UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Mabel Najdovski

OBRNLJIVE FUNKCIJE SO SFERE V SVETU

Delo diplomskega seminarja

Mentor: prof. dr. Andrej Bauer
Somentor: asist. - razisk. PhD. Egbert Marteen Rijke

Ljubljana, 2024

Kazalo

Obrnljive funkcije so sfere v svetu

Povzetek

Predstavimo definicijo sodb in kontekstov ter pokažemo njihovo uporabo za definicijo konstrukcij tipov v Martin-Löfovi odvisni teoriji tipov.

Na funkcijah vpeljemo pojma obrnljivosti in ekvivalence ter pokažemo, da sta logično ekvivalentna. Na tipih vpeljemo pojma kontraktibilnosti in propozicij ter pokažemo, da je pojem ekvivalence propozicija. Vpeljemo tip krožnice in aksiom univalence ter ju uporabimo kot protiprimer, da pokažemo, da pojem obrnljivosti ni vedno propozicija. Posledično pojma obrnljivosti in ekvivalence nista ekvivalentna, saj pokažemo, da ekvivalence ohranjajo propozicionalnost. Na tipih vpeljemo še pojem množic in skiciramo razlog, zakaj sta pojma obrnljivosti in ekvivalence na funkcijah med množicami ekvivalentna.

Predstavimo še nekaj standardnih trditev homotopske teorije tipov in predstavimo karakterizacijo obrnljivosti, ki jo poveže z ekvivalenco. Karakterizacijo uporabimo, da pokažemo povezavo med obrnljivostjo in tipom sfere.

Invertible maps are spheres in the universe

Abstract

We present the definition of judgments and contexts and use them to show the definitions of type formers in Martin-Löf dependent type theory.

We introduce the notions of invertibility and equivalence of functions and show that they are logically equivalent. We introduce the notions contractibility and propositionality of types and show that the notion of equivalence always forms a proposition. We introduce the circle type and the univalence axiom and use them as a counterexample to show that the notion of invertibility need not always be a proposition. Consequently, the notions of invertibility and equivalence cannot be equivalent, since we show that equivalences preserve propositionality.

We present a few standard results of homotopy type theory and present a characterisation of invertibility that connects it with equivalence. We use this characterisation to show a connection between invertibility and the sphere type.

Math. Subj. Class. (2020): 03B38

Ključne besede: homotopska teorija tipov, obrnljivost, ekvivalenca, sfera

Keywords: homotopy type theory, invertibility, equivalence, sphere

1 Uvod

Teorije tipov so logični formalizmi, ki slonijo na objektih, imenovanih tipi, opremljenih s tako imenovanimi konstruktorji indukcijskimi principi. Z razliko od teorije množic ne predpostavimo obstoja vesolja množic, znotraj katerega prepoznamo in kodiramo matematične objekte, kot so produkti, funkcije in naravna števila, vendar le te aksiomatiziramo kot prvorazredne objekte. Konstruktorji nam povejo, kako lahko tvorimo njihove elemente, indukcijski principi pa nam povejo, kako o njih dokazujemo trditve in na njih gradimo konstrukcije.

Osnove sodobne teorije tipov segajo v leto 1971, ko je švedski matematik Per Martin-Löf v neobjavljenem članku prvič opisal sistem, obliko katerega dandanes imenujemo Martin-Löfova odvisna teorija tipov. Dve leti pozneje je teorijo razširil in takrat tudi prvič podal induktivno definicijo tipa identifikacij, elementi katerega predstavlajo dokaze enakosti med elementi drugih tipov [4]. Tip identifikacij v tej obliki – imenovani intezionalna enakost – dolgo časa ni bil dobro razumljen, njegova raba je začela zamirati in pojavljati so se začele tudi druge teorije tipov z drugačnimi pojmi enakosti, imenovane ekstenzionalna enakost.

Ponovno zanimanje za intenzionalno enakost je začelo vznikati v prvem desetletju tega tisočletja, ko se je za teorijo tipov začel zanimati zdaj pokojni Vladimir Vojevodski. Ta je izhajal iz področja homotopske teorije, na katerem je pred vstopom v teorijo tipov prejel Fieldsovo priznanje. Za petami pa je imel zaporedje dogodkov, v katerem so se dokazi večih matematikov na področju homotopske teorije, vključno z njim, vrsto let po objavi izkazali za napačne. To je v njem vzbudilo zanimanje za teorije tipov, saj na njih slonijo dokazovalni pomočniki; programski jeziki, znotraj katerih je moč izraziti in dokazati matematične trditve [6].

Izkušnje Vojevodskega na področju homotopske teorije pa so v teorijo tipov pripeljale novo interpretacijo. Tipe lahko namreč interpretiramo kot topološke prostore, elemente intenzionalnega tipa identifikacij pa kot poti v teh prostorih. S tem je dodatno interpretacijo dobila tudi tako imenovana *relevanca dokazov* (ang. proof relevance); ideja iz konstruktivne matematike, ki pravi, da dokazov, predvsem dokazov enakosti, ne smemo zavreči, temveč da lahko nosijo pomembne informacije. Ločeni dokazi enakosti se med seboj lahko razlikujejo, analogno pa med dvema točkama v prostoru lahko konstruiramo več različnih poti. Kljub temu se dva dokaza lahko izkažeta za različna na nebistven način, to pa je analogno potema v prostoru, med katerima lahko konstruiramo homotopijo.

Vojevodski je v teorijo tipov vpeljal vrsto pomembnih konceptov, vsak izmed katerih je izvirno izhajal iz homotopske teorije [6]. Prepoznal je, da je struktura identifikacij v tipih za njihovo razumevanje ključna in vpeljal koncepte kot so kontraktibilnost, propozicije in množice, vse izmed katerih bomo v tem delu spoznali. Ta pristop do teorije tipov pogosto imenujemo tudi homotopska teorija tipov.

Prepoznal pa je tudi, da je dosedanje razumevanje ekvivalence med tipi v določenem smislu zmotno, zmotno pa je natanko v primeru, ko tipi pod vprašanjem nosijo višjo homotopsko strukturo. Prejšnji pojem ekvivalence bomo v tem delu imenovali obrnljivost, popravljeni pojem Vojevodskega pa ekvivalenca. Želimo namreč, da je pojem ekvivalence *lastnost* funkcij, pojem obrnljivosti pa je na funkcijah predstavljal *strukturo*. To je v konstrukcije z obrnljivostjo vpeljalo nepotrebne arbitrarne izbire, najpomembneje pa je pojem obrnljivostji nekompatibilen z Vojevodskijevem aksiomom univalence. Ta aksiom zatrdi, da se dokazi enakost med tipi sklada z ekvivalencami med njimi; ideja, ki je za razvoj homotopske teorije v teoriji tipov ključna. Če pa bi analogno postavili aksiom, ki zatrdi, da se dokazi enakost med tipi skladajo z obrnljivimi funkcijami med njimi, bi teorija postala dokazljivo nekonsistenta.

S tem se je zgodba obrnljivosti do neke mere končala; Vojevodski je kvalitativno prepoznal, da je s pojmom v določenih primerih nekaj narobe in ga nadomestil. V tem delu pa se k obrnljivosti ponovno obrnemo in podamo kvantitaivno obravnavo, ki karakterizira povezavo med obrnljivostjo in ekvivalenco. S tem postane jasneje, kako višja homotopska struktura v tipih vpliva na njuno razliko. Ne nazadnje karakterizacijo uporabimo za to, da poiščemo nepričakovano povezavo med obrnljivostjo in homotopskim tipom sfere.

V prvem poglavju kratko predstavimo osnove Martin-Löfove odvisne teorije tipov, njena pravila sklepanja in intezionalni tip identifikacij. V drugem poglavju definiramo pojma obrnljivosti in ekvivalence ter kvalitativno predstavimo razliko med njima, spotoma pa vpeljemo več pomembnih konceptov in elementarnih izrekov homotopske teorije tipov. V zadnjem poglavju dokažemo nekaj močnejših izrekov homotopske teorije tipov in nazadnje predstavimo našo karakterizacijo.

Rezultata zadnjega poglavja sta formalizirana v dokazovalnem pomočniku Agda, ki implementira Martin-Löfovo teorijo tipov. To pomeni, da je bila pravilnost dokazov v celoti računalniško preverjena in sloni le na konsistenci teorije tipov in njeni pravilni implementaciji v Agdi. Formalizacija je bila narejena s pomočjo knjižnice 1Lab, dostopne na povezavi [1], sama formalizacija pa je dostopna na github repozitoriju dela [2].

2 Osnove Martin-Löfove odvisne teorije tipov

Sledeč [3] 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.

2.1 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 lahko teoriji tipov tvorimo še tri vrste sodb. Tvorimo lahko sodbo A type, s katero izrazimo, da je A tip, konstruiran po veljavnih pravilih sklepanja. 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. Tako lahko na primer tvorimo tip funkcij med tipoma A in B. Tvorimo lahko 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 $\Gamma \vdash \mathcal{J}$. Kontekste najpogosteje potrebujemo za tvoritev elementov funkcijskega tipa, kar storimo s tako imenovano *lambda abstrakcijo.* Če namreč velja sodba $\Gamma, x : A \vdash b : B$, lahko spremenljivko $x : A$ *vežemo* in tvorimo sodbo $\Gamma \vdash \lambda x.b(x) : A \to B$.

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 2.1. V Martin-Löfovi odvisni teoriji tipov lahko tvorimo 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
$$\Gamma \vdash x : A.$$
Kadar velja sodba $x : A$ pogosto pravimo tudi, da je tip A *naseljen.*
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. $\bullet$ je kontekst. Predstavlja prazen kontekst brez predpostavk.
2. Če je Γ kontekst in velja sodba $\Gamma \vdash A \ \mathsf{type}$, je tedaj $\Gamma, x : A$ kontekst. Da bi kontekst Γ lahko razširili s predpostavko $x : A$ moramo namreč v kontekstu Γ najprej tvoriti tip A.

Ekspliciten zapis kontekstov in sodb bomo deloma izpuščali in o njih govorili v 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 smo dosedanji kontekst razširili s spremenljivko $x : A$.

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 2.2. Naj bosta A in B tipa. Tedaj lahko tvorimo *funkcijski tip* $A \to B$, njegove elemente pa imenujemo *funkcije*. Zanj veljajo sledeča pravila sklepanja:

1. Iz elementa $t : A$ in funkcije $f : A \to B$ lahko tvorimo element $f(t) : B$.
2. Če lahko pod predpostavko $x : A$ tvorimo element $b(x) : B$, lahko tvorimo tudi funkcijo $\lambda x.b(x) : A \to B$.
3. Naj bo $x : A$. Tedaj za vsaka $b(x) : B$ in $t : A$ velja enakost
$$(\lambda x.b(x))(t) \doteq b(t).$$
4. Za vsako funkcijo $f : A \to B$ velja enakost $\lambda x.f(x) \doteq f$.

Definicija 2.3. Naj bosta A in B tipa. Tedaj lahko tvorimo *produktni tip* $A \times B$, za katerega veljajo sledeča pravila sklepanja.

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

Elemente produktnega tipa imenujemo *pari*.

2.2 Odvisne vsote in odvisni produkti

Pomemben element *odvisne* teorije tipov je dejstvo, da lahko sodbe $A \ \mathsf{type}$ tvorimo v poljubnem kontekstu, to pa pomeni da lahko izrazimo tudi sodbe oblike $x : A \vdash B(x) \ \mathsf{type}$. 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 gledemo 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 2.4. 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 elementa $t : A$ in odvisne funkcije $f : \prod_{(x:A)} B(x)$ lahko tvorimo element $f(t) : B(t)$.
2. Če lahko pod predpostavko $x : A$ tvorimo element $b(x) : B(x)$, lahko tvorimo tudi funkcijo $\lambda x.b(x) : \prod_{(x:A)} B(x)$.
3. Naj bo $x : A$. Tedaj za vsaka $b(x) : B$ in $t : A$ velja enakost
$$(\lambda x.b(x))(t) \doteq b(t).$$
4. Za vsako funkcijo $f : A \to B$ velja enakost $\lambda x.f(x) \doteq f$.

Definicija 2.5. 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 elementa $t : \sum_{(x:A)} B(x)$ lahko tvorimo elementa $\mathsf{pr}_1(t) : A$ in
$$\mathsf{pr}_2(t) : B(\mathsf{pr}_1(t)).$$
2. Iz elementov $a : A$ in $b : B(a)$ lahko tvorimo element $(a, b) : \sum_{(x:A)} B(x)$.
3. Za vsaka elementa $a : A$ $b : B(x)$ veljata enakosti $\mathsf{pr}_1(a, b) \doteq a$ in $\mathsf{pr}_2(a, b) \doteq b$.
4. Za vsak element $t : \sum_{(x:A)} B(x)$ velja enakost $(\mathsf{pr}_1(t), \mathsf{pr}_2(t)) \doteq t$.

Opomba 2.6. 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 2.7. 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 $B(n)$, da 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 tem lahko prepoznamo podobnost z običajnim principom indukcije v teoriji množic. $\diamondsuit$

2.3 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 dodelimo tip, elementi katerega so dokazi, da ta trditev velja. Z drugimi besedami, če tip P predstavlja trditev, jo tedaj dokažemo tako, da konstruiramo element $p : P$.

Vsak tip lahko predstavlja trditev, največkrat pa jih želimo predstaviti s posebnim razredom tipov, imenovanih *propozicije*. O njih bomo več povedali v naslednjem poglavju.

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. Naj namreč tipa P in Q predstavljata trditvi. Dokazi trditve $P \wedge Q$ so sestavljeni iz parov dokazov posameznih trditev P in Q, zato lahko trditev $P \wedge Q$ predstavimo s produktom tipov $P \times Q$. Ker pa dokaze implikacije $P \Rightarrow Q$ lahko razumemo kot predpise, ki iz dokazov P konstruirajo dokaze Q, lahko trditev $P \Rightarrow Q$ predstavimo s tipom $P \to Q$. Uporaba funkcije tipa $P \to Q$ tako ustreza pravilu *modus ponens*, ki pravi, da lahko iz veljavnosti izjav P in $P \Rightarrow Q$ sklepamo veljavnost izjave Q.

Kadar veljata tako $P \to Q$ kot $Q \to P$ pravimo, da sta tipa P in Q *logično ekvivalentna*. To terminologijo vpeljemo zato, ker med tipi kasneje definiramo tudi močnejši pojem ekvivalence.

Denimo sedaj, da je A tip in P družina tipov nad A, vsak od katerih predstavlja določeno trditev. Tako družino tipov imenujemo tudi *predikat na A*. Tedaj lahko logično interpretacijo podamo tudi odvisni vsoti in odvisnemu produktu; ustrezata namreč eksistenčni in univerzalni kvantifikaciji. Elementi odvisne vsote $\sum_{(x:A)} P(x)$ so namreč pari (x, p), kjer je p dokaz trditve $P(x)$, zato lahko nanje gledamo kot na dokaze veljavnosti trditve $\exists\, x : A.P(x)$. Elementi odvisnega produkta $\prod_{(x:A)} P(x)$ so predpisi, ki vsakemu elementu $x : A$ priredijo dokaz izjave $P(x)$, zato lahko nanje gledamo kot na dokaze veljavnosti $\forall x : A.P(x)$.

V skladu z interpretacijo *izjave kot tipi* bomo v tem delu definicije in trditve formuliramo kot tipe. V dokazih trditev bomo kljub temu pogosto uporabljali naravni jezik sklepanja, vedno pa pravzaprav konstruiramo element določenega tipa, ki predstavlja trditev, ki jo dokazujemo.

2.4 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 seštevanja naravnih števil.

Primer 2.8. Seštevanje naravnih števil definiramo kot funkcijo

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

njeno evaluacijo $\mathsf{sum}(m, n)$ pa kot običajno pišemo kot $m+n$. Ker je tip $\mathbb{N} \to (\mathbb{N} \to \mathbb{N})$ po opombi 2.6 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 $m + \mathsf{0} := m$ in $m + \mathsf{S}(n) := \mathsf{S}(m + n)$. 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, za vsaki naravni števili n in m velja identifikacija med izrazoma $n + m$ in $m + n$, torej konstruirali element tipa

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

$\diamondsuit$

Definicija 2.9. 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 $a : A$ velja 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 lahko za vsak element $a : A$ tvorimo kanonično identifikacijo 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 $x, y : A$ lahko tvorimo funkcijo

$$\mathsf{sym} : (x = y) \to (y = x).$$

   Identifikacijo $\mathsf{sym}(p)$ imenujemo *inverz* identifikacije p in ga pogosto označimo z p^{-1}. Po principu eliminacije identifikacij zadošča, da za vsak $x : A$ definiramo $\mathsf{refl}_x^{-1} : x = x$, za kar podamo refl_x.

2. Velja *tranzitivnost*: za vsake elemente $x, y, z : A$ lahko tvorimo funkcijo

$$\mathsf{concat} : (x = y) \to ((y = z) \to (x = z)),$$

   imenovano *konkatenacija identifikacij*, $\mathsf{concat}(p, q)$ pa pogosto označimo z $p \cdot q$. Po principu eliminacije identifikacij zadošča, da za vsake $y, z : A$ in $q : y = z$ definiramo $\mathsf{refl}_y \cdot q$, za kar podamo q. Dokažemo lahko tudi, da velja identifikacija tipa $q \cdot \mathsf{refl}_z = q$.

3. Funkcije ohranjajo identifikacije: za vsaka elementa $x, y : A$ in vsako funkcijo $f : A \to B$ lahko tvorimo funkcijo

$$\mathsf{ap}_f : (x = y) \to (f(x) = f(y)),$$

   imenovano *aplikacija* funkcije f na identifikacije v A. Po principu eliminacije identifikacij zadošča, da za vsak $x : A$ definiramo $\mathsf{ap}_f\, \mathsf{refl}_x : f(x) = f(x)$, za kar podamo $\mathsf{refl}_{f(x)}$.

4. Družine tipov spoštujejo identifikacije: za vsaka elementa $x, y : A$ in družino tipov B nad A lahko tvorimo funkcijo

$$\mathsf{tr}_B : (x = y) \to B(x) \to B(y),$$

   imenovano *transport vzdolž identifikacij.* Po principu eliminacije identifikacij zadošča, da z vsak $x : A$ definiramo funkcijo $\mathsf{tr}_B(\mathsf{refl}_x) : B(x) \to B(x)$, za kar podamo id_B.

   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 $p : x = y$, sta tedaj tipa $P(x)$ in $P(y)$ logično ekvivalentna. Transport vzdolž identifikacije p nam da eno implikacijo, transport vzdolž njenega inverza pa drugo.

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 2.10. *Naj bosta $(x, y), (x', y') : \sum_{(x:A)} B(x)$. Identifikacije med (x, y) in (x', y') lahko tedaj karakteriziramo kot pare 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. Več o karakterizaciji identifikacij v odvisnih vsotah lahko poiščemo v [3, Poglavje II.9.3]

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.

3 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. Funkciji concat in sym, ki smo ju opisali v prejšnjem poglavju, nam ne podata samo logičnih pojmov tranzitivnosti in simetričnosti, temveč tudi homotopska pojma konkatenacije in inverza poti. Nadaljno nam funkcija ap za vsako funkcijo predstavlja določeno obliko zveznosti, saj zatrdi, da funkcije identifikacije vedno slikajo v identifikacije. Preko identifikacij lahko tako brez omembe odprtih množic ali zveznosti pridemo do mnogih rezultatov iz klasične homotopske teorije.

V tem delu se posvetimo predvsem 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.

3.1 Homotopije

Ekvivalenco tipov A in B definiramo kot funkcijo $f : A \to B$, ki je v primernem smislu obrnljiva, za to pa potrebujemo dobro karakterizacijo tipa identifikacij med funkcijami. V obravnavi obrnljivosti namreč potrebujemo 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 3.1. 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 3.2. 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 operacijo, s katero lahko homotopije z leve ali z desne razširimo s funkcijo.

Trditev 3.3. *Naj bosta A in B tipa in $f, g, h : A \to B$ funkcije. Denimo, da imamo homotopiji $H : f \sim g$ in $K : g \sim h$.*

Tedaj lahko konstruiramo 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 3.4. *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 imamo homotopijo $H : f \sim g$. Tedaj lahko konstruiramo 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 $\lambda x.H(h(x))$. □

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, velja 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 v primeru karakterizacije identifikacij v odvisnih vsotah bomo enakost med funkcijami prosto izmenjevali z homotopijo med funkcijami. Več o funkcijski ekstenzionalnosti lahko poiščemo v [3, Poglavje II.13]

Vredno je poudariti, da je bila karakterizacija enakosti v odvisnih vsotah *izrek* Martin-Löfove teorije tipov, karakterizacija enakosti v funkcijskih tipih preko funkcijske ekstenzionalnosti pa je *aksiom*, zato njena uporaba nosi nekoliko več teže. Ko bomo enakost nadomeščali s homotopijo, bomo zato to tudi izpostavili.

3.2 Obrnljivost in ekvivalenca

Opremljeni s homotopijami lahko sedaj dokaz obrnljivost funkcije $f : A \to B$ definiramo kot funkcijo $g : B \to A$, 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 3.5. Naj bo $f : A \to B$ funkcija. Pravimo, da je $g : B \to A$ *inverz* funkcije f, če veljata homotopiji tipov $f \circ g \sim \mathsf{id}$ in $g \circ f \sim \mathsf{id}$. *Tip inverzov funkcije* f predstavimo s tipom

$$\mathsf{inverse}(f) := \sum_{(g:B\to A)}(f \circ g \sim \mathsf{id}) \times (g \circ f \sim \mathsf{id}).$$

Če ima funkcija inverz, pravimo tudi, da je *obrnljiva*.

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

Definicija 3.6. Naj bo $f : A \to B$ funkcija. Pravimo, da je funkcija $g : B \to A$ *prerez* funkcije f, če velja homotopija tipa $f \circ g \sim \mathsf{id}$. *Tip prerezov funkcije* f predstavimo s tipom

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

Pravimo, da je funkcija $g : B \to A$ *retrakcija* funkcije f, če velja homotopija tipa $g \circ f \sim \mathsf{id}$. *Tip retrakcij funkcije* f predstavimo s tipom

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

Alternativa pojmu obrnljivosti je pojem *ekvivalence*. Pravimo, da je funkcija f ekvivalenca, če obstajata (potencialno različni) funkciji g in h, za kateri veljata homotopiji tipov $f \circ g \sim \mathsf{id}$ in $h \circ f \sim \mathsf{id}$. Z drugimi besedami, funkcija f ima tako prerez, kot retrakcijo.

Definicija 3.7. Pravimo, da je funkcija f *ekvivalenca*, če ima tako prerez kot retrakcijo, kar predstavimo s tipom

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

Pravimo, da je tip A *ekvivalenten* tipu B, če med njima obstaja ekvivalenca. Ekvivalenco tipov torej predstavimo s tipom $A \simeq B :\equiv \sum_{(f:A \to B)} \mathsf{is\text{-}equiv}(f)$.

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. Pokažemo, 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 sodbeno, lahko pa med njima konstruiramo homotopijo.

Kot spodaj za boljšo berljivost daljša zaporedja homotopij med funkcijami označimo s puščicami.

Trditev 3.8. *Funkcija je ekvivalenca natanko tedaj, ko je obrnljiva.*

Dokaz. Denimo, da je funkcija f obrnljiva. Tedaj je njen inverz tako njen prerez, kot njena retrakcija, 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:

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

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

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

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 dve družini tipov, $\mathsf{inverse}$ in $\mathsf{is\text{-}equiv}$, v prejšnji trditvi pa dokazali, da je tip $\mathsf{inverse}(f)$ naseljen natanko tedaj kot $\mathsf{inverse}(f)$. Vprašamo pa se lahko tudi nekoliko več: ali velja ekvivalenca tipov $\mathsf{inverse}(f) \simeq \mathsf{is\text{-}equiv}(f)$?

Drugače povedano smo v prejšnji trditvi konstruirali funkciji tipa $\mathsf{inverse}(f) \to \mathsf{is\text{-}equiv}(f)$ in obratno, ekvivalenca med tipoma $\mathsf{inverse}(f)$ in $\mathsf{is\text{-}equiv}(f)$ pa bi pomenila, da sta si ti funkciji med seboj tudi inverzni.

Nekoliko presenetljivo se izkaže, da taka ekvivalenca za vsak f ne more veljati, 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 $\mathsf{inverse}(f)$ pa je to odvisno od strukture tipov A in B. Nadaljno bomo pokazali, da ekvivalnce ohranjajo lastnost propozicije, torej da za tipa $A \simeq B$ velja, da tip A to lastnost izpolnjuje natanko tedaj kot tip B. Posledično ekvivalenca ne mora veljati za tiste funkcije f, za katere $\mathsf{inverse}(f)$ ni propozicija.

3.3 Kontraktibilnost in propozicije

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

Definicija 3.9. Naj bo A tip. Pravimo, da je A *kontraktibilen*, če obstaja element $c : A$, za katerega za vsak element $x : A$ velja identifikacija tipa $c = x$. Kontraktibilnost torej predstavimo s tipom

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

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

Če naivno preberemo definicijo, se na prvi pogled zdi, da smo s tem zajeli le pojem povezanosti s potmi, 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* en element, želimo s pojmom propozicije izraziti, da ima tip A *največ* en elemnt. Z drugimi besedami, poljubna elementa tipa A sta identificirana.

Definicija 3.10. Naj bo A tip. Pravimo, da je A *propozicija*, če za vsaka elementa $x, y : A$ velja identifikacija $x = y$. Propozicionalnost torej predstavimo s tipom

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

Opomba 3.11. Kot omenjeno želimo v interpretaciji *izjave kot tipi* izjave predstaviti s propozicijami. Če je namreč tip P propozicija, tedaj predpostavka $p : P$ resnično tvori predpostavko *izjave* P in ne izbire arbitrarnega elementa tipa P. Ker so vsi elementi tipa P identificirani, nadaljne konstrukcije pod predpostavko $p : P$ niso odvisne od izbire p.

Sedaj lahko tudi točneje definiramo pojem *predikata* P nad A, namreč kot družino tipov, vsak izmed katerih je propozicija. Ker za vsak $x : A$ tip $P(x)$ vsebuje največ en element, družina tipov P resnično predstavlja *lastnost* na tipu A. Drugače povedano, vsak $x : A$ lastnost $P(x)$ izpoljuje na največ en način. Z razliko od tega pravimo, da splošna družina tipov B nad A tvori *strukturo* na tipu A. Vsak element $x : A$ lahko strukturo $B(x)$ nosi na mnogo različnih načinov.

S to terminologijo želimo torej dokazati, da $\mathsf{is\text{-}equiv}$ tvori predikat na tipu $A \to B$, $\mathsf{inverse}$ pa strukturo. Funkcija je torej lahko ekvivalenca na največ en način, obrnljivost pa na njej lahko predstavlja dodatno strukturo. Ta struktura ne nosi nobenih bistvenih informacij, temveč je le biprodukt definicije, zato v homotopski teoriji tipov preferiramo pojem ekvivalence.

Da ima tip A največ eno točko lahko izrazimo tudi na drugačen način, namreč, da če tip A vsebuje element, da je ta tedaj tudi edini, torej, da je tip A tedaj kontraktibilen. Ti formulaciji sta tudi logično ekvivalentni, ob različnih priložnosti pa je katera od njiju lahko bolj prikladna.

Trditev 3.12. *Tip A je propozicija natanko tedaj, kot velja $A \to \mathsf{is\text{-}contr}(A)$.*

Dokaz. Denimo najprej, da je tip A propozicija. Konstruirati želimo funkcijo tipa $A \to \mathsf{is\text{-}contr}(A)$, zato denimo, da je $a : A$. Za središče kontrakcije tipa A lahko tedaj izberemo kar ta element, konstruirati pa moramo še kontrakcijo, torej funkcijo tipa $\prod_{(y:A)} a = y$. Ker je tip A propozicija, tako funkcijo tudi imamo, fiksirati moramo le eno od krajišč družine identifikacij $\prod_{(x,y:A)} x = y$.

Obratno denimo, da velja $A \to \mathsf{is\text{-}contr}(A)$. Dokazati moramo, da je sta tedaj poljubna elementa tipa A identificirana, zato denimo, da sta $x, y : A$. Kateri koli izmed njiju, recimo x, bi tedaj zadoščal, da dobimo kontraktibilnost tipa A. Posledično dobimo par identifikacij tipa $c = x$ in $c = y$ za neko središče kontrakcije $c : A$. Z inverzom in konkatenacijo ju lahko združimo v identifikacijo tipa $x = y$, kar zaključi dokaz. □

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

Trditev 3.13. *Naj bosta A in B ekvivalentna tipa. Tedaj je tip A propozicija natanko tedaj, kot tip B.*

Dokaz. Denimo, da je A propozicija. Dokazati želimo, da sta poljubna elementa tipa B identificirana, zato denimo, da sta $x, y : B$.

Ker sta tipa 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 x in y lahko torej s funkcijo g preslikamo v tip A, ker pa je ta propozicija, dobimo identifikaciji tipa $g(x) = g(y)$. To lahko z aplikacijo funkcije f preslikamo nazaj v tip B. Identifikacijo med x in y lahko tedaj dobimo preko konkatenacije

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

Obratno implikacijo dobimo povsem simetrično. □

Sedaj želimo pokazati, da je družina tipov $\mathsf{is\text{-}equiv}$ res predikat, za kar bomo uporabili alternativno formulacijo pojma propozicije. Pod predpostavko, da je funkcija f ekvivalenca moramo torej pokazati, 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, torej, 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 trdi1tve je zelo preprost, sloni pa na karakterizaciji tipa identifikacij v produktih.

Trditev 3.14. *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 $\lambda(x, y).(C_A(x), C_B(y))$. □

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

Trditev 3.15. *Naj bo f ekvivalenca med tipoma A in B. Tedaj je tip prerezov funkcije 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:

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

Kompozitum homotopij označimo z L in s funkcijsko ekstenzionalnostjo pretvorimo v identifikacijo, ki jo označimo z L'. S tem smo konstruirali identifikcijo na prvi komponenti, po karakterizaciji identifikacij v odvisnih vsotah pa 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:

$$f \circ g \xrightarrow[\sim]{fL^{-1}} f \circ s \xrightarrow[\sim]{H} \mathsf{id}.$$

2. Želeno 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 $rfL = Ks \cdot L \cdot K^{-1}g$. Ne nazadnje želeno identifikacijo preoblikujemo v

$$rfL \cdot Kg = Ks \cdot L.$$

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 tipa

$$hH \cdot Kg = Kf \cdot kH.$$

Homotopiji H in K lahko v homotopijo med funkcijama $h \circ f$ in $k \circ g$ združimo 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.

Želeno identifikacijo tedaj 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.

Diskusijo povzamemo v sledečem izreku:

Izrek 3.16. *Družina tipov* is-equiv *je predikat.*

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 is-equiv(f). Sledi, da je is-equiv(f) propozicija. □

3.4 Množice

Obrnimo se nazaj h tipu inverse(f). Omenili smo, da je propozicionalnost tega tipa lahko odvisna od strukture tipov A in B. Fiksirajmo torej funkcijo f in denimo, da je tip inverse(f) propozicija. Razmislili bomo, ali lahko iz tega izpeljemo kak pogoj na tipa A in B.

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

$$gf \xrightarrow[\sim]{gfK^{-1}} gfgf \xrightarrow[\sim]{gHf} gf \xrightarrow[\sim]{K} \mathsf{id}.$$

Ker je po predpostavki tip inverse(f) propozicija, 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 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 $Hf = fK$. Če povzamemo:

Trditev 3.17. *Naj bo $f : A \to B$ funkcija in denimo, da je njen tip inverzov propozicija. Tedaj za vsak inverz (g, H, K) velja identifikacija $Hf = fK$.*

Ker smo v strukturi inverza predpostavili obstoj dveh homotopij H in K, ki obe govorita o funkcijah f in g, sta nastali dve različni možnosti za homotopijo tipa $f \circ g \circ f \sim f$, Hf in fK, če pa bi bil tip inverse(f) propozicija, bi bili možnosti identificirani. Ali pa taka identifikacija nujno vedno velja? 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 lahko v tipu B med poljubnima točkama obstajala največ ena identifikacija, bi lahko pokazali, da lahko tedaj tudi med poljubnima funkcijama s kodomeno B obstaja največ ena homotopija. Take tipe imenujemo *množice*.

Definicija 3.18. Naj bo A tip. Pravimo, da je tip A *množica*, če za vsaka elementa $x, y : A$ velja, da je tip $x = y$ propozicija. Lasnost množice torej predstavimo s tipom

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

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

Trditev 3.19. *Naj bosta A in B tipa ter denimo, da je tip B množica. Tedaj velja*

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

Dokaz. Naj bosta f in g funkciji in denimo, da sta H in K homotopiji tipa $f \sim g$. 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 lahko 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 identifikaciji $H(x)$ in $K(x)$ identificirani. □

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 tipa $\mathsf{inverse}(f)$ in še več, za ekvivalenco med tipoma $\mathsf{is\text{-}equiv}(f)$ in $\mathsf{inverse}(f)$. Dokaz tega dejstva je podobno tehničen kot dokaz, da imajo ekvivalence kontraktibilen tip prerezov, zato ga bomo izpustili.

Opomba 3.20. Omenimo lahko, da je bila izbira tipa B kot tistega, za katerega smo izpeljali pogoj, arbitrarna, to pa sloni na dejstvu, da tudi za lastnost množice velja, da jo ekvivalence ohranjajo. Denimo namreč, da je tip A množica. Za dokaz propozicionalnosti $\mathsf{inverse}(f)$ bomo zopet uporabili alternativno formulacijo propozicij, zato denimo, da je tip funkcija f obrnljiva. Dokazati želimo, da je tedaj tip $\mathsf{inverse}(f)$ kontraktibilen. Ker je funkcija f obrnljiva, sta po trditi 3.8 tipa A in B tudi ekvivalentna, od koder sledi, da je tip B množica. Po prejšnji diskusiji je tedaj tip $\mathsf{inverse}(f)$ propozicija, ker pa je po predpostavki tudi naseljen, je kontraktibilen. Velja torej sledeča trditev:

Izrek 3.21. *Naj bo $f : A \to B$ funkcija in denimo, da je vsaj eden izmed tipov A in B množica. Tedaj je tip $\mathsf{inverse}(f)$ propozicija.*

Da bi poiskali funkcijo $f : A \to B$, katere tip inverzov ni propozicija, jo moramo torej poiskati med funkcijami, katerih domena in kodomena nista množici. Izkaže pa se, da je obstoj tipov, ki niso množice, od Martin-Löfove teorije tipov neodvisen.

Teorijo lahko zato razširimo na enega izmed dveh načinov: razširimo jo lahko z aksiomom UIP (ang. *Uniqueness of Identity Proofs*), ki v grobem zatrdi, da za vsak tip A in vsak element $a : A$ velja, da je tip $a = a$ kontraktibilen na element refl_a. Od tod posledično sledi tudi, da je vsak tip množica. Konsistenco aksioma UIP lahko preprosto pokažemo tako, da opazimo, da množice v Martin-Löfovi teoriji tipov tvorijo tudi njen interni model. Velja namreč, da vsi konstruktorji Martin-Löfove teorije tipov ohranjajo lastnost množice: funkcijski tip med množicama je množica, odvisna vsota družine množic nad množico je množica, ipd. Ker ta model validira aksiom UIP, to pokaže tudi njegovo konsistenco.

Alternativno lahko za razvoj sintetične homotopske teorije predpostavimo obstoj različnih tipov, imenovanih *višji induktivni tipi*, ki poleg običajnih konstruktorjev za elemente vsebujejo tudi konstruktorje za identifikacije, in *aksiom univalence*, več o katerem bomo povedali spodaj. V tem delu predstavimo enega najpreprostejših primerov višjih induktivnih tipov, *krožnico* $\mathbb{S}^1$, in pokažemo, da za identitetno funkcijo $\mathsf{id}_{\mathbb{S}^1}$ velja, da $\mathsf{inverse}(\mathsf{id}_{\mathbb{S}^1})$ *ni* propozicija, to pa tudi ključno sloni na aksiomu univalence.

3.5 Svetovi in aksiom univalence

Aksiom univalence je za homotopsko teorijo tipov zelo pomemben, v tem delu pa ga nekajkrat tudi ključno potrebujemo. Da bi lahko govorili o univalenci, pa moramo najprej spregovoriti o *svetovih*.

V grobem so svetovi tipi, katerih elementi so drugi tipi. Natančneje pravimo, da je tip $\mathcal{U}$ svet, če iz sodbe $A : \mathcal{U}$ lahko sklepamo, da velja sodba A type. Formalno gledano elementi $\mathcal{U}$ sicer niso tipi kot taki, vendar kode, katerim enolično ustrezajo tipi. V to sem v tem delu ne bomo spuščali, več o svetovih pa lahko preberemo v [3, Poglavje I.6].

Kot tipi imajo svetovi $\mathcal{U}$ tudi pripadajoči tip identifikacij. Za vsaka tipa A in B v svetu $\mathcal{U}$ imamo torej tip identifikacij $A = B$, aksiom univalence pa ta tip identifikacij karakterizira. V grobem namreč pove, da če sta tipa A in B ekvivalentna, da sta tedaj tudi identificirana. Bolj natančno:

Definicija 3.22. Za vsaka tipa A in B lahko konstruiramo funkcijo

$$\mathsf{id\text{-}to\text{-}equiv} : A = B \to A \simeq B.$$

Po principu eliminacije identifikacij namreč zadošča, da podamo ekvivalenco tipa $A \simeq A$, za kar lahko podamo identiteto id_A.

Aksiom univalence zatrdi, da je funkcija $\mathsf{id\text{-}to\text{-}equiv}$ ekvivalenca.

Aksiom univalence je nekompatibilen z aksiomom UIP, saj zatrdi, da svetovi niso množice. Med tipi lahko namreč obstaja mnogo različnih ekvivalenc, to pa preko univalence pomeni, da med njimi lahko obstaja tudi monogo različnih identifikacij.

Z univalenco med drugim tudi internaliziramo matematično prakso identifikacije in prostega izmenjevanja izomorfnih objektov. Če je namreč P predikat na svetu $\mathcal{U}$ ter A in B ekvivalentna tipa, lahko z uporabo univalence in transporta pokažemo, da $P(A)$ velja natanko tedaj kot $P(B)$. Za predikat $\mathsf{is\text{-}prop}$ smo to lahko pokazali na roke, univalenca pa nam pove, da to lahko uniformno storimo za *vse* predikate.

3.6 Krožnica $\mathbb{S}^1$

Krožnico $\mathbb{S}^1$ v homotopski teoriji tipov definiramo kot tip z enim elementom base in identifikacijo $\mathsf{loop} : \mathsf{base} = \mathsf{base}$, zanjo pa predpostavimo še določen indukcijski princip, ki zagotovi, da je krožnica med tipi A, opremljenimi z odlikovano točko $a : A$ ter odlikovano identifikacijo tipa $a = a$, v določenem smislu univerzalna. V homotopski teoriji krožnice pogosto ne obravnavamo kot množico točk v ravnini, temveč jo bolj abstraktno predstavimo kot CW kompleks z eno točko in eno zanko. Krožnico v homotopski teoriji tipov aksiomatiziramo na analogen način.

Da bi lahko formulirali pravila sklepanja za krožnico, najprej potrebujemo lemo, v kateri konstruiramo aplikacijo *odvisnih* funkcij na identifikacije.

Lema 3.23. *Naj bo $f : \prod_{(x:A)} B(x)$, $x, y : A$ in $p : x = y$. Tedaj velja identifikacija*

$$\mathsf{apd}_f(p) : \mathsf{tr}_B(p, f(x)) = f(y).$$

Dokaz. Po principu eliminacije identifikacij zadošča, da definiramo

$$\mathsf{apd}_f(\mathsf{refl}_x) : \mathsf{tr}_B(\mathsf{refl}_x, f(x)) = f(x),$$

ker pa je transport vzdolž refl_x enak identiteti, lahko podamo $\mathsf{refl}_{f(x)}$. □

Definicija 3.24. *Krožnica* $\mathbb{S}^1$ je podana s sledečimi pravili sklepanja:

1. Krožnica ima točko $\mathsf{base} : \mathbb{S}^1$.
2. V krožnici velja identifikacija $\mathsf{loop} : \mathsf{base} = \mathsf{base}$.
3. Za krožnico velja sledeči princip indukcije. Naj bo B družina tipov nad $\mathbb{S}^1$ in denimo, da imamo element $u : B(\mathsf{base})$ ter identifikacijo $p : \mathsf{tr}_B(\mathsf{loop}, u) = u$. Tedaj velja
$$\mathsf{ind}_{\mathbb{S}^1}(u, p) : \textstyle\prod_{(x:\mathbb{S}^1)} B(x).$$
4. Velja sodbena enakost $\mathsf{ind}_{\mathbb{S}^1}(u, p)(\mathsf{base}) \doteq u$.
5. Velja določena sodbena enakost $\mathsf{apd}_{\mathsf{ind}_{\mathbb{S}^1}(u,p)}(\mathsf{loop}) \doteq p$.

Če v tretjem pravilu sklepanja družino tipov B nadomestimo s tipom B, neodvsnim od $\mathbb{S}^1$, se pravilo sklepanja poenostavi v trditev, da za konstrukcijo funkcije tipa $f : \mathbb{S}^1 \to B$ zadošča, da podamo element $u : B$ in identifikacijo $p : u = u$. Zadošča torej, da smo v tipu B prepoznali instanco krožnice: bazno točko ter identifikacijo na njej. Zadnje pravilo sklepanja tedaj zatrdi, da velja sodbena enakost $\mathsf{ap}_f\, p \doteq \mathsf{loop}$.

Opomba 3.25. Kljub indukcijskemu pravilu za krožnico brez univalence ne moramo dokazati, da ni množica. Krožnico lahko v internem modelu množic namreč interpretiramo kot tip z enim elementom $*$, zanko loop pa interpretiramo kot refl_*. Dejstva, da je krožnica množica torej ne moremo ovreči, saj v internem modelu množic velja.

Z razliko od tega lahko z univalenco pokažemo, da se elementa v $\mathsf{refl}_{\mathsf{base}}$ in loop razlikujeta. Dokažemo lahko namreč, da je tip $\mathsf{base} = \mathsf{base}$ ekvivalenten tipu celih števil $\mathbb{Z}$, kjer se $\mathsf{refl}_{\mathsf{base}}$ slika v element 0 in loop v element 1. Ker se elementa 0 in 1 razlikujeta, se posledično razlikujeta tudi elementa $\mathsf{refl}_{\mathsf{base}}$ in loop. Konstrukcija ekvivalence je ključno odvisna od univalence, poiščemo pa jo lahko v [3, Poglavje III.22.4]. Dokaz, da se elementa 0 in 1 razlikujeta je z razliko od tega elementaren, sloni pa na karakterizaciji identifikacij v tipu $\mathbb{Z}$. Analogno karakterizacijo identifikacij v tipu naravnih števil $\mathbb{N}$ lahko poiščemo v [3, Poglavje II.11.33].

Osredotočimo se sedaj na obrnljivost funkcije $\mathsf{id}_{\mathbb{S}^1} : \mathbb{S}^1 \to \mathbb{S}^1$. Za njen inverz lahko podamo kar funkcijo $\mathsf{id}_{\mathbb{S}^1}$, podati pa moramo še dve homotopiji tipa $\mathsf{id}_{\mathbb{S}^1} \circ \mathsf{id}_{\mathbb{S}^1} \sim \mathsf{id}_{\mathbb{S}^1}$, torej dve funkciji tipa $\prod_{(x:\mathbb{S}^1)} x = x$. Prvo homotopijo, imenujmo jo H, definiramo kot konstantno homotopijo $\lambda x.\mathsf{refl}_x$. V sledečem bomo konstruirali še homotopijo K, ki v določenem smislu za vsako točko x poda identifikacijo med x in x, ki enkrat zaokroži okoli krožnice. V posebnem velja $K(\mathsf{base}) \doteq \mathsf{loop}$.

Če bi bil tip $\mathsf{inverse}(\mathsf{id}_{\mathbb{S}^1})$ propozicija, bi bili homotopiji H in K tedaj skladni in veljala bi identifikacija $H\mathsf{id}_{\mathbb{S}^1} = \mathsf{id}_{\mathbb{S}^1}K$, kar pa lahko nadaljno poenostavimo v identifikacijo tipa $H = K$. Posledično bi veljalo $H \sim K$, torej bi veljala tudi identifikacija

$$\mathsf{refl}_{\mathsf{base}} \doteq H(\mathsf{base}) = K(\mathsf{base}) \doteq \mathsf{loop},$$

kar pa je protislovje.

Preostane nam, da konstruiramo omenjeno homotopijo K, za to pa najprej potrebujemo določeno lemo:

Lema 3.26. *Naj bo A tip in $x, y : A$. Denimo, da imamo identifikacije $p : x = y$, $q : x = x$ in $r : y = y$, za katere velja identifikacija $q \cdot p = p \cdot r$. Tedaj velja identifikacija $\mathsf{tr}_{\lambda a.a=a}(p, q) = r$.*

Dokaz. Prepričajmo se najprej, da je lema smiselna. Transport vzdolž identifikacije p se dogaja znotraj družine tipov $a = a$, indeksirane z elementi $a : A$. Identifikaciji q in r sta torej elementa tipov te družine pri elementih x in y.

Po principu eliminacije identifikacij zadošča pokazati, da lema velja za $p \doteq \mathsf{refl}_x$. Ker je refl enota za konkatenacijo, se predpostavka poenostavi v identifikacijo $q = r$, ker pa je transport vzdolž refl identiteta, se v $q = r$ poenostavi tudi željena identifikacija, kar zaključi dokaz. $\square$

Sedaj lahko konstruiramo želeno homotopijo K. Po indukcijskem principu za krožnico velja, da za konstrukcijo funkcije $\prod_{(x:\mathbb{S}^1)} x = x$ zadošča, da podamo element $u : \mathsf{base} = \mathsf{base}$ ter identifikacijo $\mathsf{tr}_{\lambda x.x=x}(\mathsf{loop}, u) = u$. Veljala bo tudi sodbena enakost $K(\mathsf{base}) \doteq u$. Podamo lahko $\mathsf{loop} : \mathsf{base} = \mathsf{base}$, ker pa očitno velja identifikacija $\mathsf{loop} \cdot \mathsf{loop} = \mathsf{loop} \cdot \mathsf{loop}$, tedaj po prejšnji lemi sledi, da velja tudi želena identifikacija $\mathsf{tr}_{\lambda x.x=x}(\mathsf{loop}, \mathsf{loop}) = \mathsf{loop}$. Kot želeno velja $K(\mathsf{base}) = \mathsf{loop}$. Diskusijo povzemimo v sledeči trditvi.

Trditev 3.27. *Tip inverzov funkcije $\mathsf{id}_{\mathbb{S}^1} : \mathbb{S}^1 \to \mathbb{S}^1$ ni propozicija.*

Dokaz. Denimo, da je tip inverzov funkcije $\mathsf{id}_{\mathbb{S}^1}$ propozicija. Ker imamo identifikacijo $\mathsf{refl} : \mathsf{loop} \cdot \mathsf{loop} = \mathsf{loop} \cdot \mathsf{loop}$, imamo po lemi 3.26 tudi identifikacijo $p : \mathsf{tr}(\mathsf{loop}, \mathsf{loop}) = \mathsf{loop}$. Trojica $(\mathsf{id}_{\mathbb{S}^1}, \lambda x.\mathsf{refl}_x, \mathsf{ind}_{\mathbb{S}^1}(\mathsf{loop}, p))$ je tedaj inverz funkcije $\mathsf{id}_{\mathbb{S}^1}$, ker pa je $\mathsf{inverse}(\mathsf{id}_{\mathbb{S}^1})$ propozicija, po trditvi 3.17 sledi, da imamo identifikacijo med homotopijama $\lambda x.\mathsf{refl}_x$ in $\mathsf{ind}_{\mathbb{S}^1}(\mathsf{loop}, p)$. Če homotopiji evaluiramo pri elementu base, dobimo identifikacijo med identifikacijama $\mathsf{refl}_{\mathsf{base}}$ in loop, kar pa je v protislovju z univalenco. $\square$

Za konec tega poglavja imamo sledeči izrek:

Izrek 3.28. *Obstaja funkcija f, za katero tipa $\mathsf{is\text{-}equiv}(f)$ in $\mathsf{inverse}(f)$ nista ekvivalentna.*

Dokaz. Po izreku 3.16 je tip $\mathsf{is\text{-}equiv}(\mathsf{id}_{\mathbb{S}^1})$ propozicija, tip $\mathsf{inverse}(\mathsf{id}_{\mathbb{S}^1})$ pa po trditvi 3.27 ni. Ker po trditvi 3.13 ekvivalence ohranjajo lastnost propozicij, tipa nista ekvivalentna. $\square$

Še enkrat poudarimo, da razlika med pojmoma ekvivalence in obrnljivosti leži izključno v višji strukturi identifikacij in homotopij. V strukturi ekvivalence sta homotopiji prereza in retrakcije druga od druge ločeni, zato tip ostane propozicija ne glede na strukturo tipov A in B. Kot pa smo videli, sta homotopiji v strukturi inverza med seboj prepleteni, zato se tip inverzov navzame višje strukture identifikacij, ki je lahko prisotna v tipih A in B.

V tem poglavju smo na protiprimeru *ene* funkcije predstavili razliko med pojmom obrnljivosti in pojmom ekvivalence, v sledečem poglavju pa se bomo bolj kvalitativno poglobili v povezavo med tipom *vseh* obrnljivih funkcij in tipom *vseh* ekvivalenc med tipoma A in B.

4 Karakterizacija obrnljivosti

Karakterizacije tipa $\mathsf{inverse}(f)$ za povsem arbitrano funkcijo f nimamo, fiksiramo pa lahko tipa A in B in poskusimo karakterizirati tip vseh obrnljivih funkcij med njima. Tip ekvivalenc med tipoma A in B smo že označili z $A \simeq B$, označimo pa sedaj še tip obrnljivih funkcij:

$$\mathsf{inv\text{-}map}(A, B) :\equiv \textstyle\sum_{(f:A\to B)} \mathsf{inverse}(f).$$

Raziskali bomo torej povezavo med tipoma $A \simeq B$ in $\mathsf{inv\text{-}map}(A, B)$, najprej pa potrebujemo še nekaj pomožnih rezultatov.

4.1 Pomožni rezultati

V tem razdelku predstavimo nekaj rezultatov iz homotopske teorije tipov, ki jih bomo v konstrukciji potrebovali. Ti so zelo standardni, zato se v njihovo motivacijo ne bomo poglabljali.

Delali bomo s funkcijami in ekvivalencami med odvisnimi vsotami, zato najprej povejmo nekaj o družinah funkcij. V tem razdelku fiksirajmo tip A ter B in C družini tipov nad A.

Definicija 4.1. Naj bo $F : \prod_{(x:A)} (B(x) \to C(x))$ družina funkcij. Definiramo funkcijo $\mathsf{tot}(F) : \sum_{(x:A)} B(x) \to \sum_{(x:A)} C(x)$ s predpisom $\mathsf{tot}(F)(x, y) = (x, F(x)(y))$.

Trditev 4.2. *Naj bo $F : \prod_{(x:A)} (B(x) \to C(x))$ družina funkcij in denimo, da je za vsak $x : A$ funkcija $F(x)$ ekvivalenca. Tedaj je ekvivalenca tudi funkcija $\mathsf{tot}(F)$.*

Dokaz. Ker je za vsak $x : A$ funkcija $F(x)$ ekvivalenca, imamo tudi družino njihovih prerezov $S(x) : C(x) \to B(x)$. Trdimo, da je tedaj $\mathsf{tot}(S)$ prerez funkcije $\mathsf{tot}(F)$, saj za vsak $(x, y) : \sum_{(x:A)} C(x)$ 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 konstruiramo tudi retrakcijo funkcije $\mathsf{tot}(F)$, kar zaključi dokaz. $\square$

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

Posledica 4.3. *Denimo, da za vsak $x : A$ velja $B(x) \simeq C(x)$. Tedaj velja tudi $\sum_{(x:A)} B(x) \simeq \sum_{(x:A)} C(x)$.*

Naslednja preprosta trditev, ki jo bomo nekajkrat potrebovali, je tako imenovana asociativnost odvisnih vsot.

Trditev 4.4. *Naj bo A tip, B družina tipov, indeksirana z A in C družina tipov, indeksirana z $x : A$ in $B(x)$. Tedaj velja ekvivalenca:*

$$\sum_{(x:A)} \sum_{(y:B(x))} C(x, y) \simeq \sum_{\left(t:\, \sum_{(x:A)} B(x)\right)} C(t).$$

Dokaz. Za funkciji podamo $\lambda(x, (y, z)).((x, y), z)$ in obratno. Ti sta očitno inverzni, zato ekvivalenca velja. $\square$

Na kratko spregovorimo o podtipih. Naj bo A tip in P predikat na A. Tip $\sum_{(x:A)} P(x)$ tedaj imenujemo *podtip* elementov tipa A, ki izpolnjujejo predikat P. Za vsak $x : A$ namreč do identifikacije natanko obstaja največ en element $P(x)$, zato se tudi x v odvisni vsoti pojavi največ enkrat.

S to terminologijo je torej tip $A \simeq B$ podtip tipa $A \to B$, tip $\mathsf{inv\text{-}map}(A, B)$ pa lahko na tipu $A \to B$ predstavlja dodatno strukturo.

Za podtipe velja sledeča trditev:

Trditev 4.5. *Naj bo A tip, P predikat na A, B pa družina tipov nad A. Denimo, da obstaja družina funkcij tipa $\prod_{(x:A)}(B(x) \to P(x))$. Tedaj velja ekvivalenca*

$$\sum_{(x:A)} Bx \simeq \sum_{\left(t:\, \sum_{(x:A)} P(x)\right)} B(\mathsf{pr}_1 t).$$

Trditev lahko interpretiramo na sledeč način. Predpostavka nam pove, da če za element $x : A$ obstaja elment tipa $B(x)$, da tedaj x tudi izpolnjuje predikat P. Za konstrukcijo odvisne vsote družine B nad A tedaj zadošča, da se omejimo na konstrukcijo odvisne vsote nad podtipom elementov A, ki zadoščajo predikatu P.

Dokaz. Po asociativnosti odvisnih vsot je desna stran ekvivalence ekvivalentna tipu $\sum_{(x:A)} \sum_{(p:P(x))} B(x) \doteq \sum_{(x:A)}(P(x) \times B(x))$. Po posledici 4.3 torej zadošča pokazati, da za vsak $x : A$ velja ekvivalenca $B(x) \simeq P(x) \times B(x)$.

Naj bo torej $a : A$. Med tipoma konstruirajmo inverzni funkciji. Po predpostavki imamo družino funkcij

$$s : \prod_{(x:A)}(B(x) \to P(x)).$$

Funkcijo $f : B(a) \to P(a) \times B(a)$ lahko tedaj definiramo kot

$$\lambda\, y.\, (s(a,y),\, y)\,,$$

za funkcijo $g : P(a) \times B(a) \to B(a)$ pa vzemimo kar drugo projekcijo.

Za vsak $y : B(a)$ očitno velja sodbena enakost $g(f(y)) \doteq y$. Naj bo sedaj $(p, y) : P(a) \times B(a)$. Ker je P predikat, velja identifikacija $s(a, y) = p$, zato pa velja tudi identifikacija

$$f(g\,(p,y)) \doteq (s(x,y),y) = (p,y)\,.$$

Funkciji f in g sta torej inverzni, zato ekvivalenca velja. □

Brez dokaza predstavimo še sledečo trditev, ki pove, da se tip identifikacij v tipu $\sum_{(x:A)} P(x)$ sklada s tipom identifikacij v tipu A. Bolj natančno:

Trditev 4.6. *Naj bo A tip, P predikat na A in $s, t : \sum_{(x:A)} P(x)$. Tedaj je tip $s = t$ ekvivalenten tipu $\mathsf{pr}_1(s) = \mathsf{pr}_1(t)$.*

Z aplikacijo funkcije pr_1 lahko za vsako identifikacijo tipa $s = t$ dobimo tudi identifikacijo tipa $\mathsf{pr}_1(s) = \mathsf{pr}_1(t)$, trditev pa nam pove, da lahko v primeru podtipov konstruiramo tudi enoličen dvig v nasprotno smer. Trditev bi najlažje dokazali s tako imenovanim osnovnim izrekom o tipih identifikacij, vendar le tega v tem delu nismo razvili. Dokaz trditve in več o podtipih lahko poiščemo v [3, Poglavje II.12.2].

Naslednj trditev spregovori o povezavi med kontraktibilnostjo in odvisnimi vsotami.

Trditev 4.7. *Naj bo A tip, B družina tipov nad A in denimo, da je tip A kontraktibilen s središčem kontrakcije $c : A$. Tedaj je tip $\sum_{(x:A)} B(x)$ ekvivalenten tipu $B(c)$.*

Dokaz. Med tipoma konstruiramo inverzni funkciji.

Funkcijo $f : B(c) \to \sum_{(x:A)} B(x)$ definiramo kot $\lambda y.(c, y)$. Ker je tip A kontraktibilen, imamo kontrakcijo $C : \prod_{(x:A)} c = x$. Funkcijo $g : \sum_{(x:A)} B(x) \to B(c)$ lahko torej definiramo kot

$$\lambda(x,y).\mathsf{tr}_B(C(x)^{-1}, y).$$

$C(x)$ je namreč identifikacija tipa $c = x$, zato lahko element $y : B(x)$ transportiramo v tip $B(c)$ vzdolž inverzne identifikacije $C(x)^{-1}$.

Brez škode za splošnost lahko poskrbimo, da je $C(c) \doteq \mathsf{refl}_c$. Sledi, da velja sodbena enakost $g(f(y)) \doteq \mathsf{tr}_B(C(c)^{-1}, y) \doteq \mathsf{tr}_B(\mathsf{refl}_c^{-1}, y)$, ker pa je inverz identifikacije refl enak refl in transport vzdolž identifikacije refl enak identiteti, je $g(f(y)) = y$ za vsak $y : B(c)$.

Obratno velja sodbena enakost $f(g(x,y)) \doteq (c, \mathsf{tr}_B(C(x)^{-1}, y))$. Po karakterizaciji identifikacij v odvisnih vsotah za konstrukcijo identifikacije tipa

$$(x,y) = (c, \mathsf{tr}_B(C(x)^{-1}, y))$$

zadošča, da podamo identifikaciji $p : x = c$ in $\mathsf{tr}_B(p, y) = \mathsf{tr}_B(C(x)^{-1}, y)$. Podamo lahko $C(x)^{-1}$ in $\mathsf{refl}_{\mathsf{tr}_B(C(x)^{-1},y)}$. □

Trditev nam pove, da lahko v konstrukciji ekvivalenc kontraktibilne tipe v odvisnih vsotah v določenem smislu krajšamo.

Nazadnje imamo še trditev, ki spregovori o odvisni vsoti *vseh* tipov identifikacij v danem tipu.

Trditev 4.8. *Naj bo A tip in $a : A$. Tedaj je tip $\sum_{(x:A)} a = x$ kontraktibilen.*

Dokaz. Za središče kontrakcije izberemo element (a, refl_a). Dokazati moramo, da imamo tedaj za vsaka $x : A$ in $p : a = x$ identifikacijo tipa

$$(a, \mathsf{refl}_a) = (x, p).$$

Po principu eliminacije identifikacij zadošča, da podamo identifikacijo tipa

$$(a, \mathsf{refl}_a) = (a, \mathsf{refl}_a),$$

za kar lahko podamo $\mathsf{refl}_{(a,\mathsf{refl}_a)}$. □

Poudarimo, da je za posamezna elementa $a, x : A$ tip $a = x$ pogosto daleč od kontraktibilnosti. Trditev pove nekaj veliko šibkejšega, namreč, da je kontraktibilen totalni prostor vseh tipov $a = x$.

4.2 Konstrukcija

Sedaj lahko predstavimo karakterizacijo tipa obrnljivih funkcij med tipoma A in B. V prvi trditvi fiksiramo tipa A in B ter pokažemo povezavo med tipom obrnljivih funkcij in tipom ekvivalenc med njima, za tem pa trditev uporabimo za to, da pokažemo povezavo med tipom *vseh* obrnljivih funkcij v danem svetu $\mathcal{U}$ in višjim induktivnim tipom *sfere* $\mathbb{S}^2$.

Trditev 4.9. *Tip obrnljivih funkcij med A in B je ekvivalenten tipu $\sum_{(e:A\simeq B)} e = e$.*

Za boljšo berljivost vpeljemo sledeče oznake: Naj bo $e : A \simeq B$. Tedaj z $\mathsf{map}(e)$ označimo funkcijo, pripadajočo elementu e, z $\mathsf{sec}(e)$ pa prerez funkcije $\mathsf{map}(e)$. Naj bo še $\mathcal{I} : \mathsf{inverse}(f)$ za neko funkcijo f. Tedaj z $\mathsf{map}(\mathcal{I})$ označimo inverz funkcije f. Oznaki map sta pravzaprav samo preimenovanji prve projekcije, sec pa je okrajšava za $\mathsf{pr}_1 \circ \mathsf{pr}_2$.

Dokaz. Konstruirati želimo ekvivalenco tipa

$$\textstyle\sum_{(f:A\to B)} \mathsf{inverse}(f) \simeq \sum_{(e:A\simeq B)}(e = e).$$

Ker je po trditvi 3.16 $\mathsf{is\text{-}equiv}$ predikat na tipu $A \to B$ in ker po trditvi 3.8 vsaka funkcija f porodi funkcija tipa $\mathsf{is\text{-}invertible}(f) \to \mathsf{is\text{-}equiv}(f)$, najprej opazimo, da po trditvi 4.5 velja ekvivalenca

$$\textstyle\sum_{(f:A\to B)} \mathsf{inverse}(f) \simeq \sum_{(e:A\simeq B)} \mathsf{inverse}(\mathsf{map}(e)).$$

Po posledici 4.3 torej zadošča, da za vsak element $e : A \simeq B$ konstruiramo ekvivalenco tipa

$$\mathsf{inverse}(\mathsf{map}(e)) \simeq (e = e).$$

Oglejmo si tip

$$\mathsf{inverse}(\mathsf{map}(e)) \doteq \sum_{(g:B\to A)}(\mathsf{map}(e)\circ g \sim \mathsf{id}) \times (g\circ \mathsf{map}(e) \sim \mathsf{id}).$$

Po asociativnosti odvisnih vsot je ta ekvivalenten tipu

$$\sum_{\left(\mathcal{I}:\, \sum_{(g:B\to A)} \mathsf{map}(e)\circ g\sim \mathsf{id}\right)}(\mathsf{map}(\mathcal{I})\circ \mathsf{map}(e)\sim \mathsf{id}),$$

ta pa je po definiciji tipa prerezov sodbeno enak tipu

$$\sum_{(\mathcal{I}:\mathsf{sec}(\mathsf{map}(e)))}(\mathsf{map}(\mathcal{I})\circ \mathsf{map}(e)\sim \mathsf{id}).$$

Po trditvi 3.15 ima ekvivalenca $\mathsf{map}(e)$ kontraktibilen tip prerezov s središčem kontrakcije pri funkciji $\mathsf{sec}(e)$, svojem prerezu. Po trditvi 4.7 torej sledi, da ga v odvisni vsoti lahko krajšamo, torej, da velja ekvivalenca

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

Sledi, da velja ekvivalenca $\mathsf{inverse}(\mathsf{map}(e)) \simeq (\mathsf{sec}(e)\circ \mathsf{map}(e)\sim \mathsf{id})$. Tip inverzov ekvivalence $\mathsf{map}(e)$ je torej ekvivalenten tipu dokazov, da je prerez funkcije $\mathsf{map}(e)$ hkrati tudi njena retrakcija.

Dokazati moramo še, da velja ekvivalenca med tipoma $\mathsf{sec}(e)\circ \mathsf{map}(e)\sim \mathsf{id}$ in $e = e$. V prejšnjem poglavju smo že uporabili dejstvo, da so ekvivalence levo krajšljive, sedaj pa ga zopet uporabimo v še bolj točnem smislu, namreč, da sta tipa $\mathsf{sec}(e)\circ\mathsf{map}(e)\sim \mathsf{id}$ in $\mathsf{map}(e)\circ\mathsf{sec}(e)\circ\mathsf{map}(e)\sim \mathsf{map}(e)$ ekvivalentna. Ker je $\mathsf{sec}(e)$ prerez $\mathsf{map}(e)$, je drugi tip ekvivalenten tipu $\mathsf{map}(e)\sim\mathsf{map}(e)$, ta pa je po aksiomu funkcijske ekstenzionalnosti ekvivalenten tipu $\mathsf{map}(e) = \mathsf{map}(e)$. Po trditvi 4.6 je ta ekvivalenten tipu $e = e$. □

Da bi lahko formulirali zadnji izrek, predstavimo še višji induktivni tip *sfere* $\mathbb{S}^2$. Tako kot krožnica vsebuje točko base, namesto 1-dimenzionalne identifikacije $\mathsf{base} = \mathsf{base}$ pa vsebuje 2-dimenzionalno identifikacijo $\mathsf{refl}_{\mathsf{base}} = \mathsf{refl}_{\mathsf{base}}$. Njen indukcijski princip bomo predstavili le v nepopolni obliki neodvisne univerzalne lastnosti, saj ga potrebujemo le v tej splošnosti. Za njegovo formulacijo potrebujemo sledečo lemo:

Lema 4.10. *Naj bo $f : A\to B$ funkcija, $x, y : A$, $p, q : x = y$ in $r : p = q$. Tedaj velja identifikacija*

$$\mathsf{ap}^2_f\, r : \mathsf{ap}_f\, p = \mathsf{ap}_f\, q.$$

Dokaz. Po principu eliminacije identifikacije zadošča, da definiramo

$$\mathsf{ap}^2_f\, \mathsf{refl}_p : \mathsf{ap}_f\, p = \mathsf{ap}_f\, p,$$

za kar lahko podamo $\mathsf{refl}_{\mathsf{ap}_f\, p}$. □

Definicija 4.11. *Sfera* $\mathbb{S}^2$ je podana s sledečimi pravili sklepanja:

- Sfera ima element $\mathsf{base} : \mathbb{S}^2$.
- V sferi velja identifikacija $\mathsf{surf} : \mathsf{refl}_{\mathsf{base}} = \mathsf{base}$.

- Naj bo B tip. Tedaj lahko definiramo funkcijo tipa

  $$(\mathbb{S}^2 \to B) \to \sum_{(y:B)} (\mathsf{refl}_y = \mathsf{refl}_y)$$

  s predpisom $\lambda f.(f(\mathsf{base}), \mathsf{ap}^2_f\,\mathsf{surf})$. Element $\mathsf{ap}^2_f\,\mathsf{surf}$ je namreč identifikacija tipa $\mathsf{ap}_f\,\mathsf{refl}_{\mathsf{base}} = \mathsf{ap}_f\,\mathsf{refl}_{\mathsf{base}}$, ker pa je aplikacija funkcij na refl sodbeno enaka refl, je pravzaprav identifikacija tipa $\mathsf{refl}_{f(\mathsf{base})} = \mathsf{refl}_{f(\mathsf{base})}$.

  Univerzalna lastnost sfere zatrdi, da je ta funkcija ekvivalenca.

Več o sferi in tudi o krožnici lahko poiščemo v [5, Poglavje II.6.4].

Izrek 4.12. *Obrnljive funkcije so sfere v svetu. Natančneje, za vsak svet $\mathcal{U}$ velja ekvivalenca med tipom obrnljivih funkcij v svetu $\mathcal{U}$, torej tipom*

$$\sum_{(A,B:\mathcal{U})} \mathsf{inv\text{-}map}(A, B),$$

in funkcijskim tipom $\mathbb{S}^2 \to \mathcal{U}$.

Dokaz. Po trditvi 4.9 za vsaka $A, B : \mathcal{U}$ velja ekvivalenca med tipom $\mathsf{inv\text{-}map}(A, B)$ in tipom $\sum_{(e:A\simeq B)} e = e$, iz aksioma univalence pa nadaljno sledi, da je drugi tip ekvivalenten tipu $\sum_{(e:A=B)} e = e$. Imamo torej družino ekvivalenc, indeksirano z $B : \mathcal{U}$, zato po posledici 4.3 velja ekvivalenca

$$\sum_{(B:\mathcal{U})} \mathsf{inv\text{-}map}(A, B) \simeq \sum_{(B:\mathcal{U})} \sum_{(e:A=B)} e = e.$$

Po asociativnosti odvisnih vsot je desni tip ekvivalenten tipu

$$\sum_{(\mathcal{E}:\, \sum_{(B:\mathcal{U})} A = B)} \mathsf{pr}_2(\mathcal{E}) = \mathsf{pr}_2(\mathcal{E}),$$

ker pa je po trditvi 4.8 tip $\sum_{(B:\mathcal{U})} A = B$ kontraktibilen s središčem kontrakcije (A, refl_A), ga po trditvi 4.7 v odvisni vsoti krajšamo in nam ostane le

$$(\mathsf{pr}_2(A, \mathsf{refl}_A) = \mathsf{pr}_2(A, \mathsf{refl}_A)) \doteq (\mathsf{refl}_A = \mathsf{refl}_A).$$

Konstruirali smo torej družino ekvivalenc med tipi $\sum_{(B:\mathcal{U})} \mathsf{inv\text{-}map}(A, B)$ in tipi $\mathsf{refl}_A = \mathsf{refl}_A$, indeksirano z $A : \mathcal{U}$. Po posledici 4.3 sledi, da velja tudi ekvivalenca

$$\sum_{(A,B:\mathcal{U})} \mathsf{inv\text{-}map}(A, B) \simeq \sum_{(A:\mathcal{U})} (\mathsf{refl}_A = \mathsf{refl}_A),$$

po univerzalni lastnosti sfere pa je desni tip ekvivalenten tipu $\mathbb{S}^2 \to \mathcal{U}$. □

Slovar strokovnih izrazov

type tip
judgment sodba
rule of inference pravilo sklepanja
judgmental equality sodbena enakost
function type funkcijski tip
dependent type odvisen tip

type family družina tipov
dependent product odvisni produkt
dependent function odvisna funkcija
dependent sum odvisna vsota
induction principle princip indukcije
identity type tip identifikacij
identification elimination, path induction eliminacija identifikacij
homotopy homotopija
function extensionality funkcijska ekstenzionalnost
section prerez
retraction retrakcija
mere proposition, h-proposition propozicija
contractible kontraktibilen
h-set množica
higher inductive type višji induktivni tip
subtype podtip
universe svet
univalence univalenca

Literatura

[1] T. 1Lab Development Team, *The 1Lab*, 2024, dostopno na https://1lab.dev.

[2] T. Najdovski, dostopno na https://github.com/maybemabeline/invertible-maps-are-spheres-in-the-universe/blob/master/IsoSpheres/IsoSpheres.lagda.md.

[3] E. Rijke, *Introduction to Homotopy Type Theory*, 2022, arXiv: 2212.11082 [math.LO].

[4] P. Martin-Löf, *An intuitionistic theory of types: predicative part*, v: Logic Colloquium '73, Proceedings of the Logic Colloquium (ur. H. Rose in J. Shepherdson), Studies in Logic and the Foundations of Mathematics **80**, North-Holland, 1975, str. 73–118.

[5] T. Univalent Foundations Program, *Homotopy type theory: univalent foundations of mathematics*, https://homotopytypetheory.org/book, Institute for Advanced Study, 2013.

[6] V. Voevodsky, *The Origins and Motivations of Univalent Foundations*, 2014, dostopno na https://www.ias.edu/ideas/2014/voevodsky-origins.