Constructive decision via redundancy-free proof-search

Dominique Larchey-Wendling
TYPES team, ANR TICAMORE

LORIA – CNRS
Nancy, France

Second TICAMORE meeting
Marseille, Nov. 2017

Constructive termination of proof-search

- How constructive ?
  - Many different/competing conceptions of "constructive"
    - proof backed by algorithm (intuitive)
    - proof in Intui. Set Theory or Type Theory (formal)
    - proof mechanized in Coq (or Agda) (w/o axioms)
  - Post-check pen&pencil proofs are constructive (hard)
    - chains of results, each of which should be constructive
- Termination of backward proof-search ?
  - proof-search is well-founded (easy constructive argument)
  - proof-search is redundant (Dickson's lemma, König's lemma)

Overview of the talk

- Don't be afraid, no Coq code in this talk
  - but Inductive Type Theory notations (vs. Set Theory)
- Minimal intuitionistic logic and Relevant logic
  - as simple targets (one connective) of the method
  - but implicational relevant logic is significant
- Hilbert systems and Sequent systems
  - for clean definitions and completeness theorems
  - cut-elimination
  - absorption of contraction
- Replace König's lemma and Kripke/Dickson's lemma
  - almost full relations as constructive Well Quasi Orders

Hilbert system for (minimal) intuitionistic logic

- Positive implictional calculus

$$\frac{}{\vdash A \supset B \supset A}\;[K] \qquad \frac{\vdash A \supset B \quad \vdash A}{\vdash B}\;[MP]$$

$$\frac{}{\vdash (A \supset B \supset C) \supset (A \supset B) \supset (A \supset C)}\;[S]$$

- Coq implementation, the *type of proofs of* A <u>outright liar!</u>

$\texttt{Inductive HI\_proof} : \texttt{Form} \to \texttt{Set} :=$

$\quad | \; \texttt{K} \;:\; \forall A\ B, \quad \vdash A \supset B \supset A$

$\quad | \; \texttt{S} \;:\; \forall A\ B\ C, \quad \vdash (A \supset B \supset C) \supset (A \supset B) \supset (A \supset C)$

$\quad | \; \texttt{MP} \;:\; \forall A\ B, \quad \vdash A \supset B \to \vdash A \to \vdash B$

$\texttt{where}$ "$\vdash A$" $:= (\texttt{HI\_proof}\ A)$.

Hilbert system for (imp) relevance logic

```
Inductive HR_proof : Form → Set :=
    | id   : ∀A,       ⊢ A ⊃ A
    | pfx  : ∀A B C,   ⊢ (A ⊃ B) ⊃ (C ⊃ A) ⊃ (C ⊃ B)
    | comm : ∀A B C,   ⊢ (A ⊃ B ⊃ C) ⊃ (B ⊃ A ⊃ C)
    | cntr : ∀A B,     ⊢ (A ⊃ A ⊃ B) ⊃ (A ⊃ B)
    | mp   : ∀A B,     ⊢ A ⊃ B → ⊢ A → ⊢ B
where "⊢ A" := (HR_proof A).
```

Hilbert proof systems and decision

- Decidability: algorithm which decides if A has proof or not

$$\forall A, \{\texttt{inhabited}(\vdash A)\} + \{\neg\texttt{inhabited}(\vdash A)\}$$

- Decider: (proof-search) algorithm computes a proof of A (or not)

$$\forall A, (\vdash A) + (\vdash A) \to \texttt{False}$$

- Hilbert systems directly translate into inductive types
- Hilbert systems are very bad for proof-search
  - ND/λ-calculus ws. Hilbert/Combinatory Logic
  - try to program with combinators ...
  - find a `HI_proof` of $A \supset A$ ... (SKK)

Contructively deciders with sequents

$$\frac{}{A \vdash A}\,[id] \quad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \supset B}\,[impr] \quad \frac{\Gamma \vdash A \qquad B, \Delta \vdash C}{\Gamma, \Delta, A \supset B \vdash C}\,[impl]$$

$$\frac{\Gamma, A, A \vdash B}{\Gamma, A \vdash B}\,[cntr] \quad \frac{\Gamma \vdash B}{\Gamma, A \vdash B}\,[weak] \quad \frac{\Gamma \vdash A \qquad A, \Delta \vdash B}{\Gamma, \Delta \vdash B}\,[cut]$$

- A collection of sequent rules for each logic
  - Minimal Intuitionistic Logic = all these rules
  - Relevance Logic = no weakening (system LR1)
- Soundness/completeness wrt. Hilbert systems
  - Hilbert proof of $\vdash A \quad \leftrightsquigarrow \quad$ sequent proof $\emptyset \vdash A$
- Problems with sequent systems
  - the [*cut*]-rule is like the [*mp*]-rule
  - the [*cntr*]-rule forbids well-foundedness

Backward sequent proof-search termination ?

- Rules must have finite inverse images:
  - finitely many instance for a given conclusion sequent $\Gamma \vdash A$
  - remove the $[cut]$-rule
    - algorithmic cut-elimination (see Negri&Von Plato)
    - semantic cut-admissibility via phase semantics (see Okada)
- Backward application of rules well-founded ?
  - at some point, backward application must stop
  - cannot hold with contraction $[cntr]$-rule
  - absorb contraction in the other rules?

Absorbing contraction in other rules

- For CL, for IL with LJT (also called G4IP) (see Dyckhoff contraction-free)
- But LJ is not well-founded:

$$\frac{}{\Gamma, A \vdash A} \qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \supset B} \qquad \frac{\Gamma, A \supset B \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \supset B \vdash C}$$

- However LJ is redundant (with sets instead of multisets)
  - LJ has sub-formula property
  - any ∞ proof-search branch contains a duplicated sequent
- Terminate proof-search by detecting loops (history mechanism)
  - Any proof transformed into a loop-free proof
  - König's lemma + PHP

Absorbing contraction in relevance logic

- Solved by Kripke (see Riche&Meyer 99) with LR2

$$\frac{\Gamma \vdash A \quad B, \Delta \vdash C}{\Theta, A \supset B \vdash C} \quad \text{with condition}(A \supset B, \Gamma, \Delta, \Theta)$$

- condition$(A \supset B, \Gamma, \Delta, \Theta)$ a bit complicated to state formally
  - every formula $\neq A \supset B$ can be contracted once
  - $A \supset B$ can be contracted twice
- Rules have finite inverse image
- Curry's lemma:
  - contraction is height-preserving admissible
  - hence equivalence between (cut-free) LR1 and LR2

Review of decision argument for Relevant LR2 (i)

- $\Delta \vdash B$ is *redundant over* $\Gamma \vdash A$ (denoted $\Gamma \vdash A \prec_{\mathrm{R}} \Delta \vdash B$):
  - $\Gamma \vdash A$ obtained from $\Delta \vdash B$ by repeating $[\mathit{cntr}]$
  - $A = B$ and for any f, $|\Gamma|_f \prec_{\mathrm{R}}^{\mathbb{N}} |\Delta|_f$
  - $n \prec_{\mathrm{R}}^{\mathbb{N}} m$ iff $(n \leqslant m) \wedge (n = 0 \Leftrightarrow m = 0)$
- Redundancy is Well Quasi Order (WQO) (Kripke's lemma)
  - ∞ seq. have redundant pairs: $\forall (\mathcal{S}_n)_{n<\infty}, \exists i < j, \mathcal{S}_i \prec_{\mathrm{R}} \mathcal{S}_j$
- by Ramsey's theorem: finite direct products of WQOs is a WQO

$$\Gamma \vdash A \prec_{\mathrm{R}} \Delta \vdash B \quad \text{iff} \quad A \stackrel{\mathrm{SF}}{=} B \wedge \bigwedge_{f \in \mathrm{SF}} |\Gamma|_f \prec_{\mathrm{R}}^{\mathbb{N}} |\Delta|_f$$

- where SF is the finite set of sub-formulæ of the initial sequent

Decision arguments for LR2 (ii)

- every LR2 provable sequent has a redundancy-free proof
  - use Curry's lemma to remove redundancies
- redundancy-free proof-search terminates
  - every branch must be finite (Kripke's lemma)
  - the proof-search tree is finite (König lemma)
- a bunch of non-constructive arguments (see Riche 2005)
  - Kripke's lemma involves Dickson's lemma or IDP
  - König's lemma (infinite branch)
- we *constructivize theses arguments in an abstract setting*

Good sequences, bad sequences and redundancy

- For X : `Type` and $R : X \to X \to$ `Prop` $=$ `rel`$_2\, X$
- Given a sequence $(x_n)_{n<\infty} : \mathbb{N} \to X$, or a list $[x_0; \dots; x_{n-1}]$
  - when $i < j$, (x_i, x_j) is good if $x_i\ R\ x_j$ and bad if $\neg(x_i\ R\ x_j)$
  - We write `good` $R\ (x_n)_{n<\infty}$ iff $\exists i \exists j, i < j \wedge x_i\ R\ x_j$
  - We write `good` $R\ [x_0; \dots; x_{n-1}]$ iff $\exists i \exists j,\ i < j < n \wedge x_i\ R\ x_j$
  - And `bad` is simply $\neg$`good`, i.e. contains no good pair
- If R is a redundancy relation:
  - `good` R means there is a redundant pair
  - `bad` R means the sequence (or list) is irredundant

Almost full relations are inductive WQO

- For $X : \texttt{Type}$ and $R : X \to X \to \texttt{Prop} = \texttt{rel}_2\, X$
- Lifted relation: $x\ (R \uparrow u)\ y = x\ R\ y \lor u\ R\ x$
  - in $R \uparrow u$, elements above u are forbidden in bad sequences
- $\texttt{full} : \texttt{rel}_2\, X \to \boxed{\texttt{Prop}}$ and $\texttt{af}_t : \texttt{rel}_2\, X \to \boxed{\texttt{Type}}$

$$\frac{\forall x, y,\ x\ R\ y}{\texttt{full}\ R} \qquad \Bigg| \qquad \frac{\texttt{full}\ R}{\texttt{af}_t\ R} \qquad \frac{\forall u, \texttt{af}_t(R \uparrow u)}{\texttt{af}_t\ R}$$

- Almost full (AF) relations = constructive WQO
  - $\texttt{good}\ R\ [x_0; \ldots; x_{n-1}]$ iff $\exists i \exists j,\ i < j < n \land x_i\ R\ x_j$
  - if $\texttt{af}_t\ R$ then $\forall x : \mathbb{N} \to X, \{n : \mathbb{N} \mid \texttt{good}\ R\ [x_0; \ldots; x_{n-1}]\}$
  - $\texttt{af}_t\ R$, $\texttt{af}_t\ S$ imply $\texttt{af}_t(R \cap S)$ and $\texttt{af}_t(R \times S)$ (Coquand)
  - this is the $\boxed{\text{intuitionistic Ramsey theorem}}$

Kripke's lemma, constructively

- Remember

$$\Gamma \vdash A \prec_{\mathrm{R}} \Delta \vdash B \quad \text{iff} \quad A \overset{\mathrm{SF}}{=} B \wedge \bigwedge_{f \in \mathrm{SF}} |\Gamma|_f \prec_{\mathrm{R}}^{\mathbb{N}} |\Delta|_f$$

- when SF is finite, $\overset{\mathrm{SF}}{=}$ is almost full (PHP)
- the relation $\prec_{\mathrm{R}}^{\mathbb{N}} : \mathtt{rel}_2\, \mathbb{N}$ is almost full
- we get an AF relation as a (finite) intersection of AF relations
- from $\mathtt{af}_t(\prec_{\mathrm{R}})$ we deduce every ∞ sequence have redundant pairs
- but *what about König's lemma ?*

König's lemma replaced constructive FAN theorem

- Weak König's lemma = Brouwer's FAN thm (Schwichtenberg 05)
- Inductive FAN theorem (Fridlender 98)
  - the list of *choice sequences* for $[l_1; \ldots; l_n] : \texttt{list}(\texttt{list} X)$:

$$[x_1; \ldots; x_n] \in \texttt{list\_expo}\,[l_1; \ldots; l_n] \quad \text{iff} \quad x_1 \in l_1 \wedge \cdots \wedge x_n \in l_n$$

  - if $\texttt{af}_t\, R$ and $f : \mathbb{N} \to \texttt{list}\, X$ then

$$\left\{ n : \mathbb{N} \;\middle|\; \forall l \in \texttt{list\_expo}\,[f_0; \ldots; f_{n-1}], \texttt{good}\; R\; l \right\}$$

- Better than König's lemma, we get a uniform bound:
  - proof-search branches are choices sequences
  - of the proof-search iterator: $f_0 = [\mathcal{S}_0]$, $f_{1+n} = \texttt{next}\, f_n$
  - $\mathcal{H} \in \texttt{next}\, ll \quad \text{iff} \quad \exists \mathcal{C}, \mathcal{C} \in ll \wedge \dfrac{\cdots \quad \mathcal{H} \quad \cdots}{\mathcal{C}}$

Summary of the constructive argument

- Different refinements on proof:
  - `proof` is a tree where every node is a rule instance
  - n-bounded proof is a `proof` of height bounded by n
  - minimal proof = a `proof` of minimal height
  - everywhere minimal proof = every sub-proof is minimal
  - irredundant proof = every branch is bad (not good)
- We show:
  - $\mathcal{S}$ proof $\rightsquigarrow$ $\mathcal{S}$ has (everywhere) minimal proof
  - any everywhere minimal proof is irredundant (Curry's lemma)
  - irredundant proofs have n-bounded height (n by constr. FAN)

If $\mathcal{S}_0$ has a proof then it has a n-bounded proof

Mechanized redundancy-free decider

$$\texttt{Variables} \quad (\texttt{stm} : \texttt{Type}) \;\; (\texttt{rules} : \texttt{stm} \to \texttt{list stm} \to \texttt{Prop})$$

$$(H_{\texttt{rules}} : \forall c, \texttt{finite\_t}(\texttt{rules}\ c))$$

$$(\texttt{sf} : \texttt{rel}_2\ \texttt{stm})(\forall s, \texttt{sf}\, s\, s)(\forall r\, s\, t, \texttt{sf}\, r\, s \to \texttt{sf}\, s\, t \to \texttt{sf}\, r\, t)$$

$$(H_{\texttt{sf}} : \forall c\ hh, \texttt{rules}\ c\ hh \to \forall h \in hh, \texttt{sf}\ c\ h)$$

$$(\prec_{\mathrm{R}} : \texttt{rel}_2\ \texttt{stm})$$

$$(\texttt{Curry} : \forall s\ t\ p, \texttt{proof rules}\ t\ p \to s \prec_{\mathrm{R}} t$$

$$\to \exists q, \texttt{proof rules}\ s\ q \wedge \texttt{ht}\, q \leqslant \texttt{ht}\, p)$$

$$(\texttt{Kripke} : \forall s, \texttt{af}_t(\prec_{\mathrm{R}} \downarrow \texttt{sf}\ s))$$

$$\texttt{Thm decider} : \; \forall s, \{p \mid \texttt{proof rules}\ s\ p\} + \{\forall p, \neg\texttt{proof rules}\ s\ p\}$$

Mechanized constructive deciders

- Instantiate the `decider` term on minimal and relevance logics
  - for minimal IL, via LJ
  - for relevance logic, via LR2
- For e.g. relevance logic, we proceed as:
  - Hilbert to LR1, LR1 to cut-free LR1 (cut admissibility)
  - cut-free LR1 to LR2 (Curry's lemma)
  - LR2 to Hilbert
  - decider for LR2 (Curry's lemma and Kripke's lemma)

`Theorem HI_decider` $(f : \texttt{Form}) : \texttt{HI\_proof}\ f + (\texttt{HI\_proof}\ f \to \texttt{False})$

`Theorem HR_decider` $(f : \texttt{Form}) : \texttt{HR\_proof}\ f + (\texttt{HR\_proof}\ f \to \texttt{False})$