RACHUNEK λ

Wojciech Buszkowski

Zakład Teorii Obliczeń

Wydział Matematyki i Informatyki UAM

1. Czysty rachunek λ

Symbole

- zmienne: $x, y, z, x', y_1, \ldots$ i inne małe litery,

- operator λ (lambda-abstraktor),

- nawiasy (,) i kropka .

Przyjmujemy, że dany jest nieskończony, przeliczalny zbiór zmiennych V.

Definicja 1. (lambda-termy, krótko: termy) Termy proste to zmienne. Termy złożone są postaci (MN) (aplikacja M do N) i $(\lambda x.M)$ (lambda-abstrakcja termu M), gdzie M, N są termami.

Litery $M, N, P, Q, \ldots, X, Y, Z$ i inne duże litery to metazmienne dla termów.

Λ oznacza zbiór wszystkich lambda-termów.

Przykłady lambda-termów.

x, (xy), $((xy)z)$, $(\lambda x.(xy))$, $((\lambda x.(xy))z)$. Czwarty term jest lambda-abstrakcją termu (xy), a piąty aplikacją czwartego do z.

Interpretacja termów. Termy interpretujemy intuicyjnie jako funkcje dane w postaci procedur obliczania, a nie - jak w teorii mnogości - w postaci relacji argument-wartość (wejście-wyjście). Możliwa jest sytuacja, że różne procedury (termy) mają tę samą relację argument-wartość.

Oznaczenia.

Pomijamy zewnętrzne nawiasy, np. piszemy xy zamiast (xy).

W napisach postaci $M_1 M_2 \ldots M_n$ grupujemy nawiasy do lewej strony, np. $xyzu$ to term $((xy)z)u$.

W napisach postaci $\lambda x_1.\lambda x_2.\ldots.\lambda x_k.M$ grupujemy nawiasy do prawej strony, np. $\lambda x.\lambda y.\lambda z.M$ to term $\lambda x.(\lambda y.(\lambda z.M))$.

Piszemy $\lambda x_1 x_2 \ldots x_k.M$ zamiast $\lambda x_1.\lambda x_2 \ldots \lambda x_k.M$.

Ten term interpetujemy jako funkcję $k-$argumentową, która dowolnym wartościom zmiennych $x_1, \ldots, x_k$ przyporządkowuje wartość termu M dla tych wartości zmiennych.

Niech f oznacza funkcję zależną od dwóch argumentów x, y. W matematyce wartość tej funkcji zapisujemy $f(x, y)$, a w rachunku λ jako $f\,xy$. To znaczy, że f interpretujemy jako jednoargumentową funkcję, która dowolnemu argumentowi x przyporządkowuje jednoargumentową funkcję f_x, taką że $f_x(y) = f(x, y)$.

Takie reprezentowanie funkcji wieloargumentowych przez jednoargumentowe nazywa się po angielsku ‘currying’ od nazwiska: Haskell B. Curry.

Definicja 2. ($V(M)$ - zbiór zmiennych wolnych w termie M)

$V(x) = \{x\}$

$V(MN) = V(M) \cup V(N)$

$V(\lambda x.M) = V(M) - \{x\}$

Definicja 3. ($M[x/N]$ - wynik podstawienia termu N za zmienną x w termie M)

$x[x/N] \equiv N$

$y[x/N] \equiv y$ dla zmiennych y różnych od x

$(M_1 M_2)[x/N] \equiv M_1[x/N]M_2[x/N]$

$(\lambda x.M)[x/N] \equiv \lambda x.M$

$(\lambda y.M)[x/N] \equiv \lambda y.M[x/N]$, jeżeli $y \not\equiv x$, $y \notin V(N)$

$(\lambda y.M)[x/N] \equiv \lambda z.M[y/z][x/N]$, jeżeli $y \not\equiv x$, $y \in V(N)$, z jest dowolną zmienną nie występującą po lewej stronie równości.

Przykłady. $V(xy) = \{x, y\}$, $V(\lambda x.xy) = \{y\}$.

$(\lambda x.xy)[y/x] = \lambda z.zx$

Definicja 4. ($M[x_1/N_1, \ldots, x_k/N_k]$ - wynik równoczesnego podstawienia N_i za x_i dla $i = 1, \ldots, k$ w termie M)

$M[x_1/N_1, \ldots, x_k/N_k] \equiv M[x_1/z_1] \ldots [x_k/z_k][z_1/N_1] \ldots [z_k/N_k]$,

gdzie $z_1, \ldots, z_k$ są różnymi zmiennymi nie występującymi po lewej stronie równości.

Przykład.

$(xy)[x/y, y/\lambda z.z] \equiv (z_1z_2)[z_1/y][z_2/\lambda z.z] \equiv (yz_2)[z_2/\lambda z.z] \equiv y(\lambda z.z)$

Definicja 5. Określamy relację: $M \equiv_\alpha N$, jeżeli N powstaje z M przez pewną liczbę zastąpień podtermów postaci $\lambda x.P$ przez $\lambda y.P[x/y]$, gdzie y jest zmienną nie występującą w $\lambda x.P$.

Jeżeli $M \equiv_\alpha N$, to mówimy, że N jest $\alpha-$wariantem termu M.

Fakt 1. Relacja $\equiv_\alpha$ jest relacją równoważności na zbiorze Λ, tzn. jest zwrotna ($M \equiv_\alpha M$), symetryczna (jeżeli $M \equiv_\alpha N$, to $N \equiv_\alpha M$) i przechodnia (jeżeli $M \equiv_\alpha N$ i $N \equiv_\alpha P$, to $M \equiv_\alpha P$).

Dowód. Zwrotność i przechodniość są oczywiste. Symetria nie jest oczywista, ponieważ po zamianie $\lambda x.P$ na $\lambda y.P[x/y]$, gdzie y nie występuje w $\lambda x.P$, niekoniecznie możemy zamienić z powrotem $\lambda y.P[x/y]$ na $\lambda x.P$, ponieważ x może występować w $\lambda y.P[x/y]$ jako zmienna związana.

Można jednak zamienić wszystkie związane wystąpienia x w $\lambda y.P[x/y]$ na nową zmienną tworząc term $\lambda y.P'[x/y]$, następnie zastąpić $\lambda y.P'[x/y]$ przez $\lambda x.P'[x/y][y/x]$, czyli $\lambda x.P'$, a na koniec zamienić tę nową zmienną na x krok po kroku (od termów większych do mniejszych). Q.E.D.

Przykład. $\lambda x.x(\lambda x.x(\lambda x.x)) \equiv_\alpha \lambda y.y(\lambda x.x(\lambda x.x))$.

$\lambda y.y(\lambda x.x(\lambda x.x))$, $\lambda y.y(\lambda z.z(\lambda x.x))$, $\lambda y.y(\lambda z.z(\lambda z.z))$, $\lambda x.x(\lambda z.z(\lambda z.z))$, $\lambda x.x(\lambda x.x(\lambda z.z))$, $\lambda x.x(\lambda x.x(\lambda x.x))$

W rachunku λ dowodzimy równości $M = N$, interpretowane jako równość wartości termów M i N.

Aksjomaty.

(α) $M = N$, jeżeli $M \equiv_\alpha N$ ($\alpha-$konwersja)

(β) $(\lambda x.M)N = M[x/N]$ ($\beta-$konwersja)

(η) $\lambda x.Mx = M$, jeżeli $x \notin V(M)$ ($\eta-$konwersja)

Reguły. (Id) $M = M$ (tutaj niepotrzebne, bo mamy (α))

$$\text{(sym)}\ \frac{M = N}{N = M} \quad \text{(tran)}\ \frac{M = N,\ N = P}{M = P}$$

$$\text{(l-con)}\ \frac{M = N}{PM = PN} \quad \text{(r-con)}\ \frac{M = N}{MP = NP}$$

$$(\xi)\ \frac{M = N}{\lambda x.M = \lambda x.N}$$

W rachunku λ przyjmujemy tylko aksjomaty (α), (β). Dodając aksjomat (η), otrzymujemy rachunek $\lambda\eta$.

Piszemy $\lambda \vdash M = N$, jeżeli $M = N$ jest twierdzeniem rachunku λ. Podobnie dla $\lambda\eta$.

W rachunku $\lambda\eta$ wyprowadzalna jest *reguła ekstensjonalności*:

$$\text{(EXT)}\ \frac{Mx = Nx}{M = N},\ \text{dla}\ x \notin V(MN)$$

1. $Mx = Nx$, 2. $\lambda x.Mx = \lambda x.Nx$ na mocy (ξ), 3. $M = \lambda x.Mx$ na mocy (η) i (sym), 4. $\lambda x.Nx = N$ na mocy (η), 5. $M = N$ na mocy (tran) (kilkakrotnie).

Odwrotnie, w rachunku λ wzbogaconym o regułę (EXT) można udowodnić (η).

1. $(\lambda x.Mx)x = Mx$ na mocy (β), 2. $\lambda x.Mx = M$ na mocy (EXT).

Twierdzenie 1. (o punkcie stałym) Dla dowolnego termu F istnieje term X taki, że $\lambda \vdash FX = X$.

Dowód. Oznaczmy $W \equiv \lambda x.F(xx)$, $X \equiv WW$.

$X = WW = (\lambda x.F(xx))W = F(WW) = FX$. Q.E.D.

Definicja 6. Termy bez zmiennych wolnych nazywamy *kombinatorami*.

Λ_0 oznacza zbiór wszystkich kombinatorów.

Uwaga. W tw. 1, jeżeli F jest kombinatorem, to X jest kombinatorem.

Twierdzenie 1'. Istnieje kombinator punktu stałego, tzn. taki kombinator $\mathbf{Y}$, że dla każdego termu F mamy $\lambda \vdash F(\mathbf{Y}F) = \mathbf{Y}F$.

Dowód. $\mathbf{Y} \equiv \lambda f.(\lambda x.f(xx))(\lambda x.f(xx))$. Przy oznaczeniach z poprzedniego dowodu mamy:

$\mathbf{Y}F = X = FX = F(\mathbf{Y}F)$. Q.E.D.

$M[x_1, \ldots, x_n]$ oznacza term M taki, że $V(M) \subseteq \{x_1, \ldots, x_n\}$ (te zmienne są wszystkie różne). Wtedy $M[N_1, \ldots, N_n]$ oznacza term $M[x_1/N_1, \ldots, x_n/N_n]$.

Fakt 2. Niech $x_1, \ldots, x_n$ będą różnymi zmiennymi. Dla dowolnych termów $M, N_1, \ldots, N_n$ mamy
$\lambda \vdash (\lambda x_1 \ldots x_n.M)N_1 \ldots N_n = M[x_1/N_1, \ldots, x_n/N_n]$.

Twierdzenie 2. (o definicjach rekurencyjnych) Dla dowolnego termu $M[f, x_1, \ldots, x_n]$ istnieje kombinator F taki, że
$\lambda \vdash F x_1 \ldots x_n = M[F, x_1, \ldots, x_n]$.

Dowód. Określamy $F \equiv \mathbf{Y}(\lambda f x_1 \ldots x_n.M[f, x_1, \ldots, x_n])$. Mamy:

$F = (\lambda f x_1 \ldots x_n.M[f, x_1, \ldots, x_n])F$ (tw. 1')
$= \lambda x_1 \ldots x_n.M[F, x_1, \ldots, x_n]$ (aks. (β)).

Stąd $F x_1 \ldots x_n = M[F, x_1, \ldots, x_n]$. Q.E.D.

Przykłady użytecznych kombinatorów.

$\mathbf{I} \equiv \lambda x.x$ (kombinator identyczności) $\lambda \vdash \mathbf{I}X = X$

$\mathbf{K} \equiv \lambda xy.x$ (kombinator funkcji stałej) $\lambda \vdash \mathbf{K}XY = X$

$\mathbf{K}^* \equiv \lambda xy.y$. $\lambda \vdash \mathbf{K}^*XY = Y$

$\mathbf{S} \equiv \lambda xyz.xz(yz)$. $\lambda \vdash \mathbf{S}XYZ = XZ(YZ)$

$\mathbf{B} \equiv \lambda xyz.x(yz)$ (kombinator złożenia) $\lambda \vdash \mathbf{B}FGX = F(GX)$

$\mathbf{C} \equiv \lambda xyz.xzy$ (komutator) $\lambda \vdash \mathbf{C}XYZ = XZY$

Przykład. Wykażemy $\lambda \vdash \mathbf{SKK} = \mathbf{I}$.

$\mathbf{SKK} = (\lambda xyz.xz(yz))\mathbf{KK} = \lambda z.\mathbf{K}z(\mathbf{K}z) = \lambda z.z = \mathbf{I}$

Wykażemy $\lambda \vdash \mathbf{B} = \mathbf{S}(\mathbf{KS})\mathbf{K}$.

$\mathbf{S}(\mathbf{KS})\mathbf{K} = (\lambda xyz.xz(yz))(\mathbf{KS})\mathbf{K} = \lambda z.\mathbf{KS}z(\mathbf{K}z) = \lambda z.\mathbf{S}(\mathbf{K}z) =$
$\lambda z.(\lambda xyz.xz(yz))(\mathbf{K}z) = \lambda zyu.\mathbf{K}zu(yu) = \lambda zyu.z(yu) = \mathbf{B}$

2. Logika kombinatorowa

ang. Combinatory Logic (CL)

Symbolami CL są zmienne $x, y, z, \ldots$ i stałe $\mathbf{S}, \mathbf{K}$.

Złożone termy kombinatorowe (CL-termy) tworzymy tylko przez aplikację (MN).

$V(M)$ oznacza zbiór zmiennych występujących w termie M. Termy nie zawierające zmiennych nazywamy kombinatorami.

Aksjomaty CL.

(S) $\mathbf{S}XYZ = XZ(YZ)$ dla wszystkich termów X, Y, Z

(K) $\mathbf{K}XY = X$ dla wszystkich termów X, Y

Reguły są te same, co w rachunku λ bez (ξ), lecz z (Id).

Definiujemy $\mathbf{I} \equiv \mathbf{SKK}$.

Wykażemy $\mathrm{CL} \vdash \mathbf{I}X = X$

$\mathbf{I}X = \mathbf{SKK}X = \mathbf{K}X(\mathbf{K}X) = X$

Definiujemy $\mathbf{B} \equiv \mathbf{S}(\mathbf{KS})\mathbf{K}$.

Wykażemy $\mathrm{CL} \vdash \mathbf{B}XYZ = X(YZ)$.

$\mathbf{B}XYZ = \mathbf{S}(\mathbf{KS})\mathbf{K}XYZ = \mathbf{KS}X(\mathbf{K}X)YZ = \mathbf{S}(\mathbf{K}X)YZ = \mathbf{K}XZ(YZ) = X(YZ)$

Można zdefiniować przekształcenie λ^*, które dla każdego termu kombinatorowego M i dowolnej zmiennej x tworzy term kombinatorowy $\lambda^* x.M$ taki, że $\mathrm{CL} \vdash (\lambda^* x.M)N = M[x/N]$ dla wszelkich termów N. Podamy jedną z możliwych definicji.

$\lambda^* x.x \equiv \mathbf{I}$

$\lambda^* x.M \equiv \mathbf{K}M$, jeżeli $x \notin V(M)$

$\lambda^* x.M_1 M_2 \equiv \mathbf{S}(\lambda^* x.M_1)(\lambda^* x.M_2)$, jeżeli $x \in V(M_1 M_2)$

Przykład. $\lambda^* x.\lambda^* y.y = \lambda^* x.\mathbf{I} = \mathbf{KI}$

W ten sposób każdy lambda-term można ‘przetłumaczyć’ na term kombinatorowy. CL ma własności podobne do rachunku λ.

3. Definiowalność funkcji rekurencyjnych

Liczebniki Churcha

Pomocnicza notacja: $M^n(N) \equiv M(M(\ldots(MN)\ldots))$, gdzie M jest iterowane n razy. Podamy definicję rekurencyjną.

$M^0(N) \equiv N$, $M^{n+1}(N) \equiv M(M^n(N))$

Fakt 3. $M^m(M^n(N)) \equiv M^{m+n}(N)$ dla wszelkich $m, n \in \mathbb{N}$.

Dowód. Indukcja względem m. Dla $m = 0$ mamy:

$M^0(M^n(N)) \equiv M^n(N) \equiv M^{0+n}(N)$.

Zakładamy, że równość jest prawdziwa dla m i wykazujemy ją dla $m + 1$.

$M^{m+1}(M^n(N)) \equiv M(M^m(M^n(N))) \equiv_{ZI} M(M^{m+n}(N)) \equiv M^{m+n+1}(N) \equiv M^{m+1+n}(N)$. Q.E.D.

Liczbę naturalną n reprezentujemy jako kombinator $c_n \equiv \lambda fx.f^n(x)$.

$c_0 \equiv \lambda fx.x$, $c_1 \equiv \lambda fx.fx$, $c_2 \equiv \lambda fx.f(fx)$, $c_3 \equiv \lambda fx.f(f(fx))$ itd.

Definicje podstawowych działań arytmetycznych są łatwe.

Definiujemy $\mathrm{Suc} \equiv \lambda nfx.f(nfx)$. Wykażemy $\lambda \vdash \mathrm{Suc}\, c_n = c_{n+1}$ dla wszelkich $n \in \mathbb{N}$.

$\mathrm{Suc}\, c_n = \lambda fx.f(c_n f x) = \lambda fx.f(f^n(x)) = \lambda fx.f^{n+1}(x) = c_{n+1}$.

Definiujemy $\mathrm{Add} \equiv \lambda mnfx.mf(nfx)$. Wykażemy $\lambda \vdash \mathrm{Add}\, c_m c_n = c_{m+n}$ dla wszelkich $m, n \in \mathbb{N}$.

$\mathrm{Add}\, c_m c_n = \lambda fx.c_m f(c_n f x) = \lambda fx.c_m f(f^n(x)) = \lambda fx.f^m(f^n(x)) = \lambda fx.f^{m+n}(x) = c_{m+n}$

Definiujemy $\mathrm{Mult} \equiv \lambda mnf.m(nf)$. Wykażemy $\lambda \vdash \mathrm{Mult}\, c_m c_n = c_{m\cdot n}$ dla wszelkich $m, n \in \mathbb{N}$.

Przez indukcję względem m łatwo wykazać $(\lambda x.f^n(x))^m(x) = f^{m\cdot n}(x)$.

$\mathrm{Mult}\, c_m c_n = \lambda f.c_m(c_n f) = \lambda f.c_m(\lambda x.f^n(x)) = \lambda fx.(\lambda x.f^n(x))^m(x) = \lambda fx.f^{m\cdot n}(x) = c_{m\cdot n}$

Liczebniki Barendregta

Definiujemy wartości logiczne: $true = \mathbf{K}$, $false = \mathbf{K}^*$.

Para uporządkowana: $[M, N] \equiv \lambda z.zMN$, gdzie $z \notin V(MN)$.

Mamy: $\lambda \vdash [M, N]true = M$, $\lambda \vdash [M, N]false = N$.

Określamy liczebniki $\bar{n}$ dla $n \in \mathbb{N}$.

$\bar{0} \equiv \mathbf{I}, \quad \overline{n+1} \equiv [false, \bar{n}]$

Definicja 7. Funkcję $f : \mathbb{N}^n \mapsto \mathbb{N}$ nazywamy *definiowalną* w rachunku λ, jeżeli istnieje kombinator F taki, że dla wszelkich $k_1, \ldots, k_n \in \mathbb{N}$ mamy $\lambda \vdash F\bar{k}_1 \ldots \bar{k}_n = \overline{f(k_1, \ldots, k_n)}$. Wtedy mówimy, że kombinator F definiuje funkcję f w rachunku λ.

Twierdzenie 3. Wszystkie całkowite funkcje rekurencyjne są definiowalne w rachunku λ.

Uwaga. To twierdzenie można rozszerzyć na częściowe funkcje rekurencyjne.

Operacja minimum efektywnego.

Niech $f : \mathbb{N}^{n+1} \mapsto \mathbb{N}$ spełnia *warunek efektywności*:

(WE) *dla wszelkich* $k_1, \ldots, k_n \in \mathbb{N}$ *istnieje* $k \in \mathbb{N}$ *takie, że* $f(k_1, \ldots, k_n, k) = 0$.

Określamy funkcję $h : \mathbb{N}^n \mapsto \mathbb{N}$ wzorem:

$h(x_1, \ldots, x_n) = \mu y(f(x_1, \ldots, x_n, y) = 0)$.

Mówimy, że h powstaje z f przez operację *minimum efektywnego*.

Skorzystamy z następującego twierdzenia teorii funkcji rekurencyjnych.

Twierdzenie. Rodzina całkowitych funkcji rekurencyjnych jest najmniejszą rodziną funkcji numerycznych, do której należą wszystkie podstawowe funkcje rekurencyjne i która jest zamknięta ze względu na podstawianie, rekursję prostą i operację minimum efektywnego.

Dowód twierdzenia 3.

Wykażemy, że podstawowe funkcje rekurencyjne są definiowalne w rachunku λ.

Funkcja $\mathcal{Z}(x) = 0$ jest definiowana przez kombinator $\lambda x.\bar{0}$.
Oczywiście $\lambda \vdash (\lambda x.\bar{0})\bar{n} = \bar{0}$.

Funkcja $\sigma(x) = x + 1$ jest definiowana przez kombinator
Suc$\equiv \lambda x.[\mathit{false},x]$. W rachunku λ obliczamy:

$(\lambda x.[\mathit{false},x])\bar{n} = [\mathit{false},\bar{n}] = \overline{n+1}$.

Funkcja $I_i^n(x_1, \ldots, x_n) = x_i$ jest definiowana przez kombinator $\lambda x_1 \ldots x_n.x_i$.

$\lambda \vdash (\lambda x_1 \ldots x_n.x_i)\bar{k}_1 \ldots \bar{k}_n = \bar{k}_i$

Wykażemy, że funkcje definiowalne w rachunku λ są zamknięte ze względu na podstawianie.

$h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n))$

Zakładamy, że funkcje $f, g_1, \ldots, g_k$ są definiowane przez kombinatory $F, G_1, \ldots, G_k$. Wtedy kombinator H określony tak:

$$H \equiv \lambda x_1 \ldots x_n . F(G_1 x_1 \ldots x_n) \ldots (G_k x_1 \ldots x_n)$$

definiuje funkcję h.

$$H\bar{k}_1 \ldots \bar{k}_n = F(G_1\bar{k}_1 \ldots \bar{k}_n) \ldots (G_k\bar{k}_1 \ldots \bar{k}_n) =$$
$$F\,\overline{g_1(k_1, \ldots, k_n)} \ldots \overline{g_k(k_1, \ldots, k_n)} =$$
$$\overline{f(g_1(k_1, \ldots, k_n), \ldots, g_k(k_1, \ldots, k_n))} = \overline{h(k_1, \ldots, k_n)}$$

Określamy pomocnicze kombinatory.

$\mathrm{Zero} \equiv \lambda x . x\, true$. Wtedy:

$\lambda \vdash \mathrm{Zero}\, \bar{0} = true$, $\lambda \vdash \mathrm{Zero}\, \overline{n+1} = false$.

$P^- \equiv \lambda x . x\, false$. Wtedy: $\lambda \vdash P^- \overline{n+1} = \bar{n}$.

$if\ B\ then\ M\ else\ N \equiv BMN$. Mamy:

$true\, MN = \mathbf{K} MN = M$, $false\, MN = \mathbf{K}^* MN = N$.

Wykażemy, że funkcje definiowalne w rachunku λ są zamknięte ze względu na rekursję prostą.

$h(0, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$

$h(y + 1, x_1, \ldots, x_n) = g(h(y, x_1 \ldots x_n), y, x_1, \ldots, x_n)$

Zakładamy, że kombinatory F, G definiują funkcje f, g. Określamy term:

$C[h', y, x_1, \ldots, x_n] \equiv$

$\mathit{if}\ (\mathrm{Zero}\, y)\ \mathit{then}\ (F x_1 \ldots x_n)\ \mathit{else}\ (G(h'(P^{-}y)x_1 \ldots x_n)(P^{-}y)x_1 \ldots x_n)$

Na mocy Tw. 2 istnieje kombinator H taki, że

$\lambda \vdash Hyx_1 \ldots x_n = C[H, y, x_1, \ldots, x_n]$.

Wykażemy, że kombinator H definiuje funkcję h. Mamy:

$H\bar{k}\bar{k}_1 \ldots \bar{k}_n = (\lambda yx_1 \ldots x_n.Hyx_1 \ldots x_n)\bar{k}\bar{k}_1 \ldots \bar{k}_n =$
$(\lambda yx_1 \ldots x_n.C[H, y, x_1, \ldots, x_n])\bar{k}\bar{k}_1 \ldots \bar{k}_n = C[H, \bar{k}, \bar{k}_1, \ldots, \bar{k}_n]$

Wykazujemy $\lambda \vdash H\bar{k}\bar{k}_1 \dots \bar{k}_n = \overline{h(k, k_1, \dots, k_n)}$ przez indukcję względem k.

$k = 0$.

$H\bar{0}\bar{k}_1 \dots \bar{k}_n = C[H, \bar{0}, \bar{k}_1, \dots, \bar{k}_n] = F\bar{k}_1 \dots \bar{k}_n = \overline{f(k_1, \dots, k_n)} =$
$\overline{h(0, k_1, \dots, k_n)}$

Zakładamy tezę dla k i dowodzimy dla $k + 1$.

$H\overline{k+1}\bar{k}_1 \dots \bar{k}_n = C[H, \overline{k+1}, \bar{k}_1, \dots, \bar{k}_n] =$
$G(H(P^-\overline{k+1})\bar{k}_1 \dots \bar{k}_n)(P^-\overline{k+1})\bar{k}_1 \dots \bar{k}_n =$
$G(H\bar{k}\bar{k}_1 \dots \bar{k}_n)\bar{k}\bar{k}_1 \dots \bar{k}_n =_{ZI} G\overline{h(k, k_1, \dots, k_n)}\bar{k}\bar{k}_1 \dots \bar{k}_n =$
$\overline{g(h(k, k_1, \dots, k_n), k, k_1, \dots, k_n)} = \overline{h(k+1, k_1, \dots, k_n)}$

Wykażemy, że funkcje definiowalne w rachunku λ są zamknięte ze względu na operację minimum efektywnego.

$h(x_1, \dots, x_n) = \mu y(f(x_1, \dots, x_n, y) = 0)$ (zakładamy (WE))

Zakładamy, że kombinator F definiuje funkcję f. Określamy term:

$C[h', x_1, \ldots, x_n, y] \equiv$

if (Zero($F x_1 \ldots x_n y$)) *then* y *else* ($h' x_1 \ldots x_n$(Suc y))

Na mocy Tw. 2 istnieje kombinator H' taki, że
$\lambda \vdash H' x_1 \ldots x_n y = C[H', x_1, \ldots, x_n, y]$.

Określamy $H \equiv \lambda x_1 \ldots x_n . H' x_1 \ldots x_n \bar{0}$.

Wykazujemy $\lambda \vdash H \bar{k}_1 \ldots \bar{k}_n = \overline{h(k_1, \ldots, k_n)}$.

$H \bar{k}_1 \ldots \bar{k}_n = H' \bar{k}_1 \ldots \bar{k}_n \bar{0} = C[H', \bar{k}_1, \ldots, \bar{k}_n, \bar{0}] = ?$

Oznaczmy $k = h(k_1, \ldots, k_n)$.

Jeżeli $k = 0$, to $f(k_1, \ldots, k_n, 0) = 0$, więc $? = \bar{0}$.

Jeżeli $k > 0$, to:

$? = H' \bar{k}_1 \ldots \bar{k}_n \bar{1} = H' \bar{k}_1 \ldots \bar{k}_n \bar{2} = \cdots = H' \bar{k}_1 \ldots \bar{k}_n \bar{k} = \bar{k}$.

Q.E.D.

4. Redukcja i normalizacja

Definicja 8. Term postaci $(\lambda x.M)N$ nazywamy β−*redeksem* (krótko: redeksem), a term $M[x/N]$ *reduktem* (contractum) tego redeksu.

Definicja 9. Mówimy, że term P jest *normalny* (albo: w postaci normalnej), jeżeli nie zawiera żadnych redeksów (jako podtermów).

Definicja 10. Term P nazywamy *normalizowalnym*, jeżeli istnieje term normalny Q taki, że $\lambda \vdash P = Q$. Taki term Q nazywamy *postacią normalną* termu P.

Sprowadzanie termu do postaci normalnej opiera się na procedurze *redukcji*, tzn. kolejnym zastępowaniu redeksów ich reduktami (β−kroki) oraz podtermów ich α−wariantami (α−kroki).

W rachunku $\lambda\eta$ dopuszczamy też η−kroki, polegające na zastąpieniu η−redeksu $\lambda x.Mx$, gdzie $x \notin V(M)$, jego reduktem M. Odpowiednio też modyfikujemy pojęcia termu normalnego i normalizowalnego.

Definicja 11. ($\alpha,\beta-$redukcja, krótko: redukcja)

$M \to_\beta N$ wtw, gdy N powstaje z M przez zastąpienie pewnego redeksu jego reduktem.

$M \to^* N$ wtw, gdy istnieje ciąg $(M_0, \ldots, M_n)$, gdzie $n \in \mathbb{N}$, taki że $M_0 = M$, $M_n = N$ oraz $M_{i-1} \to_\beta M_i$ lub $M_{i-1} \equiv_\alpha M_i$ dla każdego $i = 1, \ldots, n$.

Taki ciąg $(M_0, \ldots, M_n)$ nazywamy *redukcją* termu M do termu N. Liczbę n nazywamy długością tej redukcji.

Fakt 3. Relacja $\to^*$ jest zwrotna ($M \to^* M$) i przechodnia (jeżeli $M \to^* N$ i $N \to^* P$, to $M \to^* P$).

Dowód. Ciąg (M_0), gdzie $M_0 = M$, jest redukcją M do M. Jeżeli $(M_0, \ldots, M_n)$ jest redukcją M do N, a $(N_0, \ldots, N_p)$ jest redukcją N do P, to $M_n = N = N_0$ i ciąg $(M_0, \ldots, M_{n-1}, N_0, \ldots, N_p)$ jest redukcją M do P. Q.E.D.

Relację $\to^*$ można też zdefiniować aksjomatycznie, podobnie jak relację $=$.

Aksjomaty.

(α') $M \to^* N$, jeżeli $M \equiv_\alpha N$,

(β') $(\lambda x.M)N \to^* M[x/N]$.

Reguły. (Id) $M \to^* M$ (tu zbyteczne)

$$\text{(tran')}\ \frac{M \to^* N,\ N \to^* P}{M \to^* P} \quad (\xi')\ \frac{M \to^* N}{\lambda x.M \to^* \lambda x.N}$$

$$\text{(l-mon)}\ \frac{M \to^* N}{PM \to^* PN} \quad \text{(r-mon)}\ \frac{M \to^* N}{MP \to^* NP}$$

Fakt 4. Term jest normalny wtw, gdy ma jedną z dwóch postaci:

(1) $xM_1 \ldots M_n$, gdzie $n \geq 0$ i termy $M_1, \ldots, M_n$ są normalne,

(2) $\lambda x_1 \ldots x_k.M$, gdzie $k \neq 0$ i term M jest normalny.

Przykłady. Ptzykładami termów normalnych są x ((1) dla $n = 0$), xy, xyz, $xz(yz)$ (z (1)), $\lambda xyz.xz(yz)$ (z (2)), $x(\lambda x.xy)$ (z (1) i (2)).

Nie są normalne termy $(\lambda x.x)y$, $z((\lambda x.x)y)$.

Przykład redukcji:

$(\lambda x.x)((\lambda xy.x)y) \to_\beta (\lambda x.x)(\lambda z.y) \to_\beta \lambda z.y \equiv_\alpha \lambda x.y$

Ostatnie dwa termy są normalne.

Oznaczmy $U \equiv \lambda x.f(xx)$. Otrzymujemy redukcję nieskończoną.

$UU \to_\beta f(UU) \to_\beta f(f(UU)) \to_\beta f(f(f(UU))) \to_\beta \ldots$.

Twierdzenie 4. (tw. Churcha-Rossera) Dla wszystkich termów M, N_1, N_2 takich, że $M \to^* N_1$ i $M \to^* N_2$, istnieje term P taki, że $N_1 \to^* P$ i $N_2 \to^* P$.

Dowód tego twierdzenia można znaleźć w książce J.R. Hindley i J.P. Seldin, *Lambda-Calculus and Combinators: an Introduction*.

Jeżeli relacja redukcji ma własność opisaną w Tw. 4, to mówimy, że ta relacja ma *własność Churcha-Rossera* (albo: własność CR, własność diamentu). Tę własność mają też relacje redukcji w rachunku $\lambda\eta$ i CL.

Przykład. Niech $M \equiv (\lambda x.x)((\lambda y.xy)z)$, $N_1 \equiv (\lambda x.x)(xz)$, $N_2 \equiv (\lambda y.xy)z$.

Wtedy $M \to^* N_1$ i $M \to^* N_2$ (obie redukcje mają tylko jeden $\beta-$krok). Oczywiście $N_1 \to^* xz$ i $N_2 \to^* xz$.

Wniosek 1. $\lambda \vdash M = N$ wtw, gdy istnieje term P taki, że $M \to^* P$ i $N \to^* P$.

Dowód. ($\Leftarrow$). Załóżmy, że $M \to^* P$ i $N \to^* P$. Wtedy $\lambda \vdash M = P$ i $\lambda \vdash N = P$. Stąd $\lambda \vdash M = N$ na mocy reguł (sym) i (tran).

($\Rightarrow$). Zakładamy $\lambda \vdash M = N$. Dowodzimy:

(T) istnieje P takie, że $M \to^* P$ i $N \to^* P$

przez indukcję po liczbie reguł użytych w dowodzie $M = N$ w rachunku λ.

Krok początkowy. 0 reguł. Wtedy $M = N$ jest aksjomatem (α) lub (β), a więc $M \to^* N$ na mocy (α') lub (β'). Ponieważ $N \to^* N$, więc przyjmujemy $P \equiv N$.

Krok indukcyjny. k reguł (k>0). Zakładamy, że (T) jest prawdziwe dla równości $M = N$, w których dowodzie użyto mniej niż k reguł (założenie indukcyjne, ZI). Rozważamy przypadki w zależności od reguły użytej na końcu w dowodzie $M = N$.

(1) Reguła (sym). Wtedy przesłanka $N = M$ ma dowód z mniejszą liczbą reguł. Na mocy ZI istnieje P takie, że $N \to^* P$ i $M \to^* P$, a więc (T) jest prawdziwe.

(2) Reguła (l-con). Wtedy $M \equiv QM'$, $N \equiv QN'$, a przesłanką jest $M' = N'$. Na mocy ZI istnieje P' takie, że $M' \to^* P'$ i $N' \to^* P'$. Wtedy $QM' \to^* QP'$ i $QN' \to^* QP'$ na mocy (l-mon), a więc (T) jest prawdziwe (dla $P \equiv QP'$). Podobnie dla reguły (r-con).

(3) Reguła (ξ). Wtedy $M \equiv \lambda x.M'$, $N \equiv \lambda x.N'$, a przesłanką jest $M' = N'$. Na mocy ZI istnieje P' takie, że $M' \to^* P'$ i $N' \to^* P'$. Wtedy $\lambda x.M' \to^* \lambda x.P'$ i $\lambda x.N' \to^* \lambda x.P'$ na mocy (ξ'), a więc (T) jest prawdziwe (dla $P \equiv \lambda x.P'$).

(4) Reguła (tran). Wtedy $M = N$ wywnioskowano z przesłanek $M = Q$ i $Q = N$ dla pewnego termu Q. Na mocy ZI istnieją termy P_1, P_2 takie, że $M \to^* P_1$ i $Q \to^* P_1$ oraz $Q \to^* P_2$ i $N \to^* P_2$. Na mocy Tw. 4 istnieje term P taki, żę $P_1 \to^* P$ i $P_2 \to^* P$, a więc $M \to^* P$ i $N \to^* P$ na mocy (tran'). Q.E.D.

Wniosek 2. Dla dowolnych termów normalnych M, N: $\lambda \vdash M = N$ wtw, gdy $M \equiv_\alpha N$.

Dowód. ($\Leftarrow$) jest oczywiste. Dowodzimy ($\Rightarrow$). Zakładamy, że $\lambda \vdash M = N$, gdzie M, N są normalne. Na mocy Wniosku 1 istnieje P takie, że $M \rightarrow^* P$ i $N \rightarrow^* P$. Te dwie redukcje składają się wyłącznie z $\alpha-$kroków, więc $M \equiv_\alpha P$ i $N \equiv_\alpha P$, a stąd $M \equiv_\alpha N$, bo relacja $\equiv_\alpha$ jest symetryczna i przechodnia. Q.E.D.

Wobec tego rachunek λ jest *niesprzeczny*, tzn. nie wszystkie równości są twierdzeniami. Dla różnych zmiennych x, y $\lambda \nvdash x = y$.

$\bar{0}$ jest termem normalnym $\lambda x.x$. Podobnie *false*, czyli term $\lambda xy.y$. Przypomnijmy, że $[M, N] \equiv \lambda z.zMN$, a więc $[M, N]$ jest normalny, jeżeli M, N są normalne. W konsekwencji każdy liczebnik $\bar{n}$ jest normalny (przypomnijmy, że $\overline{n+1} = [\mathit{false}, \bar{n}]$).

Jeżeli $m, n \in \mathbb{N}$ są różne, to $\lambda \nvdash \bar{m} = \bar{n}$. Jeżeli $\lambda \vdash F\bar{k}_1 \ldots \bar{k}_n = \overline{f(k_1, \ldots, k_n)}$, to $f(k_1, \ldots, k_n)$ jest jedyną liczbą $k \in \mathbb{N}$ taką, że $\lambda \vdash F\bar{k}_1, \ldots, \bar{k}_n = \bar{k}$.

Wniosek 3. Jeżeli N jest postacią normalną termu M, to $M \rightarrow^* N$. Wszystkie postacie normalne jednego termu są w relacji $\equiv_\alpha$.

Dowód. Niech N będzie postacią normalną termu M. Wtedy $\lambda \vdash M = N$. Na mocy Wniosku 1 istnieje P takie, że $M \rightarrow^* P$ i $N \rightarrow^* P$. Ponieważ term N jest normalny, więc $N \equiv_\alpha P$, a stąd $P \equiv_\alpha N$. Mamy $M \rightarrow^* P$ i $P \rightarrow^* N$, a więc $M \rightarrow^* N$ na mocy (trans'). Druga część twierdzenia wynika z Wniosku 2. Q.E.D.

Przykłady.

Niech $U \equiv \lambda x.f(xx)$. Wszystkie $\beta-$redukcje termu UU można przedłużać w nieskończoność, więc żadna z nich nie prowadzi do termu normalnego (dodanie $\alpha-$kroków nie naprawi sytuacji). Zatem term UU nie jest normalizowalny.

Term $\mathbf{K}x(UU)$, czyli $(\lambda xy.x)x(UU)$ jest normalizowalny: redukuje się do x. Istnieje jednak nieskończona $\beta-$redukcja

$$\mathbf{K}x(UU) \rightarrow_\beta \mathbf{K}x(f(UU)) \rightarrow_\beta \mathbf{K}x(f(f(UU))) \rightarrow_\beta \ldots.$$

5. Nierozstrzygalność rachunku λ

Każdemu termowi M przyporządkujemy liczbę naturalną $\nu(M)$, zwaną *numerem* termu M.

Funkcja pary: $\pi(m,n) = 2^m \cdot (2n+1)$. Funkcja π jest bijekcją zbioru $\mathbb{N}^2$ na zbiór dodatnich liczb naturalnych (każda liczba $k \geq 1$ jest jednoznacznie przedstawialna w postaci $k = \pi(m,n)$).

Przyjmujemy, że zmienne są ustawione w ciąg nieskończony: $x_0, x_1, x_2, \ldots$.

$\nu(x_i) = \pi(0,i)$

$\nu(MN) = \pi(1, \pi(\nu(M), \nu(N)))$

$\nu(\lambda x_i.M) = \pi(2, \pi(i, \nu(M)))$

Różne termy mają różne numery. Ponadto istnieje prosty algorytm sprawdzania, czy liczba k jest numerem jakiegoś termu, a jeżeli tak, to wyznaczania jedynego termu M takiego, że $k = \nu(M)$.

Liczba $2^m \cdot (2n+1)$, gdzie $m > 2$, nie jest numerem termu.

Liczba nieparzysta $2^0 \cdot (2i+1)$ jest numerem zmiennej x_i.

Liczba parzysta $2^1 \cdot (2k+1)$ może być tylko numerem termu postaci MN. Znajdujemy m, n takie, że $k = \pi(m, n)$, i uruchamiamy algorytm dla liczb m, n.

Liczba parzysta $2^2 \cdot (2k+1)$ może być tylko numerem termu $\lambda x_i.M$. Znajdujemy i, m takie, że $k = \pi(i, m)$ (stąd mamy x_i), i uruchamiamy algorytm dla liczby m.

Przykład. Niech $M \equiv \lambda x_0.x_0x_1$.

$\nu(x_0) = \pi(0, 0) = 1$, $\nu(x_1) = \pi(0, 1) = 3$

$\nu(x_0x_1) = \pi(1, \pi(1, 3)) = 2^1 \cdot (2\pi(1, 3) + 1) = 2 \cdot (2 \cdot (2^1 \cdot 7) + 1) = 58$

$\nu(M) = \pi(2, \pi(0, 58)) = 2^2 \cdot (2\pi(0, 58) + 1) =$
$4 \cdot (2 \cdot (2 \cdot 58 + 1) + 1) = 4 \cdot (2 \cdot 117 + 1) = 4 \cdot 235 = 940$

Liczba $100 = 4 \cdot 25 = 4 \cdot (2 \cdot 12 + 1)$ to numer termu $\lambda x_2.x_0$.

Definicja 12. Określamy relację $\mathrm{Ter} \subseteq \mathbb{N}$:

$\mathrm{Ter}(n) \Leftrightarrow \exists_{M\in\Lambda} n = \nu(M)$

Dla dowolnego n takiego, że $\mathrm{Ter}(n)$, symbolem $t(n)$ oznaczamy term M taki, że $n = \nu(M)$.

Fakt 5. Istnieje algorytm, który dla dowolnego n sprawdza, czy $\mathrm{Ter}(n)$, a jeżeli tak, to wyznacza $t(n)$.

Fakt 6. Relacja Ter jest rekurencyjna.

Twierdzenie 5. Określamy relację $\mathrm{Eq} \subseteq \mathbb{N}^2$:

$\mathrm{Eq}(m, n) \Leftrightarrow \mathrm{Ter}(m) \wedge \mathrm{Ter}(n) \wedge \lambda \vdash t(m) = t(n)$.

Twierdzenie 5. Relacja Eq nie jest rekurencyjna.

Stosując tezę Churcha, stwierdzamy, że relacja $\lambda \vdash M = N$ jest nierozstrzygalna (rachunek λ jest nierozstrzygalny).

Definicja 13. Relację $S \subseteq \mathbb{N}^2$ nazywamy *relacją uniwersalną dla relacji rekurencyjnych*, jeżeli dla każdej relacji rekurencyjnej $R \subseteq \mathbb{N}$ istnieje $k \in \mathbb{N}$, spełniające warunek:

(UN) $\forall_{n\in\mathbb{N}}(R(n) \Leftrightarrow S(k, n))$.

Lemat 1. (lemat przekątniowy) Nie istnieje rekurencyjna relacja uniwersalna dla relacji rekurencyjnych.

Dowód. Przypuśćmy, że istnieje rekurencyjna relacja $S \subseteq \mathbb{N}^2$, uniwersalna dla relacji rekurencyjnych. Określamy relację przekątniową $R \subseteq \mathbb{N}$:

(D) $\forall_{n\in\mathbb{N}}(R(n) \Leftrightarrow \neg S(n, n))$.

Na mocy własności (R1), (R2) relacja R jest rekurencyjna. Stąd istnieje $k \in \mathbb{N}$, spełniające (UN). Stosując (UN) i (D) do $n = k$, otrzymujemy równoważności $R(k) \Leftrightarrow S(k, k)$ oraz $R(k) \Leftrightarrow \neg S(k, k)$, a stąd $S(k, k) \Leftrightarrow \neg S(k, k)$, co jest zdaniem logicznie fałszywym. Zatem przypuszczenie jest fałszywe. Q.E.D.

Określamy pomocnicze funkcje rekurencyjne.

$ap(m, n) = \pi(1, \pi(m, n))$.

Wtedy $ap(\nu(M), \nu(N)) = \nu(MN)$.

$\tau(m, n, k) = ap(ap(m, n), k)$.

Wtedy $\tau(\nu(M), \nu(N), \nu(P)) = \nu(MNP)$.

$p(m, n) = \pi(2, \pi(0, \tau(\pi(0, 0), m, n)))$.

Wtedy $p(\nu(M), \nu(N)) = \nu(\lambda x_0.x_0 MN) = \nu([M, N])$.

Określamy liczby: $\mathbf{i} = \nu(\mathbf{I})$, $\mathbf{k}^* = \nu(\mathbf{K}^*)$.

$\mathrm{Num}(0) = \mathbf{i}$

$\mathrm{Num}(n + 1) = p(\mathbf{k}^*, \mathrm{Num}(n))$.

Wtedy $\mathrm{Num}(n) = \nu(\bar{n})$.

Dowód Tw. 5. Określamy relację $S \subseteq \mathbb{N}^2$:

$S(m, n) \Leftrightarrow \mathrm{Eq}(ap(m, \mathrm{Num}(n)), \nu(\bar{1}))$.

Wtedy: $S(\nu(M), n) \Leftrightarrow \lambda \vdash M\bar{n} = \bar{1}$.

Wykażemy, że S jest relacją uniwersalną dla relacji rekurencyjnych. Stąd na mocy Lematu 1 relacja S nie jest rekurencyjna. Zatem relacja Eq nie jest rekurencyjna na mocy (R1).

Niech $R \subseteq \mathbb{N}$ będzie relacją rekurencyjną. Wtedy funkcja c_R jest rekurencyjna. Na mocy Tw. 3 istnieje kombinator C_R definiujący funkcję c_R w rachunku λ.

Dla każdego $n \in \mathbb{N}$ prawdziwe są równoważności:

$R(n) \Leftrightarrow c_R(n) = 1 \Leftrightarrow \lambda \vdash C_R\bar{n} = \bar{1}$, a stąd:

$R(n) \Leftrightarrow S(\nu(C_R), n)$,

czyli (UN) dla $k = \nu(C_R)$. Q.E.D.