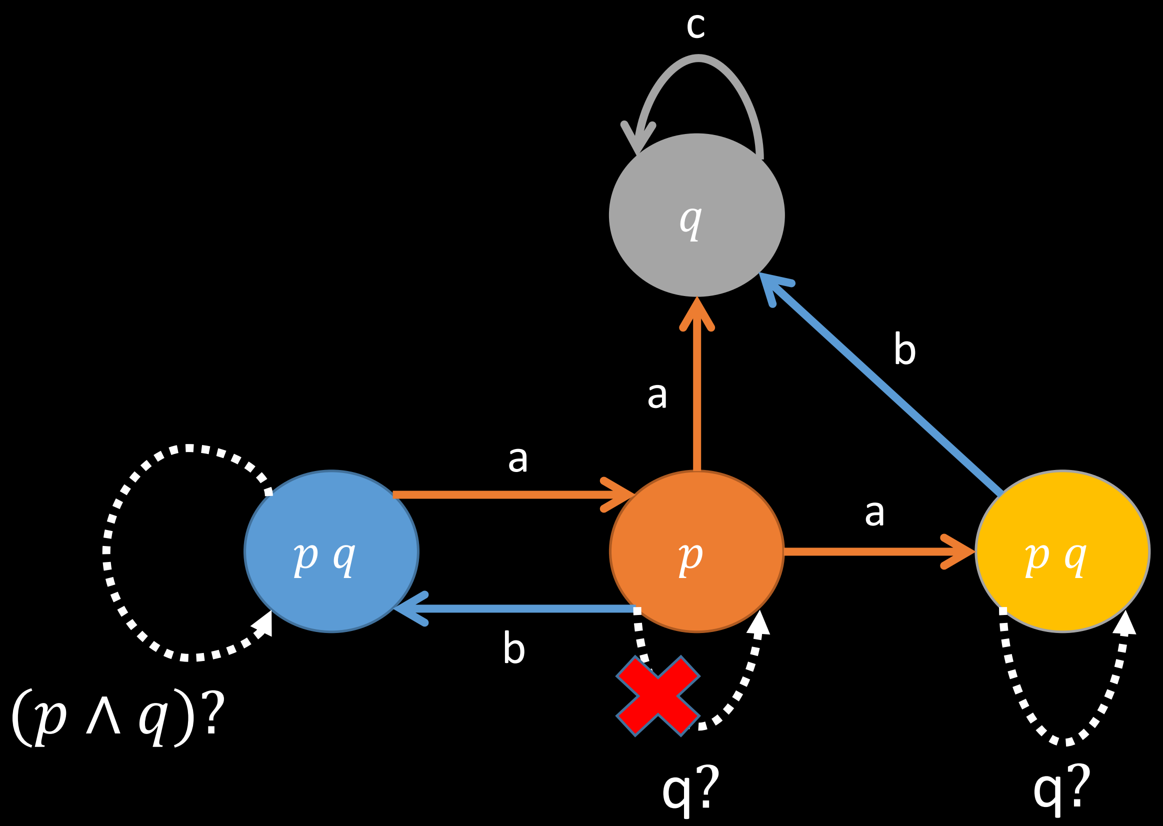
$|\alpha_1^*$ (非決定的繰り返し)

$|\varphi?$ (テスト)

テスト

$$\varphi ::= \ p \mid 0 \mid \varphi_1 \rightarrow \ \varphi_2$$

PDL : Propositional Dynamic Logic



PDL 論理式

$$A\ ::=\ p\mid 0\mid A_1 \rightarrow A_2 \mid [\alpha]A_1$$

プログラム

α ::= a (ベースプログラム)

$|\alpha_1 ; \alpha_2$ (結合)

$|\alpha_1 \cup \alpha_2$ (非決定的選択)

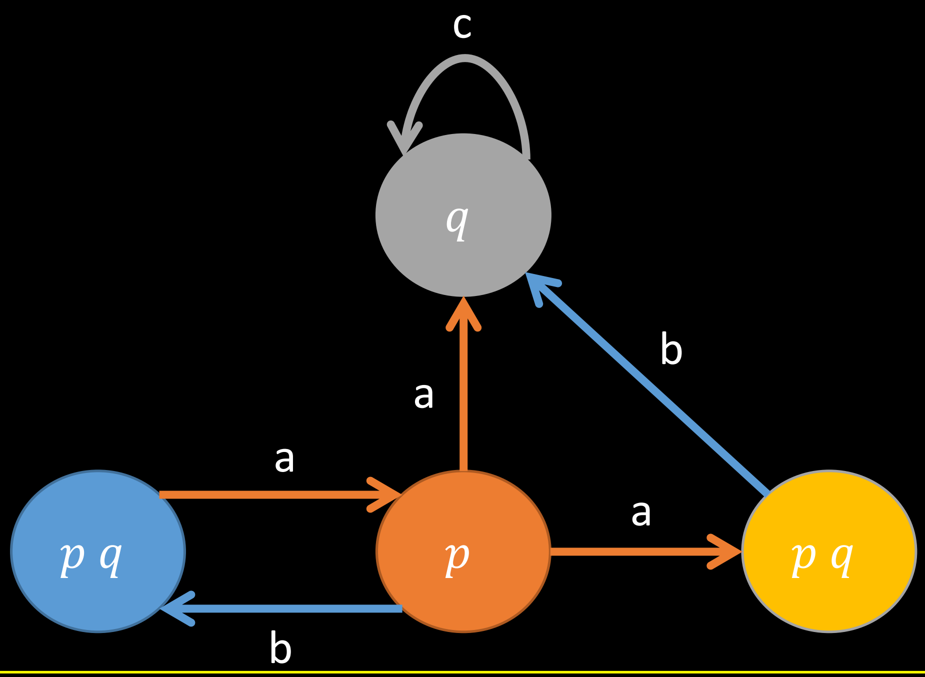
$|\alpha_1^*$ (非決定的繰り返し)

$|\varphi?$ (テスト)

テスト

$$\varphi ::= \ p\mid 0\mid \varphi_1 \rightarrow\ \varphi_2$$

PDL : Propositional Dynamic Logic



true

$\langle a \cup b \rangle \neg p$

$\langle b; q?; c \rangle q$

false

$[(a; b)^*]p$

$\langle b; p?; c \rangle q$

PDL 論理式

$$A \ ::= \ p \mid 0 \mid A_1 \to A_2 \mid [\alpha]A_1$$

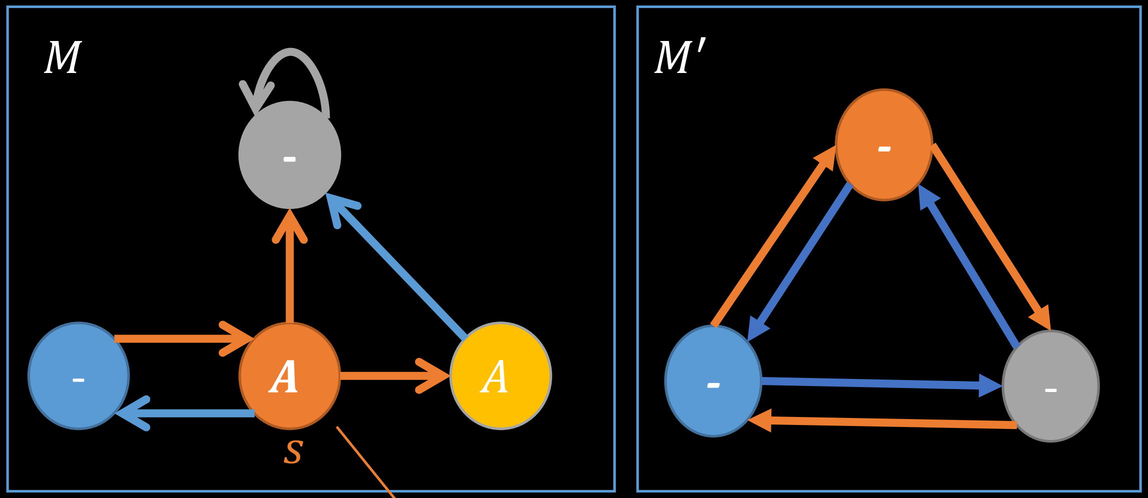
プログラム

$$\alpha \ ::= a \mid \alpha_1; \alpha_2 \mid \alpha_1 \cup \alpha_2 \mid \alpha_1^* \mid \varphi?$$

テスト

$$\varphi ::= \ p \mid 0 \mid \varphi_1 \to \varphi_2$$

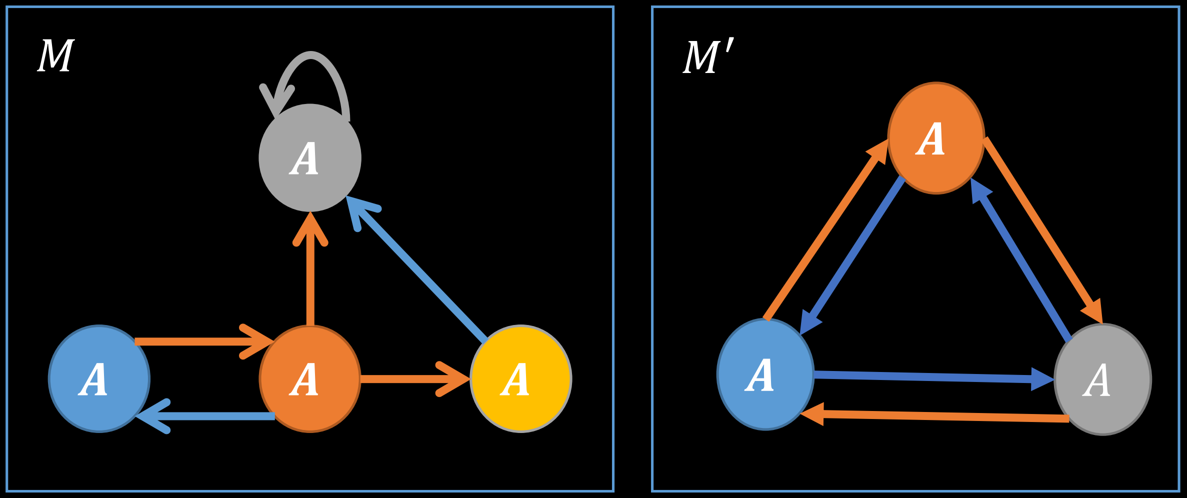
A が充足可能

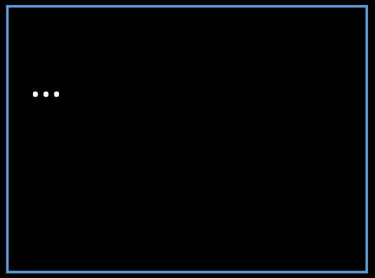


$(M, s) \vDash A$

あるモデル M の
ある点 s で$(M, s) \vDash A$

A が恒真





任意のモデル M の
任意の点 s で $(M, s) \vDash A$

モデルに関する性質

- ツリーモデル性

  任意の A について

  A が　恒真　⇔ ツリーモデル上で A が恒真

  (　〃　(充足可能)　⇔　　　〃　　　　(充足可能)　と同値)

- 有限モデル性

  任意の A について

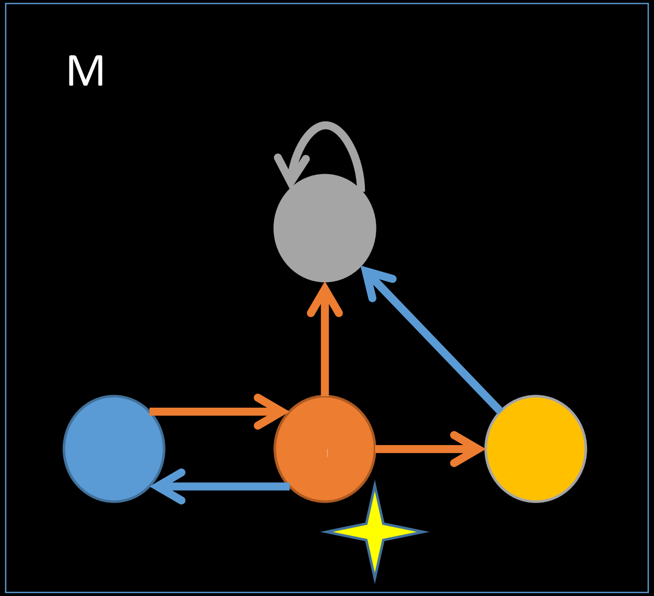
  A が　恒真　⇔ 有限モデル上で A が恒真

  (　〃　(充足可能)　⇔　　　〃　　　　(充足可能)　と同値)

PDLはツリーモデル性を持つ

- tree unfolding
  - 各点の論理式の真偽を変えずにツリーモデルに変換する手法[Sahlqvist 1973]

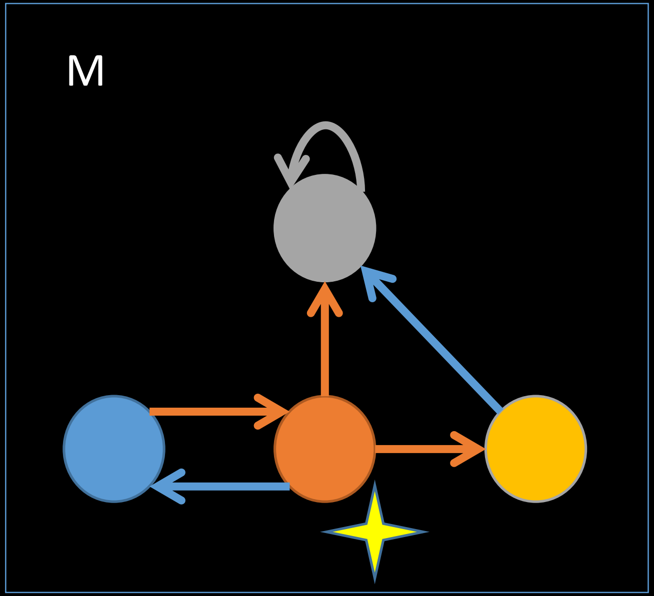
(証明略)

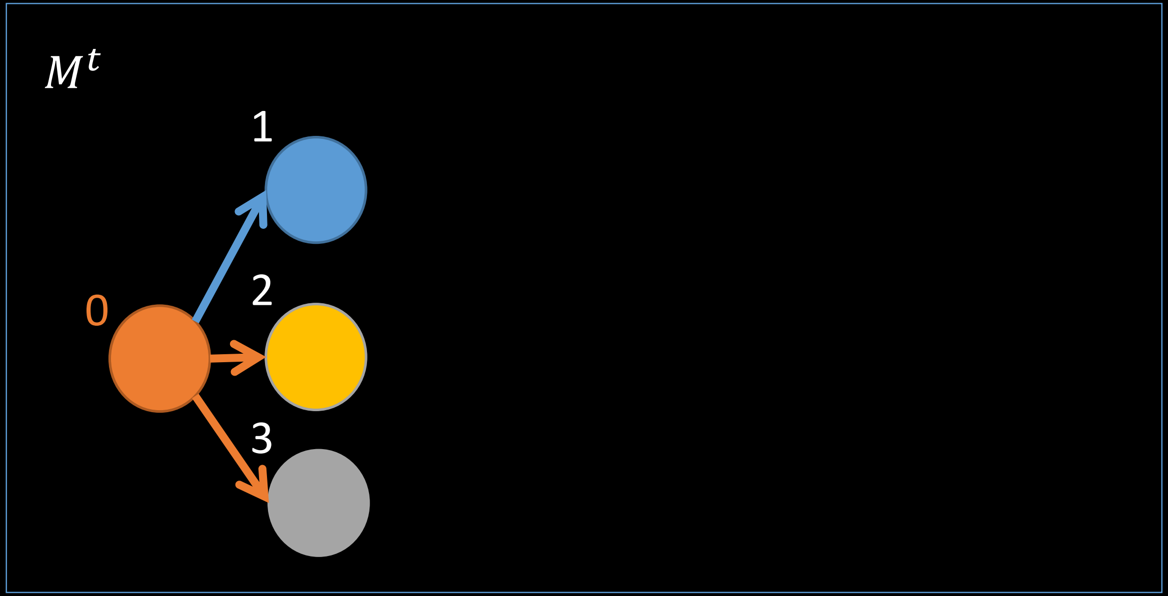


PDLはツリーモデル性を持つ

- tree unfolding
  - 各点の論理式の真偽を変えずにツリーモデルに変換する手法[Sahlqvist 1973]

(証明略)

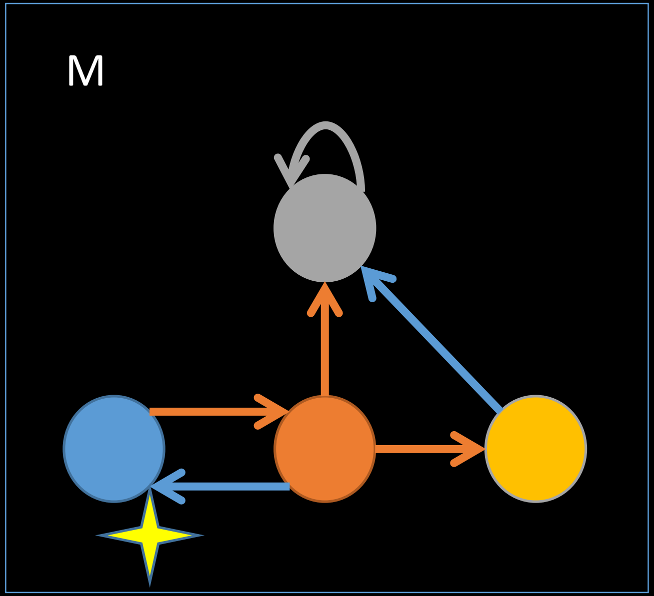


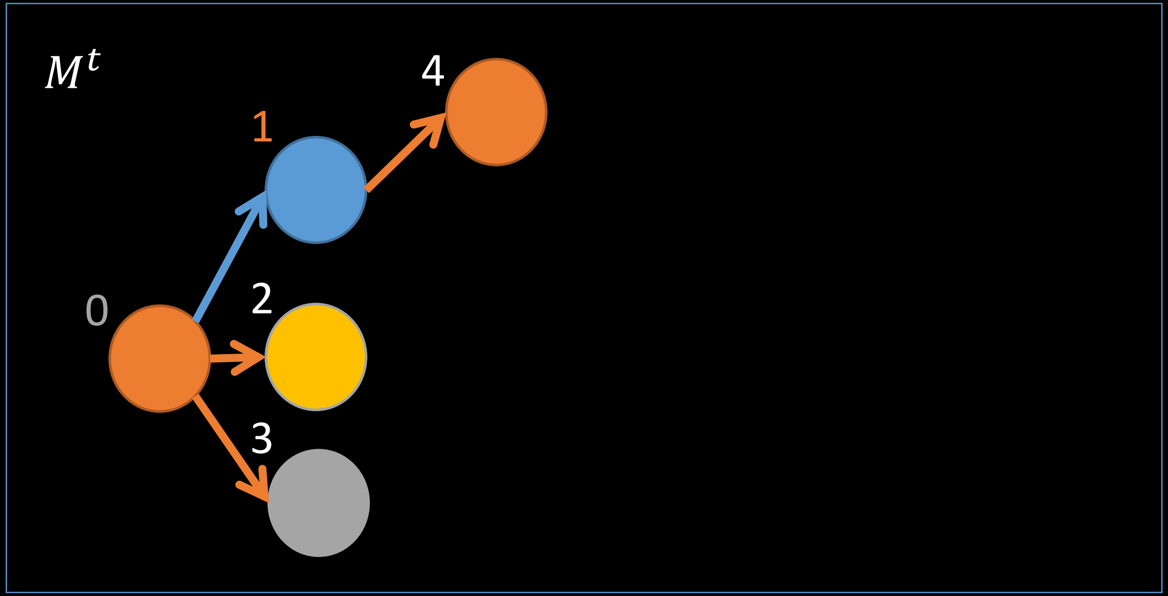


PDLはツリーモデル性を持つ

- tree unfolding
  - 各点の論理式の真偽を変えずにツリーモデルに変換する手法[Sahlqvist 1973]

(証明略)

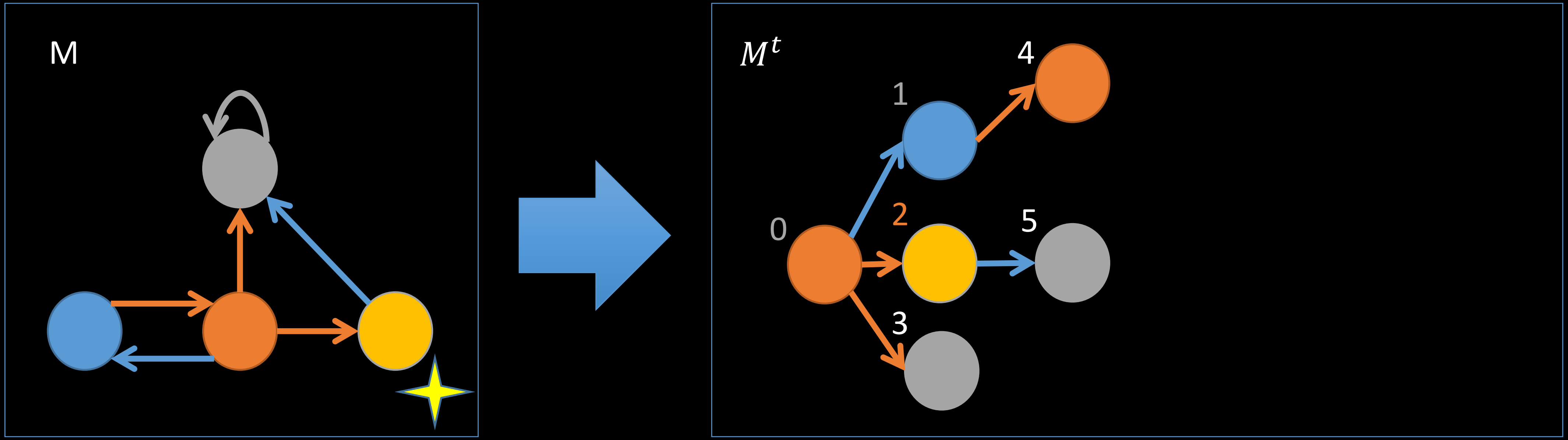




PDLはツリーモデル性を持つ

- tree unfolding
  - 各点の論理式の真偽を変えずにツリーモデルに変換する手法[Sahlqvist 1973]

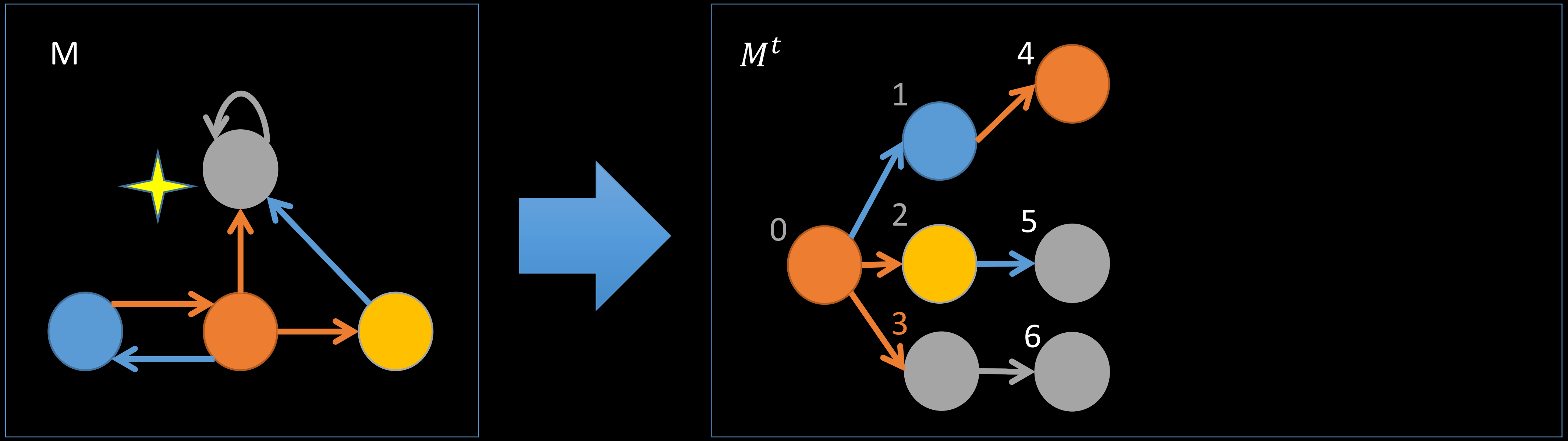
(証明略)



PDLはツリーモデル性を持つ

- tree unfolding
  - 各点の論理式の真偽を変えずにツリーモデルに変換する手法[Sahlqvist 1973]

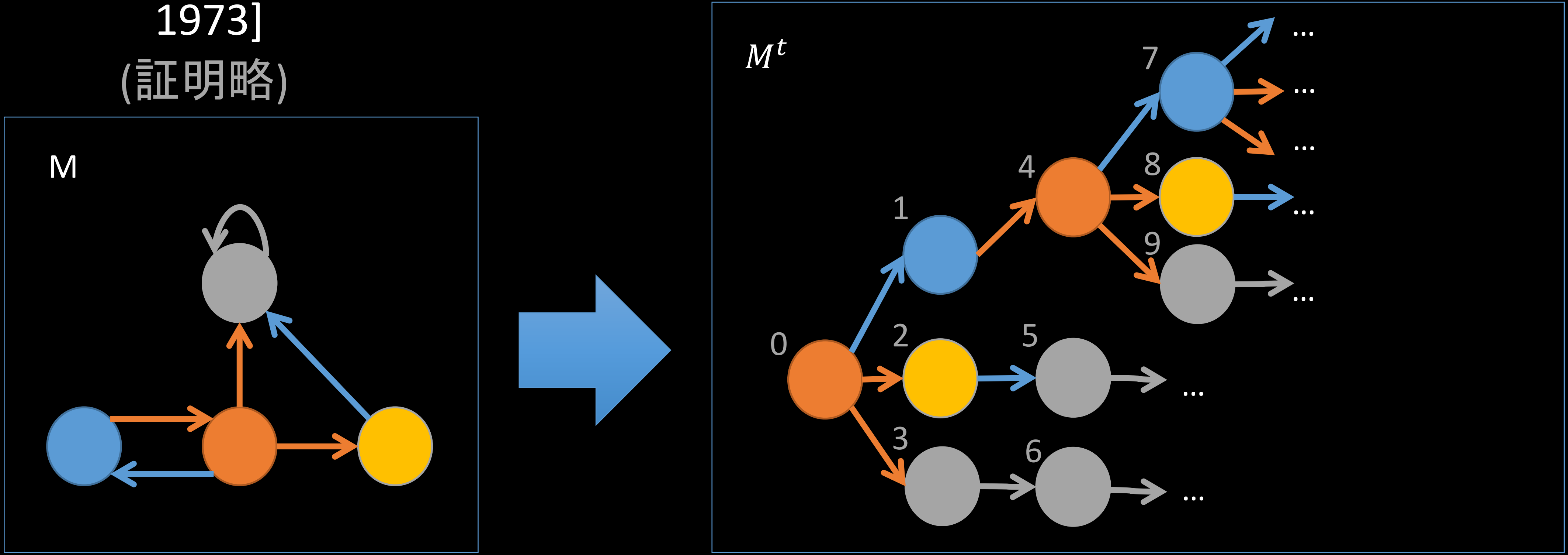
(証明略)



PDLはツリーモデル性を持つ

- tree unfolding
  - 各点の論理式の真偽を変えずにツリーモデルに変換する手法[Sahlqvist 1973]

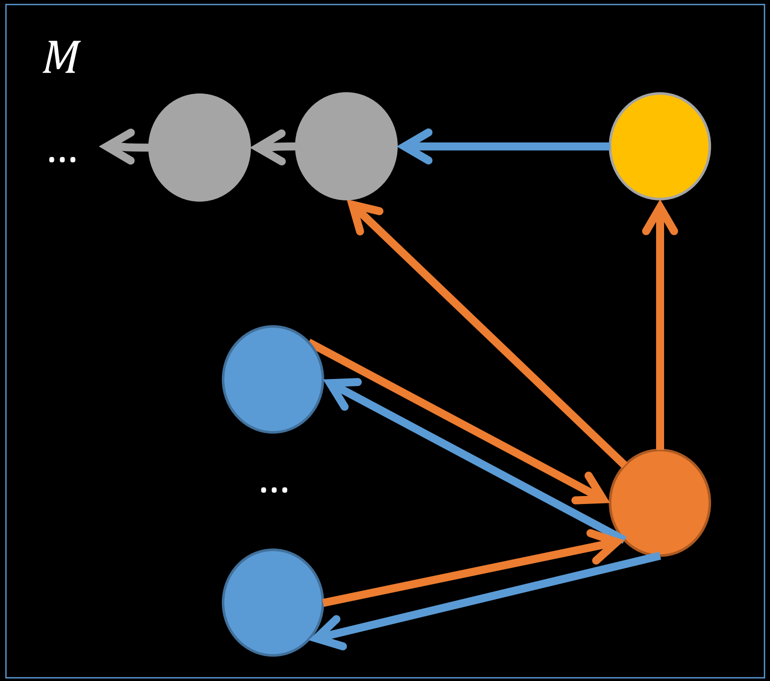
(証明略)

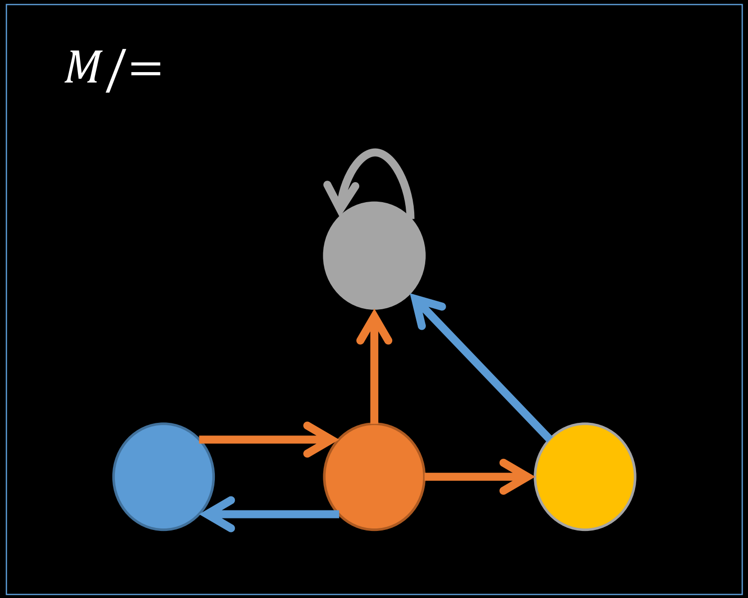


PDLは有限モデル性を持つ

- filtration
  - Aの部分論理式に関して同値な点を同一視して有限化する手法 [Fischer,Ladner 1979]

(証明略)





IPDL : PDL with Intersection (1983)

- IPDL 論理式

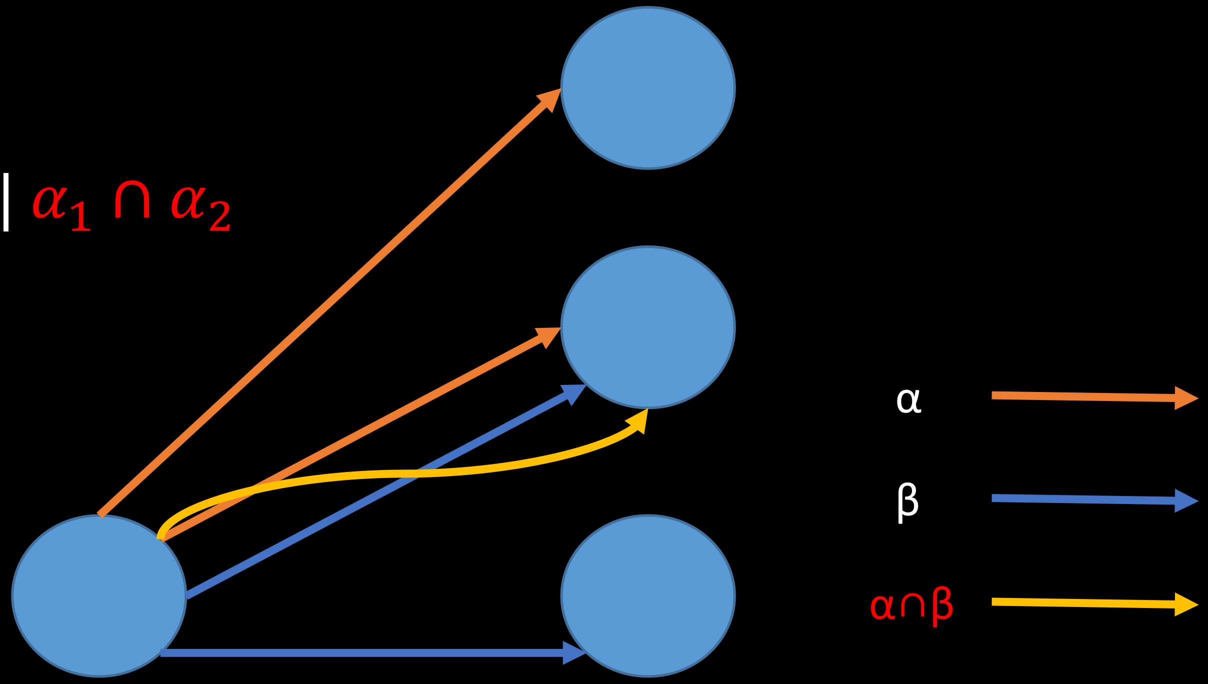
  $A ::= p \mid 0 \mid A_1 \to A_2 \mid [\alpha]A_1$

- プログラム

  $\alpha ::= a \mid \alpha_1 ; \alpha_2 \mid \alpha_1 \cup \alpha_2 \mid \alpha_1^* \mid \varphi? \mid \alpha_1 \cap \alpha_2$

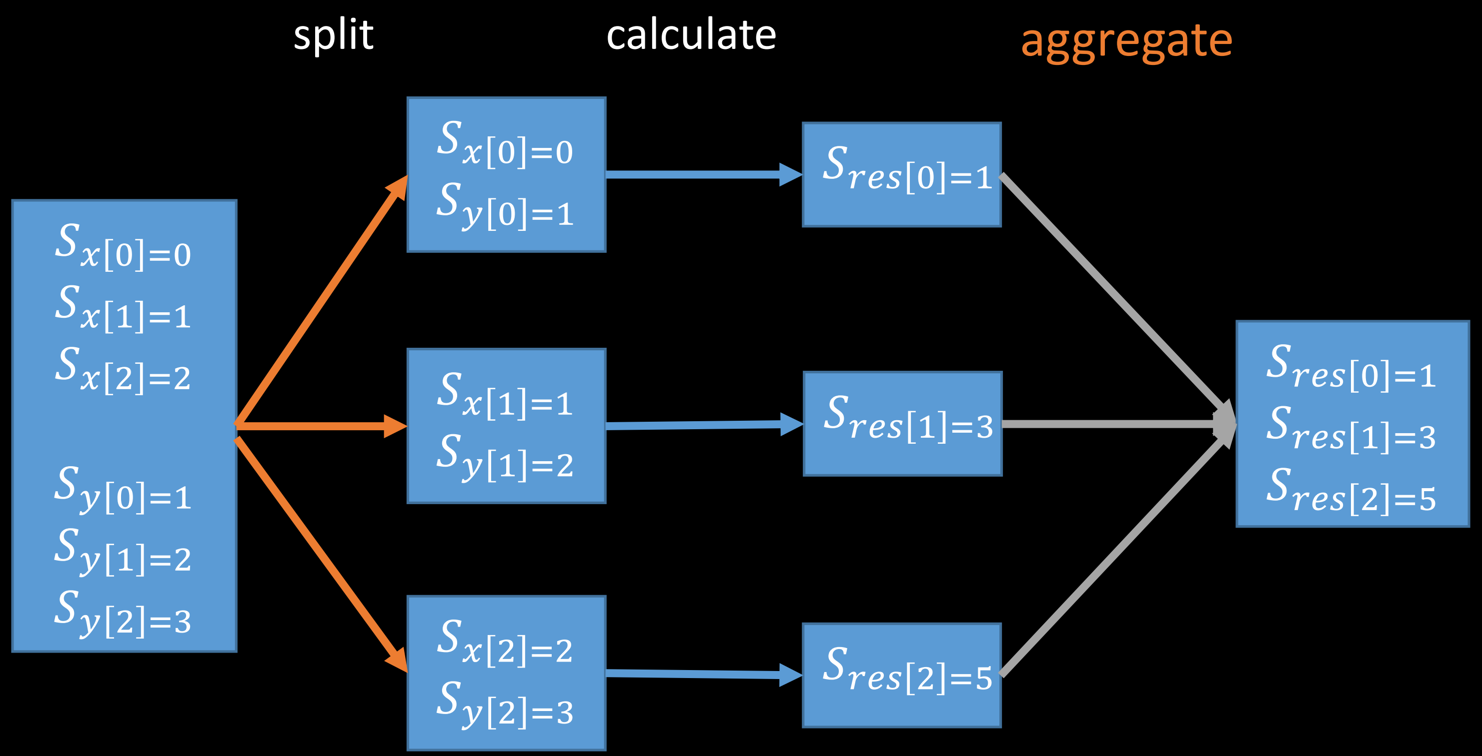
- テスト

  $\varphi ::= p \mid 0 \mid \varphi_1 \to \varphi_2$



IPDL : PDL with Intersection (1983)

- ∩は並列プログラムを扱える

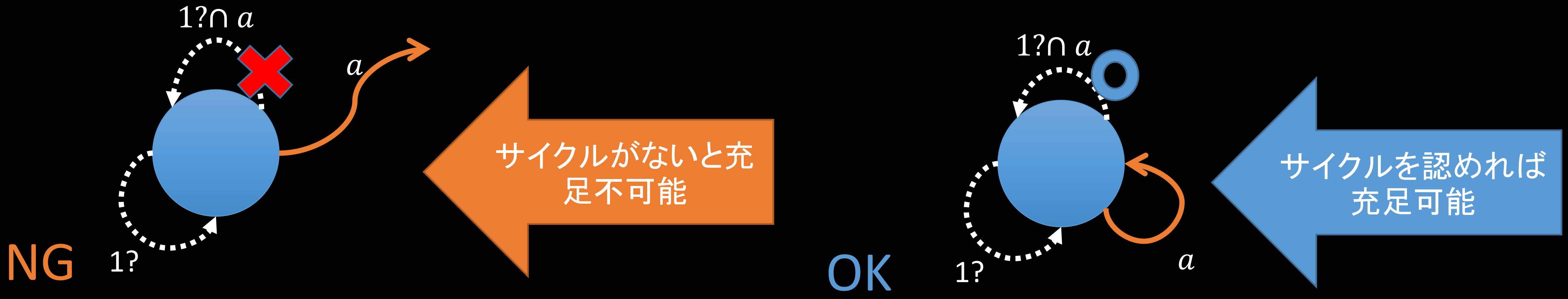


$$S_{x=[0,1,2]} \wedge S_{y=[1,2,3]} \rightarrow [split_0; cal_0; aggregate_0 \cap split_1; cal_1; aggregate_1 \cap split_2; cal_2; aggregate_2]S_{res=[1,3,5]}$$

IPDLはツリーモデル性を持たない

- 反例　$\langle 1? \cap a \rangle 1$

ツリーモデル上では充足不可能だが、サイクルを認めれば充足可能



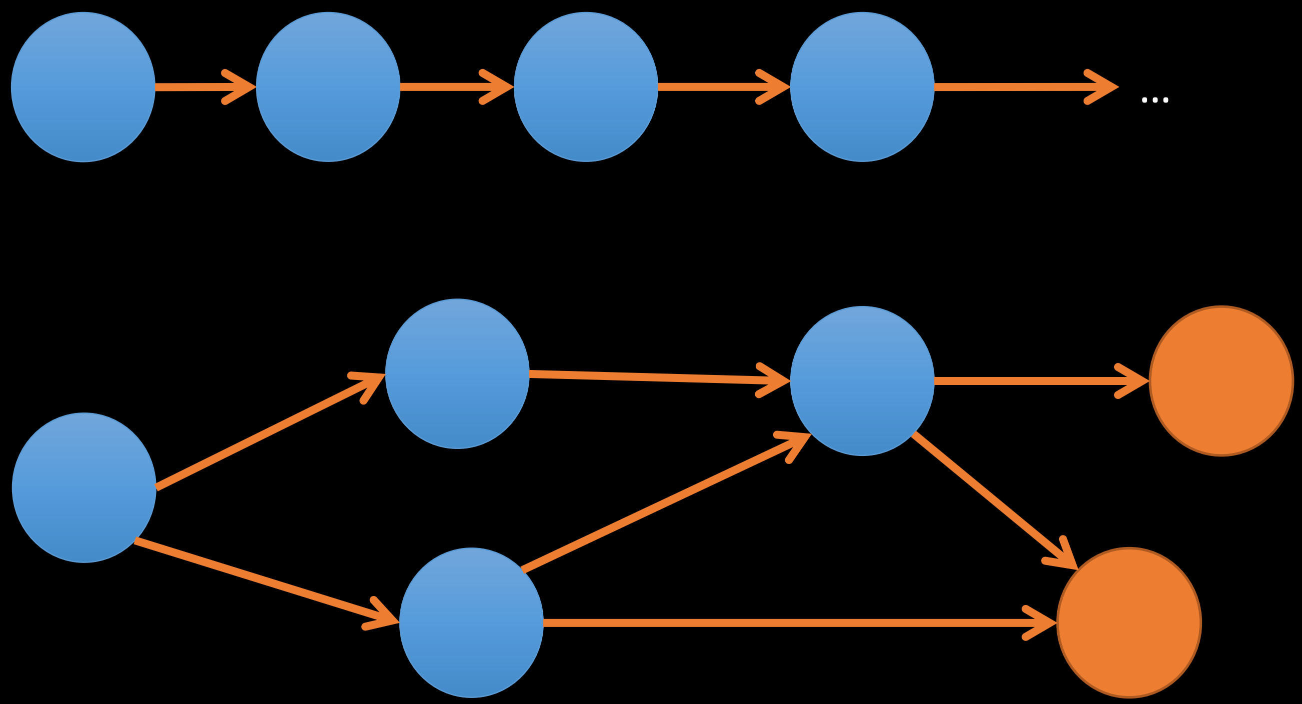
➡ IPDLでは、tree unfoldingが出来ない

IPDLは有限モデル性を持たない

行き先が存在

サイクルが無い

- 反例 $[a^*](\langle a\rangle 1 \wedge [1?\cap a^+]0)$



無限の直線を許せば充足可能

有限のdagは必ず葉を持つ
⇒充足不可能

IPDLでは、filtrationが出来ない

IPHL : PHL with Intersection

- IPHL 論理式

  $$A ::= \{\varphi_1\}\alpha\{\varphi_2\}$$

- プログラム

  $$\alpha ::= a \mid \alpha_1 ; \alpha_2 \mid \alpha_1 \cup \alpha_2 \mid \alpha_1^* \mid \varphi ? \mid \alpha_1 \cap \alpha_2$$

- テスト

  $$\varphi ::= p \mid 0 \mid \varphi_1 \rightarrow \varphi_2$$

- $\{\varphi_1\}\alpha\{\varphi_2\}$ … φ_1が成り立つ時、αの遷移先で必ずφ_2が成り立つ
  - 意味として、IPDLの$[\varphi_1 ? ; \alpha]\varphi_2$と同じ
  - IPDLの部分論理式として扱える

IPHLの恒真性、充足可能性

IPHL 論理式 $\{\varphi_1\}\alpha\{\varphi_2\}$ が恒真⇔ IPDL 論理式 $[\varphi_1?;\alpha]\varphi_2$ が恒真
⇔ 〃 $[\varphi_1?;\alpha;\neg\varphi_2?]0$ が恒真
⇔ 〃 $\langle\varphi_1?;\alpha;\neg\varphi_2?\rangle 1$ が充足可能

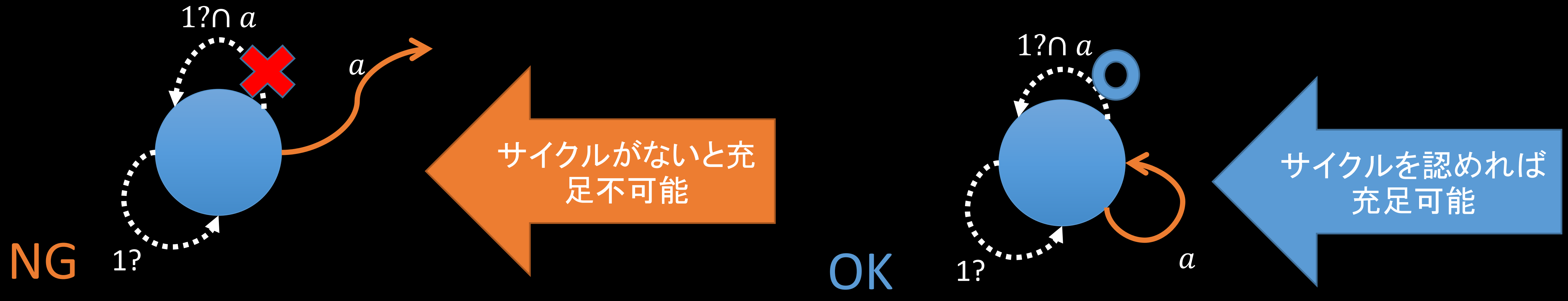
よって、IPHLの恒真性はIPDLの$\langle\varphi_1?;\alpha;\neg\varphi_2?\rangle 1$の形の充足可能性を考えればよい.

記述が煩雑になるため、少し一般化して$\langle\alpha\rangle 1$の形の論理式の充足可能性を扱う.

IPHLはツリーモデル性を持たない

- 反例　$\langle 1?\cap a\rangle 1$

（IPDLと同様の反例をそのままIPHLの反例に使える）



IPHLでは、tree unfoldingが出来ない

IPHLは有限モデル性を持つ？

- IPDLの時の反例 $[X^*](\langle X\rangle 1 \land [1? \cap X^+]0)$ はIPHLで記述出来ない

→別の反例を探す？ or 有限モデル性を持つ？

IPHLは有限モデル性を持つ

- IPDLの時の反例　$[X^*](\langle X\rangle 1 \land [1?\cap X^+]0)$　はIPHLで記述出来ない

→別の反例を探す？ or 有限モデル性を持つ？

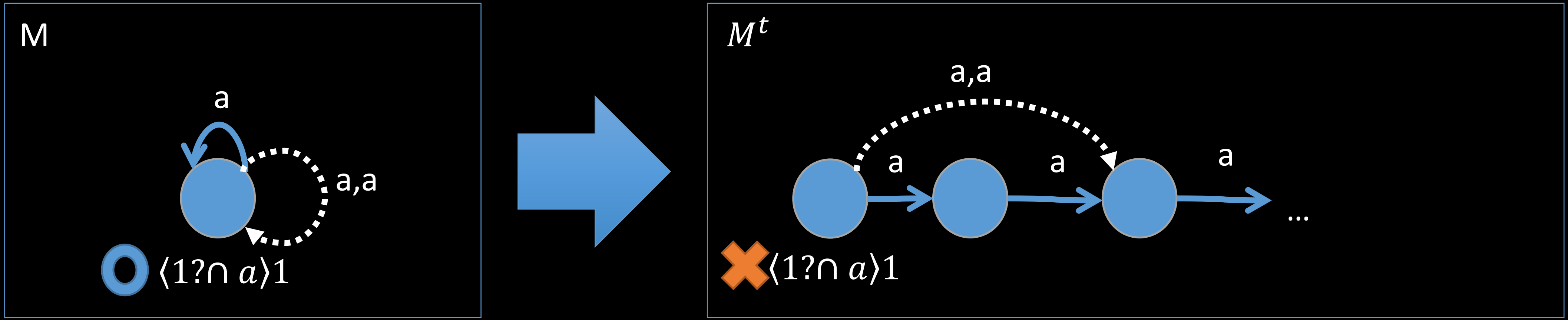
→IPHLは有限モデル性を持つ

- 本発表

IPDLにおけるtree unfoldingの問題点

- 点が複製されると遷移が分散する

→ どうにかして遷移をマージしたい



t^* 変換

- ベースプログラムとテストの後ろに t^*を置く.
  - $T(a) = a; t^*$
  - $T(\varphi?) = \varphi?; t^*$
  - $T(\alpha;\beta) = T(\alpha); T(\beta)$
  - $T(\alpha \cup \beta) = T(\alpha) \cup T(\beta)$
  - $T(\alpha^*) = T(\alpha)^*$
  - $T(\alpha \cap \beta) = T(\alpha) \cap T(\beta)$

  - $T([\alpha]A) = [T(\alpha)]T(A)$
  - $T(A \to B) = T(A) \to T(B)$

補題　任意の二点 u, vについて

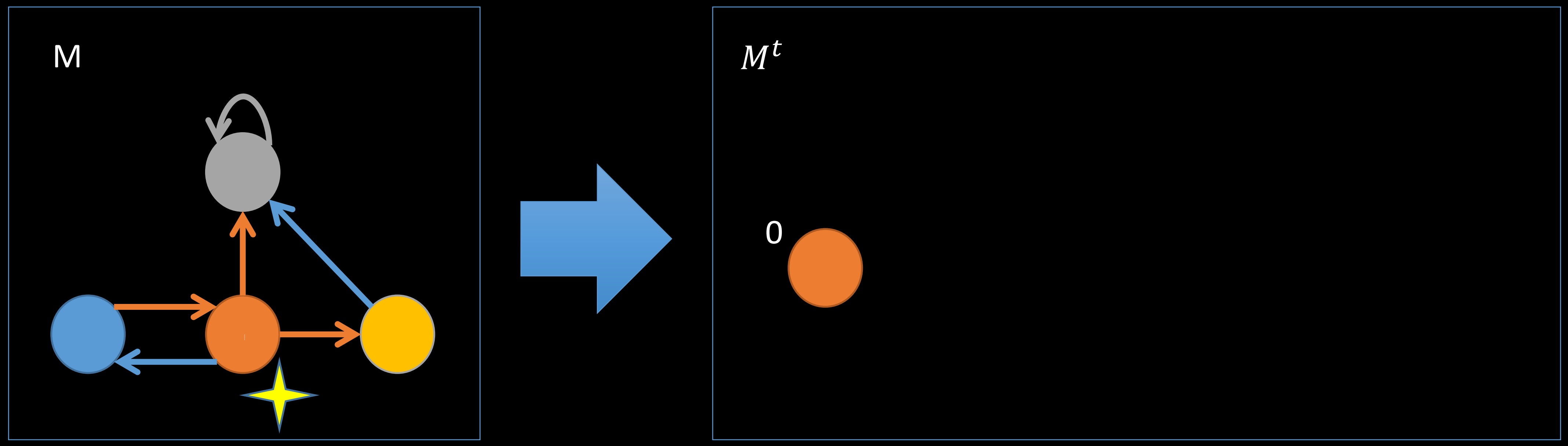
$$u \xrightarrow{T(\alpha)} v \Leftrightarrow u \xrightarrow{T(\alpha);t^*} v$$

証明　αの構造に関する帰納法

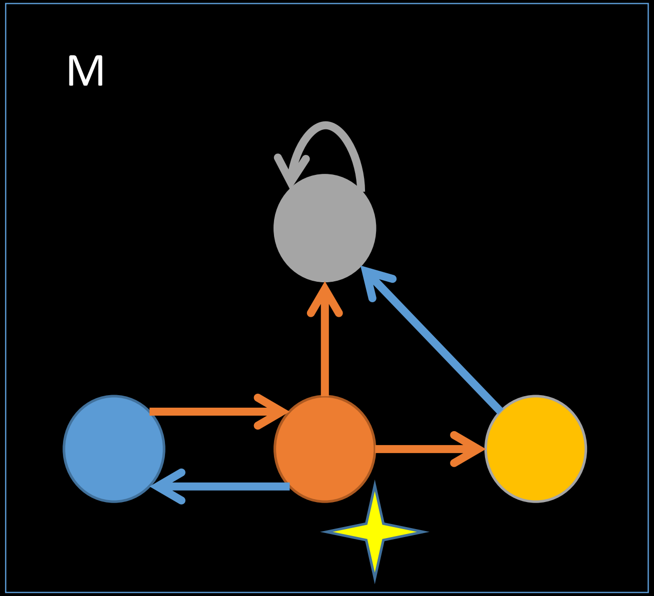
$$u \xrightarrow{T(a)} v \Leftrightarrow u \xrightarrow{a;t^*} v \Leftrightarrow u \xrightarrow{a;t^*;t^*} v \Leftrightarrow u \xrightarrow{T(a);t^*} v$$

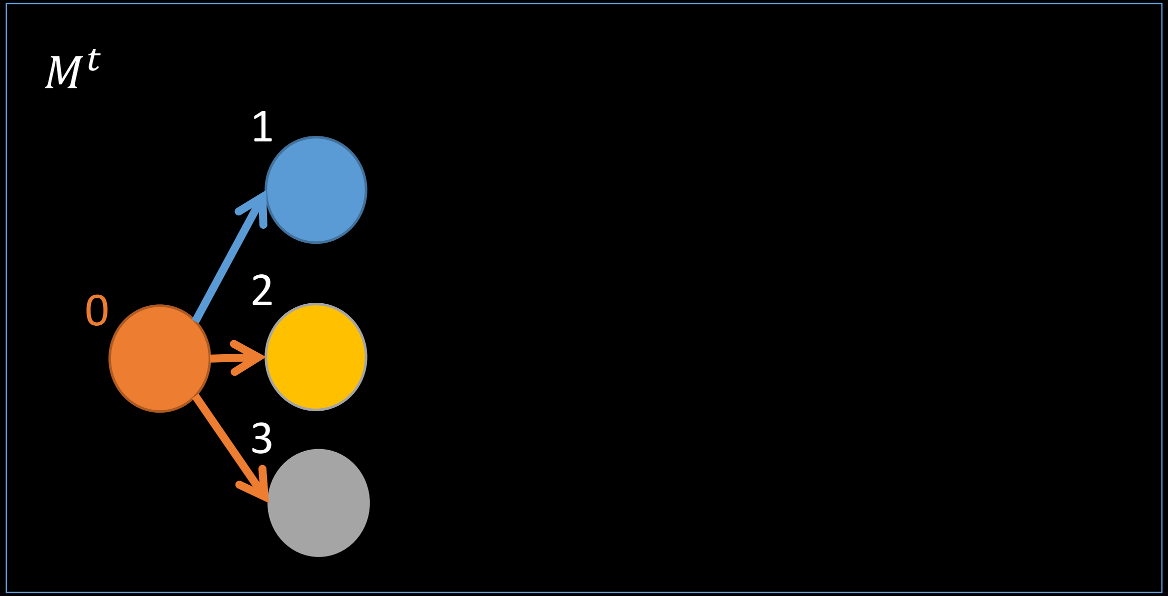
$$\begin{aligned} u \xrightarrow{T(\alpha;\beta)} v &\Leftrightarrow \exists w.\, u \xrightarrow{T(\alpha)} w \xrightarrow{T(\beta)} v \\ &\Leftrightarrow \exists w.\, u \xrightarrow{T(\alpha)} w \xrightarrow{T(\beta);t^*} v \\ &\Leftrightarrow u \xrightarrow{T(\alpha);T(\beta);t^*} v \\ &\Leftrightarrow u \xrightarrow{T(\alpha;\beta);t^*} v \end{aligned}$$

t^* unfolding



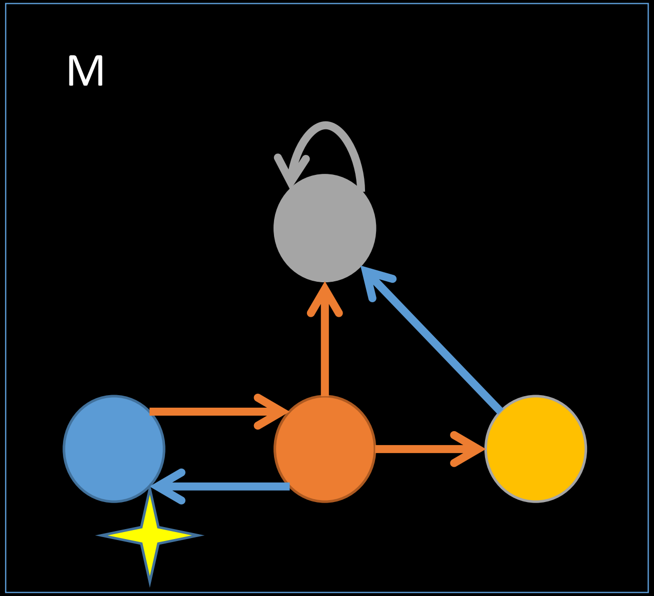
t^* unfolding

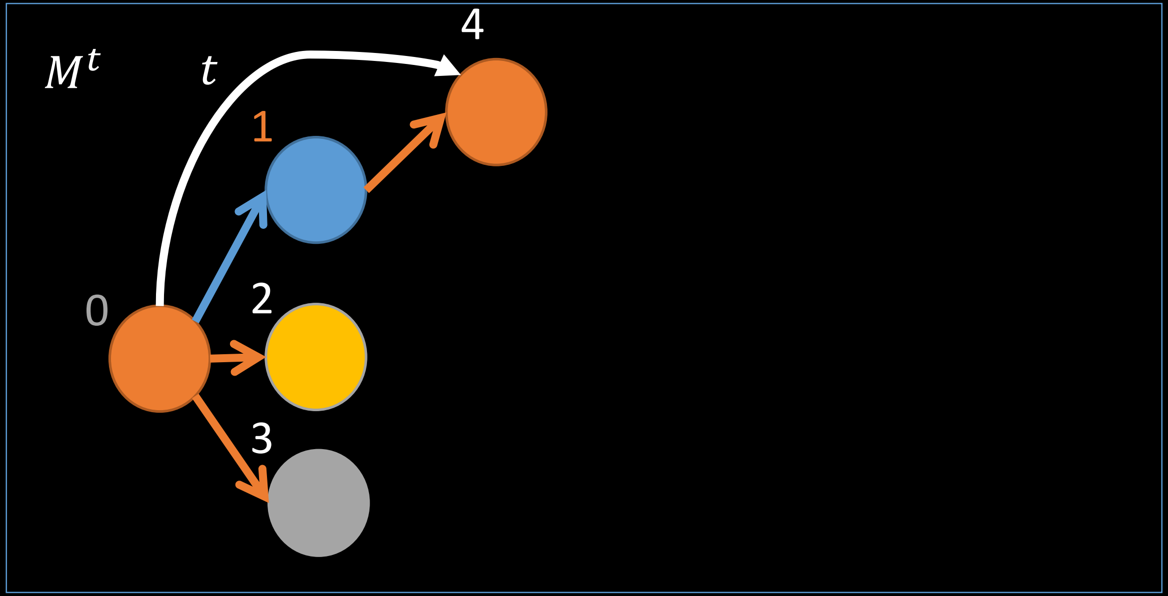




t^* unfolding

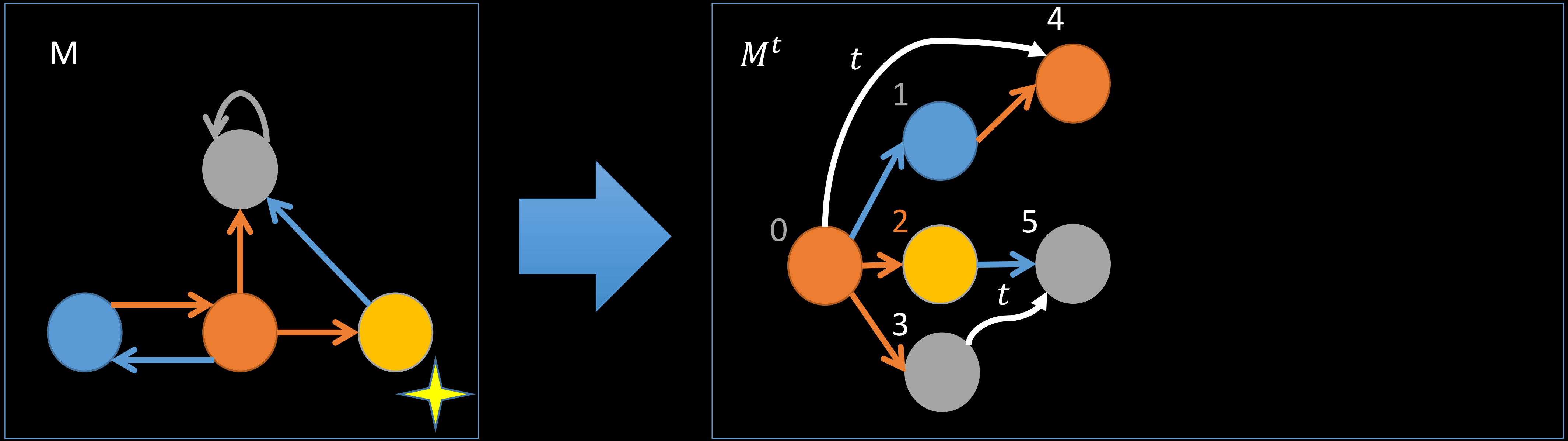
変換前同じだった点同士について
直近の古い点から新しい点に遷移 t を張る.





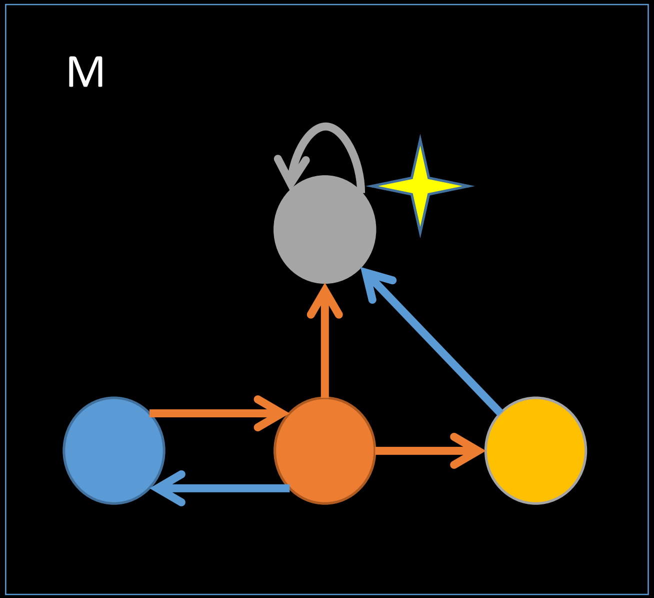
t^* unfolding

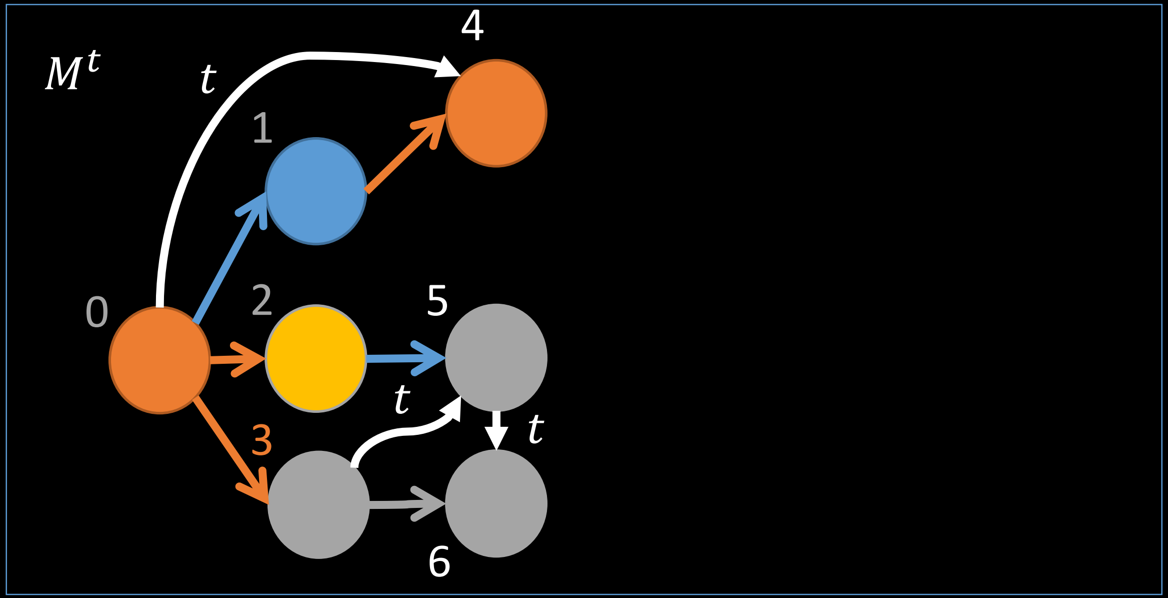
変換前同じだった点同士について
直近の古い点から新しい点に遷移 t を張る.



t^* unfolding

変換前同じだった点同士について
直近の古い点から新しい点に遷移 t を張る.





t^* unfolding

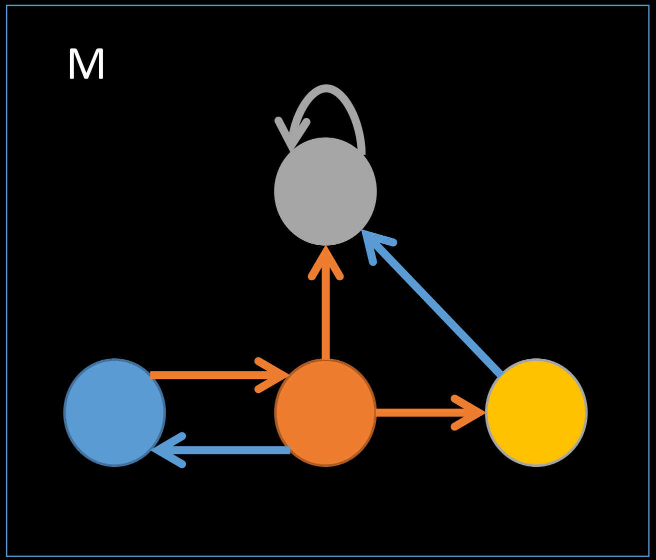
$f: S^t \to S$ … 変換後と変換前の点の対応を表す関数

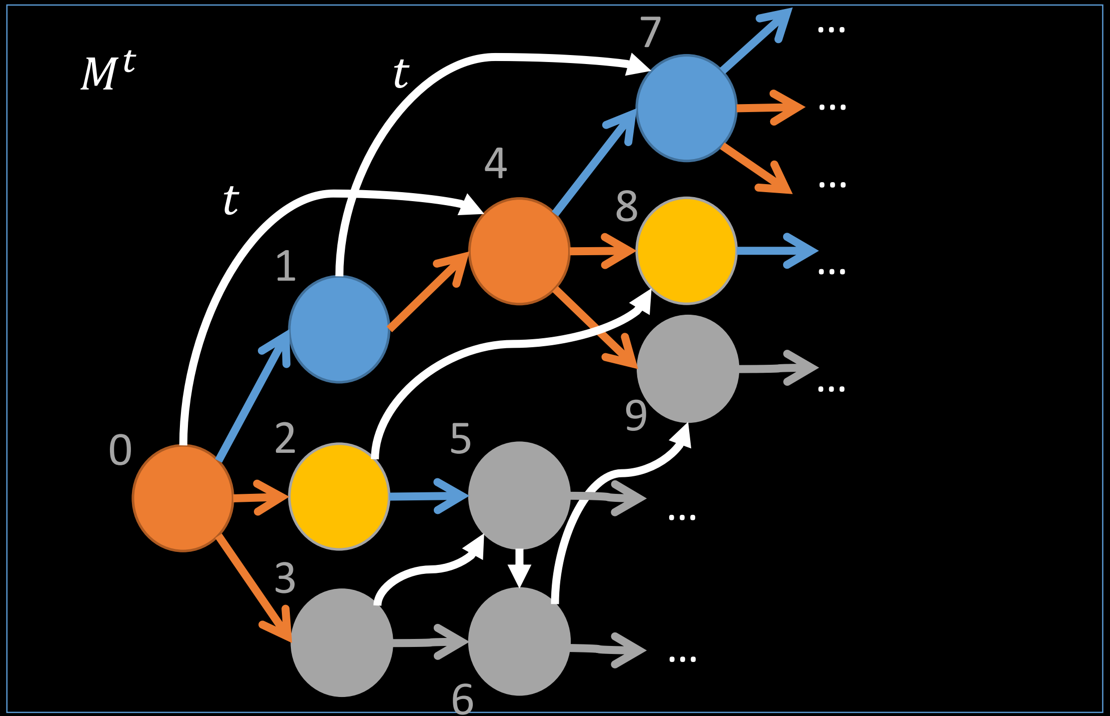
定理　M^tは、次の条件を満たす

(1) $u \xrightarrow{M^t, T(\alpha)} v \Rightarrow f(u) \xrightarrow{M,\alpha} f(v)$ (back)

(2) $\mathrm{f}(u) \xrightarrow{M,\alpha} f(v) \Rightarrow \exists v'. u \xrightarrow{M^t, T(\alpha)} v' \; (f(v') = f(v))$ (forth)

(3) $(M, f(u)) \vDash A \iff (M^t, u) \vDash T(A)$





t^* unfolding

(2) $f(u) \xrightarrow{M,\alpha} f(v) \Rightarrow \exists v'. u \xrightarrow{M^t, T(\alpha)} v'$ $(f(v') = f(v))$ (forth)

case : $\alpha \equiv \alpha \cap \beta$

$$f(u) \xrightarrow{M,\alpha\cap\beta} f(v) \Leftrightarrow f(u) \xrightarrow{M,\alpha} f(v) \text{ and } f(u) \xrightarrow{M,\beta} f(v)$$

$$\overset{I.H}{\Rightarrow} \exists v'. \exists v''. \left(u \xrightarrow{M^t, T(\alpha)} v' \text{ and } u \xrightarrow{M^t, T(\beta)} v''\right)$$

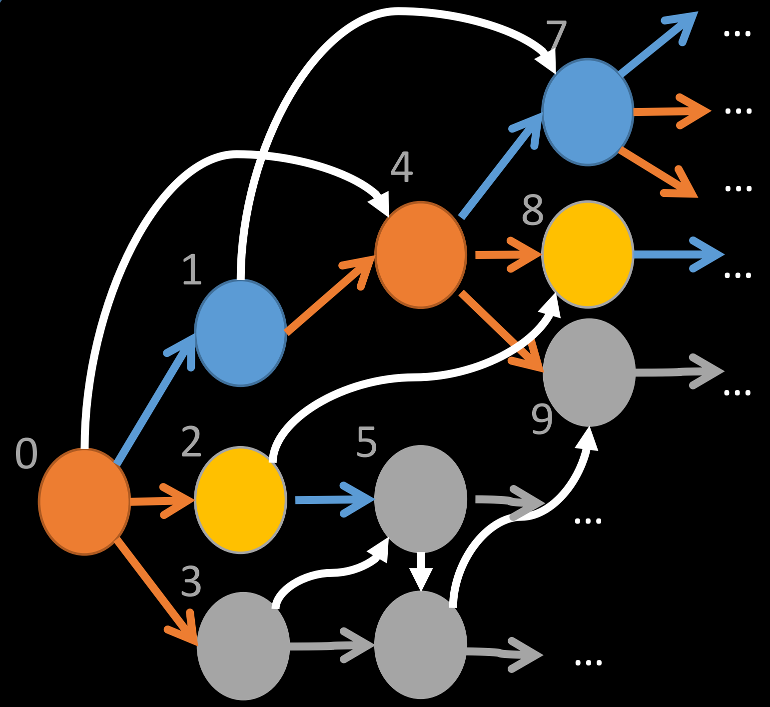
$$\overset{*}{\Rightarrow} \exists v''. \left(u \xrightarrow{M^t, T(\alpha); t^*} v'' \text{ and } u \xrightarrow{M^t, T(\beta)} v''\right)$$

$$\overset{\text{lem}}{\Longrightarrow} \exists v''. \left(u \xrightarrow{M^t, T(\alpha)} v'' \text{ and } u' \xrightarrow{M^t, T(\beta)} v''\right)$$

$$\overset{\cap \text{ def}}{\Longrightarrow} \exists v''. u \xrightarrow{M^t, T(\alpha)\cap T(\beta)} v''$$

$$\overset{\text{T def}}{\Longrightarrow} \exists v''. u \xrightarrow{M^t, T(\alpha\cap\beta)} v''$$

* 構成法から
$v' \xrightarrow{t^*} v''$ または $v'' \xrightarrow{t^*} v'$

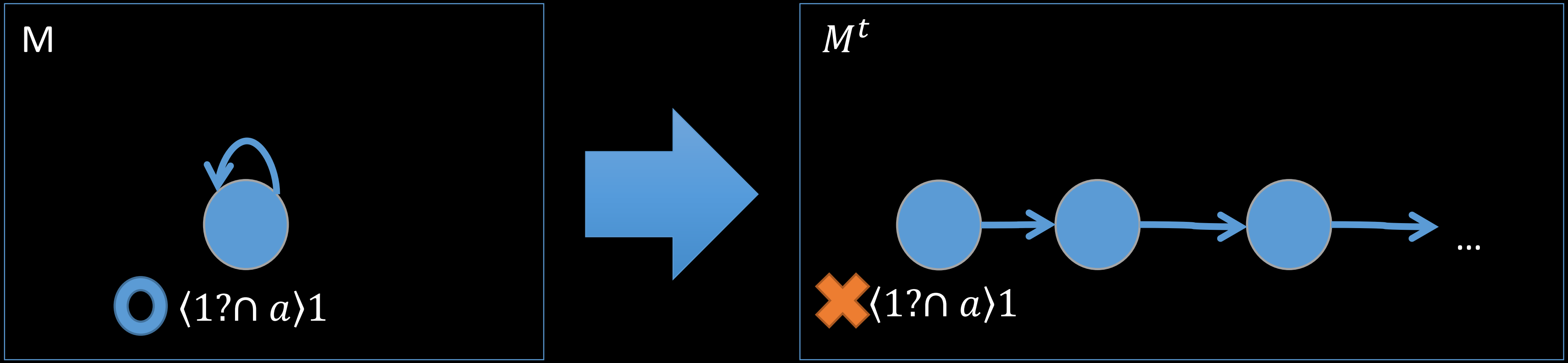


t^* unfolding

- t^* unfoldingでIPDLのモデルをdagモデルに変換出来る.

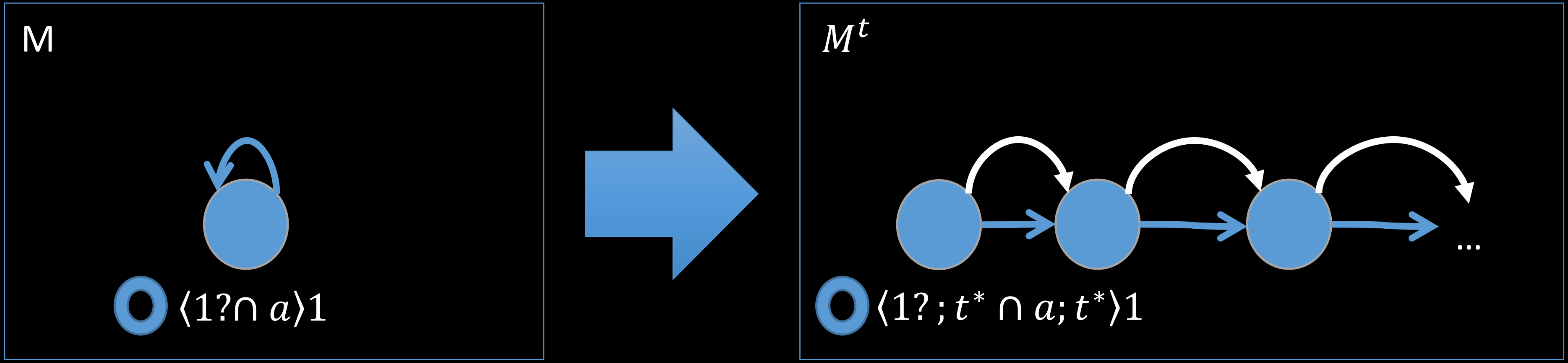
tree unfolding

NG



t^* unfolding

OK



IPHLの有限モデル性

定理　IPDL 論理式 $\langle\alpha\rangle 1$ について

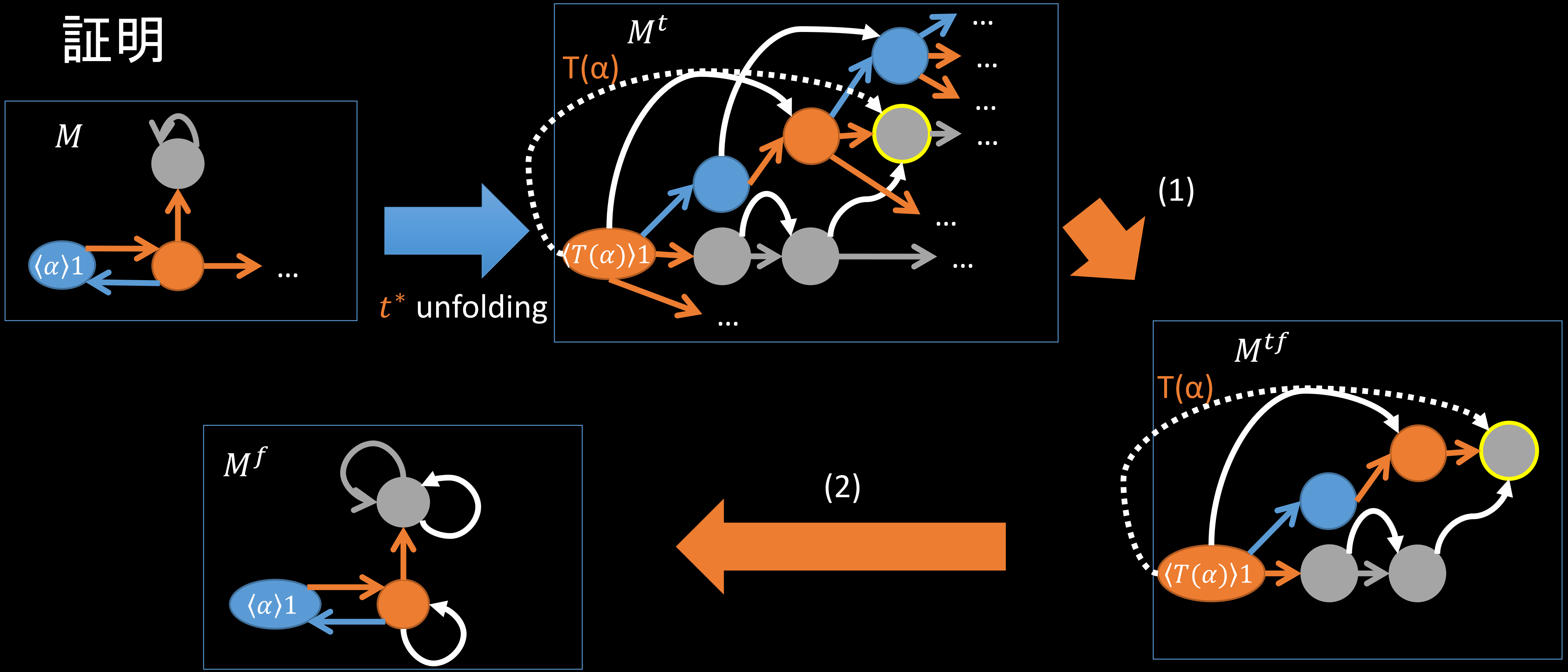
$\langle\alpha\rangle 1$ が充足可能⇒有限モデル上で $\langle\alpha\rangle 1$ が充足可能

注: IPHL 論理式 $\{\varphi_1\}\alpha\{\varphi_2\}$ が恒真 ⇔ IPDL 論理式 $\langle\varphi_1?;\alpha;\neg\varphi_2?\rangle 1$ が充足可能
これより $\langle\alpha\rangle 1$ の充足可能性を考える

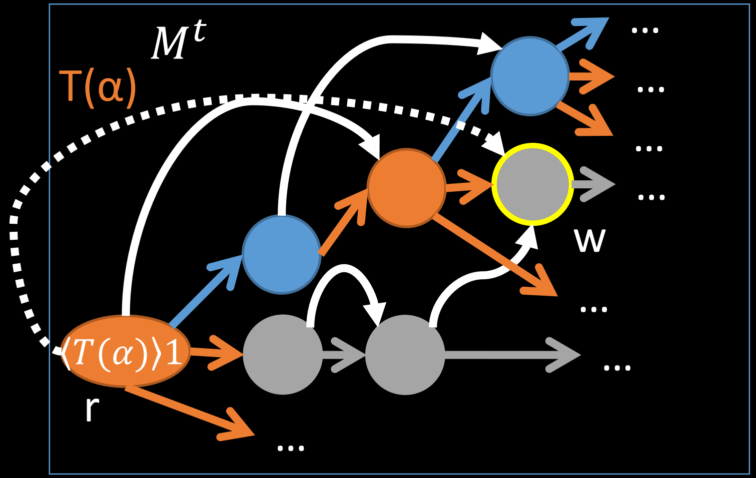
IPHLの有限モデル性

定理 $\langle\alpha\rangle 1$ が充足可能 ⇒ 有限モデル上で $\langle\alpha\rangle 1$ が充足可能

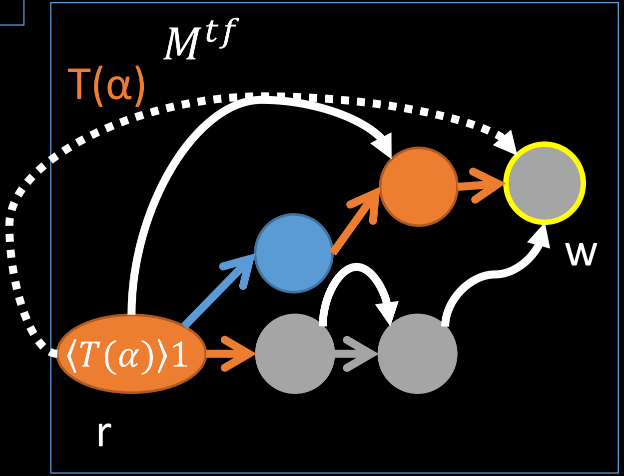
証明



IPHLの有限モデル性



(1)



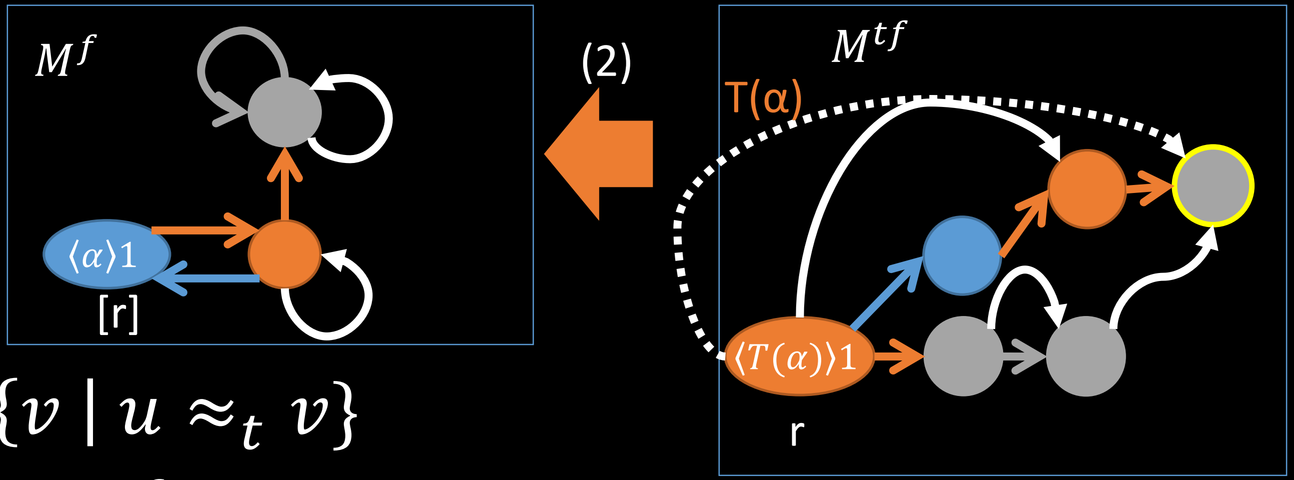
w … $T(\alpha)$のwitness

M^{tf} … $r \overset{-}{\rightarrow} x$ かつ $x \overset{-}{\rightarrow} w$を満たす$x$に制限した$M^t$

M^{tf}は、次を満たす

1. M^{tf}は有限
   - witnessの深さは有限
   - 各点の逆辺の数は有限
2. $(M^{tf}, \mathrm{r}) \vDash \langle T(\alpha)\rangle 1$

IPHLの有限モデル性



$$u \approx_t v \Leftrightarrow u \xrightarrow{(t \cup t^{-1})^*} v \qquad [u] = \{v \mid u \approx_t v\}$$

$$M^f = M^{tf}/\approx_t = (S^{tf}/\approx_t, R^{tf}/\approx_t, V^{tf}/\approx_t)$$

- $S^{tf}/\approx_t = \{[u] \mid u \in S^{tf}\}$
- $R^{tf}/\approx_t (a) = \{([u],[v]) \mid (u,v) \in R^{tf}(a)\}$
- $V^{tf}/\approx_t (p) = \{[u] \mid u \in V^{tf}(p)\}$

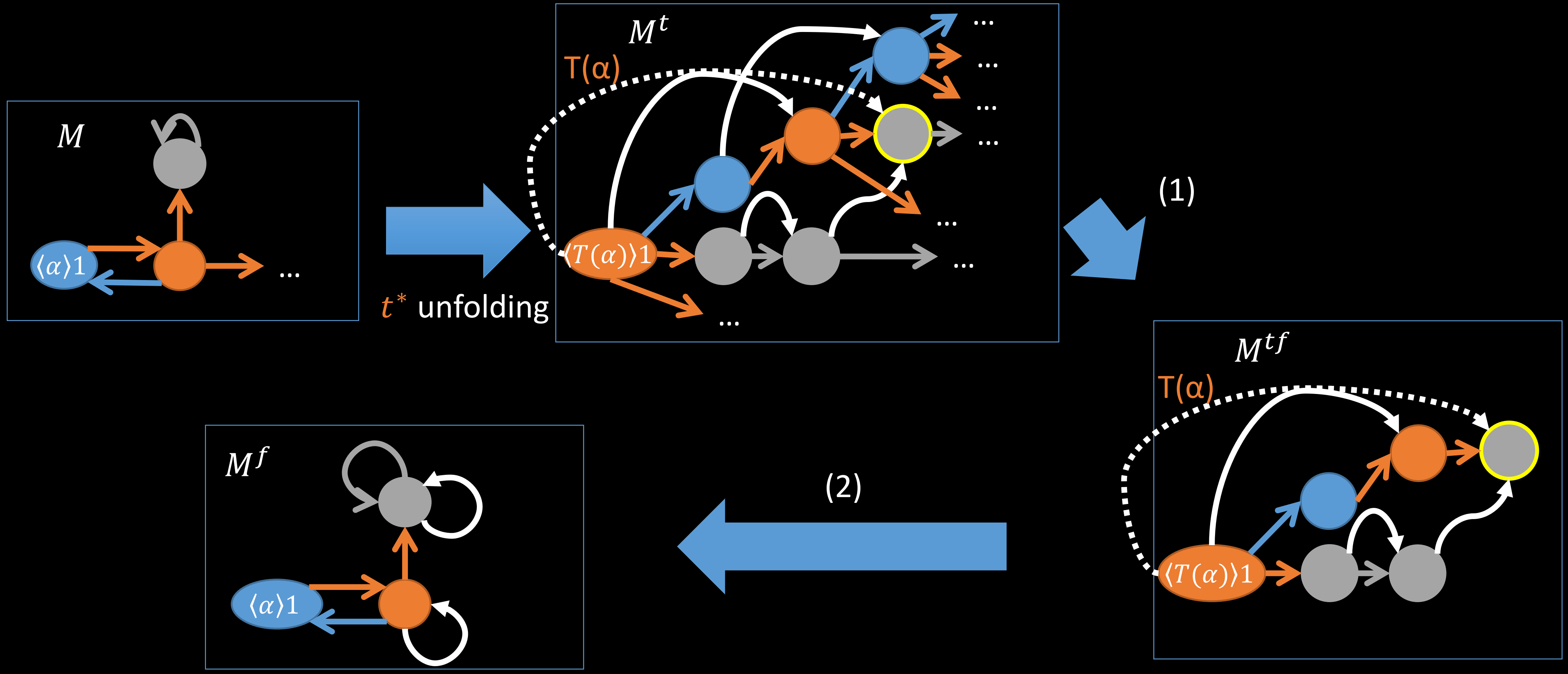
M^fは、次を満たす

1. M^fは、有限($\because M^{tf}$が有限)
2. $(M^f, [r]) \vDash \langle\alpha\rangle 1$

IPHLの有限モデル性

定理 $\langle\alpha\rangle 1$ が充足可能 ⇒ 有限モデル上で $\langle\alpha\rangle 1$ が充足可能

以上より、IPHLは有限モデル性を持つ



まとめ・今後の課題

- t^* unfolding : IPDLのモデルをdagモデルへ変換

	PHL	PDL	IPHL	IPDL
ツリーモデル性	○	○	×	×
有限モデル性	○	○ [Fischer,Ladner 1977]	○	×
充足可能性判定	PSPACE [Kozen 2000]	EXPTIME [Fischer,Ladner 1977]	EXPSPACE?	2-EXPTIME [M LANGE 2005]
公理化可能性	○ [Kozen 2000]	○ [Segerberg 1977]	○?	○ [Balbiani 2003]