Stability of intuitionistic verification systems

Sergei Artemov

PRL seminar

Department of Computer Science

Cornell University

April 24, 2000

Plan:

1. Constructive existence
2. Provability and reflection
3. Stability of verification systems
4. Explicit verification
5. Typical intuitionistic system is stable
6. Metamathematics of stability

1. Constructive existence

Classical $\exists$ is not constructive: $\exists x F \ \sim \ \neg\forall x \neg F$

Cla ical logic cannot di tingui h between

$\exists x A \to \exists y B \quad \sim \quad \forall x \exists y (A \to B) \quad \sim \quad \exists y \forall x (A \to B)$

(implici func ion) func ion) (cons n)

positive $\exists$'s are constructive

$\exists x F$ *s ronger h n* $\neg\forall x \neg F$

$\vdash \exists x F(x) \quad \Rightarrow \quad \vdash F(t)$ *fo some ground erm* t

$\vdash \forall x \exists y G(x, y) \quad \Rightarrow \quad \vdash \forall x G(x, f(x))$ *some erm* $f(x)$

logic all three p

function a ove.

Negative $\exists$ are not quite con tructive

$\neg\exists x F \ \sim \ \forall x \neg F, \ (\exists x A(x) \to C) \ \sim \ \forall x (A(x) \to C)$

re cla ically true ell

2. rovability and reflection

(- a con i tent theory containing arith etic)

Adequacy: $\mathit{Proof}_T(p, F) \Leftrightarrow p$ *is a proof of* F

$\mathit{Prew}_T(F) = \exists p \mathit{Proof}_T(p, F) \sim$ *"F is provable"*

" is consis en " = Consis $= \neg \mathit{Prew}_T(\mathit{false})$

Reflec ion scheme: $\mathit{Prew}_T(\phi) \to$

Gödel Incompleteness Theorem: $\nvdash$ *Consis*

Consistency is a special case of reflection:

$$\neg \mathit{Prew}_T(\mathit{false}) = \mathit{Prew}_T(\mathit{false}) \to \mathit{false}$$

Reflection is not provable:

$$\nvdash \mathit{Prew}_T(\;) \to$$

Explicit reflection is provable: *for each specific* p

$$\vdash \mathit{Proof}_T(p, \phi) \to$$

3. Stability of veri cation systems

The co on architecture of verification y te : a - u e that a all core y te i correct and extend it by internally verified fact and rule . Stability: ex- tended y te =

S abili y: $V = V + \mathcal{R}$ for every verified rule $\mathcal{R}$

Let $\Box_{\mathcal{R}}$ denote the prov.ilit y in $V + \mathcal{R}$

Theorem (contrary to a clai by Davi -Schwartz)

A s abili y scheme $\forall F[\Box_{\mathcal{R}} F \leftrightarrow \Box F]$ *is in ern lly prov ble*

Proof An induction on a proof in $V + \mathcal{R}$ in ide V.

However doe not yield that the "real" ta-

bility i prov.ble in

We try $V \vdash ,\ \Rightarrow\ V$

$V \vdash \Box,\ \Rightarrow\ V \vdash \Box\mathcal{R}$

$V \vdash \Box\mathcal{R}(,)\ \Rightarrow\ V \vdash$

4. Explicit veri cation

Explici ly verified rule:

there i a co puta le ter f t f nn ny p f f p f f

V $\forall$ proof $\{p, p,$

5. Typical intuitionistic system

Co s ruc ive proper ies:

Disjunc ion Proper y

$$V \vdash A \lor B \ \Rightarrow\ V \vdash A \text{ or } V \vdash B$$

Explici Defin bili y for Numbers

$$V \vdash \exists x A(x \quad V \vdash A(n) \text{ for } \text{ o } \text{ e } n$$

Explici Defin bili y

$$V \vdash \forall x \exists y A(x, y) \quad V \vdash \forall x A(x, f$$

for o e co puta le ter f

Independence of Premises

$$V \vdash A \to \exists y B(y \qquad V \vdash \exists y[A \to B$$

Corollary

A sys em wi h cons ruc ive proper ies is ble

Proof

$V \vdash \forall, [\Box, \qquad \Rightarrow \mathcal{R}(,)]$ *verified rule*

$V \vdash \forall\forall y[Proof(x,,) \to \exists y Proof(y, \mathcal{R}(,))]$

$V \vdash \forall y[Proof(x,,) \to Proof(y, \mathcal{R}(,))]$

$V \vdash \forall[Proof(x,,) \to Proof(f(x), \mathcal{R}(,))]$ *for some compu ble erm* f

explicitly verified

For typical intuitioni tic y te con tructive prop- ertie are e ta li hed y con tructive (though

. Metamat ematics of stability

S abili y of classical verifica io sys ems –
require e antical et-theoretical propertie which cannot be e tabli hed con tructively, not auto atically a u ed even in athe atic

S abili y of i ui io is ic sys ems –
fduow fro the tandard propertie which are u ually for a typical intuitioni tic y te by con tructive ean