

# Nyelvek típusrendszere (jegyzet)

Kaposi Ambrus  
Eötvös Loránd Tudományegyetem  
akaposi@inf.elte.hu

2016. november 14.

## Tartalomjegyzék

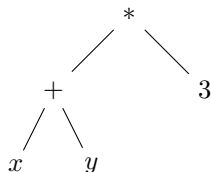
<b>1. Bevezető</b>	<b>2</b>
<b>2. Induktív definíciók</b>	<b>3</b>
2.1. Absztrakt szintaxisfák . . . . .	3
2.2. Absztrakt kötéses fák . . . . .	5
2.3. Levezetési fák . . . . .	8
<b>3. Számok és szövegek</b>	<b>11</b>
3.1. Szintaxis . . . . .	11
3.2. Típusrendszer . . . . .	11
3.3. Operációs szemantika . . . . .	16
3.4. Típusrendszer és szemantika kapcsolata . . . . .	18
3.5. Futási idejű hibák . . . . .	20
<b>4. Függvények</b>	<b>21</b>
4.1. Elsőrendű függvények . . . . .	21
4.2. Magasabbrendű függvények . . . . .	22
<b>5. Véges adattípusok</b>	<b>23</b>
5.1. Szorzat típusok . . . . .	24
5.1.1. Nulláris és bináris szorzat típus . . . . .	24
5.1.2. Általános véges szorzat típusok . . . . .	25
5.2. Összeg típusok . . . . .	27
5.2.1. Nulláris és bináris összeg . . . . .	27
5.2.2. Általános véges összeg típusok . . . . .	28
5.3. Véges típusok alkalmazásai . . . . .	28
<b>6. Konstruktív ítéletlogika</b>	<b>30</b>
6.1. Szintaxis . . . . .	30
6.2. Bizonyítások . . . . .	30
6.3. Állítások mint típusok . . . . .	32
6.4. Klasszikus logika . . . . .	32

<b>7. Természetes számok</b>	<b>34</b>
7.1. Szintaxis . . . . .	34
7.2. Típusrendszer . . . . .	34
7.3. Operációs szemantika . . . . .	34
7.4. Definiálható függvények . . . . .	36
<b>8. Végtelen adattípusok</b>	<b>37</b>
<b>9. Parcialitás, rekurzív típusok</b>	<b>37</b>
<b>10. Imperatív programozás</b>	<b>37</b>
<b>11. Polimorfizmus</b>	<b>37</b>
<b>12. Altípus</b>	<b>37</b>
<b>13. Függő típus</b>	<b>37</b>
<b>14. Megoldások</b>	<b>37</b>

## 1. Bevezető

Típusrendszerek helye a fordítóprogramokban:

1. Lexikális elemző (lexer): karakterek listájából tokenek listáját készíti, pl. "(x + y) \* 3"-ból `brOpen var[x] op[+] var[y] brClose op[*] const[3]`.
2. Szintaktikus elemző (parser): a tokenek listájából absztrakt szintaxisfát épít, az előbbi példából a következőt.



3. Típusellenőrzés: megnézi, hogy a szintaxisfa megfelel-e bizonyos szabályoknak (a típusrendszernek), pl. szükséges, hogy  $x$  és  $y$  numerikus típusú legyen. Általánosságban, nem enged át értelmetlen programokat. Mi ezzel a résszel foglalkozunk.
4. Kódgenerálás: ha a típusellenőrző átengedte a szintaxisfát, akkor ezt lefordítjuk a gép számára érthető kóddá.

Típusrendszerek és logika:

- Mi az, hogy számítás? Erre egy válasz a lambda kalkulus (alternatíva a Turing-gépekre), amely a Lisp programozási nyelv alapja. A különböző típusrendszereket azért fejlesztették ki, hogy megszorítsák a programokat a jó programokra.
- Mi az, hogy bizonyítás? Erre válaszol a logika az ítéletlogikával, predikátumkalkulussal.

- Típuselmélet: egy olyan rendszer, mely a két nézőpontot egyesíti. Ez egy típusrendszer, melynek speciális eseteit fogjuk tanulni. Megmutatja, hogy az intuitívan hasonlóan viselkedő fogalmak (pl. matematikai függvények, logikai következtetés, függvény típusú program, univerzális kvantor) valójában ugyanazok. Elvezet az egyenlőség egy új nézőpontjára, ami egy új kapcsolatot nyit a homotópia-elmélet és a típuselmélet között.

A magas kifejezőerejű típusrendszerekben már nem az a kérdés, hogy egy megírt program típusozható -e. A nézőpont megfordul: először adjuk meg a típust (specifikáljuk, hogy mit csinálhat a program), majd a típus alapján megírjuk a programot (ez akár automatikus is lehet, ha a típus eléggé megszorítja a megírható programok halmazát).

Két könyv alapján haladunk, de nem szükséges egyik sem a tananyag elsajátításához.

- Robert Harper. Practical Foundations for Programming Languages. Cambridge University Press, 2012.
- Csörnyei Zoltán. Bevezetés a típusrendszerek elméletébe. ELTE Eötvös Kiadó, 2012.

## 2. Induktív definíciók

Harper könyv: I. rész.

### 2.1. Absztrakt szintaxisfák

*Absztrakt szintaxisfának* (AST, abstract syntax tree) nevezzük az olyan fákat, melyek leveleinél *változók* vannak, közbenső pontjaikon pedig *operátorok*. Például a természetes szám kifejezések és az ezekből és összeadásból álló kifejezések AST-it az alábbi definíciókkal adhatjuk meg.

$$n, n', \dots \in \text{Nat} ::= i \mid \text{zero} \mid \text{suc } n \quad (2.1)$$

$$e, e', \dots \in \text{Exp} ::= x \mid \text{num } n \mid e + e' \quad (2.2)$$

Nat-ot és Exp-et *fajtának* nevezzük. A Nat fajtájú AST-ket  $n$ -el,  $n'$ -vel stb. jelöljük. Nat fajtájú AST lehet egy  $i$  változó, vagy létre tudjuk hozni a nulláris zero operátorral (*aritása*  $()\text{Nat}$ ) vagy az unáris suc operátorral (*aritása*  $(\text{Nat})\text{Nat}$ ).  $n$  egy tetszőleges Nat fajtájú AST-t jelöl, míg  $i$  maga egy Nat fajtájú AST, mely egy darab változóból áll.

Az Exp fajtájú AST-ket  $e$ -vel és ennek vesszőzött változataival jelöljük, az Exp fajtájú változókat  $x$ -el jelöljük. Exp fajtájú AST-t egy unáris operátorral (num, *aritása*  $(\text{Nat})\text{Exp}$ ) és egy bináris operátorral (+, *aritása*  $(\text{Exp}, \text{Exp})\text{Exp}$ ) tudunk létrehozni. A num operátorral Nat fajtájú AST-ket tudunk kifejezésekbe beágyazni.

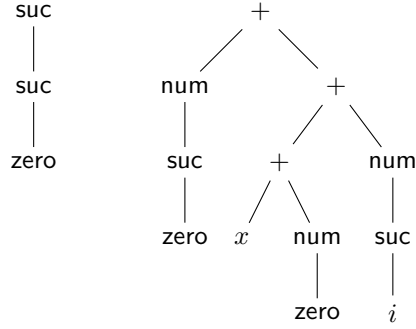
Minden fajtához változóknak egy külön halmaza tartozik, ezért jelöljük őket különböző betűkkel. A változók halmaza végtelen (mindig tudunk *friss* változót kapni, olyat, amelyet még sehol nem használtunk) és eldönthető, hogy két változó egyenlő -e. Az előbbi két fajtához tartozó változók halmazát így adhatjuk meg.

$$i, i', i_1, \dots \in \text{Var}_{\text{Nat}}$$

$$x, x', x_1, y, z, \dots \in \text{Var}_{\text{Exp}}$$

A metaváltozókat ( $n, n', e, e'$  stb.) megkülönböztetjük a kifejezésekben szereplő változóktól, melyek  $\text{Var}_{\text{Nat}}$ ,  $\text{Var}_{\text{Exp}}$  elemei. A metaváltozók a metanyelvünkben használt változók, a metanyelv az a nyelv, amiben ezek a mondatok íródnak.

Az AST-ket lerajzolhatjuk, pl.  $\text{suc}(\text{suc zero}) + (\text{num}(\text{suc zero}) + ((x + \text{num zero}) + \text{num}(\text{suc } i)))$ .



Az  $x + \text{num zero}$  részfája az  $(x + \text{num zero}) + \text{num}(\text{suc } i)$  AST-nek, ami pedig részfája a teljes AST-nek.

Az olyan AST-ket, melyek nem tartalmaznak változót, *zártak* nevezzük, egyébként *nyíltak*. A változók értékét *helyettesítéssel* (substitution) adhatjuk meg. Ha  $a$  egy  $A$  fajtájú AST,  $x$  pedig egy  $A$  fajtájú változó,  $t$  pedig tetszőleges fajtájú AST, akkor  $t[x \mapsto a]$ -t úgy kapjuk meg  $t$ -ből, hogy  $x$  összes előfordulása helyére  $a$ -t helyettesítünk. A helyettesítést az alábbi módon adjuk meg ( $f$  egy  $n$ -paraméteres operátor).

$$\begin{aligned} x[x \mapsto a] &:= a \\ y[x \mapsto a] &:= y && \text{feltéve, hogy } x \neq y \\ (f \ t_1 \dots t_n)[x \mapsto a] &:= f \ (t_1[x \mapsto a]) \dots (t_n[x \mapsto a]) \end{aligned}$$

Néhány példa:

$$\begin{aligned} (x + \text{num zero})[x \mapsto \text{num}(\text{suc zero})] &= \text{num}(\text{suc zero}) + \text{num zero} \\ (x + x)[x \mapsto x' + \text{num zero}] &= (x' + \text{num zero}) + (x' + \text{num zero}) \\ (x + \text{num}(\text{suc } i))[i \mapsto \text{zero}] &= x + \text{num}(\text{suc zero}) \end{aligned}$$

Megjegyezzük, hogy a  $\text{num}(\text{suc zero}) + \text{num}(\text{suc zero})$  egy formális kifejezés, amelynek a jelentését (szemantikáját) még nem adtuk meg. Fontos, hogy emiatt ne keverjük össze az  $1 + 1 = 2$  természetes számmal. Pl. nem igaz, hogy  $\text{num}(\text{suc zero}) + \text{num}(\text{suc zero}) = \text{num}(\text{suc}(\text{suc zero}))$ , ez két különböző AST.

Ha szeretnénk bizonyítani, hogy egy állítás az összes adott fajtájú AST-re igaz, elég megmutatni, hogy a változókra igaz az állítás, és az összes operátor megtartja az állítást. Pl. ha minden  $n \in \text{Nat}$ -ra szeretnénk belátni, hogy  $\mathcal{P}(n)$ , akkor elég azt belátni, hogy  $\mathcal{P}(i)$  minden  $i$ -re, hogy  $\mathcal{P}(\text{zero})$  és hogy minden  $m$ -re  $\mathcal{P}(m)$ -ből következik  $\mathcal{P}(\text{suc } m)$ . Ha minden  $e \in \text{Exp}$ -re szeretnénk  $\mathcal{Q}(e)$ -t belátni, elég azt belátni, hogy minden  $x$ -re  $\mathcal{Q}(x)$ , hogy  $n \in \text{Nat}$ -ra igaz  $\mathcal{Q}(\text{num } n)$  és ha igaz  $\mathcal{Q}(e)$  és  $\mathcal{Q}(e')$ , akkor igaz  $\mathcal{Q}(e + e')$  is. Ezt az érvelési formát szerkezeti *indukciónak* nevezzük (structural induction).

Ha egy függvényt szeretnénk megadni, ami az összes adott fajtájú AST-n működik, akkor hasonlóképp azt kell meghatározni, hogy az egyes operátorokon hogyan működik a függvény (felhasználva azt, hogy mi a függvény eredménye az

operátorok paraméterein). Ezt a megadási módot szerkezeti *rekurzió*nak hívjuk (structural recursion).

**2.1. Feladat.** Végezzük el a következő helyettesítéseket:

$$\begin{aligned} & ((x + x')[x \mapsto x'])[x' \mapsto x] \\ & (x + x)[x \mapsto x' + x] \\ & (\text{succ}(\text{succ } i))[i \mapsto \text{succ } i'] \\ & (\text{num}(\text{succ } i))[x \mapsto \text{num zero}] \end{aligned}$$

**2.2. Feladat.** Adjuk meg a  $\text{Nat}$ -ok listájának fajtáját az operátorok aritásával együtt.

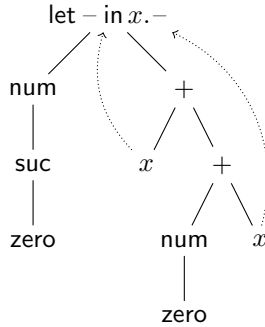
$$xs \in \text{List}_{\text{Nat}} ::= ?$$

További információ:

- A különböző fajtájú AST-k halmazait finomíthatjuk aszerint, hogy milyen változók vannak bennük. Ha egy  $\text{Exp}$  fajtájú  $e$  AST-ben  $x, x'$  a szabad változók, azt mondjuk, hogy  $e \in \text{Exp}_{x,x'}$  halmazban van. Ekkor pl.  $e + x'' \in \text{Exp}_{x,x',x''}$  és  $e[x \mapsto \text{num zero}] \in \text{Exp}_{x'}$ . Általános esetben szükségünk van minden fajtához egy különböző változó-halmazra, így ha  $a \in A_{X_A \dots X_B}$  és  $b \in B_{Y_A, \dots, Y_B}$ , akkor  $b[y \mapsto a] \in B_{X_A \cup Y_A \dots X_B \cup Y_B}$ .
- Az ABT-ket polinomiális funktorok (polynomial functor, container) szabad monádjaiként (free monad) adjuk meg. Ezzel biztosítjuk, hogy pl. minden szintaxisfa véges.

## 2.2. Absztrakt kötési fák

Az *absztrakt kötési fák* (ABT, abstract binding tree) az AST-khez hasonló, de változót *kötő* operátorok is szerepelhetnek benne. Ilyen például a  $\text{let } e \text{ in } x.e'$ , mely pl. azt fejezheti ki, hogy  $e'$ -ben az  $x$  előfordulásai  $e$ -t jelentenek (ez a  $\text{let}$  kifejezések egy lehetséges szemantikája, de ebben a fejezetben csak szintaxisal foglalkozunk, emiatt nem igaz, hogy  $\text{let } e \text{ in } x.x + x = e + e$ ). Azt mondjuk, hogy az  $x$  változó kötve van az  $e'$  kifejezésben. A  $\text{let}$  operátor aritását  $(\text{Exp}, \text{Exp}.\text{Exp})\text{Exp}$ -el jelöljük, az operátor második paraméterében köt egy  $\text{Exp}$  fajtájú változót. Pl.  $\text{let num}(\text{succ zero}) \text{ in } x.x + (\text{num zero} + x)$  kifejezésben a  $+$  operátor  $x$  paraméterei a kötött  $x$ -re vonatkoznak. Ezt a következőképp ábrázolhatjuk. A felfele mutató szaggatott nyilak mutatják, hogy az  $x$  változók melyik kötésre mutatnak. A pont után szereplő  $x + (\text{num zero} + x)$  rész kifejezést az  $x$  változó *hatáskörének* nevezzük.



A `let`-tel kiegészített `Exp` fajtájú ABT-eket a következő jelöléssel adjuk meg. A pont azelőtt a paraméter előtt van, amiben kötjük a változót.

$$e, e' \in \text{Exp} ::= x \mid \text{num } n \mid e + e' \mid \text{let } e \text{ in } x.e'$$

A `let num zero in x.x + x` ABT  $x + x$  részfája tartalmaz egy *szabad változót*, az  $x$ -et, emiatt az  $x + x$  ABT nyílt. Mivel  $x + x$ -ben csak az  $x$  a szabad változó, a kötés zárttá teszi a kifejezést, tehát a `let num zero in x.x + x` ABT zárt. A kötések hatásköre a lehető legtovább tart, emiatt

$$\text{let } e \text{ in } x.(e_0 + e_1) = \text{let } e \text{ in } x.e_0 + e_1 \neq (\text{let } e \text{ in } x.e_0) + e_1.$$

Az alábbi `Exp` fajtájú ABT-k kötött változóit aláhúztuk, szabad változóit felülhúztuk.

`let num zero in x.x + x`

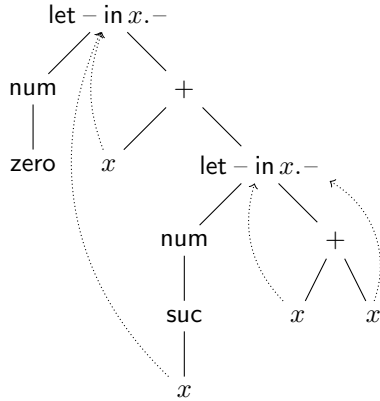
`let y in x.x + x`

`let y in x.x + let x in z.z`

`let y in x.x + let z in z.z`

A kötött változók csak pozíciókra mutatnak, a nevük nem érdekes. Például a `let num zero in x.x + x` és a `let num zero in y.y + y` ABT-k megegyeznek ( $\alpha$ -konvertálhatónak vagy  $\alpha$ -ekvivalensnek szokás őket nevezni). A szabad változókra ez nem igaz, pl.  $x + x \neq y + y$ .

Ha többször ugyanazt a változót kötjük egy ABT-ben, az újabb kötés *elfedi* az előzőt. Pl. `let num zero in x.x + (let num (suc x) in x.x + x)`-ben az  $x + x$ -ben levő  $x$ -ek a második kötésre (ahol `num (suc x)`-et adtunk meg) mutat (a `num (suc x)`-ben levő  $x$  viszont az első kötésre mutat).



Az elfedés megszüntethető a változónevek átnevezésével: `let num zero in y.y + + (let num (suc y) in x.e)`. Ebben az ABT-ben már hivatkozhatunk az  $e$  részében az  $x$ -re is meg a külső  $y$ -ra is.

Helyettesíteni tudunk ABT-kben is, pl. szeretnénk a következő egyenlőségeket.

$$(\text{let } x \text{ in } x'.x' + x'')[x'' \mapsto \text{num zero}] = \text{let } x \text{ in } x'.x' + \text{num zero}$$

$$(\text{let } x \text{ in } x'.x' + x'')[x' \mapsto \text{num zero}] = \text{let } x \text{ in } x'.x' + x''$$

$$(\text{let } x \text{ in } x'.x' + x'')[x'' \mapsto x'] = \text{let } x \text{ in } x'''.x''' + x'$$

Az első esetben egyszerűen behelyettesítünk az  $x'$ -t kötő művelet alatt. A második esetben, mivel a kötés elfedi az  $x'$  változót, a kötés hatáskörében levő  $x'$ -k mind a kötésre vonatkoznak, ezért nem történik semmi. A harmadik eset érdekesebb: itt azért, hogy a kötés alá mentünk, naivan csak lecserélnénk az  $x''$ -t  $x'$ -re, de ezzel az  $x'$  kötötté válna, és nem a „külső”  $x'$ -re, hanem a kötöttre vonatkozna, megváltoztatva ezzel az ABT jelentését. Emiatt a kötésre egy másik, még nem használt változót,  $x'''$ -t használjuk.

Általánosságban a következőképp tudjuk megadni a helyettesítést egy  $f$  operátorra, mely az első paraméterében köt<sup>1</sup>.

$$(f(y.t) t_1 \dots t_n)[x \mapsto a] := f\left(\left(z.(t[y \mapsto z])[x \mapsto a]\right)(t_1[x \mapsto a]) \dots (t_n[x \mapsto a])\right)$$

(ahol  $z$  friss változónév)

A biztonság kedvéért (lásd a fenti harmadik példát), a kötött változót átnevezzük egy friss  $z$  változóra, és csak ezután a helyettesítés után helyettesítjük a megmaradt  $x$ -eket  $a$ -val.

Ha szeretnénk szerkezeti indukcióval egy  $Q$  állítást a  $\text{let}$ -tel kiegészített  $\text{Exp}$  ABT-kről bizonyítani, a következőket kell belátnunk:

- minden  $x$  változóra  $Q(x)$ ,
- minden  $n \in \text{Nat}$ -ra  $Q(n)$ ,
- minden  $e, e' \in \text{Exp}$ -re, ha  $Q(e)$  és  $Q(e')$ , akkor  $Q(e + e')$ ,
- minden  $e, e' \in \text{Exp}$ -re és  $x$  változóra, ha  $Q(e)$  és  $Q(e')$ , akkor  $Q(\text{let } e \text{ in } x.e')$ .

**2.3. Feladat.** *Húzd alá a kötött változókat és fölé a szabad változókat! A kötött változóknál rajzolj egy nyilat, hogy melyik kötésre mutatnak!*

```

x + num i
let x in x.num i + x
let x in x.x' + let x in x'.x' + x
let x in x.x + let x in x.x + x
let x in x.(let x in x'.x'' + x') + let x' in x'.x' + x''

```

**2.4. Feladat.** *Lehet-e egy  $i \in \text{Var}_{\text{Nat}}$  egy  $\text{Exp}$  fájtájú ABT-ben kötött?*

**2.5. Feladat.** *Adj algoritmust arra, hogy két ABT mikor egyenlő általános esetben. Az érdekes rész annak eldöntése, hogy egy  $f x.t t_1 \dots t_n$  alakú és egy  $f x'.t' t'_1 \dots t'_n$  alakú ABT egyenlő-e.*

**2.6. Feladat.** *Végezd el a következő helyettesítéseket!*

```

(let x in x.x + x)[x ↦ num zero]
(let x' in x.x' + x)[x' ↦ num zero]
(let x' in x.x' + x')[x' ↦ x]

```

<sup>1</sup> Ha több paraméterben van kötés, azt is hasonlóan lehet megadni.

**2.7. Feladat.** *Döntsd el, hogy a következő Exp fajtájú ABT-k megegyeznek-e!*

$$\begin{aligned}
x + \text{num } i &\stackrel{?}{=} x + \text{num } i' \\
\text{let } x \text{ in } x.\text{num } i + x &\stackrel{?}{=} \text{let } x \text{ in } x'.\text{num } i + x' \\
\text{let } x \text{ in } x.\text{num } i + x &\stackrel{?}{=} \text{let } x \text{ in } x.\text{num } i + x' \\
\text{let } x \text{ in } x.x' + \text{let } x \text{ in } x'.x' + x &\stackrel{?}{=} \text{let } x \text{ in } x'.x + \text{let } x' \text{ in } x.x + x' \\
\text{let } x \text{ in } x.x' + \text{let } x \text{ in } x'.x' + x &\stackrel{?}{=} \text{let } x \text{ in } x''.x' + \text{let } x'' \text{ in } x.x + x'' \\
\text{let } x \text{ in } x.x + \text{let } x \text{ in } x.x + x &\stackrel{?}{=} \text{let } x \text{ in } x'.x' + \text{let } x' \text{ in } x'.x' + x'
\end{aligned}$$

**2.8. Feladat.** *Írj minél több zárt ABT-t az alább megadott fajtában. d aritása (A.A)A, g aritása (A, A)A.*

$$\begin{aligned}
a \in A &::= y \mid d \ y.a \mid g \ a \ a \\
y, y', \dots &\in \text{Var}_A
\end{aligned}$$

További információ:

- Az  $\alpha$ -ekvivalencia legegyszerűbb implementációja a De Bruijn indexek használata. Változónevek helyett természetes számokat használunk, melyek azt mutatják, hogy hányadik kötésre mutat a változó. Pl.  $d \ y.d \ y'.y$  helyett  $d \ (d \ 1)\text{-et}$  írunk (0 mutatna a legközelebbi kötésre).

### 2.3. Levezetési fák

*Ítéleteket* ABT-kről mondunk. Néhány példa ítéletekre és a lehetséges jelentésükre:

$n \text{ nat}$	$n$ egy természetes szám
$n + n' \text{ is } n''$	az $n$ és $n'$ természetes számok összege $n''$
$e \text{ hasHeight } n$	az $e$ bináris fának $n$ a magassága
$e : \tau$	az $e$ kifejezésnek $\tau$ a típusa
$e \mapsto e'$	az $e$ kifejezés $e'$ -re redukálódik

Az ítéletek *levezetési szabályokkal* vezethetők le. A levezetési szabályok általános formája az alábbi.  $J_1, \dots, J_n$ -t feltételeknek,  $J$ -t következménynek nevezzük.

$$\frac{J_1 \quad \dots \quad J_n}{J}$$

Az  $n + n' \text{ is } n''$  ítélethez például az alábbi kettő levezetési szabályt adjuk meg.

$$\frac{}{\text{zero} + n' \text{ is } n'} \quad (2.3)$$

$$\frac{n + n' \text{ is } n''}{\text{suc } n + n' \text{ is } \text{suc } n''} \quad (2.4)$$

Az első szabály azt fejezi ki, hogy nullát hozzáadva bármilyen számhoz ugyanazt a számot kapjuk. A második szabály azt fejezi ki, hogy ha tudjuk két szám összegét, akkor az első rákövetkezőjének és a másodiknak az összege az összeg



rákövetkezője lesz. Az  $n, n', n''$  metaváltozók bármilyen Nat fajtájú ABT-t jelenthetnek. A 2.3 szabályban fontos, hogy a két  $n'$  mindig ugyanaz kell, hogy legyen. Megjegyezzük, hogy ebben az ítéletben a  $+$ -nak semmi köze nincsen az Exp fajtájú ABT-kben szereplő  $+$  operátorhoz, csak véletlenül ugyanazzal a karakterrel jelöljük.

A levezetési szabályok *levezetési fává* (levezetéssé) kombinálhatók. Pl. azt, hogy  $2 + 1 = 3$ , a következőképp tudjuk levezetni.

$$\frac{\frac{\overline{\text{zero} + \text{suc zero is suc zero}} \quad (2.3)}{\text{(suc zero)} + \text{suc zero is suc (suc zero)}} \quad (2.4)}{\text{suc (suc zero)} + \text{suc zero is suc (suc (suc zero))}} \quad (2.4)$$

A levezetési fa gyökerénél van, amit levezettünk, és mindegyik lépésben valamelyik szabályt alkalmaztuk: az alkalmazott szabály száma a vízszintes vonal mellé van írva.

Az olyan levezetési szabályokat, melyeknek nincs feltétele, *axiómának* nevezzük. A levezetési fák leveleinél mindig axiómák vannak.

Az  $n$  nat ítélet azt fejezi ki, hogy  $n$  egy természetes szám. A következő szabályokkal tudjuk levezetni.

$$\overline{\text{zero nat}} \quad (2.5)$$

$$\frac{n \text{ nat}}{\text{suc } n \text{ nat}} \quad (2.6)$$

Ezek azt fejezik ki, hogy a 0 természetes szám, és bármely természetes szám rákövetkezője is az. N.b. azt nem tudjuk levezetni, hogy  $i$  nat egy  $i$  változóra. A természetes számokra gondolhatunk úgy, mint a zárt Nat fajtájú ABT-kre.

A következő levezetési szabályok azt fejezik ki, hogy az Exp fajtájú AST kiegyensúlyozott, és magassága  $n$ . Az ítélet általános alakja  $e$  isBalanced  $n$ .

$$\overline{x \text{ isBalanced zero}} \quad (2.7)$$

$$\overline{\text{num } n \text{ isBalanced zero}} \quad (2.8)$$

$$\frac{e \text{ isBalanced } n \quad e' \text{ isBalanced } n}{e + e' \text{ isBalanced suc } n} \quad (2.9)$$

Egy példa levezetés.

$$\frac{\frac{\overline{x' \text{ isBalanced zero}} \quad \overline{x \text{ isBalanced zero}}}{x + x \text{ isBalanced suc zero}} \quad \frac{\overline{x' \text{ isBalanced zero}} \quad \overline{\text{num } i \text{ isBalanced zero}}}{x' + \text{num } i \text{ isBalanced suc zero}}}{(x + x) + (x' + \text{num } i) \text{ isBalanced suc (suc zero)}}$$

Ha valamit be szeretnénk bizonyítani minden levezethető ítéletről, ehhez a szabályok szerinti szerkezeti indukciót használhatjuk. Azt szeretnénk belátni, hogy ha  $J$  levezethető, akkor  $\mathcal{P}(J)$  igaz. Ebben az esetben elég belátnunk azt, hogy minden szabályra, melynek feltételei  $J_1, \dots, J_n$  és következménye  $J$ , ha  $\mathcal{P}(J_1), \dots, \mathcal{P}(J_n)$  mind teljesül, akkor  $\mathcal{P}(J)$  is.

A szerkezeti indukció konkrét használatára mutatunk két példát.

A fenti 2.3 szabály alapján bármely  $n \in \text{Nat}$ -ra le tudjuk vezetni, hogy  $\text{zero} + n$  is  $n$ . Megmutatjuk a másik irányt.

**2.9. Lemma.** *Ha  $n$  egy természetes szám, akkor  $n + \text{zero}$  is  $n$ .*

*Bizonyítás.* Indukció a természetes számok levezetésén. A fenti  $P$ -t úgy választjuk meg, hogy  $P(n \text{ nat}) := n + \text{zero}$  is  $n$ . Ha a 2.5 szabályt használtuk, akkor  $P(\text{zero nat}) = \text{zero} + \text{zero}$  is  $\text{zero}$ -t kell bizonyítanunk, ezt megtesszük a 2.3 szabállyal. Ha a 2.6 szabályt használtuk, akkor az indukciós hipotézis azt mondja, hogy  $P(n \text{ nat}) = n + \text{zero}$  is  $n$ , nekünk pedig azt kell bizonyítani, hogy  $P(\text{suc } n \text{ nat}) = \text{suc } n + \text{zero}$  is  $\text{suc } n$ . A 2.4 szabályt használjuk, a feltételét az indukciós feltevésünk adja meg.  $\square$

Második példaként bebizonyítjuk, hogy ha van egy kiegyensúlyozott fánk, és ebbe behelyettesítünk egy 0 magasságú fát, akkor a kapott fa is kiegyensúlyozott lesz.

**2.10. Lemma.** *Ha  $e_1$  isBalanced zero és  $e$  isBalanced  $n$ , akkor bármely  $x_1$ -re  $e[x_1 \mapsto e_1]$  isBalanced  $n$ .*

*Bizonyítás.*  $e$  isBalanced  $n$  levezetése szerinti indukcióval bizonyítunk, tehát  $P(e \text{ isBalanced } n) = e[x_1 \mapsto e_1] \text{ isBalanced } n$ . A következő eseteket kell ellenőriznünk.

- Ha a 2.7 szabályt használtuk  $e$  isBalanced  $n$  levezetésére, akkor azt kell belátnunk, hogy  $e[x_1 \mapsto e_1]$  isBalanced zero. Ha  $x = x_1$ , akkor ez azzal egyezik meg, hogy  $e'_1$  isBalanced zero, ezt pedig tudjuk. Ha  $x \neq x_1$ , akkor a 2.7 szabályt használjuk újra.
- Ha a 2.8 szabályt használtuk, akkor azt kell belátnunk, hogy  $(\text{num } n)[x_1 \mapsto e_1]$  isBalanced zero, viszont a helyettesítés itt nem végez semmit, tehát a 2.8 szabályt újra alkalmazva megkapjuk a kívánt eredményt.
- Ha a 2.9 szabályt alkalmaztuk, akkor az indukciós feltevésekből tudjuk, hogy  $e[x_1 \mapsto e_1]$  isBalanced  $n$  és  $e'[x_1 \mapsto e_1]$  isBalanced  $n$ , és azt szeretnénk belátni, hogy  $(e + e')[x_1 \mapsto e_1]$  isBalanced  $\text{suc } n$ , de a helyettesítés definíciója alapján ez megegyezik  $e[x_1 \mapsto e_1] + e'[x_1 \mapsto e_1]$  isBalanced  $\text{suc } n$ -al, amit pedig a 2.9 szabály alapján látunk.

$\square$

**2.11. Feladat.** *Adjuk meg a  $\max n n'$  is  $n''$  ítélet levezetési szabályait. Az ítélet azt fejezi ki, hogy  $n$  és  $n'$  Nat-beli AST-k maximuma  $n''$ .*

**2.12. Feladat.** *Ennek segítségével adjuk meg a  $e$  hasHeight  $n$  ítélet levezetési szabályait, ahol  $e$  egy Exp fajtájú,  $n$  pedig egy Nat fajtájú AST.*

**2.13. Feladat.** *Adjuk meg a isEven  $n$  és isOdd  $n$  ítéletek levezetési szabályait, melyek azt fejezik ki, hogy  $n$  páros ill. páratlan szám. A levezetési szabályok hivatkozhatnak egymásra.*

**2.14. Feladat.** *Igaz -e, hogy bármely két zárt természetes számra levezethető, hogy mennyi azok összege a természetes számok összegének két levezetési szabályával?*

További információ:

- Az AST-k, ABT-k és a levezetési fák mind induktív definíciók, típuselméletben induktív családokként formalizálhatók (inductive families). A szerkezeti indukció elvét ebben az esetben az eliminátor fejezi ki.

### 3. Számok és szövegek

Harper könyv: II. rész.

Ebben a fejezetben egy egyszerű nyelvet tanulmányozunk, mely számokból és szövegekből álló kifejezéseket tartalmaz. A nyelv szintaxisa az ABT-k definíciója, melyekből a nyelv áll. A típusrendszer az összes lehetséges ABT-t megszorítja értelmes ABT-kre. A szemantika pedig a nyelv jelentését adja meg: azt, hogy futási időben mi történik az ABT-kkel.

#### 3.1. Szintaxis

A szintaxis két fajtából áll, a típusokból és a kifejezésekből.

$$\begin{array}{ll} \tau, \tau', \dots \in \text{Ty} ::= \text{int} & \text{egész számok típusa} \\ & | \text{str} \quad \text{szövegek típusa} \end{array} \quad (3.1)$$

$$\begin{array}{ll} e, e', \dots \in \text{Exp} ::= x & \text{változó} \\ & | n \quad \text{egész szám beágyazása} \\ & | "s" \quad \text{szöveg beágyazása} \\ & | e + e' \quad \text{összeadás} \\ & | e - e' \quad \text{kivonás} \\ & | e \bullet e' \quad \text{összefűzés} \\ & | |e| \quad \text{hossz} \\ & | \text{let } e \text{ in } x.e' \quad \text{definíció} \end{array} \quad (3.2)$$

A típusok kétfélék lehetnek, `int` és `str`, típusváltozókat nem engedélyezünk. A kifejezések mellé írtuk a jelentésüket, általában így gondolunk ezekre a kifejezésekre, hogy ezek számokat, szövegeket reprezentálnak. De fontos, hogy ezek nem tényleges számok, csak azok szintaktikus reprezentációi. A szintaxis csak egy formális dolog, karakterek sorozata (pontosabban egy ABT), jelentését majd a szemantika adja meg.

Az `Exp` fajtájú változókat  $x, y, z$  és ezek indexelt változatai jelölik.

A két beágyazás operátor paramétere egy egész szám ill. egy szöveg, ezeket adottnak tételezzük fel, tehát a metanyelvünkben léteznek egész számok, pl. `0, 1, -2` és szövegek, pl. `hello`. A (jelöletlen) egész szám beágyazása operátorral a nyelvünkben `Exp` fajtájú kifejezés a `0, 1` és a `-2` is, míg az idézőjelekkel jelölt szöveg beágyazása operátorral `Exp` fajtájú kifejezés a `"hello"`. A `let` operátorral tudunk definíciókat írni ebben a nyelvben, pl. `let "ello" in x."h" • x • "b" • x`.

Az operátorok aritásai a szintaxis definíciójából leolvashatók, pl. a (jelöletlen) beágyazás operátor aritása  $(\mathbb{Z})\text{Exp}$ ,  $| - |$  aritása  $(\text{Exp})\text{Exp}$ , `let` aritása  $(\text{Exp}, \text{Exp}.\text{Exp})\text{Exp}$ .

**3.1. Feladat.** Írjuk fel az összes operátor aritását!

#### 3.2. Típusrendszer

A típusrendszer megszorítja a leírható kifejezéseket azzal a céllal, hogy az értelmetlen kifejezéseket kiszűrje. Pl. a  $|3|$  kifejezést ki szeretnénk szűrni, mert szeretnénk, hogy a `hossz` operátort csak szövegekre lehessen alkalmazni. Az,

hogy pontosan milyen hibákat szűr ki a típusrendszer, nincs egységesen meghatározva, ez a típusrendszer tervezőjén múlik.

Hogy a típusrendszert le tudjuk írni, szükségünk van még a környezetek (context) fajtájára. Egy környezet egy változókból és típusokból álló lista.

$$\Gamma, \Gamma', \dots \in \text{Con} ::= \cdot \mid \Gamma, x : \tau \quad (3.3)$$

A célunk a környezettel az, hogy megadja a kifejezésekben levő szabad változók típusait. A típusozási ítélet  $\Gamma \vdash e : \tau$  formájú lesz, ami azt mondja, hogy az  $e$  kifejezésnek  $\tau$  típusa van, feltéve, hogy a szabad változói típusai a  $\Gamma$  által megadottak.

Emiatt bevezetünk egy megszorítást a környezetekre: egy változó csak egyszer szerepelhet. Először is megadunk egy függvényt, mely kiszámítja a környezet változóit tartalmazó halmazt.

$$\begin{aligned} \text{dom}(\cdot) &:= \{\} \\ \text{dom}(\Gamma, x : \tau) &:= \{x\} \cup \text{dom}(\Gamma) \end{aligned} \quad (3.4)$$

A  $\Gamma \text{ wf}$  ítélet azt fejezi ki, hogy a  $\Gamma$  környezet jól formált.

$$\overline{\cdot \text{ wf}} \quad (3.5)$$

$$\frac{\Gamma \text{ wf} \quad x \notin \text{dom}(\Gamma)}{\Gamma, x : \tau \text{ wf}} \quad (3.6)$$

Ezután csak jól formált környezetekkel fogunk dolgozni.

Bevezetünk egy ítéletet, amely azt mondja, hogy egy változó-típus pár benne van egy környezetben.

$$\frac{\Gamma \text{ wf} \quad x \notin \text{dom}(\Gamma)}{(x : \tau) \in \Gamma, x : \tau} \quad (3.7)$$

$$\frac{(x : \tau) \in \Gamma \quad y \notin \text{dom}(\Gamma)}{(x : \tau) \in \Gamma, y : \tau'} \quad (3.8)$$

Az első szabály azt fejezi ki, hogy ha egy környezet utolsó alkotóeleme  $x : \tau$ , akkor ez természetesen szerepel a környezetben. Továbbá, ha egy környezetben  $x : \tau$  szerepel, akkor egy  $y$  változóval kiegészített környezetben is szerepel.

A típusrendszerrel  $\Gamma \vdash e : \tau$  formájú ítéleteket lehet levezetni, ami azt jelenti, hogy a  $\Gamma$  környezetben az  $e$  kifejezésnek  $\tau$  típusa van. Úgy is gondolhatunk erre, hogy  $e$  egy program, melynek típusa  $\tau$  és a program paraméterei és azok típusai  $\Gamma$ -ban vannak megadva. A levezetési szabályok a következők.

$$\frac{(x : \tau) \in \Gamma}{\Gamma \vdash x : \tau} \quad (3.9)$$

$$\frac{\Gamma \text{ wf}}{\Gamma \vdash n : \text{int}} \quad (3.10)$$

$$\frac{\Gamma \text{ wf}}{\Gamma \vdash "s" : \text{str}} \quad (3.11)$$

$$\frac{\Gamma \vdash e_1 : \text{int} \quad \Gamma \vdash e_2 : \text{int}}{\Gamma \vdash e_1 + e_2 : \text{int}} \quad (3.12)$$

$$(3.13)$$

(3.14)

(3.15)

$$(3.16)$$

Példa levezetés:

$$\begin{array}{c}
\frac{\cdot \text{wf}^{3.5} \quad x \notin \{\}}{(x : \text{str}) \in \cdot, x : \text{str}}^{3.7} \quad \frac{\cdot \text{wf}^{3.5} \quad x \notin \{\}}{\cdot, x : \text{str} \text{ wf}}^{3.6} \\
\frac{\cdot, x : \text{str} \vdash x : \text{str}}{\cdot, x : \text{str} \vdash |x| : \text{int}}^{3.9} \quad \frac{\cdot, x : \text{str} \text{ wf}}{\cdot, x : \text{str} \vdash 2 : \text{int}}^{3.10} \\
\frac{\cdot \text{wf}^{3.5}}{\cdot \vdash \text{"a"} : \text{str}}^{3.11} \quad \frac{\cdot, x : \text{str} \vdash |x| : \text{int}}{\cdot, x : \text{str} \vdash |x| + 2 : \text{int}}^{3.15} \\
\frac{\cdot \vdash \text{"a"} : \text{str} \quad \cdot, x : \text{str} \vdash |x| + 2 : \text{int}}{\cdot \vdash \text{let "a" in } x. |x| + 2 : \text{int}}^{3.16}
\end{array}$$

A [3] kifejezés nem típusozható, mert csak a 3.15. szabállyal vezethető le  $|e|$  alakú kifejezés, ez a szabály viszont azt követeli meg, hogy a 3 kifejezés str típusú legyen. Ezt azonban egyik szabállyal sem lehet levezetni.

Most tételeket fogunk kimondani a típusrendszeréről. Fontos, hogy legyen intuíciónk arról, hogy miért igazak ezek a tételek. A bizonyítások általában egyszerű szerkezeti indukciók, de némely lépésben korábbi tételeket is felhasználunk. A bizonyítások megértéséhez feltétlenül szükséges, hogy ne csak elolvassuk őket, hanem magunk is levezessük őket papíron.

A típusrendszer nem triviális, tehát nem igaz, hogy minden kifejezés típusozható.

**3.2. Lemma.** *Van olyan  $e$  melyre nem létezik  $\Gamma$  és  $\tau$  hogy  $\Gamma \vdash e : \tau$ .*

*Bizonyítás.* Például az előbbi [3].

Minden kifejezés maximum egyféleképpen típusozható (típusok unicitása).

**3.3. Lemma.** *Egy e kifejezéshez és  $\Gamma$  környezethez maximum egy  $\tau$  típus tartozik, melyre  $\Gamma \vdash e : \tau$ .*

*Bizonyítás.* Azt látjuk be a  $\Gamma \vdash e : \tau$  levezetése szerinti indukcióval, hogy másik  $\tau' \neq \tau$  típusra nincs olyan szabály, mely levezetné  $\Gamma \vdash e : \tau'$ -t. A változó esetén a szabály szerinti indukcióval belátjuk, hogy ha  $(x : \tau) \in \Gamma$ , akkor nem lehet, hogy  $(x : \tau') \in \Gamma$  valamely  $\tau' \neq \tau$ -ra.  $\square$

A típusrendszer ezenkívül szintaxisvezérelt: ez azt jelenti, hogy minden kifejezésformát pontosan egy szabály tud levezetni. Emiatt a típusozás megfordítható. A típus levezetési szabályok azt adják meg, hogy melyek az elégséges feltételek ahhoz, hogy egy kifejezés típusozható legyen. Pl. ahhoz, hogy  $e_1 + e_2$  típusa int legyen, elég az, hogy  $e_1$  és  $e_2$  típusa int ugyanabban a környezetben. Mi meg tudjuk adni a szükséges feltételeket is (típusozás inverziója). Ez mutatja meg, hogyan tudunk egy típusellenőrző programot írni ehhez a típusrendszerhez.

**3.4. Lemma.**  $\Gamma \vdash e : \tau$  levezethető. Ekkor, ha  $e = e_1 + e_2$ , akkor  $\tau = \text{int}$ ,  $\Gamma \vdash e_1 : \text{int}$  és  $\Gamma \vdash e_2 : \text{int}$ . Hasonlóképp az összes többi operátorra.

*Bizonyítás.* A levezetés szerinti indukcióval.  $\square$

A környezetben a változó-típus párok sorrendje nem számít ebben a típusrendszerben. Ezt fejezi ki a következő lemma.

**3.5. Lemma.** Ha  $\Gamma \vdash e : \tau$ , akkor  $\Gamma' \vdash e : \tau$ , feltéve, hogy  $\Gamma'$  a  $\Gamma$  egy permutációja (ugyanazok a változó-típus párok, csak más sorrendben).

*Bizonyítás.* A  $\Gamma \vdash e : \tau$  levezetése szerinti indukcióval. A 3.10–3.15. szabályoknál csak az induktív hipotéziseket, majd a szabályt használjuk. A 3.16. szabály esetén azt szeretnénk belátni, hogy  $\Gamma' \vdash \text{let } e_1 \text{ in } x.e_2 : \tau_2$ , feltéve, hogy  $\Gamma' \vdash e_1 : \tau_1$  és  $\Gamma'' \vdash e_2 : \tau_2$ , ha  $\Gamma''$  a  $\Gamma, x : \tau_1$  egy permutációja. Mivel  $\Gamma'$  a  $\Gamma$  egy permutációja, ezért a  $\Gamma', x : \tau_1$  a  $\Gamma, x : \tau_1$  permutációja, így ez az indukciós feltevés azt mondja, hogy  $\Gamma', x : \tau_1 \vdash e_2 : \tau_2$ . Ezt felhasználva a 3.16. szabály alapján megkapjuk, hogy  $\Gamma' \vdash \text{let } e_1 \text{ in } x.e_2 : \tau_2$ . A 3.9. szabály esetén azt látjuk be, hogy ha  $(x : \tau) \in \Gamma$ , és  $\Gamma'$  a  $\Gamma$  egy permutációja, akkor  $(x : \tau) \in \Gamma'$ . Itt egyszerűen annyiszor alkalmazzuk a 3.6 szabályt, ahányadik komponens  $(x : \tau)$  hátulról  $\Gamma'$ -ben.  $\square$

A típusrendszer egy további fontos tulajdonsága a gyengítési tulajdonság.

**3.6. Lemma.** Ha  $\Gamma \vdash e : \tau$  levezethető, és  $y \notin \text{dom}(\Gamma)$ , akkor  $\Gamma, y : \tau' \vdash e : \tau$  is levezethető bármely  $\tau'$ -re.

Ez a tulajdonság azt fejezi ki, hogy egy jól típusozott kifejezést tetszőleges olyan környezetben használhatunk, amiben meg vannak adva a szabad változói. Tehát ha írunk egy típushelyes programot, és ezután további paramétereket adunk meg a programnak, akkor a program ugyanúgy típushelyes marad.

*Bizonyítás.* A levezetés szerinti indukcióval. Tehát  $P(\Gamma \vdash e : \tau) = \Gamma, y : \tau' \vdash e : \tau$ , ahol  $y \notin \text{dom}(\Gamma)$ . A változó esetében eggyel többször használjuk a 3.8. szabályt, a 3.10–3.11. szabályok esetén ugyanazeket a szabályokat alkalmazzuk más környezetekre, a 3.12–3.15. szabályok esetén az indukciós feltevést használjuk, majd magát a szabályt. A 3.16. szabály esetén az indukciós feltevés azt mondja, hogy  $\Gamma, y : \tau' \vdash e_1 : \tau_1$  és  $\Gamma, x : \tau_1, y : \tau' \vdash e_2 : \tau_2$ , nekünk pedig azt kell belátnunk, hogy  $\Gamma, y : \tau' \vdash \text{let } e_1 \text{ in } x.e_2 : \tau_2$ . Mivel  $\Gamma, y : \tau', x : \tau_1$  a  $\Gamma, x : \tau_1, y : \tau'$  környezet egy permutációja, a 3.5. lemma alapján megkapjuk, hogy  $\Gamma, y : \tau', x : \tau_1 \vdash e_2 : \tau_2$ , így alkalmazhatjuk a 3.16. szabályt.  $\square$

Helyettesítési lemma.

**3.7. Lemma.** Ha  $\Gamma, x : \tau \vdash e' : \tau'$  és  $\Gamma \vdash e : \tau$ , akkor  $\Gamma \vdash e'[x \mapsto e] : \tau'$ .

Ez a lemma a modularitást fejezi ki: van két külön programunk,  $e : \tau$  és  $e' : \tau'$ , utóbbi deklarál egy  $\tau$  típusú változót.  $e$ -t  $\tau$  implementációjának,  $e'$ -t pedig  $e$  kliensének nevezzük. A 3.7. lemma azt mondja, hogy külön-külön típusellenőrizhetjük a két modult, és ekkor összetevés (linking) után is típushelyes lesz a programunk.

*Bizonyítás.*  $\Gamma, x : \tau \vdash e' : \tau'$  levezetése szerinti indukció. A 3.10–3.11. szabályok esetén nem csinál semmit a helyettesítés. A 3.12–3.15. szabályok esetén az indukciós feltevésekből következik a helyettesítés helyessége. Pl. a 3.12. szabály esetén tudjuk, hogy  $\Gamma, x : \tau \vdash e_1, e_2 : \text{int}$  és  $\Gamma \vdash e_1[x \mapsto e], e_2[x \mapsto e] : \text{int}$ , és azt szeretnénk belátni, hogy  $\Gamma \vdash (e_1 + e_2)[x \mapsto e] : \text{int}$ . Ez a helyettesítés definíciója alapján megegyezik azzal, hogy  $\Gamma \vdash e_1[x \mapsto e] + e_2[x \mapsto e] : \text{int}$ . Ezt a 3.12. szabály alkalmazásával megkapjuk. A 3.9 szabály alkalmazása esetén a kifejezésünk egy változó. Ha ez megegyezik  $x$ -szel, akkor a helyettesítés eredménye  $e$  lesz, és  $\tau = \tau'$ . Ekkor  $\Gamma \vdash e : \tau$  miatt készen vagyunk. Ha a változónevek nem egyeznek meg, a helyettesítés nem csinál semmit. A 3.16. szabály esetén az indukciós feltevés alapján tudjuk, hogy  $\Gamma \vdash e_1[x \mapsto e] : \tau_1$ . Ezenkívül  $\Gamma, x : \tau, y : \tau_1 \vdash e_2 : \tau_2$ , ebből a 3.5. lemma alapján  $\Gamma, y : \tau_1, x : \tau \vdash e_2 : \tau_2$ , majd az indukciós feltevés alapján kapjuk, hogy  $\Gamma, y : \tau_1 \vdash e_2[x \mapsto e] : \tau_2$ . Mivel  $(\text{let } e_1 \text{ in } y.e_2)[x \mapsto e] = \text{let } e_1[x \mapsto e] \text{ in } y.e_2[x \mapsto e]$ , a 3.16. szabály alapján kapjuk, hogy  $\Gamma \vdash (\text{let } e_1 \text{ in } y.e_2)[x \mapsto e] : \tau_2$ .  $\square$

A helyettesítési lemma ellentéte a dekompozíció. Ez azt fejezi ki, hogy ha egy programrészlet többször előfordul egy programban, akkor azt kiemelhetjük (és ezzel rövidebbé, érthetőbbé, könnyebben karbantarthatóbbá tesszük a programot).

**3.8. Lemma.** *Ha  $\Gamma \vdash e'[x \mapsto e] : \tau'$ , akkor minden olyan  $\tau$ -ra, melyre  $\Gamma \vdash e : \tau$ ,  $\Gamma, x : \tau \vdash e' : \tau'$ .*

*Bizonyítás.*  $\Gamma \vdash e'[x \mapsto e] : \tau'$  szerinti indukció.  $\square$

Összefoglalás: a következő tulajdonságokat bizonyítottuk a szövegek és számok nyelvének típusrendszeréről.

- 3.2. lemma: nem triviális.
- 3.3. lemma: típusok unicitása.
- 3.4. lemma: típusozás inverziója.
- 3.5. lemma: környezet változóinak sorrendje nem számít.
- 3.6. lemma: gyengítési tulajdonság.
- 3.7. lemma: helyettesítés.
- 3.8. lemma: dekompozíció.

**3.9. Feladat.** *Típusozhatók-e az alábbi kifejezések az üres környezetben? Próbáljuk meg levezetni a típusukat.*

- $|"ab" \bullet "cd" + |\text{let } "e" \text{ in } x.x + x|$
- $|"ab" \bullet "cd" + |\text{let } "e" \text{ in } x.x \bullet x|$
- $\text{let }|"ab" \bullet "cd"| \text{ in } x.x + x$
- $\text{let }|"ab" \bullet "cd"| \text{ in } x.x \bullet x$
- $|(|"aaa"|)|$

**3.10. Feladat.** Írjuk fel a 3.4. lemma összes esetét, és bizonyítsuk be őket.

**3.11. Feladat.** Bizonyítsuk be, hogy ha  $\Gamma \vdash e : \tau$ , akkor  $\Gamma \text{ wf}$ .

**3.12. Feladat.** Hogyan változna a típusrendszer, ha ugyanazt a  $+$  szimbólumot használnánk szövegek összefűzésére és számok összeadására is? Változnának-e a típusrendszer tulajdonságai?

További információ:

- A később tanulandó polimorf ill. függő típusrendszerekben nem igaz, hogy a környezet permutálható.
- A lineáris típusrendszerekben nem teljesül a gyengítési tulajdonság.

### 3.3. Operációs szemantika

A szemantika a szintaxis jelentését adja meg. Ez megtehető valamilyen matematikai struktúrával, ilyenkor minden szintaktikus objektumhoz az adott struktúra valamely elemét rendeljük. Ezt denotációs szemantikának hívják, és nem tárgyaljuk. Az operációs szemantika azt írja le, hogy melyik kifejezéshez melyik másik kifejezést rendeljük, tehát a program hogyan fut.

Az operációs szemantika megadható átíró rendszerekkel.

Egy átíró rendszerben  $e \mapsto e'$  alakú ítéleteket tudunk levezetni. Ez azt jelenti, hogy  $e$  kifejezés egy lépésben  $e'$ -re íródik át.

Az átírást iterálhatjuk, az iterált átíró rendszert az alábbi szabályokkal adjuk meg.

$$\overline{e \mapsto^* e} \quad (3.17)$$

$$\frac{e \mapsto e' \quad e' \mapsto^* e''}{e \mapsto^* e''} \quad (3.18)$$

A számok és szövegek nyelv bizonyos kifejezéseit *értékeknek* nevezzük. Értékek a zárt egész számok és a szövegek lesznek, melyekben a beágyazás operátorokon kívül más operátorok nincsenek. A program futását emiatt *kiértékelésnek* nevezzük: egy zárt kifejezésből értéket fogunk kapni.

Először megadjuk a nyelvünk értékeit az  $e \text{ val}$  formájú ítélettel.

$$\overline{n \text{ val}} \quad (3.19)$$

$$\overline{''s'' \text{ val}} \quad (3.20)$$

Az átíró rendszert az alábbi szabályok adják meg. A rövidség kedvéért a bináris operátorokra vonatkozó szabályok egy részét összevontuk.

$$\frac{n_1 + n_2 = n}{n_1 + n_2 \mapsto n} \quad (3.21)$$

$$\frac{n_1 - n_2 = n}{n_1 - n_2 \mapsto n} \quad (3.22)$$

$$\frac{s_1 \text{ és } s_2 \text{ konkatenáltja } s}{''s_1'' \bullet ''s_2'' \mapsto ''s''} \quad (3.23)$$

$$\frac{s \text{ hossza } n}{|''s''| \mapsto n} \quad (3.24)$$



$$\frac{e_1 \mapsto e'_1}{e_1 \circ e_2 \mapsto e'_1 \circ e_2} \quad \circ \in \{+, -, \bullet\} \quad (3.25)$$

$$\frac{e_1 \text{ val} \quad e_2 \mapsto e'_2}{e_1 \circ e_2 \mapsto e_1 \circ e'_2} \quad \circ \in \{+, -, \bullet\} \quad (3.26)$$

$$\frac{e \mapsto e'}{|e| \mapsto |e'|} \quad (3.27)$$

$$\left[ \frac{e_1 \mapsto e'_1}{\text{let } e_1 \text{ in } x.e_2 \mapsto \text{let } e'_1 \text{ in } x.e_2} \right] \quad (3.28)$$

$$\frac{[e_1 \text{ val}]}{\text{let } e_1 \text{ in } x.e_2 \mapsto e_2[x \mapsto e_1]} \quad (3.29)$$

A szemantikának két változata van: *érték szerinti* (by value) és *név szerinti* (by name) paraméterátadás. Utóbbinál elhagyjuk a zárójelezett 3.28. szabályt és a zárójelezett feltételt a 3.29. szabályból.

A 3.21–3.24. és a 3.29. szabályok utasítás szabályok, ezek adják meg, hogy ha egy operátornak már ki vannak értékelve a paraméterei, hogyan adjuk meg az eredményét. A 3.25–3.28. szabályok sorrendi szabályok, ezek adják meg, hogy milyen sorrendben történjék a kiértékelés. Például a  $| \text{"aa"} | + (3 - 2)$  kifejezés kiértékelését kezdhethjük úgy, hogy először a szöveg hosszát értékeljük ki, majd a jobb oldali számot, de úgy is, hogy először a számot, majd a szöveg hosszát. A fenti operációs szemantika az előbbit fogja választani, minden operátornak először kiértékeljük az első paraméterét, majd a másodikat, majd alkalmazzuk az operátort az értékekre.

Példa kiértékelés:

$$\begin{aligned} & | \text{"aa"} | + (3 - 2) \\ 3.25 \quad & \mapsto 2 + (3 - 2) \\ 3.22, 3.26 \quad & \mapsto 2 + 1 \\ 3.21 \quad & \mapsto 3 \end{aligned}$$

Érték szerinti paraméterátadásnál, mielőtt egy kifejezést hozzákötünk egy változóhoz, azt kiértékeljük. Így maximum egyszer értékelünk ki egy változót. Név szerinti paraméterátadás esetén nem értékeljük ki a kifejezést a kötés előtt, így ahányszor hivatkozunk rá, annyiszor fogjuk kiértékelni. Az érték szerinti paraméterátadás akkor pazarló, ha egyszer sem hivatkozunk a kötésre, a név szerinti akkor, ha több, mint egyszer hivatkozunk. A kettő előnyeit kombinálja az igény szerinti kiértékelés (call by need).

**3.13. Feladat.** Értékeljük ki a  $(1 + 1) - | \text{"aa"} \bullet \text{"bb"} |$  kifejezést, írjuk ki, hogy az egyes lépésekben melyik szabály(oka)t alkalmazzuk.

**3.14. Feladat.** Írjunk let kifejezést, amelynek kiértékelése megmutatja, hogy mi a különbség az érték szerinti és a név szerinti paraméterátadás között.

**3.15. Feladat.** Írjunk olyan let kifejezést, melynek kiértékelése érték szerinti paraméterátadásnál hatékonyabb.

**3.16. Feladat.** Írjunk olyan let kifejezést, melynek kiértékelése név szerinti paraméterátadásnál hatékonyabb.

Nyílt kifejezések kiértékelése nem juttat el minket egy értékeléshez, egy adott ponton *elakad*.

**3.17. Feladat.** *Értékeljük ki az  $x + (1 + 2)$  és az  $(1 + 2) + x$  kifejezéseket!*

Ha szeretnénk valamit bizonyítani az átíró rendszerünkről, a szerkezeti indukciót alkalmazhatjuk rá. Ez azt jelenti, hogy ha  $P(e \mapsto e')$ -t szeretnénk belátni minden  $e \mapsto e'$ -re, akkor azt kell megmutatni, hogy a 3.21–3.29. szabályok megtartják  $P$ -t.

Például bebizonyítjuk az alábbi lemmát.

**3.18. Lemma.** *Nincs olyan  $e$ , hogy  $e$  val és  $e \mapsto e'$  valamely  $e'$ -re.*

*Bizonyítás.*  $e \mapsto e'$  szerinti indukció: egyik szabálykövetkezmény sem  $n \mapsto e'$  vagy " $s$ "  $\mapsto e'$  alakú.  $\square$

Determináltság.

**3.19. Lemma.** *Ha  $e \mapsto e'$  és  $e \mapsto e''$ , akkor  $e' = e''$ .*

*Bizonyítás.*  $e \mapsto e'$  és  $e \mapsto e''$  szerinti indukció.  $\square$

A nyelvünk különböző típusokhoz tartozó operátorai kétféle csoportba oszthatók: *bevezető- és eliminációs operátorokra*. int típusú kifejezések bevezető operátora a jelöletlen egész szám beágyazása operátor, eliminációs operátorai a  $+$  és a  $-$ . A *sorrendi szabályok* azt mondják meg, hogy melyek egy eliminációs operátor *principális paraméterei* ( $+$  és  $-$  esetén mindkettő az), míg az utasítás szabályok azt adják meg, hogy ha a principális paraméterek a bevezető szabályokkal megadott alakúak, akkor hogyan kell kiértékelni az eliminációs operátort. Hasonlóképp, str típus esetén a " $-$ " a bevezető operátor, míg  $- \bullet -$  és  $|-|$  az eliminációs operátorok. Az *utasítás szabályok* itt is hasonló szimmetriát mutat: megmondja, mit kapunk, ha az eliminációs operátorokat alkalmazzuk a bevezető operátorra. A változó bevezetése és a let szerkezeti operátorok, nem kapcsolódnak specifikus típusokhoz.

**3.20. Feladat.** *Mutassuk meg, hogy bármely  $s_1, s_2$ -re létezik olyan  $e$ , hogy  $|s_1 \bullet s_2| \mapsto^* e$  és  $|s_1| + |s_2| \mapsto^* e$ .*

### 3.4. Típusrendszer és szemantika kapcsolata

A legtöbb programozási nyelv biztonságos, ami azt jelenti, hogy bizonyos hibák nem fordulhatnak elő a program futtatása során. Ezt úgy is nevezik, hogy a nyelv erős típusrendszerrel rendelkezik. A számok és szövegek nyelv esetén ez például azt jelenti, hogy nem fordulhat elő, hogy egy számhoz hozzáadunk egy szöveget, vagy két számot összefűzünk.

A típusmegőrzés (tárgyredukció, subject reduction, preservation) azt mondja ki, hogy ha egy típusozható kifejezésünk van, és egy átírási lépést végrehajtunk, ugyanazzal a típussal az átírt kifejezés is típusozható.  $\cdot \vdash e : \tau$  helyett egyszerűen  $e : \tau$ -t írunk.

**3.21. Tétel.** *Ha  $e : \tau$  és  $e \mapsto e'$ , akkor  $e' : \tau$ .*

*Bizonyítás.*  $e \mapsto e'$  szerinti indukció. A 3.21. szabály esetén tudjuk, hogy  $n_1 + n_2 \mapsto n$ , és  $n_1 + n_2 : \tau$ , és az inverziós lemmából (3.4) tudjuk, hogy  $\tau = \text{int}$ , és azt is tudjuk, hogy  $n : \text{int}$ . Hasonló a bizonyítás a 3.22–3.24. esetekben. A 3.25. esetén nézzük a  $+$  esetet: tudjuk, hogy  $e_1 + e_2 \mapsto e'_1 + e_2$ , és, hogy  $e_1 + e_2 : \tau$ . Az inverziós lemma azt mondja, hogy  $\tau = \text{int}$  és  $e_1 : \text{int}$ . Az indukciós hipotézisből azt kapjuk, hogy  $e_1 \mapsto e'_1$  és  $e'_1 : \text{int}$ . Így az összeadás levezetési szabálya (3.12) megadja, hogy  $e'_1 + e_2 : \text{int}$ . A 3.26. esetén ugyanilyen az indoklás, csak a második paraméter változik. A 3.27. esetén tudjuk, hogy  $|e| \mapsto |e'|$  és az indukciós hipotézisből és az inverzióból kapjuk, hogy  $e' : \text{str}$ , ebből a 3.15. szabály alapján kapjuk, hogy  $|e'| : \text{int}$ . A 3.28. szabály (érték szerinti paraméterátadás) esetén az inverzióból és az indukciós feltevésből tudjuk, hogy valamely  $\tau_1$  típusra  $e'_1 : \tau_1$ , és ebből a let típusozási szabálya (3.16) alapján kapjuk, hogy  $\text{let } e'_1 \text{ in } x.e_2 : \tau_2$ . A 3.29. szabály esetén inverzióból kapjuk, hogy  $e_1 : \tau_1$  valamilyen  $\tau_1$ -re és  $\cdot, x : \tau_1 \vdash \tau_2 : \tau_2$ . Azt szeretnénk belátni, hogy  $e_2[x \mapsto e_1] : \tau_2$ . Ezt a helyettesítési lemmával (3.7) látjuk be.  $\square$

Haladás (progress). Ez a tétel azt fejezi ki, hogy egy zárt, jól típusozott program nem akad el: vagy már ki van értékelve, vagy még egy átírási lépést végre tudunk hajtani.

**3.22. Tétel.** *Ha  $e : \tau$ , akkor vagy  $e$  val, vagy létezik olyan  $e'$ , hogy  $e \mapsto e'$ .*

A bizonyításhoz szükségünk van a következő lemmára a kanonikus alakokról.

**3.23. Lemma.** *Ha  $e : \tau$  és  $e$  val, akkor ha*

- $\tau = \text{int}$ , akkor  $e = n$  valamely  $n$ -re,
- $\tau = \text{str}$ , akkor  $e = "s"$  valamely  $s$ -re.

*Bizonyítás.*  $e$  val és  $e : \tau$  szerinti indukció.  $\square$

*A tétel bizonyítása.*  $e : \tau$  levezetése szerinti indukció. A 3.9. levezetés nem fordulhat elő, mert a környezet üres. A 3.10–3.11. esetén már értékeink vannak, és nincs olyan átírási szabály, mely alkalmazható lenne. A 3.12. szabály esetén az indukciós feltevésből azt kapjuk, hogy  $e_1 : \text{int}$  és vagy  $e_1$  val vagy létezik  $e_1 \mapsto e'_1$  lépés. Utóbbi esetben alkalmazhatjuk az  $e_1 + e_2 \mapsto e'_1 + e_2$  lépést, előbbi esetben megnézzük a másik indukciós feltevést, mely  $e_2$ -re vonatkozik. Ez azt mondja, hogy vagy  $e_2$  val, vagy  $e_2 \mapsto e'_2$ . Utóbbi esetben alkalmazzuk az  $e_1 + e_2 \mapsto e_1 + e'_2$  átírási szabályt, előbbi esetben tudjuk, hogy  $e_1$  val és  $e_2$  val, és hogy  $e_1 : \text{int}$  és  $e_2 : \text{int}$ . A 3.23. lemmából és ebből kapjuk, hogy  $e_1 = n_1$  és  $e_2 = n_2$ , így ha  $n_1$  és  $n_2$  összege  $n$ , akkor a 3.21. szabály szerinti  $e_1 + e_2 \mapsto n$  átírást hajtjuk végre. A 3.13–3.14. esetben hasonló módon járunk el. A 3.15. esetben az indukciós feltevésből tudjuk, hogy  $e : \text{str}$  és vagy  $e$  val vagy  $e \mapsto e'$ . Előbbi esetben a 3.23. lemmából kapjuk, hogy  $e = "s"$  valamely  $s$ -re, és ha  $s$  hossza  $n$ , akkor végrehajtjuk a  $"s" \mapsto n$  átírást (a 3.24. szabály), utóbbi esetben a 3.27. szabály alapján lépünk  $|e| \mapsto |e'|$ -t. A 3.16. szabály használatakor név szerinti paraméterátadás esetén a  $\text{let } e_1 \text{ in } x.e_2 \mapsto e_2[x \mapsto e_1]$  lépést tesszük meg (3.29), érték szerinti paraméterátadás esetén az indukciós feltevéstől függően tesszük meg a 3.29. vagy a 3.28. lépést.  $\square$

### 3.5. Futási idejű hibák

Ha a nyelvünkbe beteszünk egy  $-/-$  operátort, mely az egész osztást adja meg, a típusrendszert ill. az operációs szemantikát az alábbi szabályokkal egészítenénk ki.

$$\frac{\Gamma \vdash e_1 : \text{int} \quad \Gamma \vdash e_2 : \text{int}}{\Gamma \vdash e_1/e_2 : \text{int}} \quad (3.30)$$

$$\frac{n_1 \text{ osztva } n_2\text{-vel } n}{n_1/n_2 \mapsto n} \quad (3.31)$$

A probléma, hogy az  $n_1/0$  kifejezés kiértékelése elakad, nem igaz, hogy  $n_1$  osztva 0-val  $n$ , bármilyen  $n$ -et is választunk. Ezt kétféleképpen lehet kezelni:

1. A típusrendszer kizárja az ilyen eseteket, tehát  $n/0$  nem lesz típusozható. Ehhez az kell, hogy a típusrendszer eldöntse, hogy egy kifejezés 0 lesz -e, ha kiértékeljük. Ez nehéz.
2. Az ilyen típusú hibát futási időben ellenőrizzük, hibát ad a program futtatása.

Utóbbival foglalkozunk.

Az operációs szemantikát kiegészítjük az  $e \text{ err}$  ítélettel, ami azt fejezi ki, hogy  $e$  kiértékelése hibával végződik. A következő levezetési szabályokkal egészítjük ki a 3.21–3.29. szabályokkal megadott átíró rendszert.

$$\frac{e_1 \text{ val}}{e_1/0 \text{ err}} \quad (3.32)$$

$$\frac{e_1 \text{ err}}{e_1/e_2 \text{ err}} \quad (3.33)$$

$$\frac{e_1 \text{ val} \quad e_2 \text{ err}}{e_1/e_2 \text{ err}} \quad (3.34)$$

Hasonlóan a többi szabály is propagálja a hibákat. Például az összeadás a következőképp.

$$\frac{e_1 \text{ err}}{e_1 + e_2 \text{ err}} \quad (3.35)$$

$$\frac{e_1 \text{ val} \quad e_2 \text{ err}}{e_1 + e_2 \text{ err}} \quad (3.36)$$

**3.24. Feladat.** *Add meg a többi operátorra is a hibák propagálási szabályait.*

Bevezetjük a hiba kifejezést. A nyelvet kiegészítjük egy **error** kifejezéssel.

$$\text{Exp} ::= \dots \mid \text{error} \quad (3.37)$$

A típusrendszert a következő szabállyal egészítjük ki.

$$\frac{\Gamma \text{ wf}}{\Gamma \vdash \text{error} : \tau} \quad (3.38)$$

Az operációs szemantika a következő szabállyal egészül ki.

$$\overline{\text{error err}} \quad (3.39)$$

**3.25. Feladat.** *Egészítsük ki a 3.22. tételt hibákkal. Tehát bizonyítsuk be, hogy ha  $e : \tau$ , akkor vagy  $e \text{ err}$ , vagy  $e \text{ val}$ , vagy létezik olyan  $e'$ , hogy  $e \mapsto e'$ .*

**3.26. Feladat.** *Egészítsük ki a nyelvet (szintaxist, típusrendszert, operációs szemantikát) egy operátorral, mely egy szövegnek kiveszi az első betűjét (és egy egy karakter hosszú szöveget készít belőle). Ha üres szövegre alkalmazzuk, hibát adjon.*

## 4. Függvények

### 4.1. Elsőrendű függvények

A számok és szövegek nyelvének típusait (3.1) lecseréljük a következőre.

$$\rho, \rho_1, \dots \in \text{BTy} ::= \text{str} \mid \text{int} \quad (4.1)$$

$$\tau, \tau', \dots \in \text{Ty} ::= \rho \mid \rho_1 \rightarrow \rho_2 \quad (4.2)$$

$\rho_1 \rightarrow \rho_2$  alakúak a függvény típusok, ahol  $\rho_1$  és  $\rho_2$  is alaptípus (base type).  $\rho_1$  a függvény értelmezési tartománya,  $\rho_2$  az értékkészlete.

**4.1. Feladat.** *Írjuk fel az összes lehetséges  $\tau$ -t.*

A kifejezéseket kiegészítjük függvénnyel és függvény-alkalmazással.

$$e, e', \dots \in \text{Exp} ::= \dots \mid \text{fun}^\rho x.e \mid \text{app } e e' \quad (4.3)$$

A fun operátor aritása  $(\text{BTy}, \text{Exp}.\text{Exp})\text{Exp}$ , második paraméterében köt egy Exp fajtájú kifejezést. Első paramétere (felső indexben) megadja a függvény értelmezési tartományát.

A típusrendszert a következő szabályokkal egészítjük ki.

$$\frac{\Gamma, x : \rho_1 \vdash e_2 : \rho_2}{\Gamma \vdash \text{fun}^{\rho_1} x.e_2 : \rho_1 \rightarrow \rho_2} \quad (4.4)$$

$$\frac{\Gamma \vdash e : \rho_1 \rightarrow \rho_2 \quad \Gamma \vdash e_1 : \rho_1}{\Gamma \vdash \text{app } e e_1 : \rho_2} \quad (4.5)$$

**4.2. Feladat.** *Írjuk fel azt az  $\text{str} \rightarrow \text{str}$  típusú függvényt, ami egy szöveget háromszor egymás után másol.*

Többparaméteres függvényt majd akkor tudunk megadni, ha bevezettük a szorzat típusokat (5. fejezet), ekkor pl. az összeadást elvégző függvény típusa  $(\text{int} \times \text{int}) \rightarrow \text{int}$  lesz.

A 3.2–3.8. lemmák az elsőrendű függvényekkel kiegészített típusrendszerre is igazak, bizonyításuk ugyanolyan módon történik.

**4.3. Feladat.** *A fentiek közül melyik lemma nem teljesülne, ha a fun operátor paraméterei közül kihagynánk a  $\rho$  alaptípust? Gondoljunk arra, hogy milyen típusa lehet ebben az esetben a  $\text{fun } x.x$  kifejezésnek.*

Az operációs szemantikát a következő szabályokkal egészítjük ki.

$$\overline{\text{fun}^\rho x.e \text{ val}} \quad (4.6)$$

$$\frac{e \mapsto e'}{\text{app } e e_1 \mapsto \text{app } e' e_1} \quad (4.7)$$

$$\left[ \frac{e \text{ val} \quad e_1 \mapsto e'_1}{\text{app } e e_1 \mapsto \text{app } e e'_1} \right] \quad (4.8)$$

$$\frac{[e_1 \text{ val}]}{\text{app } (\text{fun}^\rho x. e_2) e_1 \mapsto e_2[x \mapsto e_1]} \quad (4.9)$$

A szögletes zárójelezett szabály ill. feltétel az érték szerinti paraméterátadás esetén szükséges.

A függvény típus bevezető operátora a **fun**, eliminációs operátora az **app**. A 4.7–4.8. szabályok sorrendi szabályok, míg a 4.9. szabály utasítás szabály, azt mondja meg, hogy mi történik, ha az eliminációs operátort a bevezető operátorra alkalmazzuk. Az **app** operátor principális paramétere az első paraméter.

Az így kiegészített operációs szemantikára is igaz, hogy nincs olyan kifejezés, mely egyszerre érték és át tudjuk írni (3.18. lemma) és determinisztikus (3.19. lemma).

Továbbá igaz a típusmegőrzés (3.21) és a haladás (3.22) tétele is, utóbbi bizonyításához a kanonikus alakok lemmáját (3.23) ki kell egészítenünk azzal, hogy ha  $e : \rho_1 \rightarrow \rho_2$  és  $e \text{ val}$ , akkor  $e = \text{fun}^{\rho_1} x. e'$  valamely  $x$ -re és  $e'$ -re, melyekre  $x : \rho_1 \vdash e' : \rho_2$ .

## 4.2. Magasabbrendű függvények

A típusrendszer egyszerűsödik, ha nem szorítjuk meg a függvénytípus értékkészletét és értelmezési tartományát alaptípusokra. A típusok a következők lesznek.

$$\tau, \tau', \dots \in \text{Ty} ::= \text{str} \mid \text{int} \mid \tau_1 \rightarrow \tau_2 \quad (4.10)$$

### 4.4. Feladat. Írjunk fel 10 különböző $\tau$ -t.

Kifejezések:

$$e, e', \dots \in \text{Exp} ::= \dots \mid \lambda^\tau x. e \mid e e' \quad (4.11)$$

A függvénydefiníciót most lambdával írjuk, az alkalmazást egyszerűen egymás mellé írással. A  $\lambda$  operátor aritása  $(\text{Ty}, \text{Exp}, \text{Exp})\text{Exp}$  (az első paraméterét felső indexbe írjuk), az alkalmazásé  $(\text{Exp}, \text{Exp})\text{Exp}$ .

A típusrendszer csak abban különbözik az elsőrendű esettől, hogy tetszőleges  $\tau$  típusokat engedélyezünk.

$$\frac{\Gamma, x : \tau_1 \vdash e_2 : \tau_2}{\Gamma \vdash \lambda^{\tau_1} x. e_2 : \tau_1 \rightarrow \tau_2} \quad (4.12)$$

$$\frac{\Gamma \vdash e : \tau_1 \rightarrow \tau_2 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash e e_1 : \tau_2} \quad (4.13)$$

Most már tudunk többparaméteres függvényeket is megadni. Például egy  $\text{int} \rightarrow (\text{str} \rightarrow \text{int})$  típusú függvény bemenete  $\text{int}$ , kimenete pedig egy újabb függvény, mely  $\text{str}$ -ből  $\text{int}$ -be képez. Úgy is tekinthetünk erre, mint egy két bemenettel, egy  $\text{int}$  és egy  $\text{str}$  típusúval rendelkező függvényre, melynek kimenete  $\text{int}$ . Ezt azzal is kihangsúlyozzuk, hogy a  $\rightarrow$  operátor jobbra zárójeleződik, tehát  $\tau_1 \rightarrow \tau_2 \rightarrow \tau_3 = \tau_1 \rightarrow (\tau_2 \rightarrow \tau_3)$ .

**4.5. Feladat.** Adjunk meg  $\text{int} \rightarrow (\text{str} \rightarrow \text{int})$  típusú függvényt, mely kezd valamit az  $\text{str}$  típusú paraméterével is.

**4.6. Feladat.** Adjuk meg az  $\text{apply}_3 : (\text{str} \rightarrow \text{str}) \rightarrow \text{str} \rightarrow \text{str} \rightarrow \text{str}$  függvényt, mely az első paramétereként kapott függvényt háromszor alkalmazza a második paraméterében kapott szövegre.

A 3.2–3.8. lemmák a magasabbrendű függvényekkel kiegészített típusrendszerre is igazak. Pl. inverzió (3.4 lemma).

**4.7. Lemma.** Tfh.  $\Gamma \vdash e : \tau$ . Ekkor, ha  $e = \lambda^{\tau_1} x.e_2$ , akkor  $\tau = \tau_1 \rightarrow \tau_2$  valamely  $\tau_2$ -re és  $\Gamma, x : \tau_1 \vdash e_2 : \tau_2$ . Ha  $e = e' e_1$ , akkor valamely  $\tau_1$ -re  $\Gamma \vdash e' : \tau_1 \rightarrow \tau$  és  $\Gamma \vdash e_1 : \tau_1$ .

*Bizonyítás.*  $\Gamma \vdash e : \tau$  szerinti indukció. □

Az operációs szemantika az elsőrendű esettel analóg.

$$\overline{\lambda^{\tau} x.e \text{ val}} \quad (4.14)$$

$$\frac{e \mapsto e'}{e e_1 \mapsto e' e_1} \quad (4.15)$$

$$\left[ \frac{e \text{ val} \quad e_1 \mapsto e'_1}{e e_1 \mapsto e e'_1} \right] \quad (4.16)$$

$$\frac{[e_1 \text{ val}]}{(\lambda^{\tau} x.e_2) e_1 \mapsto e_2[x \mapsto e_1]} \quad (4.17)$$

A szögletes zárójelezett szabály ill. feltétel az érték szerinti paraméterátadás esetén szükséges.

Az így kiegészített operációs szemantikára is igaz, hogy nincs olyan kifejezés, mely egyszerre érték és át tudjuk írni (3.18. lemma) és determinisztikus (3.19. lemma).

Továbbá igaz a típusmegőrzés (3.21) és a haladás (3.22) tétele is, utóbbi bizonyításához a kanonikus alakok lemmáját (3.23) ki kell egészítenünk azzal, hogy ha  $e : \tau_1 \rightarrow \tau_2$  és  $e \text{ val}$ , akkor  $e = \lambda^{\tau_1} x.e'$  valamely  $x$ -re és  $e'$ -re, melyekre  $x : \tau_1 \vdash e' : \tau_2$ .

**4.8. Feladat.** Bizonyítsd be a típusmegőrzés és a haladás tételét.

**4.9. Feladat.** Értékelj ki név és érték szerinti paraméterátadással a  $(\lambda^{\text{int}} x.x + x)(1 + 1)$  kifejezést.

**4.10. Feladat.** Értékelj ki a  $\left( (\lambda^{\text{int} \rightarrow \text{int}} f. \lambda^{\text{int}} x.f(f x)) (\lambda^{\text{int}} x.x + 1) \right) (3 + 1)$  kifejezést.

## 5. Véges adattípusok

Harper könyv: IV. rész.

## 5.1. Szorzat típusok

A bináris szorzat típusokkal rendezett párokat tudunk leírni. A projekciókkal ki tudjuk szedni a párban levő elemeket. A nulláris szorzat az egyelemű típus, mely nem hordoz információt, így nincsen eliminációs szabálya. Ezek általánosításai a véges szorzat típusok, melyeknek a felhasználó által megadott nevű projekciókkal rendelkező változatát nevezik rekordnak.

A szorzat típusok operációs szemantikája lehet *lusta* (lazy) és *mohó* (eager).<sup>2</sup> Lusta szemantika esetén egy tetszőleges  $\langle e, e' \rangle$  pár érték, míg mohó szemantika esetén szükséges, hogy  $e$  és  $e'$  már eleve értékek legyenek.

### 5.1.1. Nulláris és bináris szorzat típus

A szintaxis a következő.

$$\tau, \tau', \dots \in \mathbf{Ty} ::= \dots \mid \top \mid \tau \times \tau' \quad (5.1)$$

$$e, e', \dots \in \mathbf{Exp} ::= \dots \mid \mathbf{tt} \mid \langle e_1, e_2 \rangle \mid \mathbf{proj}_1 e \mid \mathbf{proj}_2 e \quad (5.2)$$

A nulláris szorzat típust egyelemű típusnak (top, unit) is nevezik, szokásos jelölései a  $\top$ -on kívül 1 és (). Az egyetlen elemét  $\mathbf{tt}$ -vel (trivially true) jelöljük. A bináris szorzatot (binary product) Descartes-szorzatnak vagy keresztszorzatnak is nevezik.

A típusrendszer a következő.

$$\frac{\Gamma \mathbf{wf}}{\Gamma \vdash \mathbf{tt} : \top} \quad (5.3)$$

$$\frac{\Gamma \vdash e_1 : \tau_1 \quad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash \langle e_1, e_2 \rangle : \tau_1 \times \tau_2} \quad (5.4)$$

$$\frac{\Gamma \vdash e : \tau_1 \times \tau_2}{\Gamma \vdash \mathbf{proj}_1 e : \tau_1} \quad (5.5)$$

$$\frac{\Gamma \vdash e : \tau_1 \times \tau_2}{\Gamma \vdash \mathbf{proj}_2 e : \tau_2} \quad (5.6)$$

**5.1. Feladat.** *Hány eleme van a  $(\top \times \top) \times \top$  és a  $\top \times (\top \times \top)$  típusoknak?*

Az operációs szemantika a következő.

$$\overline{\mathbf{tt} \mathbf{val}} \quad (5.7)$$

$$\frac{[e_1 \mathbf{val}] \quad [e_2 \mathbf{val}]}{\langle e_1, e_2 \rangle \mathbf{val}} \quad (5.8)$$

$$\left[ \frac{e_1 \mapsto e'_1}{\langle e_1, e_2 \rangle \mapsto \langle e'_1, e_2 \rangle} \right] \quad (5.9)$$

$$\left[ \frac{e_1 \mathbf{val} \quad e_2 \mapsto e'_2}{\langle e_1, e_2 \rangle \mapsto \langle e_1, e'_2 \rangle} \right] \quad (5.10)$$

<sup>2</sup> A név szerinti és az érték szerinti paraméterátadás szemantikáról a függvény típusoknál beszélünk, véges adattípusoknál és induktív típusoknál (lásd később) *lusta* és *mohó* szemantikát mondunk.



$$\frac{e \mapsto e'}{\text{proj}_1 e \mapsto \text{proj}_1 e'} \quad (5.11)$$

$$\frac{e \mapsto e'}{\text{proj}_2 e \mapsto \text{proj}_2 e'} \quad (5.12)$$

$$\frac{[e_1 \text{ val}] \quad [e_2 \text{ val}]}{\text{proj}_1 \langle e_1, e_2 \rangle \mapsto e_1} \quad (5.13)$$

$$\frac{[e_1 \text{ val}] \quad [e_2 \text{ val}]}{\text{proj}_2 \langle e_1, e_2 \rangle \mapsto e_2} \quad (5.14)$$

A szögletes zárójelbe tett feltételek és szabályok csak a mohó szemantikában használatosak. A  $-$ ,  $-$  operátor konstruktor, míg a  $\text{proj}_1$  és  $\text{proj}_2$  az eliminátorok. Mohó kiértékelés esetén az utasítás szabályok (5.13–5.14) csak akkor működnek, ha a  $-$ ,  $-$  operátor mindkét paramétere ki van értékelve.

**5.2. Feladat.** Értékelj ki a  $(\lambda^{\text{int}} x. \langle x + 3, x + 4 \rangle) (1 + 2)$  kifejezést az alábbi négy módon:

- Érték szerint, mohón.
- Név szerint, mohón.
- Érték szerint, lustán.
- Név szerint, lustán.

A 3.2–3.8, 3.18, 3.19 lemmák, és a 3.21) és a 3.22. tételek mind igazak erre a típusrendszerre is.

**5.3. Feladat.** Bizonyítsd be a típusmegőrzés és a haladás tételét.

A szorzat típusokkal lehet megadni többparaméteres ill. több visszatérési értékű függvényeket.

**5.4. Feladat.** Add meg a három-paraméteres összeadás függvényt, melynek típusa  $(\text{int} \times \text{int} \times \text{int}) \rightarrow \text{int}$ .

### 5.1.2. Általános véges szorzat típusok

Van egy  $I = \{i_1, \dots, i_n\}$  véges halmazunk, mely neveket tartalmaz, és egy olyan szorzat típust adunk meg, mely minden névhez tartalmaz egy elemet.

A szintaxisban a típusok a következők.

$$\tau, \tau', \dots \in \text{Ty} ::= \dots \mid \Pi(i_1 \hookrightarrow \tau_1, \dots, i_n \hookrightarrow \tau_n) \quad (5.15)$$

$\Pi$  aritása  $(\text{Ty}^I)\text{Ty}$ , ami azt jelenti, hogy  $I$  minden elemére meg kell adnunk egy típust ( $A^B$ -vel jelöljük a  $B$ -ből  $A$ -ba történő leképezések halmazát). A leképezés jelölésére használjuk a  $\hookrightarrow$  jelölést, a megadás sorrendje nem számít, tehát pl.  $(i \hookrightarrow a, j \hookrightarrow b)$  megegyezik  $(j \hookrightarrow b, i \hookrightarrow a)$ -val.

A kifejezések a következők.

$$e, e', \dots \in \text{Exp} ::= \dots \mid \langle i_1 \hookrightarrow e_1, \dots, i_n \hookrightarrow e_n \rangle \mid \text{proj}_{i_k} e \quad (5.16)$$

$\langle - \rangle$  aritása  $(\text{Exp}^I)\text{Exp}$ .  $\text{proj}_i$  aritása  $(\text{Exp})\text{Exp}$ , minden  $k \in \{1, \dots, n\}$ -re van egy ilyen operátorunk.

Például az  $I = \{\text{name, age, postcode}\}$  egy olyan rekord típust ad meg, mely egy nevet, életkort és irányítószámot tartalmaz.

$$\Pi(\text{name} \hookrightarrow \text{str}, \text{age} \hookrightarrow \text{int}, \text{postcode} \hookrightarrow \text{int})$$

Egy eleme így adható meg.

$$\langle \text{name} \hookrightarrow \text{"Judit"}, \text{age} \hookrightarrow 38, \text{postcode} \hookrightarrow 1092 \rangle$$

A típusrendszer a következő.

$$\frac{\Gamma \text{wf} \quad \Gamma \vdash e_1 : \tau_1 \quad \dots \quad \Gamma \vdash e_n : \tau_n}{\Gamma \vdash \langle i_1 \hookrightarrow e_1, \dots, i_n \hookrightarrow e_n \rangle : \Pi(i_1 \hookrightarrow \tau_1, \dots, i_n \hookrightarrow \tau_n)} \quad (5.17)$$

$$\frac{\Gamma \vdash e : \Pi(i_1 \hookrightarrow \tau_1, \dots, i_n \hookrightarrow \tau_n)}{\Gamma \vdash \text{proj}_{i_k} e : \tau_k} \quad (5.18)$$

$\Pi(i_1 \hookrightarrow \tau_1, \dots, i_n \hookrightarrow \tau_n)$ -nek ugyanannyi eleme van, mint a  $\tau_1 \times \dots \times \tau_n$  típusnak, csak előbbi elemeinek a megadása kényelmesebb: név szerint adjuk meg az egyes komponenseket, és a sorrend sem számít. Ezenkívül név szerint ki tudjuk őket vetíteni, nem kell iterálva alkalmaznunk a  $\text{proj}_1$ ,  $\text{proj}_2$  operátorokat.

Operációs szemantika.

$$\frac{[e_1 \text{ val} \quad \dots \quad e_n \text{ val}]}{\langle i_1 \hookrightarrow e_1, \dots, i_n \hookrightarrow e_n \rangle \text{ val}} \quad (5.19)$$

$$\left[ \frac{e_1 \text{ val} \quad \dots \quad e_{k-1} \text{ val} \quad e_k \mapsto e'_k}{\langle i_1 \hookrightarrow e_1, \dots, i_n \hookrightarrow e_n \rangle \mapsto \langle i_1 \hookrightarrow e_1, \dots, i_{k-1} \hookrightarrow e_{k-1}, i_k \hookrightarrow e'_k, i_{k+1} \hookrightarrow e_{k+1}, \dots, i_n \hookrightarrow e_n \rangle} \right] \quad (5.20)$$

$$\frac{e \mapsto e' \quad k \in \{1, \dots, n\}}{\text{proj}_{i_k} e \mapsto \text{proj}_{i_k} e'} \quad (5.21)$$

$$\frac{[e_1 \text{ val} \quad \dots \quad e_n \text{ val}]}{\text{proj}_{i_k} \langle i_1 \hookrightarrow e_1, \dots, i_n \hookrightarrow e_n \rangle \mapsto e_{i_k}} \quad (5.22)$$

A szögletes zárójellel megadott feltételek és szabály mohó kiértékelés esetén van megadva.

**5.5. Feladat.** Jelöld be, hogy melyik a konstruktor, eliminátor, melyek a sorrendi és melyek az utasítás szabályok.

**5.6. Feladat.** A nulláris és a bináris szorzat típusokat megkapjuk, ha  $I$  az üres halmaz ill. a kételemű halmaz. Mutasd meg, hogy az így megadott nulláris és bináris típus ugyanúgy viselkedik típusrendszer és operációs szemantika szempontjából, mint az 5.1.1. alfejezetben megadott.

**5.7. Feladat.** Bizonyítsd be a típusmegmaradás és a haladás tételét.

## 5.2. Összeg típusok

### 5.2.1. Nulláris és bináris összeg

Szintaxis.

$$\tau, \tau', \dots \in \mathbf{Ty} ::= \dots \mid \perp \mid \tau_1 + \tau_2 \quad (5.23)$$

$$e, e', \dots \in \mathbf{Exp} ::= \dots \mid \mathbf{abort} \, e \mid \mathbf{inj}_1^{\tau_1, \tau_2} e \mid \mathbf{inj}_2^{\tau_1, \tau_2} e \mid \mathbf{case} \, e \, x_1.e_1 \, x_2.e_2 \quad (5.24)$$

A nulláris összeg típus (bottom, 0 típus, void típus) egy olyan választási lehetőség ad meg, ahol egy alternatíva sincs. Emiatt nincs konstruktora. Az eliminációs operátora pedig abortálja a számítást, amint kap egy bottom típusú értéket (ami nem lehetséges). A bináris összeg típusba kétféleképpen injektálhatunk: vagy az első, vagy a második komponensébe, ezt jelöli  $\mathbf{inj}_1$  és  $\mathbf{inj}_2$ . Ezek aritása  $(\mathbf{Ty}, \mathbf{Ty}, \mathbf{Exp})\mathbf{Exp}$ . Egy összeg típusú kifejezést esetésválasztással ( $\mathbf{case}$ ) tudunk eliminálni, aritása  $(\mathbf{Exp}, \mathbf{Exp}, \mathbf{Exp}, \mathbf{Exp})\mathbf{Exp}$ .

Típusrendszer.

$$\frac{\Gamma \vdash e : \perp}{\Gamma \vdash \mathbf{abort} \, e : \tau} \quad (5.25)$$

$$\frac{\Gamma \vdash e_1 : \tau_1}{\Gamma \vdash \mathbf{inj}_1^{\tau_1, \tau_2} e_1 : \tau_1 + \tau_2} \quad (5.26)$$

$$\frac{\Gamma \vdash e_2 : \tau_2}{\Gamma \vdash \mathbf{inj}_2^{\tau_1, \tau_2} e_2 : \tau_1 + \tau_2} \quad (5.27)$$

$$\frac{\Gamma \vdash e : \tau_1 + \tau_2 \quad \Gamma, x_1 : \tau_1 \vdash e_1 : \tau \quad \Gamma, x_2 : \tau_2 \vdash e_2 : \tau}{\Gamma \vdash \mathbf{case} \, e \, x_1.e_1 \, x_2.e_2 : \tau} \quad (5.28)$$

Operációs szemantika. Az  $\mathbf{inj}_1$  és  $\mathbf{inj}_2$  típusparamétereit nem írtuk ki a rövidség kedvéért, de ott vannak.

$$\frac{e \mapsto e'}{\mathbf{abort} \, e \mapsto \mathbf{abort} \, e'} \quad (5.29)$$

$$\frac{[e \, \mathbf{val}]}{\mathbf{inj}_1 \, e \, \mathbf{val}} \quad (5.30)$$

$$\frac{[e \, \mathbf{val}]}{\mathbf{inj}_2 \, e \, \mathbf{val}} \quad (5.31)$$

$$\left[ \frac{e \mapsto e'}{\mathbf{inj}_1 \, e \mapsto \mathbf{inj}_1 \, e'} \right] \quad (5.32)$$

$$\left[ \frac{e \mapsto e'}{\mathbf{inj}_2 \, e \mapsto \mathbf{inj}_2 \, e'} \right] \quad (5.33)$$

$$\frac{e \mapsto e'}{\mathbf{case} \, e \, x_1.e_1 \, x_2.e_2 \mapsto \mathbf{case} \, e' \, x_1.e_1 \, x_2.e_2} \quad (5.34)$$

$$\frac{[e \, \mathbf{val}]}{\mathbf{case} \, (\mathbf{inj}_1 \, e) \, x_1.e_1 \, x_2.e_2 \mapsto e_1[x_1 \mapsto e]} \quad (5.35)$$

$$\frac{[e \, \mathbf{val}]}{\mathbf{case} \, (\mathbf{inj}_2 \, e) \, x_1.e_1 \, x_2.e_2 \mapsto e_2[x_2 \mapsto e]} \quad (5.36)$$

**5.8. Feladat.** Add meg a Bool típust összeg típusként, és az if-then-else konstrukciót.

**5.9. Feladat.** Van-e különbség a lusta és a mohó if-then-else között?

**5.10. Feladat.** Add meg az tagadás, logika és, logikai vagy függvényeket a case operátor használatával.

A 3.2–3.8, 3.18, 3.19 lemmák, és a 3.21) és a 3.22. tételek mind igazak erre a típusrendszerre is.

**5.11. Feladat.** Bizonyítsd be a típusozás unicitását! Mi lenne, ha nem adnánk meg a típusokat az injektáló operátoroknál?

### 5.2.2. Általános véges összeg típusok

$I = \{i_1, \dots, i_n\}$  véges halmaz. Szintaxis.

$$\tau, \tau', \dots \in \text{Ty} ::= \dots \mid \Sigma(i_1 \hookrightarrow \tau_1, \dots, i_n \hookrightarrow \tau_n) \quad (5.37)$$

$$e, e', \dots \in \text{Exp} ::= \dots \mid \text{inj}_{i_k}^{i_1 \hookrightarrow \tau_1, \dots, i_n \hookrightarrow \tau_n} e \mid \text{case } e (i_1 \hookrightarrow x_1.e_1, \dots, i_n \hookrightarrow x_n.e_n) \quad (5.38)$$

$\Sigma$  aritása  $(\text{Ty}^I)\text{Ty}$ . Itt sem számít a sorrend.  $\text{inj}_{i_k}$  aritása  $(\text{Ty}^I, \text{Exp})\text{Exp}$ . Az általános case aritása  $(\text{Exp}, (\text{Exp}.\text{Exp})^I)\text{Exp}$ .

Típusrendszer.

$$\frac{\Gamma \vdash e : \tau_k}{\Gamma \vdash \text{inj}_{i_k}^{i_1 \hookrightarrow \tau_1, \dots, i_n \hookrightarrow \tau_n} e : \Sigma(i_1 \hookrightarrow \tau_1, \dots, i_n \hookrightarrow \tau_n)} \quad (5.39)$$

$$\frac{\Gamma \vdash e : \Sigma(i_1 \hookrightarrow \tau_1, \dots, i_n \hookrightarrow \tau_n) \quad \Gamma, x_1 : \tau_1 \vdash e_1 : \tau \quad \dots \quad \Gamma, x_n : \tau_n \vdash e_n : \tau}{\Gamma \vdash \text{case } e x_1.e_1 \dots x_n.e_n : \tau} \quad (5.40)$$

**5.12. Feladat.** Írd fel az operációs szemantikát, a lusta és a mohó változatot is!

**5.13. Feladat.** Mutasd meg, hogyan lesz a nulláris és a bináris összeg speciális esete az általánosnak!

### 5.3. Véges típusok alkalmazásai

Fontos megkülönböztetni a  $\top$  és a  $\perp$  típusokat. A  $\top$ -nak pontosan egy eleme van, és nem hordoz semmi információt. Ezt unitnak nevezik a legtöbb nyelvben, de sokszor hibásan voidnak (üresnek) nevezik. Utóbbi esetben arra gondolnak, hogy nincs benne információ, nem pedig arra, hogy nincs egy eleme sem. A  $\perp$ -nak nincs egy eleme sem, ez a teljes információ. Ha van egy  $\perp$  típusú értékünk (ami lehetetlen), akkor tetszőleges más típusú értéket létre tudunk hozni (abort művelet).

Bool típus.

Felsorolások, pl. Észak, Dél, Kelet, Nyugat. Ez tkp.  $1 + 1 + 1 + 1$  típus. Ilyen a beépített karakter típus is, általában egyenlőség-vizsgálattal van megadva a case ezekre.

Opt típus, mely opcionálisan tartalmaz valamilyen értéket. Szintaxis.

$$\tau, \tau', \dots \in \text{Ty} ::= \dots \mid \text{Opt } \tau \quad (5.41)$$

$$e, e', \dots \in \text{Exp} ::= \dots \mid \text{null}^\tau \mid \text{just } e \mid \text{ifnull } e \ e_1 \ x.e_2 \quad (5.42)$$

Típusrendszer. Úgy tudunk eliminálni Opt-ból, ha megadjuk, mi történjen, ha null értéket kaptunk. Ezt fejezi ki az ifnull.

$$\frac{\Gamma \text{ wf}}{\Gamma \vdash \text{null}^\tau : \text{Opt } \tau} \quad (5.43)$$

$$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{just } e : \text{Opt } \tau} \quad (5.44)$$

$$\frac{\Gamma \vdash e : \text{Opt } \tau \quad \Gamma \vdash e_1 : \tau' \quad \Gamma, x : \tau \vdash e_2 : \tau'}{\Gamma \vdash \text{ifnull } e \ e_1 \ x.e_2 : \tau'} \quad (5.45)$$

Operációs szemantika.

$$\overline{\text{null}^\tau \text{ val}} \quad (5.46)$$

$$\frac{[e \text{ val}]}{\text{just } e \text{ val}} \quad (5.47)$$

$$\left[ \frac{e \mapsto e'}{\text{just } e \mapsto \text{just } e'} \right] \quad (5.48)$$

$$\frac{e \mapsto e'}{\text{ifnull } e \ e_1 \ x.e_2 \mapsto \text{ifnull } e \ e_1 \ x.e_2} \quad (5.49)$$

$$\frac{}{\text{ifnull } \text{null}^\tau \ e_1 \ x.e_2 \mapsto e_1} \quad (5.50)$$

$$\frac{[e \text{ val}]}{\text{ifnull } (\text{just } e) \ e_1 \ x.e_2 \mapsto e_2[x \mapsto e]} \quad (5.51)$$

**5.14. Feladat.** Mutasd meg, hogy ha véges összegként adjuk meg az Opt típust, a fenti típusrendszer és operációs szemantika szabályait megkapjuk.

**5.15. Feladat.** Hogyan tudunk objektum-orientált programozási nyelveken (pl. Java) megadni összeg típusokat?

$\tau_1$  és  $\tau_2$  típusokat *izomorf*nek nevezzük, ha megadhatók  $f_1$  és  $f_2$  kifejezések, melyekre  $x_1 : \tau_1 \vdash f_2 : \tau_2$  és  $x_2 : \tau_2 \vdash f_1 : \tau_1$  és bármely  $e_1 : \tau_1$ -re  $f_1[x_2 \mapsto (f_2[x_1 \mapsto e_1])] = e_1$  és fordítva, bármely  $e_2 : \tau_2$ -re  $f_2[x_1 \mapsto (f_1[x_2 \mapsto e_2])] = e_2$ .

**5.16. Feladat.** Döntsd el, hogy az alábbi típusok izomorfak -e, ha igen, add meg  $f_1$ -et és  $f_2$ -t!

$$\begin{aligned} \text{Bool} \times \top & \quad \text{és} \quad \text{Bool} \\ (\top + \top) + \top & \quad \text{és} \quad \top + (\top + \top) \\ (\tau + \tau') \times \tau'' & \quad \text{és} \quad (\tau \times \tau'') + (\tau' \times \tau'') \\ \tau + \perp & \quad \text{és} \quad \tau \\ \tau \times \tau' & \quad \text{és} \quad \tau' \times \tau \\ \tau \times \perp & \quad \text{és} \quad \perp \end{aligned}$$

**5.17. Feladat.** Mutasd meg, hogy a véges típusok a fenti izomorfizmust egyenlőségnek véve kommutatív félgyűrűt (semiring)-et alkotnak.

## 6. Konstruktív ítéletlogika

Harper könyv: V. rész.

Ebben a fejezetben a konstruktív ítéletlogikával (propozicionális, nulladarendű) logikával és az eddig tanult típusrendszerekkel való kapcsolatával foglalkozunk.

### 6.1. Szintaxis

$$A, B, \dots \in \text{Prop} ::= X \mid \top \mid \perp \mid A \wedge B \mid A \vee B \mid A \supset B \quad (6.1)$$

Egy konstruktív ítéletlogikai állítás (propozíció) vagy egy ítéletváltozó ( $X, Y, \dots$ -al jelöljük), vagy igaz, vagy hamis, vagy egy konjunkció, diszjunkció vagy egy implikáció.

### 6.2. Bizonyítások

Bevezetünk egy ítéletet, mely  $A_1, \dots, A_n \vdash A$  alakú, mely azt mondja, hogy  $A_1, \dots, A_n$ -t feltéve  $A$  bizonyítható. A feltételek (hipotézisek) listáját  $\Delta$ -val jelöljük és a következőképp adjuk meg.

$$\Delta, \Delta_1 \dots \in \text{Hipos} ::= \cdot \mid \Delta, A \quad (6.2)$$

Először megadunk egy újabb ítéletet, mely azt mondja, hogy a  $\Delta$  feltételek között szerepel az  $A$  állítás:  $\Delta \ni A$ .

$$\overline{\Delta, A \ni A} \quad (6.3)$$

$$\frac{\Delta \ni A}{\Delta, B \ni A} \quad (6.4)$$

Megadjuk a bizonyíthatóság levezetési szabályait. Először is, ha feltettünk valamit, akkor azt bizonyíthatjuk.

$$\frac{\Delta \ni A}{\Delta \vdash A} \quad (6.5)$$

A logikai összekötők levezetési szabályait bevezető és eliminációs szabályokként adjuk meg.

Az igaz állítást bármikor levezethetjük, eliminációs szabálya nincs.

$$\overline{\Delta \vdash \top} \quad (6.6)$$

A hamis állításból bármi következik.

$$\frac{\Delta \vdash \perp}{\Delta \vdash A} \quad (6.7)$$

Konjunkciót akkor vezethetünk le, ha mindkét tagja igaz. Két eliminációs szabálya van, mellyel a benne levő információ nyerhető ki.

$$\frac{\Delta \vdash A \quad \Delta \vdash B}{\Delta \vdash A \wedge B} \quad (6.8)$$

$$\frac{\Delta \vdash A \wedge B}{\Delta \vdash A} \quad (6.9)$$

$$\frac{\Delta \vdash A \wedge B}{\Delta \vdash B} \quad (6.10)$$

Diszjunkciót akkor vezethetünk le, ha vagy az egyik, vagy a másik komponense igaz. Eliminálni akkor tudunk  $A \vee B$ -ből  $C$ -be, ha  $A$ -t ill.  $B$ -t feltételezve is bizonyítható  $C$ .

$$\frac{\Delta \vdash A}{\Delta \vdash A \vee B} \quad (6.11)$$

$$\frac{\Delta \vdash B}{\Delta \vdash A \vee B} \quad (6.12)$$

$$\frac{\Delta \vdash A \vee B \quad \Delta, A \vdash C \quad \Delta, B \vdash C}{\Delta \vdash C} \quad (6.13)$$

Az  $A \supset B$  implikáció bevezetéséhez  $B$ -t kell bizonyítanunk  $A$  feltételezésével. Az eliminációs szabály a modus ponens.

$$\frac{\Delta, A \vdash B}{\Delta \vdash A \supset B} \quad (6.14)$$

$$\frac{\Delta \vdash A \supset B \quad \Delta \vdash A}{\Delta \vdash B} \quad (6.15)$$

A logikai tagadást rövidítésként adjuk meg, nem kell külön logikai összekötőt bevezetnünk hozzá:  $\neg A := A \supset \perp$ , vagyis  $A$  hamis, ha a hamisat implikálja.

Az „akkor és csak akkor” logikai összekötő a következő rövidítésként adható meg:  $A \leftrightarrow B := (A \supset B) \wedge (B \supset A)$ .

**6.1. Feladat.** *Bizonyítsuk be az alábbi állításokat (üres feltételista mellett).*

1.  $(X \supset (Y \supset Z)) \supset (Y \supset X \supset Z)$
2.  $X \leftrightarrow (X \wedge \top)$
3.  $X \leftrightarrow (X \vee \perp)$
4.  $(X \supset (Y \wedge Z)) \supset ((X \supset Y) \wedge (X \supset Z))$
5.  $((X \vee Y) \supset Z) \supset ((X \supset Z) \wedge (Y \supset Z))$
6.  $X \supset \neg \neg X$
7.  $\neg \neg (X \vee \neg X)$
8.  $\neg \neg (\neg \neg X \supset X)$
9.  $\neg \neg \neg X \leftrightarrow \neg X$
10.  $\neg (X \leftrightarrow \neg X)$
11.  $(\neg X \vee Y) \supset (X \supset Y)$
12.  $\neg (X \vee Y) \leftrightarrow (\neg X \wedge \neg Y)$
13.  $(\neg X \vee \neg Y) \supset \neg (X \wedge Y)$

### 6.3. Állítások mint típusok

A fenti levezetési szabályok eléggé hasonlítanak a véges típusok (nulláris és bináris szorzat és összeg) és a magasabbrendű függvények típusrendszeréhez. Az állítások helyett ott típusok voltak, mégpedig az alábbi táblázat szerint.

Prop	Ty
$\top$	$\top$
$\perp$	$\perp$
$A_1 \wedge A_2$	$\tau_1 \times \tau_2$
$A_1 \vee A_2$	$\tau_1 + \tau_2$
$A_1 \supset A_2$	$\tau_1 \rightarrow \tau_2$
$X$	lásd 11. fejezet

A levezetési szabályok megfeleltethetők egymásnak azzal a különbséggel, hogy a kifejezéseket az ítéletlogikában elhagyjuk. Például a modus ponens szabály kétféle változata.

$$\frac{\Delta \vdash A \supset B \quad \Delta \vdash A}{\Delta \vdash B} \qquad \frac{\Gamma \vdash e : \tau_1 \rightarrow \tau_2 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash e e_1 : \tau_2}$$

A különbség annyi, hogy elhagyjuk a kifejezéseket: a bizonyításoknak nem adunk nevet, mert logikában nem érdekes, hogy pontosan melyik a bizonyítás.

**6.2. Feladat.** A 6.1. feladatban megadott állításokat írjuk át típusokká. Az ítéletváltozók helyett használjunk típus-metaváltozókat, pl.  $\tau_1, \tau_2$ . Írjunk kifejezéseket, melyek az üres környezetben a megadott típusúak (bárhogyan is választjuk meg a típus-metaváltozókat).

További információ:

- A bizonyításoknak is lehet operációs szemantikája, cut elimination-nek nevezzük. Ez pontosan megfelel a magasabbrendű függvények operációs szemantikájának (4.2).

### 6.4. Klasszikus logika

A fenti logika egy denotációs szemantikáját meg tudjuk adni igazságtáblával. Egy olyan függvényt, mely az ítéletváltozók halmazáról a  $\{t, f\}$  halmazba képez, interpretációnak nevezzük. Egy  $A$  állítás jelenetését  $I$  interpretáció esetén az



$|A|^I \in \{t, f\}$  adja meg,  $|-|^I$  a következőképp van definiálva.

$$\begin{aligned} |X|^I &= I(X) \\ |\top|^I &= t \\ |\perp|^I &= f \\ |A \wedge B|^I &= \begin{cases} t, & \text{ha } |A|^I = t \text{ és } |B|^I = t \\ f, & \text{egyébként} \end{cases} \\ |A \vee B|^I &= \begin{cases} t, & \text{ha } |A|^I = t \text{ vagy } |B|^I = t \\ f, & \text{egyébként} \end{cases} \\ |A \supset B|^I &= \begin{cases} t, & \text{ha } |A|^I = f \text{ vagy } |B|^I = t \\ f, & \text{egyébként} \end{cases} \end{aligned}$$

Hasonlóképp megadjuk egy feltétellista jelentését.

$$\begin{aligned} |\cdot|^I &= t \\ |\Delta, A|^I &= \begin{cases} t, & \text{ha } |\Delta|^I = t \text{ és } |A|^I = t \\ f, & \text{egyébként} \end{cases} \end{aligned}$$

Azt mondjuk, hogy  $I \models A$ , ha  $|A|^I = t$ . Azt mondjuk, hogy  $\Delta \models A$ , ha minden  $I$ -re, ha  $|\Delta|^I = t$ , akkor  $|A|^I = t$ .

A bizonyíthatóság és a fenti szemantika kapcsolata az, hogy  $\Delta \vdash A$ -ból következik, hogy  $\Delta \models A$ .

### 6.3. Feladat. Bizonyítsd be!

A másik irány (teljesség) csak akkor igaz, ha a logikát klasszikussá tesszük, vagyis a bizonyítások levezetési szabályaihoz hozzávesszük a kizárt harmadik elvének (tertium non datur) alábbi szabályát.

$$\overline{\Delta \vdash A \vee \neg A} \quad (6.16)$$

További információ:

- A konstruktív logika denotációs szemantikáját Kripke-modellekkel adhatjuk meg, ezek nem validálják a kizárt harmadik elvét. Megadható egy olyan Kripke modell, mely teljes, tehát  $\Delta \models A$ -ból következik  $\Delta \vdash A$  a kizárt harmadik elvétől függetlenül.
- A kizárt harmadik elvének típusrendszerbeli megfelelője másfajta operációs szemantikát kíván, amit itt nem tárgyalunk (lásd Harper könyv 13. fejezet). Tehát a magasabbrendű függvények és véges típusok operációs szemantikája már nem megfelelő.

**6.4. Feladat.** Bizonyítsuk be az alábbi állításokat (üres feltétellista mellett), a kizárt harmadik elvét is felhasználva.

1.  $(X \supset Y) \supset (\neg X \vee Y)$
2.  $\neg(X \wedge Y) \supset (\neg X \vee \neg Y)$

## 7. Természetes számok

Harper könyv: III. rész, 9. fejezet.

Ebben a fejezetben bevezetjük a természetes számok típusát. A számok és szövegek típusrendszerében (3. fejezet) megadott int típusnak ad-hoc módonadtuk meg az operátorait. Most egy általános mechanizmust adunk meg, a *primitív rekurziót*, mellyel sokféle, természetes számokon értelmezett függvényt tudunk megadni. Ezt a típusrendszert Gödel System T-jének is nevezik.

### 7.1. Szintaxis

$$\begin{aligned}\tau, \tau', \dots &\in \text{Ty} ::= \text{Nat} \mid \tau_1 \rightarrow \tau_2 \\ e, e', \dots &\in \text{Exp} ::= x \mid \text{zero} \mid \text{suc } e \mid \text{rec } e_0 \ x.e_1 \ e \mid \lambda^\tau x.e \mid e \ e'\end{aligned}$$

Kétféle természetes szám van (két konstruktora van a természetes számoknak): **zero** (nulla) és **suc  $e$** , amely valamely más természetes számnak,  $e$ -nek a rákövetkezője. Pl. az 1-et úgy írjuk, hogy **suc zero**, a 2-t úgy, hogy **suc (suc zero)** stb. A **rec** operátor a természetes számok eliminátora, aritása  $(\text{Exp}, \text{Exp}.\text{Exp}, \text{Exp})\text{Exp}$ . Ezzel tudunk függvényeket megadni a természetes számokon. **rec  $e_0 \ x.e_1 \ e$**  az  $e_0$  és  $x.e_1$  által megadott függvény alkalmazva  $e$  bemenetre. Ha a bemenet nulla, a függvény  $e_0$ -t fog adni, ha a függvény kimenete valamilyen számra  $x$ , akkor a rákövetkezőjére  $e_1$  (ami ugye függhet  $x$ -től).

### 7.2. Típusrendszer

A környezetre és változókra vonatkozó szabályok a szokásosak (3.4–3.9).

$$\frac{\Gamma \text{ wf}}{\Gamma \vdash \text{zero} : \text{Nat}} \quad (7.1)$$

$$\frac{\Gamma \vdash e : \text{Nat}}{\Gamma \vdash \text{suc } e : \text{Nat}} \quad (7.2)$$

$$\frac{\Gamma \vdash e_0 : \tau \quad \Gamma, x : \tau \vdash e_1 : \tau \quad \Gamma \vdash e : \text{Nat}}{\Gamma \vdash \text{rec } e_0 \ x.e_1 \ e : \tau} \quad (7.3)$$

A függvényekre vonatkozó szabályok a szokásosak.

$$\frac{\Gamma, x : \tau_1 \vdash e : \tau_2}{\Gamma \vdash \lambda^{\tau_1} x.e : \tau_1 \rightarrow \tau_2} \quad (7.4)$$

$$\frac{\Gamma \vdash e : \tau_1 \rightarrow \tau_2 \quad \Gamma \vdash e_1 : \tau_1}{\Gamma \vdash e \ e_1 : \tau_2} \quad (7.5)$$

### 7.3. Operációs szemantika

Értékek a nulla, a rákövetkező (mely egy érték rákövetkezője kell, hogy legyen mohó kiértékelésnél) és az absztrakció.

$$\overline{\text{zero val}} \quad (7.6)$$

$$\frac{[e \text{ val}]}{\text{suc } e \text{ val}} \quad (7.7)$$

$$\overline{\lambda^\tau e \text{ val}} \quad (7.8)$$

$$\left[ \frac{e \mapsto e'}{\text{suc } e \mapsto \text{suc } e'} \right] \quad (7.9)$$

$$\frac{e \mapsto e'}{\text{rec } e_0 \ x.e_1 \ e \mapsto \text{rec } e_0 \ x.e_1 \ e'} \quad (7.10)$$

$$\overline{\text{rec } e_0 \ x.e_1 \ \text{zero} \mapsto e_0} \quad (7.11)$$

$$\frac{\text{suc } e \text{ val}}{\text{rec } e_0 \ x.e_1 \ (\text{suc } e) \mapsto e_1 [x \mapsto \text{rec } e_0 \ x.e_1 \ e]} \quad (7.12)$$

$$\frac{e \mapsto e'}{e \ e_1 \mapsto e' \ e_1} \quad (7.13)$$

$$\left[ \frac{e \text{ val} \quad e_1 \mapsto e'_1}{e \ e_1 \mapsto e \ e'_1} \right] \quad (7.14)$$

$$\frac{[e_1 \text{ val}]}{(\lambda^\tau x.e_2) \ e_1 \mapsto e_2 [x \mapsto e_1]} \quad (7.15)$$

A szögletesen zárójelezett szabályok a mohó rákövetkezőhöz és érték szerinti függvényalkalmazáshoz kellenek. Ha nem vesszük őket hozzá az operációs szemantikához, akkor lusta rákövetkezőt és név szerinti paraméterátadást kapunk.

Például az összeadás függvényt az alábbi módon adjuk meg.

$$\lambda^{\text{Nat}} y. \lambda^{\text{Nat}} z. \text{rec } z \ (x. \text{suc } x) \ y : \text{Nat} \rightarrow (\text{Nat} \rightarrow \text{Nat})$$

Ez a következőképp működik:  $y$ -t és  $z$ -ta akarjuk összeadni, emiatt  $y$ -on végzünk rekurziót. Ha  $y = \text{zero}$ , akkor  $z$ -t adunk vissza (hiszen  $0 + z$  egyenlő  $z$ -vel). Ha  $y = \text{suc } e$ , akkor  $x$ -ben megkötjük  $\text{rec } z \ (x. \text{suc } x) \ e$  eredményét, majd hozzáadunk egyet. Pl. a következőképp zajlik az átírás mohó rákövetkező esetén, ha a bemenetek 2 és 1.

$$\begin{aligned} & \left( (\lambda^{\text{Nat}} y. \lambda^{\text{Nat}} z. \text{rec } z \ (x. \text{suc } x) \ y) \ (\text{suc } (\text{suc } \text{zero})) \right) \ (\text{suc } \text{zero}) \\ & \xrightarrow{(7.13)} (\lambda^{\text{Nat}} z. \text{rec } z \ (x. \text{suc } x) \ (\text{suc } (\text{suc } \text{zero}))) \ (\text{suc } \text{zero}) \\ & \xrightarrow{(7.15)} \text{rec } (\text{suc } \text{zero}) \ (x. \text{suc } x) \ (\text{suc } (\text{suc } \text{zero})) \\ & \xrightarrow{(7.12)} (\text{suc } x) [x \mapsto \text{rec } (\text{suc } \text{zero}) \ (x. \text{suc } x) \ (\text{suc } \text{zero})] = \text{suc } (\text{rec } (\text{suc } \text{zero}) \ (x. \text{suc } x) \ (\text{suc } \text{zero})) \\ & \xrightarrow{(7.9)} \text{suc } ((\text{suc } x) [x \mapsto \text{rec } (\text{suc } \text{zero}) \ (x. \text{suc } x) \ \text{zero}]) = \text{suc } (\text{suc } (\text{rec } (\text{suc } \text{zero}) \ (x. \text{suc } x) \ \text{zero})) \\ & \xrightarrow{(7.9)} \text{suc } (\text{suc } (\text{suc } \text{zero})) \end{aligned}$$

A nyilak fölé mindig csak az adott lépés levezetési fájának gyökerénél levő szabály sorszámát adtuk meg. Lusta kiértékelés esetén az utolsó két lépés elmarad, hiszen ekkor csak addig értékeljük ki az eredményt, hogy egy rákövetkezőnk van, nem foglalkozunk azzal, hogy a  $\text{suc}$  paraméterében is érték legyen.

A rekurzor primitív rekurziót valósít meg. A fenti definíciót rekurzívan ilyen-  
mi szintaxissal is írhatnánk:

$$\begin{aligned} \text{plus } y \ z &:= \text{case } y \text{ of} \\ &\quad \text{zero} \mapsto z \\ &\quad \text{suc } y' \mapsto \text{suc } (\text{plus } y' \ z) \end{aligned}$$

A rekurzió azért primitív, mert a plus függvény rekurzív hívása csak pontosan  
eggyel kisebb paraméteren lehetséges. Ha  $y = \text{suc } y'$  volt az első paraméter,  
akkor csak  $y'$ -n hívható meg a függvény.

$\bar{n}$ -el jelöljük azt a kifejezést, ahol zero-ra  $n$ -szer van alkalmazva a suc operá-  
tor.

**7.1. Feladat.** Add meg a pred függvényt, mely egy számhoz hozzárendeli a nála  
eggyel kisebb számot (0-hoz rendeljen 0-t).

**7.2. Feladat.** Add meg a természetes számok szorzását! (Egy olyan  $e$  kifejezést,  
mely  $\text{Nat} \rightarrow (\text{Nat} \rightarrow \text{Nat})$  típusú, és  $(e \ \bar{n}) \ n'$  több lépésben  $n * n'$ -re íródik át.)

**7.3. Feladat.** Bizonyítsd be, hogy ha az összeadás fenti definícióját  $e$ -vel jelöl-  
jük, akkor bármely  $n \in \mathbb{N}$ -re  $e \ \bar{n} \text{ zero} \mapsto^* \bar{n}$ .

**7.4. Feladat.** Bizonyítsd a haladás és a típusmegmaradás tételét.

## 7.4. Definiálható függvények

Azt mondjuk, hogy egy  $f : \mathbb{N} \rightarrow \mathbb{N}$  függvény *definiálható* System T-ben, ha  
létezik olyan  $e_f$  kifejezés, mely  $\text{Nat} \rightarrow \text{Nat}$  típusú, és igaz rá, hogy minden  
 $n \in \mathbb{N}$ -re

$$e_f \ \bar{n} \mapsto^* \overline{f(n)}.$$

**7.5. Feladat.** Mutassuk meg, hogy a duplázás függvény definiálható System T-  
ben!

System T-ben (és az eddig tanult összes nyelvben) nem tudunk írni végtelen  
ciklust.

**7.6. Tétel.** Ha  $e : \tau$ , akkor létezik egy olyan  $e'$ , hogy  $e' \text{ val}$  és  $e \mapsto^* e'$ .

Emiatt a System T-beli  $\tau_1 \rightarrow \tau_2$  típusú kifejezések úgy működnek, mint a  
matematikai függvények.

**7.7. Tétel.** Létezik olyan matematikai függvény, mely nem definiálható System  
T-ben.

A bizonyítás a (Cantor-féle) átlós metszés technikáját használja (hasonló  
bizonyítások: a természetes számok részhalmazai többben vannak, mint a termé-  
szetes számok; Gödel-tétel; Turing-gépek megállásának eldönthetetlensége).

*Bizonyítás.* Először is létrehozunk egy kódolást, mely egy ABT-t egy szám-  
mal kódol. Ennek a részleteibe nem megyünk bele, de a lényeg, hogy minden  $e$   
ABT-nek megfelel egy  $\ulcorner e \urcorner$  természetes szám, és két különböző ABT-t különböző  
természetes számokkal reprezentálunk.

A következő matematikai függvényt adjuk meg.  $u : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \mathbb{N}$  tetszőleges  $e : \text{Nat} \rightarrow \text{Nat}$  kifejezésre úgy van megadva, hogy  $e \overline{m} \mapsto^* \overline{u(\ulcorner e \urcorner)(m)}$ . Tehát  $u$  egy olyan függvény, mely tetszőleges  $e : \text{Nat} \rightarrow \text{Nat}$  program működését szimulálja. Mivel az átíró rendszer úgy van megadva, hogy mindig csak egy átírási lépést választhatunk, és mivel minden átírási sorozat véges, emiatt  $u$  jól definiált.

Tfh. hogy  $u$  definiálható System T-ben, mégpedig az  $e_u : \text{Nat} \rightarrow \text{Nat} \rightarrow \text{Nat}$  kifejezéssel, vagyis a következő igaz:  $e_u \overline{m} \overline{n} \mapsto^* \overline{u(m)(n)}$ .

Ekkor megadjuk az  $e_\Delta : \text{Nat} \rightarrow \text{Nat}$  kifejezést a következőképp:  $e_\Delta := \lambda^{\text{Nat}} x. \text{suc}(e_u x x)$ . Ekkor egyrészt tudjuk, hogy  $u$ -ra teljesül, hogy

$$e_\Delta \overline{\ulcorner e_\Delta \urcorner} \mapsto^* \overline{u(\ulcorner e_\Delta \urcorner)(\ulcorner e_\Delta \urcorner)},$$

másrészt  $e_\Delta$  definíciójából és  $e_u$  tulajdonságából

$$e_\Delta \overline{\ulcorner e_\Delta \urcorner} \mapsto \text{suc}(e_u \overline{\ulcorner e_\Delta \urcorner} \overline{\ulcorner e_\Delta \urcorner}) \mapsto^* \text{suc}(\overline{u(\ulcorner e_\Delta \urcorner)(\ulcorner e_\Delta \urcorner)}).$$

Ebből az következik, hogy a kiértékelés nem egyértelmű, hiszen két különböző értéket is kapnánk ugyanabból a kifejezésből. Ez ellentmondás, tehát  $u$  nem definiálható System T-ben.  $\square$

## 8. Végtelen adattípusok

## 9. Parcialitás, rekurzív típusok

## 10. Imperatív programozás

## 11. Polimorfizmus

## 12. Altípus

## 13. Függő típus

## 14. Megoldások

2.1. feladat megoldása.

$$\begin{aligned} ((x + x')[x \mapsto x'])[x' \mapsto x] &= (x + x) \\ (x + x)[x \mapsto x' + x] &= ((x' + x) + (x' + x)) \\ (\text{suc}(\text{suc } i))[i \mapsto \text{suc } i'] &= \text{suc}(\text{suc}(\text{suc } i')) \\ (\text{num}(\text{suc } i))[x \mapsto \text{num zero}] &= \text{num}(\text{suc } i) \end{aligned}$$

2.2. feladat megoldása.

$$\begin{aligned} xs \in \text{List}_{\text{Nat}} &::= \text{nil} \mid \text{cons } n \ xs \\ \text{nil aritása} & \ () \text{List}_{\text{Nat}} \\ \text{cons aritása} & (\text{Nat}, \text{List}_{\text{Nat}}) \text{List}_{\text{Nat}} \end{aligned}$$

2.3. feladat megoldása. Nyilak helyett a kötések alá egy sorszámot írtunk, és a kötött változók alá írtuk a kötés sorszámát.

$$\begin{aligned}
& \bar{x} + \text{num } \bar{i} \\
& \text{let } \bar{x} \text{ in } x.\text{num } \bar{i} + \frac{x}{1} \\
& \text{let } \bar{x} \text{ in } x.\bar{x}' + \text{let } \frac{x}{1} \text{ in } \frac{x'}{2}.\frac{x'}{2} + \frac{x}{1} \\
& \text{let } \bar{x} \text{ in } \frac{x}{1}.\frac{x}{1} + \text{let } \frac{x}{1} \text{ in } \frac{x}{2}.\frac{x}{2} + \frac{x}{2} \\
& \text{let } \bar{x} \text{ in } x.(\text{let } \frac{x}{1} \text{ in } \frac{x'}{2}.\bar{x}'' + \frac{x'}{2}) + \text{let } \bar{x}' \text{ in } \frac{x'}{3}.\frac{x'}{3} + \bar{x}''
\end{aligned}$$

2.4. feladat megoldása. Nem, mivel a let csak Exp fajtájú változót köt.

2.5. feladat megoldása.

$$\begin{aligned}
x & \stackrel{?}{=} x' && \text{:=igaz, ha } x = x' \\
& && \text{hamis, egyébként} \\
x & \stackrel{?}{=} \text{f } x'.t' t'_1 \dots t'_n && \text{:= hamis} \\
\text{f } x.t t_1 \dots t_n & \stackrel{?}{=} x && \text{:=hamis} \\
\text{f } x.t t_1 \dots t_n & \stackrel{?}{=} \text{f } x'.t' t'_1 \dots t'_n && \text{:=igaz, ha } t_1 = t'_1 \text{ és } \dots \text{ és } t_n = t'_n \text{ és } t[x \mapsto y] = t'[x' \mapsto y], \text{ ahol } y \text{ friss} \\
& && \text{hamis, egyébként} \\
\text{f } x.t t_1 \dots t_n & \stackrel{?}{=} \text{g } x'.t' t'_1 \dots t'_m && \text{:=hamis}
\end{aligned}$$

2.6. feladat megoldása.

$$\begin{aligned}
(\text{let } x \text{ in } x.x + x)[x \mapsto \text{num zero}] &= \text{let num zero in } x.x + x \\
(\text{let } x' \text{ in } x.x' + x)[x' \mapsto \text{num zero}] &= \text{let num zero in } x.\text{num zero} + x \\
(\text{let } x' \text{ in } x.x' + x')[x' \mapsto x] &= \text{let } x \text{ in } y.x + x
\end{aligned}$$

2.7. Nem, igen, nem, nem, igen, igen.

2.8 feladat megoldása. Példák:

$$\begin{aligned}
& \text{d } y.y \\
& \text{d } y.\text{g } y y \\
& \text{d } y.\text{d } x.\text{g } x y \\
& \text{d } y.\text{g } (\text{d } x.x) y
\end{aligned}$$

2.11 feladat megoldása.

$$\begin{array}{c}
\hline
\text{max zero } n \text{ is } n \\
\hline
\text{max } n \text{ zero is } n \\
\hline
\text{max } n n' \text{ is } n'' \\
\hline
\text{max } (\text{suc } n) (\text{suc } n') \text{ is } \text{suc } n''
\end{array}$$

2.12 feladat megoldása.

$$\begin{array}{c}
\hline
x \text{ hasHeight zero} \\
\hline
\end{array}$$

$$\frac{\frac{\text{num } n \text{ hasHeight zero}}{t \text{ hasHeight } n} \quad t' \text{ hasHeight } n' \quad \text{max } n \ n' \text{ is } n''}{t + t' \text{ hasHeight suc } n''}$$

2.13 feladat megoldása.

$$\frac{\frac{\frac{\text{isEven zero}}{\text{isEven } n}}{\text{isOdd suc } n}}{\text{isOdd } n}}{\text{isEven suc } n}$$

Pl. a következőképp vezetjük le, hogy a 3 páratlan.

$$\frac{\frac{\frac{\text{isEven zero}}{\text{isOdd suc zero}}}{\text{isEven (suc (suc zero))}}}{\text{isOdd (suc (suc (suc zero)))}}$$

2.14 feladat megoldása.

Igaz.

*Bizonyítás.* Az **Exp** fajtájú AST-ken szerkezeti indukcióval bizonyítjuk.  $P(n) =$  bármely  $n'$ -re létezik olyan  $n''$ , hogy  $n + n'$  is  $n''$  levezethető.  $n$  háromféle lehet (lásd 2.1. definíciót).

- Változó, ebben az esetben nem zárt, tehát nem felel meg a feladat feltételeinek, ezért nem kell bizonyítanunk semmit.
- $n = \text{zero}$ , ekkor  $P(\text{zero})$ -t kell belátnunk, tehát azt, hogy bármely  $n'$ -re létezik olyan  $n''$ , hogy  $\text{zero} + n'$  is  $n''$  levezethető.  $n''$ -t  $n'$ -nek választjuk, és alkalmazzuk a 2.3. levezetési szabályt.
- $n = \text{suc } n_1$ , ekkor azt kell belátnunk, hogy ha  $P(n_1)$  igaz, akkor  $P(\text{suc } n_1)$  is igaz.  $P(n_1)$  azt mondja, hogy minden  $n'$ -höz létezik olyan  $n_2$ , hogy  $n_1 + n'$  is  $n_2$  levezethető.  $P(\text{suc } n_1)$  bizonyításához egy tetszőleges  $n'$ -höz keresnünk kell egy olyan  $n''$ -t, melyre  $\text{suc } n_1 + n'$  is  $n''$  levezethető.  $n''$ -t a  $P(n_1)$  bizonyítása által megadott  $n_2$ -t felhasználva  $\text{suc } n_2$ -nek választjuk. Ekkor, mivel tudjuk, hogy  $n_1 + n'$  is  $n_2$  levezethető, a 2.4. levezetési szabállyal megkapjuk, hogy  $\text{suc } n_1 + n'$  is  $\text{suc } n_2$ .

□

3.1. feladat megoldása.

operátor	aritás
(egész szám beágyazása)	$(\mathbb{Z})\text{Exp}$
" – "	$(\text{szöveg})\text{Exp}$
– + –	$(\text{Exp}, \text{Exp})\text{Exp}$
– – –	$(\text{Exp}, \text{Exp})\text{Exp}$
– • –	$(\text{Exp}, \text{Exp})\text{Exp}$
–	$(\text{Exp})\text{Exp}$
let – in $x$ . –	$(\text{Exp}, \text{Exp}.\text{Exp})\text{Exp}$

3.9. feladat megoldása.

- $\cdot \vdash \text{"ab"} \bullet \text{"cd"} \mid + \mid \text{let "e" in } x.x + x \mid : \text{int}$  nem típusozható. A 3.4. lemma alapján mindig csak egyféle levezetési szabályt alkalmazhatunk, amikor alulról felfele felépítjük a levezetést. A ? lépésnél azonban elakadunk.

$$\begin{array}{c}
 \frac{}{\cdot \vdash \text{"ab"} : \text{str}} 3.11 \quad \frac{}{\cdot \vdash \text{"cd"} : \text{str}} 3.11 \quad \frac{}{\cdot \vdash \text{"e"} : \text{str}} 3.11 \quad \frac{}{\cdot, x : \text{str} \vdash x + x : \text{str}} ? \\
 \frac{}{\cdot \vdash \text{"ab"} \bullet \text{"cd"} : \text{str}} 3.15 \quad \frac{}{\cdot \vdash \text{"ab"} \bullet \text{"cd"} \mid : \text{int}} 3.15 \quad \frac{}{\cdot \vdash \text{let "e" in } x.x + x : \text{str}} 3.15 \quad \frac{}{\cdot \vdash \mid \text{let "e" in } x.x + x \mid : \text{int}} 3.12 \\
 \frac{}{\cdot \vdash \text{"ab"} \bullet \text{"cd"} \mid + \mid \text{let "e" in } x.x + x \mid : \text{int}} 3.12
 \end{array}$$

- Típusozható:

$$\begin{array}{c}
 \frac{}{\cdot \vdash \text{"ab"} : \text{str}} 3.11 \quad \frac{}{\cdot \vdash \text{"cd"} : \text{str}} 3.11 \quad \frac{}{\cdot \vdash \text{"e"} : \text{str}} 3.11 \quad \frac{(x : \text{str}) \in \cdot, x : \text{str}}{\cdot, x : \text{str} \vdash x : \text{str}} 3.9 \quad \frac{(x : \text{str}) \in \cdot, x : \text{str}}{\cdot, x : \text{str} \vdash x : \text{str}} 3.9 \\
 \frac{}{\cdot \vdash \text{"ab"} \bullet \text{"cd"} : \text{str}} 3.15 \quad \frac{}{\cdot \vdash \text{"ab"} \bullet \text{"cd"} \mid : \text{int}} 3.12 \quad \frac{}{\cdot \vdash \text{let "e" in } x.x \bullet x : \text{str}} 3.15 \quad \frac{}{\cdot \vdash \mid \text{let "e" in } x.x \bullet x \mid : \text{int}} 3.12 \\
 \frac{}{\cdot \vdash \text{"ab"} \bullet \text{"cd"} \mid + \mid \text{let "e" in } x.x \bullet x \mid : \text{int}} 3.12
 \end{array}$$

- $\text{let "ab"} \bullet \text{"cd"} \mid \text{ in } x.x + x$  típusozható.
- $\text{let "ab"} \bullet \text{"cd"} \mid \text{ in } x.x \bullet x$  nem típusozható.
- $\mid (\text{"aaa"}) \mid$  nem típusozható.

3.10. feladat megoldása.

A 3.4. lemma kiegészítése minden esetre. Tfh.  $\Gamma \vdash e : \tau$ . Ekkor:

- Ha  $e = x$ , akkor  $(x : \tau) \in \Gamma$ .
- Ha  $e = n$ , akkor  $\tau = \text{int}$ .
- Ha  $e = \text{"s"}$ , akkor  $\tau = \text{str}$ .
- Ha  $e = e_1 + e_2$ , akkor  $\tau = \text{int}$ ,  $\Gamma \vdash e_1 : \text{int}$  és  $\Gamma \vdash e_2 : \text{int}$ .
- Ha  $e = e_1 - e_2$ , akkor  $\tau = \text{int}$ ,  $\Gamma \vdash e_1 : \text{int}$  és  $\Gamma \vdash e_2 : \text{int}$ .
- Ha  $e = e_1 \bullet e_2$ , akkor  $\tau = \text{str}$ ,  $\Gamma \vdash e_1 : \text{str}$  és  $\Gamma \vdash e_2 : \text{str}$ .
- Ha  $e = \mid e' \mid$ , akkor  $\tau = \text{int}$  és  $\Gamma \vdash e' : \text{str}$ .
- Ha  $e = \text{let } e_1 \text{ in } x.e'$ , akkor valamely  $\tau_1$ -re  $\Gamma \vdash e_1 : \tau_1$  és  $\Gamma, x : \tau_1 \vdash e' : \tau$ .

*Bizonyítás.*  $\Gamma \vdash e : \tau$  szerinti indukció. Ha a 3.9. szabállyal vezettük le, akkor  $e = x$  és az indukciós hipotézisből kapjuk, hogy  $(x : \tau) \in \Gamma$ . Más szabály nincs, amivel  $e = x$ -et vezettünk volna le. Hasonlóan az összes többi esetre: minden operátorra pontosan egy levezetési szabályunk van.  $\square$

3.11. feladat megoldása.

Azt bizonyítjuk, hogy ha  $\Gamma \vdash e : \tau$ , akkor  $\Gamma \text{ wf}$ .

*Bizonyítás.*  $\Gamma \vdash e : \tau$  levezetése szerinti indukció.



- Ha a 3.9. szabályt használtuk, tudjuk, hogy  $(x : \tau) \in \Gamma$ , és ebből szeretnénk belátni, hogy  $\Gamma$  wf. Ezt  $(x : \tau) \in \Gamma$  levezetése szerinti indukcióval látjuk be.
  - Ha a 3.7. szabályt használtuk, akkor  $\Gamma = \Gamma', x : \tau$ , és a szabály feltételeiből kapjuk, hogy  $\Gamma'$  wf és  $x \notin \text{dom}(\Gamma)$ . Ezekből a 3.6. szabállyal megkapjuk, hogy  $\Gamma', x : \tau$  wf.
  - Ha a 3.8. szabályt használtuk, akkor  $\Gamma = \Gamma', y : \tau'$  és  $y \notin \text{dom}(\Gamma)$ . Az indukciós feltevésből pedig tudjuk, hogy  $\Gamma'$  wf. Megint a 3.6. szabállyal kapjuk, hogy  $\Gamma', y : \tau'$  wf.
- Ha a 3.10–3.11. szabályok valamelyikét használtuk, akkor a szabály feltételéből kapjuk, hogy  $\Gamma$  wf.
- Ha a 3.12–3.16. szabály valamelyikét használtuk, akkor az (egyik) indukciós feltevésből megkapjuk, hogy  $\Gamma$  wf.

□

3.12. feladat megoldása.

Ha  $\bullet$  helyett is  $+$  szimbólumot használnánk, akkor a 3.14. szabály helyett a következő lenne.

$$\frac{\Gamma \vdash e_1 : \text{str} \quad \Gamma \vdash e_2 : \text{str}}{\Gamma \vdash e_1 + e_2 : \text{str}}$$

Ekkor a 3.2–3.8. lemmák mind teljesülnének, kivéve a 3.4. lemmát, amit kissé módosítani kellene. A következőt mondaná: ha  $\Gamma \vdash e : \tau$  és  $e = e_1 + e_2$ , akkor  $\Gamma \vdash e_1 : \tau$  és  $\Gamma \vdash e_2 : \tau$ , anélkül, hogy tudnánk, hogy  $\tau = \text{int}$  vagy  $\tau = \text{str}$ .

3.13. feladat megoldása.

$$\begin{aligned} & (1 + 1) - |\text{''aa''} \bullet \text{''bb''}| \\ 3.25 & \mapsto 2 - |\text{''aa''} \bullet \text{''bb''}| \\ 3.26 & \mapsto 2 - 4 \\ 3.22 & \mapsto -2 \end{aligned}$$

3.14. feladat megoldása.

Érték szerinti paraméterátadás esetén a  $\text{let } (1 + 1) \text{ in } x.x$  kifejezés kiértékelése során először elvégezzük az  $1 + 1$  összeadást, majd a helyettesítés következik:

$$\frac{\overline{1 + 1 \mapsto 2} \quad 3.21}{\text{let } (1 + 1) \text{ in } x.x \mapsto \text{let } 2 \text{ in } x.x} \quad 3.28 \quad \frac{\overline{2 \text{ val}} \quad 3.19}{\text{let } 2 \in x.x \mapsto x[x \mapsto 2] = 2} \quad 3.29$$

Név szerinti paraméterátadás esetén először helyettesítünk, majd összeadunk:

$$\overline{\text{let } (1 + 1) \text{ in } x.x \mapsto x[x \mapsto 1 + 1] = 1 + 1} \quad 3.29 \quad \overline{1 + 1 \mapsto 2} \quad 3.21$$

3.15. feladat megoldása.  $\text{let } (1 + 1) \text{ in } x.x + x$ .

3.16. feladat megoldása.  $\text{let } (1 + 1) \text{ in } x.1$ .

3.17. feladat megoldása.

$x + (1 + 2)$  kiértékelése elakad, egyik szabályt sem tudjuk alkalmazni, a 3.25. szabályt azért nem, mert a feltételét nem tudjuk biztosítani.

$$\frac{\overline{1 + 2 = 3} \quad 3.21}{(1 + 2) + x \mapsto 3 + x} \quad 3.25,$$

de aztán a kiértékelés elakad, mert a 3.26. szabály második feltételét nem tudjuk biztosítani.

3.20. feladat megoldása.

Megmutatjuk, hogy bármely  $s_1, s_2$ -re létezik olyan  $e$ , hogy  $|"s_1" \bullet "s_2"|\mapsto^* * e$  és  $|"s_1"| + |"s_2"| \mapsto^* e$ . Ha  $s_1$  hossza  $n_1$ ,  $s_2$  hossza pedig  $n_2$ , és  $n_1$  és  $n_2$  összege  $n$ , akkor  $e$ -t  $n$ -nek választjuk. Megjegyezzük, hogy  $e = n_1 + n_2$  nem lenne jó választás. Megmutatjuk, hogy mindkét kifejezés  $n$ -re értékelődik.

$$\begin{array}{c} \frac{\overline{|"s_1" \bullet "s_2"|\mapsto "s_1 s_2"} \quad 3.23}{|"s_1" \bullet "s_2"|\mapsto |"s_1 s_2"|} \quad 3.27 \quad \frac{s_1 s_2 \text{ hossza } n}{|"s_1 s_2"|\mapsto n} \quad 3.27 \\ \\ \frac{\overline{|"s_1"|\mapsto n_1} \quad 3.24}{|"s_1"| + |"s_2"|\mapsto n_1 + |"s_2"|} \quad 3.25 \quad \frac{n_1 \text{ val } \quad \overline{|"s_2"|\mapsto n_2} \quad 3.24}{n_1 + |"s_2"|\mapsto n_1 + n_2} \quad 3.26 \quad \overline{n_1 + n_2 \mapsto n} \quad 3.21 \end{array}$$

3.24. feladat.

További szabályok:

$$\begin{array}{c} \frac{e_1 \text{ err}}{e_1 \circ e_2 \text{ err}} \circ \in \{-, \bullet\} \\ \\ \frac{e_1 \text{ val} \quad e_2 \text{ err}}{e_1 \circ e_2 \text{ err}} \circ \in \{-, \bullet\} \\ \\ \frac{e \text{ err}}{|e| \text{ err}} \\ \\ \frac{e_1 \text{ err}}{\text{let } e_1 \text{ in } x. e_2 \text{ err}} \\ \\ \frac{[e_1 \text{ val}] \quad e_2 \text{ err}}{\text{let } e_1 \text{ in } x. e_2 \text{ err}} \end{array}$$

3.25. feladat.

3.26. feladat megoldása.

Megjegyezzük, hogy nem vezetünk be egy új karakter típust itt, hanem a `head` operátor csak egy egy-hosszú szöveget hoz létre (ha tud). Szintaxis kiegészítése:

$$e \in \text{Exp} ::= \dots \mid \text{head } e$$

Típusrendszer kiegészítése:

$$\frac{\Gamma \vdash e : \text{str}}{\Gamma \vdash \text{head } e : \text{str}}$$

Operációs szemantika kiegészítése:

$$\begin{array}{c} \frac{e \mapsto e'}{\text{head } e \mapsto \text{head } e'} \\ \\ \frac{s \text{ első betűje } s_1}{\text{head } "s" \mapsto "s_1"} \end{array}$$

$$\frac{s \text{ \u00e9res sz\u00f6veg}}{\text{head "s" err}}$$

4.1. feladat.

$\text{int}, \text{str}, \text{int} \rightarrow \text{int}, \text{int} \rightarrow \text{str}, \text{str} \rightarrow \text{str}, \text{str} \rightarrow \text{int}$

4.2. feladat.

$\text{fun}^{\text{str}} x.x \bullet (x \bullet x)$

4.3. feladat. Az unicit\u00e1s (3.3. lemma) nem teljes\u00fcl, hiszen pl.  $\cdot \vdash \text{fun } x.x : \text{str} \rightarrow \text{str}$  \u00e9s  $\cdot \vdash \text{fun } x.x : \text{int} \rightarrow \text{int}$  is levezethet\u0151. A t\u00f6bbi lemma ugyan\u00fagy bizony\u00edthat\u00f3, mint a 3. fejezetben.

4.4. feladat.

V\u00e9gtelen sz\u00e1m\u00fa ilyen l\u00e9tezik:

$\text{str}$   
 $\text{int}$   
 $\text{str} \rightarrow \text{str}$   
 $\text{str} \rightarrow \text{int}$   
 $\text{int} \rightarrow \text{str}$   
 $\text{int} \rightarrow \text{int}$   
 $\text{str} \rightarrow (\text{str} \rightarrow \text{str})$   
 $\text{str} \rightarrow (\text{str} \rightarrow \text{int})$   
 $\text{str} \rightarrow (\text{int} \rightarrow \text{str})$   
 $\text{str} \rightarrow (\text{int} \rightarrow \text{int})$   
 $(\text{str} \rightarrow \text{str}) \rightarrow \text{str}$   
 $(\text{str} \rightarrow \text{str}) \rightarrow \text{int}$   
 $\text{str} \rightarrow (\text{str} \rightarrow (\text{str} \rightarrow \text{str}))$   
 $\text{str} \rightarrow (\text{int} \rightarrow (\text{str} \rightarrow (\text{int} \rightarrow \text{str})))$   
 $(\text{int} \rightarrow \text{int}) \rightarrow (\text{str} \rightarrow (\text{int} \rightarrow \text{str}))$   
 $\dots$

4.5. feladat.  $\lambda^{\text{int}} x. \lambda^{\text{str}} y. x + |y|$

4.6. feladat.  $\lambda^{\text{str} \rightarrow \text{str}} y. \lambda^{\text{str}} x. y (y (y x))$

4.8. feladat.

4.9. feladat.

4.10. feladat.