Λογική Πρώτης Τάξης

Γιώργος Κορφιάτης

Εθνικό Μετσόβιο Πολυτεχνείο

Νοέμβριος 2008

Σύνταξη

Ορισμός (Σύνταξη της λογικής πρώτης τάξης)

Λεξιλόγιο $\Sigma = (\Phi, \Pi, r)$

- Συναρτήσεις $f \in \Phi$
- Σχέσεις $R \in \Pi$
- $r(\cdot)$ η πληθικότητα (arity) των f και R

Μεταβλητές $V = \{x, y, z, \ldots\}$

Παράδειγμα (Θεωρία Αριθμών)

$\Sigma_{\mathbf{N}} = (\Phi_{\mathbf{N}}, \Pi_{\mathbf{N}}, r_{\mathbf{N}})$

- $\Phi_{\mathbf{N}} = \{0, \sigma, +, \times, \uparrow\}$
- $\Pi_{\mathbf{N}} = \{=, <\}$
- $r(0) = 0,\ r(\sigma) = 1,\ r(+) = r(\times) = r(\uparrow) = 2$
- $r(=) = r(<) = 2$

Όροι και Εκφράσεις

- Όροι t:
  - $x \in V$
  - $\underline{f(t_1, \ldots, t_k)}$
- Εκφράσεις ϕ, ψ:
  - $\underline{R(t_1, \ldots, t_k)}$
  - $\underline{\neg\phi}$, $\underline{(\phi \vee \psi)}$ και $\underline{(\phi \wedge \psi)}$
  - $\underline{(\forall x \phi)}$
  - Συντομογραφίες $\Rightarrow$, $\Leftrightarrow$ και $\exists$
    $\underline{(\phi \Rightarrow \psi)} \equiv \underline{(\neg\phi \vee \psi)}$ $\quad$ $\underline{(\exists x \phi)} \equiv \underline{\neg(\forall x \neg\phi)}$

Όροι και Εκφράσεις στη Θεωρία Αριθμών

Όροι:

$$\underline{\sigma(\sigma(0))} \quad \rightsquigarrow \quad \underline{2}$$
$$\underline{+(x, \sigma(\sigma(0)))} \quad \rightsquigarrow \quad \underline{x + 2}$$

Εκφράσεις:

$$\underline{< (x, \sigma(\sigma(0)))} \quad \rightsquigarrow \quad \underline{x < 2}$$
$$\underline{\forall x < (+(x, \sigma(\sigma(0))), \sigma(\uparrow (x, \sigma(\sigma(0)))))} \quad \rightsquigarrow \quad \underline{\forall x((x + 2) < \sigma(x \uparrow 2))}$$

Ελεύθερες και Δεσμευμένες Μεταβλητές

$$\underline{(\forall x(x + y > 0)) \wedge (x > 0)}$$

- Το πρώτο x δεσμευμένο
- Το δεύτερο x ελεύθερο
- Το y ελεύθερο

Μετονομασία δεσμευμένης μεταβλητής:

$$\underline{(\forall z(z + y > 0)) \wedge (x > 0)}$$

Μοντέλα

- Ανάλογο με την ανάθεση αλήθειας του προτασιακού λογισμού
- $M = (U, \mu)$ μοντέλο κατάλληλο για ένα $\Sigma = (\Phi, \Pi, r)$
- σύνολο $U \neq \emptyset$ (σύμπαν)
- συνάρτηση $\mu : V \cup \Phi \cup \Pi \overset{\mu}{\mapsto} U$
  - $x \in V \overset{\mu}{\mapsto} x^M \in U$
  - $f \in \Phi$ (πληθικότητας k) $\overset{\mu}{\mapsto} f^M : U^k \mapsto U$
  - $R \in \Pi$ (πληθικότητας k) $\overset{\mu}{\mapsto} R^M \subseteq U^k$

Ερμηνεία με βάση μοντέλο M

- Σημασία όρου t υπό μοντέλο M

t	t^M
x	x^M
$f(t_1, \ldots, t_k)$	$f^M(t_1^M, \ldots, t_k^M)$

- Ικανοποίηση έκφρασης από μοντέλο ($M \models \phi$)

ϕ	$M \models \phi$ if
$R(t_1, \ldots, t_k)$	$(t_1^M, \ldots, t_k^M) \in R^M$
$\neg\psi$	$M \not\models \psi$
$\psi_1 \vee \psi_2$	$M \models \psi_1 \vee M \models \psi_2$
$\psi_1 \wedge \psi_2$	$M \models \psi_1 \ \wedge M \models \psi_2$
$\forall x \psi$	$\forall u \in U : M_{x=u} \models \psi$

όπου $M_{x=u}$ ίδιο με το M εκτός του ότι $x^{M_{x=u}} = u$

Μοντέλο της Θεωρίας Αριθμών

Ορισμός

Μοντέλο $\mathbf{N} = (U, \mu)$, με $U = \mathbb{N}$

- $0^{\mathbf{N}} = 0$
- $\sigma^{\mathbf{N}}(n) = n + 1$
- $+^{\mathbf{N}}(n_1, n_2) = n_1 + n_2$
- $<^{\mathbf{N}}(n_1, n_2) = n_1 < n_2$
- $\ldots$

Παράδειγμα

$\mathbf{N} \vDash \underline{\forall x(x < x + 1)} \quad \rightsquigarrow$

$\forall n \in \mathbb{N},\ \mathbf{N}_{x=n} \vDash \underline{x < x + 1} \quad \rightsquigarrow$

$\forall n \in \mathbb{N},\ n <^{\mathbf{N}} n +^{\mathbf{N}} 1^{\mathbf{N}}$

Μοντέλο Ισοτιμίας (parity) για Θεωρία Αριθμών

Ορισμός

Μοντέλο $\mathbf{N}_p = (U, \mu)$, με $U = \{0, 1, \ldots, p-1\}$, όπου $p > 1$

- $0^{\mathbf{N}_p} = 0$
- $\sigma^{\mathbf{N}_p}(n) = n + 1 \mod p$
- $m +^{\mathbf{N}_p} n = m + n \mod p$
- ...

Παράδειγμα

$\mathbf{N}_p \not\models \underline{\forall x(x < x + 1)} \rightsquigarrow$

$\mathbf{N}_{p(x=p-1)} \not\models \underline{x < x + 1} \rightsquigarrow$

δεν ισχύει $(p-1) <^{\mathbf{N}_p} (p-1) +^{\mathbf{N}_p} 1^{\mathbf{N}_p} \rightsquigarrow$

δεν ισχύει $(p-1) < (p-1) + 1 \mod p$

Μοντέλο για Θεωρία Γράφων

- Λεξιλόγιο Σ_G με σχέσεις $\{=, G\}$ πληθικότητας 2
- Μοντέλο Γ με U σύνολο 5 κόμβων της Εικόνας 5-2 και $G^{\Gamma}(x, y)$ αληθές αν υπάρχει ακμή από το x στο y στο γράφο
- $\phi = \underline{\forall x(\forall y(G(x, y) \Rightarrow G(y, x)))}$ (η G είναι συμμετρική)
- $\Gamma \models \phi$
- $\phi' = \underline{\forall x(\forall y(\forall z(G(x, z) \wedge G(z, y)) \Rightarrow G(x, y)))}$ (G μεταβατική)
- $\Gamma \not\models \phi'$
- Και τα δύο ελέγχονται σε πολυωνυμικό χρόνο

ϕ-GRAPHS

Ορισμός (Πρόβλημα ϕ-GRAPHS)

Δοσμένου ενός μοντέλου Γ (ενός γράφου G_Γ) για μία έκφραση ϕ, ισχύει $\Gamma \models \phi$;

Θεώρημα

Για κάθε έκφραση ϕ στο Σ_G, το ϕ-GRAPHS είναι στο **P**

Απόδειξη

Με επαγωγή στη δομή του ϕ:

- $\phi = \underline{G(x, y)}$, *προφανές*
- $\phi = \underline{\neg\psi}$, $\underline{\psi_1 \vee \psi_2}$, $\underline{\psi_1 \wedge \psi_2}$, *αφού ισχύει για* ψ, ψ_1, ψ_2
- $\phi = \underline{\forall x \psi}$, *αφού ισχύει για* ψ, *ελέγχουμε για κάθε κόμβο του γράφου*

Έγκυρες Εκφράσεις

Ορισμός

Μία έκφραση ϕ λέγεται ικανοποιήσιμη αν υπάρχει ένα μοντέλο που να την ικανοποιεί ($M \models \phi$)

Ορισμός

Αν μία έκφραση ϕ ικανοποιείται από κάθε μοντέλο, λέγεται έγκυρη (γράφουμε $\models \phi$)

Πρόταση

Μία έκφραση δεν είναι ικανοποιήσιμη αν και μόνο αν η άρνησή της είναι έγκυρη ($\neg\exists M : M \models \phi \Leftrightarrow \models \neg\phi$)

Αποδείξεις

- Συστηματικός τρόπος για να δείχνουμε την εγκυρότητα προτάσεων
- Βασιζόμενοι σε (αξιώματα):
  - Εγκυρότητα στη λογική Boole (ταυτολογίες)
  - Ιδιότητες της ισότητας
  - Ιδιότητες των ποσοδεικτών

Πρόταση (Modus Ponens)

Αν οι εκφράσεις ψ *και* $\psi \Rightarrow \phi$ *είναι έγκυρες, τότε η* ϕ *είναι έγκυρη*

Βασικά Λογικά Αξιώματα

ΑΞ0: Κάθε έκφραση που είναι ταυτολογία στη λογική Boole

ΑΞ1: Κάθε έκφραση της μορφής:

ΑΞ1α: $\underline{t = t}$

ΑΞ1β: $\underline{(t_1 = t'_1 \wedge \ldots \wedge t_k = t'_k) \Rightarrow f(t_1, \ldots, t_k) = f(t'_1, \ldots, t'_k)}$

ΑΞ1γ: $\underline{(t_1 = t'_1 \wedge \ldots \wedge t_k = t'_k) \Rightarrow R(t_1, \ldots, t_k) = R(t'_1, \ldots, t'_k)}$

ΑΞ2: Κάθε έκφραση της μορφής $\underline{\forall x \phi \Rightarrow \phi[x \leftarrow t]}$

ΑΞ3: Κάθε έκφραση της μορφής $\underline{\phi \Rightarrow \forall x \phi}$ (x όχι ελεύθερο στο ϕ)

ΑΞ4: Κάθε έκφραση της μορφής $\underline{(\forall x(\phi \Rightarrow \psi)) \Rightarrow (\forall x \phi \Rightarrow \forall x \psi)}$

Αποδείξεις

Βασιζόμαστε στα αξιώματα και το modus ponens

Ορισμός (Απόδειξη μίας έκφρασης ϕ_n)

Έστω ακολουθία εκφράσεων $S = (\phi_1, \ldots, \phi_2, \ldots, \phi_n)$ και Λ σύνολο αξιωμάτων. Αν για κάθε ϕ_i ισχύει:

- είτε $\phi_i \in \Lambda$
- είτε υπάρχουν $\psi,\ \psi \Rightarrow \phi_i$ στα $\phi_1, \ldots, \phi_{i-1}$

τότε το S είναι μια απόδειξη για το ϕ_n.
Το ϕ_n λέγεται *θεώρημα πρώτης τάξης* και γράφουμε

$$\vdash \phi_n$$

Αποδείξεις

Παράδειγμα (Συμμετρία της ισότητας)

1. $\underline{(x = y \wedge x = x) \Rightarrow (x = x \Rightarrow y = x)}$ (ΑΞ1γ)
2. $\underline{(x = x)}$ (ΑΞ1α)
3. $\dfrac{x=x \Rightarrow ((x=y \wedge x=x) \Rightarrow (x=x \Rightarrow y=x)) \Rightarrow (x=y \Rightarrow y=x)}{\text{(ΑΞ0) ταυτολογία } a \Rightarrow ((b \wedge a) \Rightarrow (a \Rightarrow c)) \Rightarrow (b \Rightarrow c)}$
4. $\underline{((x=y \wedge x=x) \Rightarrow (x=x \Rightarrow y=x)) \Rightarrow (x=y \Rightarrow y=x)}$ (2,3)
5. $\underline{(x = y \Rightarrow y = x)}$ (1,4)

THEOREMHOOD

Μπορούμε να κωδικοποιήσουμε τις εκφράσεις και τις αποδείξεις (ακολουθία εκφράσεων) σαν συμβολοσειρές.

Ορισμός (Πρόβλημα THEOREMHOOD)

Έστω μία κωδικοποίηση για την ϕ. Είναι η ϕ θεώρημα πρώτης τάξης ($\vdash \phi$);

Πρόταση

Το THEOREMHOOD *είναι αναδρομικά αριθμήσιμο.*

Απόδειξη

Η μηχανή Turing δοκιμάζει όλες τις πεπερασμένες ακολουθίες εκφράσεων με λεξικογραφική σειρά και απαντά θετικά αν κάποια ακολουθία είναι απόδειξη της δοσμένης έκφρασης.

VALIDITY

Ορισμός (Πρόβλημα VALIDITY)

Έστω δοσμένη έκφραση ϕ. Είναι έγκυρη ($\models \phi$);

Θεώρημα (Εγκυρότητας και Πληρότητας)

$$\begin{array}{ccc} \text{VALIDITY} & \equiv & \text{THEOREMHOOD} \\ \models \phi & \Leftrightarrow & \vdash \phi \end{array}$$

Όμως, πιο ενδιαφέρον αν η ϕ ικανοποιείται από *συγκεκριμένο* μοντέλο!

$\Rightarrow$ Στόχος: Αξιωματικοποίηση του μοντέλου

Απόδειξη από Προκείμενες

Ορισμός (Έγκυρη Συνέπεια από Προκείμενες, $\Delta \models \phi$)

Έστω σύνολο εκφράσεων Δ. Αν κάθε μοντέλο που ικανοποιεί κάθε έκφραση του Δ ικανοποιεί και τη ϕ, τότε η ϕ είναι έγκυρη συνέπεια του Δ.

Ορισμός (Απόδειξη από Προκείμενες, $\Delta \vdash \phi$)

Ακολουθία $S = (\phi_1, \phi_2, \ldots, \phi_n)$, αξιώματα Λ, προκείμενες Δ.
Αν για κάθε ϕ_i ισχύει $\phi_i \in \Lambda \cup \Delta$ ή προκύπτει με modus ponens, τότε η S είναι απόδειξη της ϕ_n από Δ.

Ιδέα: Εισάγουμε επιπλέον αξιώματα Δ που *περιγράφουν* το μοντέλο μας

Παράδειγμα: Αξιωματικοποίηση της Θεωρίας Ομάδων

- Λεξιλόγιο με σταθερά 1 και πράξη $\circ$
- «Μη λογικά» αξιώματα:

  GR1: $\forall x \forall y \forall z \big((x \circ y) \circ z = x \circ (y \circ z) \big)$ (προσεταιριστικότητα)

  GR2: $\forall x \big(x \circ 1 \big) = x$ (ουδέτερο στοιχείο)

  GR3: $\forall x \exists y \big(x \circ y = 1 \big)$ (ύπαρξη αντιστρόφου)

Τεχνικές Μαθηματικού Συλλογισμού

Θεώρημα (Τεχνική Παραγωγής, deduction)

Αν $\Delta \cup \{\phi\} \vdash \psi$, *τότε* $\Delta \vdash \underline{\phi \Rightarrow \psi}$.

Απόδειξη

Έστω $S = (\phi_1, \ldots, \phi_n)$ *απόδειξη του* ψ *από* $\Delta \cup \{\phi\}$. *Με επαγωγή στο* ϕ_i *(υποθέτουμε* $\underline{\phi \Rightarrow \phi_j}$ *για κάθε* $j < i$*).*

- *Αν* $\phi_i \in \Delta \cup \Lambda$, *προσθέτουμε* $\{\phi_i, \underline{\phi_i \Rightarrow (\phi \Rightarrow \phi_i)}, \underline{\phi \Rightarrow \phi_i}\}$
- *Αν* ϕ_i *από* $\{\phi_j, \underline{\phi_j \Rightarrow \phi_i}\}$ *με modus ponens, προσθέτουμε κατάλληλες εκφράσεις παρομοίως*

Τεχνικές Μαθηματικού Συλλογισμού

Ορισμός (Συνεπές, consistent)

Αν $\Delta \vdash \phi$ για κάθε ϕ (και το $\underline{\neg\phi}$), τότε το Δ λέγεται ασυνεπές. Αν δεν υπάρχει καμία αντίφαση, τότε είναι συνεπές.

Θεώρημα (Απαγωγή σε Άτοπο)

Αν το $\Delta \cup \{\underline{\neg\phi}\}$ *είναι ασυνεπές, τότε* $\Delta \vdash \phi$.

Απόδειξη

Ασυνεπές: $\Delta \cup \{\underline{\neg\phi}\} \vdash \phi$. *Από θεώρημα παραγωγής* $\Delta \vdash \underline{\neg\phi \Rightarrow \phi}$, *ισοδύναμο με* ϕ.

Θεώρημα (Γενίκευση)

Αν $\Delta \vdash \phi$ *και το* x *δεν είναι ελεύθερο στο* Δ, *τότε* $\Delta \vdash \forall x\phi$.