Contents

0.1 Úvod

0.2 Počítačom asistované dokazovanie

0.3 Prirodzená intuionistická logika

0.3.1 Formalizovanie dôkazu

Dôkaz z teórie usporiadania. Tak ako je Program = Proof

Otázka ohľadom konzistentnosti dôkazu.

0.3.2 Prirodzená dedukcia

Theorem 1 (Výroková premenná, formula)**.** *Majme spočítateľnú množinu $\mathcal{X}$ výrokových premenných. Množina výrokov alebo formúl $\mathcal{A}$ generovanú nasledovnou gramatikou:*

$$A, B ::= X|A \implies B|A \wedge B|A \vee B|\neg A|\top|\bot \tag{1}$$

Kde $X \in \mathcal{X}$ reprezentuje výrokovú premennú, a $A, B \in \mathcal{A}$ výrok.

V prípade nasledovného výroku je precedencia $\neg$ vyššia ako $\vee$ alebo $\wedge$ a tá je vyššia ako $\implies$. Binárne operátory sú asociatívne z prava.

$$\neg A \wedge B \wedge C \implies A \vee B$$
$$(\neg A \wedge (B \wedge C)) \implies (A \vee B)$$

Theorem 2. *Kontextom(systém predpokladov) rozuemieme zoznam výrokov značených*

$$\Gamma = P_1, \dots, P_n \tag{2}$$

Dedukciou nazývame dvojicu pozostávajúcu z kontextu a výroku.

$$\Gamma \vdash A \tag{3}$$

Výraz čítame ako A je možné dokázať zo systému predpokladov Γ.

Theorem 3. *Dedukčné pravidlo pozostáva z množiny dedukcií Γ_i ktoré nazývame prepokladom. Dolnú časť dedukčného pravidla Γ nazývame záverom.*

$$\frac{\Gamma_1 \vdash A_1 \quad \dots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A} \tag{4}$$

Pravidlá prirodzenej intuicionistickej logiky:

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

$$\frac{\Gamma \vdash A \implies B \quad \Gamma \vdash A}{\Gamma : B} \ (\implies_E) \qquad \frac{\Gamma, A \vdash B}{\Gamma : B} \implies_I$$

$$\frac{\Gamma, A \vdash B}{\Gamma : A} \ (\wedge_E^l) \ \frac{\Gamma, A \vdash B}{\Gamma : B} \ (\wedge_E^r) \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \ (\wedge_I)$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \ (\vee_E) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \ (\vee_I^r) \ \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \ (\vee_I^l)$$

$$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \bot} \ (\neg_E) \qquad \frac{\Gamma, A \vdash \bot \quad \Gamma \vdash A}{\Gamma \vdash \neg A} \ (\neg_I)$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A} \ (\bot_E)$$

V prípade že tieto pravidlá čítame zhora nadol hovoríme o dedukcii. Ak čítame pravidlá zdola nahor hovoríme o indukčnom spôsobe.

Theorem 4. *Fragmentom intuionistickej logiky nazývame, systém ktorý dostaneme ak ho obmedzíme len na niektoré z predchádzajúcich pravidiel.*

Theorem 5. *Implikačným fragmentom intuionistickej logiky dostaneme v prípade ak formuly budú tvorené gramatikou*

$$A, B ::= X | A \implies B \tag{5}$$

a pravidlami (ax), ($\implies_E$), ($\implies_I$)

V prípade že chceme aby výrokove formuly korenšpondovali s typmi ktoré su prezentované neskôr. Ich booleova reprezentácia s hodnotami $1, 0$ je nahradená otázkou existencie prvkov v množine. V prípade implikácie o existencii funkcie v množine. Funkcie v programoch ale môžu mať pri rovnakých vstupoch a výstupoch mať rôznu výpočtovú zložitosť. Dôvod prečo by sme sa mali pozerať na dôkazy(podľa publikácie Gir11) v troch rovinách.

- 1. Booleovský - tvrdenia sú booleovské hodnoty, zaujímame sa o dokázateľnosť tvrdenia
- 2. Existenčný - tvrdenia sú množiny, aké funkcie môžu byť
- 3. Úmyselný/Zámerový(Intentional) - zaujímame sa o zložitosť vytvoreného dôkazu a ako sa zjednoduší cez (cut eliminitation)

0.3.3 Intuicionizmus

Jedným zo smerov matematickej filozofie týkajucej sa rozvoja teórie je konštruktivizmus. Konštruktivizmus hovorí o potrebe nájsť alebo zostrojiť matematický objekt k tomu aby bola dokázaná jeho existencia. Jeden z motivačných príkladov takéhoto prístupu je možnosť dokázania pravdivosti výroku $p \vee \neg p$ cez dôkaz sporom $\neg p$ ktorý nehovorí ako zostrojiť objekt p len o jeho existencii. Tento smer tvorí viacero "škôl" okrem iných finitizmus, predikativizmus, intuicionizmus. Intuitionizmus je teda konštruktívny prístup k matematike v duchu Brouwera(1881-1966) a Heytinga(1898-1980). Filozofickým základom tochto prístupu princíp že matematika je výtvorom mentálnej činnosti a nepozostáva z výsledkov formálnej manipulácie symbolov ktoré sú iba sekundárne. Jedným z princípov intuicionizmus je odmietnutie tvrdenia postulátu klasickej logiky a to zákona vylúčenia tretieho.

$$p \vee \neg p \tag{6}$$

Dôvodom je z konštruktívneho pohľadu nezmyselnosť uvažovania nad pravdivosťou výroku nezávisle od uvažovaného tvrdenia. Výrok je teda pravdivý ak existuje dôkaz o jeho pravidovsti a nepravdivé ak existuje dôkaz ktorý vedie k sporu.

- konjukcii $p \wedge q$ ako o výroku hovoriacom o existencii dôkazov p a zároveň q,
- disjunkcii $p \wedge q$ ako existencii konštrukcii dôkazu jedného z výrokov p, q,

- $p \implies q$ je metóda(funkcia) transformácie každej konštrukcie p k dôkazu q,
- neexistencie dôkazu nepravdivého tvrdenia, iba dôkazu ktorý vedie k sporu $p \implies \perp$
- konštrukcia $\neg p$ je metóda ktorá vytvorí každú konštrukciu p na neexistujúci objekt

konjukcii $A \wedge B$ ako $A \times B$ $A \vee B$ ako $A \sqcup B$ disjunktne zjednotenie $\neg A = A \implies \perp$ existencie kontrapríkladu

0.4 Lambda kalkulus

Theorem 6. *Majme nekonečnú množinu $\mathcal{X} = x, y, z, \ldots$ ktorých elementy nazývame premenné. Množinu Λ tvorenú λ-termínmy je potom generovaná nasledovnou gramatikou:*

$$t, u ::= x|tu|\lambda x.t \tag{7}$$

Význam jednotlivých termínov je

$$\begin{aligned} x &\text{ - je premennou} \\ tu &\text{ - je aplikáciou termínu } t \text{ s argumentom } u \\ \lambda x.t &\text{ - je abstrakciou } t \text{ nad } x \end{aligned}$$

Príklady lambda termínov:

$$\begin{aligned} &tx \\ &(\lambda y.\lambda x.ty)) \\ &(\lambda y.yx)(\lambda x.x) \\ &tuv = (tu)v \end{aligned}$$

Aplikácia λ-termínov je implicitne aplikovaná zľava.

Pri výraze

$$\lambda x.tx = \lambda x.(tx) \tag{8}$$

je precedencia aplikácie vyššia ako abstrakcia.

A abstrakciu s troma argumentmi je možné prepísať do troch po sebe nasledujúcich.

$$\lambda xyz.t = \lambda x.\lambda y.\lambda z.t \tag{9}$$

Theorem 7. *Premenná x sa vo výraze*

$$\lambda x.t \tag{10}$$

abstrakciou viaže na termín t. O premennej x hovoríme že je viazaná. O premenných ktoré nie sú viazané sú voľné.

$$\begin{aligned} VP(x) &= x \\ VP(\lambda x.t) &= VP(t) \setminus \{x\} \\ VP(tv) &= VP(t) \cup VP(v) \end{aligned}$$

Theorem 8. *Premenovaním nazývame nahradenie voľných premenných v termíne.*

$$t\{y/x\} \tag{11}$$

V termíne t je premenovaná premenná x za y.

0.4.1 α-ekvivalencia

Theorem 9. *O výrazov hovoríme že sú alfa-ekvivalentné ak sa výrazy rovnajú až na premenovanie.*

Theorem 10. *O substutícii hovoríme pri nahradení jednej premenej druhou.*

$$t[y/x] \tag{12}$$

Nahradenie je silnejšie a vieme nahradiť aj premmenné viazanné abstrakciou.

0.4.2 β-ekvivalencia

$$\frac{}{(\lambda x.t)u \to_\beta t[u/x]}\ (\beta_s) \qquad \frac{t \to_\beta t'}{(\lambda x.t)u \to_\beta t[u/x]}\ (\beta_\lambda)$$

$$\frac{t \to_\beta t'}{tu \to_\beta t'u}\ (\beta_l) \qquad \frac{u \to_\beta u'}{tu \to_\beta tu'}\ (\beta_r)$$

$$\dfrac{\dfrac{\dfrac{}{(\lambda y.y)x \to_\beta x}\ (\beta_s)}{(\lambda y.y)xz \to_\beta xz}\ (\beta_l)}{\lambda x.(\lambda y.y)xz \to_\beta \lambda x.xz}\ (\beta_\alpha) \tag{13}$$

Theorem 11. *Definujme rekurziu volania funkcie nasledovne*

$$f^0 x = x \tag{14}$$

$$f^n x = f(f^{n-1}x) \tag{15}$$

$$\tag{16}$$

Potom Churchove číslo c_n je λ-termín

$$c_n = \lambda s.\lambda z.s^n(z) \tag{17}$$

Prirodzené čísla je potom definovať

$$0 = \lambda fx.x$$

$$1 = \lambda fx.fx$$

$$1 = \lambda fx.f(fx)$$

$$2 = \lambda fx.f(f(fx))$$

$$
\begin{aligned}
succ(n) &= (\lambda nfx.f(nfx))(\lambda fx.f^n x) \\
&\rightarrow_\beta \lambda fx.f((\lambda fx.f^n x)fx) \\
&\rightarrow_\beta \lambda fx.f((\lambda x.f^n x)x) \\
&\rightarrow_\beta \lambda fx.f(f^n x) \\
&= \lambda fx.f^{n+1}x \\
&= n+1
\end{aligned}
$$

Operáciu sčítania je potom možné definovať vykonať

Theorem 12. $f_+ = \lambda x.\lambda y.\lambda s.\lambda z.xs(ysz)$

Podobným spôsobom môžeme vytvoriť

Theorem 13.

$$
\begin{aligned}
True &= \lambda xy.x \\
False &= \lambda xy.y
\end{aligned}
$$

$$
if = \lambda bxy.bxy
$$

$$
\begin{aligned}
if \text{ True } tu = (\lambda bxy.bxy)(\lambda xy.x)tu &\rightarrow_\beta (\lambda xy.(\lambda xy.x)xy)tu \\
&\rightarrow_\beta (\lambda y.(\lambda xy.x)ty)u \\
&\rightarrow_\beta (\lambda xy.x)tu \\
&\rightarrow_\beta (\lambda y.t)u \\
&\rightarrow_\beta t
\end{aligned}
$$

Theorem 14. *Jednoduchý λ kalkulus je ekvivalentný výpočtovej sile turingovho stroja. Bez dôkazu*

0.5 Typovo jednoduchý λ-calculus

Typový lambda calculus je rozšírením jednoduchého o typy

Theorem 15. *Majme množinu U spočítateľnú nekonečnú abecedu obsahujúcu typové premenné. Potom množina Π obsahuje reťazce jednoduchých typov ktoré su generované gramatikov:*

$$
\Pi ::= U|(\Pi \rightarrow \Pi) \tag{18}
$$

Theorem 16. *Kontextom rozumieme množinu C tvoriacu*

$$
x_1 : \tau_1, \ldots, x_n : \tau_n \tag{19}
$$

kde $\tau_1, \ldots, \tau_n \in \Pi$ *a* $x_1, \ldots, x_n \in$ *Koobor kontextu je množina obsahujúca*

$$domain(\Gamma) = x_1, \ldots, x_n \tag{20}$$

Oboor kontextu je množina obsahujúca

$$range(\Gamma) = \tau \in \Pi | (x : \tau) \in \Gamma \tag{21}$$

Príklady generované gramatikou

- $\vdash \lambda x.x : \sigma \to \sigma$
- $\vdash \lambda x.\lambda y.x : \sigma \to \tau \to \sigma$
- $\vdash \lambda x.\lambda y.\lambda z.xz(yz) : (\sigma \to \tau \to \rho) \to (\rho \to \tau) \to \sigma \to \rho$

Theorem 17. *Postupnosť je trojica značená*

$$\Gamma \vdash t : A \tag{22}$$

tvorená kontextom Γ*,* λ*-termínom* t *a typom* A*.*

Termín t je typu A ak v kontexte Γ ak je postupnosť derivovateľná pomocou pravidiel:

- ax: v kontexte x je typu A
- $\xrightarrow{I}$: ak je x typu A, t je typu B, potom funkcia $\lambda x.t$ ktorá asociuje x t je typu $A \to B$
- $\xrightarrow{E}$: daná je funkcia t je typu $A \to B$ a argument u je typu A, vysledok aplikácia tu je typu B

$$\frac{}{\Gamma \vdash x : \Gamma(x)}\ \text{ax}$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \lambda x^A.t : A \to B}\ \xrightarrow{I} \qquad \frac{\Gamma \vdash t : A \to B \quad \Gamma \vdash u : A}{\Gamma \vdash tu : B}\ \xrightarrow{E}$$

0.6 Curry-Howardov izomorfizmus

Intuinistická logika	Typovo jednoduchý λ kalkulus
termín	dôkaz
typová premenná	propozičná premenná

Theorem 18. *Curry-Howard isomorphism*

- *If* $\Gamma \vdash M : \varphi$ *potom* $|\Gamma| \vdash \varphi$*.*
- *If* $\Gamma \vdash \varphi$ *potom existuje* $M \in \Lambda_\Pi$ *také že* $\Delta \vdash M : \varphi$*, kde* $\Delta = (x_\varphi : \varphi) | \varphi \in \Gamma$

0.7 Lean-theorem-prover

0.7.1 Constracting proof

0.7.2 Forward proofs

assume

calc

fix

have

let

show

0.7.3 Backward proofs

cc

clear

exact

induction

intro

refl

refl

Inductive types