0.1 Úvod

Pri procese rozširovania matematickej teórie vytvárame tvrdenia generalizujúce jej princípy. Ak chceme aby náša teória bola správna, všetky jej tvrdenia musia byť logicky odvodené z postulátov alebo tvrdení z nich odvodených. Potvrdenie správnosti tvrdenia, vyslovením predpokladu, axiómu alebo napísaním formule ktorú dostaneme aplikáciou dedukčného pravidla na niektoré v postupnosti predchádzajúce formule nazývame dôkazom.

Z kvalitatívneho hľadiska pri vyslovení dôkazu uvažujeme o všeobecnosti dôkazu a správnosti aplikácie dedukčného pravidla. O nutnosti korektného dokazovania tvrdení hovorí napríklad tvrdenie z teórie čísel o hornom ohraničení počtu prvočísel logaritmickým integrálom.

$$\pi(x) \leq \int_0^x \frac{1}{\ln t} dt \tag{1}$$

Tvrdenie bolo považované za správne Bernhardom Riemannom a evidencia to taktiež naznačovala. Neskôr sa ukázalo že tvrdenie nie je správne pri čísle pod hodnotou 10^{317}. Veta o 4 farbách ktorá bola vyslovená v roku 1852 Francisom Guthrie ktorá hovorí, že každá rovinná mapa je zafarbiteľná 4 farbami. Táto veta bola nesprávne dokázaná v roku Kempom (1879) and Taitom (1880). Kempov dôkaz bol vyvrátený o 10 rokov mapov s 18 stenami. Pri dôkaze tejto vety bol neskôr v roku 1977 Appelom and Hakenom z časti využitý počítač pre kontrolu špeciálnych diskrétnych prípadov.

0.2 Počítačom asistované dokazovanie

Specializacia Typy softverov a na akych principoch su zalozene, napr. programy pre asistovane dokazovanie je zalozena na dependent type theory

0.2.1 Výroková logika

V prípade že chceme aby výrokove formuly korenšpondovali s typmi. Ich booleova reprezentácia s hodnotami $1, 0$ je nahradená otázkou existencie prvkov v množine. V prípade implikácie o existencii funkcie v množine. Funkcie v programoch ale môžu mať pri rovnakých vstupoch a výstupoch mať rôznu výpočtovú zložitosť. Dôvod prečo by sme sa mali pozerať na dôkazy(podľa publikácie Gir11) v troch rovinách.

1. Booleovský - tvrdenia sú booleovské hodnoty, zaujímame sa o dokázateľnosť tvrdenia 2. Existenčný - tvrdenia sú množiny, aké funkcie môžu byť 3. Úmyselný - zaujímame sa o zložitosť vytvoreného dôkazu a ako sa zjednoduší cez (cut eliminitation)

Intuicionizmus

Tento posunu od eixstencie dôkazu k dokázateľnosti začal z filozfie Brouwer s počiatkom v 20. storočí sa nazývy intuitionizmus.

Z intuionistického pohľadu by mali byť premennné výrokových formúl interpretované ich dôkazy. Interpretácia formúl sa potom zmení

$A \wedge B$ ako $A \times B$

$A \vee B$ ako $A \sqcup B$ zjednotenie rozdielu

$A \implies B$ spôsob skonštruovania dôkazu B z dôkazu A

$\neg A = A \implies \perp$ existencie kontrapríkladu

Z tohto pohľadu bolo Brouwerom odmietnutý princíp ktorý platí v klasickej logike $\neg\neg A$

[Gir11] Jean-Yves Girard.The Blind Spot: lectures on logic. EuropeanMathematical Society, 2011

Formalizovanie dôkazu

Dôkaz z teórie usporiadania. Tak ako je Program = Proof

Otázka ohľadom konzistentnosti dôkazu. Otázka kontrola typov by mala byť rozhodnuteľná.

Definicia formuly, postupnosti, kontextu, fragmentov ktoré navazuju na typovy lambda calculus

0.2.2 Typový lambda calculus

0.2.3 Predikátová logika

0.2.4 Teória zavislostných typov

0.3 Lean-theorem-prover

Constracting proof

Forward proofs

assume

calc

fix

have

let

show

Backward proofs

cc

clear

exact

induction

intro

refl

refl

Inductive types

```
structure point :=
  ( x : nat )
  ( y : nat )

/-- alternative notation -/
structure point_alternative :=
  mk :: (x : nat) (Y : nat)

def p1 : point :=
```

```
{
  x   := 10,
  y   := 20,
}

/- same point, different notation, same notation for ordered seti -/
def p2 : point := $\langle 10, 20 \rangle$

/- instance only one part of structure, rest implicitly from other instance
def p3 : point := {
    x := 20,
    ..p
}
```

Type classes