Mining Human Proofs from Machine Proofs

Big Proof / Isaac Newton Institute
Tuesday, 18 July 2017

Paulo Oliva
Queen Mary University of London
(joint work with Rob Arthan)
Is $A$ provable in $L$?

Is $E$ true in $C$?

Machine finds equational proof.

Logic

Equation

Reduce

Class of algebras

Recover natural deduction proof.
Case Studies

Uniqueness of halving in (minimal) continuous logic

Double negation of (double negation elimination)

Double negation translations (sub-structurally)
Logics and Algebras
Minimal Affine Logic

\[ \Gamma, A \vdash A \]

\[ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \]

\[ \frac{\Gamma \vdash A \quad \Delta \vdash A \rightarrow B}{\Gamma, \Delta \vdash B} \]

\[ \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B} \]

\[ \frac{\Delta, A, B \vdash C}{\Gamma \vdash A \otimes B} \]

\[ \frac{\Gamma \vdash A \otimes B}{\Gamma, \Delta \vdash C} \]
Further Axioms

- **EFQ:** \( \bot \vdash A \)
- **DNE:** \( \neg \neg A \vdash A \)
- **DIV:** \( A, A \rightarrow B \vdash B \otimes (B \rightarrow A) \)
- **CON:** \( A \vdash A \otimes A \)

* Assuming weakening
Nine Logics

Classical Affine Logic $\xrightarrow{DNE}$ Intuitionistic Affine Logic $\xrightarrow{EFQ}$ Minimal Affine Logic

INT

Classical Lukasiewicz Logic $\xrightarrow{DNE}$ Intuitionistic Lukasiewicz Logic $\xrightarrow{EFQ}$ Minimal Lukasiewicz Logic

DIV

Classical Logic $\xrightarrow{DNE}$ Intuitionistic Logic $\xrightarrow{EFQ}$ Minimal Logic
pocrim

$\langle X, \otimes, \rightarrow, \geq, 0 \rangle$

partially ordered commutative residuated integral monoid
hoops

pocrims satisfying

If $A \geq B$ then $A = B \otimes (B \to A)$

Buchi/Owens’74
Nine Algebras

involutive pocrims → involutive hoops → boolean algebras
bounded pocrims → bounded hoops → Heyting algebras
pocrims → hoops → Brouwer algebras
Case Study I
Continuous Logic
Continuous Logic

- Lukasiewicz logic with a halving operator axiomatised as:

\[
\frac{A}{2} \iff \frac{A}{2} \to A
\]

- Classically it's easy to show this uniquely defines the operation

- But how about in minimal logic?
...prover9
prover9

- Automated theorem prover for first-order and equational logic
- Successor of Otter
- Developed by Bill McCune
- Uses resolution and paramodulation

http://www.cs.unm.edu/~mccune/prover9/
Continuous Logic

- Wanted to show
  \[ X \leftrightarrow (X \rightarrow A) \quad Y \leftrightarrow (Y \rightarrow A) \]
  \[ \frac{X \leftrightarrow Y}{X \leftrightarrow Y} \]

- Proof found in about 3 mins (by prover9)

- Subsequently massaged into human-readable form by us
Lemma 2 Let $M = (M, 0, +, \rightarrow; \leq)$ be a hoop and let $a, b, c, x, y \in M$. If $a \rightarrow b = a$ and $c \rightarrow b = c$, then the following hold:

1. $b \geq a$ and $b \geq c$.
2. $a + a = b$.
3. $a \rightarrow (a \rightarrow c) = 0$.
4. $(x \rightarrow y) + z \geq x \rightarrow (y + (y \rightarrow x) + z)$.
5. $c \rightarrow (a + a + x) \geq c$.
6. $c \rightarrow a \geq a \rightarrow c$.
7. $c \rightarrow a = a \rightarrow c$.
8. $c + (c \rightarrow a) + ((a \rightarrow c) \rightarrow a) = b$.
9. $a + c = b$.

Theorem 3 In any hoop the following holds: if $a \rightarrow b = a$ and $c \rightarrow b = c$ then $a = c$.

Proof: By symmetry it is enough to show $c \geq a$. By Lemma 2 (9) we have $c \geq a \rightarrow b$ and hence $c \geq a$. 
Case Study II

\neg(\neg A \rightarrow A)
Deriving \( \neg(\neg A \rightarrow A) \) in IL:

\[
\begin{align*}
[\neg(\neg A \rightarrow A)] &_{\alpha} \quad \boxed{[A]_{\beta} \quad (WKN)} \\
\downarrow & \quad \neg A \\
\downarrow & \quad \beta \\
\neg A & \\
\boxed{[\neg A]_{\delta}} \\
\downarrow & \quad \boxed{A} \\
\downarrow & \quad \delta \\
\neg A & \quad \boxed{\neg(\neg A \rightarrow A)]_{\alpha}}
\end{align*}
\]
Is
\[-\neg(\neg\neg A \rightarrow A)\]
provable in
intuitionistic
Lukasiewicz logic?

Does
\[-\neg(\neg\neg x \rightarrow x) = 0\]
hold in all
bounded hoops?

Demo!
Able to find proofs using prover9

Initially, not much out of the proofs other than that the result was true but we started noticing some patterns…
Certain derived connectives kept appearing:

weak conjunction
\[ A \land B \equiv A \otimes (A \rightarrow B) \]

strong disjunction
\[ A \lor B \equiv (B \rightarrow A) \rightarrow A \]

strong implication
\[ A \Rightarrow B \equiv A \rightarrow A \otimes B \]

NOR, Peirce's ampheck
\[ A \downarrow B \equiv \neg A \otimes (B \rightarrow A) \]
prover9

extended theory

expand theory

proof of lemmas

prover9 proof

“defined” connective

spot

def. conn. properties

prover9

spot

spot
Lemma 4.2 (LL₁) \( A \otimes B \iff A \otimes (B \lor (A \Rightarrow B)) \)

Theorem 4.7 (LL₁) \( B \downarrow A \iff A \downarrow B \)

Corollary 4.8 (LL₁) \( (A \downarrow \downarrow \Rightarrow A) \downarrow \downarrow \)

**Proof:** Note that, since \( \bot \iff A \otimes A \downarrow \) we have (\(\ast\)) \( A \downarrow \downarrow \iff A \downarrow \Rightarrow A \). Moreover, it is easy to check that (\(\ast\ast\)) \( X \downarrow (Y \Rightarrow X) \iff X \downarrow \otimes (X \lor Y) \), for all \( X \) and \( Y \). Hence

\[
(A \downarrow \downarrow \Rightarrow A) \downarrow \iff ((A \downarrow \Rightarrow A) \Rightarrow A) \downarrow \downarrow
\]

(\(\ast\))

\[
\iff ((A \downarrow \Rightarrow A) \Rightarrow A) \downarrow \otimes (A \Rightarrow ((A \downarrow \Rightarrow A) \Rightarrow A))
\]

([WK])

(\text{def } \downarrow)

\[
\iff ((A \downarrow \Rightarrow A) \Rightarrow A) \downarrow A
\]

(Theorem 4.7)

\[
\iff A \downarrow ((A \downarrow \Rightarrow A) \Rightarrow A)
\]

(\(\ast\ast\))

\[
\iff A \downarrow \otimes (A \lor (A \downarrow \Rightarrow A))
\]

(Lemma 4.2)

\[
\iff A \downarrow \otimes A
\]

\[
\iff \bot.
\]
Case Study III
Double Negation Translations
Translations of $P \otimes (P \rightarrow Q)$

- Kolmogorov

$\neg \neg (\neg \neg P \otimes \neg \neg (\neg \neg P \rightarrow \neg \neg Q))$

- Gentzen

$\neg \neg P \otimes (\neg \neg P \rightarrow \neg \neg Q)$

- Glivenko

$(P \otimes (P \rightarrow Q))$
Translations of $P \otimes (P \rightarrow Q)$

$(\neg \neg \neg P \otimes \neg \neg \neg (\neg \neg \neg P \rightarrow \neg \neg \neg Q))$

$simplifications$

$\neg \neg P \otimes (P \rightarrow Q)$  \hspace{2cm} \neg \neg (P \otimes (P \rightarrow Q))$
Using CON we easily have:

\[ P \otimes Q \iff (P \otimes Q) \]

\[ P \rightarrow Q \iff (P \rightarrow Q) \]

which allows us to simplify Kolmogorov and obtain Gentzen and Glivenko

Ferreira/O.'12

Can the same be done with DIV?
Examples of lemmas:

"De Morgan" like properties:

\[ \neg(A \otimes B) \equiv A \rightarrow \neg B \]

\[ \neg(A \rightarrow B) \equiv \neg \neg A \otimes \neg B \]

\[ \neg(A \land B) \equiv A \Rightarrow \neg B \]

\[ \neg(A \Rightarrow B) \equiv \neg \neg A \land \neg B \]

\[ \neg(A \land B) \equiv \neg A \lor \neg B \]

\[ \neg(A \lor B) \equiv \neg A \land \neg B \]
Ampheck is definable in terms of conjunction and negation:

\[ A \downarrow B \equiv \neg A \land \neg B \]

Desired homomorphism properties:

\[ \neg (P \otimes Q) \iff \neg P \otimes \neg Q \]
\[ \neg (P \rightarrow Q) \iff \neg P \rightarrow \neg Q \]
Weak conjunction residuates strong implication:

\[(A \land B) \Rightarrow C \equiv A \Rightarrow (B \Rightarrow C)\]

- Found by Bob Veroff
- Yet to tease out human readable proof
Conclusions

- Successfully mined human-readable proofs from machine proofs
- Human input is identifying the “right” abstractions:
  - Find useful derived concepts
  - Recover an intuitive proof plan
- Automated support for proof refactoring?
- AI to automate human aspect?
- The late Bill McCune is the real star!