/ /

Teorema

Seja L uma assinatura. Para toda fórmula φ de L existe uma fórmula φ' de L tal que:

1) φ' é logicamente equivalente a φ;
2) φ' está na forma prenex.

Prova: Por indução sobre a complexidade de φ

1) Atômica (Caso Base)
2) Composta (Casos Indutivos)
   (i) φ é da forma $\neg\psi$
   (ii) φ é da forma $(\rho \,\square\, \theta)$
   $\square = \{\wedge, \vee, \rightarrow\}$
   (iii) φ é da forma $\forall x\, \psi$
   (iv) φ é da forma $\exists x\, \psi$

19/05

Método da Resolução para a Lógica de Primeira Ordem

Para aplicar o método da resolução para responder a uma questão sobre satisfatibilidade na lógica de predicados precisamos dos seguintes estágios:

1) encontrar a forma prenex de cada fórmula envolvida.
2) eliminar os quantificadores
   (a) existenciais
   (b) universais
3) encontrar a forma normal conjuntiva de cada fórmula envolvida;
4) aplicar o método da resolução com as devidas adaptações

Lista Adjacência
Labirinto

/ /

2(a) Eliminação de quantificadores existenciais

Objetivo: dada uma fórmula φ na forma prenex encontrar uma fórmula φ' tal que:

φ tem modelo sse φ' tem modelo.

e φ' não tem quantificadores existenciais.

Thoralf Skolem

$$\varphi \quad [\forall x \exists y\, R(x,y)]^{A} = V \quad \text{sse} \quad \varphi' \, [\forall x\, R(x, f(y))]^{A'}$$

$\varphi \quad \forall x \exists y \forall z \exists u\, (P(u) \wedge R(x,z) \rightarrow S(y))$

$\varphi' \quad \forall x \forall z \; (P(g(x,z)) \wedge R(x,z) \rightarrow S(f(x)))$

$A' = A + f^{A'} + g^{A'}$ $\qquad f \rightarrow$ função de escolha

forma skolemizada de φ

$\psi \quad \exists x \forall y \exists z \forall u\, (R(u,x) \rightarrow \neg S(y,z))$

$\psi' \quad \forall y \forall u\, (R(u,c) \rightarrow \neg S(y, h(y)))$

$A' = A + c^{A} + g^{A}$

Forma normal de Skolem

Definição:

Seja L uma assinatura, e φ uma fórmula de L tal que φ está na forma prenex.

A forma normal de Skolem de φ é uma fórmula φ' numa assinatura L tal que

(i) todos os quantificadores existenciais de φ foram removidos

(ii) as ocorrências de uma variável x quantificada existencialmente em φ foram substituídas por uma expressão do tipo $f(x_1, \ldots, x_n)$ onde f é um símbolo novo de função e $x_1, \ldots, x_n$

tilibra

são variáveis quantificadas universalmente anteriores a x.

Teorema (Skolem, 1920)
Seja φ uma fórmula numa assinatura L, tal que φ está na forma prenex. Então existe φ', na forma normal de Skolem, numa assinatura L' que inclui L, e φ tem modelo sse φ' tem modelo.

Exemplo:
① Premissa: Estudantes são cidadãos
Conclusão: Os votos dos estudantes são votos de cidadãos.

Formalizando
$E(x)$ – "x é estudante" $V(x,y)$ – "x é voto de y"
$C(x)$ – "x é cidadão"
Premissa: $\forall x (E(x) \to C(x))$
Conclusão: $\forall x (\exists y (E(y) \wedge V(x,y)) \to \exists y (C(z) \wedge V(x,z)))$

$$\{\forall x (E(x) \to C(x))\} \overset{?}{\models} \forall x (\exists y (E(y) \wedge V(x,y)) \to \exists z (C(z) \wedge V(x,z)))$$

$\Gamma \models \varphi$ sse

1 → $\Gamma \cup \{\neg\varphi\}$ é insat.

$\{\forall x (E(x) \to C(x))\} \cup \{\neg \forall x (\exists y (E(y) \wedge V(x,y)) \to \exists z (C(z) \wedge V(x,z)))\}$

$\{\forall x (E(x) \to C(x)), \exists x \neg (\exists y (E(y) \wedge V(x,y)) \to \exists z (C(z) \wedge V(x,z))$

$\exists x \neg (\neg \exists y (E(y) \wedge V(x,y)) \vee \exists z (C(z) \wedge V(x,z))$

$\exists x (\neg\neg \exists y (E(y) \wedge V(x,y)) \wedge \neg \exists z (C(z) \wedge V(x,z))$

$\exists x (\exists y (E(y) \wedge V(x,y)) \wedge \neg \exists z (C(z) \wedge V(x,z))$

$\exists x ((\exists y (E(y) \wedge V(x,y)) \wedge \forall z \neg (C(z) \wedge V(x,z))$

$\exists x \forall z (\exists y (E(y) \wedge V(x,y)) \wedge \neg (C(z) \wedge V(x,z)))$

$\exists x \forall z \exists y (E(y) \wedge V(x,y)) \wedge \neg (C(z) \wedge V(x,z)))$

2 → $\forall z \exists y (E(y) \wedge V(a,y) \wedge \neg(C(z) \wedge V(a,z)))$
$\forall z (E(f(z)) \wedge V(a, f(z)) \wedge \neg(C(z) \wedge V(a,z)))$

3 → $\{(E(x) \to C(x)),\ (E(f(z)) \wedge V(a, f(z)) \wedge \neg(C(z) \wedge V(a,z))\}$
$(E(x) \to C(x)) \wedge (E(f(z)) \wedge V(a, f(z)) \wedge \neg(C(z) \wedge V(a,z)))$
$(\neg E(x) \vee C(x)) \wedge E(f(z)) \wedge V(a, f(z)) \wedge ((\neg C(z) \vee \neg V(a,z))$

(2) Verifique se
$\{\forall x (P(x,b) \vee Q(x)),\ \forall y (\neg P(f(y), b)) \vee Q(y))\} \models \forall y (Q(y) \vee Q(f(y)))$
$\Gamma \models \mathcal{C}$ sse $\Gamma \cup \{\neg \mathcal{C}\}$ é insat.
$\{\forall x (P(x,b) \vee Q(x)),\ \forall y (\neg P(f(y), b)) \vee Q(y))\} \cup \{\neg \forall y (Q(y) \vee Q(f(y)))\}$
$\Gamma \cup \exists y \neg (Q(y) \vee Q(f(y))$
$\neg (Q(a) \vee Q(f(a))$

$\{\forall x (P(x,b) \vee Q(x)),\ \forall y (\neg P(f(y), b) \vee Q(y)),\ \neg (Q(a) \vee Q(f(a)))\}$
$\{P(x,b) \vee Q(x),\ \neg P(f(y), b) \vee Q(y),\ \neg (Q(a) \vee Q(f(a)))\}$
$(P(x,b) \vee Q(x)) \wedge (\neg P(f(y), b) \vee Q(y)) \wedge \neg Q(a) \wedge \neg Q(f(a))$
C_1 $x \mapsto a$ C_2 C_3 C_4
$P(a,b) \wedge (\neg P(f(y), b) \vee Q(y)) \wedge \neg Q(a) \wedge \neg Q(f(a))$

Unificação de Termos 21/05/09

Suponha que t_1 e t_2 sejam termos de uma assinatura L nos quais aparecem ocorrências das variáveis $x_1, \dots, x_n$. Uma <u>unificação</u> de t_1 e t_2 é uma substituição de $x_1, \dots, x_n$ por termos $s_1, \dots, s_n$, respectivamente, tal que ao ser aplicada a ambos t_1 e t_2 os resultados são termos idênticos. E neste caso dizemos que t_1 e t_2 são <u>unificáveis</u>

<u>O problema da unificação de termos</u>

Sejam $t_1, t_2, \dots, t_k$ termos de uma assinatura L nos quais podem estar ocorrendo as variáveis $x_1, \dots, x_n$.
Pergunta-se: $t_1, \dots, t_k$ são unificáveis?

Exemplos.

(1) $t_1 = f(x, g(a, y))$ $[a/x, a/y]$
$t_2 = f(x, g(y, x))$ $[a/x, a/y]$
Pergunta-se:
t_1 e t_2 são unificáveis?
existe s_1, s_2 tal que
$t_1 [s_1/x, s_2/y] = t_2 [s_1/x, s_2/y]$

(2) $t_1 = f(g(z), x)$
$t_2 = f(y, x)$
$t_3 = f(y, h(a))$
t_1, t_2 e t_3 são unificáveis?

x

Regras:

- Decomposição de termos
- Eliminação de eq. triviais
- Eliminação de variáveis

$S = \{ f(g(z), x) = f(y, x),\ f(y, x) = f(y, h(a)),\ f(g(z), x) = f(y, h(a)) \}$

$g(z) = y \qquad y = y\ ✓ \qquad g(z) = y$

$x = x\ ✓ \qquad x = h(a) \qquad x = h(a)$

$S' = \{ g(z) = y,\ x = h(a) \}$

$\left[{}^{h(a)}/_{x},\ {}^{g(z)}/_{y},\ {}^{z}/_{z} \right]$

Definição: (Equações e Sist. de Equações)

Seja L uma assinatura. Uma equação é um par de termos de L, denotada por exemplo por $t_1 \stackrel{?}{=} t_2$, e se t_1 e t_2 têm variáveis, então dizemos que $t_1 \stackrel{?}{=} t_2$ é uma equação básica. Uma substituição θ é chamada de unificadora de uma equação $t_1 \stackrel{?}{=} t_2$ se $\theta(t_1) = \theta(t_2)$. Um sistema de equações é um conjunto de equações, e uma substituição θ é um unificador de um sistema S se ela o unifica.

Definição: (Forma Resolvida)

Seja S um sistema de equações. Uma equação de S no formato $x \stackrel{?}{=} t$ é dita estar na forma resolvida (e, nesse caso, x é uma variável resolvida), se x não ocorre em mais lugar algum de S; em particular, se x não ocorre no termo t. Um sistema está na forma resolvida se todas as suas equações estão na forma resolvida.

Regras:

- Decomposição de termos
- Eliminação de eq. triviais
- Eliminação de variáveis

$S = \{ f(g(z), x) = f(y, x),\ f(y, x) = f(y, h(a)),\ f(g(z), x) = f(y, h(a))$

$g(z) = y \qquad y = y \checkmark \qquad g(z) = y$

$x = x \checkmark \qquad x = h(a) \qquad x = h(a)$

$S' = \{ g(z) = y \ ; \ x = h(a) \}$

$\left[{}^{h(a)}/_{x} ,\ {}^{g(z)}/_{y} ,\ {}^{z}/_{z} \right]$

Definição: (Equações e Sist. de Equações)

Seja L uma assinatura. Uma equação é um par de termos de L, denotada por exemplo por $t_1 \stackrel{?}{=} t_2$, e se t_1 e t_2 têm variáveis, então dizemos que $t_1 \stackrel{?}{=} t_2$ é uma equação básica. Uma substituição θ é chamada de unificadora de uma equação $t_1 \stackrel{?}{=} t_2$ se $\theta(t_1) = \theta(t_2)$. Um sistema de equações é um conjunto de equações, e uma substituição θ é um unificador de um sistema S se ela o unifica.

Definição: (Forma Resolvida)

Seja S um sistema de equações. Uma equação de S no formato $x \stackrel{?}{=} t$ é dita estar na forma resolvida (e, nesse caso, x é uma variável resolvida), se x não ocorre em mais lugar algum de S; em particular, se x não ocorre no termo t. Um sistema está na forma resolvida se todas as suas equações estão na forma resolvida.

$\theta = [h(a)/x, \; g(z)/y, \; z/z]$

$\theta' = [h(a)/x, \; g(g(a))/y, \; g(a)/z]$

$\theta'' = [h(a)/x, \; g(a)/y, \; a/z]$

Uma unificadora θ é a mais geral se ela for a mais simples, isto é, provoca o mínimo de substituição

Método da Unificação por Transformações em Sistemas de Equações (Jacques Herbrand, 1930)

Dado um sistema de equações S, para o qual se deseja encontrar, caso exista, uma unificadora, aplica-se um conj. de regras simples de transformação de S em S', S' em S'', ..., sucessivamente até que se chegue a um ponto em que nenhuma das tais regras possa ser aplicada. Nesse ponto é possível decidir se há ou não a unificadora. E quando há, ela é a mais geral.

Definição (Método de Herbrand):
Seja S um sistema de equações, f um símbolo de função da assinatura de S, e u e v termos quaisquer. As transformações são as seguintes.
(Eliminação de Equação Trivial)

$$\{u \stackrel{?}{=} v\} \cup S \stackrel{S}{\Longrightarrow} S$$

(Decomposição de Termos)
Para qualquer símbolo de função f

$$\{f(u_1, \dots, u_m) \stackrel{?}{=} f(v_1, \dots, v_m)\} \cup S \Longrightarrow \{u_1 \stackrel{?}{=} v_1, \dots, u_m \stackrel{?}{=} v_m\} \cup S$$

(Eliminação de Variáveis)

$\{x \stackrel{?}{=} v\} \cup S \Rightarrow \{x \stackrel{?}{=} v\} \cup S[v/x]$

onde $x \stackrel{?}{=} v$ não está na forma resolvida, e x não ocorre em t.

Exemplos:

③ $t_1 = g(f(x,x))$

$t_2 = g(f(h(a), g(b)))$

$S = \{t_1 \stackrel{?}{=} t_2\}$

$S = \{g(f(x,x)) \stackrel{?}{=} g(f(h(a), g(b)))\}$

↓ decomposição

$S' = \{f(x,x) \stackrel{?}{=} f(h(a), g(b))\}$

↓

$S'' = \{x \stackrel{?}{=} h(a),\ x \stackrel{?}{=} g(b)\} \rightarrow S''' = \{x = h(a),\ h(a) = g(b)\}$

Não são unificáveis.

④ $t_1 = f(x, g(x))$

$t_2 = f(g(x), g(g(x)))$

$S = \{t_1 \stackrel{?}{=} t_2\}$

$S = \{f(x, g(x)) \stackrel{?}{=} f(g(x), g(g(x)))\}$

↓ decomposição

$S' = \{x \stackrel{?}{=} g(x),\ g(x) \stackrel{?}{=} g(g(x))\}$

↓

$S'' = \{x \stackrel{?}{=} g(x),\ x \stackrel{?}{=} g(x)\} \rightarrow S'' = \{x \stackrel{?}{=} g(x)\}$

Método da Resolução com Unificação

Vamos retomar nossos exemplos anteriores para incorporar o algoritmo da unificação como uma das adaptações necessárias ao método da resolução para a L.P.

Exemplo:

2) $\{\forall x(P(x,b) \vee Q(x)),\ \forall y(\neg P(f(y),b) \vee Q(y))\} \models^{?}$
$\forall y(Q(y) \vee Q(f(y)))$

$$\underbrace{(P(x,b) \vee Q(x))}_{C_1} \wedge \underbrace{(\neg P(f(y),b) \vee Q(y))}_{C_2} \wedge \underbrace{\neg Q(a)}_{C_3} \wedge \underbrace{\neg Q(f(a))}_{C_4}$$

$x \stackrel{?}{=} f(y)$
$b \stackrel{?}{=} b$

$S = \{x \stackrel{?}{=} f(y),\ b \stackrel{?}{=} b\}$ $\quad (Q(f(y)) \vee Q(y)) \rightarrow C_5$
$S = \{x \stackrel{?}{=} f(y)\}$
$\theta = [f(y)/x]$

- C_5 e C_4

$f(y) = f(a)$ $\qquad Q(a) \wedge \neg Q(a)$
$S = \{f(y) \stackrel{?}{=} f(a)\}$ $\qquad \perp$
$S' = \{y \stackrel{?}{=} a\}$

Corretude e Completude do método da Resolução c/ Unificação

É necessário mostrar que o método é confiável, ou seja, para uma pergunta do tipo $\Gamma \models^{?} \varphi$

1) Se toda estrutura que satisfaz Γ também satisfaz φ, então o método deve fornecer uma "prova" de $\Gamma \cup \{\neg\varphi\}$ é insatisfatível (completude)

Murilo Raphael

x / /

② Se há como se chegar numa "prova" de que $\Gamma \cup \{\neg \mathcal{C}\}$ é insatisfatível, então toda estrutura que satisfaz Γ, satisfaz $\mathcal{C}$.

(xerox)

O uso da lógica simbólica nas ciências

28/05/09

Vimos que a lógica de predicados dispõe de pelo menos um método simbólico "perfeitamente confiável" para se resolver questões do tipo "$\mathcal{C}$ é uma consequência lógica de Γ" onde $\mathcal{C}$ é uma sentença da lógica de predicados, e Γ é um conjunto de premissas, sob a forma de sentenças da lógica de predicados.

Poderíamos perguntar se esse método funciona para qualquer conjunto Γ e qualquer sentença $\mathcal{C}$ em caso positivo, poderíamos vislumbrar a construção de uma "máquina" (ou programa) que pudesse servir de "oráculo" para perguntas sobre uma dada ciência cujas leis básicas pudessem ser formalizadas na lógica de predicados.

O Programa de Hilbert

Usar o método simbólico da lógica de predicados para provar a consistência de teorias matemáticas. Período: 1890's a 1920's

Obs: Alguns lógicos da época desconfiavam que não seria possível provar a consistência de certas teorias. 1904

BOBÃO BOBÃO

seria preciso identificar quais teorias matemáticas poderiam ser demonstradas como consistentes.

Fato marcante do ano de 1930

Kurt Gödel, um lógico austríaco provou que era impossível provar a consistência da aritmética usando apenas as leis básicas da própria aritmética.
Vamos tentar entender como foi essa argumentação de Gödel.

Teorias axiomáticas e seus modelos

- Definição (Teoria):
Seja L uma assinatura. Uma teoria em L é um conjunto de sentenças de L.

- Definição (Teoria consistente)
Seja T uma teoria numa assinatura L. T é consistente se não existe sentença ℓ de L tal que ℓ seja demonstrável a partir de T e $\neg \ell$ também seja demonstrável a partir de T.

- Definição (modelos de uma teoria)
Seja T uma teoria numa assinatura L. Um modelo de T é uma L-estrutura A que satisfaz a todas as sentenças de T.

Definição (Corretude e Completude)

Seja T uma teoria numa assinatura L, e A um modelo de T. Dizemos que T é <u>correta</u> com relação ao modelo A, se toda sentença e demonstrável a partir de T é verdadeira em A.

Dizemos que T é <u>completa</u> com relação ao modelo A, se toda sentença de L que é verdadeira em A é demonstrável a partir de T.

Em 1930, Kurt Gödel mostrou que a teoria axiomática da aritmética, que havia sido formalizada em 1889 por um italiano chamado Giuseppe Peano, não pode ser completa e correta (em relação ao modelo "padrão" da aritmética) ao mesmo tempo. Isto é, ou a aritmética é incompleta ou é incorreta.

<u>Estratégia de Gödel</u>

Encontrar uma sentença da aritmética que não pudesse ser verdadeira e demonstrável. Tomando por base o famoso "Paradoxo do Mentiroso" (i.e. "Esta sentença é falsa"), Gödel então mostrou que a seguinte sentença pode ser formalizada na linguagem da aritmética: "Esta sentença não é demonstrável".

<u>Aritmética de Peano</u>

(Giuseppe Peano, 1889)

1. $\forall x \ \neg(0 = s(x))$
2. $\forall x \forall y (s(x) = s(y) \rightarrow x = y)$

3 $\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(s(x))) \rightarrow \forall x\, \varphi(x)$

4. $\forall x\, ((x+0) = x)$

5. $\forall x \forall y ((x + s(y)) = s(x+y))$

6. $\forall x\, ((x.0) = 0)$

7. $\forall x \forall y\, ((x.s(y)) = ((x.y) + x))$

$x < y \equiv \exists z\, ((x+z) = y \wedge \neg(z=0))$

x divisível por y $\equiv \exists z\, ((y.z) = x)$

L

- $= (-,-)$
- 0
- $s(-)$

  $+(-,-)$

  $\times(-,-)$

Incompletude da Teoria Axiomática da Aritmética

Em 1930, Kurt Gödel mostrou que existe pelo menos uma sentença da aritmética que não pode ser verdadeira e demonstrável:

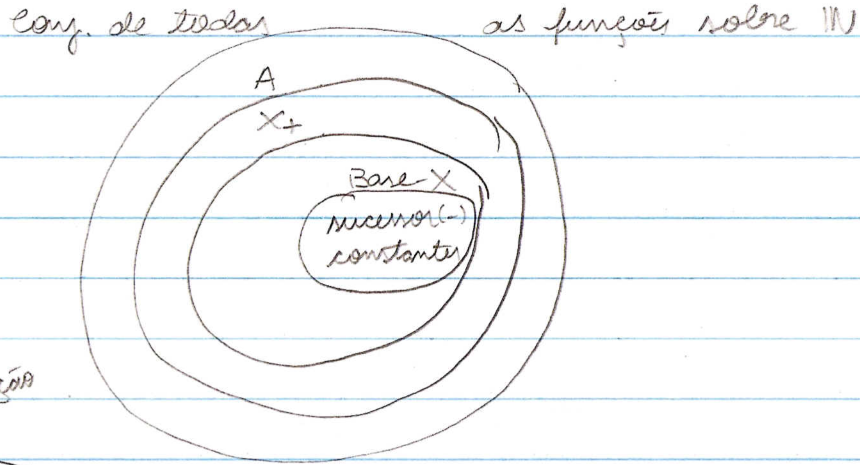
$\varphi \equiv$ "Esta sentença não é demonstrável"

A prova de que a sentença φ acima é formalizável / definível na linguagem da aritmética envolve duas grandes etapas:

① provar a existência de funções definíveis na aritmética que constroem um código numérico para cada sentença, e um código numérico para cada seqüência de sentenças (esta última serve para codificar provas).

Murilo

② provar a existência de uma formalização do predicado unário "demonstrável" na linguagem da aritmética



F
substituição

composição
recursão-primitiva
projeção

A: funções definidas pra aritmética
X'_+

Exemplo de função aritmética que é "calculável" pela aritmética, mas que não está no fecho indutivo

X_+ :

$f(x)$ = pegue o menor y maior que x tal que y seja maior que 2 seja par e não seja igual à soma de dois primos

Corretude e Completude do Método de Resolução com Unificação

É necessário mostrar que o método é confiável, ou seja, para uma pergunta do tipo $\Gamma \overset{?}{\models} \varphi$

(1) Se toda estrutura que satisfaz Γ também satisfaz φ, então o método deve fornecer uma "prova" de $\Gamma \cup \{\neg\varphi\}$ é insatisfatível (completude)

(2) Se há como se chegar numa "prova" de que $\Gamma \cup \{\neg\varphi\}$ é insatisfatível, então toda estrutura que satisfaz Γ, satisfaz φ. (corretude)

Corretude e Completude da Lógica de Predicados

Quando temos um problema de satisfatibilidade (ou um problema correlato) para sentenças da lógica de predicados, temos que aplicar um método algorítmico (que pode ser o método da resolução com unificação) para resolvê-lo. Como não há "tabela-verdade" nesse caso, resta saber se há algum método perfeitamente confiável. Para que um método seja perfeitamente confiável é preciso que ele seja:

CORRETO: tudo que é demonstrável é verdadeiro.

COMPLETO: tudo que é verdadeiro é demonstrável.

Notação:

$\Gamma \models \varphi$ significa "φ é uma consequência lógica do conjunto Γ", ou seja, "todo modelo de Γ também é um modelo de φ"

$\Gamma \vdash \varphi$ significa "existe uma demonstração (usando um método algorítmico) de que φ é uma consequência lógica do conjunto Γ"

Corretude e Completude de um Método Algorítmico

Seja Γ um conjunto de sentenças, e φ uma sentença

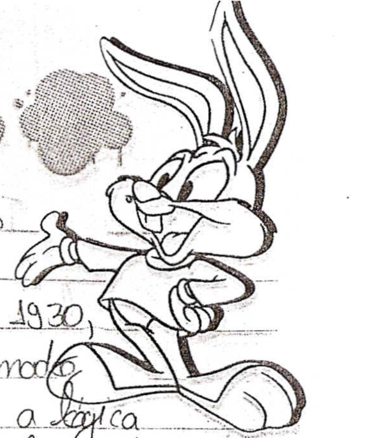
CORRETUDE:

Se $\Gamma \vdash \varphi$ então $\Gamma \models \varphi$

COMPLETUDE

Se $\Gamma \models \varphi$ então $\Gamma \vdash \varphi$

Em geral se usa o termo completude para $\Gamma \models \varphi$ se e somente se $\Gamma \vdash \varphi$



Corretude e Completude do Método da Resolução com unificação.

Ao definir o método da unificação de termos em 1930, Jacques Herbrand teve que mostrar que ele, combinado com algum método algorítmico de decisão para a lógica de predicados era correto e completo. Aí surge o chamado "Teorema de Herbrand"

Corretude e Completude da Lógica de Predicados.

Teorema de Herbrand

Seja S um conjunto de cláusulas numa assinatura L de primeira ordem. Então S é insatisfatível se e somente se algum conjunto finito de instâncias básicas de S é insatisfatível

$\Gamma \vDash \varphi$ se e somente se $\Gamma \cup \{\neg \varphi\}$, é insatisfatível

$\Gamma \vdash \varphi$ se e somente se existe $\Gamma, \neg\varphi, \Gamma', \Gamma'', \ldots, \bot$

S é insatisfatível se e somente se existe $\{\Gamma, \neg\varphi, \Gamma', \Gamma''\}$ que é insatisfatível.

Definição (instância básica de uma cláusula)

Suponha que C seja uma cláusula numa assinatura L. Uma instância básica (em inglês "ground instance") de C é uma cláusula de L obtida a partir da substituição uniforme das variáveis de C por termos fechados de L

Exemplo

Seja S o seguinte conjunto de cláusulas $S = \{\underbrace{(P(x,b) \vee Q(x))}_{C_1}, \underbrace{(\neg P(f(y),b) \vee Q(y))}_{C_2}, \underbrace{\neg Q(a)}_{C_3}, \underbrace{\neg Q(f(a))}_{C_4}\}$

Termos fechados de L:

a, b, f(a), f(b), f(f(a)), f(f(b)), f(f(f(a))), f(f(f(b)))

$L \begin{cases} - P(-,-) \\ \quad Q(-) \\ - a, b \\ - f(-) \end{cases}$

Teorema da Compacidade

Seja Γ um conjunto qualquer de sentenças da lógica proposicional. Então Γ é satisfatível se e somente se todo subconjunto finito Γ é satisfatível. (ou, Γ é insatisfatível se e somente se existe subconjunto finito de Γ que é insatisfatível).

Prova:

($\rightarrow$) Trivial pois toda valoração que satisfaz Γ satisfaz qualquer subconjunto finito de Γ

($\leftarrow$) Suponha que todo subconjunto finito de Γ seja satisfatível. Temos que mostrar que Γ propriamente dito é satisfatível, i.e. temos que encontrar uma valoração v que satisfaz Γ. Uma coisa é certa: não existe subconjunto finito de Γ que seja inconsistente. Vamos estender Γ até o máximo de consistência possível, e depois definir uma valoração para esse conjunto estendido.

Seja $\alpha_0, \alpha_1, \alpha_2 \ldots$ uma enumeração de todas as fórmulas bem formadas (isto é, os elementos de PROP).

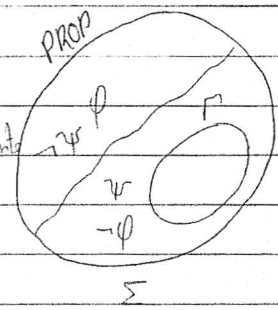
Seja:

$\Sigma_0 = \Gamma$

$$\Sigma_{n+1} = \Sigma_n \cup \begin{cases} \alpha_n & \text{se for consistente com } \Sigma_n \\ \neg\alpha_n & \text{caso contrário} \end{cases}$$

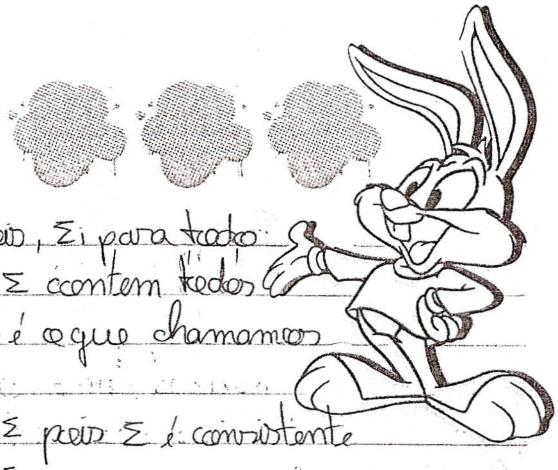
Seja

$$\Sigma = \bigcup_{i \geq 0} \Sigma_i$$



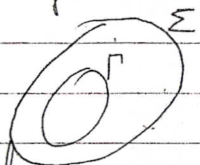
$$\Sigma_1 = \Sigma_0 \cup \begin{cases} \alpha_0 & \text{se consistente} \\ \neg\alpha_0 & \text{caso contrário} \end{cases}$$

$$\Sigma_2 = \Sigma_1 \cup \begin{cases} \alpha_1 \\ \neg\alpha_1 \end{cases}$$



Σ contem Γ, e Σ é consistente, pois, Σ_i para todo $i \geq 0$, é consistente, portanto; como Σ contem todos os Σ_i, Σ é consistente. Mais ainda, Σ é o que chamamos de maximalmente consistente, pois:

(1) não existe φ tal que $\varphi \in \Sigma$ e $\neg\varphi \in \Sigma$ pois Σ é consistente
(2) qualquer $\psi \in PROP$ ou $\psi \in \Sigma$ ou $\neg\psi \in \Sigma$



Se definirmos uma valoração que satisfaz Σ estaremos também definindo uma valoração que satisfaz Γ

Definição:
Seja a seguinte valoração
$v(x) = 1$ se e somente se $x \in \Sigma$

Agora vamos mostrar que v satisfaz não apenas as fórmulas atômicas de Σ, mas satisfaz todas as fórmulas de Σ.

Lema:
Para toda $\varphi \in PROP$
$\hat{v}(\varphi) = 1$ se e somente se $\varphi \in \Sigma$
Prova: Por indução sobre a complexidade de φ.
- Caso base: φ é atômica (trivial)
- Casos indutivos
(1) φ é da forma $\neg\psi$
(2) φ é da forma $(\rho \wedge \theta)$
(3) φ é da forma $(\rho \vee \theta)$
(4) φ é da forma $(\rho \rightarrow \theta)$

(1) φ é da forma $\neg\psi$
Hipótese Indutiva: $\hat{v}(\psi) = 1$ se e somente se $\psi \in \Sigma$
Tese: $\hat{v}(\neg\psi) = 1$ se e somente se $\neg\psi \in \Sigma$

Para provar a tese, vamos dividir em ida e volta
(→) Se $\hat{v}(\neg\psi)=1$ então $\neg\psi\in\Sigma$. Suponha que não é verdade que $\neg\psi\in\Sigma$. Ou seja, $\neg\psi\notin\Sigma$. Como Σ é maximalmente consistente, então $\psi\in\Sigma$. Da "Hipótese Indutiva", $\psi\in\Sigma$ se e somente se $\hat{v}(\psi)=1$. Logo $\hat{v}(\psi)=1$. Daí, $\hat{v}(\neg\psi)=0$.
Ou seja $\hat{v}(\neg\psi)\neq 1$.
(←) Se $\neg\psi\in\Sigma$ então $\hat{v}(\neg\psi)=1$. Assuma que $\neg\psi\in\Sigma$. Logo, $\psi\notin\Sigma$. Da "Hipótese Indutiva" $\psi\in\Sigma$ se e somente se $\hat{v}(\psi)\neq 1$. Logo $\hat{v}(\psi)\neq 1$. Daí, $\hat{v}(\psi)=0$. Portanto $\hat{v}(\neg\psi)=1$.

(2) φ é da forma $(\rho\wedge\theta)$
Hipótese Indutiva
$\hat{v}(\rho)=1$ se e somente se $\rho\in\Sigma$
$\hat{v}(\theta)=1$ se e somente se $\theta\in\Sigma$
Tese
$\hat{v}(\rho\wedge\theta)=1$ se e somente se $(\rho\wedge\theta)\in\Sigma$
(→) Assuma que $\hat{v}(\rho\wedge\theta)=1$ e $(\rho\wedge\theta)\in\Sigma$. Vamos mostrar que isso leva a um absurdo. Ora, como $(\rho\wedge\theta)\notin\Sigma$, e Σ é maximalmente consistente $\neg(\rho\wedge\theta)\in\Sigma$. Agora pelo caso anterior $\neg(\rho\wedge\theta)\in\Sigma$. Agora, pelo caso anterior $\hat{v}(\neg(\rho\wedge\theta))=1$

(←) Se $(\rho\wedge\theta)\in\Sigma$ então $\hat{v}(\rho\wedge\theta)=1$. Por contrapositiva, assuma que $\hat{v}(\rho\wedge\theta)\neq 1$ e vamos provar que $(\rho\wedge\theta)\in\Sigma$. Como $\hat{v}(\rho\wedge\theta)\neq 1$, temos que