Automating Coherent Logic: an overview

Marc Bezem

Status as of Today

- ACL = NFR 177562/V30
  - PhD: Andrew Polonsky (UiB, Marc Bezem)
  - PostDoc: Roger Antonsen (UiO, Arild Waaler)
- Collaboration
  - John Fisher (CalPolytech, Pomona)
  - Hans de Nivelle (U Wroclaw)
  - Stefan Berghofer (TU Munich)

CL as a fragment of FOL

Coherent formula: $C \rightarrow D$, where

$C = A_1 \wedge \ldots \wedge A_n$ ($n \geq 0$, A_i atoms) and

$D = E_1 \vee \ldots \vee E_m$ ($m \geq 0$), where each

$E_j = \sum x_1 \ldots x_k .\ C_j$ ($\sum$ for `exists´, $k \geq 0$ and each C_j a conjunction of atoms).

Coherent theory = set of coherent formulas

CL ctnd

- Skolem (1920): lattices and projective geometry
- Extends Horn clauses and CNF (resolution)
- General form: $A_1 \wedge \ldots \wedge A_n \rightarrow$

  $\sum x\ .\ (A_{11} \wedge \ldots \wedge A_{1i}) \vee \ldots \vee \sum y\ .\ (A_{m1} \wedge \ldots \wedge A_{mj})$
- Applications in rewriting theory (confluence)
- E.g.: $red(x,y) \rightarrow x=y \vee \sum z.(step(x,z) \wedge red(z,y))$
- Ground forward chaining + case distinction + introduction of witnesses = sound and complete

Rationale

- More expressive than CNF (but ...)
- Skolemization not necessary
  - Skolemization changes meaning
  - Why skolemize $p(x,y) \rightarrow \sum z \,.\, p(x,z)$?
  - Skolem functions make the H-universe infinite
- Natural proof theory/objects (but ...)
- Middleground between resolution and the tableau-method for FOL

ACL goal

- Goal of ACL: build a competitive AR system (based on CL) for supporting FOL reasoning in proof assistants (ITP, logical frameworks) such as Coq and Isabelle.
- Working prototypes:
  - CL (Bezem): proof objects for Coq and Isabelle
  - Geolog (Fisher): only CL, no proof objects
  - Geo (de Nivelle): full FOL but no proof objects
  - (Isabelle) coherent (Polonsky, Berghofer)

Challenges

- A good translation FOL → CL
- Efficient proof search in CL
- Extension with native equality
- Proof objects all the way
- Integration in Coq, Isabelle

Translations from FOL to CL

- Bezem/Coquand LPAR’05, based on the tableau-method (disadvantage: too many $\vee$’s)
- de Nivelle/Meng IJCAR’06, eliminates all function symbols (!)
- Polonsky, minimizing $\vee$’s by playing with polarities
- Idempotent, preferably

Tableau translation by example

- Peirce's Law: $((p \rightarrow q) \rightarrow p) \rightarrow p$
- F,T: Prop $\rightarrow$ Prop `freezing their arguments´
- $F(((p \rightarrow q) \rightarrow p) \rightarrow p) \rightarrow T((p \rightarrow q) \rightarrow p) \wedge F(p)$
- $T((p \rightarrow q) \rightarrow p) \rightarrow (F(p \rightarrow q) \vee T(p))$
- $F(p \rightarrow q) \rightarrow T(p) \wedge F(q)$
- $F(p) \wedge T(p) \rightarrow false$

- To be refuted in CL: $F(((p \rightarrow q) \rightarrow p) \rightarrow p)$
- Proof + transformation on blackboard

Disadvantages

- Translation CL $\rightarrow$ CL not the identity!!
- Too many positive disjunctions (inefficient)
- Horror-example: Modus Ponens
  - $T(p \rightarrow q), T(p), F(q)$ (three facts)
  - $T(p \rightarrow q) \rightarrow F(p) \vee T(q)$
  - $T(p) \wedge F(p) \rightarrow false$
  - $T(q) \wedge F(q) \rightarrow false$
- Polonsky's translation improves on this

Proof techniques

- Ground forward reasoning
  - Depth-first (rule-order sensitive, incomplete)
  - Breadth-first (complete, can be slow)
  - Queueing depth-first (complete, new)
- Non-ground techniques
  - Based on tableaux and unification
  - Under development
  - Challenge: proof objects for Delta+

Geo2006/7 by Hans de Nivelle

- Implemented in C++
- Translation FOL → CL quite original
- Native (dis)equality
- Function symbols (eliminated in translation)
- Finite-model complete
- No proof objects (equisatisfiability)
- Participates in CASC

Geo2006/7 in CASC

Category	Geo2006	Geo2007	Winner07
FOF	73/150	104/300	270/300 Vampire
CNF	45/150	41/200	182/200 Vampire
SAT	51/100	54/100	96/100 Paradox
FNT	-	81/100	85/100 Paradox

Geo2006/7 format

- $A1 \wedge \ldots \wedge An \wedge x \neq x' \wedge \ldots \wedge y \neq y' \rightarrow Z$ with:
  - $Z = false$, or
  - $Z = B_1 \vee \ldots \vee B_m$ (non-equality atoms), or
  - $Z = \sum x.\ B$ (non-equality atom B)
- ONLY variables, NO constants, functions!!

Specialties of the translation

- unary predicates for constants: $c(x)$ for $c=x$
- $n+1$-ary predicates for n-ary functions
- ONLY disequalities:
  - $a=b$ expressed by $a(x) \wedge b(y) \wedge x \neq y \rightarrow \mathit{false}$
  - $b=c$ expressed by $b(x) \wedge c(y) \wedge x \neq y \rightarrow \mathit{false}$
  - $a \neq c$ expressed by $a(x) \wedge c(x) \rightarrow \mathit{false}$
  - Refutation requires $\sum x.a(x)$, $\sum x.b(x)$, $\sum x.c(x)$

Example

- Refute:

$$q(x) \to p(f(x))$$

$$p(x) \to q(f(f(x)))$$

$$p(x) \lor q(x)$$

$$p(x) \land q(x) \to false$$

- Proof on blackboard

Geo-translation

Function $f(x)$ eliminated using relation $g(x,y)$:

$\sum y \,.\, g(x,y)$ (unicity not needed!!)

$q(x) \wedge g(x,y) \rightarrow p(y)$

$p(x) \wedge g(x,y) \wedge g(y,z) \rightarrow q(z)$

$p(x) \vee q(x)$

$p(x) \wedge q(x) \rightarrow \mathit{false}$

Proof Recovery

- Geo-proof valid for all relations $g(x,y)$
- In particular for $g(x,y) := f(x)=y$
- $\sum y \,.\, g(x,y)$ becomes $\sum y \,.\, f(x)=y$ (tautology)
- $q(x) \wedge g(x,y) \rightarrow p(y)$ becomes $q(x) \wedge f(x)=y \rightarrow p(y)$, equivalent to $q(x) \rightarrow p(f(x))$
- Similarly for all other axioms
- Proof of original formula is obtained