Preprint MCS-P376-0793, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, Ill., July 1993.

Automated Reasoning about Cubic Curves

R. Padmanabhan[*]
Department of Mathematics
University of Manitoba
Winnipeg, Manitoba R3T 2N2
Canada

W. McCune[†]
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60439-4844
U.S.A.

Abstract

It is well known that the n-ary morphisms defined on projective algebraic curves satisfy some strong local-to-global equational rules of derivation not satisfied in general by universal algebras. For example, every rationally defined group law on a cubic curve must be commutative. Here we extract from the geometry of curves a first-order property (gL) satisfied by all morphisms defined on these curves such that the equational consequences known for projective curves can be derived automatically from a set of six rules (stated within the first-order logic with equality). First, the rule (gL) is implemented in the theorem-proving program OTTER. Then we use OTTER to automatically prove some incidence theorems on projective curves without any further reference to the underlying geometry or topology of the curves.

AMS Subject Classification (1991). Primary: 68T15, 08B05. Secondary:14H52, 20N05.

1 Introduction

The term "equational logic" refers to the study of various metalogical notions related to the processes of deriving new equations, say Φ, from given ones, say Σ, that is,

$$\Sigma \models \Phi \quad \text{(modulo, a class } \mathbf{K}\text{)}.$$

Here, the crucial concept is that of "deriving (modulo $\mathbf{K}$)". In universal algebras, $\mathbf{K}$ is usually the class of all algebras of a specific type satisfying Σ; hence, in this case, Φ is derivable from Σ iff Φ formally follows from Σ by the now famous five rules of Garrett Birkhoff. This is the so-called completeness theorem of equational logic (see, e.g., [12, p. 180]).

In a variety of situations, however, one works with special classes $\mathbf{K}$ of algebras of a given type, usually richer in structure than the class of *all* models of that type. We mention a

[*]Supported by an operating grant from NSERC of Canada (#A8215)
[†]Supported by the Office of Scientific Computing, U.S. Department of Energy, under Contract W-31-109-Eng-38.

famous example from classical algebraic geometry: Every group law definable on an elliptic curve is commutative. In other words, we have the implication

$$\{\text{group axioms}\} \models \{xy = yx\} \quad (\text{modulo } \mathbf{K} = \text{“groups on elliptic curves”}).$$

If one uses the powerful fact that an elliptic curve is a one-dimensional Abelian variety, the above implication is possible through a local-to-global lifting principle called the “rigidity” of regular (= rational) functions. However, since the starting assumption (i.e., being a group) and the conclusion (i.e., being commutative) are both first-order algebraic, it is natural to ask whether there is any “purely algebraic way” to prove such statements within the realms of first-order logic with equality. Here we answer this question in the affirmative by formalizing the rigidity principle. This results in the equational process “ $=\!(gL)\!\Rightarrow$ ”.

Let us recall this local-to-global principle from, say, I. R. Shafarevich [10, p. 152]:

LEMMA. *Let X be a projective curve and Y and Z be irreducible algebraic varieties, all defined over an algebraically closed field k. Let f be a regular mapping from $X \times Y$ into Z such that $f(X \times \{y_0\})$ is a singleton z_0 for some $y_0 \in Y$. Then $f(X \times \{y\})$ is a singleton for every $y \in Y$.*

Proofs of this basic fact may be be found in [11, p. 156] or in [7, p. 104]. In this paper we present one example, that of an elliptic curve, a one-dimensional Abelian variety.

Elliptic Curves. Let $p(x, y)$ be an irreducible cubic polynomial over an algebraically closed field k. Then the curve $\Gamma = \{(x, y) | p(x, y) = 0\} \cup \{\infty\}$ is called an elliptic curve if the curve $p(x, y) = 0$ has no singular points in the projective plane over the field k.

Now we turn the curve Γ into an algebra in the following natural way: Let A and B be any two points of Γ.

(i) If $A \neq B$, then $A \cdot B$ is the unique third point where the chord AB intersects Γ (a line and a third-degree curve have only three common points).

(ii) If $A = B$, then $A \cdot B$ is the unique point where the tangent at A meets the curve again.

It is clear that the algebra $\langle \Gamma; \cdot \rangle$ satisfies the following two laws: $x \cdot y = y \cdot x$ and $x \cdot (y \cdot x) = y$. Moreover, an element $e \in \Gamma$ is idempotent iff $e \cdot e = e$ iff the tangent at e meets the curve Γ again at e, in other words, iff e is a point of inflexion (see Figure 1).

This is the classical binary operation of chord-tangent construction on a cubic curve. It is well known that Γ is a “nice” algebraic variety, in fact, a one-dimensional Abelian variety and hence, in particular, satisfies the above rigidity lemma for all its morphisms, including those in the clone of the “$\cdot$” (cf. [10, p. 148] or [11, Example 5, p. 34]).

2 Methodology and Theorems

We now rewrite the rigidity lemma as a formal implication:[1]

$$\exists y_0 \exists z_0 \forall x (f(x, y_0) = z_0) \Rightarrow \forall x \forall y \forall z (f(x, y) = f(z, y)) \qquad \text{(gL)}$$

[1] (gL) for “Local to global”, “geometric Logic”, “geometric Law”.

We view the rule (gL) as an equation-deriving principle extending the scope of the usual equational logic: whenever the program meets the local equality $f(x, y_0) = z_0$ for some word f and some elements y_0, z_0, it churns out the global multivariable identity $f(x, y) = f(z, y)$ (multivariable because here x, y, or z could be vectors, namely, $x = (x_1, x_2, .., x_m)$, because x, y, or z could themselves be product spaces). This idea of viewing (gL) as an inference rule was first stated and systematically used by R. Padmanabhan in [8]. See R. W. Quackenbush [9] for the history of a closely related and recently discovered concept of "term condition".

We use the following notation. If Σ is a set of identities and if σ is an identity in the language of Σ, then we write

$$\Sigma \Rightarrow_{(gL)} \sigma$$

if $\Sigma \cup$ (gL) $\Rightarrow \sigma$ in the usual equational logic. Whenever convenient, we also say that the axioms Σ "(gL)-implies" σ, etc.

Using the rule (gL), let us now give a "mindless" proof of the powerful four-variable median law just from the relatively weak two-variable Steiner quasigroup laws $\{x \cdot (y \cdot x) = y, (y \cdot z) \cdot z = y\}$.

THEOREM 1. $\{x(yx) = y, (yz)z = y\} \Rightarrow_{(gL)} \{(xy)(zt) = (xz)(yt)\}$.

Proof. Define the 5-ary composite operation $f(x, y, z, t, u)$ by $f \doteq ((xy)(zt))(u((xz)(yt)))$. Now we have, by the law $x(yx) = y$, $f(x, c, c, t, d) = d$ for all x. Thus by the rule (gL), the 5-ary expression $f(x, y, z, t, u)$ does not depend upon x *for all* y, z, t, u. In particular, we have

$$\begin{array}{lll}
f(x,y,z,t,u) & = f(x_1,y,z,t,u) & \forall x \forall x_1 \\
\text{i.e.,} \quad ((xy)(zt))(u((xz)(yt))) & = ((x_1y)(zt))(u((x_1z)(yt))) & \forall x \forall x_1 \\
& = (((yz)y)(zt))(u(((yz)z)(yt))) & \text{letting } x_1 = yz \\
& = t(ut) & \text{by the Steiner laws} \\
& = u & \\
& = ((xz)(yt))(u((xz)(yt))) &
\end{array}$$

and hence one right-cancellation of the common term $(u((xz)(yt)))$ immediately yields the desired median law $(xy)(zt) = (xz)(yt)$.

Let us now apply this to the geometry of plane cubic curves without any further reference to the geometry or the topology of curves.

COROLLARY 1. *Every binary morphism "$\cdot$" defined on a nonsingular cubic curve* Γ *over an algebraically closed field satisfying the Steiner quasigroup identities must be medial* (see, e.g., Figure 2).

Historical remark. This corollary was first proved for plane cubic curves by I. M. S. Etherington using the classical Bezout theorem (see [1]). In [8], Padmanabhan gave a proof for elliptic curves over an arbitrary algebraically closed field k. (See OTTER's more general proof in the Appendix).

Proof. A nonsingular cubic curve is an Abelian variety and hence, as mentioned in the introduction, satisfies (the rigidity lemma and consequently) the rule (gL) for all morphisms.

3 OTTER and Implementation of the Rule (gL)

OTTER [3, 4] is a computer program that attempts to prove theorems stated in first-order logic with equality. Here we restrict our attention to its capabilities in equational logic. The user inputs axioms and the denial of the goal(s), and OTTER searches for a contradiction by working both forward from the axioms and backward from the goal(s). Equational reasoning is accomplished by paramodulation and demodulation. Paramodulation is equality substitution extended with unification: if the two terms in question can be made identical by instantiating variables, then equality substitution is applied to the corresponding instances. Demodulation is the use of equalities as rewrite rules to simplify other equalities. The following example illustrates the interplay between paramodulation and demodulation. Consider $\{f(x, f(g(x), y)) = y, f(u, g(u)) = e, f(w, e) = w\}$, with e nullary; OTTER can infer $x = g(g(x))$ "in one step" by unifying $f(u, g(u))$ and $f(g(x), y))$ (which instantiates u to $g(x)$ and y to $g(g(x))$), replacing $f(g(x), g(g(x)))$ with e, and then demodulating with $f(w, e) = w$.

The rule (gL) was implemented in a special version of OTTER[2] in two ways that are analogous to paramodulation and demodulation. Let f be the operator to which (gL) applies, and let $F[a_1, x]$ represent a term in f that contains a subterm a_1 at a particular position, with x representing everything else in the term. Suppose we have $F[a_1, x] = F[a_2, y]$, (i.e., a_1, and a_2 are in corresponding positions), with a_1 and a_2 unifiable. By (gL) we infer $F[z, x'] = F[z, y']$, where z is a new variable, and x' and y' are the appropriate instances of x and y. For example, from

$$f(f(x, y), f(z, f(x, z))) = f(u, f(y, u)),$$

we can (gL)-infer

$$f(f(x, y), f(z, w)) = f(f(x, z), f(y, w))$$

by unifying u and $f(x, z)$. We also use (gL) as a rewrite rule whenever possible. That is, we rewrite $F[a, x] = F[a, y]$ to $F[z, x] = F[z, y]$ (again, z is a new variable).

OTTER Proof Notation. Variables are distinguished from constants by starting with u, v, w, x, y, or z. Proofs are by contradiction, and the denials of the goals contain constants, that is, objects for which the goal fails to hold. The justification for each step is in brackets and specifies the inference rule and any rewriting that occurs. The inference rules are "para_from" (substitute into the second equality), "para_into" (substitute into the first equality) and "gL". Rewriting is specified with either "demod, ..." (simplification with ...) or "gL-id".

THEOREM 2. *Let Γ be a nonsingular cubic curve defined over an algebraically closed field and let e be an inflexion point on Γ. Then the binary morphism of chord-tangent construction on Γ is completely characterized by the identities*

$$A = \{f(x, y) = f(y, x), f(x, f(y, x)) = y, f(e, e) = e\}.$$

[2] Write to the second author or send electronic mail to otter@mcs.anl.gov for information on obtaining a version of OTTER with (gL).

Proof. Let f and g be two binary morphisms satisfying the laws in the set A. Let $C = \{f(x,y) = f(y,x), f(x,f(y,x)) = y, f(e,e) = e, g(x,y) = g(y,x), g(x,g(y,x)) = y, g(e,e) = e\}$. Then we claim that $C \ =(gL)\Rightarrow \ g(x,y) = f(x,y)$. Here is OTTER's proof complete with input and output files (line 21039 has the desired conclusion: it is a direct proof).

Input to OTTER:

```
set(para_from).
set(para_into).
set(para_from_vars).
set(para_into_vars).
set(order_eq).
set(geometric_rule).
set(geometric_rewrite).
set(lex_rpo).
lex([a,b,e,f(x,x),g(x,x)]).
lrpo_lr_status([f(x,x),g(x,x)]).
assign(pick_given_ratio, 5).
assign(max_weight, 130).
assign(max_mem, 16000).
clear(print_kept).
clear(print_back_sub).
list(usable).
x = x.
end_of_list.
list(sos).
f(x,y) = f(y,x).
f(x,f(y,x)) = y.
f(e,e) = e.
g(x,y) = g(y,x).
g(x,g(y,x)) = y.
g(e,e) = e.
end_of_list.
list(passive).
g(a,b) != f(a,b).
end_of_list.
```

Output (OTTER 2.2xb, (gL)-version):

```
UNIT CONFLICT at 137679.71 sec ----> 21040 [binary,21039,8] $F.
---------------- PROOF ----------------
2 [] f(x,y)=f(y,x).
3 [] f(x,f(y,x))=y.
4 [] f(e,e)=e.
5 [] g(x,y)=g(y,x).
6 [] g(x,g(y,x))=y.
7 [] g(e,e)=e.
8 [] g(a,b)!=f(a,b).
21 [para_from,7,2] f(x,g(e,e))=f(e,x).
```

```
42 [para_into,3,3] f(f(x,y),x)=y.
97 [para_into,6,6] g(g(x,y),x)=y.
98 [para_into,6,5] g(x,g(x,y))=y.
100 [para_into,6,5] g(g(x,y),y)=x.
395 [para_from,97,4] f(e,g(g(x,e),x))=e.
447 [para_into,98,42] f(f(x,g(y,g(y,z))),x)=z.
1601 [para_into,21,100] f(e,g(g(x,y),y))=f(x,g(e,e)).
12584 [gL,1601] f(e,g(g(x,e),y))=f(x,g(e,y)).
12652 [para_into,12584,395] f(x,g(e,x))=e.
13120 [para_into,12652,5] f(x,g(x,e))=e.
13300 [para_from,12652,447] f(e,g(e,x))=x.
16821 [para_into,13120,13120,gL-id] f(x,g(x,z))=f(y,g(y,z)).
20249 [para_into,13300,16821] f(x,g(x,y))=y.
21039 [para_into,20249,98] g(x,y)=f(x,y).
21040 [binary,21039,8] $F.
------------ end of proof -------------
```

COROLLARY 2. *Any two group laws defined on* Γ *differ by a constant. That is, if* $(+,-,0)$ *and* $(\cdot,^{-1},e)$ *are both group laws on the curve* Γ*, then* $(x+y)-(xy)$ *is a constant.*

Proof. Define $f(x,y) = -x-y+3e$ and $g(x,y) = x^{-1}y^{-1}$, where $3e = e+e+e$ is some fixed element of Γ. It is clear that both f and g satisfy the axioms C, for example, $f(x,f(y,x)) = -x-(-y-x+3e)+3e = y$. Also, $g(e,e) = e$ and $f(e,e) = -e-e+3e = e$. Thus by Theorem 2, we obtain the equality $-x-y+e = x^{-1}y^{-1}$. Putting $y = e$, we get $-x = x^{-1}$. So $-x-y+e = (-x)(-y)$. Replacing x by $-a$ and y by $-b$, we get $a+b+e = ab$. Thus any two group laws must differ only by a constant. In the literature this is often stated as follows (see, e.g., J.S. Milne, "Abelian Varieties" [7, Remark 2.3 on p. 105]): "A group structure on Γ is uniquely determined by the choice of the zero element". In fact, in the above calculation, if $e = 0$, then $a+b = ab$ itself.

THEOREM 3. *Let* e *be an inflexion point on* Γ*. Then the binary morphism* $f(x,y) = x\cdot y$ *of chord-tangent construction on* Γ *is characterized by the single identity* $(x\cdot((z\cdot(x\cdot y))\cdot(e\cdot y)))\cdot(e\cdot e) = z$.

Proof. By Theorem 2, it is enough if we prove that

$$\{x\cdot(y\cdot x) = y, x\cdot y = y\cdot x, e\cdot e = e\} \Leftarrow (gL) \Rightarrow (x\cdot((z\cdot(x\cdot y))\cdot(e\cdot y)))\cdot(e\cdot e) = z.$$

Define the ternary composite function $g(x,y,z) \doteq (x((z(xy))(ey)))(ee)$. Now $g(x,e,e) = (x\cdot((e\cdot(x\cdot e))\cdot e))\cdot e = (x\cdot(x\cdot e))e = e$ and hence, by the rule (gL), we obtain the identity $g(x,y,z) = g(u,y,z) = g(e,y,z) = (e\cdot((z\cdot(e\cdot y))\cdot(e\cdot y)))\cdot e = (e\cdot z)\cdot e = z$. See the Appendix for the complete OTTER proofs.

COROLLARY 3. *Let* e *be an inflexion point on a nonsingular cubic curve* Γ*. Then for all points* x,y,z *on the curve* Γ*, the three points* $\{x\cdot((z\cdot(x\cdot y))\cdot(e\cdot y)), z, e\}$ *are always colinear, where "*$\cdot$*" is the binary operation of chord-tangent construction* (see Figures 3 and 4).

COROLLARY 4. *The equational theory of the algebra* $\langle\Gamma;\cdot\rangle$ *contains all the identities satisfied by the double inversion operation* $x^{-1}y^{-1}$ *true in every Abelian group.*

W. McCune has shown (in [5]) that the single 3-variable identity on the right side characterizes the binary operation of double inversion $x\cdot y = x^{-1}y^{-1}$ in Abelian groups

with the element e as the group identity. The converse is also true, namely, that the equational theory of G is precisely the set of all identities true for $x^{-1}y^{-1}$ in *every* Abelian group. In fact, even the set of all implications valid in these two classes of algebra are the same. This was proved by Harry Lakser and R. Padmanabhan in [2].

4 Concluding Remarks

The rule " $=(gL)\Rightarrow$ " viewed as an inference rule to derive stronger equations from relatively weaker ones is, in a sense, custom-made for the equational theory of Abelian varieties. If this process meets a set of laws, it tries to solve them so that the set can be interpreted in group theory and then, if it succeeded, it gets all the laws true for *that* interpretation in Abelian groups. All the configuration theorems on cubic curves are of this category and hence provable by this process. To further illuminate this metaprinciple, let us take, for example,

$$A = \{x/e = x, e/(e/x) = x, x/x = e\}$$

as our initial set of laws of type (2,0), with one binary "/" and one nullary e. Solving for these, we find that the only group-interpretation of the laws A are $x/y = xy^{-1}$ and $e = 1$. Thus we predict that A $=(gL)\Rightarrow$ {all the axioms for Abelian groups with $a/b = ab^{-1}$}. This is indeed the case. If an initial set of axioms ia not solvable in this way, then it will (gL)-imply $x = y$. (see Theorem 5 in the Appendix).

Appendix

Two new proofs of Theorem 1 under much weaker assumptions were obtained by OTTER. We mention just one example.

THEOREM 4. $\{x(ex) = e\}$ $=(gL)\Rightarrow$ $\{(xy)(zt) = (xz)(yt)\}$.

Proof.

```
----> UNIT CONFLICT at   7.11 sec ----> 987 [binary,986,5] $F.

---------------- PROOF ----------------
3 [] f(x,f(e,x))=e.
5 [] f(f(A,B),f(C,D))!=f(f(A,C),f(B,D)).
8 [para_into,3,3,gL-id] f(x,f(z,x))=f(y,f(z,y)).
23 [para_into,8,8] f(f(x,y),f(z,f(x,z)))=f(u,f(y,u)).
986 [gL,23] f(f(x,y),f(z,u))=f(f(x,z),f(y,u)).
987 [binary,986,5] $F.
------------ end of proof -------------
```

THEOREM 5. $\{x/e = x, e/(e/x) = x, x/x = e\}$ $=(gL)\Rightarrow$ {*all the axioms for Abelian groups with* $a/b = ab^{-1}$}.

Proof.

```
----> UNIT CONFLICT at 130.34 sec ----> 10852 [binary,10851,9] $F.

---------------- PROOF ----------------
2 [] f(x,e)=x.
3 [] f(e,f(e,x))=x.
4 [] f(x,x)=e.
9 [] f(a,f(f(a,b),f(c,b)))!=c.
24 [para_into,4,2] f(f(x,e),x)=e.
25 [para_into,4,2] f(x,f(x,e))=e.
49 [para_from,24,2] f(x,f(f(y,e),y))=x.
59 [para_into,25,25,gL-id] f(x,f(x,z))=f(y,f(y,z)).
310 [para_into,59,3] f(y,f(y,x))=x.
362 [para_into,310,2] f(x,f(f(x,e),y))=y.
3535 [para_into,362,49,gL-id] f(x,f(f(x,u),y))=f(y,f(f(z,u),z)).
10851 [para_into,3535,310] f(x,f(f(x,y),f(z,y)))=z.
10852 [binary,10851,9] $F.
------------ end of proof -------------
```

THEOREM 6. *A cancellative (gL)-semigroup is commutative.*

Note that this theorem generalizes the well-known result that every (gL)-group is Abelian.

Proof.

```
----> UNIT CONFLICT at  97.00 sec ----> 1559 [binary,1558,3] $F.

---------------- PROOF ----------------
2 [] f(f(x,y),z)=f(x,f(y,z)).
3 [] f(a,b)!=f(b,a).
4 [] (f(x,y)=f(x,z))=(y=z).
5 [] (f(y,x)=f(z,x))=(y=z).
6 [para_into,2,2] f(f(f(x,y),z),u)=f(x,f(f(y,z),u)).
7 [para_into,2,2] f(f(x,f(y,z)),u)=f(f(x,y),f(z,u)).
14 [para_into,6,2] f(f(f(x,f(y,z)),u),v)=f(f(x,y),f(f(z,u),v)).
539 [gL,14] f(f(f(x,f(y,z)),u),v)=f(f(x,u),f(f(z,y),v)).
653 [para_into,539,7,demod,5] f(f(x,f(y,z)),u)=f(x,f(u,pf(z,y))).
1019 [para_into,653,2,demod,4] f(f(y,z),u)=f(u,f(z,y)).
1558 [gL,1019,demod,4] f(y,z)=f(z,y).
1559 [binary,1558,3] $F.
------------ end of proof -------------
```

In fact, OTTER has obtained a much stronger result, namely, that any cancellative (gL)-algebra satisfying just the two-variable consequences of associativity is commutative (and associative). This proof, along with other aspects of associativity, will appear elsewhere. Readers are encouraged to try this on the (gL)-version of OTTER (i.e., OTTER 2.2xb).

THEOREM 7. *No nontrivial (gL)-algebra contains a semilattice function in its clone of operations. In other words,* $\{f(x,x)=x, f(x,f(y,z))=f(y,f(z,x))\} \Rightarrow\!\!\!\!\!\!= (gL) \{x=y\}$.

Note that the starting axioms themselves are consistent: take any Boolean algebra and define $f(x,y)$ as $x \wedge y$. Similarly, for the next result, take $f(x,y,z)$ as $(x \wedge y) \vee (y \wedge z) \vee$

$(z \wedge x)$. However, there are no group words that will model these equations; hence, by our metaprinciple, these identities must (gL)-imply $x = y$. OTTER happily confirms this, as shown below.

Proof.

```
----> UNIT CONFLICT at  19.96 sec ----> 1915 [binary,1914,4] $F.

---------------- PROOF ----------------
2 [] f(x,x)=x.
3 [] f(x,f(y,z))=f(y,f(z,x)).
4 [] a!=b.
249 [para_into,3,2,gL-id] f(z,f(y,f(x,y)))=f(z,y).
258 [para_into,3,2] f(x,f(y,x))=f(y,x).
286 [gL,3] f(x,f(y,z))=f(x,f(z,y)).
414 [para_into,249,2] f(x,f(x,f(y,x)))=x.
1505 [para_into,414,258] f(x,f(y,x))=x.
1726 [para_into,1505,258] f(x,y)=y.
1730 [para_into,1505,286] f(x,f(x,y))=x.
1888 [para_into,1730,1726] f(x,y)=x.
1914 [para_into,1888,1726] x=y.
1915 [binary,1914,4] $F.
------------ end of proof -------------
```

THEOREM 8. *No nontrivial (gL)-algebra contains a majority function in its clone of operations. In other words,* $\{f(x,x,y) = f(x,y,x) = f(y,x,x) = x\} \Rightarrow (gL) \Rightarrow \{x = y\}$.

Proof.

```
----> UNIT CONFLICT at   6.28 sec ----> 398 [binary,397,5] $F.

---------------- PROOF ----------------
2 [] f(x,x,y)=x.
3 [] f(x,y,x)=x.
4 [] f(y,x,x)=x.
5 [] a!=b.
6 [para_into,2,2] f(f(x,x,y),f(x,x,y),z)=x.
11 [para_into,4,3] f(f(x,y,y),z,f(x,y,y))=y.
14 [para_from,4,2] f(x,f(y,y,z),f(y,y,z))=y.
15 [para_into,6,6] f(x,f(f(x,x,y),f(x,x,y),z),u)=f(x,x,y).
201 [para_into,11,4] f(x,y,f(z,x,x))=x.
310 [para_into,14,2] f(x,y,f(y,y,z))=y.
320 [para_into,14,2] f(x,f(y,y,z),y)=y.
343 [para_into,15,320] f(x,x,y)=f(x,x,z).
369 [gL,343] f(x,y,z)=f(x,y,u).
371 [para_into,369,310] f(y,x,z)=x.
374 [para_into,369,201] f(x,y,z)=x.
397 [para_into,374,371] x=y.
398 [binary,397,5] $F
 --------end of proof ---------
```

In particular, Theorems 7 and 8 show that no elliptic curve will admit binary or ternary morphisms satisfying the respective assumptions in question. Theorem 7 is new, and OTTER's proof as given above is the first equational proof. The last result about the majority polynomial is really folklore among universal algebraists, albeit via the term condition (see references in [9]). Here we include them just to demonstrate the ease with which OTTER handles such equational proofs.

References

[1] I. M. S. Etherington. Quasigroups and cubic curves. *Proc. Edinburgh Math. Soc.*, 14:273–291, 1965.

[2] H. Lakser and R. Padmanabhan. Preprint, 1993.

[3] W. McCune. OTTER 2.0 Users Guide. Tech. Report ANL-90/9, Argonne National Laboratory, Argonne, Ill., March 1990.

[4] W. McCune. What's New in OTTER 2.2. Tech. Memo ANL/MCS-TM-153, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, Ill,, July 1991.

[5] W. McCune. Single axioms for groups and Abelian groups with various operations. *Journal of Automated Reasoning*, 10(1):1–13, 1993.

[6] N. S. Mendelsohn, R. Padmanabhan, and B. Wolk. Straight edge constructions on cubic curves. *C. R. Math. Rep. Acad. Sci. Canada*, 10:77–82, 1988.

[7] J. S. Milne. Abelian varieties. In *Arithmetic Geometry*, pages 103–150. Springer-Verlag, New York, 1986.

[8] R. Padmanabhan. Logic of equality in geometry. *Discrete Mathematics*, 15:319–331, 1982.

[9] R. W. Quackenbush. Quasi-affine algebras. *Algebra Universalis*, 20:318–327, 1985.

[10] I. R. Shafarevich. *Basic Algebraic Geometry*. Springer-Verlag, New York, 1977.

[11] T. A. Springer. *Linear Algebraic Groups*. Birkhauser, Boston, 1980.

[12] W. Wechler. *Universal Algebra for Computer Scientists*. Springer-Verlag, New York, 1992.

Captions for Figures 1–4*

Figure 1: The algebra of an eliptic curve.

Figure 2: $\{x(yx) = y\} \Rightarrow (gL) \Rightarrow \{(xy)(zt) = (xz)(yt)\}$, that is, the validity of the medial law $(xy)(zt) = (xz)(yt)$ for the binary operation "$\cdot$" of the chord-tangent construction on a cubic curve (Theorem 1).

Figure 3: $\{x \cdot (y \cdot x) = y, e \cdot e = e\} \Leftarrow (gL) \Rightarrow (x \cdot ((z \cdot (x \cdot y)) \cdot (e \cdot y))) \cdot (e \cdot e) = z$, that is, the validity of McCune's single identity for "double inversion in Abelian groups" on a nonsingular cubic curve in the projective plane. In other words, let e be an inflexion point on the cubic curve. Then for all points x, y, z on the curve, the three points e, z, and $(x \cdot ((z \cdot (x \cdot y)) \cdot (y \cdot e)))$ are collinear. The point e is at infinity.

Figure 4: See the caption for Figure 3. The difference is that here, e is not at infinity.

*The figures are not available electronically.