Izomorfizm Curry'ego-Howarda: obliczenia, dowody, programy

Tomasz Połacik

Letnia Szkoła Instytutu Matematyki
wrzesień 2014

Obliczalność: Idee

D. Hilbert

- X Problem — *Entscheidungsproblem*, 1900.

  „problem decyzyjny”

- Program Hilberta — *Neubegründung der Mathematik*, “Abhandlungen aus dem math. Seminar der Hamburgischen Univ.”, 1922.

  „finitystyczne procedury dowodowe”

Obliczalność: Trzy drogi

- funkcje rekurencyjne — K. Gödel, J. Herbrand 1930;
- “a-machine”, automatic machine — A. Turing, 1936;
- rachunek lambda — A. Church, 1936.

Funkcje rekurencyjne

Klasa funkcji rekurencyjnych $\mathcal{R}$ jest najmniejszą klasą, która zawiera

- zero,
- następnik,
- rzutowania

i jest domknięta na:

- złożenia,
- schemat rekursji,
- operację minimum.

Arytmetyka a funkcje rekurencyjne

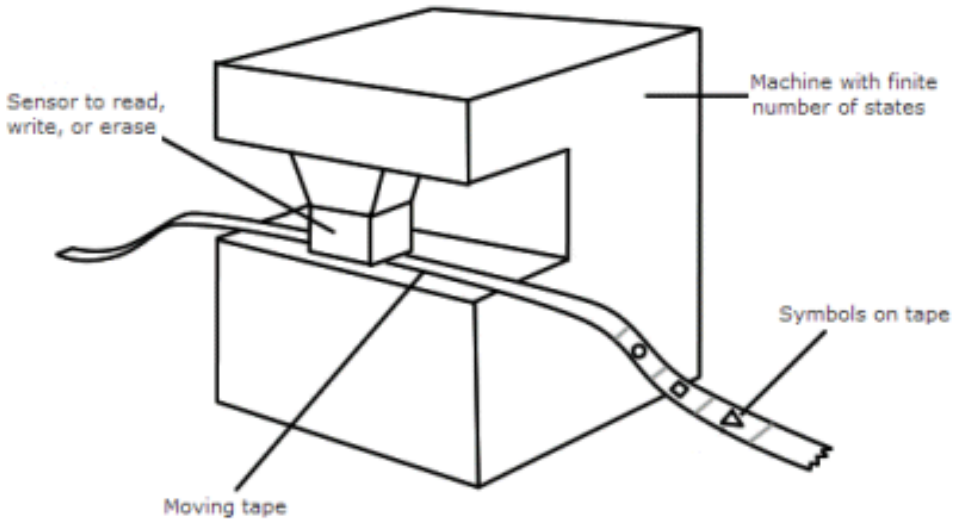
Twierdzenie

Wszystkie funkcje rekurencyjne są reprezentowalne w Arytmetyce Peano.

Maszyny Turinga

Wond'rous Machine!

A Turing machine is a theoretical generalized computer, composed of a tape on which symbols representing instructions are imprinted. The tape can move backwards and forwards in the machine, which can read the intructions and write the resultant output back onto the tape.



Źródło: `http://www.storyofmathematics.com`

Maszyny Turinga a funkcje rekurencyjne

Twierdzenie

Klasa funkcji obliczalnych przez (uniwersalną) maszynę Turinga pokrywa się z klasą funkcji rekurencyjnych.

Rachunek lambda

λ-termy:

- zmienne: $x, y, z, \ldots,$
- λ-abstrakcja: $\lambda x.M$
- aplikacja: (MN)

β-redukcja:

- $(\lambda x.M)N \rightarrow_\beta M[x := N]$

Rachunek lambda

$$
\begin{aligned}
\mathbf{I} &= \lambda x\,.\,x \\
\mathbf{K} &= \lambda x \lambda y\,.\,x \\
\mathbf{S} &= \lambda x \lambda y \lambda z\,.\,xz(yz) \\
\omega &= \lambda x\,.\,xx
\end{aligned}
$$

β-redukcja

$$
\begin{array}{lcl}
\mathbf{I}\mathbf{K}z & = & ((\lambda x.x)\mathbf{K})z \\
 & \to_\beta & x[x := \mathbf{K}]z \\
 & \to_\beta & \mathbf{K}z \;=\; (\lambda y \lambda x\,.\,y)z \\
 & \to_\beta & \lambda x.z\;.
\end{array}
$$

β-redukcja

$$
\begin{aligned}
\omega\omega \quad &= \quad (\lambda x.xx)(\lambda x.xx) \\
&\to_\beta \quad (xx)[x := \lambda x.xx] \\
&\to_\beta \quad (x[x := \lambda x.xx])(x[x := \lambda x.xx]) \\
&\to_\beta \quad (\lambda x.xx)(\lambda x.xx) \;=\; \omega\omega \;.
\end{aligned}
$$

Twierdzenie Churcha-Rossera

Twierdzenie

Dla dowolnych λ-termów M, M_1, M_2 takich, że

$$M \to_\beta M_1 \quad \text{oraz} \quad M \to_\beta M_2$$

istnieje λ-term N taki, że

$$M_1 \to_\beta N \quad \text{oraz} \quad M_2 \to_\beta N.$$

Postać normalna λ-termu

Term N jest w postaci normalnej, gdy nie istnieje λ-term N_1 taki, że $N_1 \neq N$ oraz $N \rightarrow_\beta N_1$.

Arytmetyka w rachunku lambda

$$
\begin{aligned}
\mathbf{0} &= \lambda f \lambda x.x \\
\mathbf{1} &= \lambda f \lambda x.fx \\
\mathbf{2} &= \lambda f \lambda x.f(fx) \\
&\dots \\
\boldsymbol{n} &= \lambda f \lambda x \,.\, f^n(x) \\
&\dots \\
S &= \lambda n \lambda f \lambda x \,.\, f(nfx) \\
A &= \lambda m \lambda n \lambda f \lambda x \,.\, mf(nfx) \\
&\dots
\end{aligned}
$$

Arytmetyka w rachunku lambda

$$
\begin{aligned}
S\,\mathbf{2} &= (\lambda n \lambda f \lambda x.f(nfx))(\lambda f \lambda x.f(fx)) \\
&\to_\beta \lambda f \lambda x.f((\lambda f \lambda x.f(fx))fx) \\
&\to_\beta \lambda f \lambda x.f((\lambda x.f(fx))x) \\
&\to_\beta \lambda f.\lambda x.f(f(fx)) \\
&= \mathbf{3}
\end{aligned}
$$

λ-definiowalność

Dla dowolnej częściowej funkcji rekurencyjnej f istnieje λ-term F taki, że

- jeżeli $f(n_1, \ldots, n_k) = m$, to $F\boldsymbol{n}_1 \ldots \boldsymbol{n}_k \to_\beta \boldsymbol{m}$,
- jeżeli $f(n_1, \ldots, n_k) = m$ nie istnieje, to term $F\boldsymbol{n}_1 \ldots \boldsymbol{n}_k \to_\beta \boldsymbol{m}$ nie ma postaci normalnej.

Rachunek lambda a funkcje rekurencyjne

Twierdzenie

Wszystkie (częściowe) funkcje rekurencyjne są definiowalne w rachunku lambda.

Obliczalność a funkcje rekurencyjne

Teza Churcha

Zbiór funkcji typu $\mathbb{N}^k \to \mathbb{N}$ obliczalnych w intuicyjnym sensie pokrywa się ze zbiorem

- funkcji rekurencyjnych,
- funkcji obliczalnych przez Maszyny Turinga,
- funkcji definiowalnych w rachunku lambda.

Rachunek lambda z typami prostymi, $\lambda_{\rightarrow}$

Typy:

- Typy atomowe: $p, q, r, \ldots$.
- Jeżeli σ i τ są typami, to typem jest również wyrażenie $\sigma \rightarrow \tau$.

NB Zbiór typów pokrywa się ze zbiorem czysto implikacyjnych formuł logiki zdaniowej.

Rachunek lambda z typami prostymi, $\lambda_{\rightarrow}$

Otoczenie typowe:

- skończony zbiór par postaci

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

gdzie x_i są parami różnymi λ-zmiennymi, a τ_i są typami.

Rachunek lambda z typami prostymi, $\lambda_{\rightarrow}$

Asercja:

- trójka postaci

$$\Gamma \vdash M : \tau$$

gdzie Γ jest otoczeniem typowym, M jest λ-termem oraz τ jest typem.

Rachunek lambda z typami prostymi, $\lambda_{\rightarrow}$

Reguły systemu $\lambda_{\rightarrow}$:

$$\text{(Var)} \quad \frac{}{\Gamma, x : \tau \vdash x : \tau}$$

$$\text{(Abs)} \quad \frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash (\lambda x.M) : \sigma \rightarrow \tau}$$

$$\text{(App)} \quad \frac{\Gamma \vdash M : \sigma \rightarrow \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash (MN) : \tau}$$

Jednoznaczność

Twierdzenie

Jeżeli

$$\Gamma \vdash M : \sigma, \quad \Gamma \vdash N : \tau \quad \text{oraz} \quad M =_\beta N,$$

to $\sigma = \tau$.

Silna normalizacja

Twierdzenie

Jeżeli $\Gamma \vdash M : \sigma$, to istnieje skończony ciąg β-redukcji

$$M \to_\beta M_1 \to_\beta \cdots \to_\beta M_n \to_\beta N$$

taki, że N jest w postaci normalnej.

Przykłady

$$\vdash \mathbf{I} : \sigma \to \sigma$$

$$\vdash \mathbf{K} : \sigma \to (\tau \to \sigma)$$

$$\vdash \mathbf{S} : (\sigma \to (\tau \to \rho)) \to ((\sigma \to \tau) \to (\sigma \to \rho))$$

H. Curry, 1958

Istnieje ścisły związek miedzy logiką intuicjonistyczną i logiką kombinatorów.

Minimalna Logika Implikacyjna, $L_{\to}$

$$(\text{Ax}) \quad \frac{}{\Gamma, \tau \vdash \tau}$$

$$(\to\text{-I}) \quad \frac{\Gamma, \sigma \vdash \tau}{\Gamma \vdash \sigma \to \tau}$$

$$(\to\text{-E}) \quad \frac{\Gamma \vdash \sigma \to \tau \qquad \Gamma \vdash \sigma}{\Gamma \vdash \tau}$$

$\lambda_{\rightarrow}$ versus $L_{\rightarrow}$

$$\text{(Var)} \quad \frac{}{\Gamma, x : \tau \vdash x : \tau}$$

$$\text{(Abs)} \quad \frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash (\lambda x.M) : \sigma \rightarrow \tau}$$

$$\text{(App)} \quad \frac{\Gamma \vdash M : \sigma \rightarrow \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash (MN) : \tau}$$

$\lambda_{\to}$ versus $L_{\to}$

$$\text{(Ax)} \quad \frac{}{\Gamma, \cancel{x}: \tau \vdash \cancel{x}: \tau}$$

$$\text{($\to$-I)} \quad \frac{\Gamma, \cancel{x}: \sigma \vdash \cancel{M}: \tau}{\Gamma \vdash \cancel{(\lambda x.M)}: \sigma \to \tau}$$

$$\text{($\to$-E)} \quad \frac{\Gamma \vdash \cancel{M}: \sigma \to \tau \qquad \Gamma \vdash \cancel{N}: \sigma}{\Gamma \vdash \cancel{(MN)}: \tau}$$

$L_{\to}$

Nie istnieje domknięty λ-term typu $((p \to q) \to p) \to p$.

Prawo Peirce'a, $((p \to q) \to p) \to p$, nie jest dowodliwe w $L_{\to}$.

$L_{\rightarrow}$

Nie istnieje domknięty λ-term typu $((p \rightarrow q) \rightarrow p) \rightarrow p$.

Prawo Peirce'a, $((p \rightarrow q) \rightarrow p) \rightarrow p$, nie jest dowodliwe w $L_{\rightarrow}$.

$$L_{\rightarrow} \subsetneq CPL_{\rightarrow}$$

$L_{\to}$

Interpretacja klasyczna implikacji $\varphi \to \psi$:

- nie zachodzi φ lub zachodzi ψ.

Interpretacja intuicjonistyczna (BHK) implikacji $\varphi \to \psi$:

- każdy dowód formuły φ można przekształcić w dowoód formuły ψ.

$L_{\to}$

Interpretacja klasyczna implikacji $\varphi \to \psi$:

- nie zachodzi φ lub zachodzi ψ.

Interpretacja intuicjonistyczna (BHK) implikacji $\varphi \to \psi$:

- każdy dowód formuły φ można przekształcić w dowoód formuły ψ.

$$L_{\to} = IPL_{\to}.$$

Izomorfizm Curry'ego-Howarda

Dla dowolnego otoczenia typowego Γ:

$$|\Gamma| := \{\tau \in \mathcal{L}_{\rightarrow} : (x : \tau) \in \Gamma, \text{dla pewnego x}\}$$

Twierdzenie (W.A. Howard, 1969)

Jeżeli $\Gamma \vdash M : \varphi$ w systemie $\lambda_{\rightarrow}$, to $|\Gamma| \vdash \varphi$ w systemie $L_{\rightarrow}$.

Jeżeli $\Gamma \vdash \varphi$ w systemie $L_{\rightarrow}$, to istnieje takie otoczenie typowe Δ i λ-term M, że $|\Delta| = \Gamma$, oraz $\Delta \vdash M : \phi$ w systemie $\lambda_{\rightarrow}$.

Izomorfizm Curry'ego-Howarda, nieformalnie

$IPL_{\to}$-formuły $\cong$ $\lambda_{\to}$-typy

dowody w $IPL_{\to}$ $\cong$ λ-termy $\cong$ programy

Izomorfizm Curry'ego-Howarda, nieformalnie

$IPL_{\to}$-formuły $\cong$ $\lambda_{\to}$-typy

dowody w $IPL_{\to}$ $\cong$ λ-termy $\cong$ programy

Program wykonuje to, co opisuje związany z nim dowód.

Dowód opisuje to, co wykonuje związany z nim program.

Rozszerzenia Izomorfizmu Curry'ego-Howarda

- Pełny język logiki intuicjonistycznej.
- Językowe rozszerzenia logiki intuicjonistycznej.
- Logika intuicjonistyczna wyższych rzędów.
- Połączenia logiki intuicjonistycznej z logika klasyczną.