EXPLICIT MODAL LOGICS
of single-conclusion proof systems

Vladimir Krupski (MSU)

Joint work with

Sergei Artemov (CUNY) and Nikolai Krupski (MSU)

September 2005

Formal proof theory T – a theory in which the human arguments about proofs and provability should be formalized.

Requirements:

- encodings for formulas, proofs and programs
- $Provable(x)$ – "x is provable"
- $Proof(x,y)$ – "x is a proof of y"

Suitable candidates: $T = PA, ZF, \ldots$

But all of them are VERY UNFRIENDLY in this role: axioms and rules say nothing about proofs and provability.

Improvements – proof theoretical interfaces for T:

$Provable$ — modal provability logics (**GL**/**S4**)
$Proof$ — logics of proofs (**FPL**/**LP**)

Verification of decision procedures.

$$Decide(\ulcorner\varphi\urcorner) \longrightarrow \begin{cases} \text{yes } (\varphi \text{ is valid}) \\ \text{fail} \end{cases}$$

"Private" verification (for oneself):

establish $\quad Decide(\ulcorner\varphi\urcorner) = \text{yes} \Rightarrow Provable(\ulcorner\varphi\urcorner)$.

"Public" verification:

construct $\boxed{t}$ s.t. $\quad Decide(\ulcorner\varphi\urcorner) = \text{yes} \Rightarrow Proof(t, \ulcorner\varphi\urcorner)$,

$\boxed{\text{distribute } t + \text{trusted } ProofChecker().}$

Core proof logic language:

$$\left.\begin{array}{l} p_0, p_1, \ldots \text{ – proof variables} \\ !^1, \times^2 \text{ – operations on proofs} \end{array}\right\} \longmapsto \mathbf{Tm}$$

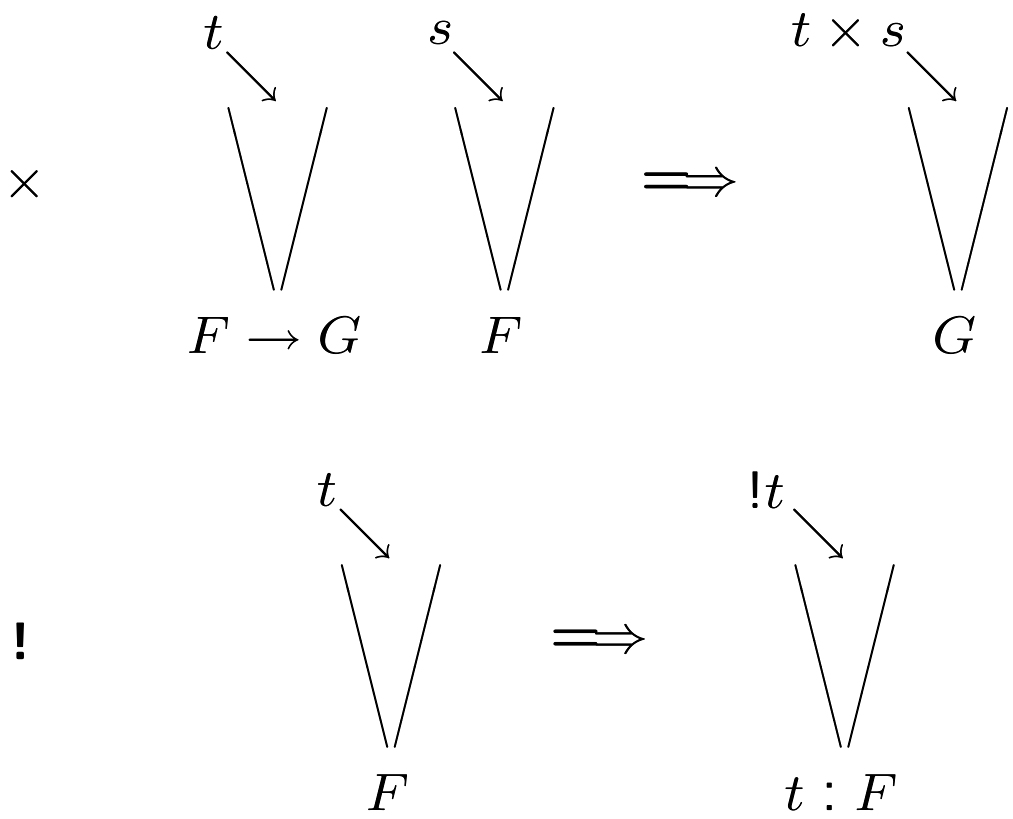
$$\left.\begin{array}{l} S_0, S_1, \ldots \text{ – sentence variables} \\ \neg, \vee, \wedge, \rightarrow, (\_ : \_) \end{array}\right\} \longmapsto \mathbf{Fm}$$

$$\frac{t \in \mathbf{Tm}, \quad F \in \mathbf{Fm}}{(t : F) \in \mathbf{Fm}}$$

Informal semantics:

$t : F$ – the arithmetical statement "t proves F",

$\times, !$ – act on proof codes:



Single-valued proof predicates – reflect the external derivations:

"x is a code of a derivation and
y is the code of its last formula"

$p{:}F \wedge p{:}G \Rightarrow F = G$	How to formalize this without "=" ?

$$t_1{:}F_1 \wedge \ldots \wedge t_n{:}F_n \longmapsto S{:=}\{\, t_i = t_j \Rightarrow F_i = F_j \mid 1 \le i,j \le n \,\}$$

Def: A unifier σ of S is a substitution s.t. $t_i\sigma \not\equiv t_j\sigma$ or $F_i\sigma \equiv F_j\sigma$ holds for every i,j.
Def: $A = B\,(mod\,S)$ iff $A\sigma \equiv B\sigma$ for every unifier σ of S.
Lemma: *The relation* $A = B\,(mod\,S)$ *is decidable.*

Unification axioms:

$$t_1{:}F_1 \wedge \ldots \wedge t_n{:}F_n \rightarrow (A \leftrightarrow B) \text{ when } A = B\,(mod\,S).$$

System **FLP** (Single-conclusion proof logic)

A0. Propositional axioms and rules
A1. $t{:}(F \to G) \to (s{:}F \to ts{:}G)$
A2. $t{:}F \to F$
A3. $t{:}F \to !t{:}(t{:}F)$
A4. Unification axioms

Theorem 1: **FLP** is sound and complete w.r. to arithmetical provability interpretations based on single-valued proof predicates.

Theorem 2: **FLP** is decidable.

Theorem 3: The rule with a scheme $\dfrac{F_1, \ldots, F_n}{F}$ is **PA**-admissible iff **FLP**$\vdash F_1 \wedge \ldots \wedge F_n \to F$.
Moreover, all the operations on **PA**-derivations induced by admissible rules of this kind can be represented by proof terms (Lifting Lemma).

Language extension by references

Ex: $\texttt{goal}(t)$ such that $\quad t : F \ \Rightarrow\ \texttt{goal}(t) = F \qquad \forall t, F$

Axiom scheme: $\boxed{t : F \rightarrow t : \texttt{goal}(t)}$

NB: $\texttt{goal}$ cannot be a constant function symbol here:

$(A \wedge B)$ and $\texttt{goal}(t)$ must be unifiable, otherwise

$t{:}(A \wedge B),\ t{:}\texttt{goal}(t) \vdash \bot$ (from Unification axiom).

So, $\vdash \neg t{:}(A \wedge B)$. The same with $\neg, \vee, \rightarrow, :$.

$\boxed{\texttt{goal()} \text{ is SO variable, or reference}}$

We use more powerful unification algorithm that can deal with SO variables. The set of all Unification axioms is still decidable.

Example with pattern matching:

$\mathtt{refl}(t)$ such that $\quad t:(s:F) \Rightarrow \mathtt{refl}(t) = s \qquad \forall t, s, F$

Axiom scheme: $\boxed{t:\underbrace{(s:F)}_{\varphi(s)} \to t:(\mathtt{refl}(t):F)}$

Here $\varphi(x)$ is a pattern, x is a metavariable.

$t \longmapsto G := \mathtt{goal}(t) \longmapsto \mathtt{match}\ G\ \mathtt{with}\ \varphi(x); \mathtt{return}\ x.$

General case:

$\mathtt{f}(t)$ such that $\quad t:\varphi(\ldots, Y, \ldots) \Rightarrow \mathtt{f}(t) = Y;$

$\varphi = F_0 \wedge p_1 : F_1 \wedge \ldots \wedge p_n : F_n$ where $F_i = F_i(p_1, \ldots, p_n; S_1, \ldots, S_m)$.

System $\mathbf{FLP}_{ref}$ $= \mathbf{FLP} +$ (all references)

The scope of Unification axioms (*A4*) now includes references. The semantics of $A = B\,(mod\,S)$ relation involves Second Order unification, but in restricted form which still remains decidable.

Theorems 1',2',3'. $\mathbf{FLP}_{ref}$ *is decidable, sound and complete w.r. to arithmetical single-conclusion proof interpretations. It provides the same admissibility test for arithmetical inference rules specified by schemes in* $\mathbf{FLP}_{ref}$*-language.*

Ex:

$\texttt{is\_proof}(t) := t : \texttt{goal}(t)$ means "t is a complete proof";

$\exists \bar{x}_{t:\varphi(\bar{x})} F(\bar{x}) := t : \varphi(\overline{\mathrm{g}}(t)) \wedge F(\overline{\mathrm{g}}(t))$;

$\forall \bar{x}_{t:\varphi(\bar{x})} F(\bar{x}) := t : \varphi(\overline{\mathrm{g}}(t)) \to F(\overline{\mathrm{g}}(t))$.

$$\frac{\texttt{is\_proof}(p)}{\texttt{goal}(p)} \qquad \frac{\texttt{is\_proof}(p)}{\texttt{refl}(!p) : \texttt{goal}(p)} \qquad \frac{p : \neg\texttt{goal}(p)}{\bot}$$

$$\frac{\exists S_0, S_{1\,p_0:(S_0 \to S_1)}\, p_1 : S_0}{\texttt{is\_proof}(p_0 p_1)}$$

Reflexive combinatory logic

RCL$_\rightarrow$ (Artemov, 2003), extends **CL**$_\rightarrow$ (Curry).

$$!t, \quad t \cdot s, \quad t : F, \quad F \rightarrow G$$

Rigid typing: x_i^F (typed proof variables);

$\mathbf{k}^{(\dots)}$ $\mathbf{s}^{(\dots)}$, $\mathbf{d}^{(\dots)}$, $\mathbf{o}^{(\dots)}$, $\mathbf{c}^{(\dots)}$ (typed proof constants).

Inductive definitions for two judgements:

- "F is well formed formula"
- "$\Gamma \vdash F$"

For every t there is at most one F s.t. $t : F$ is well formed.

$\mathbf{RCL}_{\rightarrow}$, wf-rules:

Standard wf-rules from $\mathbf{CL}_{\rightarrow}$ for $\rightarrow$, $\cdot$, $\mathbf{k}^{(\ldots)}$, $\mathbf{s}^{(\ldots)}$;

$$\frac{F \textbf{ -wf}}{x_i^F : F \textbf{ -wf}} \qquad \frac{t : F \textbf{ -wf}}{!t : t : F \textbf{ -wf}} \qquad \frac{t : F \textbf{ -wf}}{\mathbf{d}^{\,t:F \rightarrow F} : (t : F \rightarrow F) \textbf{ -wf}}$$

$$\frac{u : (F \rightarrow G),\ v : F \textbf{ -wf}}{\mathbf{o}^{(\ldots)} : (\, u : (F \rightarrow G) \rightarrow (v : F \rightarrow uv : G)\,) \textbf{ -wf}}$$

$$\frac{t : F \textbf{ -wf}}{\mathbf{c}^{(\ldots)} : (\, t : F \rightarrow !t : t : F\,) \textbf{ -wf}}$$

"F **-wf**" is polynomial time decidable. (N. Krupski)

$\mathbf{RCL}_{\rightarrow}$, derivability:

Precondition: all formulas below must be well formed.

Axioms: $t{:}F \rightarrow F$

$\mathbf{k}^{(\dots)}{:}(F \rightarrow (G \rightarrow F))$

$\mathbf{s}^{(\dots)}{:}((F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H)))$

$\mathbf{d}^{(\dots)}{:}(t{:}F \rightarrow F)$

$\mathbf{o}^{(\dots)}{:}(u{:}(F \rightarrow G) \rightarrow (v{:}F \rightarrow uv{:}G))$

$\mathbf{c}^{(\dots)}{:}(t{:}F \rightarrow !t{:}t{:}F)$

Rule: $F \rightarrow G,\ F \vdash G$.

"$\Gamma \vdash F$" is $PSPACE$-complete. (N. Krupski)