ETI 2014/2015
CODIFICHE E PREDICATO SAT

VINCENZO MANTOVA

1. Codifica di formule

Definizione 1.1. Sia ϕ una formula del linguaggio della teoria degli insiemi. Definiamo la **codifica** $\ulcorner\phi\urcorner \in \mathbb{N}$ di ϕ per induzione nel seguente modo. Supponiamo che le variabili siano indicate come $x_1, x_2, \ldots, x_n, \ldots$. Per semplicità, traduciamo i quantificatori universali in esistenziali (cioè sostituiamo $\forall x$ con $\neg\exists x\neg$) e le disgiunzioni con congiunzioni (cioè sostituiamo $\phi \vee \psi$ con $\neg(\neg\phi \wedge \neg\psi)$. Definiamo:

- $\ulcorner x_i = x_j \urcorner := 2^i 3^j$;
- $\ulcorner x_i \in x_j \urcorner := 5^i 7^j$;
- $\ulcorner \neg\phi \urcorner := 11^{\ulcorner\phi\urcorner}$;
- $\ulcorner \phi \wedge \psi \urcorner := 13^{\ulcorner\phi\urcorner} 17^{\ulcorner\psi\urcorner}$;
- $\ulcorner \exists x_i \phi \urcorner := 19^i 23^{\ulcorner\phi\urcorner}$.

È facile, ma un po' lungo, scrivere la definizione del sottoinsieme $\mathrm{Form} \subseteq \mathbb{N}$ dei naturali che sono codifiche di formule. Inoltre, Form è Δ_1. (Vedi 1.3.)

Definizione 1.2. Definiamo $\mathrm{FV} : \mathrm{Form} \to \mathcal{P}_{\mathrm{fin}}(\mathbb{N})$ nel seguente modo:

- se $n = 2^i 3^j$ o $n = 5^i 7^j$, $\mathrm{FV}(n) := \{i, j\}$;
- se $n = 11^i$, allora $\mathrm{FV}(n) := \mathrm{FV}(i)$;
- se $n = 13^i 17^j$, allora $\mathrm{FV}(n) := \mathrm{FV}(i) \cup \mathrm{FV}(j)$;
- se $n = 19^i 23^j$, allora $\mathrm{FV}(n) := \mathrm{FV}(j) \setminus \{i\}$.

È facile verificare che FV è Δ_1 (1.4).

Esercizi

Esercizio 1.3. Definire l'insieme Form e verificare che è Δ_1. [Suggerimento: scrivere innanzitutto una formula vera sui numeri che sono codifiche di formule del tipo $x_i = x_j$ e $x_i \in x_j$ e poi lavorare per induzione. Ricordare che le operazioni di aritmetica ordinale sono Δ_1.]

Esercizio 1.4. Verificare che FV è Δ_1. [Ricordare che definire una funzione significa dare una definizione di «$y = \mathrm{FV}(x)$».]

Esercizio 1.5. Scrivere delle codifiche per $x_1 = \emptyset$, $x_1 = \{\emptyset\}$. [Nota: ricordare che $x = \emptyset$ è un abbreviazione per $\forall y(\neg y \in x)$, e indicare una formula simile per $x = \{\emptyset\}$.] Definire una funzione $N_j : \omega \to \mathrm{Form}$ a ogni ordinale finito $k \in \omega$ associa delle codifiche per $x_j = k$.

Esercizio 1.6. Definire una funzione $A_j : \omega \times \mathrm{Form} \to \mathrm{Form}$ che dato un ordinale finito $k \in \omega$ ed una formula ϕ restituisce la formula $\exists x_j(x_j = k \wedge \phi(x_j))$. [Usare l'esercizio precedente per codificare $x_j = k$.]

Date: 14 giugno 2015, v0.1.

2. Predicato di verità «Sat»

Sia (M, E) un insieme dotato di una relazione binaria, $\phi(x_1, \dots, x_n)$ una formula, e $a_1, \dots, a_n$ degli elementi di M. Ricordiamo che

$$(M, E) \models \phi(a_1, \dots, a_n)$$

significa che «$\phi(a_1, \dots, a_n)$ è vera in (M, E)», o più precisamente che la formula relativizzata $\phi^{M,E}(a_1, \dots, a_n)$ è vera. Possiamo dire in modo analogo se la *codifica* di una formula è vera in (M, E).

Definizione 2.1. Definiamo il predicato $\mathrm{Sat}_{M,E}$ che prende due argomenti: un numero $n \in \mathrm{Form}$ e una funzione $f : \mathrm{FV}(n) \to M$. Definiamo:

- se $n = 2^i 3^j$, allora $\mathrm{Sat}_{M,E}(n, f)$ vale se e solo se $f(i) = f(j)$;
- se $n = 5^i 7^j$, allora $\mathrm{Sat}_{M,E}(n, f)$ vale se e solo se $f(i) \in f(j)$;
- se $n = 11^i$, allora $\mathrm{Sat}_{M,E}(n, f)$ vale se e solo non vale $\mathrm{Sat}_{M,E}(i, f)$;
- se $n = 13^i 17^j$, allora $\mathrm{Sat}_{M,E}(n, f)$ vale se e solo se vale $\mathrm{Sat}_{M,E}(i, f_{\restriction \mathrm{FV}(i)}) \wedge \mathrm{Sat}_{M,E}(j, f_{\restriction \mathrm{FV}(j)})$;
- se $n = 19^i 23^j$, allora $\mathrm{Sat}_{M,E}(n, f)$ vale se e solo se $\forall x \in M(\mathrm{Sat}_{M,E}(j, f \cup \{\langle i, x\rangle\})$.

Nota 2.2. La definizione di $\mathrm{Sat}_{M,E}$ è per ricorsione sull'insieme delle coppie $\langle n, f\rangle$, con $f : \mathrm{FV}(n) \to M$, con la relazione $\langle n, f\rangle R \langle m, g\rangle$ se e solo se nRm (si può usare una R più raffinata notando che f e g devono essere correlate). La relazione R è ben fondata.

Tuttavia, se M fosse una classe transitiva *propria*, allora R non sarebbe ben fondata: $\mathrm{ext}_R(\langle n, f\rangle)$ sarebbe (nella maggior parte dei casi) una classe propria! Infatti, il predicato $\mathrm{Sat}_{M,R}$ non è definibile quando M è una classe propria. Per esempio, non si può definire $\mathrm{Sat}_{V,\in}$.

È facile verificare che $\mathrm{Sat}_{M,E}$ è Δ_1 (2.4).

Proposizione 2.3. *Sia (M, E) un insieme con una relazione binaria, $\phi(x_1, \dots, x_n)$ una formula, e $a_1, \dots, a_n$ degli elementi di M. Allora*

$$(M, E) \models \phi(a_1, \dots, a_n) \leftrightarrow \mathrm{Sat}_{M,E}(\ulcorner \phi \urcorner, \{\langle 1, a_1\rangle, \dots, \langle n, a_n\rangle\}).$$

Dimostrazione. Si verifica facilmente per induzione. Per esempio, se $\phi(a_1, a_2)$ è la formula $a_1 = a_2$, allora per definizione di Sat abbiamo

$$a_1 = a_2 \leftrightarrow \mathrm{Sat}_{M,E}(\ulcorner \phi \urcorner, \{\langle 1, a_1\rangle, \langle 2, a_2\rangle\}).$$

Chiaramente, $(M, E) \models a_1 = a_2 \leftrightarrow a_1 = a_2$, perché $(a_1 = a_2)^{M,E}$ è $a_1 = a_2$. Il caso generale si ottiene facilmente per induzione. □

Esercizi

Esercizio 2.4. Verificare che $\mathrm{Sat}_{M,E}$ è Δ_1.

Esercizio 2.5. Sia $\phi(x_1)$ una formula con unica variabile libera x_1 e k un ordinale finito. Allora $\phi(k)$ è vera in (M, E) se e solo se vale $\mathrm{Sat}_{M,E}(A_1(\ulcorner \phi(x_1) \urcorner, k))$.

3. Teorema del punto fisso

Sia ϕ una formula con un'unica variabile libera x_1. Definiamo:

- $x_2 = \text{Self}(x_1)$ se e solo se $x_2 = A_1(x_1, x_1)$;
- Fix_ϕ se e solo se

$$\exists x_2 \exists x_3(\phi(x_3) \wedge x_3 = \text{Self}(x_2) \wedge x_2 = \ulcorner \exists x_2 \exists x_3(\phi(x_3) \wedge x_3 = \text{Self}(x_2) \wedge x_2 = x_1)\urcorner).$$

Teorema 3.1. *Sia ϕ una formula con unica variabile libera x_1. Allora Fix_ϕ è vera se e solo se $\phi(\ulcorner \text{Fix}_\phi \urcorner)$ è vera.*

Dimostrazione. Per definizione, Fix_ϕ è vera se e solo se ϕ è soddisfatta dal numero

$$\text{Self}(\ulcorner \exists x_2 \exists x_3(\phi(x_3) \wedge x_3 = \text{Self}(x_2) \wedge x_2 = x_1)\urcorner).$$

Applicare Self ad una codifica significa sostituire la codifica stessa al posto della variabile x_1. Quindi il numero sopra è uguale a

$$\ulcorner \exists x_2 \exists x_3(\phi(x_3) \wedge x_3 = \text{Self}(x_2) \wedge x_2 = \ulcorner \exists x_2 \exists x_3(\phi(x_3) \wedge x_3 = \text{Self}(x_2) \wedge x_2 = x_1)\urcorner)\urcorner$$

che è esattamente $\ulcorner \text{Fix}_\phi \urcorner$. Quindi Fix_ϕ è vera se e solo se $\phi(\ulcorner \text{Fix}_\phi \urcorner)$. □

Teorema 3.2 (Tarski)**.** *Non è possibile definire* $\text{Sat}_{V,\in}$.

Dimostrazione. Supponiamo per assurdo che si possa definire $\text{Sat}_{V,\in}$. Sia $\phi(x_1) := \neg\text{Sat}_{V,\in}(x_1)$. Per il teorema del punto fisso, Fix_ϕ è vera se e solo se $\phi(\ulcorner \text{Fix}_\phi \urcorner)$ è vera, quindi se e solo se $\neg\text{Sat}_{V,\in}(\ulcorner \text{Fix}_\phi \urcorner)$ è vera, ovvero se e solo se Fix_ϕ è falsa, assurdo. □

4. Teorema di incompletezza di Gödel (secondo Jech)

Il secondo teorema di incompletezza di Gödel, in piena generalità, asserisce che se una teoria è *coerente*, ovvero non produce contraddizioni, e riesce ad interpretare un frammento sufficientemente potente dell'aritmetica (ad esempio, l'aritmetica di Peano), allora la teoria non è in grado di dimostrare la propria coerenza. In particolare, dato che ZFC è in grado di definire l'aritmetica dei numeri naturali e dimostrare gli assiomi di Peano, ZFC non può dimostrare che ZFC è coerente.

Nel caso di ZFC, «ZFC non dimostra la coerenza di ZFC» è equivalente a «ZFC non dimostra l'esistenza di un modello di ZFC» (ovvero, non dimostra l'esistenza di un insieme M e una relazione $E \subseteq M \times M$ tale che (M, E) soddisfa gli assiomi di ZFC). È facile verificare che ZFC non dimostra l'esistenza di un modello *transitivo* di ZFC.

Proposizione 4.1. *La classe dei modelli transitivi di ZFC è Δ_1.*

Dimostrazione. È possibile definire un predicato $\text{ZFC}(n)$ per $n \in \text{Form}$ vero se e solo se n codifica un assioma di ZFC. Il predicato è chiaramente Δ_1. Allora M è un modello transitivo di ZFC se e solo se M è transitivo e $\forall x \in \text{Form}(\text{ZFC}(x) \to \text{Sat}_M(x))$. Essere transitivo è una proprietà Δ_0, mentre l'ultima formula è Δ_1, quindi essere un modello transitivo di ZFC è Δ_1. □

Proposizione 4.2. *ZFC non dimostra l'esistenza di un modello transitivo di ZFC.*

Dimostrazione. Supponiamo per assurdo che ZFC implichi l'esistenza di un modello transitivo. Sia M un modello transitivo $\in$-minimale. Dato che M è un modello di ZFC, allora pensa di contenere un modello transitivo N. D'altra parte, essere un modello transitivo è una proprietà Δ_1, quindi assoluta; dato che M pensa che N è

un modello transitivo, allora N è davvero un modello transitivo. Questo contraddice la minimalità di M. □

D'altra parte, la teoria di ZFC più un cardinale inaccessibile dimostra l'esistenza di un modello transitivo (l'insieme H_κ con κ inaccessibile). Quindi ZFC non può né dimostrare né negare l'esistenza di un modello transitivo di ZFC.

Per dimostrare che ZFC non dimostra l'esistenza di un modello di ZFC, seguiamo la strategia di Jech.

Definizione 4.3. Sia T una teoria (cioè un insieme di formule chiuse). Diciamo che T **implica** ϕ, o $T \models \phi$, se e solo se in ogni modello M di T vale $M \models \phi$.

Teorema 4.4 (Compattezza)**.** *Sia T una teoria e ϕ una formula. Se $T \models \phi$, allora esiste un sottoinsieme finito $\Sigma \subseteq T$ tale che $\Sigma \models \phi$.*

Dimostrazione. Per semplicità, dimostriamo solo il caso in cui T è numerabile (vero sempre se il linguaggio stesso è numerabile, perché allora l'insieme di tutte le formule è numerabile). Numeriamo le formule di T come $\psi_0, \psi_1, \psi_2, \dots$. Chiaramente, se esiste n tale che $\psi_0, \dots, \psi_n \models \phi$, allora $T \models \phi$.

Supponiamo invece che per ogni n abbiamo $\psi_0, \dots, \psi_n \not\models \phi$. Fissato n, dobbiamo avere due modelli M_n^+, M_n^- di $\psi_0, \dots, \psi_n$ tali che $M_n^+ \models \phi$ e $M_n^- \models \neg\phi$. Se fissiamo un qualsiasi ultrafiltro non principale su $\mathbb{N}$, l'ultraprodotto degli M_n^+ è un modello di T in cui ϕ è vera, mentre l'ultraprodotto degli M_n^- è un modello di T in cui ϕ è falsa. Quindi $T \not\models \phi$. □

Sia ora Σ un qualche sottoinsieme finito di ZFC grande abbastanza da dimostrare che per ogni (M, E), $\mathrm{Sat}_{M,E}$ è ben definito.

Proposizione 4.5. *Esiste una formula ϕ_Σ che è vera se e solo se esiste (M, E) modello di Σ tale che ϕ è falsa in (M, E).*

Dimostrazione. Sia ψ la formula che dice «esiste (M, E) tale che $(M, E) \models \Sigma$ e $\neg\mathrm{Sat}_{M,E}(x_1)$», dove x_1 è l'unica variabile libera. Allora $\phi_\Sigma := \mathrm{Fix}_\psi$ ha la proprietà che vogliamo. □

Supponiamo che (M, E) sia un modello di Σ, e che ci sia (N, F) in M tale che $(M, E) \models ((N, F) \models \Sigma)$. Allora definiamo N^* come l'insieme degli x tali che xEN e la relazione F^* su N^* dicendo che xF^*y vale se e solo se abbiamo $(M, E) \models xFy$.

Definiamo $(M_1, E_1) <_J (M_2, E_2)$ se e solo se esiste (N, F) tale che $(M_1, E_1) = (N^*, F^*)$. È facile, e cruciale per quello che segue, verificare che $<_J$ è *transitiva*: se $(M_1, E_1) <_J (M_2, E_2) <_J (M_3, E_3)$, allora $(M_1, E_1) < (M_3, E_3)$ (4.8).

Proposizione 4.6. *Per ogni formula ψ abbiamo $(N^*, F^*) \models \psi$ se e solo se $(M, E) \models ((N, F) \models \psi)$.*

Dimostrazione. È vero per definizione sulle formule atomiche, e segue facilmente per induzione sulla complessità delle formule. □

Teorema 4.7 (Jech)**.** *ZFC non dimostra l'esistenza di un modello di ZFC.*

Dimostrazione. Supponiamo che ZFC dimostri l'esistenza di un modello. Prendiamo come Σ un sottoinsieme finito di ZFC che dimostra l'esistenza di un modello e anche che per ogni (M, E), $\mathrm{Sat}_{M,E}$ è ben definito. Sia $\phi = \phi_\Sigma$. Per definizione, se $(M, E) \models \neg\phi$, allora ogni modello in (M, E) di Σ soddisfa ϕ. In altre parole, se $(M, E) \models \neg\phi$ allora ogni $(N, F) <_J (M, E)$ modello di Σ soddisfa $(N, F) \models \phi$.

Supponiamo che ϕ sia falsa nell'universo V. Allora ϕ è vera in *tutti* i modelli di Σ. Per ipotesi, esiste almeno un modello (M, E) di ZFC, ed in particolare di Σ, e ϕ è vera in quel modello. Allora esiste $(N, F) <_J (M, E)$ tale che $(N, F) \models \neg\phi$, assurdo.

Supponiamo che ϕ sia vera nell'universo V. Allora esiste un modello (M, E) di Σ tale che $(M, E) \models \neg\phi$. Quindi $(N, F) \models \phi$ per ogni $(N, F) <_J (M, E)$ modello di Σ. D'altra parte, questo significa che esiste $(O, G) <_J (N, F)$ modello di Σ tale che $(O, G) \models \neg\phi$. Per transitività di $<_J$, questo implica che esiste $(O, G) <_J (M, E)$ modello di Σ tale che $(O, G) \models \neg\phi$, assurdo. □

Esercizi

Esercizio 4.8. Verificare che l'ordine $<_J$ è transitivo.