

УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ



Андрија Д. Урошевић

ИНТУИЦИОНИСТИЧКА ТЕОРИЈА
ТИПОВА КАО УВОД У ХОМОТОПНУ
ТЕОРИЈУ ТИПОВА

мастер рад

Београд, 2024.

Ментор:

др Сана СТОЈАНОВИЋ-ЂУРЂЕВИЋ, доцент
Универзитет у Београду, Математички факултет

Чланови комисије:

проф. др Филип МАРИЋ, редовни професор
Универзитет у Београду, Математички факултет

др Иван ЧУКИЋ, доцент
Универзитет у Београду, Математички факултет

Датум одбране: 29. фебруар 2024.

*Породици, пријатељима, колеџама,
планети Земљи и Универзуму*

Наслов мастер рада: Интуиционистичка теорија типова као увод у хомотопну теорију типова

Резиме: Homotopy Type Theory/Univalent Foundations (HoTT/UF) is a revolutionary approach to the foundation of mathematics. Although it's revolutionary, HoTT/UF is very slowly gaining popularity among a broader circle of mathematicians and computer scientists. One of the reasons is that during formalization one requires both theoretical knowledge and proof-assistance skills. Acquiring those prerequisites is partially based on one's background. Mathematicians lack functional programming skills, on the other hand, computer scientists lack theoretical knowledge. A few materials tackle both areas, but they are lacking interactability. This thesis proposes a material that formalizes one theoretical area of HoTT/UF in Agda and is doing so while interacting with the user input.

Кључне речи: хомотопна теорија типова, интерактивно доказивање, агда

Садржај

1	Увод	2
1.1	Филозофија и историја	3
1.2	Мотивација и циљ рада	5
1.3	Друге формализације	6
2	Интуиционистичка теорија типова	8
2.1	Правила закључивања	9
2.2	Зависни типови	10
2.3	Типови зависних функција	11
2.4	Индуктивни типови	12
2.5	Искази као типови	20
2.6	Хијерархија универзума и универзум типови	22
2.7	Типови идентитета	23
3	AGDA	35
3.1	Основе језика AGDA	35
3.2	Резултат	38
4	Закључак	40
	Литература	42

Глава 1

Увод

Хомотопна теорија типова (ХоТТ) (енгл. *Homotopy Type Theory*) је нова област математике која повезује многе друге области. Ослања се на *хомотопну теорију* и *теорију типова*. Хомотопна теорија је област настала из алгебарске топологије и хомолошке алгебре, са идејама више теорије категорија, док теорија типова има корене у математичкој логици и теоријском рачунарству. Сматра се да ХоТТ представља алтернативно заснивање математике, поступком формализације уз помоћу интерактивних доказивача. Програм заснивања математике у ХоТТ се назива *унивалентно заснивање* (енгл. *Univalent Foundations*) [9].

Хомотопна теорија типова представља надоградњу *Мартин-Луф теорије типова* (МЛТТ) (енгл. *Martin-Löf Type Theory*) са *вишим индуктивним типовама* и *аксиомом унивалентности*. Виши индуктивни типови омогућавају логичко описивање основних простора и конструкција у хомотопној теорији (сфере, цилиндри, итд.). Са друге стране, аксиома унивалентности тврди да $(A = B) \simeq (A \simeq B)$, односно да је једнакост еквивалентна еквиваленцији.

Постоји пуно разлога за изучавање ХоТТ-а и заснивање математике кроз интерактивне доказиваче теорема, али један од главних је дао један од оснивача, Владимир Војводски (*Владимир Воеводский*), увидевши пропусте у туђим и својим радовима [vlad14]:

A technical argument by a trusted author, which is hard to check and looks similar to arguments known to be correct, is hardly ever checked in detail. (Владимир Војводски, 2014.)

1.1 Филозофија и историја

Теорију типова је оригинално представио Берtrand Расел [rus08] (*Bertrand Russell*), решавајући парадокс у заснивању математике тог времена. Након њега Алонзо Черч (*Alonzo Church*), развија *једно типизирани ламбда рачун* (ПТЛР) (енгл. *Simply Typed Lambda Calculus*) [crc40, crc41]. Николас де Брујн (*Nicolaas de Bruijn*) инспирисан ПТЛР-ом развија први аутоматски доказивач теорема АУТОМАТН [automath]. Теорију типова даље развија Пер Мартин-Луф (*Per Martin-Löf*) коју данас знамо као МЛТТ, или *интуиционистичка/конструктивистичка/зависна теорија типова* [pml75, pml82, pml84, pml98]. МЛТТ представља основу за друге теорије које је проширују и које имплементирају разни интерактивни доказивачи теорема: AGDA [agda], COQ [coq], EPIGRAM [epigram], IDRIS [idris], NUPRL [nuprl]. Инспирисани резултатом да теорија типова може да се интерпретира као ∞ -группоид [hs98], Владимир Војводски [vlad06], Стив Ауоди (*Steve Awodey*) и Мајкл Ворен (*Michael Warren*) [aw09] независно развијају ХоТТ.

МЛТТ, па самим тим и ХоТТ, се заснива на Брауверовом *интуиционистичком приступу* [brw] који тврди да се сва математика, укључујући и концепт доказа, изводи из концепта *конструкције* (рачуна/алгоритма/програма класификованог типом). Браувер је сматрао да је математичко резоновање људска активност и да је математика језик у коме се преносе математички концепти. Другим речима, способност извршавања алгоритма у сврху извођења менталне конструкције је фундаментално људска. Због тога, једини начин на кој субјекат може доћи до математичке истине је да доживи истинитост, тако што изведе корак-по-корак одговарајућу менталну конструкцију. Случно, једини начин да субјекат дође до математичке неистине је да даживу њену неистинитост, тако што схвати да извођење одговарајуће менталне конструкције није могуће. Интуиционистички приступ даље развијају Колмогоров (*Андрей Николаевич Колмогоров*) [kol32] и Хејтинг (*Arend Heyting*) [hey] формулисањем интуиционистичке логике.

Интуиционистички приступ глобално искључује *закон искључења шрећ* $P \vee \neg P$ [brw]. Разлог томе су *слаби контра-примери* (енгл. *weak counterexamples*). Пример једног слабог контра-примера је Голдбахова претпоставка: *Сваки непаран број већи од 2 се може представити у облику збира два проста*. Конструктивистички, не можемо конструисати доказ да је Голдбахова претпо-

ставка тачна, нити да је нетачна, а поред тога немамо ни процедуру одлучивања. Због тога, не можемо тврдити да је Голдбахова претпоставка тачна или нетачна. Општије, не можемо тврдити да важи закон искључења трећег. Приметимо да закон искључења трећег искључујемо само глобално, односно да уколико је за конструкцију неког доказа потребно искористити закон искључења трећег, довољно је навести га у претпоставкама тврђења. Тиме добијамо да теореме које не користе закон искључења трећег имају снажнији резултат (јер користе мањи скуп претпоставки), док задржавамо и резултат теорема за које је неопходно користити закон искључења трећег.

У сржи теорије типова је појам *типске расуђивања* (енгл. *type judgment*)

$$t : T$$

који читамо као *t је терм типа T* или *терм t настањује тип T* (енгл. *t inhabits T*). Термови и типови се узимају као примитивни појмови који се не дефинишу. По Брауверу, терм *t* представља начин на који спроводимо конструкцију *T*. На пример, уколико желимо да конструишемо терм типа *B* и ако имамо конструисане термове *a : A* и *f : A → B*, онда терм *f(a)* описује начин на који конструишемо терм типа *B*, односно *f(a) : B*. Често се у ХоТТ-у, за терм каже *тачка*, а за тип *простор*, па се тако за расуђивање *t : T* каже да тачка *t* *припада* простору *T*.

Термови и типови у теорији типова имају три интерпретације: (1) докази исказа (логичка интерпретација), (2) програми типова (програмерска интерпретација) и (3) пресликавања структура (категоричка интерпретација). На пример, расуђивање *f : A → B* се може сматрати као: (1) доказ импликације, (2) функција која за дати улаз типа *A* враћа излаз типа *B* и (3) морфизам из објеката *A* у објекат *B*. Ову доктрину је поставио Роберт Харпер (Robert Harper) и назвао ју је *рачунарски тринитаризам* (енгл. *computational trinitarianism*) [rob11]. Рачунарски тринитаризам подразумева да сваки концепт који се јавља у једној интерпретацији треба да има значење у друге два интерпретације.

Теорија типова се заснива на идеји о *доказној релевантности* (енгл. *proof relevance*) која тврди да су математичка тврђења, па и сами докази, грађани првог реда, што значи да се различити докази истог исказа могу међусобно поредити. Прецизније, ако су *p₀ : P* и *p₁ : P* докази исказа *P*, односно начини на који можемо конструисати тип *P*, тада се они могу поредити и у том

смислу су *релевантни*. Са друге стране, код *доказно ирелевантних* система битно је само постојање доказа.

Доказивање исказа представља конструисање програма одређеног типа (за детаље видети поглавље 2.5). У том смислу, логика представља област математике, која се бави конструкцијама које су докази. Штавише, по Брауверу, математика је област рачунарства, како су конструкције представљене рачуном/алгоритмом/програмом. Напоменимо да постоје и друге конструкције које нису докази (на пример, природни бројеви).

Још једна карактеристика МЛТТ-а, па самим тим и ХоТТ-а, је да користи *синтептички*, а не *аналитички* приступ. У синтетичком приступу, основни објекти су примитиве чије се особине и релације аксиоматизују, из којих се даље логички дедукују последице. У аналитичком приступу, основни објекти су конструисани од других објеката, а њихове особине и релације су дедуковане из математичког окружења у ком су дефинисани. Често се за пример синтетичног приступа узима Еуклидска геометрија (где су основни објекти тачка, права и раван), а за аналитички приступ Декартова/аналитичка геометрија (где се основни објекти конструишу помоћу скупова).

1.2 Мотивација и циљ рада

Формализација математике представља једну од примарних делатности математичара. Од самог настанка математике, математичари су покушавали да прецизно заснују математику уводећи прецизно дефинисан дедуктивни систем, као и аксиоме теорије које формализују. Један од првих сачуваних примера су Еуклидови Елементи [ее], који су, након Библије, највише проучавано, преписивано и штампано дело у људској историји. Елементи су представљали прво увођење аксиоматизације у област геометрије, накнадно су уочени одређени пропусти које су наредне аксиоматизације исправиле.

Стотинама година касније, многи велики математичари настоје да унапреде поступак формализације у смислу прецизнијег дефинисања дедуктивног система, а и самих метода/алата који се користе при формализацији. Вековима се уводе нови симболи, како би се резонување у мозгу одвило механички, једноставним погледом. Почетком двадесетог века, математика и разноликост симбола се у тој мери шири да се многи математичари из исте области међусобно не разумеју. Другим речима, користе различите симболе за исте

појмове. Из тог разлога, 1934. године, формира се група математичара под колективним псеудонимом Николас Бурбаки (Nicolas Bourbaki). Бурбаки група, оригинално, има за циљ да формализује уџбенике математичке анализе. Након почетног успеха, објављује низ уџбеника из разних области математике као што су теорија скупова, апстрактна алгебра, топологија, и Лијева алгебра.

Данас се за било коју формализацију која се изводи помоћу *оловке и ња-ири* сматра да је *неформална*. Због тога, модерни поступак формализације подразумева коришћење интерактивних доказивача теорема. Интерактивни доказивачи омогућавају алгоритамску проверу доказа која је од кључног значаја за исправност доказа. Иако интерактивни доказивачи представљају конкретну програмску имплементацију, па могу садржати грешке при имплементацији, те грешке скоро никада неће утицати на то да интерактивни доказивач прихвати неисправан доказ као исправан. Због тога се формализација унутар интерактивних доказивача сматра *формалном*.

ХоТТ, тренутно, представља најбољи начин формалног заснивања математике. Такође, сматра се да ће имати велики утицај и бити део неких нових покушаја заснивања у будућности. Као такав, вредан је изучавања. Са друге стране, како је МЛТТ у основи ХоТТ-а, циљ овог рада се састоји у:

1. Детаљном теоријском и практичном изучавању МЛТТ;
2. Формализацији основних објеката и конструкција МЛТТ-а у типски зависном програмском језику AGDA.

1.3 Друге формализације

Тренутно постоји неколицина библиотеке које за циљ имају да формализују математику у оквиру ХоТТ-а. Прву и основну библиотеку, написану у интерактивном доказивачу Coq, објавио је Владимир Војводски, 2010. године, под називом FOUNDATIONS [vlad_found]. Ова библиотека постала је део проширене библиотеке UNIMATH [unimath], коју је оригинално написало неколико аутора, такође у интерактивном доказивачу Coq. Након успеха ове две библиотеке, настаје пројекат унивалантног заснивања у коме се паралелно развијају две нове библиотеке HOTТ-Coq [hottcoq] и HOTТ-AGDA

[**hottagda**]. Посебне¹ 2013. године, у Институту за напредне студије у Принстону, пише се и објављује прва неформална књига *Homotopy Type Theory: Univalent Foundations of Mathematics*, или краће *The HoTT Book* [9]. По узору на UNIMATH, од 2021. године, развија се и библиотека AGDA-UNIMATH [**agda-unimath**]. Такође, од 2021. године, на основу библиотеке UNIMATH, пише се књига *Symmetry* [**symm**]. Све четири библиотеке се, и данас, активно развијају.

Једна мана ХоТТ-а је недостатак конструкције унивалентности. Унивалентност се аксиоматизује, те нема правило израчунавања. Због тога, није могуће конструисати типове за чију се конструкцију користи унивалентност. Другим речима, када систем наиђе на унивалентност неће знати како да је редукује. Као решење овог проблема настаје *коцкаста теорија типова* (енгл. *cubical type theory*) [**cube**]. Коцкаста теорија типова је имплементирана проширењем програмског језика AGDA који се назива CUBICAL AGDA. То је омогућило да настане библиотека CUBICAL [**cubi**] која се, такође, активно развија.

¹Многи ову годину сматрају *посебном* зато што је имала огроман утицај на област и заједницу.

Глава 2

Интуиционистичка теорија типова

Интуиционистичка теорија типова или Пер Мартин-Луф теорија типова је математичка теорија конструкција. Тип представља врсту конструкције. Елемент, терм или тачка представља резултат конструкције неког типа. Прецизније, елемент a типа A записујемо као $a : A$, и кажемо да елемент a *настањује* тип A . Битно је напоменути да терм не може да “живи самостално” тј. терм увек мора да настањује неки тип.

Конструкција типова се састоји из низа дедуктивних *правила закључивања*. Правило закључивања записујемо као

$$\frac{\mathcal{H}_1 \quad \mathcal{H}_2 \quad \dots \quad \mathcal{H}_n}{\mathcal{C}}$$

где расуђивања $\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_n$ називамо *премисе* или *хипотезе*, а расуђивање \mathcal{C} називамо *закључак*.

Дефиниција 2.0.1. Свако *расуђивање* је облика $\Gamma \vdash \mathcal{J}$, где је Γ *контекст* и \mathcal{J} *теза* расуђивања.

Дефиниција 2.0.2. *Контекст расуђивања* је коначна листа узајамно зависних променљивих декларисаних на следећи начин

$$x_1 : A_1, x_2 : A_2(x_1), \dots, x_n : A_n(x_1, \dots, x_{n-1}),$$

под условом да за свако $1 \leq k \leq n$ можемо да изведемо расуђивање

$$x_1 : A_1, x_2 : A_2(x_1), \dots, x_{k-1} : A_{k-1}(x_1, \dots, x_{k-2}) \vdash A_k(x_1, x_2, \dots, x_{k-1}).$$

Дефиниција 2.0.3. *Теза расуђивања* може имати четири врсте расуђивања и то су:

(i) A је (*добро-формиран*) *тип* у контексту Γ

$$\Gamma \vdash A \text{ type}$$

(ii) A и B су *расуђивачки једнаки типови* у контексту Γ

$$\Gamma \vdash A \equiv B \text{ type}$$

(iii) a је *елемент* типа A у контексту Γ

$$\Gamma \vdash a : A$$

(iv) a и b су *расуђивачки једнаки елементи* типа A у контексту Γ

$$\Gamma \vdash a \equiv_A b : A$$

2.1 Правила закључивања

Интуиционистичка теорија типова, као и други математички формализми, захтева скуп правила закључивања на којима ће се формализам заснивати. Та правила називамо *структурна правила*.

Пример структурних правила закључивања која описују да је расуђивачка једнакост релација еквиваленције:

$$\frac{\Gamma \vdash A \text{ type}}{\Gamma \vdash A \equiv A \text{ type}} \quad \frac{\Gamma \vdash A \equiv A' \text{ type}}{\Gamma \vdash A' \equiv A \text{ type}} \quad \frac{\Gamma \vdash A \equiv A' \text{ type} \quad \Gamma \vdash A' \equiv A'' \text{ type}}{\Gamma \vdash A \equiv A'' \text{ type}}$$

$$\frac{\Gamma \vdash a : A}{\Gamma \vdash a \equiv_A a : A} \quad \frac{\Gamma \vdash a \equiv_A a' : A}{\Gamma \vdash a' \equiv_A a : A} \quad \frac{\Gamma \vdash a \equiv_A a' : A \quad \Gamma \vdash a' \equiv_A a'' : A}{\Gamma \vdash a \equiv_A a'' : A}$$

Исцрпна листа структурних правила закључивања у интуиционистичкој теорији типова се може наћи у [8].

2.2 Зависни типови

Из дефиниције контекста можемо видети да неки типови могу зависити од неких термова. На пример, тип $A_2(x_1)$ зависи од терма $x_1 : A_1$, тј. за разне термове $x_1 : A_1$ имамо разне типове $A_2(x_1)$. Ову идеју можемо уопштити помоћу следећих дефиниција:

Дефиниција 2.2.1. Нека је тип A у контексту Γ . *Фамилија типова* над A у контексту Γ је тип $B(x)$ у контексту $\Gamma, x : A$, тј.

$$\Gamma, x : A \vdash B(x) \text{ type.}$$

Кажемо да је B *фамилија типова* над A у контексту Γ . Алтернативно, кажемо да је $B(x)$ тип *индексиран* са $x : A$ у контексту Γ .

Дефиниција 2.2.2. Нека је B фамилија типова над A у контексту Γ . *Секција фамилије* B над типом A у контексту Γ је елемент типа $B(x)$ у контексту $\Gamma, x : A$, тј.

$$\Gamma, x : A \vdash b(x) : B(x).$$

Кажемо да је b *секција фамилије* B над A у контексту Γ . Алтернативно, кажемо да је $b(x)$ елемент типа $B(x)$ *индексиран* са $x : A$ у контексту $\Gamma, x : A$.

Дефиниција 2.2.3. Нека је B фамилија типова над A у контексту Γ , и нека је $a : A$. Кажемо да је $B[a/x]$ *нит* (енгл. *fiber*) од B за параметар a , где $B[a/x]$ представља замену свих појављивања x у B са a . Нит од B за параметар a краће записујемо као $B(a)$.

Дефиниција 2.2.4. Нека је b секција фамилије типова B над A у контексту Γ . Кажемо да је $b[a/x]$ *вредност* од b за параметар a , где $b[a/x]$ представља замену свих појављивања x у b са a . Такође, вредност од b за параметар a краће записујемо као $b(a)$.

2.3 Типови зависних функција

У математици заснованој на теорији скупова функција $f : A \rightarrow B$ дефинисана је над одређеним доменом A и кодоменом B . У теорији типова то не мора да буде случај, тј. кодомен може зависити од елемента над којим се функција примењује. Прецизније, посматрајмо секцију b фамилије типова B над A у контексту Γ . Један начин је да b посматрамо као функцију $x \mapsto b(x)$. Тада $b(x)$ настањује тип $B(x)$ који зависи од $x : A$. Због тога за разне елементе $x : A$ домена имамо разне кодомене, те има смисла говорити о типу *зависних функција* $\prod_{(x:A)} B(x)$.

Спецификација типа зависних функција $\prod_{(x:A)} B(x)$ је дата следећим правилима закључивања:

$$\begin{array}{c} \frac{[\prod\text{-form}]}{\Gamma, x : A \vdash B(x) \text{ type}} \quad \frac{[\prod\text{-intro}]}{\Gamma, x : A \vdash b(x) : B(x)} \quad \frac{[\prod\text{-elim}]}{\Gamma \vdash f : \prod_{(x:A)} B(x)} \\ \frac{[\prod\text{-comp}_1]}{\Gamma, x : A \vdash b(x) : B(x)} \quad \frac{[\prod\text{-comp}_2]}{\Gamma \vdash f : \prod_{(x:A)} B(x)} \\ \frac{}{\Gamma \vdash \prod_{(x:A)} B(x) \text{ type}} \quad \frac{}{\Gamma \vdash \lambda x. b(x) : \prod_{(x:A)} B(x)} \quad \frac{}{\Gamma, x : A \vdash f(x) : B(x)} \\ \frac{}{\Gamma \vdash (\lambda y. b(y))(x) \equiv b(x) : B(x)} \quad \frac{}{\Gamma \vdash \lambda x. f(x) \equiv f : \prod_{(x:A)} B(x)} \end{array}$$

Специјалан случај типа зависних функција је тип (уобичајених) *функција* $A \rightarrow B$. Уколико су типови A и B у контексту Γ , тј. тип B не зависи од елемената типа A , тада $\prod_{(x:A)} B$ представља тип (уобичајених) функција.

Дефиниција 2.3.1. Тип (уобичајених) *функција* $A \rightarrow B$ дефинишемо као:

$$A \rightarrow B := \prod_{(x:A)} B.$$

Ако је $f : A \rightarrow B$ функција, тада је A *домен*, а B *кодомен* функције f .

Дефиниција 2.3.2. За сваки тип A дефинишемо *функцију идентитета* $\text{id}_A : A \rightarrow A$ као $\text{id}_A := \lambda x. x$.

Дефиниција 2.3.3. За свака три типа A , B , и C дефинишемо *композицију* $\text{comp} : (B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C$ као $\text{comp} := \lambda g. \lambda f. \lambda g(f(x))$.

Може се показати да је композиција асоцијативна, као и да је функција идентитета неутрал за композицију функција. Због сагласности типова имамо леви неутрал id_B и десни неутрал id_A .

2.4 Индуктивни типови

Поред типова зависних функција постоји и класа *индуктивних типова*. Сваки индуктивни тип се дефинише помоћу следеће спецификације:

- (i) *Формирање* типа описује начин на који се дати тип формира. Прецизније, дефинише хипотезе на основу којих је могуће формирати дати тип.
- (ii) *Конструисање* описује на који начин се уводе нови канонични термови датог типа. Прецизније, дефинише функције које конструирају каноничне термове датог типа, као и потребне хипотезе за њихово постојање. Те функције се често називају *конструктори*.
- (iii) *Индуктивни принцип* описује податке који су потребни да би се конструисала секција произвољне фамилије типова над датим типом. Другим речима, дефинише хипотезе за постојање функције $\text{ind}_A : \prod_{(x:A)} P(x)$.
- (iv) *Правила израчунавања* захтевају да се индуктивно дефинисана секција произвољне фамилије типова над датим типом поклапа по конструкторима који уводе нове каноничне термове. Другим речима, за сваки конструктор $c : A$, мора да важи $\text{ind}_A(c) \equiv \square : P(c)$, где \square представља одговарајући израз/рачун.

Обично се, поред ових спецификација, уводи и *правило рекурзије* које је специјални случај правила индукције. Код правила рекурзије не конструирамо секцију произвољне фамилије типова над датим типом, већ само константну фамилију над датим типом. Другим речима, дефинишемо хипотезе за постојање функције $\text{rec}_A : A \rightarrow P$, као и одговарајућа правила израчунавања.

У наставку су наведене спецификације за уобичајене индуктивне типове: тип природних бројева \mathbb{N} , празни тип $\mathbb{0}$, јединични тип $\mathbb{1}$, типови копроизвода $A + B$, тип зависних парова $\sum_{(x:A)} B(x)$, као и специјални случајеви ових типова. Поред њих, у засебном поглављу ће бити представљени типови идентитета $x =_A y$.

Тип природних бројева

Тип природних бројева \mathbb{N} представља тип кога настањују природни бројеви $0_{\mathbb{N}}, 1_{\mathbb{N}}, 2_{\mathbb{N}}, \dots$. Прецизније, тип природних бројева \mathbb{N} дефинишемо следећом спецификацијом:

$$\begin{array}{c}
 \frac{[\mathbb{N}\text{-form}]}{\vdash \mathbb{N} \text{ type}} \qquad \frac{[\mathbb{N}\text{-intro}_{0_{\mathbb{N}}}] }{\vdash 0_{\mathbb{N}} : \mathbb{N}} \qquad \frac{[\mathbb{N}\text{-intro}_{\text{succ}_{\mathbb{N}}}] }{\vdash \text{succ}_{\mathbb{N}} : \mathbb{N} \rightarrow \mathbb{N}} \\
 \\
 \frac{
 \begin{array}{c}
 [\mathbb{N}\text{-ind}] \\
 \Gamma, n : \mathbb{N} \vdash P(n) \text{ type} \\
 \Gamma \vdash p_{0_{\mathbb{N}}} : P(0_{\mathbb{N}}) \\
 \Gamma \vdash p_{\text{succ}_{\mathbb{N}}} : \prod_{(n:\mathbb{N})} P(n) \rightarrow P(\text{succ}_{\mathbb{N}}(n))
 \end{array}
 }{\Gamma \vdash \text{ind}_{\mathbb{N}}(p_{0_{\mathbb{N}}}, p_{\text{succ}_{\mathbb{N}}}) : \prod_{(n:\mathbb{N})} P(n)}
 \quad
 \frac{
 \begin{array}{c}
 [\mathbb{N}\text{-comp}_{0_{\mathbb{N}}}^{\text{ind}_{\mathbb{N}}}] \\
 \Gamma, n : \mathbb{N} \vdash P(n) \text{ type} \\
 \Gamma \vdash p_{0_{\mathbb{N}}} : P(0_{\mathbb{N}}) \\
 \Gamma \vdash p_{\text{succ}_{\mathbb{N}}} : \prod_{(n:\mathbb{N})} P(n) \rightarrow P(\text{succ}_{\mathbb{N}}(n))
 \end{array}
 }{\Gamma \vdash \text{ind}_{\mathbb{N}}(p_{0_{\mathbb{N}}}, p_{\text{succ}_{\mathbb{N}}}, 0_{\mathbb{N}}) \equiv p_{0_{\mathbb{N}}} : P(0_{\mathbb{N}})} \\
 \\
 \frac{
 \begin{array}{c}
 [\mathbb{N}\text{-comp}_{\text{succ}_{\mathbb{N}}}^{\text{ind}_{\mathbb{N}}}] \\
 \Gamma, n : \mathbb{N} \vdash P(n) \text{ type} \\
 \Gamma \vdash p_{0_{\mathbb{N}}} : P(0_{\mathbb{N}}) \\
 \Gamma \vdash p_{\text{succ}_{\mathbb{N}}} : \prod_{(n:\mathbb{N})} P(n) \rightarrow P(\text{succ}_{\mathbb{N}}(n))
 \end{array}
 }{\Gamma, n : \mathbb{N} \vdash \text{ind}_{\mathbb{N}}(p_{0_{\mathbb{N}}}, p_{\text{succ}_{\mathbb{N}}}, \text{succ}_{\mathbb{N}}(n)) \equiv p_{\text{succ}_{\mathbb{N}}}(n, \text{ind}_{\mathbb{N}}(p_{0_{\mathbb{N}}}, p_{\text{succ}_{\mathbb{N}}}, n)) : P(\text{succ}_{\mathbb{N}}(n))} \\
 \\
 \frac{
 \begin{array}{c}
 [\mathbb{N}\text{-rec}_{\mathbb{N}}] \\
 \Gamma \vdash A \text{ type} \\
 \Gamma \vdash a_{0_{\mathbb{N}}} : A \\
 \Gamma \vdash a_{\text{succ}_{\mathbb{N}}} : \mathbb{N} \rightarrow A \rightarrow A
 \end{array}
 }{\Gamma \vdash \text{rec}_{\mathbb{N}}(a_{0_{\mathbb{N}}}, a_{\text{succ}_{\mathbb{N}}}) : \mathbb{N} \rightarrow A}
 \quad
 \frac{
 \begin{array}{c}
 [\mathbb{N}\text{-comp}_{0_{\mathbb{N}}}^{\text{rec}_{\mathbb{N}}}] \\
 \Gamma \vdash A \text{ type} \\
 \Gamma \vdash a_{0_{\mathbb{N}}} : A \\
 \Gamma \vdash a_{\text{succ}_{\mathbb{N}}} : \mathbb{N} \rightarrow A \rightarrow A
 \end{array}
 }{\Gamma \vdash \text{rec}_{\mathbb{N}}(a_{0_{\mathbb{N}}}, a_{\text{succ}_{\mathbb{N}}}, 0_{\mathbb{N}}) \equiv a_{0_{\mathbb{N}}} : A} \\
 \\
 \frac{
 \begin{array}{c}
 [\mathbb{N}\text{-comp}_{\text{succ}_{\mathbb{N}}}^{\text{rec}_{\mathbb{N}}}] \\
 \Gamma \vdash A \text{ type} \\
 \Gamma \vdash a_{0_{\mathbb{N}}} : A \\
 \Gamma \vdash a_{\text{succ}_{\mathbb{N}}} : \mathbb{N} \rightarrow A \rightarrow A
 \end{array}
 }{\Gamma, n : \mathbb{N} \vdash \text{rec}_{\mathbb{N}}(a_{0_{\mathbb{N}}}, a_{\text{succ}_{\mathbb{N}}}, \text{succ}_{\mathbb{N}}(n)) \equiv a_{\text{succ}_{\mathbb{N}}}(n, \text{rec}_{\mathbb{N}}(a_{0_{\mathbb{N}}}, a_{\text{succ}_{\mathbb{N}}}, n)) : A}
 \end{array}$$

По правилу $\mathbb{N}\text{-form}$, тип природних бројева \mathbb{N} може да се формира из празног контекста. Другим речима, постојање типа природних бројева \mathbb{N} не зависи од постојања других типова. Даље, имамо два конструктора помоћу којих конструишемо све каноничке термове типа \mathbb{N} . Први конструктор је константа $0_{\mathbb{N}} : \mathbb{N}$ и он говори да је $0_{\mathbb{N}}$ канонични терм типа \mathbb{N} . Други конструктор је функција $\text{succ}_{\mathbb{N}} : \mathbb{N} \rightarrow \mathbb{N}$ и она говори да ће $\text{succ}_{\mathbb{N}}(n)$ бити канонични терм

типа \mathbb{N} ако је $n : \mathbb{N}$ канонични терм. Због тога су $0_{\mathbb{N}}, \text{succ}_{\mathbb{N}}(0_{\mathbb{N}}), \text{succ}_{\mathbb{N}}(\text{succ}_{\mathbb{N}}(0_{\mathbb{N}})), \dots$ канонични термови који настајују тип \mathbb{N} .

Правила формирања и конструкције нам говоре под којим условима се може формирати тип, и како конструисати каноничне термове тог типа. Потребно је још дефинисати и начин на који се тип и елементи тог типа користе. Због тога се уводи индуктивно правило и правила израчунавања. Да би конструисали елемент $\text{ind}_{\mathbb{N}}(p_{0_{\mathbb{N}}}, p_{\text{succ}_{\mathbb{N}}}) : \prod_{(n:\mathbb{N})} P(n)$ потребно је конструисати елемент $p_{0_{\mathbb{N}}} : P(0_{\mathbb{N}})$ (*база индукције*) и $p_{\text{succ}_{\mathbb{N}}} : \prod_{n:\mathbb{N}} P(n) \rightarrow P(\text{succ}_{\mathbb{N}}(n))$ (*индуктивни корак*). Даље, за сваки од конструктора треба увести правило израчунавања у складу са зависном функцијом $\text{ind}_{\mathbb{N}}(p_{0_{\mathbb{N}}}, p_{\text{succ}_{\mathbb{N}}}) : \prod_{(n:\mathbb{N})} P(n)$. Због тога имамо два правила израчунавања $\mathbb{N}\text{-comp}_{0_{\mathbb{N}}}$ и $\mathbb{N}\text{-comp}_{\text{succ}_{\mathbb{N}}}$.

Специјални случај индукције типа природних бројева је рекурзија типа природних бројева, у којој тип P не зависи од \mathbb{N} . Тада добијамо функцију $\text{rec}_{\mathbb{N}}(a_{0_{\mathbb{N}}}, a_{\text{succ}_{\mathbb{N}}}) : \mathbb{N} \rightarrow A$, под условом да имамо елементе $a_{0_{\mathbb{N}}} : A$ и $a_{\text{succ}_{\mathbb{N}}} : \mathbb{N} \rightarrow A \rightarrow A$.

Правило индукције, заједно са правилом рекурзије, омогућава дефинисање разних функција над природним бројевима. Да би дефинисали операцију сабирања природних бројева $+_{\mathbb{N}} : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \mathbb{N}$ можемо искористити правило рекурзије, тј. функцију $\text{rec}_{\mathbb{N}} : A \rightarrow (\mathbb{N} \rightarrow A \rightarrow A) \rightarrow \mathbb{N} \rightarrow A$. За тип A узећемо \mathbb{N} . Због тога, сабирање природних бројева дефинишемо као:

$$m +_{\mathbb{N}} n \equiv \text{rec}_{\mathbb{N}}(m, \lambda n. \lambda r. \text{succ}_{\mathbb{N}}(r), n).$$

Заиста, за овако дефинисану операцију сабирања важи:

$$\begin{aligned} m +_{\mathbb{N}} 0_{\mathbb{N}} &\equiv m; \\ m +_{\mathbb{N}} \text{succ}_{\mathbb{N}}(n) &\equiv \text{succ}_{\mathbb{N}}(m +_{\mathbb{N}} n). \end{aligned}$$

Слично, множење природних бројева $\times_{\mathbb{N}} : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \mathbb{N}$ можемо дефинисати као:

$$m \times_{\mathbb{N}} n \equiv \text{rec}_{\mathbb{N}}(0_{\mathbb{N}}, \lambda n. \lambda r. m +_{\mathbb{N}} r, n).$$

Такође, за овако дефинисану операцију множења важи:

$$\begin{aligned} m \times_{\mathbb{N}} 0_{\mathbb{N}} &\equiv 0_{\mathbb{N}}; \\ m \times_{\mathbb{N}} \text{succ}_{\mathbb{N}}(n) &\equiv (m +_{\mathbb{N}} (m \times_{\mathbb{N}} n)). \end{aligned}$$

Можемо приметити шаблон између дефинисања операција преко рекурзивног правила и правила која захтевамо да важе по конструкторима. Наиме,

уколико желимо да дефинишемо функцију $f : \mathbb{N} \rightarrow A$ за коју важи:

$$\begin{aligned} f(0_{\mathbb{N}}) &\equiv \Phi_{0_{\mathbb{N}}}; \\ f(\text{succ}_{\mathbb{N}}(n)) &\equiv \Phi_{\text{succ}_{\mathbb{N}}}, \end{aligned}$$

где је $\Phi_{0_{\mathbb{N}}}$ израз типа A , и $\Phi_{\text{succ}_{\mathbb{N}}}$ израз типа A који може садржати n и $f(n)$. Тада функцију $f : \mathbb{N} \rightarrow A$ дефинишемо као:

$$f \equiv \text{rec}_{\mathbb{N}}(\Phi_{0_{\mathbb{N}}}, \lambda n. \lambda r. \Phi'_{\text{succ}_{\mathbb{N}}}),$$

где $\Phi'_{\text{succ}_{\mathbb{N}}}$ добијемо из $\Phi_{\text{succ}_{\mathbb{N}}}$ тако што сва појављивања $f(n)$ заменимо са r . Овај поступак дефинисања можемо уопштити и на индуктивно правило, и тада се он назива *ујаривање шаблона* (енгл. *pattern matching*).

Празни тип

Празни тип \emptyset је дегенерисани пример индуктивног типа кога не настањује ни један елемент. Прецизније, празни тип \emptyset дефинишемо следећом спецификацијом:

$$\begin{array}{lll} [\emptyset\text{-form}] & \frac{}{\vdash \emptyset \text{ type}} & [\emptyset\text{-ind}] \quad \frac{\Gamma, 0 \vdash P(x) \text{ type}}{\Gamma \vdash \text{ind}_0 : \prod_{(x:\emptyset)} P(x)} \quad [\emptyset\text{-rec}] \quad \frac{\Gamma \vdash A \text{ type}}{\Gamma \vdash \text{rec}_0 : \emptyset \rightarrow A} \end{array}$$

Како празан тип \emptyset не настањује ни један елемент, за њега не постоји ни један конструктор, и самим тим нема ни једно правило израчунавања. Може да се формира из празног контекста, а његово правило индукције тврди да за било коју фамилију типова P над \emptyset постоји елемент $\text{ind}_0 : \prod_{(x:\emptyset)} P(x)$. Чешће се користи правило рекурзије које тврди да уколико конструишемо елемент $x : \emptyset$, онда можемо да конструишемо елемент $\text{rec}_0(x) : A$ било ког типа A . Правило рекурзије за празни тип \emptyset се обично назива и *уравило контрадикције* или *уравило противречности*.

Дефиниција 2.4.1. За сваки тип A дефинишемо тип *негације* од A као $\neg A := A \rightarrow \emptyset$. Поред тога, кажемо да је тип A *уразан* ако његову негацију настањује неки елемент, тј. $\text{empty}(A) := A \rightarrow \emptyset$.

Приметимо да је *двукратна негација* од A дефинисана као $\neg\neg A := (A \rightarrow \emptyset) \rightarrow \emptyset$. Због тога, не мора да важи $\neg\neg A \rightarrow A$, те у општем случају није могуће изводити доказе контрадикцијом.

Јединични тип

Јединични тип $\mathbb{1}$ је индуктивни тип кога настањује само елемент \star . Прецизније, јединични тип $\mathbb{1}$ дефинишемо следећом спецификацијом:

$$\begin{array}{c}
 [\mathbb{1}\text{-form}] \quad \overline{\vdash \mathbb{1} \text{ type}} \qquad [\mathbb{1}\text{-intro}_\star] \quad \overline{\vdash \star : \mathbb{1}} \\
 \\
 [\mathbb{1}\text{-ind}] \quad \frac{\Gamma, x : \mathbb{1} \vdash P(x) \text{ type} \quad \Gamma \vdash p_\star : P(\star)}{\Gamma \vdash \text{ind}_{\mathbb{1}}(p_\star) : \prod_{(x:\mathbb{1})} P(x)} \qquad [\mathbb{1}\text{-comp}] \quad \frac{\Gamma, 1 \vdash P(x) \text{ type} \quad \Gamma \vdash p_\star : P(\star)}{\Gamma \vdash \text{ind}_{\mathbb{1}}(p_\star, \star) \equiv p_\star : P(\star)} \\
 \\
 [\mathbb{1}\text{-rec}] \quad \frac{\Gamma \vdash A \text{ type} \quad \Gamma \vdash a : A}{\Gamma \vdash \text{rec}_{\mathbb{1}}(a) : \mathbb{1} \rightarrow A}
 \end{array}$$

Јединични тип $\mathbb{1}$ може да се формира из празног контекста, а његово правило индукције тврди да за било коју фамилију типова P над $\mathbb{1}$ постоји елемент $\text{ind}_{\mathbb{1}}(p_\star) : \prod_{(x:\mathbb{1})} P(x)$ уколико постоји елемент $p_\star : P(\star)$. Како постоји само један конструктор $\star : \mathbb{1}$, имамо једно правило израчунавања које треба да се поклопи са индуктивним правилом. Због тога, $\text{ind}_{\mathbb{1}}(p_\star, \star) \equiv p_\star : P(\star)$.

Специјални случај правила индукције типа $\mathbb{1}$ је правило рекурзије типа $\mathbb{1}$, које добијамо када фамилија типова P над $\mathbb{1}$ не зависи од $x : \mathbb{1}$. Тада за сваки елемент $a : A$ имамо функцију $\text{rec}_{\mathbb{1}}(a) : \mathbb{1} \rightarrow A$.

Дефиниција 2.4.2. За сваки тип A дефинишемо тип *јединствене функције* од A као $!A := A \rightarrow \mathbb{1}$. Специјално, јединствена функција од $\mathbb{0}$, тј. $\mathbb{0} \rightarrow \mathbb{1}$, се назива *вакумска функција*.

У хомотопној теорији типова за вакумску функцију важи да је јединствена.

Типови копроизвода

За типове A и B из контекста Γ можемо дефинисати тип копроизвода $A+B$ кога ће настањивати елементи или из типа A (ако $a : A$, онда $\text{inl}(a) : A+B$)

или из типа B (ако $b : B$, онда $\text{inr}(b) : A + B$). Прецизније, тип копроизвода $A + B$ дефинишемо следећом спецификацијом:

$$\begin{array}{c}
 \frac{\Gamma \vdash A \text{ type}, B \text{ type}}{\Gamma \vdash A + B \text{ type}} \quad \frac{[+ \text{-intro}_{\text{inl}}]}{\Gamma \vdash \text{inl} : A \rightarrow A + B} \quad \frac{[+ \text{-intro}_{\text{inr}}]}{\Gamma \vdash \text{inr} : B \rightarrow A + B} \\
 \\
 \begin{array}{c}
 \Gamma, z : A + B \vdash P(z) \text{ type} \\
 \Gamma \vdash p_{\text{inl}} : \prod_{(a:A)} P(\text{inl}(a)) \\
 \Gamma \vdash p_{\text{inr}} : \prod_{(b:B)} P(\text{inr}(b)) \\
 \hline
 \Gamma \vdash \text{ind}_+(p_{\text{inl}}, p_{\text{inr}}) : \prod_{(z:A+B)} P(z)
 \end{array} \\
 \\
 \begin{array}{c}
 \Gamma, z : A + B \vdash P(z) \text{ type} \\
 \Gamma \vdash p_{\text{inl}} : \prod_{(a:A)} P(\text{inl}(a)) \\
 \Gamma \vdash p_{\text{inr}} : \prod_{(b:B)} P(\text{inr}(b)) \\
 \hline
 \Gamma, a : A \vdash \text{ind}_+(p_{\text{inl}}, p_{\text{inr}}, \text{inl}(a)) \equiv p_{\text{inl}}(a) : P(\text{inl}(a)) \\
 \Gamma, b : B \vdash \text{ind}_+(p_{\text{inl}}, p_{\text{inr}}, \text{inr}(b)) \equiv p_{\text{inr}}(b) : P(\text{inr}(b))
 \end{array} \\
 \\
 \begin{array}{c}
 \Gamma \vdash \text{type} \\
 \Gamma \vdash f : A \rightarrow X \\
 \Gamma \vdash g : B \rightarrow X \\
 \hline
 \Gamma \vdash \text{rec}_+(f, g) : A + B \rightarrow X
 \end{array}
 \end{array}$$

Тип копроизвода $A + B$ због своје природе има два конструктора $\text{inl} : A \rightarrow A + B$ и $\text{inr} : B \rightarrow A + B$. Правило индукције тврди да за било коју фамилију типова P над $A + B$ постоји елемент $\text{ind}_+(p_{\text{inl}}, p_{\text{inr}}) : \prod_{(z:A+B)} P(z)$ уколико постоје елементи $p_{\text{inl}} : \prod_{(a:A)} P(\text{inl}(a))$ и $p_{\text{inr}} : \prod_{(b:B)} P(\text{inr}(b))$. Како постоје два конструктора, имамо два правила израчунавања која треба да се поклопе са правилом индукције. Због тога, $\text{ind}_+(p_{\text{inl}}, p_{\text{inr}}, \text{inl}(a)) \equiv p_{\text{inl}}(a) : P(\text{inl}(a))$ и $\text{ind}_+(p_{\text{inl}}, p_{\text{inr}}, \text{inr}(b)) \equiv p_{\text{inr}}(b) : P(\text{inr}(b))$.

Специјални случај правила индукције типа $A + B$ је правило рекурзије типа $A + B$, које добијамо када фамилија типова P над $A + B$ не зависи од $z : A + B$. Тада за сваку функцију $f : A \rightarrow X$ и за сваку функцију $g : B \rightarrow X$ имамо функцију $\text{rec}_+(f, g) : A + B \rightarrow X$. Из правила индукције, за свако $f : A \rightarrow X$ и за свако $g : B \rightarrow Y$, имамо функцију $f + g : A + B \rightarrow X + Y$.

Специјални случај типа копроизвода је *Булов шии* $2 := \mathbb{1} + \mathbb{1}$, чије једине елементе дефинишемо као $\text{true} := \text{inl}(\star)$ и $\text{false} := \text{inr}(\star)$. Из спецификације

типа копроизвода можемо извући правило индукције и правило израчунавања, за буловски тип 2. Правило индукције 2-ind се назива и *if-then-else*.

$$\begin{array}{c}
 \text{[2-ind]} \quad \frac{\begin{array}{c} \Gamma, x : 2 \vdash P(x) \text{ type} \\ \Gamma \vdash p_{\text{true}} : P(\text{true}) \\ \Gamma \vdash p_{\text{false}} : P(\text{false}) \end{array}}{\Gamma \vdash \text{ind}_2(p_{\text{true}}, p_{\text{false}}) : \prod_{(x:2)} P(x)} \\
 \\
 \text{[2-comp]} \quad \frac{\begin{array}{c} \Gamma, x : 2 \vdash P(x) \text{ type} \\ \Gamma \vdash p_{\text{true}} : P(\text{true}) \\ \Gamma \vdash p_{\text{false}} : P(\text{false}) \end{array}}{\begin{array}{c} \Gamma \vdash \text{ind}_2(p_{\text{true}}, p_{\text{false}}, \text{true}) \equiv p_{\text{true}} : P(\text{true}) \\ \Gamma \vdash \text{ind}_2(p_{\text{true}}, p_{\text{false}}, \text{false}) \equiv p_{\text{false}} : P(\text{true}) \end{array}}
 \end{array}$$

Типови зависних парова

Ако је B фамилија типова над A из контекста Γ , онда можемо формирати тип зависних парова $\sum_{(x:A)} B(x)$ кога ће настањивати *парови* $(x, y(x))$, где је $x : A$ и $y(x) : B(x)$. Прецизније, тип зависних парова $\sum_{(x:A)} B(x)$ дефинишемо следећом спецификацијом.

$$\begin{array}{c}
 \text{[}\sum\text{-form]} \quad \frac{\Gamma, x : A \vdash B(x) \text{ type}}{\Gamma \vdash \sum_{(x:A)} B(x) \text{ type}} \qquad \text{[}\sum\text{-intro]} \quad \frac{\Gamma, x : A \vdash y(x) : B(x)}{\Gamma \vdash (x, y(x)) : \sum_{(x:A)} B(x)} \\
 \\
 \text{[}\sum\text{-ind]} \quad \frac{\Gamma, (x, y) : \sum_{(x:A)} B(x) \vdash P((x, y)) \text{ type} \quad \Gamma \vdash f : \prod_{(x:A)} \prod_{(y:B(x))} P((x, y))}{\Gamma \vdash \text{ind}_{\sum}(f) : \prod_{(p:\sum_{(x:A)} B(x))} P(p)} \\
 \\
 \text{[}\sum\text{-comp]} \quad \frac{\Gamma, (x, y) : \sum_{(x:A)} B(x) \vdash P((x, y)) \text{ type} \quad \Gamma \vdash f : \prod_{(x:A)} \prod_{(y:B(x))} P((x, y))}{\Gamma, (x, y) : \sum_{(x:A)} B(x) \vdash \text{ind}_{\sum}(f, (x, y)) \equiv f(x, y) : P((x, y))}
 \end{array}$$

Тип зависних парова $\sum_{(x:A)} B(x)$ има један конструктор помоћу кога се могу формирати елементи који га настањују, и то једноставним упаривањем елемената $x : A$ и $y(x) : B(x)$. Правило индукције тврди да за било коју фамилију типова P над $\sum_{(x:A)} B(x)$ постоји елемент $\text{ind}_{\sum}(f) : \prod_{p:\sum_{(x:A)} B(x)} P(p)$ уколико постоји елемент $f : \prod_{(x:A)} \prod_{(y:B(x))} P((x, y))$. Како постоји само један конструктор, имамо само једно правило израчунавања које треба да се поклопи са правилом индукције. Због тога, важи $\text{ind}_{\sum}(f, (x, y)) \equiv f(x, y) : P((x, y))$.

Правило индукције нам омогућава да дефинишемо функције у наставку.

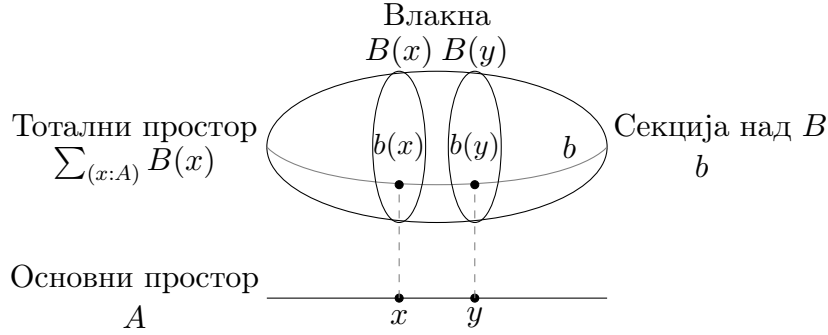
Дефиниција 2.4.3. Нека је B фамилија типова над A . Тада елемент $\text{pr}_1 : \sum_{(x:A)} B(x) \rightarrow A$ *пројекције на први елемент* дефинишемо као:

$$\text{pr}_1((a, b)) \equiv a, \quad (2.1)$$

а елемент $\text{pr}_2 : \prod_{p:\sum_{(x:A)} B(x)} B(\text{pr}_1(p))$ *пројекције на други елемент* дефинишемо као:

$$\text{pr}_2((a, b)) \equiv b. \quad (2.2)$$

Ако претпоставимо да имамо елемент $f : \prod_{((x,y):\sum_{(x:A)} B(x))} P((x, y))$ тада конструишемо елемент типа $\prod_{(x:A)} \prod_{(y:B(x))} P((x, y))$ као $\lambda x. \lambda y. f((x, y))$. Ова конструкција се назива *каријевање* (енгл. *carry*), и како је супротна правилу \sum -ind, правило \sum -ind често називамо *одкаријевање* (енгл. *uncarry*).



Слика 2.1: Геометријска репрезентација типа зависних парова.

Специјални случај типа зависних парова је тип (независних) *парова* или (*Декартов*) *производ* $A \times B$. Уколико су типови A и B у контексту Γ , тј. тип B не зависи од елемената типа A , тада $\sum_{(x:A)} B$ представља тип (независних) парова.

Дефиниција 2.4.4. Тип (независних) *парова* $A \times B$ дефинишемо као:

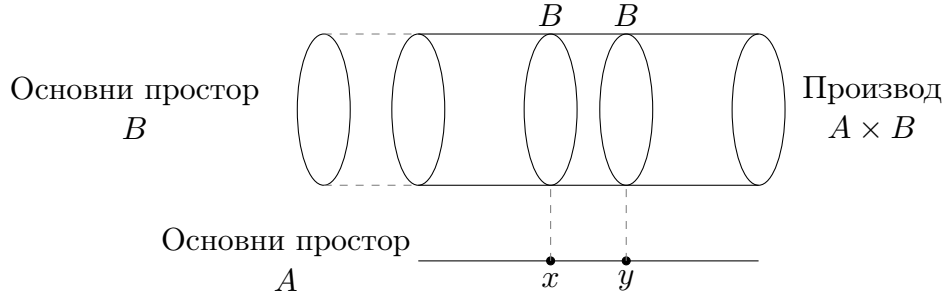
$$A \times B := \sum_{(x:A)} B.$$

Такође, *пројекцију на први елемент* $\text{fst} : A \times B \rightarrow A$ и *пројекцију на други елемент* $\text{snd} : A \times B \rightarrow B$ дефинишемо као:

$$\text{fst}((a, b)) \equiv a, \quad \text{snd}((a, b)) \equiv b.$$

Правило индукције и израчунавања за тип (независних) парова $A \times B$ директно добијамо из правила индукције и израчунавања за тип зависних парова $\sum_{(x:A)} B(x)$.

$$\begin{array}{c}
 \Gamma, (x, y) : A \times B \vdash P((x, y)) \text{ type} \\
 [\times\text{-ind}] \quad \frac{\Gamma \vdash f : \prod_{(x:A)} \prod_{(y:B)} P((x, y))}{\Gamma \vdash \text{ind}_{\times}(f) : \prod_{(p:A \times B)} P(p)} \\
 \\
 \Gamma, (x, y) : A \times B \vdash P((x, y)) \text{ type} \\
 [\times\text{-comp}] \quad \frac{\Gamma \vdash f : \prod_{(x:A)} \prod_{(y:B)} P((x, y))}{\Gamma, (x, y) : A \times B \vdash \text{ind}_{\times}(f, (x, y)) \equiv f(x, y) : P((x, y))}
 \end{array}$$



Слика 2.2: Геометријска репрезентација типа независних парова.

Тип независних парова можемо уопштити на тип k -торки $A_1 \times A_2 \times \dots \times A_k$.

2.5 Искизи као типови

Интерпретација *искази као типови* (енгл. *propositions as types*) (често се назива и *Кари-Хаувардова кореспонденција* или *Брауверу-Хејшинг-Колмоџоров интерпретација* (БХК интерпретација)) неформално посматра исказе као типове, доказе као елементе типова, и предикате као фамилије типова. Да би показали да је исказ тачан у теорији типова треба конструисати елемент који настањује одговарајући тип. Прецизније, за дати исказ A (добро-формирани тип) уколико конструишемо елемент $x : A$ (кога често називамо и *сведок* за A) тада сматрамо да је исказ A тачан. Приметимо да исказ није тачан или нетачан, већ да представља колекцију својих сведока који могу да потврде његову истинитост. Због тога су и сами докази математички објекти. У

Искази	Типови
\perp	0
\top	1
$\neg A$	$A \rightarrow 0$
$A \implies B$	$A \rightarrow B$
$A \wedge B$	$A \times B$
$A \vee B$	$\ A + B\ $
$\forall x.P(x)$	$\prod_{(x:A)} P(x)$
$\exists x.P(x)$	$\ \sum_{(x:A)} P(x)\ $

Табела 2.1: Интерпретација логике првог реда.

табели 2.1 приказани су искази заједно са њиховом одговарајућом интерпретацијом у теорији типова.

Прокоментаришимо неке интерпретације из табеле 2.1. Да би показали да важи $A \implies B$ треба претпоставити да важи A и доказати да важи B . У теорији типова треба конструисати елемент типа $A \rightarrow B$, тј. треба конструисати елемент типа B који користи претпоставку дату постојањем елемента типа A . Остали типови имају сличне интерпретације сем типа копроизвода $A + B$ и типа зависних парова $\sum_{(x:A)} B(x)$.

Да би показали $A \vee B$ треба показати да важи бар један од A и B . У теорији типова треба конструисати елемент типа $A + B$, помоћу једног од конструктора `inl` или `inr`. Због тога тип $A + B$, у односу на $A \vee B$, носи информацију о исказу који је тачан (тачно је или A или тачно је B). Слично, да би показали $\exists x.P(x)$ у теорији типова треба конструисати елемент типа $\sum_{(x:A)} P(x)$. У овом случају теорија типова нам даје и више од тога. Наиме, P је фамилија типова, што значи да $P(x)$ не мора да буде типа 2, тј. P не мора да буде предикат. Поред тога, тип $\sum_{(x:A)} P(x)$ можемо схватити као тип свих елемената $x : A$ за које $P(x)$.

Како ова два типа дају више информација у односу на традиционално значење исказа $A \vee B$ и $\exists x.P(x)$, користе се *окрњени искази* (енгл. *propositional truncation*) $\|A + B\|$ и $\|\sum_{(x:A)} B(x)\|$ који заборављају све информације о својим сведоцима сем да они постоје. Окрњени искази су ван опсега овог рада, тако да се неће детаљно описивати.

2.6 Хијерархија универзума и универзум типови

Универзум *типови* се могу посматрати као типови које настањују други типови. Универзум тип \mathcal{U} омогућава да се исказ „ A type” запише формално као $A : \mathcal{U}$. Поред тога, омогућава да се фамилија типова B над типом A дефинише као функција $B : A \rightarrow \mathcal{U}$.

Желимо да типови који могу да се формирају из празног контекста настањују универзум \mathcal{U} (то су, на пример, 0 , 1 , и \mathbb{N}). Штавише, како универзум \mathcal{U} настањују и други типови, желимо да универзум \mathcal{U} буде затворен по свим начинима формирања нових типова помоћу типова универзума \mathcal{U} . На пример, ако $A : \mathcal{U}$ и $B : A \rightarrow \mathcal{U}$, онда $\prod_{(x:A)} B(x) : \mathcal{U}$. Међутим, не сме доћи то тога да универзум настањује сам себе, тј. не сме да важи $\mathcal{U} : \mathcal{U}$. Другим речима, не смомо обезбедити услове настанка *Раселовог парадокса*.

У многим случајевима довољно је постојање једног универзума \mathcal{U} , међутим, некада желимо да универзум настањује неки други универзум. Како би избегли Раселов парадокс захтевамо постојање *хијерархије универзума*

$$\mathcal{U}_0, \quad \mathcal{U}_1, \quad \mathcal{U}_2, \quad \dots \quad (2.3)$$

за коју важе следећа правила:

$$[\mathcal{U}\text{-intro}] \quad \frac{}{\Gamma \vdash \mathcal{U}_i : \mathcal{U}_{i+1}} \quad [\mathcal{U}\text{-cumul}] \quad \frac{\Gamma \vdash A : \mathcal{U}_i}{\Gamma \vdash A : \mathcal{U}_{i+1}}$$

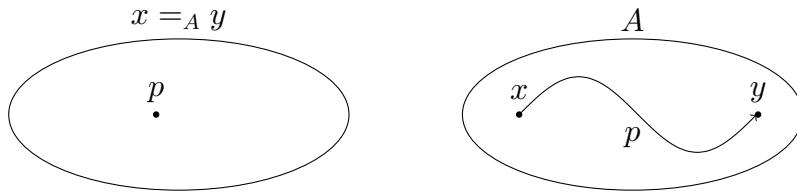
Универзум \mathcal{U}_0 називамо *базни универзум*. Базни универзум настањују типови који могу да се формирају из празног контекста, као и сви типови за чије се формирање користе типове који се већ налазе у базном универзуму. За универзум \mathcal{U}_i има смисла посматрати и \mathcal{U}_{i+1} кога називамо и *универзум следбеник*. Често није битно знати редни број универзума у хијерархији, те се следбеник универзума \mathcal{U} обележава са \mathcal{U}^+ . За два универзума \mathcal{U} и \mathcal{V} можемо дефинисати њихову најмању горњу границу $\mathcal{U} \sqcup \mathcal{V}$. На пример, за \mathcal{U}_0 и \mathcal{U}_1 , најмања горња граница $\mathcal{U}_0 \sqcup \mathcal{U}_1$ је \mathcal{U}_1 .

2.7 Типови идентитета

Подсетимо се да из дефиниције операције $+\mathbb{N}$ важи $m + \mathbb{N} 0_{\mathbb{N}} \equiv m$. Природно се намеће питање: Да ли важи $0_{\mathbb{N}} + \mathbb{N} m \equiv m$? Јасно је да одговор на ово питање треба да буде позитиван, али то није случај у интуиционистичкој теорији типова. Тиме долазимо до фундаменталног проблема интуиционистичке теорије типова: *Шта значи да су елементи неког типа једнаки?* Одговор на ово питање нам дају *типови идентитета* (енгл. *identity types*).

Како расуђивачка једнакост не може описати све врсте једнакости, потребно је дефинисати *исказну једнакост* (енгл. *propositional equality*) која тврди да ће два елемента $x, y : A$ бити исказно једнака. Исказна једнакост је исказ, и по Кари-Хауардовој интерпретацији представља неки тип, а како зависи од два елемента типа A мора бити фамилија типова. Исказне једнакости другачије називамо *типови идентитета*, и обележавамо као $\text{Id}_A : A \rightarrow A \rightarrow \mathcal{U}$. За два конкретна елемента $x, y : A$, тип $\text{Id}_A(x, y)$ обележавамо и као $x =_A y$ и кажемо да су x и y *једнаки* или *исказно једнаки*.

У хомотопној теорији типова, уколико интерпретирамо тип као простор, и елементе типа као тачке тог простора, онда елементе типа $x =_A y$ можемо интерпретирати као *путовање* или *еквиваленције* између тачака x и y у простору A . Као што је могуће да између две тачке у простору постоји више различитих путања, тако је могуће да постоји више од једног сведока једнакости $x =_A y$. Другим речима, $x =_A y$ се може посматрати као тип *идентификације* елемената x и y , и може постојати више начина на који x и y могу да се *идентификују*.



Слика 2.3: Геометријска репрезентација типова идентитета. Лево је представљена класична интерпретација, у којој $x =_A y$ представља исказ, са много различитих сведока $p : x =_A y$ који оправдавају његову истинитост. Док је десно представљена хомотопна интерпретација, у којој између тачака x и y постоји много различитих путања p у простору A .

Ако је A тип и ако су дати елементи $x, y : A$ у контексту Γ , онда можемо

формирати тип идентитета $x =_A y$ кога ће настањивати путање, еквиваленције или идентификације. Основна идентификација коју можемо да конструисамо је *рефлексива*:

$$\text{refl}_x : x =_A x.$$

Рефлексива refl_x тврди да је било који елемент $x : A$ једнак самом себи. Рефлексиву refl_x , у хомотопном смислу, можемо посматрати као константну путању у тачки $x : A$. Формално, начин формирања и конструисања типова идентитета дат је следећом спецификацијом:

$$\frac{\Gamma \vdash A \text{ type} \quad \frac{[-\text{form}]}{\Gamma \vdash x : A} \quad \Gamma \vdash y : A}{\Gamma \vdash x =_A y \text{ type}} \quad \frac{\Gamma \vdash A \text{ type} \quad \frac{[-\text{intro}]}{\Gamma \vdash x : A}}{\Gamma \vdash \text{refl}_x : x =_A x}$$

Уколико су два елемента $x, y : A$ расуђивачки једнака, тј. важи $x \equiv_A y$, онда су и исказно једнака и важи $\text{refl}_x : x =_A y$. Оправдање проналазимо у $\text{refl}_x : (x =_A x) \equiv (x =_A y)$, јер важи $x \equiv_A y$. Обратно, у општем случају, не важи. Другим речима, уколико су два елемента $x, y : A$ исказно једнака, тј. важи $x =_A y$, у општем случају, неће бити расуђивачки једнака, тј. не важи $x \equiv_A y$. Због тога, расуђивачку једнакост често можемо посматрати као *дефинициону једнакост*.

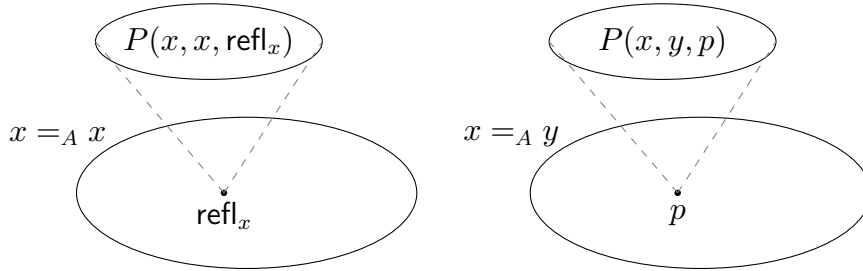
Индукција путање

Правило индукције за типове идентитета називамо *индукција путање*. Индукција путање тврди да за било коју фамилију типова P над типовима A и $x =_A y$ постоји функција $\text{ind}_= : \prod_{(x,y:A)} \prod_{(p:x=_A y)} P(x, y, p)$ уколико постоји функција $f : \prod_{(x:A)} P(x, x, \text{refl}_x)$. Како постоји само један конструктор $\text{refl}_x : x =_A x$, постоји само једно правило израчунавања које треба да се поклопи са правилом индукције. Због тога је правило израчунавања $\text{ind}_=(x, x, \text{refl}_x) \equiv f(x) : P(x, x, \text{refl}_x)$. Формално, правило индукције и правило

израчунавања је дато следећом спецификацијом:

$$\begin{array}{c}
 \Gamma, x : A, y : A, p : x =_A y \vdash P(x, y, p) \text{ type} \\
 \text{[=-ind]} \quad \frac{\Gamma \vdash f : \prod_{(x:A)} P(x, x, \text{refl}_x)}{\Gamma \vdash \text{ind}_= : \prod_{(x,y:A)} \prod_{(p:x=_A y)} P(x, y, p)} \\
 \Gamma, x : A, y : A, p : x =_A y \vdash P(x, y, p) \text{ type} \\
 \text{[=-comp]} \quad \frac{\Gamma \vdash f : \prod_{(x:A)} P(x, x, \text{refl}_x)}{\Gamma, x : A \vdash \text{ind}_=(x, x, \text{refl}_x) \equiv f(x) : P(x, x, \text{refl}_x)}
 \end{array}$$

Једно од кључних питања је шта оправдава индукцију путањом? Другим речима, зашто ће $P(x, y, p)$ важити за било које тачке $x, y : A$ и било коју путању $p : x =_A y$ уколико важи $P(x, x, \text{refl}_x)$ за било коју тачку $x : A$? Кључно запажање лежи у томе да типови идентитета нису индуктивни тип, већ да су индуктивна фамилија типова. То значи да индукција путањом тврди да је фамилија типова $x =_A y$, где су x и y слободне тачке простора A , индуктивно дефинисана константном путањом refl_x . Односно, $\sum_{(x,y:A)} (x =_A y)$ је индуктивно генерисан константним путањама у свакој тачки $x : A$. Битно је напоменути да су обе тачке слободне. Такође, можемо фиксирати једну тачку (у том случају долазимо до другачије еквивалентне индукције путањом, која се назива и *базна индукција путањом*).



Слика 2.4: Геометријска репрезентација индукције путањом.

Неформално, оправдање индукција путањом је осликано следећим примером: Посматрајмо петљу на пробушениом диску која полази из једне тачке, обилази једном рупу, и враћа се у исту тачку. Уколико су почетна тачка и крајња тачка фиксирани, није могуће непрекидно деформисати петљу у константну путању. Када допустимо један крај петље да буде слободна, он може обићи рупу, те је могуће непрекидно деформисати петљу у константну путању. Слично је могуће ако допустимо да обе краја петље буду слободна.

Особине типова идентитета

У хомотопној теорији, над тополошким простором A , $\bar{u}y\bar{u}$ ања између две тачке x и y представља непрекидно пресликавање $p : [0, 1] \rightarrow A$, за које важи $p(0) = x$ и $p(1) = y$. Путања $p : [0, 1] \rightarrow A$ је $\bar{u}e\bar{u}$ ља уколико почиње и завршава се у тачки a_0 , тј. важи $a_0 = p(0) = p(1)$. Једни од корисних појмова над путањама су инверз путање и надовезивање путања. *Инверз $\bar{u}y\bar{u}$ ање* $p : [0, 1] \rightarrow A$ је путања $p^{-1} : [0, 1] \rightarrow A$ за коју важи $p^{-1}(t) = p(1 - t)$ за свако $t \in [0, 1]$. *Надовезивање $\bar{u}y\bar{u}$ ања* $p : [0, 1] \rightarrow A$ и $q : [0, 1] \rightarrow A$ којима се крај и почетак поклапају, тј. за које $p(1) = q(0)$, представља путању $p \cdot q : [0, 1] \rightarrow A$ за коју важи $(p \cdot q)(t) = p(2t)$ за свако $t \in [0, 1/2]$, и $(p \cdot q)(t) = q(2t - 1)$ за свако $t \in [1/2, 1]$. Инверз путање и надовезивање путања, у теорији типова, се карактеришу преко типова идентитета и дате су у следећим лемама:

Лема 1. *Нека је A $\bar{u}u\bar{u}$ у контексту Γ . Тада можемо конструисати функцију*

$$\text{inv}_A : \prod_{(x,y:A)} (x =_A y) \rightarrow (y =_A x)$$

индукцијом $\bar{u}y\bar{u}$ ање $p : x =_A y$ као $\text{inv}_A(x, x, \text{refl}_x) \equiv \text{refl}_x$. Функцију inv_A називамо инверз путање. Чесћо, за дају $\bar{u}y\bar{u}$ ању $p : x =_A y$, њен инверз означавамо са $p^{-1} \equiv \text{inv}_A(x, y, p)$.

Доказ. Да би конструисали елемент типа $\prod_{(x,y:A)} (x =_A y) \rightarrow (y =_A x)$, конструирамо функцију

$$f(x) : \prod_{(y:A)} (x =_A y) \rightarrow (y =_A x)$$

за било који елемент $x : A$. По индукцији путање $p : x =_A y$ довољно је конструисати путању

$$f(x, x, \text{refl}_x) : x =_A x$$

за било који елемент $x : A$. Конструкција ове путање је тривијална и због тога узимамо да је $f(x, x, \text{refl}_x) \equiv \text{refl}_x$. Коначно, тражена конструкција је

$$\text{inv}_A(x, x, \text{refl}_x) \equiv \text{refl}_x.$$

□

Лема 2. Нека је A тип у контексту Γ . Тада можемо конструисати функцију

$$\text{conc}_A : \prod_{(x,y,z:A)} (x =_A y) \rightarrow (y =_A z) \rightarrow (x =_A z)$$

индукцијом њућање $p : x =_A y$ као $\text{conc}_A(x, x, z, \text{refl}_x, q) := q$. Функцију conc_A називамо надовезивање путања. Често, за даће њућање $p : x =_A y$ и $q : y =_A z$, надовезану њућању означавамо са $p \cdot q := \text{conc}_A(x, y, z, p, q)$.

Доказ. Прво конструишемо функцију

$$f(x) : \prod_{(y:A)} (x =_A y) \rightarrow \prod_{(z:A)} (y =_A z) \rightarrow (x =_A z)$$

за било који елемент $x : A$. По индукцији путање $p : (x =_A y)$ довољно је конструисати функцију

$$f(x, x, \text{refl}_x) : \prod_{(z:A)} (x =_A z) \rightarrow (x =_A z)$$

за било који елемент $x : A$. Даље, довољно је конструисати функцију

$$f(x, x, \text{refl}_x, z) : (x =_A z) \rightarrow (x =_A z)$$

за било које елементе $x, z : A$. Конструисање ове функције је тривијално и због тога имамо да је $f(x, x, \text{refl}_x, z, q) := q$. Коначно, тражена конструкција је

$$\text{conc}_A(x, x, z, \text{refl}_x, q) := f(x, x, \text{refl}_x, z, q) := q.$$

□

Код једнакосне логике, инверз путање представља особину симетрије једнакости, док надовезивање путања представља особину транзитивности једнакости. Транзитивност једнакости се користи када доказујемо неку једнакост ланцем једнакости. На пример, уколико желимо да пронађемо сведока за $a = d$, и знамо да су $p : a = b$, $q : b = c$ и $r : c = d$, једноставним надовезивањем путања добијемо сведока $(p \cdot q) \cdot r : a = d$. Ово може бити тешко за тумачење па се често користи следећа синтакса:

$$\begin{array}{ll} a = b & (p) \\ = c & (q) \\ = d & (r). \end{array}$$

Строге једнакости над путањама често нису корисне. Због тога, дефинишемо појам хомотопије. *Хомотопија* између две путање $p : [0, 1] \rightarrow A$ и $q : [0, 1] \rightarrow A$ је непрекидно пресликавање $H : [0, 1] \times [0, 1] \rightarrow A$, за које важи $H(s, 0) = p(s)$ и $H(s, 1) = q(s)$ за свако $s \in [0, 1]$, и $H(0, t) = x$ и $H(1, t) = y$ за свако $t \in [0, 1]$. За две путање кажемо да су *хомотопне*, уколико постоји хомотопија између њих.

Релација хомотопности између две путање је релација еквиваленције, и операције инверз путање и надовезивање путања одржавају еквиваленцију. Над простором A , класа еквиваленција хомотопних петљи у тачки a_0 формира групу коју називамо *фундаментална група* и обележавамо са $\pi_1(A, a_0)$. За разлику од простора свих петљи у тачки a_0 , фундаментална група $\pi_1(A, a_0)$ нам омогућава да лакше испитујемо простор A . Прецизније, фундаментална група је алгебарска инваријанта простора, која може да се искористи за испитивање *хомотопне еквиваленције* два простора.

Хомотопију можемо сматрати као дводимензиону путању, то природно можемо уопштити на тродимензиону путању, четвородимензиону путању, итд. Ово нам дају бесконачни низ појмова: тачка, путања, хомотопија, хомотопија између хомотопија, хомотопија између хомотопија између хомотопија, итд. Заједно са операцијама фундаменталне групе (константна путања, инверз путање, надовезивање путања) добијамо инстанцу алгебарске структуре која се зове (*слаби*) ∞ -*групоид*.

∞ -групоид представља алгебарску структуру која садржи колекцију *објеката* и колекцију *морфизама* између објеката, *морфизама између морфизама*, итд. Морфизме на ниву k зовемо k -морфизми. Морфизми сваког нивоа имају комплексну алгебарску структуру, па тако у случају слабог ∞ -групоида, сваки морфизам датог нивоа има идентитет, композицију, и инверз који задовољавају закон асоцијативности, идентитета и инверза, до на морфизме следећег нивоа.

Ову идеју можемо интерпретирати у теорији типова преко типова идентитета. На основном нивоу имамо елементе неког типа које можемо да идентификујемо. На пример, за $x, y : A$, разматрамо идентификацију $x =_A y$. Како је теорија типова доказно релевантна, могуће је да постоји више различитих сведока за $x =_A y$. Нека су то путање $p, q : x =_A y$. Типови идентитета нам даље омогућавају да разматрамо једнакост између p и q , односно омогућавају нам да формирамо тип $p =_{x=_A y} q$. Како су p и q путање, сведока $r : p =_{x=_A y} q$

Једнакости	Хомотопија	∞ -Групоид
рефлексивност	константна путања	идентички морфизам
симетричност	обртање путања	инверз морфизма
транзитивност	надовезивање путања	композиција морфизама

Табела 2.2: Разне интерпретације особина типова идентитета

можемо сматрати као хомотопијом између путања p и q , или као дводимензионом путањом. Можемо даље итерирати и добити тип тродимензионих путања $r =_{p=x=Ayq} s$, итд. У табели 2.2 приказана је веза између једнакосне логике, хомотопне теорије и структуре ∞ -групоид.

На слици 2.7 приказана је групоидна структура типова, док следећа лема карактерише да тип идентитета на датом нивоу има својства слабог ∞ -групоида:

Лема 3. Нека је A \mathcal{U} , нека су елементи $x, y, z, w : A$ и нека су путање $p : x =_A y$, $q : y =_A z$ и $r : z =_A w$ у контексту Γ . Тада важи:

$$(i) \text{ refl}_x \cdot p = p \text{ и } p \cdot \text{ refl}_y = p$$

$$(ii) p^{-1} \cdot p = \text{ refl}_y \text{ и } p \cdot p^{-1} = \text{ refl}_x$$

$$(iii) (p^{-1})^{-1} = p$$

$$(iv) (p \cdot q) \cdot r = p \cdot (q \cdot r)$$

(i) Доказ. Желимо да конструишемо путању

$$\text{unit}_l(p) : \text{ refl}_x \cdot p = p,$$

$$\text{unit}_r(p) : p \cdot \text{ refl}_y = p.$$

Индукцијом по путањи $p : x =_A y$ довољно је конструисати

$$\text{unit}_l(\text{ refl}_x) : \text{ refl}_x \cdot \text{ refl}_x = \text{ refl}_x,$$

$$\text{unit}_r(\text{ refl}_x) : \text{ refl}_x \cdot \text{ refl}_x = \text{ refl}_x.$$

Обе путање је тривијално конструисати као $\text{ refl}_{\text{ refl}_x}$.

□

(ii) *Доказ.* Желимо да конструишемо путању

$$\begin{aligned} \text{inv}_l(p) : p^{-1} \cdot p &= \text{refl}_y, \\ \text{inv}_r(p) : p \cdot p^{-1} &= \text{refl}_x. \end{aligned}$$

Индукцијом по путањи $p : x =_A y$ довољно је конструисати путању

$$\begin{aligned} \text{inv}_l(\text{refl}_x) : \text{refl}_x^{-1} \cdot \text{refl}_x &= \text{refl}_x, \\ \text{inv}_r(\text{refl}_x) : \text{refl}_x \cdot \text{refl}_x^{-1} &= \text{refl}_x. \end{aligned}$$

Али како је $\text{refl}_x^{-1} \equiv \text{refl}_x$ претходне путање се свде на оне као и у претходном доказу. Због тога обе путање тривијално конструишемо као $\text{refl}_{\text{refl}_x}$. \square

(iii) *Доказ.* Желимо да конструишемо путању

$$\text{doubleInv}(p) : (p^{-1})^{-1} = p.$$

Индукцијом по путањи $p : x =_A y$ довољно је конструисати путању

$$\text{doubleInv}(\text{refl}_x) : (\text{refl}_x^{-1})^{-1} = \text{refl}_x.$$

Али како је $(\text{refl}_x^{-1})^{-1} \equiv \text{refl}_x^{-1} \equiv \text{refl}_x$ претходна путања се своди на $\text{refl}_x = \text{refl}_x$. Због тога путању тривијално конструишемо као $\text{refl}_{\text{refl}_x}$. \square

(iv) *Доказ.* Желимо да конструишемо путању

$$\text{assoc}_A(p, q, r) : (p \cdot q) \cdot r = p \cdot (q \cdot r).$$

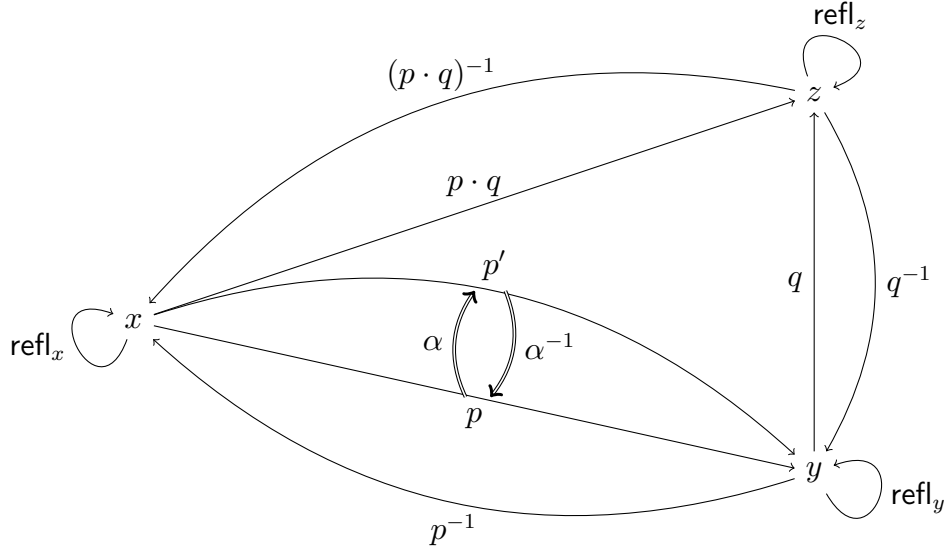
Индукцијом по путањи $p : x =_A y$ довољно је конструисати путању

$$\text{assoc}_A(\text{refl}_x, q, r) : (\text{refl}_x \cdot q) \cdot r = \text{refl}_x \cdot (q \cdot r)$$

Али како је $\text{refl}_x \cdot q \equiv q$ и $\text{refl}_x \cdot (q \cdot r) \equiv q \cdot r$ претходна путања се своди на

$$\text{assoc}_A(\text{refl}_x, q, r) : q \cdot r = q \cdot r.$$

Због тога путању тривијално конструишемо као $\text{assoc}_A(\text{refl}_x, q, r) :\equiv \text{refl}_{q \cdot r}$. \square



Слика 2.5: Групоидна структура типова.

Акције над путањама

Функција $f : A \rightarrow B$ се понаша као функтор у односу на путање. Другим речима, функције поштују једнакости, или функције одржавају путање. Ова особина дата је следећом лемом:

Лема 4. Нека су A и B типови, и нека је $f : A \rightarrow B$ функција у контексту Γ . Тада можемо конструисати функцију

$$\text{ap}_f : \prod_{(x,y:A)} (x =_A y) \rightarrow (f(x) =_B f(y))$$

индукцијом путање $p : x =_A y$ као $\text{ap}_f(\text{refl}_x) = \text{refl}_{f(x)}$. Функцију ap_f називамо акција над путањама функције $f : A \rightarrow B$.

Доказ. Индукцијом по путањи $p : x =_A y$ треба конструисати путању

$$\text{ap}_f(x, x, \text{refl}_x) : f(x) =_B f(x).$$

Тривијално конструирамо ову путању као $\text{ap}_f(x, x, \text{refl}_x) :\equiv \text{refl}_{f(x)}$. □

Важе уобичајене особине за функторе:

Лема 5. Нека су A, B и C типови, нека су елементи $x, y, z : A$ и нека су путање $p : x =_A y$ и $q : y =_A z$ у контексту Γ . Тада важи:

$$(i) \text{ap}_f(p \cdot q) = \text{ap}_f(p) \cdot \text{ap}_f(q)$$

$$(ii) \text{ap}_f(p^{-1}) = \text{ap}_f(p)^{-1}$$

$$(iii) \text{ap}_g(\text{ap}_f(p)) = \text{ap}_{g \circ f}(p)$$

$$(iv) \text{ap}_{\text{id}_A}(p) = p$$

Доказ. Доказ изостављамо како је сличан претходним. \square

Транспорт

Уколико посматрамо функцију $f : \prod_{(x:A)} B(x)$ и путању $p : x =_A y$, онда не можемо размазрати једнакост елемената $f(x) : B(x)$ и $f(y) : B(y)$, јер нису истог типа. Али можемо разматрати функцију $B(x) \rightarrow B(y)$, коју карактерише следећа лема:

Лема 6. *Нека је A тип и B фамилија типова над A у контексту Γ . Тада можемо конструисати функцију*

$$\text{tr}_B : \prod_{(x,y:A)} (x =_A y) \rightarrow B(x) \rightarrow B(y)$$

индукцијом упућање $p : x =_A y$ као $\text{tr}_B(\text{refl}_x) \equiv \text{id}_{B(x)}$. Функцију tr_B називамо транспорт над B .

Доказ. Индукцијом по путањи $p : x =_A y$ треба конструисати функцију

$$\text{tr}_B(x, x, \text{refl}_x) \rightarrow B(x) \rightarrow B(x).$$

Тривијално конструирамо ову путању као $\text{tr}_B(x, x, \text{refl}_x) \equiv \text{id}_{B(x)}$. \square

Фамилија типова B над типом A , може се сматрати као својство елемената типа A . Другим речима, $B(x)$ је својство елемента $x : A$. Због тога и претходне леме, можемо тврдити да својства поштују једнакости, у смислу да ако је $x =_A y$, онда $B(x)$ акко $B(y)$.

Друге врсте једнакости

Некада расуђивачка и исказна једнакост нису довољне да би се показале све тврдње. На пример, не можемо пронаћи сведоке за $\neg(\text{succ}_{\mathbb{N}}(n) =_{\mathbb{N}} 0_{\mathbb{N}})$ и $(\text{succ}_{\mathbb{N}}(m) =_{\mathbb{N}} \text{succ}_{\mathbb{N}}(n)) \rightarrow m =_{\mathbb{N}} n$ без следеће карактеризације:

Дефиниција 2.7.1. *Простор кодова* над природним бројевима \mathbb{N} се може дефинисати као бинарна релација $\text{code}_{\mathbb{N}} : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \mathcal{U}_0$ тако да задовољава следеће расуђивачке једнакости:

$$\begin{aligned}\text{code}_{\mathbb{N}}(0_{\mathbb{N}}, 0_{\mathbb{N}}) &\equiv \mathbb{1} \\ \text{code}_{\mathbb{N}}(0_{\mathbb{N}}, \text{succ}_{\mathbb{N}}(m)) &\equiv \mathbb{0} \\ \text{code}_{\mathbb{N}}(\text{succ}_{\mathbb{N}}(n), 0_{\mathbb{N}}) &\equiv \mathbb{0} \\ \text{code}_{\mathbb{N}}(\text{succ}_{\mathbb{N}}(n), \text{succ}_{\mathbb{N}}(m)) &\equiv \text{code}_{\mathbb{N}}(n, m)\end{aligned}$$

Лема 7. *Простор кодова је рефлексивна релација, тј. можемо конструисати функцију*

$$\text{reflcode}_{\mathbb{N}} : \prod_{(n:\mathbb{N})} \text{code}_{\mathbb{N}}(n, n).$$

Доказ. Функцију конструишемо индукцијом по $n : \mathbb{N}$ као

$$\begin{aligned}\text{reflcode}_{\mathbb{N}}(0_{\mathbb{N}}) &:\equiv \star \\ \text{reflcode}_{\mathbb{N}}(\text{succ}_{\mathbb{N}}(n)) &:\equiv \text{reflcode}_{\mathbb{N}}(n).\end{aligned}$$

□

Лема 8. *За било које природне бројеве $n, m : \mathbb{N}$ важи $m =_{\mathbb{N}} n \rightarrow \text{code}_{\mathbb{N}}(m, n)$ и $\text{code}_{\mathbb{N}}(m, n) \rightarrow m =_{\mathbb{N}} n$.*

Доказ. Прво конструишемо

$$\text{encode}_{\mathbb{N}} : \prod_{(m,n:\mathbb{N})} m =_{\mathbb{N}} n \rightarrow \text{code}_{\mathbb{N}}(m, n).$$

Индукцијом по путањи $p : m =_{\mathbb{N}} n$ треба конструисати

$$\text{encode}_{\mathbb{N}}(m, m, \text{refl}_m) : \text{code}_{\mathbb{N}}(m, m).$$

Што смо конструисали у претходној леми, тако да $\text{encode}_{\mathbb{N}}(m, m, \text{refl}_m) :\equiv \text{reflcode}_{\mathbb{N}}(m)$. Даље конструишемо

$$\text{decode}_{\mathbb{N}} : \prod_{(m,n:\mathbb{N})} \text{code}_{\mathbb{N}}(m, n) \rightarrow m =_{\mathbb{N}} n$$

индукцијом по $m : \mathbb{N}$ и $n : \mathbb{N}$. У случају када су оба природна броја нуле, онда $\text{decode}_{\mathbb{N}}(0_{\mathbb{N}}, 0_{\mathbb{N}}, c) : 0_{\mathbb{N}} =_{\mathbb{N}} 0_{\mathbb{N}}$ конструишемо као $\text{decode}_{\mathbb{N}}(0_{\mathbb{N}}, 0_{\mathbb{N}}, c) :\equiv \text{refl}_{0_{\mathbb{N}}}$. У

случају када је тачно један од њих нула, тада конструишемо елемент типа $\emptyset \rightarrow m =_{\mathbb{N}} n$. Овај елемент је тривијално конструисати правилом индукције празног типа. На крају, у случају када су оба различита од нуле, треба конструисати

$$\text{code}_{\mathbb{N}}(\text{succ}_{\mathbb{N}}(m), \text{succ}_{\mathbb{N}}(n)) \rightarrow \text{succ}_{\mathbb{N}}(m) =_{\mathbb{N}} \text{succ}_{\mathbb{N}}(n).$$

Ову конструкцију изводимо на следећи начин:

$$\begin{aligned} \text{code}_{\mathbb{N}}(\text{succ}_{\mathbb{N}}(m), \text{succ}_{\mathbb{N}}(n)) &\equiv \text{code}_{\mathbb{N}}(m, n) && (\text{деф. 2.7.1}) \\ &\rightarrow m =_{\mathbb{N}} n && (\text{decode}_{\mathbb{N}}(m, n)) \\ &\rightarrow \text{succ}_{\mathbb{N}}(m) =_{\mathbb{N}} \text{succ}_{\mathbb{N}}(n) && (\text{ap}_{\text{succ}_{\mathbb{N}}}). \end{aligned}$$

Коначно, завршавамо конструкцију са

$$\text{decode}_{\mathbb{N}}(\text{succ}_{\mathbb{N}}(m), \text{succ}_{\mathbb{N}}(n), c) :\equiv \text{ap}_{\text{succ}_{\mathbb{N}}}(\text{decode}_{\mathbb{N}}(m, n, c)).$$

□

Глава 3

AGDA

AGDA је типски завијан програмски језик који проширује MLTT. Језик AGDA подсећа на функционалне програмске језике као што је HASKELL, али их проширује зависним типовима. Са друге стране, AGDA је интерактивни доказивач теорема. Њена предност у односу на друге интерактивне доказиваче је минималност, и високи степен модуларности и изражајности. То је чини идеалним интерактивним доказивачем за формализовање MLTT-а, па самим тим и HoTT-а.

3.1 Основе језика AGDA

AGDA програми се развијају интерактивно, што значи да је могуће верификовати ограничења типова (енгл. *type check*) иако код није комплетно написан. Програм који извршава верификацију ограничења типова назива се *проверивач типова* (енгл. *typechecker*). Код може садржати празнине које се могу допунити касније. Многи текстуални едитори подржавају интерактивни развој AGDA програма: EMACS, VIM, АТОМ, VISUAL STUDIO CODE.

Када се интерактивно развија AGDA програм користе се команде које пружају информације од проверивача типова, као и начине на које можемо обрађивати празнине. Неке од корисних команда су:

C-c C-l: Учитава фајл и извршава верификацију ограничења типова. Свако појављивање знак ? замењује са новом празнином.

C-c C-d: Одређује тип датог израза.

- C-c C-n: Нормализује дати израз.
- C-c C-f: Поставља курсор на прву следећу празнину.
- C-c C-b: Поставља курсор на прву претходну празнину.
- C-c C-,: Приказује очекивани тип празнине на којој се налази курсор, као и типове свих променљивих из контекста.
- C-c C-c: Раздваја променљиву на све могуће случајеве.
- C-c C-SPC: Замењује празнину датим изразом, ако је дати израз одговарајућег типа.
- C-c C-r: Прерађује празнину тако што је замени са изразом заједно са новим одговарајућим празнинама.
- C-c C-a: Аутоматски покушава да пронађе одговарајући израз за празнину на којој се налази курсор.
- C-x C-c: Преводи програм.

Прођимо кроз један основни пример. Како се име сваког AGDA фајла завршава екстензијом `.agda`, нека се наш фајл зове `Tutorial.agda`.

На почетку фајла описујемо неке мета-податке:

```
{-# OPTIONS -without-K -safe #-}
```

У овом случају то су опције `-without-K` и `-safe`, које обезбеђују сигурну аксиоматизацију унивалантности. Без ових опција дошло би до контрадикције.

AGDA програм је сачињен од *модула*. Сваки модул има своје име (које мора да се поклопи са именом фајла) као и низ декларација. Модул за наш фајл `Tutorial.agda` започињемо на следећи начин:

```
module Tutorial where
```

Једна врста декларација је увожење других модула. Тако, на пример, можемо увести модул `Universes` на следећи начин:

```
open import Universes public
```

Друга врста декларација је декларисање променљивих. На пример, можемо рећи да \mathcal{U} , \mathcal{V} и \mathcal{W} представљају универзум:

variable $\mathcal{U} \ \mathcal{V} \ \mathcal{W} : \text{Universe}$

Једна од кључних декларација је декларација индуктивних типова. Декларисање индуктивних типова подразумева навођење имена тог типа, начин на који се он формира, као и начин за конструисање каноничних елемената тог типа. У теорији типова, то смо називали правило формирања типова и правила конструисања. Подсетимо се правила формирања и правила конструисања типа природних бројева \mathbb{N} . Тип природних бројева \mathbb{N} може да се формира из празног контекста, односно $\mathbb{N} : \mathcal{U}_0$, као и да су му једини конструктори $0_{\mathbb{N}} : \mathbb{N}$ и $\text{succ}_{\mathbb{N}} : \mathbb{N} \rightarrow \mathbb{N}$. У језику AGDA то записујемо као:

```
data  $\mathbb{N} : \mathcal{U}_0 \cdot$  where
  zero :  $\mathbb{N}$ 
  succ :  $\mathbb{N} \rightarrow \mathbb{N}$ 
```

```
{-# BUILTIN NATURAL  $\mathbb{N}$  #-}
```

Поред правила формирања и правила конструисања, за комплетну спецификацију индуктивних типова имали смо и правило индукције и правило израчунавања. Правило индукције типа природних бројева \mathbb{N} , у језику AGDA записујемо као:

```
 $\mathbb{N}$ -induction : ( $P : \mathbb{N} \rightarrow \mathcal{U}_0 \cdot$ )
   $\rightarrow P \ 0$ 
   $\rightarrow ((n : \mathbb{N}) \rightarrow P \ n \rightarrow P \ (\text{succ } n))$ 
   $\rightarrow (n : \mathbb{N}) \rightarrow P \ n$ 
```

Са друге стране, правила израчунавања записујемо као:

```
 $\mathbb{N}$ -induction  $P \ p_0 \ p_s \ \text{zero} = p_0$ 
 $\mathbb{N}$ -induction  $P \ p_0 \ p_s \ (\text{succ } n) = p_s \ n \ (\mathbb{N}\text{-induction } P \ p_0 \ p_s \ n)$ 
```

У многим случајевима AGDA може помоћи при декларисању правила израчунавања. Како она описују начин конструисања елемента који оправдава правило индукције можемо поћи од:

```
 $\mathbb{N}$ -induction  $P \ p_0 \ p_s \ n = \{! \ !\}$ 
```

Командом `C-c C-c` раздвајамо `n` на случајеве:

```
N-induction P po ps zero = {! !}
N-induction P po ps (succ n) = {! !}
```

Командом `C-c C-a` аутоматски решавамо први случај, док на други примењујемо `C-c C-r` над изразом `ps`:

```
N-induction P po ps zero = po
N-induction P po ps (succ n) = ps {! !} {! !}
```

На првом пољу, командом `C-c C-.`, сазнајемо да је потребно конструисати тип \mathbb{N} , као и да је у контексту $n : \mathbb{N}$. Због тога, једноставно, попуњавамо поље са `n` командом `C-c C-SPC`. На другом пољу, командом `C-c C-.`, сазнајемо да је потребно конструисати тип $P(n)$ за $n : \mathbb{N}$. Приметимо да је `N-induction` функција која враћа $P(n)$, те примењујемо команду `C-c C-r` над `N-induction P`.

```
N-induction P po ps zero = po
N-induction P po ps (succ n) = ps n (N-induction P {! !} {! !} {! !})
```

Преостала поља можемо једноставно попити аутоматски помоћу команде `C-c C-a`, или разматрањем траженог типа и контекста помоћу команде `C-c C-.`, а онда уписивањем одговарајућих израза помоћу команде `C-c C-SPC`.

3.2 Резултат

Као резултат овог рада настала је библиотека, у којој су формализовани основни појмови МЛТТ-а, а која је даље спремна за надоградњу и даље развијање ХОТТ-а. Комплетна библиотека може да се нађе на <https://github.com/andrija-urosevic/master-rad-hott/agda>. Библиотека укључује:

- Основне индуктивне типове: празан тип 0 , јединични тип 1 , тип копроизвода $A + B$, Булов тип 2 , тип зависних парова $\sum_{(x:A)} B(x)$ и тип парова $A \times B$.
- Типови идентитета: индукција путањом, инверз путање, надовезивање путања, особине ∞ -групоида, акција над путањом, транспорт путање.

- Природни бројеви: основне операције ($+\mathbb{N}$, $\times\mathbb{N}$, биномни коефицијент, фибоначијеви бројеви, итд.), разне особине ових операција, релације (простор кодова $\text{code}_{\mathbb{N}}$ и неједнакости), разне особине ових релација, коначни тип Fin_n и његове особине.
- Основне операције и особине целих бројева.
- Основне операције и особине листи.
- Својства одлучивости дефинисаних типова.

Глава 4

Закључак

Основни циљ овог рада је био теоријско и практично изучавање МЛТТ-а као и формализација основних објеката и конструкција МЛТТ-а у типски зависном програмском језику AGDA. Као што је већ напоменуто, формализација у оквиру интерактивних доказивача се једина сматра формалном. Са једне стране, формализација у оквиру интерактивних доказивача нам доноси комплетност и прецизност тако што минимизује настанак грешке. Док са друге стране, представља исцрпан посао и укључује техничке вештине, које многи математичари не поседују. Штавише, рачунарци лако савладају техничке вештине, али им недостаје теоријско знање, и због тога МЛТТ, а и ХоТТ, представљају идеалну синергију између математике и рачунарства.

Као резултат овог рада настала је библиотека основних концепата МЛТТ-а. Како су формализовани основни концепти који су неопходни у ХоТТ-у, библиотека се може користити као почетна тачка за даљу надоградњу и изучавање ХоТТ-а. Поред тога, како у обиму садржи само основне концепте и конструкције, представља идеалан почетни извор за изучавање МЛТТ-а и ХоТТ-а. Већина других библиотека покушава да формализује што више математичког знања. Резултат тога су огромни графови зависности, који могу одбити новајлије у области.

Поред практичног резултата, овај рад покушава да помери границе фундаменталног бављена математиком. Пружа један алтернативни начин заснивања математике. Одбацује теорију скупова и класичну логику уводећи теорију типова као основни систем, у коме се, даље, формулишу појмови и доказују теореме на најригорознији могући начин. Методи доказивања теорема са класичног приступа прелазе на конструктивистички приступ, пружајући

прецизније и ефектније доказе. Свеобухватно, пружа један концизан и систематски начин рада.

Овај начин формализације математике се тренутно сматра најбољим, али и он има своја ограничења. Иако је велика база знања формализована, постоји још већа база генералног математичког знања која тек треба да се формализује. Са друге стране, сво то математичко знање се чува неформално и његова основа често није теорија типова. Често је за један неформалан доказ потребно и више од 1000 линија кода. Све то читав поступак формализације, у оквиру МЛТТ-а и ХоТТ-а, чини исцрпним, тешким, спорим и изазовним.

Даљи рад подразумева надоградњу тренутне библиотеке концептима из ХоТТ-а. Тиме се добија добра основа за формализовање генералног математичког знања у оквиру ХоТТ-а. Након тога, даљи рад може да се настави у два правца: (1) наставак развијања библиотеке напреднијим концептима и генералним математичким знањем; (2) формализација генералног математичког знања и доприност у развоју библиотека AGDA-UNIMATH и HOTT-AGDA.

Коначно, овај рад има за циљ да допринесе развоју ХоТТ-а, тако што ће привући људи из разних области и подстаћи их да изучавају ХоТТ и формализују математику. Срећно формализовање!

Литература

- [1] Guillaume Brunerie и др. *Homotopy Type Theory in Agda*. URL: <https://github.com/HoTT/HoTT-Agda>.
- [2] Cyril Cohen и др. *Cubical Type Theory: a constructive interpretation of the univalence axiom*. 2016. arXiv: 1611.02108 [cs.LG].
- [3] Thierry Coquand, Simon Huber и Anders Mörtberg. *On Higher Inductive Types in Cubical Type Theory*. 2018. arXiv: 1802.01170 [cs.LG].
- [4] Martín Hötzel Escardó. „Introduction to univalent foundations of mathematics with Agda”. У: *arXiv preprint arXiv:1911.00580* (2019).
- [5] Jackson Macor. *A brief introduction to type theory and the univalence axiom*. 2015.
- [6] Per Martin-Löf и Giovanni Sambin. *Intuitionistic type theory*. Св. 9. Bibliopolis Naples, 1984.
- [7] Ulf Norell. „Dependently typed programming in Agda”. У: *Proceedings of the 4th international workshop on Types in language design and implementation*. 2009, стр. 1–2.
- [8] Egbert Rijke. *Introduction to Homotopy Type Theory*. 2022. arXiv: 2212.11082 [math.LG].
- [9] The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. Institute for Advanced Study: <https://homotopytypetheory.org/book>, 2013.
- [10] Andrea Vezzosi, Anders Mörtberg и Andreas Abel. „Cubical Agda: A dependently typed programming language with univalence and higher inductive types”. У: *Journal of Functional Programming* 31 (2021), e8.

- [11] Vladimir Voevodsky, Benedikt Ahrens, Daniel Grayson и др. *UniMath — a computer-checked library of univalent mathematics*. available at <http://unimath.org>. DOI: 10.5281/zenodo.7848572. URL: <https://doi.org/10.5281/zenodo.7848572>.
- [12] Philip Wadler. „Propositions as Types”. У: *Commun. ACM* 58.12 (НОВ. 2015), стр. 75–84. ISSN: 0001-0782. DOI: 10.1145/2699407. URL: <https://doi.org/10.1145/2699407>.

ЛИТЕРАТУРА

Биографија аутора

Вук Стефановић Караџић (*Тршић, 26. октобар/6. новембар 1787. — Беч, 7. фебруар 1864.*) био је српски филолог, реформатор српског језика, сакупљач народних умотворина и писац првог речника српског језика. Вук је најзначајнија личност српске књижевности прве половине XIX века. Стекао је и неколико почасних доктората. Учествовао је у Првом српском устанку као писар и чиновник у Неготинској крајини, а након слома устанка преселио се у Беч, 1813. године. Ту је упознао Јернеја Kopитара, цензора словенских књига, на чији је подстицај кренуо у прикупљање српских народних песама, реформу ћирилице и борбу за увођење народног језика у српску књижевност. Вуковим реформама у српски језик је уведен фонетски правопис, а српски језик је потиснуо славеносрпски језик који је у то време био језик образованих људи. Тако се као најважније године Вукове реформе истичу 1818., 1836., 1839., 1847. и 1852.