

TIPI V PROGRAMSKIH JEZIKIH IN IZREKI O VARNOSTI PROGRAMOV

FILIP KOPRIVEC

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2010): 68Q55, 68Q60, 68N18

Eno izmed pomembnejših orodij v programiranju so zagotovo tipi, saj nam omogočajo, da že pred zagonom programa preprečimo določeno vrsto napak. V članku si na primeru preprostega programskega jezika najprej ogledamo pravila sintakse in izvajanja, nato pa zanj dokažemo izrek o varnosti, ki nam s pomočjo tipov zagotavlja, da bo med izvajanjem programa njegovo stanje vedno smiselno. Na kratko predstavimo tudi lambda račun z enostavnimi tipi in njemu pripadajoči izrek o varnosti.

TYPES IN PROGRAMMING LANGUAGES AND CORRESPONDING SAFETY THEOREMS

One of the most important tools in programming is definitely the type system, which allows us to eliminate a whole class of errors before the actual evaluation of the program even takes place. This article presents a simple programming language which is used to examine syntax and evaluation rules, and proceeds with proving a safety theorem which uses types to ensure that the program state will stay sound during the execution. Simply typed lambda calculus and the corresponding safety theorem are presented at the end.

Uvod

Najpomembnejša lastnost večine programov je zagotovo pravilnost. Da bi zagotovili pravilnost programa, si pomagamo z mnogo različnimi pristopi in orodji, ki imajo različne prednosti in slabosti. Eno izmed preprostejših, a vseeno zelo močnih orodij, so *tipi*. S pomočjo tipov lahko vnaprej preprečimo nekatera stanja, ki bi utegnila privedi do napake v izvajanju.

Teoretično osnovo pri delu s tipi nam daje izrek o varnosti, ki zagotovi, da med izvajanjem programa s tipi ne bo prišlo do napake. Izrek o varnosti si bomo ogledali na preprostem programskem jeziku, na koncu pa bomo na kratko omenili, kako lahko to posplošimo tudi na funkcije.

Sintaksa

Običajno jezike podamo z različico Backus-Naurove (BNF) oblike zapisa. Jezik oziroma množico izrazov, ki jih označujemo s sintaktično spremenljivko t , definiramo tako, da naštejemo vse možne oblike izrazov, ki jih med