ΓΛΩΣΣΕΣ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ ΙΙ

Εισαγωγή στη αποδεικτικά συστήματα: λογική πρώτου βαθμού και φυσική απαγωγή

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Εθνικό Μετσόβιο Πολυτεχνείο

Ζωή Παρασκευοπούλου, 2024

ΤΙ ΕΙΝΑΙ ΕΝΑ ΣΥΣΤΗΜΑ ΑΠΟΔΕΙΞΕΩΝ;

Ένα **σύστημα αποδείξεων** μας επιτρέπει να παράγουμε θεωρήματα για μια θεωρία. Περιλαμβάνει:

- Μια **τυπική γλώσσα** (η γλώσσα των λογικών προτάσεων)
    - Π.χ. προτασιακή λογική, λογική Ν-βαθμού
- Ένα **σύνολο από αξιώματα**
    - Οι λογικές προτάσεις που θεωρούνται αληθείς (π.χ. True, αρχή του αποκλειόμενου μέσου, αξιώματα αριθμητικής, …)
- Ένα **σύνολο κανόνων συμπερασμού** (inference rules)
    - Οι κανόνες που μπορούν να χρησιμοποιηθούν για την απόδειξη θεωρημάτων

ΠΡΩΤΟΒΑΘΜΙΑ ΛΟΓΙΚΗ

- **Τυπική γλώσσα**
  - Ένα σύνολο από μεταβλητές $\mathcal{X}$ = { x, y, z, … }
  - Ένα προκαθορισμένο σύνολο από συναρτήσεις με συγκεκριμένο arity Σ
  - Ένα προκαθορισμένο σύνολο από κατηγορήματα $\mathcal{P}$
  - Όροι

$$t ::= x \mid f(t_1, \ldots, t_n) \qquad\qquad f_n \in \Sigma$$

  - Λογικές προτάσεις (formulas)

$$\begin{aligned} A, B ::= \quad & P(t_1, \ldots, t_m) \mid A \Rightarrow B \mid A \wedge B \mid A \vee B \mid \\ & \top \mid \bot \mid \neg A \mid \forall\, x, A \mid \exists\, x,\ A \end{aligned} \qquad\qquad P_m \in \mathcal{P}$$

ΠΡΩΤΟΒΑΘΜΙΑ ΛΟΓΙΚΗ

- **Τυπική γλώσσα**
  - Ένα σύνολο από μεταβλητές $\mathcal{X}$ = { x, y, z, … }
  - Ένα προκαθορισμένο σύνολο από συναρτήσεις με συγκεκριμένο arity Σ
  - Ένα προκαθορισμένο σύνολο από κατηγορήματα $\mathcal{P}$
  - Όροι

$$t ::= x \mid \underline{f(t_1, \ldots, t_n)}$$

function name

$$f_n \in \Sigma$$

arity

  - Λογικές προτάσεις (formulas)

$$A, B ::= \underline{P(t_1, \ldots, t_m)} \mid A \Rightarrow B \mid A \wedge B \mid A \vee B \mid \\ \top \mid \bot \mid \neg A \mid \forall\, x, A \mid \exists\, x,\ A$$

$$P_m \in \mathcal{P}$$

predicate name

arity

ΠΑΡΑΔΕΙΓΜΑ: ΘΕΩΡΙΑ ΑΡΙΘΜΗΤΙΚΗΣ

- Θέτω
  - $\Sigma = \{\ O_0,\ \ S_1,\ \ +_2,\ \ *_2\ \}$

    arity
  - $\mathcal{P} = \{\ =_2\ \}$
  - Παράδειγμα λογικής πρότασης $\forall\ x,\ \forall\ y,\ x + y = y + x$

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ

- Αποδεικτικό σύστημα
- Μας επιτρέπει να παράγουμε judgements («κρίσεις»)
- Η απόδειξη ενός judgment είναι ένα derivation tree που παράγεται εφαρμόζοντας κανόνες συμπερασμού (inference rules)

$$\Gamma \vdash A$$

Υποθέσεις (ή περιβάλλον)
(σύνολο από λογικές προτάσεις)

Συμπέρασμα
(λογική πρόταση)

$$\Gamma = A_1, \ldots, A_n$$

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΑΞΙΩΜΑΤΑ

$$\frac{}{\Gamma, A, \Gamma' \vdash A}\,(\mathrm{ax})$$

Το περιβάλλον μπορεί να περιλαμβάνει λογικές προτάσεις τις οποίες **δεχόμαστε** ως αληθείς.

Αυτές είναι τα αξιώματα της **θεωρίας** την οποία αναπαριστούμε.

ΠΑΡΑΔΕΙΓΜΑ: ΑΞΙΩΜΑΤΑ ΑΡΙΘΜΗΤΙΚΗΣ

Peano Arithmetic

$$\forall\ x, \neg(S\ x = O)$$
$$\forall\ x,\ \forall\ y,\ S\ x = \ S\ y \Rightarrow x = y$$

$$\forall\ x,\ x + 0 = x$$
$$\forall\ x,\ \forall\ y,\ S\ x + y = S(x + y)$$

$$\forall\ x,\ x * 0 = 0$$
$$\forall\ x\ \forall\ y,\ S\ x * y = x * y + x$$

$$A(0) \Rightarrow (\forall\ x, A(0) \Rightarrow A(S(x))) \Rightarrow \forall\ x,\ A(x)$$

$$\forall\ x,\ x = x$$
$$\forall\ x\ y,\ x = y \Rightarrow y = x$$
$$\forall\ x\ y\ z,\ x = y \Rightarrow y = z \Rightarrow x = z$$

Άλλα παραδείγματα **θεωριών πρώτου βαθμού**:
Presburger arithmetic,
Zermelo-Fraenekel set theory,
Group theory, …

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΚΑΝΟΝΕΣ ΣΥΜΠΕΡΑΣΜΟΥ

- **Συνεπαγωγή**

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}(\Rightarrow_{\mathrm{E}}) \qquad\qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}(\Rightarrow_{\mathrm{I}})$$

- **Σύζευξη**

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}(\wedge^{\mathrm{l}}_{\mathrm{E}}) \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}(\wedge^{\mathrm{r}}_{\mathrm{E}}) \qquad\qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}(\wedge_{\mathrm{I}})$$

Για κάθε λογικό σύνδεσμο: κανόνας εισαγωγής (**introduction rule**),
κανόνας εξάλειψης (**elimination rule**)

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΚΑΝΟΝΕΣ ΣΥΜΠΕΡΑΣΜΟΥ

- **Διάζευξη**

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}(\vee_{\mathrm{E}}) \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}(\vee_{\mathrm{I}}^{\mathrm{l}}) \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}(\vee_{\mathrm{I}}^{\mathrm{r}})$$

- **Άρνηση**

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}(\neg_{\mathrm{E}}) \qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}(\neg_{\mathrm{I}})$$

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΚΑΝΟΝΕΣ ΣΥΜΠΕΡΑΣΜΟΥ

- **True**

$$\frac{}{\Gamma \vdash \top}(\top_{\mathrm{I}})$$

- **False**

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}(\bot_{\mathrm{E}})$$

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΚΑΝΟΝΕΣ ΣΥΜΠΕΡΑΣΜΟΥ

- **True**

Can't eliminate True

$$\frac{}{\Gamma \vdash \top}(\top_{\mathrm{I}})$$

- **False**

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}(\bot_{\mathrm{E}})$$

Can't introduce False

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΚΑΝΟΝΕΣ ΣΥΜΠΕΡΑΣΜΟΥ

- Καθολικός ποσοδείκτης

$$\frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A[t/x]} \ (\forall_{\mathrm{E}})$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A} \ (\forall_{\mathrm{I}})$$

Υπό τη συνθήκη ότι $x \notin \mathrm{FV}(\Gamma)$

- Υπαρξιακός ποσοδείκτης

$$\frac{\Gamma \vdash \exists x.A \qquad \Gamma, A \vdash B}{\Gamma \vdash B} \ (\exists_{\mathrm{E}})$$

Υπό τη συνθήκη ότι $x \notin \mathrm{FV}(\Gamma) \cup \mathrm{FV}(B)$

$$\frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x.A} \ (\exists_{\mathrm{I}})$$

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΚΑΝΟΝΕΣ ΣΥΜΠΕΡΑΣΜΟΥ

- Καθολικός ποσοδείκτης

$$\frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A[t/x]}\ (\forall_{\mathrm{E}})$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\ (\forall_{\mathrm{I}})$$

Υπό τη συνθήκη ότι $x \notin \mathrm{FV}(\Gamma)$

Αντικατάσταση της μεταβλητής **x** από με τον όρο **t**

- Υπαρξιακός ποσοδείκτης

$$\frac{\Gamma \vdash \exists x.A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ (\exists_{\mathrm{E}})$$

Υπό τη συνθήκη ότι $x \notin \mathrm{FV}(\Gamma) \cup \mathrm{FV}(B)$

$$\frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x.A}\ (\exists_{\mathrm{I}})$$

Ελεύθερες μεταβλητές (**f**ree **v**ariables)

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΚΑΝΟΝΕΣ ΣΥΜΠΕΡΑΣΜΟΥ

- Καθολικός ποσοδείκτης

$$\frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A[t/x]}\ (\forall_{\mathrm{E}}) \qquad\qquad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\ (\forall_{\mathrm{I}}) \qquad x \notin \mathrm{FV}(\Gamma)$$

- Υπαρξιακός ποσοδείκτης

Αντικατάσταση της μεταβλητής **x** από με τον όρο **t**

$$x \notin \mathrm{FV}(\Gamma) \cup \mathrm{FV}(B)$$

$$\frac{\Gamma \vdash \exists x.A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\ (\exists_{\mathrm{E}}) \qquad\qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x.A}\ (\exists_{\mathrm{I}})$$

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΑΠΟΔΕΙΞΗ

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \land B \vdash A \land B}\ (\mathrm{ax})}{A \land B \vdash A}\ (\land_{\mathrm{E}})}{A \land B \vdash A \lor B}\ (\lor_{\mathrm{I}}^{\mathrm{l}})}{\vdash A \land B \Rightarrow A \lor B}\ (\Rightarrow_{\mathrm{I}})$$

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ

- **Συντακτικός** τρόπος παραγωγής θεωρημάτων για μια θεωρία πρώτου βαθμού
- Είναι τα θεωρήματα **σωστά**;
- **Τι σημαίνει** σωστά;

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ

- **Συντακτικός** τρόπος παραγωγής θεωρημάτων για μια θεωρία πρώτου βαθμού
- Είναι τα θεωρήματα **σωστά**;
- **Τι σημαίνει** σωστά;
- Μια θεωρεία που περιγράφεται από ένα σύνολο αξιωμάτων Γ είναι συνεπής αν $\Gamma \nvdash A \wedge \neg A$

ΛΟΓΙΚΗ ΠΡΩΤΟΥ ΒΑΘΜΟΥ: ΣΗΜΑΣΙΟΛΟΓΙΑ

- **Σημασιολογική προσέγγιση:** απόδοση νοήματος στα σύμβολα της γλώσσας
- Πώς; Ορίζω ένα μοντέλο $\mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle$
  - $\mathcal{D}$ ένα (μη κενό) σύνολο. Ονομάζεται **domain.**
  - Οι όροι της γλώσσας θα απεικονιστούν σε στοιχεία του domain
  - $\mathcal{I}$ ερμηνεία (interpretation)
    - Για κάθε $f_n \in \Sigma$ μία συνάρτηση $[f] \in \mathcal{D}_n \to \mathcal{D}$
    - Για κάθε $P_n \in \mathcal{P}$ ένα σύνολο $[P] \subseteq \mathcal{D}_n$

$$\mathcal{D}_n \stackrel{\text{def}}{=} \underbrace{\mathcal{D} \times \cdots \times D}_{n \text{ times}}$$

ΛΟΓΙΚΗ ΠΡΩΤΟΥ ΒΑΘΜΟΥ: ΣΗΜΑΣΙΟΛΟΓΙΑ

- Έστω μια ανάθεση μεταβλητών $\sigma \in \mathcal{X} \to \mathcal{D}$
- Ορίζω μια συνάρτηση που αποδίδει τιμές του $\mathcal{D}$ στους όρους της γλώσσας
- Πως; Με αναδρομή (structural recursion) στους όρους!

$$\begin{aligned} [\![x]\!]_\sigma &= \sigma(x) \\ [\![f(t_1, \ldots, t_n)]\!]_\sigma &= [f]([\![t_1]\!]_\sigma, \ldots, [\![t_n]\!]_\sigma) \end{aligned}$$

ΠΑΡΑΔΕΙΓΜΑ: ΑΡΙΘΜΗΤΙΚΗ

- Αν
  - $\Sigma = \{\ O_0,\ S_1,\ +_2,\ *_2\ \}$

    $\mathcal{P} = \{\ =_2\ \}$
- Ορίζω

$$\begin{aligned} [O] &\stackrel{\text{def}}{=} 0 \\ [S] &\stackrel{\text{def}}{=} succ \\ [+] &\stackrel{\text{def}}{=} + \\ [*] &\stackrel{\text{def}}{=} * \end{aligned}$$

$$[=] \stackrel{\text{def}}{=} \{(x, x) \mid x \in \mathcal{D}\}$$

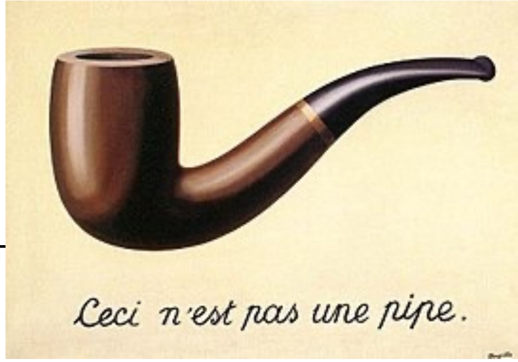
ΠΑΡΑΔΕΙΓΜΑ: ΑΡΙΘΜΗΤΙΚΗ

- Αν
  - $\Sigma = \{\ O_0,\ S_1,\ +_2,\ *_2\ \}$

    $\mathcal{P} = \{\ =_2\ \}$
- Ορίζω

$$
\begin{aligned}
[O] &\stackrel{\text{def}}{=} 0 \\
[S] &\stackrel{\text{def}}{=} succ \\
[+] &\stackrel{\text{def}}{=} + \\
[*] &\stackrel{\text{def}}{=} *
\end{aligned}
\qquad\qquad
[=] \stackrel{\text{def}}{=} \{(x, x) \mid x \in \mathcal{D}\}
$$

Διαφορετικά!



ΠΑΡΑΔΕΙΓΜΑ: ΑΡΙΘΜΗΤΙΚΗ

- Τότε

$$
\begin{aligned}
\llbracket S(S(S(S(SO)))))*(x+S(SO))\rrbracket_{x\mapsto 5} &= \\
\llbracket S(S(S(S(SO)))))\rrbracket_{x\mapsto 5} * (\llbracket x\rrbracket_{x\mapsto 5} + \llbracket S(SO))\rrbracket_{x\mapsto 5} &= \\
succ(succ(succ(succ(succ(0))))) * (5 + succ(succ(0))) &= \\
42 &
\end{aligned}
$$

ΛΟΓΙΚΗ ΠΡΩΤΟΥ ΒΑΘΜΟΥ: ΣΗΜΑΣΙΟΛΟΓΙΑ

- Ορίζω μία συνάρτηση που αποδίδει τιμές αλήθειας στις προτάσεις της γλώσσας
- Πως; Με αναδρομή (structural recursion) στις λογικές προτάσεις!

$$
\begin{aligned}
[\![P(t_1, \ldots, t_m)]\!]_\sigma &= ([\![t_1]\!]_\sigma, \ldots, [\![t_n]\!]_\sigma) \in [P] \\
[\![\top]\!]_\sigma &= \textbf{true} \\
[\![\bot]\!]_\sigma &= \textbf{false} \\
[\![A \wedge B]\!]_\sigma &= [\![A]\!]_\sigma \ \textbf{and} \ [\![B]\!]_\sigma \\
[\![A \vee B]\!]_\sigma &= [\![A]\!]_\sigma \ \textbf{or} \ [\![B]\!]_\sigma \\
[\![\forall\, x, A]\!]_\sigma &= \textbf{forall} \ v, [\![A]\!]_{\sigma[x \mapsto v]} = \textbf{true} \\
[\![\exists\, x, A]\!]_\sigma &= \textbf{exists} \ v, [\![A]\!]_{\sigma[x \mapsto v]} = \textbf{true}
\end{aligned}
$$

ΛΟΓΙΚΗ ΠΡΩΤΟΥ ΒΑΘΜΟΥ: ΛΟΓΙΚΗ ΕΓΚΥΡΟΤΗΤΑ

- Μια λογική πρόταση A είναι **έγκυρη σε ένα μοντέλο** $\mathcal{M}$ όταν
  - Για κάθε $\sigma \in \mathcal{X} \to \mathcal{D}$ ισχύει $[\![A]\!]_\sigma = \mathbf{true}$
  - Συμβολίζεται $\mathcal{M} \models A$

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΣΥΝΕΠΕΙΑ

- Έστω $\Gamma = A_1, \ldots, A_n$
- Συνέπεια (**soundness**)
  - Αν $\Gamma \vdash A$ και $\mathcal{M} \models \Gamma$ τότε $\mathcal{M} \models A$

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΠΛΗΡΟΤΗΤΑ

- Έστω $\Gamma = A_1, \ldots, A_n$
- Πληρότητα (Gödel's **Completeness** Theorem)
  - Αν για κάθε $\mathcal{M}$, $\mathcal{M} \models \Gamma$ συνεπάγεται $\mathcal{M} \models A$
  - Τότε: $\Gamma \vdash A$
  - Ισοδύναμα: $\Gamma \vdash A$ ή $\mathcal{M} \models \Gamma, \neg A$

ΦΥΣΙΚΗ ΑΠΑΓΩΓΗ: ΜΗ ΠΛΗΡΟΤΗΤΑ

- Έστω $\Gamma = A_1, \ldots, A_n$ ένα **συνεπές** σύνολο προτάσεων ικανών να περιγράψουν τα τα αξιώματα της αριθμητικής.

Πρώτο Θεώρημα Μη Πληρότητας Gödel

- Υπάρχει A τέτοιο ώστε ούτε $\Gamma \vdash A$ ούτε $\Gamma \vdash \neg A$

- **Δεύτερο** Θεώρημα Μη Πληρότητας Gödel
  - Λέμε ότι το Γ είναι συνεπές αν για κάθε A, $\Gamma \nvdash A \wedge \neg A$
  - Το παραπάνω μπορεί να κωδικοποιηθεί σαν λογική πρόταση στην ίδια τη γλώσσα (Gödel numberings). Έστω $\mathsf{Con}(\Gamma)$.
  - Τότε $\Gamma \nvdash \mathsf{Con}(\Gamma)$

ΑΠΟΦΑΝΣΙΜΟΤΗΤΑ

- Υπάρχει αποτελεσματική υπολογιστική διαδικασία που να μπορεί να αποφανθεί για την αλήθεια μιας πρότασης στην λογική πρώτης τάξης;
- Κάποιες θεωρίες είναι **αποφάνσιμες**
  - Π.χ. Presburger arithmetic (αριθμητική με πρόσθεση και ισότητα)
- Κάποιες θεωρίες είναι **μη αποφάνσιμες**
  - Π.χ. Peano arithmetic
  - Οποιαδήποτε θεωρία με ισότητα και τουλάχιστον μια ακόμα σχέση με δύο ορίσματα

SMT SOLVERS

- SMT = Satisfiability modulo theories
- Πρόβλημα **ικανοποιησιμότητας**: Υπάρχει ανάθεση μεταβλητών που να κάνει το A αληθές;
  - Γενικά **μη αποφάνσιμο** αλλά υπάρχουν αποφάνσιμα υποσύνολα
  - Το A είναι **μη ικανοποιήσιμο** αν και μόνο αν το $\neg A$ είναι **έγκυρο** (γιατί;)

- SMT solvers:
  - Εργαλεία για επίλυση του προβλήματος της ικανοποιησιμότητας για λογική πρώτης τάξης
  - Εφαρμογές σε constraint satisfaction προβλήματα, ανάλυση προγραμμάτων, επαλήθευση προγραμμάτων
  - Z3, CVC5, Bitwuzla, …
  - Z3 playground https://jfmc.github.io/z3-play/

ΣΧΕΣΗ ΜΕ ΓΛΩΣΣΕΣ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ

- **Συντακτική αναλογία** με συστήματα τύπων
  - Βλ. Curry-Howard Isomorphism
- **Αξιωματική σημασιολογία** (coming up next)
  - Αποδεικτικό σύστημα για προδιαγραφές ενός προγράμματος
- Χρήση **SMT solvers** στην **ανάλυση** π**ρογραμμάτων**