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: $\exists x F \sim \neg \forall x \neg F$

Classical logic cannot distinguish between
$\exists x A \rightarrow \exists y B \sim \forall x \exists y (A \rightarrow B) \sim \exists y \forall x (A \rightarrow B)$

(implicit function) (total function) (constant)

Intuitionistic positive $\exists$’s are constructive
$\exists x F$ is stronger than $\neg \forall x \neg F$
$\vdash \exists x F(x) \Rightarrow \vdash F(t)$ for some ground term $t$
$\vdash \forall x \exists y G(x, y) \Rightarrow \vdash \forall x G(x, f(x))$ for some term $f(x)$

Intuitionistic logic distinguishes all three presentations of functions above.

Negative $\exists$’s are not quite constructive
$\neg \exists x F \sim \forall x \neg F$, $(\exists x A(x) \rightarrow C) \sim \forall x (A(x) \rightarrow C)$
are classically true as well
2. Provability and reflection

(T - a consistent theory containing arithmetic)

Adequacy: \( \text{Proof}_T(p, F) \iff p \text{ is a proof of } F \)

\( \text{Bew}_T(F) = \exists p \text{Proof}_T(p, F) \sim "F \text{ is provable}" \)

"T is consistent" = \( \text{Consis } T = \neg \text{Bew}_T(\text{false}) \)

Reflection scheme: \( \text{Bew}_T(\phi) \to \phi \)

\text{Gödel Incompleteness Theorem: } T \not\vdash \text{Consis } T

Consistency is a special case of reflection:

\( \neg \text{Bew}_T(\text{false}) = \text{Bew}_T(\text{false}) \to \text{false} \)

Reflection is not provable:

\( T \not\vdash \text{Bew}_T(\phi) \to \phi \)

Explicit reflection is provable: \text{ for each specific } p

\( T \vdash \text{Proof}_T(p, \phi) \to \phi \)
3. Stability of verification systems

The common architecture of verification systems: assume that a small core system is correct and extend it by internally verified facts and rules. Stability: extended system = original system.

**Rule:** computable function (relation) $\mathcal{R}$
Standard notation: $\vdash /\mathcal{R}(, )$
$(, \text{ a finite set of premises, } \mathcal{R}(, ) \text{ the conclusion})$

**Verified rule:** $V \vdash \forall, [\Box, \rightarrow \Box \mathcal{R}(, )]$
(here $\Box F$ is $\text{Bew}_V(F)$)

**Derived rule:** $V \vdash \forall, \Box [, \rightarrow \mathcal{R}(, )]$

Every derived rule is verified but not vice versa.
Verified not derived rules: *generalization, renaming of free variables, formalization, Löb rule, Markov rule*, etc.
**Stability:** $V = V + \mathcal{R}$ for every verified rule $\mathcal{R}$

Let $\Box_{\mathcal{R}}$ denote the provability in $V + \mathcal{R}$

**Theorem** (contrary to a claim by Davis-Schwartz)
A stability scheme $\forall F[\Box_{\mathcal{R}} F \leftrightarrow \Box F]$ is internally provable

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

However: this does not yield that the ”real” stability is provable in $V$. Indeed, suppose $\mathcal{R}$ is verified, i.e. $V \vdash \forall, [\Box, \rightarrow \Box \mathcal{R}(, ,)]$. We have to establish that $V + \mathcal{R} \vdash F \Rightarrow V \vdash F$. Try induction on a proof in $V + \mathcal{R}$.

For the induction step we have to show that

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

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

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

$V \vdash \Box \mathcal{R}(, ,) \Rightarrow V \vdash \mathcal{R}(, ,)$ reflection is needed!
4. Explicit verification

*Explicitly verified rule:* there is a computable term $f$ which for any proof $p$ of premises returns a proof $f(p)$ of the conclusion

$$V \vdash \forall, \forall p [\text{Proof}(p, ,) \rightarrow \text{Proof}(f(p), \mathcal{R}(, ,))]$$

**Theorem** For any explicitly verified rule $\mathcal{R}$ there is a total computable function $g$ which transforms any proof $n$ of $F$ in $V + \mathcal{R}$ into a proof $g(n)$ of $F$ in $V$

$$\text{Proof}_\mathcal{R}(n, F) \Rightarrow \text{Proof}(g(n), F)$$

This theorem is a stability device:

$$V + \mathcal{R} \vdash F \Rightarrow \quad (\text{by formalization})$$

$$\text{Proof}_\mathcal{R}(n, F) \text{ holds for some } n \in \omega \Rightarrow (\text{by the theorem})$$

$$\text{Proof}(g(n), F) \Rightarrow \quad (\text{by the adequacy of Proof})$$

$$V \vdash F$$
5. Typical intuitionistic system

*Constructive properties:*

*Disjunction Property*
\[ V \vdash A \lor B \Rightarrow V \vdash A \text{ or } V \vdash B \]

*Explicit Definability for Numbers*
\[ V \vdash \exists x A(x) \Rightarrow V \vdash A(n) \text{ for some } n \]

*Explicit Definability*
\[ V \vdash \forall x \exists y A(x, y) \Rightarrow V \vdash \forall x (A(x, f(x))) \]
for some computable term \( f \)

*Independence of Premises*
\[ V \vdash A \rightarrow \exists y B(y) \Rightarrow V \vdash \exists y [A \rightarrow B(y)] \]
(for \( A \) is \( \exists, \lor \)-free, \( A \) is decidable, etc.)
Corollary

A system with constructive properties is stable

Proof

\[ \forall, [\Box, \rightarrow \Box C (, )] \quad \text{verified rule} \]

\[ \forall, \forall x[Proof(x, , ) \rightarrow \exists y Proof(y, C (, ))] \]

\[ \forall, \forall x \exists y[Proof(x, , ) \rightarrow Proof(y, C (, ))] \]

\[ \forall, \forall x[Proof(x, , ) \rightarrow Proof(f(x), C (, ))] \quad \text{for some computable term } f \]

\[ \Rightarrow C \text{ is explicitly verified} \]

For a typical intuitionistic system constructive properties are established by constructive (though not internally formalizable) means
6. Metamathematics of stability

Stability of classical verification systems - requires semantical set-theoretical properties which cannot be established constructively, not automatically assumed even in mathematics.

Stability of intuitionistic systems - follows from the standard properties which are usually established for a typical intuitionistic system by constructive means.