A calculational proof of Andrews’s challenge

David Gries\(^1\)

Computer Science, Cornell University

Ithaca, NY 14853\(^2\)

August 1996

At the Marktoberdorf summer school in August 1996, Larry Paulson lectured on his mechanical theorem prover, Isabelle; Natarajan Shankar lectured on his mechanical theorem prover, PVS; and I lectured on calculational logic. Both Paulson and Shankar suggested that I try the calculational approach on Andrew’s challenge, which is one of several theorems used to benchmark mechanical theorem provers. Andrew’s challenge is to prove the following theorem.\(^3\)

\[(1) \quad ((\exists x \forall y \cdot p.x \equiv p.y) \equiv (\exists x \cdot q.x) \equiv (\forall y \cdot p.y)) \equiv ((\exists x \forall y \cdot q.x \equiv q.y) \equiv (\exists x \cdot p.x) \equiv (\forall y \cdot q.y))\]

In proving Andrew’s challenge using the calculational approach, I use theorems given in the text [1] (or in its as-yet-unpublished second edition). The Appendix contains theorems used here that may be unfamiliar to the reader.

Now, \(\equiv\) is both associative and symmetric, so we can rewrite Andrew’s challenge as

\[P \equiv Q\]

where \(P\) and \(Q\) are defined by the following.

\[P : (\exists x \forall y \cdot p.x \equiv p.y) \equiv (\exists x \cdot p.x) \equiv (\forall y \cdot p.y)\]

\[Q : (\exists x \forall y \cdot q.x \equiv q.y) \equiv (\exists x \cdot q.x) \equiv (\forall y \cdot q.y)\]

where it is assumed that this formula is closed (so \(p.x\) and \(q.x\) contain no free variables other than \(x\)).

This form gives the impression that perhaps \(P\) is valid (or invalid), regardless of \(p\). If this is the case, then \(Q\) is also valid (or invalid). Hence, we try to prove \(P\).

We don’t have many theorems that deal with \(\equiv\) as they appear in \(P\), so we try to prove \(P\) by mutual implication, proving instead

\[\begin{align*}
(2) & \quad ((\exists x \forall y \cdot p.x \equiv p.y) \equiv (\exists x \cdot p.x)) \iff (\forall y \cdot p.y) \quad \text{and} \\
(3) & \quad ((\exists x \forall y \cdot p.x \equiv p.y) \equiv (\exists x \cdot p.x)) \Rightarrow (\forall y \cdot p.y)
\end{align*}\]

\(^1\) Supported by NSF grants CDA-9214957 and CCR-9503319.

\(^2\) http://www.cs.cornell.edu/Info/People/gries/gries.html  
  gries@cs.cornell.edu

\(^3\) We use the notation \((\forall x \cdot (\exists y \cdot P))\) may be abbreviated as \((\forall x \exists y \cdot P)\). Also, we use \(\equiv\) for equality over the bools and \(\equiv\) for equality over any type (including the bools). Our precedences are, beginning with the tightest, \(\land\), \(\lor\), \(\Rightarrow\) and \(\iff\), and \(\equiv\). Finally, in order to eliminate parentheses, we write \(p.x\) instead of \(p(x)\) for application of function \(p\) to variable \(x\).
Proof of (2). Assume \((\forall y \mid p.y)\)

\[
(\exists x \forall y \mid p.x \equiv p.y) \equiv (\exists x \mid p.x)
\]

\[
= \langle \text{Assumption, instantiated with } y := x \text{ and with } y := y, \text{ so } p.x \equiv \text{true and } p.y \equiv \text{true} \rangle
\]

\[
(\exists x \forall y \mid \text{true} \equiv \text{true}) \equiv (\exists x \mid \text{true})
\]

\[
= \langle \text{Identity of } \equiv \ (5); \ (\forall y \mid \text{true}) \equiv \text{true} \rangle
\]

\[
(\exists x \mid \text{true}) \equiv (\exists x \mid \text{true}) \quad \text{—Reflexivity of } \equiv \ (6)
\]

Proof of (3).

\[
(3)
\]

\[
= \langle \text{Contrapositive, } X \Rightarrow Y \equiv \neg Y \Rightarrow \neg X \rangle
\]

\[
\neg (\forall y \mid p.y) \Rightarrow \neg (\exists x \forall y \mid p.x \equiv p.y) \equiv (\exists x \mid p.x)
\]

\[
= \langle \text{De Morgan (12) on antecedent; } \neg (X \equiv Y) \equiv X \equiv \neg Y \text{ and De Morgan (11) on the consequent} \rangle
\]

\[
(\exists y \mid \neg p.y) \Rightarrow ((\exists x \forall y \mid p.x \equiv p.y) \equiv (\forall x \mid \neg p.x))
\]

By Metatheorem Witness (13), the last formula is a theorem iff the following one is.

\[
\neg p.y \Rightarrow (\exists x \forall y \mid p.x \equiv p.y) \equiv (\forall x \mid \neg p.x))
\]

We calculate:

Assume \(\neg p.y\), so also \(p.y \equiv \text{false}\)

\[
(\exists x \forall y \mid p.x \equiv p.y)
\]

\[
= \langle \text{Lemma (4) —heading to change } p.x \text{ to } p.y \rangle
\]

\[
(\exists x \mid (\forall y \mid p.x \equiv p.y) \land p.x \equiv p.y)
\]

\[
= \langle \text{Substitution (8)} \rangle
\]

\[
(\exists x \mid (\forall y \mid p.y \equiv p.y) \land p.x \equiv p.y)
\]

\[
= \langle \text{Lemma (4)} \rangle
\]

\[
(\exists x \forall y \mid p.y \equiv p.y)
\]

\[
= \langle \text{Assumption } p.y \equiv \text{false; false } \equiv X \equiv \neg X \rangle
\]

\[
(\exists x \forall y \mid \neg p.y)
\]

\[
= \langle \text{Provided } x \text{ doesn’t occur free in } X, (\exists x \mid X) \equiv X \rangle
\]

\[
(\forall y \mid \neg p.y)
\]

(4) Lemma. \((\forall x \mid S.x) \equiv (\forall x \mid S.x) \land S.t\)

Proof.

\[
(\forall x \mid \text{true } : S.x)
\]

\[
= \langle \text{Zero of } \lor \ (7) \rangle
\]

\[
(\forall x \mid \text{true } \lor x = t : S.x)
\]

\[
= \langle \text{Range split (10)} \rangle
\]

\[
(\forall x \mid \text{true } : S.x) \land (\forall x \mid x = t : S.x)
\]

\[
= \langle \text{One-point rule (9)} \rangle
\]

\[
(\forall x \mid \text{true } : S.x) \land S.t
\]

\[
\]
References


Appendix. Some of the theorems used in the proof

(5) Identity of ≡: true ≡ Q ≡ Q
(6) Reflexivity of ≡: P ≡ P
(7) Zero of ∨: P ∨ true ≡ true
(8) Substitution: X = Y ∧ E^X_Y ≡ X = Y ∧ E^Y_Y
(9) One-point rule: Provided x does not occur free in E,
   \((∀x \mid x = E : P) = P[x := E] \)
(10) Range split: \((∀x \mid R ∨ S : P) = (∀x \mid R : P) ∧ (∀x \mid S : P) \)
(11) De Morgan: ¬(∃x | R : P) ≡ (∀x | R : ¬P)
(12) De Morgan: ¬(∀x | R : P) ≡ (∃x | R : ¬P)

(13) Metatheorem Witness. Suppose x does not occur free in P, Q, and R. Then
    \((∃x \mid R : P) ⇒ Q \) is a theorem iff
    \((R ∧ P)[x := \hat{x}] ⇒ Q \) is a theorem.