Indecibilidade da lógica de predicados

- Em lógica proposicional podemos (teoricamente) decidir se vale $\models \phi$: se ϕ possui n átomos proposicionais sua tabela verdade possui 2^n linhas. A coluna de ϕ possui apenas T sse $\models \phi$ vale.

- Em lógica de predicados isso não é possível

- O problema de determinar se uma fórmula de lógica de predicados vale é conhecido como um problema de decisão

→ O PROBLEMA DE DETERMINAR SE UMA FÓRMULA DE LÓGICA DE PREDICADOS VALE É CONHECIDO COMO UM PROBLEMA DE DECISÃO

- UMA SOLUÇÃO PARA UM PROBLEMA DE DECISÃO É UM ALGORITMO (ESCRITO EM C, JAVA, PYTHON, OU QUALQUER LINGUAGEM COMUM) QUE RECEBE INSTÂNCIAS DO PROBLEMA NA ENTRADA (→ INPUT) E SEMPRE TERMINA, PRODUZINDO UM "SIM" OU "NÃO" CORRETAMENTE COMO SAÍDA. (→ OUTPUT)

- NO CASO DO PROBLEMA DE DECISÃO PARA LÓGICA DE PREDICADOS O INPUT É UMA FÓRMULA ϕ ARBITRÁRIA DE LÓGICA DE PREDICADOS E O PROGRAMA ESTÁ CORRETO SE PRODUZ "SIM" SEMPRE QUE ϕ É VÁLIDA E "NÃO" CASO CONTRÁRIO.

- O PROGRAMA DEVE TERMINAR PARA TODA FÓRMULA.

- NÃO É PERMITIDO UM PROGRAMA QUE FIQUE "PENSANDO" PARA SEMPRE

FORMALMENTE

<u>VALIDADE EM LÓGICA DE PREDICADOS</u>: DADA UMA FÓRMULA ϕ DE LÓGICA DE PREDICADOS, VALE OU NÃO $\models \phi$?

→ VAMOS MOSTRAR QUE ESTE PROBLEMA NÃO É SOLÚVEL: NÃO É POSSÍVEL ESCREVER UM ALGORITMO QUE FUNCIONE PARA TODOS ϕ.

→ NATURALMENTE, HÁ INSTÂNCIAS FÁCEIS DE RESOLVER

→ A PRINCÍPIO, TODO ϕ PODE SER CHECADA: EXISTE UM CERTIFICADO QUE GARANTE QUE A RESPOSTA É "SIM" OU "NÃO", MAS NÃO É POSSÍVEL CRIAR UM MÉTODO MECÂNICO PARA DETERMINAR.

→ VAMOS PROVAR ISSO POR UMA TÉCNICA CONHECIDA COMO

REDUÇÃO DE PROBLEMAS

- PEGAMOS OUTRO PROBLEMA QUE SABEMOS SER INSOLÚVEL
- E MOSTRAMOS QUE A SOLUBILIDADE DO NOSSO PROBLEMA IMPLICA NA SOLUBILIDADE DO OUTRO.

O PROBLEMA DE POS-CORRESPONDÊNCIA: DADA UMA SEQUÊNCIA FINITA DE PARES $(s_1,t_1),(s_2,t_2),\dots,(s_k,t_k)$ T.Q. s_i E t_i SÃO SEQUÊNCIAS BINÁRIAS, EXISTE UMA SEQUÊNCIA DE ÍNDICES $i_1,\dots,i_m$ COM $m \geq 1$ T.Q.

$$s_{i_1} s_{i_2} \cdots s_{i_m} = t_{i_1} t_{i_2} \cdots t_{i_m} \; ?$$

EX: $C = \big((\underset{s_1}{1}, \underset{t_1}{101}), (\underset{s_2}{10}, \underset{t_2}{00}), (\underset{s_3}{011}, \underset{t_3}{11}) \big)$

$(2,3)$ $\quad s_2 s_3 = 10\,011$

$\qquad\quad t_2 t_3 = 00\,11$

$(1,3,2,3)$ $\quad s_1 s_3 s_2 s_3 = 1\,011\,10\,011 =$

SOLUÇÃO $\quad t_1 t_3 t_2 t_3 = 101\,11\,00\,11$

EX: $C = ((011,0),(01,011),(01,101),(10,001))$

TEOREMA: O PROBLEMA DE DECISÃO DE VALIDADE DE LÓGICA DE PREDICADOS É INDECIDÍVEL: NÃO EXISTE PROGRAMA QUE, DADO ϕ, DECIDE SE $\models \phi$.

PROVA: DADO UMA INSTÂNCIA DO PROBLEMA DE PÓS-CORRESPONDÊNCIA

$$C = \begin{matrix} s_1 & s_2 & \cdots & s_k \\ t_1 & t_2 & & t_k \end{matrix}$$

VAMOS CONSTRUIR UMA FÓRMULA ϕ DE LÓGICA DE PREDICADOS T.Q. $\models \phi$ SSE C TEM UMA SOLUÇÃO ("SIM" $\Leftrightarrow$ "SIM")

FUNÇÕES: CONSTANTE e, E FUNÇÕES UNÁRIAS f_0 E f_1

- e É A PALAVRA VAZIA
- f_0 E f_1 SÃO AS FUNÇÕES DE CONCATENAÇÃO DE 0 E 1, RESP.

$$f_0(s) = s0 \quad \text{E} \quad f_1(s) = s1$$

- SE $b_1 b_2 \cdots b_l$ É UMA SEQ. BINÁRIA, ESCREVEMOS $f_{b_1 b_2 \cdots b_l}(e)$ PARA DENOTAR $f_{b_l}(f_{b_{l-1}}(\cdots f_{b_2}(f_{b_1}(e))))$

PREDICADO BINÁRIO P

$P(s,t)$ é "EXISTE SEQ. DE ÍNDICES $(i_1, \dots, i_m)$ T.Q. s é o TERMO $s_{i_1} \cdots s_{i_m}$ E t é o TERMO $t_{i_1} \cdots t_{i_m}$"

ϕ é DA FORMA $\phi_1 \wedge \phi_2 \to \phi_3$

$$P(f_{s_1}(e), f_{t_1}(e)) \wedge P(f_{s_2}(e), f_{t_2}(e)) \wedge \dots \wedge P(f_{s_k}(e), f_{t_k}(e))$$

$$\phi_1 = \bigwedge_{i=1}^{k} P\left(f_{s_i}(e), f_{t_i}(e)\right)$$

$$\phi_2 = \forall v \forall w \left(P(v,w) \to \bigwedge_{i=1}^{k} P\left(f_{s_i}(v), f_{t_i}(w)\right)\right)$$

$$\phi_3 = \exists z P(z,z)$$

$$C = \begin{matrix} s_1 & s_2 & \dots & s_k \\ t_1 & t_2 & & t_k \end{matrix}$$

→ AFIRMAMOS QUE $\models \phi$ SSE C TEM SOLUÇÃO

SUPONHA QUE $\models \phi$ VALE. VAMOS ENCONTRAR UM MODELO QUE NOS DIZ QUE C TEM SOLUÇÃO.

- A É O CONJUNTO DE TODAS STRING BINÁRIOS FINITAS
- A INTERPRETAÇÃO $e^{\mathcal{M}}$ DE e É ϵ (PALAVRA VAZIA)
- A INTERPRETAÇÃO DE f_0 É A FUNÇÃO UNÁRIA $f_0^{\mathcal{M}}$ T.Q. $f_0^{\mathcal{M}}(s) = s0$
- A INTERPRETAÇÃO DE f_1 É A FUNÇÃO UNÁRIA $f_1^{\mathcal{M}}$ T.Q. $f_1^{\mathcal{M}}(s) = s1$
- A INTERPRETAÇÃO DE P É

$$P^{\mathcal{M}} = \{ (s,t) : \text{EXISTE SEQ. DE ÍNDICES } (i_1, \dots, i_m) \text{ T.Q. } s \text{ É } s_{i_1} \cdots s_{i_m} \text{ E } t \text{ É } t_{i_1} \cdots t_{i_m} \}$$

$\rightarrow$ COMO $\models \phi$ VALE, TEMOS $\mathcal{M} \models \phi$

$$\phi_1 \wedge \phi_2 \rightarrow \phi_3$$

$$\phi_1 = \bigwedge_{i=1}^{k} P(f_{s_i}(e), f_{t_i}(e))$$

$$\phi_2 = \forall v \forall w \left(P(v,w) \rightarrow \bigwedge_{i=1}^{k} P(f_{s_i}(v), f_{t_i}(w))\right)$$

$$\phi_3 = \exists z P(z,z)$$

→ COMO $\models \phi$ VALE, TEMOS $M \models \phi$

NOTE PELA DEFINIÇÃO DE P^M, TEMOS $(s_i, t_i) \in P^M$ PARA TODO i

COMO $s_i = f_{s_i}^M(\epsilon) = f_{s_i}^M(e^M)$,
$t_i = f_{t_i}^M(\epsilon) = f_{t_i}^M(e^M)$ TEMOS $M \models P(f_{s_i}(e), f_{t_i}(e))$ PARA TODO i

$M \models \bigwedge_{i=1}^{k} P(f_{s_i}(e), f_{t_i}(e)) = \phi_1$

AFIRMAMOS QUE $M \models \phi_2$. DIZ QUE SEMPRE QUE $(s,t) \in P^M$, TEMOS $(ss_i, tt_i) \in P^M$ PARA TODO i

→ ISSO É CLARO: SE $(s,t) \in P^M$, EXISTE $i_1, \dots, i_m$ T.Q. s É $s_{i_1} \cdots s_{i_m}$ E t É $t_{i_1} \cdots t_{i_m}$, MAS $i_1, \dots, i_m, i$ É T.Q. ss_i $s_{i_1} \cdots s_{i_m} s_i$ E tt_i É $t_{i_1} \cdots t_{i_m} t_i$ PARA TODO i.

$P^M = \{(s,t)$: EXISTE SEQ. DE ÍNDICES $(i_1, \dots, i_m)$ T.Q. s É $s_{i_1} \cdots s_{i_m}$ E t É $t_{i_1} \cdots t_{i_m}\}$

$\phi_1 \wedge \phi_2 \to \phi_3$

$\phi_1 = \bigwedge_{i=1}^{k} P(f_{s_i}(e), f_{t_i}(e))$

$\phi_2 = \forall v \forall w \left(P(v,w) \to \bigwedge_{i=1}^{k} P(f_{s_i}(v), f_{t_i}(w))\right)$

$\phi_3 = \exists z P(z,z)$

COMO $M \models \phi_1$ E $M \models \phi_2$, TEMOS $M \models \phi_1 \wedge \phi_2$

E COMO $M \models \underbrace{\phi_1 \wedge \phi_2 \rightarrow \phi_3}_{\phi}$, ENTÃO $M \models \phi_3$

OU SEJA $M \models \exists z\, P(z,z)$

$P^M = \{(s,t)$: EXISTE SEQ. DE ÍNDICES $(i_1, \ldots, i_m)$ T.Q. s É $s_{i_1} \cdots s_{i_m}$ E t É $t_{i_1} \cdots t_{i_m}\}$

PELA DEFINIÇÃO DE P^M, HÁ SOLUÇÃO PARA C.

VOLTA: VAMOS MOSTRAR QUE SE C TEM SOLUÇÃO, ENTÃO $\models \phi$ VALE

SUPONHA QUE C POSSUI SOLUÇÃO, DIGAMOS $(i_1, \ldots, i_m)$

→ TEMOS QUE MOSTRAR QUE TODO MODELO M' QUE POSSUI CONSTANTE $e^{M'}$, FUNÇÕES UNÁRIAS $f_0^{M'}$ E $f_1^{M'}$, E PREDICADO BINÁRIO $P^{M'}$ SATISFAZ ϕ.

→ PELA DEFINIÇÃO DE $\rightarrow$, SE $M' \not\models \phi_1$ OU $M' \not\models \phi_2$,

ENTÃO $M' \models \underbrace{(\phi_1 \wedge \phi_2) \rightarrow \phi_3}_{\phi}$

→ ENTÃO PODEMOS SUPOR QUE $M' \models \phi_1$ E $M' \models \phi_2$, E PORTANTO $M' \models \phi_1 \wedge \phi_2$. TEMOS QUE MOSTRAR QUE $M' \models \phi_3$.

→ Vamos "interpretar" seq. binárias em μ'

$$\begin{rcases} \mathrm{INT}(\epsilon) = e^{\mu'} \\ \mathrm{INT}(s0) = f_0^{\mu'}(\mathrm{INT}(s)) \\ \mathrm{INT}(s1) = f_1^{\mu'}(\mathrm{INT}(s)) \end{rcases}$$

→ Toda seq. bin. possui interpretação

$$\mathrm{INT}(b_1 b_2 \cdots b_l) = f_{b_l}^{\mu'}\left(f_{b_{l-1}}^{\mu'}\left(\cdots\left(f_{b_2}^{\mu'}\left(f_{b_1}^{\mu'}\left(e^{\mu'}\right)\right)\right)\right)\right)$$

$$= f_{b_1 \cdots b_l}^{\mu'}\left(e^{\mu'}\right)$$

→ COMO $M' \models \phi_1$, TEMOS $\left(f_{s_i}^{M'}(e^{M'}), f_{t_i}^{M'}(e^{M'})\right) \in P^{M'}$

(a) $i=1$

$$\left(f_{s_i}^{M'}(e^{M'}), f_{t_i}^{M'}(e^{M'})\right) = \left(\text{INT}(s_i), \text{INT}(t_i)\right)$$

PARA TODO i

→ COMO $M' \models \phi_2$, TEMOS QUE SEMPRE QUE $(s,t) \in P^{M'}$,

TEMOS $\left(f_{s_i}^{M'}(s), f_{t_i}^{M}(t)\right) \in P^{M'}$ PARA TODO i

(b) $i=2$

$$\left(f_{s_i}^{M'}(s), f_{t_i}^{M}(t)\right) = \left(\text{INT}(ss_i), \text{INT}(tt_i)\right)$$

$\text{INT}(\epsilon) = e^{M'}$

$\text{INT}(s0) = f_0^{M'}(\text{INT}(s))$

$\text{INT}(s1) = f_1^{M'}(\text{INT}(s))$

$$\phi_1 = \bigwedge_{i=1}^{k} P\left(f_{s_i}(e), f_{t_i}(e)\right)$$

$$\phi_2 = \forall v \forall w \left(P(v,w) \to \bigwedge_{i=1}^{k} P\left(f_{s_i}(v), f_{t_i}(w)\right)\right)$$

→ LOGO, TEMOS $\left(\text{INT}(s_{i_j}), \text{INT}(t_{i_j})\right) \in P^{M'}$, $j=1,\ldots,n$ $(i_1, \ldots, i_n)$

$\rightarrow$ LOGO, TEMOS $\left(\text{INT}(s_{i_1}), \text{INT}(t_{i_1})\right) \in P^{M'}$

$(i_1, \dots, i_m)$
C

$\rightsquigarrow \left(\text{INT}(s_{i_1} s_{i_2}), \text{INT}(t_{i_1} t_{i_2})\right) \in P^{M'}$

$\rightsquigarrow \left(\text{INT}(s_{i_1} s_{i_2} s_{i_3}), \text{INT}(t_{i_1} t_{i_2} t_{i_3})\right) \in P^{M'}$

$\vdots$

$\rightsquigarrow \left(\text{INT}(\overset{z}{s_{i_1} \dots s_{i_m}}), \text{INT}(\overset{z}{t_{i_1} \dots t_{i_m}})\right) \in P^{M'}$

$\rightarrow$ COMO $i_1, \dots, i_m$ É SOLUÇÃO DE C, $s_{i_1} \dots s_{i_m} = t_{i_1} \dots t_{i_m}$.

LOGO, $\underbrace{\text{INT}(s_{i_1} \dots s_{i_m})}_{z}$ E $\text{INT}(t_{i_1} \dots t_{i_m})$ SÃO O MESMO ELEMENTO DE A'

$\rightarrow$ LOGO, EXISTE z T.Q.

$(z,z) \in P^{M'}$

$\Rightarrow M' \models \exists z P(z,z) = \phi_3$

$\rightarrow$ COMO $M' \models \phi_2$, TEMOS QUE SEMPRE QUE $(s,t) \in P^{M'}$,

TEMOS $\left(f^{M'}_{s s_i}(s), f^{M}_{t t_i}(t)\right) \in P^{M'}$ PARA TODO i

$\left(\text{INT}(ss_i), \text{INT}(tt_i)\right)$

$i = i_3$

(b)

Observações Finais

1) ϕ é satisfazível se existe modelo $\mathcal{M}$ em $\mathcal{L}$ t.q. $\mathcal{M} \models_{\mathcal{L}} \phi$

- Há fórmulas que não são satisfazíveis: $\exists x (P(x) \wedge \neg P(x))$

→ Além disso ϕ é não-satisfazível sse $\neg\phi$ é válida

→ Como não podemos decidir validade, também não podemos decidir satisfatibilidade.

2) Pela completude e corretude, temos

$$\vdash \phi \quad \text{sse} \quad \models \phi$$

→ Como não podemos decidir a validade, então não podemos decidir provabilidade.