UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Mabel Najdovski

OBRNLJIVE FUNKCIJE SO SFERE V SVETU

Delo diplomskega seminarja

Mentorica: izr. prof. dr. Ime Priimek
Somentor: doc. dr. Ime Priimek

Ljubljana, 2016

Kazalo

Obrnljive funkcije so sfere v svetu

Povzetek

V povzetku na kratko opišemo vsebinske rezultate dela. Sem ne sodi razlaga organizacije dela – v katerem poglavju/razdelku je kaj, pač pa le opis vsebine.

Invertible maps are spheres in the universe

Abstract

Prevod slovenskega povzetka v angleščino.

Math. Subj. Class. (2020): 74B05, 65N99
Ključne besede: naravni logaritem, nenaravni algoritem
Keywords: natural logarithm, unnatural algorithm

1 Osnove Martin-Löfove odvisne teorije tipov

Sledeč (TODO cite intro to hott) bomo v tem poglavju predstavili osnovne koncepte Martin-Löfove odvisne teorije tipov. Zaradi velike razsežnosti in dokajšnje tehničnosti formalne predstavitve teorije tipov se ne bomo do potankosti spustili v njene podrobnosti, vendar bomo koncepte predstavili v nekoliko neformalnem slogu, osredotočajoč se na analogije z bolj standardnimi matematičnimi koncepti iz formalizma teorije množic.

1.1 Sodbe in pravila sklepanja

Osnovni gradniki teorije tipov so *tipi*, ki jih bomo označevali z velikimi tiskanimi črkami, kot so A, B in C, ter njihovi *elementi*, ki jih bomo označevali z malimi tiskanimi črkami, kot so x, y, z in a, b, c. Vsak element x ima natanko določen tip A, kar izrazimo s tako imenovano *sodbo* $x : A$, ki jo preberemo kot "x je tipa A". Ta je v mnogih pogledih podobna relaciji $x \in A$ iz teorije množic, vendar se od nje razlikuje v nekaj pomembnih pogledih.

Prvič, v teoriji množic je relacija $\in$ v določenem smislu *globalna*; vsak matematični objekt je kodiran kot določena množica in za poljubni množici A in B se lahko vprašamo, ali velja $A \in B$. Tako je na primer vprašanje, ali za element g grupe $\mathbb{Z}/_5$ velja $g \in \mathcal{C}^1(\mathbb{R})$ formalno smiselno, vendar tudi povsem v nasprotju z matematično prakso. V nasprotju s tem so v teoriji tipov elementi nerazdružljivi od svojih tipov; če velja sodba $x : A$, potem vprašanja "Ali velja $x : B$?" sploh ne moremo tvoriti.

Drugič, sodba $x : A$ ni trditev, ki bi jo lahko dokazali, temveč je konstrukcija, do katere lahko pridemo po nekem končnem zaporedju *pravil sklepanja*. To so sintaktična pravila, ki nam omogočijo, da iz določenega nabora sodb tvorimo nove sodbe. Primer pravila sklepanja bi bilo pravilo, ki pravi, da lahko iz sodb $x : A$ in $f : A \to B$ sklepamo, da velja sodba $f(x) : B$, kar predstavlja uporabo funkcije f na elementu x.

Poleg sodb oblike $x : A$ v teoriji tipov obstajajo še tri vrste sodb. Prvič, obstaja sodba A type, s katero izrazimo, da je tip A dobro konstruiran. Primer pravila sklepanja s to sodbo bi bilo pravilo, ki pravi, da lahko iz sodb A type in B type sklepamo, da velja sodba $A \to B$ type, kar predstavlja konstrukcijo tipa funkcij med tipoma A in B. Drugič, obstajata še sodbi $x \doteq y : A$ in $A \doteq B$ type, s katerima izražamo *sodbeno enakost*. Za obe vrsti sodbene enakosti veljajo pravila sklepanja, preko katerih postaneta ekvivalenčni relaciji, veljajo pa še določena substitucijska pravila, ki omogočajo, da lahko v poljubnem izrazu elemente in tipe nadomeščamo s sodbeno enakimi elementi in tipi. Ker bomo kasneji spoznali še drugo vrsto enakosti, je vredno poudariti, da je sodbena enakost zelo stroga oblika enakosti. Sodbeno enake izraze lahko zato razumemo kot različne zapise za *isti* element.

Pomemben element teorije tipov, ki smo ga do sedaj izpuščali, je dejstvo, da vsaka sodba nastopa v določenem *konstekstu*. Konteksti so končni seznami deklariranih spremenljivk $x_k : A_k$, ki jih sodbe v tem kontekstu lahko vsebujejo, razumemo pa jih lahko tudi kot nabor predpostavk, pod katerimi določena sodba velja. To, da je $\mathcal{J}$ sodba v kontekstu Γ, zapišemo kot $\Gamma \vdash \mathcal{J}$. Primer pravila sklepanja s sodbo v konstekstu bi bilo pravilo, ki pravi, da lahko iz sodbe $x : A \vdash b : B$ sklepamo, da velja $\emptyset \vdash \lambda x.b(x) : A \to B$, kar predstavlja konstrukcije anonimne funkcije z vezavo spremenljivke x.

Razpravo povzamemo v sledeči vzajemno rekurzivni definiciji sodb in kontekstov. To ni popolna definicija Martin-Löfove odvisne teorije tipov, vendar samo nastavek, s pomočjo katerega lahko izrazimo pravila za konstrukcijo različnih tipov in njihovih elementov.

Definicija 1.1. V Martin-Löfovi odvisni teoriji tipov obstajajo štiri vrste sodb:

1. A je tip v kontekstu Γ, kar izrazimo z
$$\Gamma \vdash A \ \mathsf{type}.$$

2. A in B sta *sodbeno enaka tipa* tipa v kontekstu Γ, kar izrazimo z
$$\Gamma \vdash A \doteq B \ \mathsf{type}.$$

3. x je element tipa A v kontekstu Γ, kar izrazimo z
$$\Gamma \vdash x : A.$$

4. x in y sta *sodbeno enaka elementa* v kontekstu Γ, kar izrazimo z
$$\Gamma \vdash x \doteq y : A.$$

Kontekst je induktivno definiran seznam sodb, podan s praviloma:

1. Obstaja prazen kontekst $\emptyset$.

2. Če je Γ kontekst in lahko prek obstoječih pravil sklepanja izpeljemo sodbo $\Gamma \vdash A \ \mathsf{type}$, je tedaj $\Gamma, x : A$ kontekst.

Ekspliciten zapis kontekstov in sodb bomo od sedaj deloma izpuščali in o njih govorili v bolj naravnem jeziku. Ko bomo torej trditve začeli stavki kot je "Naj bo A tip in x element A...", smo pravzaprav predpostavili, da velja sodba $A \ \mathsf{type}$ in da delamo v kontestku $\Gamma = x : A$.

S temi definicijami lahko za konec tega podpoglavja predstavimo še specifikaciji funkcijskih in produktnih tipov. Velik del pravil sklepanja za funkcijske tipe smo že videli na primerih, tu pa jih še dopolnimo in zberemo v definicijo.

Definicija 1.2. Naj bosta A in B tipa. Tedaj lahko tvorimo *funkcijski tip* $A \to B$, za katerega veljajo sledeča pravila sklepanja:

1. Iz $t : A$ in $f : A \to B$ lahko tvorimo $f(t) : B$.

2. Če lahko pod predpostavko $x : A$ tvorimo $b(x) : B$, lahko tvorimo tudi $\lambda x.b(x) : A \to B$.

3. Za vsak $t : A$ velja enakost $(\lambda x.b(x))(t) \doteq b(t)$.

4. Za vsak $f : A \to B$ velja enakost $\lambda x.f(x) \doteq f$.

Elemente funkcijskega tipa imenujemo *funkcije*.

Definicija 1.3. Naj bosta A in B tipa. Tedaj lahko tvorimo *produktni tip* $A \times B$, za katerega veljajo sledeča pravila sklepanja.

1. Iz $t : A \times B$ lahko tvorimo $\mathsf{pr}_1(t) : A$ in $\mathsf{pr}_2(t) : B$.
2. Iz $a : A$ in $b : B$ lahko tvorimo $(a, b) : A \times B$.
3. Za vsaka $a : A$ in $b : B$ veljata enakosti $\mathsf{pr}_1(a, b) \doteq a$ in $\mathsf{pr}_2(a, b) \doteq b$.
4. Za vsak $t : A \times B$ velja enakost $(\mathsf{pr}_1(t), \mathsf{pr}_2(t)) \doteq t$.

Elemente produktnega tipa imenujemo *pari*.

1.2 Odvisne vsote in odvisni produkti

Pomemben element *odvisne* teorije tipov je dejstvo, da lahko sodbe A type tvorimo v poljubnem kontekstu, to pa pomeni da lahko izrazimo tudi sodbe oblike $x : A \vdash B(x)$ type. V tem primeru pravimo, da je B *odvisen tip*, oziroma, da je B *družina tipov nad A*. Odvisni tipi nam bodo omogočili, da izrazimo tipe, parametrizirane s spremenljivko nekega drugega tipa.

Za delo z odvisnimi tipi vpeljemo še dve pomembni konstrukciji. Prvič, definiramo *odvisni produkt tipov A in B*, elementi katerega so predpisi, ki vsakemu elementu $x : A$ priredijo element v pripadajočem tipu $B(x)$. Če na B gledamo kot družino tipov nad A, lahko na elemente odvisnega produkta gledamo kot na *prereze družine B*, pogosto pa jih imenujemo tudi *odvisne funkcije* ali *družine elementov B, parametrizirane z A*. Drugič, definiramo *odvisno vsoto tipov A in B*, elementi katere so pari (x, y), kjer je $x : A$ in $y : B(x)$. Z odvisno vsoto tako zberemo celotno družino tipov B v skupen tip, na pare (x, y) pa lahko gledamo kot na elemente $y : B(x)$, označene z elementom $x : A$, nad katerim ležijo. Drugače pogledano lahko na pare (x, y) gledamo tudi kot na elemente $x : A$, opremljene z dodatno strukturo y iz pripadajočega tipa $B(x)$.

Definicija 1.4. Naj bo A tip in B družina tipov nad A. Tedaj lahko tvorimo tip

$$\prod_{(x:A)} B(x),$$

imenovan *odvisni produkt tipov A in B*. Zanj veljajo sledeča pravila sklepanja:

1. Iz $t : A$ in $f : \prod_{(x:A)} B(x)$ lahko tvorimo $f(t) : B(t)$.
2. Če lahko pod predpostavko $x : A$ tvorimo $b(x) : B(x)$, lahko tvorimo tudi $\lambda x.b(x) : \prod_{(x:A)} B(x)$.
3. Za vsak $t : A$ velja enakost $(\lambda x.b(x))(t) \doteq b(t)$.
4. Za vsak $f : \prod_{(x:A)} B(x)$ velja enakost $\lambda x.f(x) \doteq f$.

Definicija 1.5. Naj bo A tip in B družina tipov nad A. Tedaj lahko tvorimo tip

$$\sum_{(x:A)} B(x),$$

imenovan *odvisna vsota tipov A in B*. Zanj veljajo sledeča pravila sklepanja

1. Iz $t : \sum_{(x:A)} B(x)$ lahko tvorimo $\mathsf{pr}_1(t) : A$ in $\mathsf{pr}_2(t) : B(\mathsf{pr}_1(t))$.

2. Iz $a : A$ in $b : B(a)$ lahko tvorimo $(a, b) : \sum_{(x:A)} B(x)$.

3. Za vsaka $a : A$ $b : B(x)$ veljata enakosti $\mathsf{pr}_1(a, b) \doteq a$ in $\mathsf{pr}_2(a, b) \doteq b$.

4. Za vsak $t : \sum_{(x:A)} B(x)$ velja enakost $(\mathsf{pr}_1(t), \mathsf{pr}_2(t)) \doteq t$.

Opomba 1.6. Opazimo lahko podobnost med pravili sklepanja za odvisne produkte in funkcije ter za odvisne vsote in produkte. Ta podobnost ni naključje, saj če je A tip in B tip, neodvisen od A, lahko nanj kljub temu gledamo kot na tip, *trivialno* odvisen od A. V tem primeru veljata enakosti $\sum_{(x:A)} B \doteq A \times B$ in $\prod_{(x:A)} B \doteq A \to B$.

Primer 1.7. S pomočjo odvisnih produktov lahko podamo specifikacijo tipa *naravnih števil* $\mathbb{N}$, za katera veljajo sledeča pravila sklepanja.

1. $\mathsf{0} : \mathbb{N}$ je naravno število.

2. Če velja $n : \mathbb{N}$, velja $\mathsf{S}(n) : \mathbb{N}$.

3. Velja sledeč *princip indukcije*. Naj bo B družina tipov nad $\mathbb{N}$ in denimo, da veljata $b_{\mathsf{0}} : B(\mathsf{0})$ in $b_{\mathsf{S}} : \prod_{(n:\mathbb{N})}(B(n) \to B(\mathsf{S}(n)))$.

   Tedaj velja $\mathsf{ind}_{\mathbb{N}}(b_{\mathsf{0}}, b_{\mathsf{S}}) : \prod_{(n:\mathbb{N})} B(n)$.

4. Veljata enakosti $\mathsf{ind}(b_{\mathsf{0}}, b_{\mathsf{S}}, \mathsf{0}) \doteq b_{\mathsf{0}}$ in $\mathsf{ind}(b_{\mathsf{0}}, b_{\mathsf{S}}, \mathsf{S}(n)) \doteq b_{\mathsf{S}}(n, \mathsf{ind}(b_{\mathsf{0}}, b_{\mathsf{S}}, n))$.

Princip indukcije nam pove, da če želimo za vsako naravno število $n : \mathbb{N}$ konstruirati element tipa $B(n)$, tedaj zadošča, da konstruiramo element tipa $B(\mathsf{0})$ in pa da znamo za vsak $n : \mathbb{N}$ iz elementov tipa $B(n)$ konstruirati elemente tipa $B(\mathsf{S}(n))$, v čemer lahko prepoznamo podobnost z običajnim principom indukcije v teoriji množic. $\diamondsuit$

1.3 Interpretacija *izjave kot tipi*

S tipi ne želimo predstaviti samo matematičnih objektov, temveč tudi matematične trditve, kar bomo dosegli preko tako imenovane interpretacije *izjave kot tipi* (ang. *propositions as types*). V tej interpretaciji vsaki trditvi P dodelimo tip z istim imenom, elementi katerega so dokazi oz. *priče*, da ta trditev velja. Konstrukcija elementa $p : P$ tako postane konstrukcija priče p, ki potrjuje veljavnost trditve P, to pa ustreza dokazu trditve P.

Če si sedaj iz vidika izjav kot tipov zopet ogledamo pravila sklepanja za produktne in funkcijske tipe, lahko v njih prepoznamo pravila sklepanja za konjunkcijo in implikacijo. Dokaz trditve $P \wedge Q$ je namreč sestavljen iz para dokazov posameznih trditev P in Q, dokaz implikacije $P \Rightarrow Q$ pa lahko razumemo kot predpis, ki iz dokazov P konstruira dokaze Q. Uporaba funkcije $P \to Q$ tako ustreza pravilu *modus ponens*, ki pravi, da lahko iz veljavnosti izjav P in $P \Rightarrow Q$ sklepamo veljavnost izjave Q.

Denimo sedaj, da je A tip in P družina tipov nad A, vsak od katerih predstavlja določeno izjavo. Tako družino izjav imenujemo tudi *predikat na A*. Tedaj lahko logično interpretacijo podamo tudi odvisni vsoti in odvisnemu produktu; ustrezata namreč eksistenčni in univerzalni kvantifikaciji. Elementi odvisnega vsote $\sum_{(x:A)} P(x)$

so pari (x, p), kjer je p dokaz $P(x)$, zato lahko nanje gledamo kot na priče veljavnosti $\exists x : A.P(x)$, elementi odvisnega produkta $\prod_{(x:A)} P(x)$ pa so predpisi, ki vsakemu elementu $x : A$ priredijo dokaz izjave $P(x)$, zato lahko nanje gledamo kot na priče veljavnosti $\forall x : A.P(x)$.

Definicije predikatov in formulacije trditev, ki jih bomo predstavili v preostanku dela, bomo izrazili v jeziku interpretacije *izjave kot tipi*, kljub temu pa se lahko eksplicitnemu zapisu prič pogosto izognemo. V dokazih trditev bomo tako pogosto uporabljali naravni jezik sklepanja, vedno pa pravzaprav konstruiramo element določenega tipa, ki predstavlja trditev, ki jo dokazujemo.

1.4 Tip identifikacij

Osnovna motivacija za vpeljavo tipa identifikacij je dejstvo, da je pojem sodbene enakosti *prestrog* in da prek nje pogosto ne moremo identificirati vseh izrazov, ki bi jih želeli. Poleg tega si v skladu z interpretacijo *izjave kot tipi* želimo tip, elementi katerega bi predstavljali dokaze enakosti med dvema elementoma.

Pomankljivost sodbene enakosti si lahko ogledamo na primeru komutativnosti naravnih števil.

Primer 1.8. Seštevanje naravnih števil bomo definirali kot funkcijo

$$\mathsf{sum} : \mathbb{N} \to (\mathbb{N} \to \mathbb{N}),$$

njeno evaluacijo $\mathsf{sum}(m, n)$ pa bomo kot običajno pisali kot $m + n$. Ker je tip $\mathbb{N} \to (\mathbb{N} \to \mathbb{N})$ po opombi 1.6 sodbeno enak tipu $\prod_{(n:\mathbb{N})} \mathbb{N} \to \mathbb{N}$, lahko njegove elemente konstruiramo po indukcijskem principu naravnih števil. Izpuščajoč nekaj podrobnosti to pomeni, da želimo vrednost izraza $m + n$ definirati z indukcijo na n, torej moramo v baznem primeru podati vrednost izraza $m + \mathsf{0}$, v primeru koraka pa moramo pod predpostavko, da poznamo vrednost izraza $m + n$, podati vrednost izraza $m + \mathsf{S}(n)$. Naravno je, da izberemo $m + \mathsf{0} :\doteq m$ in $m + \mathsf{S}(n) :\doteq \mathsf{S}(m + n)$. Za poljubni *fiksni* naravni števili, recimo $\mathsf{4}$ in $\mathsf{5}$, lahko sedaj z uporabo pravil sklepanja za naravna števila pod točko 4 dokažemo, da velja $\mathsf{4} + \mathsf{5} \doteq \mathsf{5} + \mathsf{4}$. Če pa sta po drugi strani m in n *spremenljivki* tipa $\mathbb{N}$, tedaj zaradi asimetričnosti definicije seštevanja enakosti $n + m \doteq m + n$ ne moremo dokazati. Potrebujemo tip *identifikacij* $\mathsf{Id}_{\mathbb{N}}$, z uporabo katerega bi lahko z indukcijo pokazali, da velja

$$\prod_{(m,n:\mathbb{N})} \mathsf{Id}_{\mathbb{N}}(n + m, m + n).$$

$\diamondsuit$

Definicija 1.9. Naj bo A tip in $a, x : A$. Tedaj lahko tvorimo tip $\mathsf{Id}_A(a, x)$, imenovan *tip identifikacij med elementoma a in x*. Zanj veljajo sledeča pravila sklepanja:

1. Za vsak element $a : A$ obstaja identifikacija $\mathsf{refl}_a : \mathsf{Id}_A(a, a)$.

2. Velja sledeč princip *eliminacije identifikacij*. Naj bo $a : A$ in B družina tipov, indeksirana z $x : A$ ter $p : \mathsf{Id}_A(a, x)$. Denimo, da velja $r(a) : B(a, \mathsf{refl}_a)$. Tedaj velja

$$\mathsf{ind}_{\mathsf{Id}_A}(a, r(a)) : \prod_{(x:A)} \prod_{(p:\mathsf{Id}_A(a,x))} B(x, p)$$

3. Za vsak $a : A$ velja enakost $\mathsf{ind}_{\mathsf{Id}_A}(a, r(a))(a, \mathsf{refl}_a) \doteq r(a)$.

Tip identifikacij $\mathsf{Id}_A(a, x)$ bomo od sedaj pisali kar kot $a = x$ in za boljšo berljivost izpuščali ekspliciten zapis tipa A. Kadar je p identifikacija med a in x, bomo torej pisali $p : a = x$.

Konstruktor $\mathsf{refl}_a : a = a$ nam zagotavlja, da za vsak element $a : A$ obstaja kanonična identifikacija elementa samega s sabo. Princip eliminacije identifikacij nato zatrdi, da če želimo za vsako identifikacijo $p : a = x$ konstruirati element tipa $B(x, p)$, tedaj zadošča, da konstruiramo le element tipa $B(a, \mathsf{refl}_a)$. Pravimo tudi, da je družina tipov $a = x$ *induktivno definirana* s konstruktorjem refl_a.

Preko principa eliminacije identifikacij lahko dokažemo mnoge lastnosti, ki bi jih od enakosti pričakovali. Nekaj od teh vključuje:

1. Velja *simetričnost*: za vsaka elementa $x, y : A$ obstaja funkcija
$$\mathsf{sym} : (x = y) \to (y = x).$$
Identifikacijo $\mathsf{sym}(p)$ imenujemo *inverz* identifikacije p in ga pogosto označimo z p^{-1}.

2. Velja *tranzitivnost*: za vsake elemente $x, y, z : A$ obstaja funkcija
$$\mathsf{concat} : (x = y) \to ((y = z) \to (x = z)),$$
ki jo imenujemo *konkatenacija identifikacij*, $\mathsf{concat}(p, q)$ pa pogosto označimo z $p \cdot q$.

3. Funkcije ohranjajo identifikacije: za vsaka elementa $x, y : A$ in vsako funkcijo $f : A \to B$ obstaja funkcija
$$\mathsf{ap}_f : (x = y) \to (f(x) = f(y)),$$
ki jo imenujemo *aplikacija* funkcije f na identifikacije v A.

4. Družine tipov spoštujejo identifikacije: za vsaka elementa $x, y : A$ in družino tipov B nad A obstaja funkcija
$$\mathsf{tr}_B : (x = y) \to B(x) \to B(y),$$
imenovana *transport vzdolž identifikacij.* Ker sta elementa x in y identificirana, lahko preko transporta dokažemo, da sta tudi tipa $B(x)$ in $B(y)$ v bijektivni korespondenci. Pokažemo lahko namreč, da velja $\mathsf{tr}_B(p) \circ \mathsf{tr}_B(p^{-1}) = \mathsf{id}$ in obratno.

   V interpretaciji *izjave kot tipi* nam transport pove tudi, da lahko znotraj predikatov substituiramo identificirane elemente. Če je namreč P predikat na A in velja identifikacija $x = y$, tedaj $P(x)$ velja natanko tedaj kot $P(y)$.

Konstrukcije naštetih funkcij lahko poiščemo v 5. poglavju (TODO cite intro to hott), vse izmed njih pa zahtevajo preprosto, a nekoliko tehnično, uporabo eliminacije identifikacij.

V tem delu bomo pogosto imeli opravka z identifikacijami znotraj odvisnih vsot, torej z identifikacijami oblike $(x, y) = (x', y')$, kjer sta $(x, y), (x', y') : \sum_{(x:A)} B(x)$. Izkaže se, da imajo identifikacije te oblike preprostejšo karakterizacijo, ki se je bomo pogosto poslužili. Velja namreč naslednje:

Trditev 1.10. *Naj bosta $(x, y), (x', y') : \sum_{(x:A)} B(x)$. Identifikacije med (x, y) in (x', y') lahko tedaj karakteriziramo kot par identifikacij $p : x = x'$ in $\mathsf{tr}_B(p, y) = y'$.*

Formalna formulacija in uporaba te trditve je zunaj obsega tega dela. Namesto tega bomo identifikacije znotraj odvisnih vsot vedno preprosto nadomestili z pari identifikacij, kot opisano. Trditve tudi ne bomo dokazali, povemo pa lahko nekaj o njeni interpretaciji. TODO

Vredno je omeniti sledeča posebna primera:

1. Funkcija transporta vzdolž identifikacije refl_a je sodbeno enaka identiteti na $B(a)$ za vsak $a : A$. Če na prvi komponenti identifikacije znotraj odvisne vsote torej vzamemo refl_a, nam na drugi komponenti ostanejo le identifikacije med y in y' v $B(a)$.

2. Če je tip B neodvisen od A, je funkcija transporta $\mathsf{tr}_B(p) : B \to B$ enaka identiteti za vsako identifikacijo p v A. Ker je odvisna vsota $\sum_{(x:A)} B$ enaka produktu $A \times B$, nam karakterizacija pove, da so identifikacije znotraj tipa $A \times B$ sestavljene iz dveh neodvisnih identifikacij znotraj tipov A in B.

2 Sintetična homotopska teorija

Martin-Löfovo odvisno teorijo tipov bomo v tem poglavju uporabili za razvoj t.i. *sintetične homotopske teorije*. V tej interpretaciji na tipe gledamo kot na topološke prostore, na njihove elemente pa kot na točke v teh prostorih. Za to interpretacijo je ključno opažanje, da se identifikacije med dvema elementoma v mnogih pogledih obnašajo kot poti med točkama v pripadajočih prostorih. Med dvema elementoma lahko namreč obstaja več različnih identifikacij, ki jih ni moč identificirati, to pa je analogno dejstvu, da lahko med dvema točkama v topološkem prostoru obstaja več poti, med katerimi ne obstaja zvezna deformacija. Preko funkcij sym in concat lahko identifikacije kot poti invertiramo in stikamo skupaj, funkcija ap pa nam za vsako funkcijo zagotavlja določeno obliko zveznosti, saj zatrdi, da vsaka funkcija identifikacije slika v identifikacije. Preko identifikacij lahko tako brez omembe odprtih množic ali zveznosti pridemo do mnogih rezultatov iz klasične homotopske teorije.

V tem delu se bomo predvsem posvetili problemu definicije *ekvivalence tipov*, ki je analogna homotopski ekvivalenci med pripadajočima prostoroma. Kot v definiciji tipa identifikacij želimo definirati tip, elementi katerega bi predstavljali dokaze ekvivalence med dvema tipoma. Predstavili bomo dve možnosti za definicijo takega tipa in pokazali, da je nekoliko presenetljivo ena od njiju veliko manj primerna od druge. Da bi najbolje predstavili razliko med definicijama bomo vpeljali pojem *kontraktibilnosti tipov*, ki je analogen pojmu kontraktibilnosti topoloških prostorov, in pa tip $\mathbb{S}^1$, ki je analogen topološki sferi.

2.1 Homotopije

Ekvivalenco tipov A in B bomo definirali kot obstoj funkcije $f : A \to B$, ki je v primernem smislu obrnljiva, za to pa potrebujemo dobro karakterizacijo tipa identifikacij med funkcijami. V obravnavi obrnljivosti bomo namreč potrebovali identifikacije oblike $f \circ g = \mathsf{id}_A$.

Izkaže pa se, da smo v možnostih za konstrukcijo identifikacij med funkcijami pogosto zelo omejeni, zato jih bomo nadomestili t.i. *homotopijami.* Te so v večini primerov zadostne, konstruiramo pa jih veliko lažje. Homotopijo med funkcijama definiramo kot odvisno funkcijo, ki zatrdi, da se ti ujemata na vsakem elementu domene.

Definicija 2.1. Naj bosta A in B tipa ter f in g funkciji tipa $A \to B$. Definiramo tip

$$f \sim g := \prod_{(x:A)} f(x) = g(x),$$

imenovan *tip homotopij med f in g*, njegove elemente pa imenujemo *homotopije.*

Opomba 2.2. Na kratko komentiramo o podobnosti med homotopijami v teoriji tipov in homotopijami v topologiji. Naj bosta X in Y topološka prostora in $f, g : X \to Y$ zvezni funkciji. Z I označimo interval $[0, 1]$. Homotopijo med funkcijama f in g tedaj običajno definiramo kot zvezno funkcijo $H : I \times X \to Y$, za katero velja $H(0, x) = f(x)$ in $H(1, x) = g(x)$. Ker pa je I lokalno kompakten prostor, so zvezne funkcije $H : I \times X \to Y$ v bijektivni korespondenci z zveznimi funkcijami $\hat{H} : X \to \mathcal{C}(I, Y)$, kjer je $\mathcal{C}(I, Y)$ prostor zveznih funkcij med I in Y, opremljen s kompaktno-odprto topologijo. Zvezne funkcije $\alpha : I \to Y$ ustrezajo potem v Y med točkama $\alpha(0)$ in $\alpha(1)$. Če je torej H homotopija med f in g, za pripadajočo funkcijo $\hat{H}$ velja, da je $\hat{H}(x)$ pot med točkama $f(x)$ in $g(x)$ za vsak $x \in X$. To je analogno definiciji homotopij med funkcijama f in g v teoriji tipov, ki vsaki točki $x : X$ priredijo identifikacijo $f(x) = g(x)$.

Operacije na identifikacijah lahko po elementih razširimo do operacij na homotopijah, za delo s homotopijami pa bomo potrebovali še operaciji (TODO whiskering?), s katerima lahko homotopije z leve ali z desne razširimo s funkcijo.

Trditev 2.3. *Naj bosta A in B tipa in $f, g, h : A \to B$ funkcije. Denimo, da obstajata homotopiji $H : f \sim g$ in $K : g \sim h$.*

Tedaj obstajata homotopiji $H^{-1} : g \sim f$ in $H \cdot K : f \sim h$.

Dokaz. Če homotopiji H in K evaluiramo na elementu $x : A$, dobimo identifikaciji $H(x) : f(x) = g(x)$ in $K(x) : g(x) = h(x)$. Homotopijo H^{-1} lahko torej definiramo kot $\lambda x.H(x)^{-1}$, homotopijo $H \cdot K$ pa kot $\lambda x.(H(x) \cdot K(x))$. □

Trditev 2.4. *Naj bodo A, B, C in D tipi ter $h : A \to B$, $f, g : B \to C$ in $k : C \to D$ funkcije. Denimo, da obstaja homotopija $H : f \sim g$. Tedaj obstajata homotopiji $Hh : f \circ h \sim g \circ h$ in $kH : k \circ f \sim k \circ g$.*

Dokaz. Homotopijo H zopet evaluiramo na elementu $y : B$ in dobimo identifikacijo $H(y) : f(y) = g(y)$. Če sedaj nanjo apliciramo funkcijo h, dobimo identifikacijo $\mathsf{ap}_h(H(y)) : h(f(y)) = h(g(y))$. Homotopijo kH lahko torej definiramo kot $\lambda y.\mathsf{ap}_h(H(y))$.

Naj bo sedaj $x : A$. Homotopijo H lahko tedaj evaluiramo tudi na elementu $h(x)$ in tako dobimo identifikacijo $H(h(x)) : f(h(x)) = g(h(x))$. Homotopijo Hh lahko torej definiramo kot $\lambda x.H(h(x))$. $\square$

Dejstvo, da se pojma enakosti in homotopije med funkcijami lahko razlikujeta, je lahko na prvi pogled presenetljivo, ne pomeni pa nujno, da med seboj homotopne vendar različne funkcije lahko konstruiramo. Martin-Löfova odvisna teorija tipov preprosto ne vsebuje pravil sklepanja, preko katerih bi lahko iz $f \sim g$ izpeljali $f = g$. In res, obstaja metateoretični izrek o Martin-Löfovi odvisni teoriji tipov, ki pove, da obstoja takih funkcij ne moremo ne dokazati, ne ovreči. Z drugimi besedami, njihov obstoj je od teorije neodvisen. Martin-Löfovo teorijo tipov zato pogosto razširimo z aksiomom *funkcijske ekstenzionalnosti*, ki pove, da se homotopnost funkcij sklada z enakostjo funkcij.

Ta aksiom bomo večkrat uporabili, njegova točna formulacija pa je zunaj obsega tega dela. Kot s karakterizacijo identifikacij v odvisnih vsotah, bomo enakost med funkcijami prosto izmenjevali z homotopijo med funkcijami.

Vredno je poudariti, da je bila karakterizacija enakosti v odvisnih vsotah *izrek* Martin-Löfove teorije tipov, ki ga sicer nismo dokazali, ta karakterizacija enakosti v funkcijskih tipih pa je *aksiom*, zato njegova uporaba nosi nekoliko več teže. Ko bomo enakost nadomeščali s homotopijo, bomo zato to tudi izpostavili.

2.2 Obrnljivost in ekvivalenca

Opremljeni s homotopijami lahko sedaj obrnljivost funkcije $f : A \to B$ definiramo kot obstoj funkcije $g : B \to A$, za katero velja $f \circ g \sim \mathsf{id}$ in $g \circ f \sim \mathsf{id}$. Dokazi obrnljivosti f so torej trojice (g, H, K), kjer sta H in K omenjeni homotopiji.

Definicija 2.5. Za funkcijo f pravimo, da je *obrnljiva* oziroma, da *ima inverz*, če obstaja element tipa

$$\mathsf{is\text{-}invertible}(f) := \textstyle\sum_{(g:B\to A)}(f \circ g \sim \mathsf{id}) \times (g \circ f \sim \mathsf{id}),$$

imenovanega *tip inverzov funkcije f*.

Funkcije, pripadajoče elementom $\mathsf{is\text{-}invertible}(f)$, imenujemo *inverzi funkcije f*.

Definiramo lahko tudi tip desnih inverzov, imenovanih prerezi, in pa tip levih inverzov, imenovanih retrakcije.

Definicija 2.6. Za funkcijo f pravimo, da *ima prerez*, če obstaja element tipa

$$\mathsf{sec}(f) := \textstyle\sum_{(g:B\to A)} f \circ g \sim \mathsf{id},$$

imenovanega *tip prerezov funkcije f*. Funkcije, pripadajoče elementom tipa $\mathsf{sec}(f)$ imenujemo *prerezi funkcije f*.

Za funkcijo f pravimo, da *ima retrakcijo*, če obstaja element tipa

$$\mathsf{ret}(f) := \textstyle\sum_{(g:B\to A)} g \circ f \sim \mathsf{id},$$

imenovanega *tip retrakcij funkcije f*. Funkcije, pripadajoče elementom tipa $\mathsf{ret}(f)$ imenujemo *retrakcije funkcije f*.

Naša alternativna definicija za obrnljivost bo pojem *ekvivalence*. Pravimo, da je funkcija f ekvivalenca, če obstajata (potencialno različni) funkciji g in h, za kateri obstajata homotopiji $f \circ g \sim \mathsf{id}$ in $h \circ f \sim \mathsf{id}$.

Definicija 2.7. Pravimo, da je funkcija f *ekvivalenca*, če ima tako prerez kot retrakcijo, torej, če obstaja element tipa

$$\mathsf{is\text{-}equiv}(f) := \mathsf{sec}(f) \times \mathsf{ret}(f).$$

Pravimo, da je tip A *ekvivalenten* tipu B, če obstaja ekvivalenca med njima, torej element tipa $A \simeq B := \sum_{(f:A\to B)} \mathsf{is\text{-}equiv}(f)$. Funkcijo, pripadajočo elementu $e : A \simeq B$, označimo z $\mathsf{map}(e)$.

V definiciji obrnljivosti smo zahtevali, da ima funkcija obojestranski inverz, v definiciji ekvivalence pa smo zahtevali le, da ima ločen levi in desni inverz. To bi nas lahko napeljalo k prepričanju, da je pojem obrnljivosti močnejši od pojma ekvivalence, vendar spodnja trditev pokaže da sta pravzaprav logično ekvivalentna. Pokazali bomo, da lahko prerez (ali simetrično, retrakcijo) ekvivalence f vedno izboljšamo do inverza, kar pokaže, da je f tudi obrnljiva.

Dokaz je preprost in v mnogih pogledih analogen dokazem v algebri, recimo v teoriji monoidov, kjer velja, da se levi in desni inverz danega elementa vedno ujemata. V našem primeru se levi in desni inverz ne ujemata strogo, lahko pa med njima konstruiramo homotopijo.

Trditev 2.8. *Funkcija je ekvivalenca natanko tedaj, ko je obrnljiva.*

Dokaz. Denimo, da je funkcija f obrnljiva. Tedaj lahko njen inverz podamo tako kot njen prerez, kot njeno retrakcijo, kar pokaže, da je ekvivalenca.

Obratno sedaj denimo, da je funkcija f ekvivalenca. Podan imamo torej njen prerez s s homotopijo $H : f \circ s \sim \mathsf{id}$ in njeno retrakcijo r s homotopijo $K : r \circ f \sim \mathsf{id}$. Homotopijo tipa $s \circ f \sim \mathsf{id}$ lahko tedaj konstruiramo po sledečem izračunu:

$$sf \overset{K^{-1}sf}{\sim} rfsf \overset{rHf}{\sim} rf \overset{K}{\sim} \mathsf{id}.$$

Funkcijo s lahko tako podamo kot inverz funkcije f. Kot omenjeno lahko med funkcijama s in r na sledeč način konstruiramo tudi homotopijo:

$$s \overset{K^{-1}s}{\sim} rfs \overset{rH}{\sim} r. \qquad \square$$

Spomnimo se, da v teoriji tipov želimo predikate na tipu A predstaviti z družinami tipov P nad A, kjer pravimo, da predikat $P(x)$ velja, če je pripadajoči tip $P(x)$ naseljen. V tem podpoglavju smo na tipu $A \to B$ vpeljali dva predikata, $\mathsf{is\text{-}invertible}$ in $\mathsf{is\text{-}equiv}$, v prejšnji trditvi pa dokazali, da je tip $\mathsf{is\text{-}invertible}(f)$ naseljen natanko tedaj kot $\mathsf{is\text{-}invertible}(f)$, torej da sta pripadajoči trditvi ekvivalentni. Vprašamo pa se lahko tudi nekoliko več: ali velja $\mathsf{is\text{-}invertible}(f) \simeq \mathsf{is\text{-}equiv}(f)$?

Drugače pogledano je to, da je tip $\mathsf{is\text{-}invertible}(f)$ naseljen natanko tedaj kot tip $\mathsf{is\text{-}equiv}(f)$ ekvivalentno obstoju funkcij $\mathsf{is\text{-}invertible}(f) \to \mathsf{is\text{-}equiv}(f)$ in obratno. Taki funkciji smo v prešnji trditvi implicitno tudi konstruirali, ekvivalenca med tipoma $\mathsf{is\text{-}invertible}(f)$ in $\mathsf{is\text{-}equiv}(f)$ pa bi pomenila, da sta si tudi ti funkciji med seboj tudi inverzni.

Nekoliko presenetljivo se izkaže, da taka ekvivalenca za vsak f ne more obstajati, do tega pa pride zato, ker imata tipa v določenem smislu drugačno strukturo. Vpeljali bomo namreč lastnost *propozicije* in pokazali, da jo tip $\mathsf{is\text{-}equiv}(f)$ izpolnjuje za vsak f, za tip $\mathsf{is\text{-}invertible}(f)$ pa je to odvisno od strukture tipov A in B. Nadaljno bomo pokazali, da ekvivalnce ohranjajo lastnost propozicje, torej da za tipa $A \simeq B$ velja, da tip A to lastnost izpolnjuje natanko tedaj kot tip B. To bo zaključilo dokaz, saj bi obstoj ekvivalence med $\mathsf{is\text{-}invertible}(f)$ in $\mathsf{is\text{-}equiv}(f)$ za vsak f skupaj z prejšnjimi trditvami pripeljal v protislovje.

2.3 Kontraktibilnost in propozicije

Na kratko se spomnimo pojma kontraktibilnosti iz klasične topologije. Naj bo torej X topološki prostor in $x \in X$. Tedaj pravimo, da je prostor X *kontraktibilen*, če obstaja homotopija med identiteto na X in konstantno funkcijo pri x. S tem želimo izraziti, da prostor X homotopsko gledano nima nobene bistvene strukture in da ima do homotopije natanko samo eno točko, x. V teoriji tipov lahko to lastnost izrazimo na sledeč način.

Definicija 2.9. Naj bo A tip. Pravimo, da je tip A *kontraktibilen*, če obstaja element tipa

$$\mathsf{is\text{-}contr}(A) := \textstyle\sum_{(c:A)} \prod_{(x:A)} c = x.$$

Element c imenujemo *središče kontrakcije*, funkcijo $C : \prod_{(x:A)} c = x$ pa *kontrakcija.*

Če naivno preberemo definicijo, se na prvi pogled zdi, kot da smo s tem zajeli le pojem povezanosti s potmi, saj smo zahtevali obstoj točke $c : A$, za katero velja, da je vsaka točka $x : A$ z njo identificirana. Razumeti pa moramo, da to ne ustreza le izboru poti $c = x$ za vsak x, temveč *zveznemu* izboru takih poti. Tudi v klasični topologiji je obstoj zvezne funkcije $X \to \mathcal{C}(I, X)$, ki vsaki točki x priredi pot med izbrano točko c in x, ekvivalenten kontraktibilnosti X.

Če smo s pojmom kontraktibilnosti želeli izraziti, da ima tip A *natanko* eno točko, želimo s pojmom propozicije izraziti, da ima tip A *največ* eno točko. Drugače povedano želimo reči, da če je tip propozicija in vsebuje točko, da je ta tedaj tudi edina, torej, da je tip tedaj kontraktibilen.

Definicija 2.10. Naj bo A tip. Pravimo, da je tip A *propozicija*, če obstaja element tipa

$$\mathsf{is\text{-}prop}(A) := A \to \mathsf{is\text{-}contr}(A).$$

Najprej opazimo še, da če je tip A propozicija, da sta tedaj poljubna elementa $x, y : A$ identificirana. Res, katerikoli izmed njiju, denimo x, bi zadoščal, da dobimo kontraktibilnost A, posledično pa sta oba elementa identificirana z nekim središčem kontrakcije $c : A$. Če ti identifikaciji združimo, dobimo identifikacijo med x in y. Opomnimo lahko, da to ne pomeni, da tip A nujno ima element, pomeni le, da sta poljubna, hipotetična elementa identificirana.

Kot omenjeno bomo dokazali, da ekvivalence ohranjajo propozicije. Mimogrede lahko dokažemo tudi, da ekvivalence ohranjajo kontraktibilnost, vendar tega dejstva samega po sebi ne bomo potrebovali.

Trditev 2.11. *Naj bosta A in B tipa ter $A \simeq B$. Tedaj je tip A propozicija natanko tedaj, kot tip B.*

Dokaz. Denimo, da velja $\mathsf{is\text{-}prop}(A)$. Konstruirati želimo funkcijo $B \to \mathsf{is\text{-}contr}(B)$, torej denimo, da je $b : B$. Da bi dokazali $\mathsf{is\text{-}contr}(B)$, bomo za središče kontrakcije izbrali kar b, torej moramo konstruirati še kontrakcijo $\prod_{(y:B)} b = y$. Denimo torej še, da je $y : B$.

Ker sta A in B ekvivalentna, imamo funkciji $f : A \to B$ in $g : B \to A$, za kateri velja $f \circ g \sim \mathsf{id}_B$. Elementa b in y lahko torej s funkcijo g preslikamo v tip A, zato je ta gotovo naseljen. Ker je tip A propozicija je zato tudi kontraktibilen in lahko dobimo identifikaciji $c = g(b)$ in $c = g(y)$ za neko središče kontrakcije $c : A$. Ti lahko z uporabo inverza in konkatenacije združimo v identifikacijo $g(b) = g(y)$ in jo z aplikacijo funkcije f preslikamo nazaj v tip A. Identifikacijo med b in y lahko tedaj dobimo preko konkatenacije

$$b = f(g(b)) = f(g(y)) = y.$$

Obratno implikacijo dobimo povsem simetrično. $\square$

Sedaj želimo pokazati, da je tip $\mathsf{is\text{-}equiv}(f)$ res propozicija za vsako funkcijo f. Pod predpostavko, da je funkcija f ekvivalenca, moramo torej dokazati, da je tip $\mathsf{is\text{-}equiv}(f)$ kontraktibilen.

Dokaz sloni na dejstvu, da če je funkcija f ekvivalenca, da ima tedaj tudi enoličen prerez in enolično retrakcijo, oziroma, da sta tipa $\mathsf{sec}(f)$ in $\mathsf{ret}(f)$ tedaj kontraktibilna. Dokaz te trditve je precej tehničen in zunaj obsega tega dela, zato ga bomo le skicirali. Vredno pa je omeniti, da je predpostavka, da je f ekvivalenca, tukaj potrebna. V splošnem lahko seveda obstajajo funkcije z mnogo različnimi prerezi ali retrakcijami.

Zadnje dejstvo, ki ga tedaj še potrebujemo, je to, da je produkt kontraktibilnih tipov kontraktibilen, saj je $\mathsf{is\text{-}equiv}(f) = \mathsf{sec}(f) \times \mathsf{ret}(f)$. Dokaz te trditve je zelo preprost, sloni pa na karakterizaciji tipa identifikacij v produktih.

Trditev 2.12. *Naj bosta A in B tipa ter denimo, da sta kontraktibilna. Tedaj je kontraktibilen tudi tip $A \times B$.*

Dokaz. Naj bosta $a : A$ in $b : B$ središči kontrakcij tipov A in B ter C_A in C_B njuni kontrakciji. Tip $A \times B$ je tedaj kontraktibilen s srdeščem kontrakcije (a, b) in kontrakcijo $\lambda(x, y).(C_A(x), C_B(y))$. $\square$

Sedaj bomo skicirali dokaz trditve, da imajo ekvivalence res kontraktibilen tip prerezov. Dokaz za retrakcije poteka povsem simetrično.

Trditev 2.13. *Naj bo $f : A \to B$ ekvivalenca med tipoma A in B. Tedaj je tip $\mathsf{sec}(f)$ kontraktibilen.*

Dokaz. Ker je funkcija f ekvivalenca, ima prerez $s : B \to A$ in retrakcijo $r : B \to A$ s pripadajočima homotopijama H in K. Za središče kontrakcije tipa $\mathsf{sec}(f)$ lahko torej izberemo kar par (s, H), konstruirati pa moramo še kontrakcijo, ki poljuben element $\mathsf{sec}(f)$ z njim izenači. Denimo torej, da je $g : B \to A$ s homotopijo $G : f \circ g \sim \mathsf{id}$

element $\mathsf{sec}(f)$. Tedaj lahko homotopijo med s in g konstruiramo po sledečem izračunu:

$$s \overset{K^{-1}s}{\sim} r \circ f \circ s \overset{rH}{\sim} r \overset{rG^{-1}}{\sim} r \circ f \circ g \overset{Kg}{\sim} g.$$

Kompozitum homotopij označimo z L in s funkcijsko ekstenzionalnostjo pretvorimo v identifikacijo, ki jo označimo z L'. Po karakterizaciji identifikacij v odvisnih vsotah bi sedaj morali konstruirati še identifikacijo med transportom homotopije H vzdolž identifikacije L' in homotopijo G, kjer pa nastopi tehnični del dokaza. Postopamo lahko po sledečih korakih:

1. Poračunamo lahko, da velja enakost $\mathsf{tr}(L', H) = fL^{-1} \cdot H$. Prepričamo se lahko vsaj, da se tipi ujemajo. Da bi ju lahko identificirali, mora biti homotopija $\mathsf{tr}(L', H)$ namreč enakega tipa kot homotopija G, ki je tipa $f \circ g \sim \mathsf{id}$. Spomnimo se še, da je L homotopija tipa $s \sim g$. Homotopija, ki smo jo poračunali, je tedaj pravilnega tipa:
$$f \circ g \overset{fL^{-1}}{\sim} f \circ s \overset{H}{\sim} \mathsf{id}.$$

2. Željeno identifikacijo najprej preoblikujemo v $fL = H \cdot G^{-1}$. Ker je funkcija r retrakcija ekvivalence, lahko pokažemo, da je zaradi tega ekvivalenca tudi sama in zato v določenem smislu levo krajšljiva. Konstrukcija željene identifikacije je zato ekvivalentna kontrukciji identifikacije
$$rfL = rH \cdot rG^{-1}.$$
Ker je homotopija $Ks \cdot L \cdot K^{-1}g$ enaka homotopiji $rH \cdot rG^{-1}$ po definiciji L, zadošča dokazati, da velja identifikacija
$$rfL = Ks \cdot L \cdot K^{-1}g.$$

3. Za konstrukcijo zadnje identifikacije potrebujemo določeno splošnejšo trditev. Naj bodo namreč $f, g : A \to B$ in $h, k : B \to C$ funkcije in $H : f \sim g$ in $K : h \sim k$ homotopiji. Tedaj lahko z uporabo funkcijske ekstenzionalnosti in eliminacije identifikacij konstruiramo identifikacijo
$$Kf \cdot kH = hH \cdot Kg.$$
Homotopiji H in K lahko združimo v homotopijo med funkcijama $h \circ f$ in $k \circ g$ na dva različna načina, odvisno od tega ali najprej uporabimo homotopijo H ali homotopijo K, trditev pa nam pove, da se načina pravzaprav skladata. Mimogrede to združitev imenujemo *horizontalna kompozicija* homotopij H in K, trditev pa tvori podlago za njeno dobro definiranost.

   Željeno identifikacijo lahko nazadnje dobimo tako, da trditev uporabimo na homotopijah $K : r \circ f \sim \mathsf{id}$ in $L : s \sim g$.

□

To trditev je moč dokazati tudi na bolj eleganten način, vendar za to v tem delu nismo razvili potrebnega ogrodja. Kontraktibilnost smo zato morali pokazati tako rekoč na roke, čemur se v homotopski teoriji tipov ponavadi raje izognemo.

To podpoglavje zaključimo s tem, da diskusijo povzamemo v sledečem izreku:

Izrek 2.14. *Naj bo $f : A \to B$ funkcija. Tedaj je tip* $\textsf{is-equiv}(f)$ *propozicija.*

Dokaz. Denimo, da je funkcija f ekvivalenca. Po prejšnji trditvi ima tedaj funkcija f kontraktibilen tip prerezov, simetrično pa velja tudi, da ima kontraktibilen tip retrakcij. Ker je produkt kontraktibilnih tipov kontraktibilen, je tedaj kontraktibilen tudi tip $\textsf{is-equiv}(f)$. Sledi, da je $\textsf{is-equiv}(f)$ propozicija. □

2.4 Množice in krožnica $\mathbb{S}^1$

NObrnimo se sedaj nazaj h tipu $\textsf{is-invertible}(f)$. Kot omenjeno bomo pokazali, da je propozicionalnost (TODO reword) tega tipa lahko odvisna od lastnosti tipov A in B. Ker med tipoma A in B obstaja obrnljiva funkcija, sta zato po trditvi 2.8 tipa A in B tudi ekvivaletna, torej se lahko osredotočimo na le enega izmed njiju.

Denimo torej, da je za določeno funkcijo f tip $\textsf{is-invertible}(f)$ res propozicija in razmislimo, ali lahko preko tega izpeljemo kako omejitev na tip B.

Denimo torej, da je funkcija f obrnljiva, torej da obstaja funkcija $g : B \to A$ s pripadajočima homotopijama $H : f \circ g \sim \textsf{id}$ in $K : g \circ f \sim \textsf{id}$. Tedaj lahko na sledeč način konstruiramo drugačno homotopijo tipa $g \circ f \sim \textsf{id}$:

$$gf \overset{gfK^{-1}}{\sim} gfgf \overset{gHf}{\sim} gf \overset{K}{\sim} \textsf{id}.$$

Ker je po predpostavki tip $\textsf{is-invertible}(f)$ propozicija, sledi, da sta elementa (g, H, K) in $(g, H, gfK^{-1} \cdot gHf \cdot K)$ identificirana. Brez škode za splošnost lahko poskrbimo, da sta identifikaciji na prvih dveh komponentah enaki $\textsf{refl}$, zato na tretji komponenti dobimo identifikacijo tipa

$$gfK^{-1} \cdot gHf \cdot K = K.$$

Krajšamo lahko homotopijo K in nato funkcijo g, tako da dobimo identifikacijo tipa $Hf = fK$.

S tem ko smo predpostavili obstoj dveh homotopij H in K, ki obe govorita o funkcijah f in g, sta nastali dve različni možnosti za homotopijo tipa $f \circ g \circ f \sim f$, namreč Hf in fK. Če bi bil tip $\textsf{is-invertible}(f)$ propozicija, pa bi bili ti dve možnosti identificirani. Ali pa taka identifikacija nujno vedno obstaja? Na prvi pogled ni očitno, da bi morali biti homotopiji H in K v kakeršnemkoli smislu skladni, saj sta povsem poljubni.

Tu nastopi pogoj na tip B, saj so homotopije med funkcijami s kodomeno B pravzaprav družine identifikacij v tipu B. Če bi v tipu B med poljubnima točkama obstajala največ ena identifikacija, bi lahko pokazali, da tudi med poljubnima funkcijama s kodomeno B obstaja največ ena homotopija. Take tipe imenujemo *množice*.

Definicija 2.15. Naj bo A tip. Pravimo, da je tip A *množica*, če obstaja element tipa

$$\textstyle\prod_{(x,y:A)} \textsf{is-prop}(x = y).$$

Dokažimo torej, da med funkcijama, katerih kodomena je množica, obstaja največ ena homotopija.

Trditev 2.16. *Naj bosta A in B tipa ter denimo, da je tip B množica. Tedaj velja*

$$\textstyle\prod_{(f,g:A\to B)} \textsf{is-prop}(f \sim g).$$

Dokaz. Naj bosta f in g funkciji in denimo, da velja $H : f \sim g$. Dokazujemo, da je tip $f \sim g$ kontraktibilen. Za središče kontrakcije izberemo homotopijo H in denimo, da je K homotopija med f in g. Konstruirati želimo homotopijo med homotopijama H in K, torej funkcijo tipa $\prod_{(x:A)} H(x) = K(x)$, ki bi jo z uporabo funkcijske ekstenzionalnosti spremenili v identifikacijo med H in K. Naj bo torej $x : A$. Tako $H(x)$ kot $K(x)$ sta identifikaciji tipa $f(x) = g(x)$, ker pa je tip B množica, je tip $f(x) = g(x)$ propozicija. Sledi, da sta elementa $H(x)$ in $K(x)$ identificirana. □

Vrnimo se k prejšnji diskusiji. Če nadaljno predpostavimo, da je tip B množica, tedaj po prejšnji trditvi sledi, da je tip $f \circ g \circ f \sim f$ propozicija, torej sta homotopiji Hf in fK identificirani. Izkaže se tudi, da je bila to edina omejitev za propozicionalnst (TODO reword) tipa $\mathsf{is\text{-}invertible}(f)$. Dokaz poteka podobno kot dokaz, da imaja ekvivalence kontraktbilen tip prerezov, zato ga bomo izpustili.

Velja tudi več, vpeljemo lahko pojem *koherentno obrnljivih funkcij*, namreč funkcij $f : A \to B$, za katere obstaja element tipa

$$\mathsf{is\text{-}coh\text{-}invertible}(f) := \sum_{(g:B\to A)} \sum_{(H:f\circ g\sim \mathsf{id})} \sum_{(K:f\circ g\sim \mathsf{id})} Hf = fK.$$

Zanje velja sledeči izrek:

Izrek 2.17. *Za vsako funkcijo f sta tipa $\mathsf{is\text{-}equiv}(f)$ in $\mathsf{is\text{-}coh\text{-}invertible}(f)$ ekvivalentna.*

Po prejšnji diskusiji velja tudi naslednja posledica.

Posledica 2.18. *Naj bo $f : A \to B$ funkcija in denimo, da je tip B množica. Tedaj sta tipa $\mathsf{is\text{-}equiv}(f)$ in $\mathsf{is\text{-}invertible}(f)$ ekvivalentna.*

Dokaz. Po prejšnjem izreku in tranzitivnosti ekvivalence zadošča pokazati, da sta ekvivalentna tipa $\mathsf{is\text{-}invertible}(f)$ in $\mathsf{is\text{-}coh\text{-}invertible}(f)$. Če je funkcija f koherentno obrnljiva, je tedaj očitno tudi obrnljiva. Ker pa je tip B množica, po trditvi 2.16, sledi, da lahko tudi obrnljive funkcije izboljšamo do koherentno obrnljivih. □

Definicija 2.19. Naj bo $f : \prod_{(x:A)} (Bx \to Cx)$ družina funkcij. Definiramo funkcijo $\mathsf{tot}(f) : \sum_{(x:A)} Bx \to \sum_{(x:A)} Cx$ s predpisom $\mathsf{tot}(f)(x, y) = (x, f(x)(y))$.

Trditev 2.20. *Naj bo $f : \prod_{(x:A)} (Bx \to Cx)$ družina funkcij in denimo, da je $f(x)$ ekvivalenca za vsak $x : A$. Tedaj je ekvivalenca tudi funkcija $\mathsf{tot}(f)$.*

Dokaz. Ker je funkcija $f(x)$ ekvivalenca za vsak $x : A$, lahko tvorimo družino funkcij $s : \prod_{(x:A)} (Cx \to Bx)$, kjer je $s(x)$ prerez funkcije $f(x)$. Trdimo, da je tedaj $\mathsf{tot}(s)$ prerez funkcije $\mathsf{tot}(f)$, saj za vsak $(x, y) : \sum_{(x:A)} Cx$ velja enakost

$$\mathsf{tot}(f)(\mathsf{tot}(s)(x, y)) = \mathsf{tot}(f)(x, s(x)(y)) = (x, f(x)(s(x)(y))) = (x, y).$$

Analogno lahko konstruiramo retrakcijo funkcije $\mathsf{tot}(f)$, kar zaključi dokaz. □

Zgornja trditev je pomembna, saj nam omogoči, da konstrukcijo ekvivalence med odvisnima vsotama z istim baznim tipom poenostavimo na konstrukcijo družine ekvivalenc, kar je pogosto veliko lažje. Uporabljali ga bomo v obliki sledeče posledice:

Posledica 2.21. *Naj bo A tip, B in C družini tipov nad A in denimo, da velja $Bx \simeq Cx$ za vsak $x : A$. Tedaj velja $\sum_{(x:A)} Bx \simeq \sum_{(x:A)} Cx$.*

2.5 Podtipi

Definicija 2.22. Naj bo A tip in P družina tipov nad A. Pravimo, da je P *predikat*, če velja $\mathsf{is\text{-}prop}(Px)$ za vsak $x : A$.

Trditev 2.23. *Naj bo A tip, P predikat na A, B pa družina tipov nad A. Denimo, da obstaja družina funkcij $s : \prod_{(x:A)}(Bx \to Px)$. Tedaj velja ekvivalenca*

$$\sum_{(x:A)} Bx \simeq \sum_{(t:\, \sum_{(x:A)} Px)} B(pr_1 t).$$

Dokaz. Po asociativnosti odvisne vsote je desna stran ekvivalence ekvivalentna tipu $\sum_{(x:A)} \sum_{(p:Px)} Bx = \sum_{(x:A)}(Px \times Bx)$. Po posledici 2.21 torej zadošča pokazati, da za vsak $x : A$ obstaja ekvivalenca $Bx \simeq Px \times Bx$.

Funkcijo $f : Bx \to Px \times Bx$ definiramo kot $\lambda y.\, (s(x, y),\, y)$, za funkcijo $g : Px \times Bx \to Bx$ pa lahko vzamemo drugo projekcijo. Očitno velja enakost $g(f(y)) = y$, ker pa je P predikat, velja tudi enakost $f(g\,(p, y)) = (s(x, y), y) = (p, y)$.

□

3 Karakterizacija obrnljivosti

Definicija 3.1. *Prosta zanka* na tipu A je sestavljena iz točke $a : A$ in identifikacije $a = a$. Tip vseh prostih zank na tipu A označimo s

$$\mathsf{free\text{-}loop}(A) := \sum_{(x:A)} x = x.$$

Izrek 3.2. *Tip obrnljivih funkcij med A in B je ekvivalenten tipu prostih zank na tipu $A \simeq B$.*

Dokaz. Želimo konstruirati ekvivalenco tipa

$$\sum_{(f:A\to B)} \mathsf{is\text{-}invertible}(f) \simeq \sum_{(e:A\simeq B)}(e = e).$$

Ker je $\mathsf{is\text{-}equiv}$ predikat in ker po trditvi 2.8 za vsako funkcijo f obstaja funkcija $\mathsf{is\text{-}invertible}(f) \to \mathsf{is\text{-}equiv}(f)$, najprej opazimo, da po trditvi 2.23 velja ekvivalenca

$$\sum_{(f:A\to B)} \mathsf{is\text{-}invertible}(f) \simeq \sum_{(e:A\simeq B)} \mathsf{is\text{-}invertible}(\mathsf{map}e).$$

Po posledici 2.21 torej zadošča pokazati, da za vsak element $e : A \simeq B$ obstaja ekvivalenca

$$\mathsf{is\text{-}invertible}(\mathsf{map}e) \simeq (e = e).$$

Oglejmo si tip

$$\mathsf{is\text{-}invertible}(\mathsf{map}e) = \sum_{(g:B\to A)}(\mathsf{map}e \circ g \sim id) \times (g \circ \mathsf{map}e \sim id).$$

Po asociativnosti odvisne vsote ta ekvivalenten tipu

$$\sum_{(H:\, \sum_{(g:B\to A)} \mathsf{map}e \circ g \sim id)}(\mathsf{map}H \circ \mathsf{map}e \sim id) =$$
$$\sum_{(H:\mathsf{section}(\mathsf{map}e))}(\mathsf{map}H \circ \mathsf{map}e \sim id),$$

ker pa imajo po trditvi TODO ekvivalence kontraktibilen tip prerezov, po trditvi (TODO kontraktibilen bazni prostor) velja še ekvivalenca

$$\sum_{(H:\mathsf{section}(\mathsf{map}e))}(\mathsf{map}H \circ \mathsf{map}e \sim id) \simeq (\mathsf{sec}e \circ \mathsf{map}e \sim id)\,.$$

Sledi, da velja $\mathsf{is\text{-}invertible}(\mathsf{map}e) \simeq (\mathsf{sec}e \circ \mathsf{map}e \sim id)$, dokaz pa zaključimo še z zaporedjem ekvivalenc, ki jih argumentiramo spodaj.

$$\begin{aligned}
&(\mathsf{sec}e \circ \mathsf{map}e \sim id) \simeq \\
&(\mathsf{map}e \circ \mathsf{sec}e \circ \mathsf{map}e \sim \mathsf{map}e) \simeq \\
&(\mathsf{map}e \sim \mathsf{map}e) \simeq \\
&(\mathsf{map}e = \mathsf{map}e) \simeq \\
&(e = e)
\end{aligned}$$

- Ker je e ekvivalenca, je po trditvi TODO ekvivalenca tudi delovanje $\mathsf{map}e$ na homotopije.
- Funkcija $\mathsf{sec}e$ je prerez funkcije $\mathsf{map}e$.
- TODO funext
- Po trditvi **??** lahko zanko na funkciji $\mathsf{map}e$ dvignemo do zanke na pripadajoči ekvivalenci e.

□

Slovar strokovnih izrazov

universe svet