Finding Very Short Proofs

Mark E. Stickel

Artificial Intelligence Center
SRI International
Menlo Park, California

XCB-Reflex Problem

Not an open problem, but offered as a challenge problem by Bill McCune

XCB was recently proven to be the 14th and final shortest single axiom for equivalential calculus

Proof of reflexivity from XCB leant hope to effort to find that XCB was a shortest single axiom

11 step proof of reflexivity from XCB was used to help find proof that XCB was a shortest single axiom

10 Step Proof of XCB-Reflex

```
 1  1            e(x,e(e(e(x,y),e(z,y)),z))
 2   (CD  1  1)    e(e(e(e(x,e(e(e(x,y),e(z,y)),z)),u),e(v,u)),v)
 3   (CD  2  1)    e(e(e(e(x,e(e(e(x,y),e(z,y)),z)),u),v),e(u,v))
 4   (CD  3  2)    e(e(x,e(e(e(e(y,e(e(e(y,z),e(u,z)),u)),v),e(w,v)),w)),x)
 5   (CD  1  4)    e(e(e(e(e(x,e(e(e(e(y,e(e(e(y,z),e(u,z)),u)),v),e(w,v)),w)),x),x1),e(y1,x1)),y1)
 6   (CD  5  1)    e(e(e(e(e(x,e(e(e(e(y,e(e(e(y,z),e(u,z)),u)),v),e(w,v)),w)),x),x1),y1),e(x1,y1))
 7   (CD  1  6)    e(e(e(e(e(e(e(e(x,e(e(e(e(y,e(e(e(y,z),e(u,z)),u)),v),e(w,v)),w)),x),x1),y1),
                   e(x1,y1)),z1),e(u1,z1)),u1)
 8   (CD  6  7)    e(e(x,e(e(e(e(y,e(e(e(e(z,e(e(e(z,u),e(v,u)),v)),w),e(x1,w)),x1)),y),
                     e(e(e(y1,e(e(e(y1,z1),e(u1,z1)),u1)),v1),e(w1,v1))),w1)),x)
 9   (CD  8  1)    e(e(e(e(x,e(e(e(x,y),e(z,y)),z)),u),u),e(e(e(e(v,e(e(e(v,w),e(x1,w)),
                   x1)),y1),e(z1,y1)),z1))
10   (CD  4  9)    e(e(e(x,e(e(e(x,y),e(z,y)),z)),u),u)
11   (CD  3 10)   e(x,x)
```

Using condensed detachment inference rule
e(x,y) & x -> y
(modus ponens plus unification)

Complete exhaustive search guarantees this is shortest possible

Interesting Fact about XCB

- there was doubt that XCB could be a single axiom
- failed to find any consequences that did not include an instance of XCB as a subformula (until XCB-Reflex was proved)
- now able to show that all formulas with derivations of 7 or fewer steps contain an instance of XCB
- e(e(x,y),e(x,y)) has an 8 step proof

Finding Shortest Proofs

Wos et al. at Argonne are very interested in finding short condensed-detachment proofs

- Find a proof (using Otter)
- Shorten that proof (e.g., by avoiding steps)
- Repeat

Quite successful, but unsystematic, and no guarantee of minimum length

Otter

Very good for finding proofs

Not designed to find shortest proofs

Subsumption eliminates results with short derivations
if more general result is found, even if by longer derivation

Search is ordered by term weight, not deduction length

Eliminating subsumption and using breadth-first search
is theoretically sufficient, but impractical due to memory
use

PTTP

Prolog Technology Theorem Prover provides a different style of theorem proving than Otter

- No subsumption
- Depth-first iterative deepening search instead of breadth-first search to minimize memory use
- Partial proof enumeration guarantees finding of a shortest proof (in the model elimination calculus)
- However, shortest model elimination proof may not have fewest condensed detachment steps

CODER (COndensed DEtacheR)

- Uses SNARK code for unification, term ordering, etc.
- Enumerate condensed detachment derivations
- Depth-first iterative deepening search instead of breadth-first search to minimize memory use
- Exhaustive search can guarantee that a proof is shortest
- However, there are many condensed detachment derivations up to specified length, making it impractical to search for shortest proofs beyond a very small length
- Veroff did something similar, using linked inference in Otter

How Bad Can It Be?

There are $n!^2$ n-step derivations from a single premise assuming

- every condensed detachment is successful
- no redundancy elimination (even duplicate steps are allowed)

Reducing the Number of Derivations

Reject derivations where

- Latest formula is an instance of an earlier formula in the derivation
- Latest formula is a generalization of an earlier formula in the derivation, unless the earlier formula is used to derive the latest
- Not all steps are used in the final derivation (check number of so far unused steps against number of remaining steps in search)
- Steps appear in different order than a single standard order (use LRPO to compare justifications of latest and immediately previous steps)

How Usable is This?

Severely limited as Wos et al.'s arguments against breadth-first search for finding shortest proofs suggest

Generally practical for finding guaranteed shortest proof with ~10 steps in minutes or hours

Extending a derivation by 1 step typically increases search space by factor of 10-20

Derivation of/from Shortest Single Axioms of Equivalential Calculus

=>	YCL	YQF	YQJ	UM	XGF	WN	YRM	YRO	PYO	PYM	XGK	XHK	XHN	XCB	R	S	T
YQF	5		7	8	8	7	9	8	9	9	8	8	7	8	5	5	7
YCL		4	6	7	5	7	8	7	5	7	7	7	7	8	4	5	6
YQJ	7	7		8	7	8	8	7	6	7	7	7	7	8	4	5	8
UM	-	-	-		1	11	11	-	-	11	10	-	10	-	5	10	-
XGF	-	-	-	2		-	-	-	-	11	11	-	11	-	6	10	-
PYO	-	-	-	-	-	-	-	-		-	-	-	-	-	7	-	-
XHN	-	-	-	-	-	-	-	-	-	-	-	-		-	11	-	-
XGK	-	-	-	-	-	-	-	-	10	-		-	-	-	3	10	-
WN	9	-	11	11	10		10	11	9	9	11	-	10	11	6	6	11
XHK	-	-	-	-	-	-	-	-	-	-	-		-	-	7	-	-
YRM	-	-	-	-	-	-		-	-	-	-	-	-	-	10	-	-
YRO	-	-	-	-	-	-	-		-	-	-	11	-	-	8	10	-
PYM	-	-	-	-	11	-	-	-	-		-	-	-	-	9	-	-
XCB	-	-	-	-	-	-	-	-	-	-	-	-	-		10	-	-