BDDによる実装が可能な様相論理の充足可能性判定手続き

田辺良則（産総研/JST）　高橋孝一（産総研）
山本光晴（千葉大）　佐藤貴洋（東大）
戸沢晶彦（日本IBM）　萩谷昌己（東大）

PPL2005
2005年3月9日

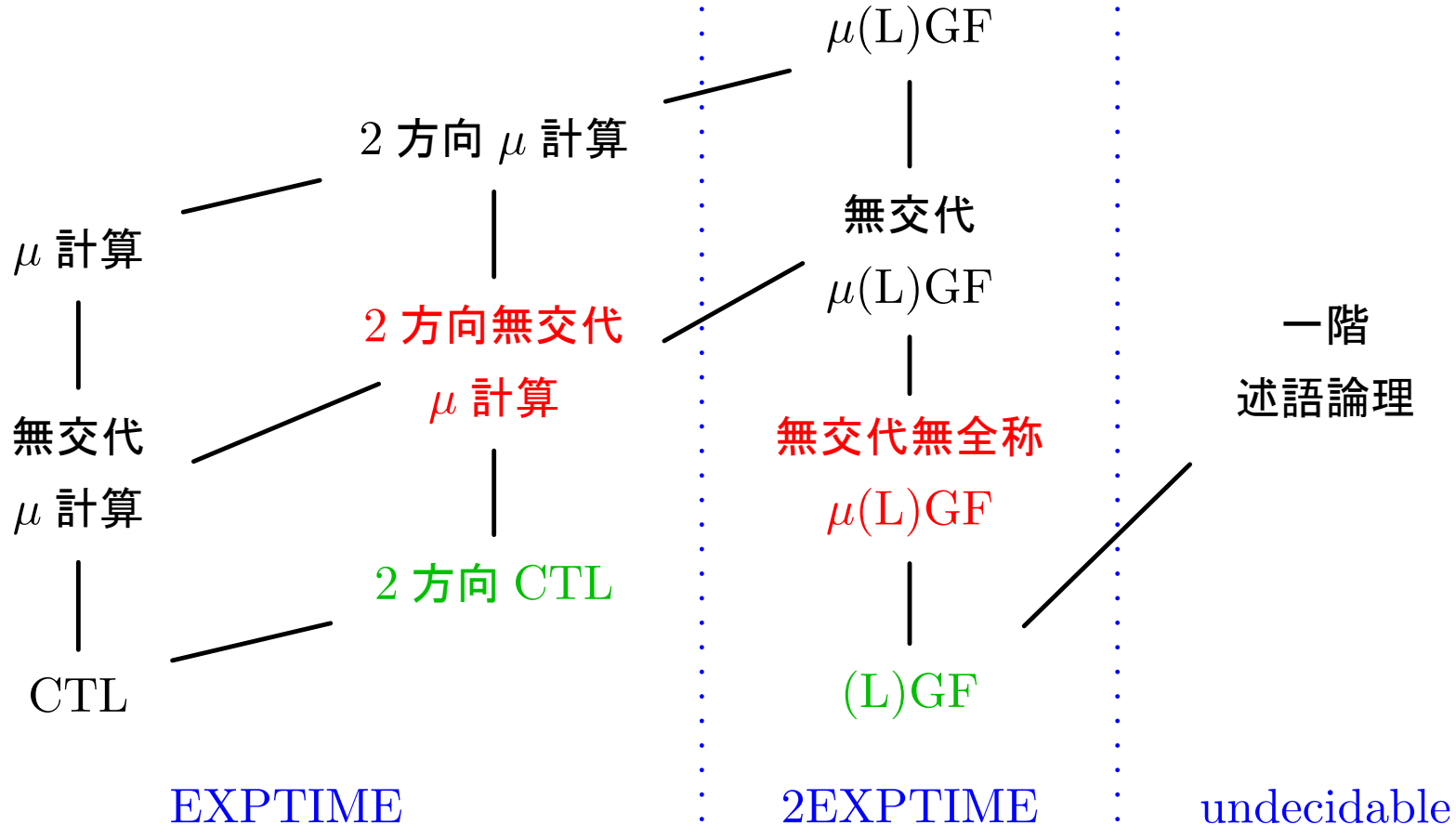
背景

- 論理式の充足可能性判定手続きの応用
  - 並行プログラムの合成
  - モデル検査における自動抽象化
- 時相論理式の充足可能性判定:
  グラフ書き換え系への応用
  - XML 文書の検証
  - セルオートマトンの解析
  - ヒープ構造の検証
- 2 方向の様相が必要

先行研究

- **対象の体系**: **ともに** 2 **方向の様相を持つ**.
  - 2 **方向** CTL
  - **一階述語論理の** (Loosely) Guarded Fragment
- **タブロー法による充足可能性判定手続き**
- BDD **による効率的な実装**

論理体系の関係


μ(L)GF
2 方向 μ 計算
無交代
μ(L)GF
μ 計算
2 方向無交代
μ 計算
一階
述語論理
無交代
μ 計算
無交代無全称
μ(L)GF
2 方向 CTL
CTL
(L)GF
EXPTIME
2EXPTIME
undecidable

概要

論理式の充足可能性判定手続き: 2 方向様相 μ 計算とその部分体系

体系	手法	実装
2 方向様相 μ 計算	Alternating Tree Automaton	報告なし
無交代 2 方向様相 μ 計算	タブロー法	BDD による効率的な実装 (?)
2 方向 CTL	タブロー法	BDD による効率的な実装

注: 問題の複雑さは，どれも EXPTIME 完全．

論理式の充足可能性判定手続き: **不動点つき** (μ) **一階述語論理の** (**弱**) **ガード付フラグメント** ((Loosely) Guarded Fragment) **とその部分体系**

体系	**手法**	**実装**
μ(L)GF	Alternating Tree Automaton	**報告なし**
無交代 μ(L)GF	??	??
無交代無全称 μ(L)GF	**タブロー法**	BDD **による効率的な実装** (?)
(L)GF	**タブロー法**	BDD **による効率的な実装**

注: **問題の複雑さは，どれも** 2EXPTIME **完全．**

２方向様相 μ 計算

- Prop: **命題変数の集合**
- Mod: **様相の集合**
  逆様相: $\overline{\ }$: Mod $\to$ Mod, $\overline{\overline{a}} = a$.
- L_μ: ２**方向様相** μ **計算** (two-way modal μ calculus) **論理式の集合**:
  - **命題変数** P**，その否定** $\neg P$**.**
  - **論理演算子** $\varphi_1 \vee \varphi_2$, $\varphi_1 \wedge \varphi_2$.
  - **演算子** $\langle a \rangle \varphi$, $[a]\varphi$ $\quad (a \in \mathrm{Mod})$.
  - **最小不動点演算子** $\mu X \varphi$, **最大不動点演算子** $\nu X \varphi$.
    ($X \in$ Prop. $\neg X$ **は** φ **に現れない.**)

無交代性

$\varphi \in L_\mu$ **が，無交代** (alternation-free) $\stackrel{\text{def}}{\Longleftrightarrow}$

- φ **の中の** μX **の内側の** νY **の内側に** X **は現れない．**
- φ **の中の** νX **の内側の** μY **の内側に** X **は現れない．**

例:

- $\mu X(\nu Y(P \wedge [a]Y \wedge [\overline{a}]X))$: NG.
- $\mu X(\nu Y(P \wedge [b]Y) \vee \langle a\rangle X \vee \langle\overline{a}\rangle X)$: OK.

下は，2 方向 CTL **論理式の** $\mathbf{E}_{a,\overline{a}}\mathbf{F}\ \mathbf{A}_b\mathbf{G}\ P$ **に相当する．**

無交代な L_μ **の論理式全体を** $\mathsf{L}_\mu^{\mathsf{af}}$ **と書く．**

意味論

Kripke **構造** $\mathcal{M} = (M, R, \lambda)$

- $a \in \mathsf{Mod}$ **に対して** $R(a) \subseteq M \times M$, $R(\overline{a}) = R(a)^{-1}$.
- $P \in \mathsf{Prop}$ **に対して** $\lambda(P) \subseteq M$.

$m \in M$ **に対して** $\mathcal{M}, m \models \varphi$ **を定義**

- $m \models P \iff m \in \lambda(P)$.
- $\neg$, $\wedge$, $\vee$ **は省略.**
- $m \models \langle a \rangle \varphi \iff m' \models \varphi$ for some $(m, m') \in R(a)$.
- $m \models [a] \varphi \iff m' \models \varphi$ for all $(m, m') \in R(a)$.
- $m \models \mu X \varphi \iff m \in \mathsf{lfp}(\varphi, X)$.
- $m \models \nu X \varphi \iff m \in \mathsf{gfp}(\varphi, X)$.

ただし，$\mathsf{lfp}(\varphi, X)$ **と** $\mathsf{gfp}(\varphi, X)$ **は，おのおの，**$S \subseteq M$ **に** $\{m \in M \mid \mathcal{M}[X \mapsto S], m \models \varphi\}$ **を対応させる関数（これは単調関数）の最小不動点と最大不動点．**

展開

μ, ν 演算子は,「展開定義」の導入とみなせる．ただし，μ の展開は有限回．ν の展開は無限回．

例: $\varphi = \mu X_1(\nu Y_1(P \wedge [b]Y_1) \vee \mu X_2(\langle a\rangle X_1 \wedge [c]X_2))$

$\Longrightarrow$

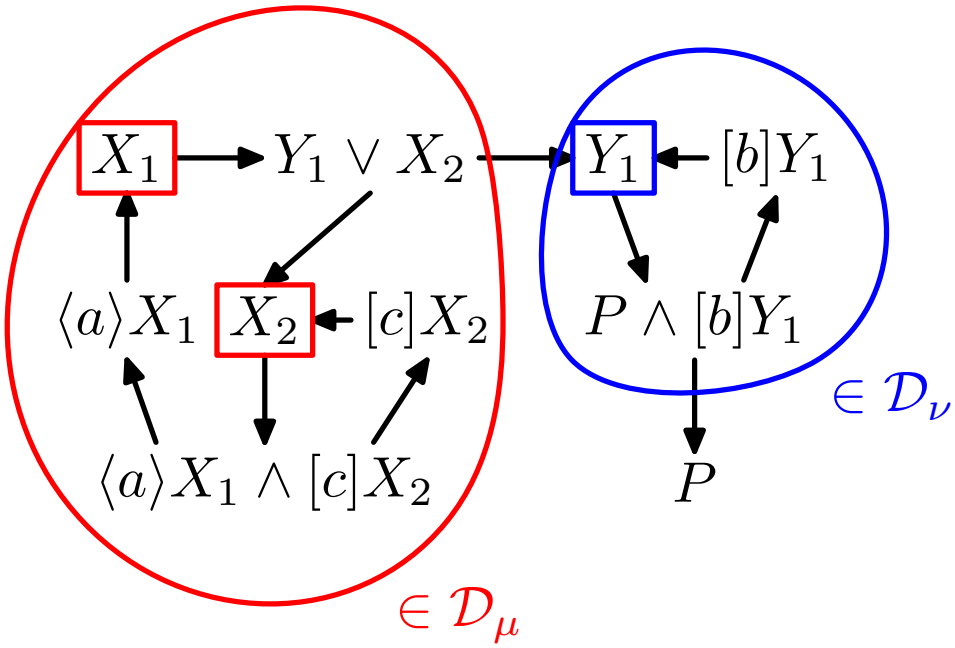
$\varphi = X_1$

ただし，

$X_1 =_\mu Y_1 \vee X_2,$

$Y_1 =_\nu P \wedge [b]Y_1,$

$X_2 =_\mu \langle a\rangle X_1 \wedge [c]X_2.$



展開定義: $X_1 =_\mu \xi_1, \ldots, X_k =_\mu \xi_k \ ; \ Y_1 =_\nu \eta_1, \ldots, Y_l =_\nu \eta_l$

関係 $\to_{\mathsf{e}}$:

$\varphi_1 \vee \varphi_2 \to_{\mathsf{e}} \varphi_i \ (i = 1, 2)$.　　$\varphi_1 \wedge \varphi_2 \to_{\mathsf{e}} \varphi_i \ (i = 1, 2)$.

$\langle a \rangle \varphi \to_{\mathsf{e}} \varphi$.　　$[a] \varphi \to_{\mathsf{e}} \varphi$.

$X_i \to_{\mathsf{e}} \xi_i \ (i = 1, \ldots, k)$　　$Y_i \to_{\mathsf{e}} \eta_i \ (i = 1, \ldots, l)$

φ **を含み，**$\to_{\mathsf{e}}$ **について閉じた最小の集合を** $\mathsf{Cl}(\varphi)$ **と書く．**

φ **が無交代** $\iff$ $\mathsf{Cl}(\varphi)$ **の** $\to_{\mathsf{e}}$ **に関する強連結成分で，**X_i **と** Y_j **の両方を含むものはない．**

X_i **を含む強連結成分の集合を** $\mathcal{D}_\mu$ **とする．**
Y_j **を含む強連結成分の集合を** $\mathcal{D}_\nu$ **とする．**

φ_{I} 型

$\varphi_{\mathrm{I}} \in \mathsf{L}_{\mu}^{\mathsf{af}}$ について，$\mathcal{M}, m \models \varphi_{\mathrm{I}}$ となる $\mathcal{M}, m$ が存在するかどうかを判定する手続きを与える．

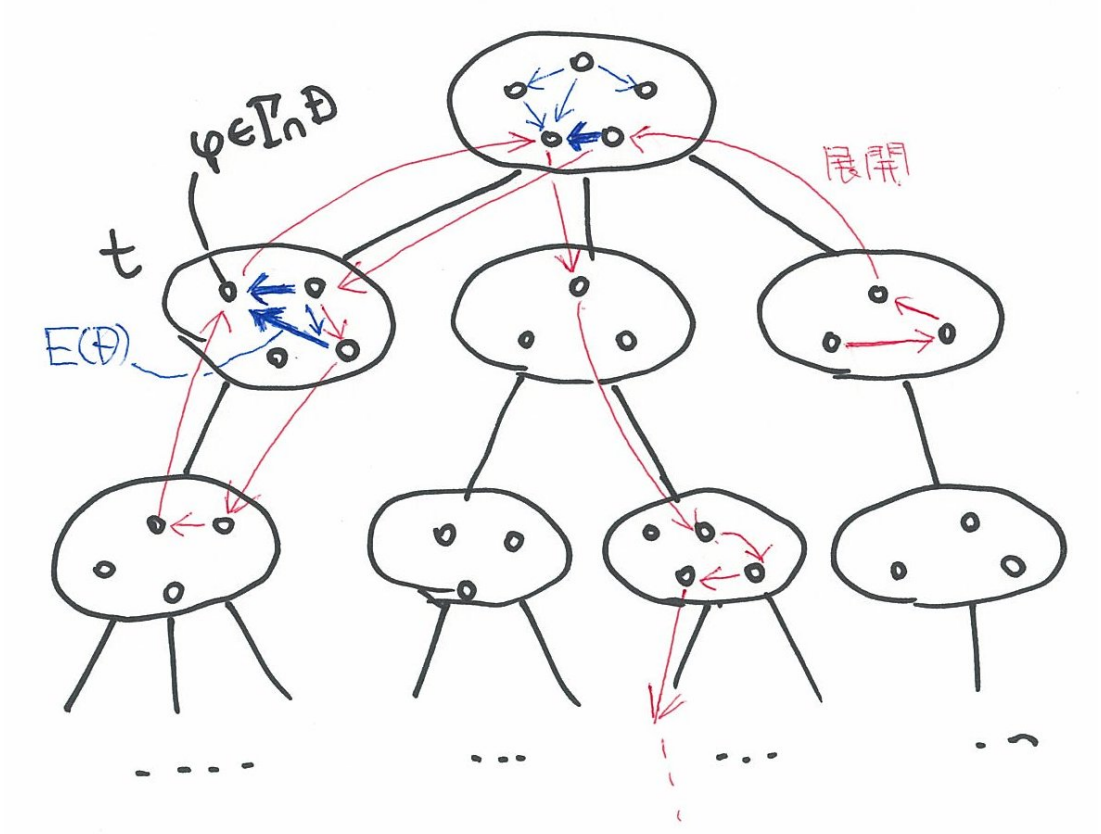
以下を満たす三つ組 $t = (\Gamma, E, f)$ を φ_{I} 型という．

- $\Gamma \subseteq \mathsf{cl}(\varphi_{\mathrm{I}})$.
- E は $\mathcal{D}_{\mu}$ 上の関数で，各 $D \in \mathcal{D}_{\mu}$ に対して $E(D)$ は D 上の非反射的，推移的 2 項関係．
- f は関数．定義域は，Γ の要素のうち $\varphi_1 \vee \varphi_2$ の形のもの．$f(\varphi_1 \vee \varphi_2) = \varphi_1$ または φ_2．

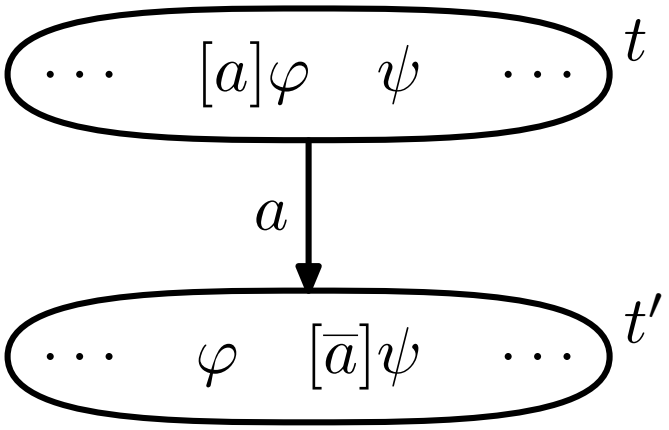
- $\varphi_1 \vee \varphi_2 \in \Gamma$ **ならば，** $f(\varphi_1 \vee \varphi_2) \in \Gamma$**．さらに** $f(\varphi_1 \vee \varphi_2) \in D \in \mathcal{D}_\mu$ **ならば，** $(\varphi_1 \vee \varphi_2, f(\varphi_1 \vee \varphi_2)) \in E(D)$**．**
- $\varphi_1 \wedge \varphi_2 \in \Gamma$ **ならば，** $\varphi_j \in \Gamma \quad (j = 1, 2)$**．さらに，** $\varphi_j \in D \in \mathcal{D}_\mu$ **ならば，** $(\varphi_1 \wedge \varphi_2, \varphi_j) \in E(D) \quad (j = 1, 2)$**．**
- $X_i \in \Gamma$ **ならば，** $\xi_i \in \Gamma$**．さらに，** $X_i \in D \in \mathcal{D}_\mu$ **ならば，** $(X_i, \xi_i) \in E(D)$**．**
- $Y_i \in \Gamma$ **ならば，** $\eta_i \in \Gamma$**．**

充足可能性判定手続き：方針

- 2 方向様相 μ 計算は，木モデル性を持つ．
- φ_{I} 型が，木の形状に並べられるかどうかを調べる．



- **隣り合う** $(t \to_a t')$ **条件**
  - $[a]\varphi \in \Gamma$
    $\Longrightarrow\ \varphi \in \Gamma'$
  - $[\overline{a}]\varphi \in \Gamma'$
    $\Longrightarrow\ \varphi \in \Gamma$

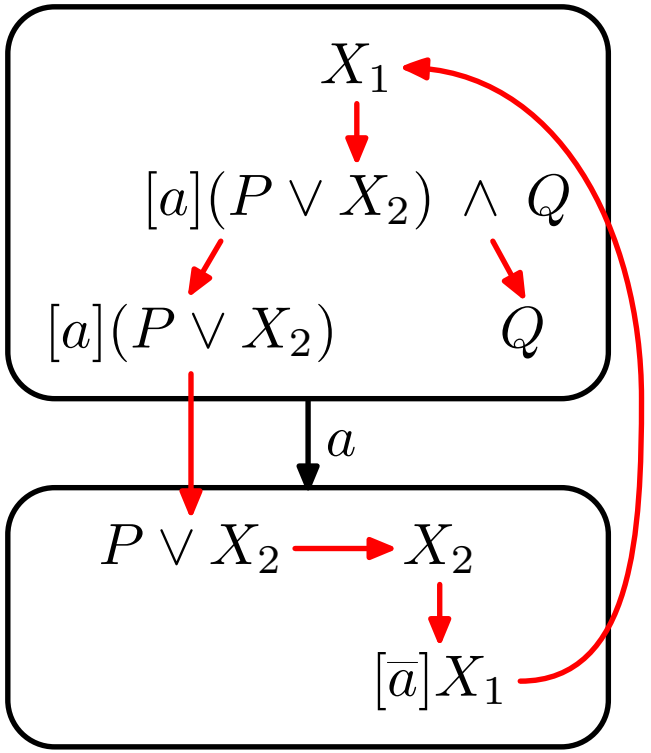


- **木のノードになり得ないものを排除していく．**
  - $P, \neg P \in \Gamma$ **(矛盾)**
  - $\langle a\rangle\varphi \in \Gamma$ **なのに，**
    $t \to_a t'$ **で** $\varphi \in \Gamma'$ **となるものが ない．(**$\Diamond$ **矛盾)**
  - $\varphi \in D \in \mathcal{D}_\mu$ **なのに，**
    φ **の展開が有限回で終わらない．(**μ **矛盾)**

展開の有限性

$\varphi \in D \in \mathcal{D}_\mu$,
$t = (\Gamma, E, f)$: φ_{I} 型.
$(\varphi, t) \in D$ の「1 回の展開」:

- $\varphi = \varphi_1 \vee \varphi_2$ のとき,
  $(f(\varphi), t)$.
- $\varphi = \varphi_1 \wedge \varphi_2$ のとき,
  (φ_1, t) および (φ_2, t).
- $\varphi = X_i$ のとき, (ξ_i, t).
- $\varphi = \langle a \rangle \psi$ または $\varphi = [a]\psi$
  のとき, $t \to_a t'$ または
  $t' \to_{\overline{a}} t$ なる t' に対して,
  (ψ, t').



$\varphi \in D$ の展開の列が

- $\varphi_1 \wedge \varphi_2$ と $[a]$ のときには，どのように展開を選んでも，
- $\langle a \rangle$ のときには，うまく展開を選べば，

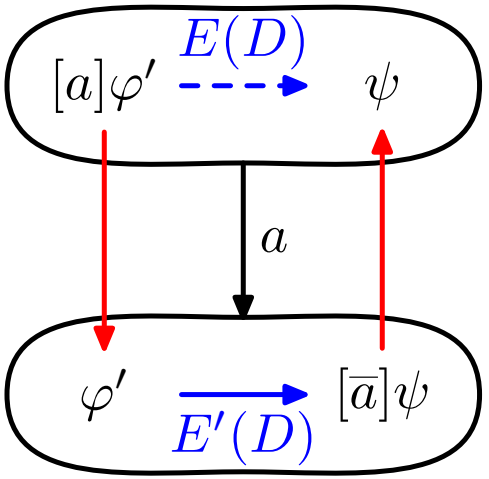
有限となるようにしたい．そのために，

- ループを起こさない．— E を使う．
- 枝を下に伸びる無限の展開がないようにする．

ループの排除

- $(\varphi, \psi) \in E(D)$
  $\Longleftrightarrow$ 「φ を展開して ψ にすることを許す」
- $E(D)$ は 推移的 非反射的.
- φ_{I} 型が隣接する $(t \to_a t')$ 条件を追加:
  $[a]\varphi', \psi \in D \cap \Gamma$, $\varphi', [\overline{a}]\psi \in D \cap \Gamma'$ とするとき,

- $(\varphi', [\overline{a}]\psi) \in \overline{E'(D)}$
  $\Longrightarrow$ $([a]\varphi', \psi) \in \overline{E(D)}$
- $(\psi, [a]\varphi') \in \overline{E(D)}$
  $\Longrightarrow$ $([\overline{a}]\psi, \varphi') \in \overline{E'(D)}$



ただし, $\overline{E(D)} = E(D) \cup \{(\varphi, \varphi) \mid \varphi \in D\}$

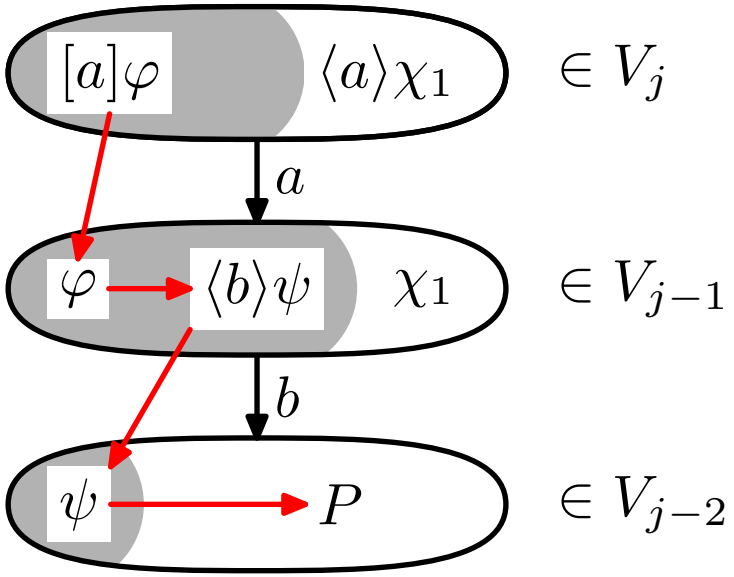
下方への展開

T: φ_{I} 型の集合，$t = (\Gamma, E, f) \in T$
$S \subseteq \Gamma \cap D$: $\vee, \wedge, X_i$ の展開について閉じている．

(t, S) たちの集合 $V_0 \subseteq V_1 \subseteq \ldots$ を作る．

$(t, S) \in V_j$ の気持ち:「各 $\varphi \in S$ について，(φ, t) の展開で，$[a]$ と $\langle a \rangle$ はたかだか j 回しか現れない．」

- $(t, S) \in V_0 \iff S = \varnothing$
- $(t, S) \in V_{j+1} \iff$
  各 $\chi = \langle a \rangle \chi' \in \Gamma$ **に対して** $(t', S') \in V_j$, $t \to_a t'$ **なる** t' **があって，**
  - $\varphi = [a]\varphi' \in S \implies \varphi' \in S'$.
  - $\chi \in S \implies \chi' \in S'$.



$(V_j \mid j < \omega)$ **は，有限集合** $T \times \mathscr{P}(\mathsf{Cl}(\varphi_{\mathrm{I}}))$ **の部分集合の包含関係に関する上昇列なので，どこか** J **で止まる．**

t **が** μ **無矛盾** $\overset{\mathsf{def}}{\iff} (t, \Gamma \cap D) \in V_J$

充足可能性判定手続き

- $T_0 = \{t \mid t$ は矛盾しない φ_I 型 $\}$.
- $T_{k+1} = \{t \in T_k \mid t$ は T_k で $\Diamond$ 無矛盾かつ μ 無矛盾 $\}$.

$(T_k \mid k < \omega)$ は，有限集合の，包含関係に関する下降列なので，どこか K で止まる．

φ_{I} が充足可能

$\Longleftrightarrow$ $\varphi_{\mathrm{I}} \in \Gamma$ なる $t = (\Gamma, E, f) \in T_K$ が存在する．

この判定手続きの計算量は EXPTIME．なお，充足可能性問題の複雑さは，EXPTIME 完全である．

GF

Var: (**一階の**) **変数の集合**

PS: **二階の変数** (i.e. **述語記号**) **の集合**

GF: **一階述語論理のガード付きフラグメント** (Guarded Fragment)

- **限量子は，常に** $\exists\vec{x}(\alpha \wedge \varphi)$, $\forall\vec{x}(\alpha \to \varphi)$ **の形．**
  これらを $\exists\vec{x}{:}\alpha.\,\varphi$, $\forall\vec{x}{:}\alpha.\,\varphi$ **と書く．** α **をガードという．**
- α **は原子論理式 (述語記号の後ろに変数を並べたもの)**
- $\mathrm{free}(\varphi) \subseteq \mathrm{free}(\alpha)$, $\vec{x} \subseteq \mathrm{free}(\alpha)$

例: (P,Q,R,S **は述語記号．**)

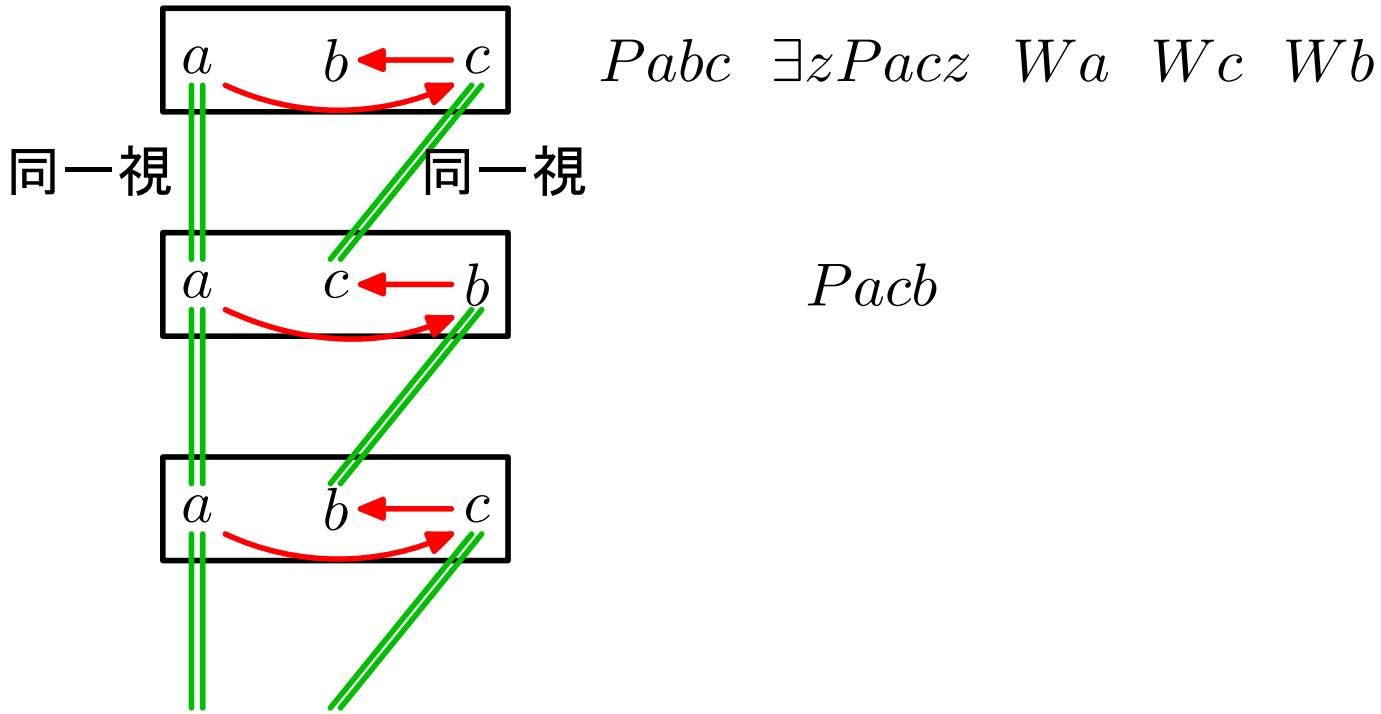
- $\exists x : Px.\ \forall yz : Qxyz.\ Rxz$: OK
- $\exists x : \neg Px.\ \forall yz : Qxyz.\ Rxz$: NG
- $\exists x : Px.\ \forall yz : (Qxyz \wedge Sxyz).\ Rxz$: NG
- $\exists x : Px.\ \forall yz : Qyz.\ Rxz$: NG
- $\exists xy : Px.\ \forall z : Qxyz.\ Rxz$: NG

μGF

- GF に不動点演算子が入る．
- 例
  - (標準書式): $(\mathsf{LFP}_{W,w}(Pw \vee \exists y\colon Rwy.\, Wy)))(x)$
  - (展開書式): Wx,
    where $Ww =_{\mathsf{LFP}} Pw \vee \exists y\colon Rwy.\, Wy$
  - これは，様相 μ 計算の $\mu X(P \vee \langle r \rangle X)$ に相当．
- W は，ガードには使えない．
- 2 方向様相 μ 計算論理式は，μGF 論理式に翻訳可能．
  ($r \in \mathsf{Mod}$ を Rxy で表現したとき，$\overline{r}$ は，Ryx で表現される．)
- 様相 μ 計算と同様に，「無交代」が定義される．

拡張木モデル性

例: $(\forall xyw : Pxyw.\, \exists z : Pxwz.\, \top) \wedge (\exists xyz : Pxyz.\, Wx)$,
where $Ww =_{\mathsf{LFP}} (\forall yz : Pwyz.\, Wz) \wedge (\forall xy : Pxyw.\, Wy)$



充足可能性決定手続き？

無交代 μGF でも無交代様相 μ 計算と同様に充足可能性が判定できるか?

$\Longrightarrow$ うまくいかない．

- 様相 μ 計算: $\mu X\varphi$ が成り立つ証拠 (witness) が，有限木になる．
- μGF: $\mathsf{LFP}_{W,w}\varphi$ が成り立つ証拠が，無限木になることがある．

全称記号 $\forall$ が，$\mathsf{LFP}_{W,w}$ の内側に現れなければ，成り立つ証拠は，有限木になる．

$\Longrightarrow$ 無交代様相 μ 計算と同様に充足可能性が判定できる．

BDD による実装

- 充足可能性決定手続きは，集合演算のみでできている．
- two-way CTL と同様に BDD による実装が可能と考えられる．
- 部分的な実装例 1：無交代様相 μ 計算充足可能性判定の変形：有限 2 分木モデルの存在判定
- 部分的な実装例 2：無全称無交代 μGF 充足可能性判定の小さなプロトタイプ：LFP 展開式を 1 つに固定して実装．

実装例 1:

論理記号数	610	1806	817	4141	4141
BDD **ノード数**	322	2164	774	4626	30523
実行時間 (ミリ秒)	20	1036	88	120	784

実装例 2:

n	5	10	15
BDD **ノード数**	27872	83499	205079
実行時間 (ミリ秒)	1382	4557	19428

まとめ

BDD による実装が可能になる，タブロー法による充足可能性判定手続きを，以下の体系について与えた．

- 無交代 2 方向様相 μ 計算
- 無交代無全称 μLGF

課題:

- 本アルゴリズムの実装
- 効率の良い実装のための，アルゴリズムの改良．
  - ループ排除の効率化，など
- 「無全称」の制限を外した，無交代 μLGF の充足可能性判定手続きの考案．