Uniqueness of Certain Algebraic Laws on Cubic Curves

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

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

May 26, 1995

Abstract. An n-ary Steiner law $f(x_1, x_2, \cdots, x_n)$ on a projective curve Γ over an algebraically closed field k is a totally symmetric n-ary morphism f from Γ^n to Γ satisfying the universal identity

$$f(x_1, x_2, \cdots, x_{n-1}, f(x_1, x_2, \cdots, x_n)) = x_n.$$

An element e in Γ is called an idempotent for f if $f(e, e, \cdots, e) = e$. The binary morphism $x * y$ of the classical chord-tangent construction on a non-singular cubic curve is an example of a binary Steiner law on the curve, and the idempotents of $*$ are precisely the inflection points of the curve. Similarly, a 5-ary Steiner morphism $f(x, y, z, u, v)$ is obtained by the intersection cycle

$$\Gamma \cap Q = \{x, y, z, u, v, f(x, y, z, u, v)\}$$

[*]Supported by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Computational and Technology Research, U.S. Department of Energy, under Contract W-31-109-Eng-38.

[†]Supported by an operating grant from NSERC of Canada (#A8215).

where Q is the unique conic passing through the five points x, y, z, u, v (see Fig. 2). Here the idempotents of f are the so-called sextatic points (e.g., [15, p. 124]). In this paper, we prove that if f and g are two n-ary Steiner laws on a non-singular cubic curve and if f and g have common idempotent element then $f = g$. First, we extract an inference rule (gL) from the Rigidity Lemma, a powerful local-to-global principle valid for projective algebraic curves. This rule is implemented in OTTER, a theorem-proving program for first order logic with equality. Then we use Otter to mechanically generate a proof of the uniqueness of the 8-ary Steiner law. Very much like the binary and the 5-ary cases, this theorem provides algebraic characterizations of synthetic geometric constructions involving the intersection cycles of non-singular cubics with algebraic curves of various degrees. As a corollary, we obtain a new proofs of classically known ruler constructions for these geometric laws. Also, the well-known theorem of the uniqueness of a group law on an elliptic curve is shown to be a consequence of this result.

1 Introduction

The so-called identity theorems of classical function theory state that if two functions (belonging to a "nice" class) agree on a dense open set, they agree everywhere. This is the heart of several uniqueness theorems of algebraic structures in mathematics. An analog in algebraic geometry is the so-called Chow's theorem [10, p. 67]: "Every compact complex manifold has at most one algebraic structure, and moreover, every compact 1-dimensional complex manifold admits a unique algebraic structure". These are analytically isomorphic to projective varieties. This is a deep theorem, and the uniqueness of a group law on an elliptic curve Γ is a special case. We say that an algebraic curve Γ admits an algebraic law, say $f(x_1, x_2, \cdots, x_n)$, if f is a n-ary morphism (i.e., a regular function or a rational function) on the curve Γ. The nonsingular cubic curves are pregnant with a number of universal algebras all of which are morphisms of the curve. These are given by a special case of the so-called Cayley-Bacharach Theorem (see [9, p. 74] or [2, p. 33]).

Cayley-Bacharach Theorem for Cubic Curves: Let Γ be a non-singular cubic curve and let F be an irreducible algebraic curve of degree n such that they meet at $3n$ distinct points. Then any plane curve H of degree n passing through all but one of $\Gamma \cap F$ necessarily passes through the remaining point

also (see e.g. the Figures 1, 2, and 3 for the binary linear process with $n = 1$, the 5-ary conic process with $n = 2$, and the 8-ary cubic process with $n = 3$ respectively).

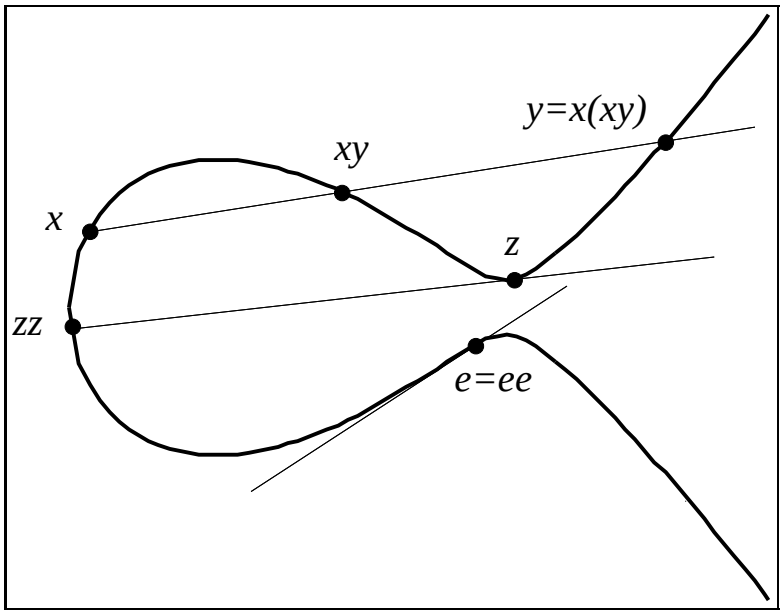

Figure 1: Chord-Tangent Construction

In this paper, we give a pure equational characterization for the n-ary morphism determined by the Cayley-Bacharach process. We believe that the blending of universal algebra and algebraic geometry is an important application of universal algebra and a new tool for algebraic geometry. And the addition of automated theorem proving will do a great deal to bring attention to the role of computers in symbolic reasoning in real mathematical questions.

With these themes as our backdrop, let us now rephrase the uniqueness

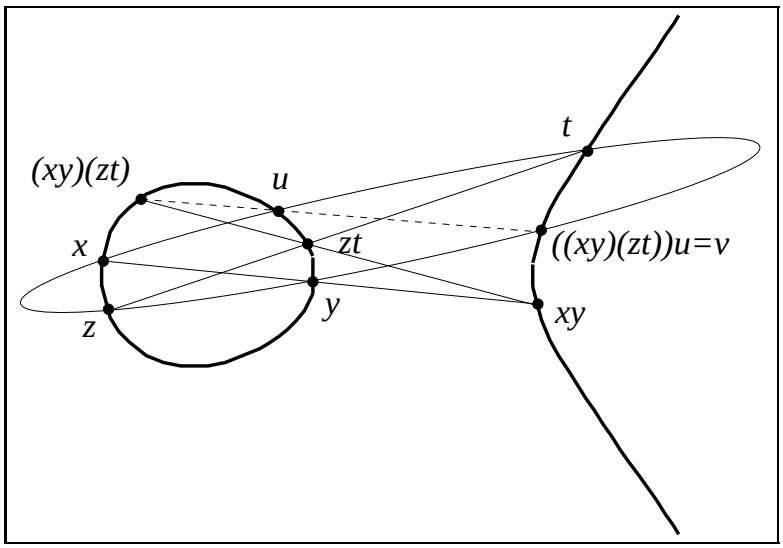

Figure 2: 5-ary Conic Process

of the Steiner law in the language of equational logic.

$$\left\{\begin{array}{l} f(x_1,\cdots,x_{n-1},f(x_1,\cdots,x_n))=x_n \\ f(e,...,e)=e \\ f(x_1,\cdots,x_n)=f(x_1,\cdots,x_{n-2},x_n,x_{n-1}) \\ f(x_1,\cdots,x_n)=f(x_2,\cdots,x_n,x_1) \\ g(x_1,\cdots,x_{n-1},g(x_1,\cdots,x_n))=x_n \\ g(e,...,e)=e \\ g(x_1,\cdots,x_n)=g(x_1,\cdots,x_{n-2},x_n,x_{n-1}) \\ g(x_1,\cdots,x_n)=g(x_2,\cdots,x_n,x_1) \end{array}\right\} \Rightarrow \{f=g\}$$

Of course, the above statement is not true if we do not insist that these are morphisms on the projective curve Γ. This gives rise to a model-theoretic question of whether one can extract some first-order properties from the theory of projective curves and formulate and prove the various uniqueness theorems within the framework of first-order logic with equality. The answer is an emphatic *yes*: the following rigidity lemma—a powerful local-to-global principle valid for morphisms of complete varieties—proves the validity of the above implications within the realms of first order logic with equality .

Lemma 1 *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*

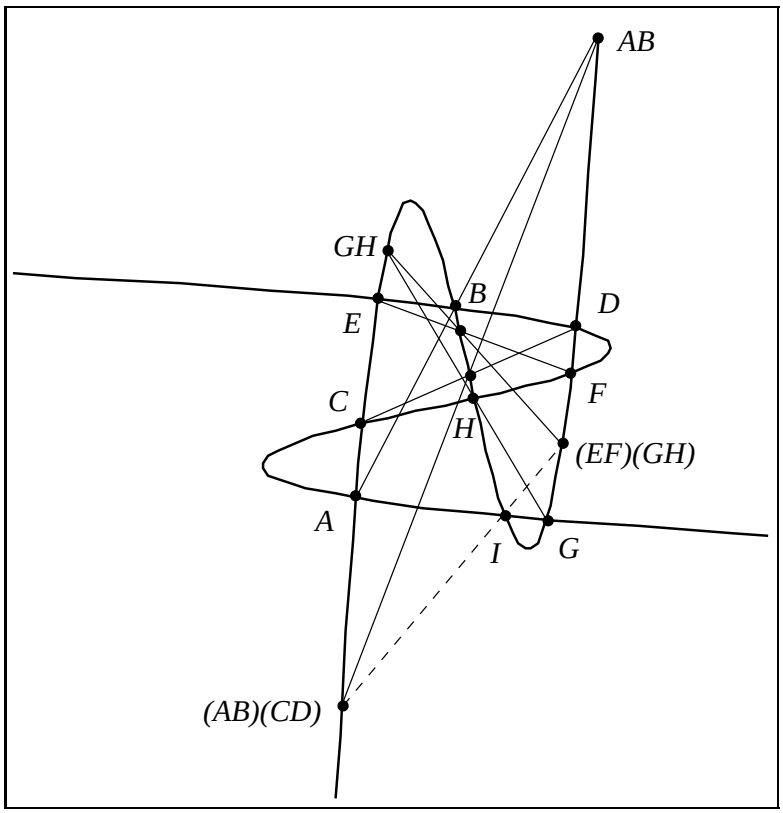

Figure 3: 8-ary Conic Process

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 found in [13, p. 156], [7, p. 104], or in [14, p. 156].

2 Methodology and Theorems

We now rewrite the rigidity lemma as a formal implication, where (gL) stands for "Local to global", "geometric Logic", "geometric Law".

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

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 [10]. See R. W. Quackenbush [12] 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, we write

$$\Sigma \ =\!(gL)\!\Rightarrow\ \sigma$$

if $\Sigma \cup (\mathrm{gL}) \Rightarrow \sigma$ 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 $\{x(yx) = y,\ (yz)z = y\}\ =\!(gL)\!\Rightarrow\ \{(xy)(zt) = (xz)(yt)\}$.

Proof. Define the 5-ary composite operation f by

$$f(x, y, z, t, u) = ((xy)(zt))(u((xz)(yt))).$$

By the law $x(yx) = y$, we have $f(x, c, c, t, d) = d$ 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

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

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 Fig. 4).*

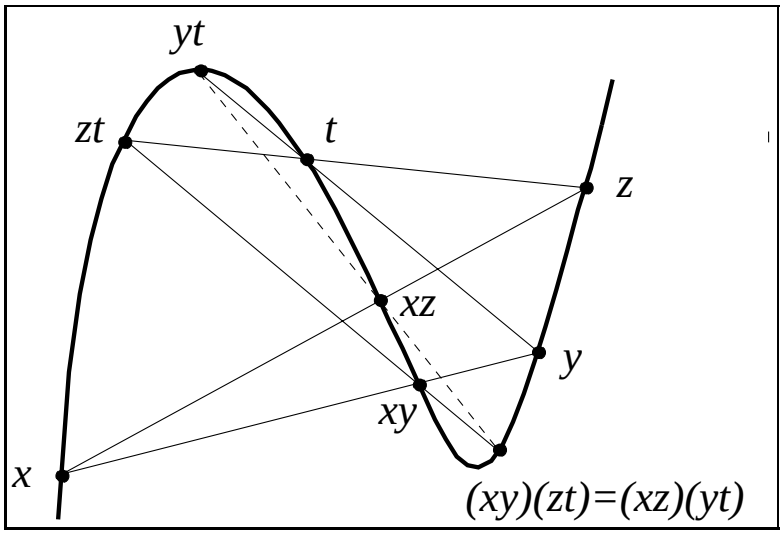

Figure 4: The Medial Law

Historical remark. This corollary was first proved for plane cubic curves by I. M. S. Etherington using the classical Bezout theorem (see [1]). In [10], Padmanabhan gave a proof for elliptic curves over an arbitrary algebraically closed field k (see also Knapp [3, pp. 67–74]).

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 the Implementation of $=\!(gL)\!\Rightarrow$

OTTER [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 an equality substitution rule 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 $\{f(x, f(g(x), y)) = y, f(u, g(u)) = e, f(w, e) = w\}$, where e is a constant; 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 OTTER in two ways that are analogous to paramodulation and demodulation. Let $F[a_1, x]$ represent a term 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 $f(x, z)$ and introducing the variable w. 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.** Each derived clause has a justification. The notation "$m \rightarrow n$" indicates paramodulation from m into n; ": $i, j, k, \ldots$" indicates rewriting with the demodulators $i, j, k, \ldots$; and ",flip" indicates that equality was reversed (usually so that the complex side occurs on the left). The justification "[(gL)" indicates the use of $=\!(gL)\!\Rightarrow$ as an inference rule, and ":(gL)" indicates its use as a rewrite rule.

As an example, we list here an OTTER proof of Theorem 1.

Proof (found by Otter 3.0.3+ on gyro at 20.49 seconds).

2	$x \cdot (y \cdot x) = y$	
4	$(x \cdot (y \cdot x)) \cdot (z \cdot y) = z$	$[2 \to 2]$
9	$(x \cdot y) \cdot x = y$	$[2 \to 2]$
38	$(x \cdot (y \cdot x)) \cdot (z \cdot y) = (u \cdot z) \cdot u$	$[9 \to 4]$
331	$(x \cdot (y \cdot z)) \cdot (u \cdot y) = (x \cdot u) \cdot z$	[(gL) 38]
333	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	$[2 \to 331]$

4 Uniqueness of n-ary Steiner Law

Theorem 2 *Let S be the set of identities of type $(n, n, 0)$ defined by*

$$S = \left\{ \begin{array}{l} p(e,e,e,e,e) = e \\ p \text{ is symmetric} \\ p(p(x,y,e,e,e),y,e,e,e) = x \end{array} \right\}$$

for p in $\{f, g\}$. Then $S \Rightarrow_{(gL)} \{f(x,y,z,u,v) = g(x,y,z,u,v)\}$.

Proof. Define the binary Steiner operation $x * y = f(x, y, e, ..., e)$. Now form the $(n+1)$-ary composite function $h(x_1, x_2, ..., x_n) = f((x_1, x_2, ..., x_n) * (u * g(x_1, x_2, ..., x_n))$. Let us substitute $x_2 = \cdots = x_n = e$ to obtain $h(x_1, e, e, ..., e) = u$. Thus, $h(x_1, e, e, ..., e) = h(z, e, e, ..., e)$.

So, by the rigidity lemma, the function h does not depend upon the variable x_1 and, by symmetry, does not depend upon x_i for all $i = 1, 2, \cdots, n$. Hence,

$$\begin{array}{rcl} f * (u * g) & = & \\ & = & h(x_1, x_2, ..., x_n) \\ & = & h(e, e, ..., e) \\ & = & f((e, e, ..., e) * (u * g(e, e, ..., e)) = e * (u * e) \\ & = & u. \end{array}$$

In other words $f * (u * g) = f * (u * f)$ and hence, by two successive right cancellations, we do obtain the desired equality $f = g$.

5 Geometric Interpretation of the Steiner Laws

First we need to borrow from [6] an inductive definition of words $W_n(x_1, \cdots, x_n)$ (mod 3), built using the binary morphism '$\cdot$' of chord-tangent construction Let $n \neq 0 \pmod 3$. Define $W_1(x_1) = x_1$, $W_2(x_1, x_2) = x_1 \cdot x_2$,

$W_4(x_1, x_2, x_3, x_4) = (x_1 \cdot x_2) \cdot (x_3 \cdot x_4)$ and $W_{i+1} = W_i \cdot x_{i+1}$ if $i = 1 \pmod 3$, and $W_{i+2} = W_i \cdot (x_{i+1} \cdot x_{i+2})$. Thus, for example, $W_5(x_1, x_2, x_3, x_4, x_5) = ((x_1 \cdot x_2) \cdot (x_3 \cdot x_4)) \cdot x_5$ which is precisely the ruler construction for finding the unique sixth point common to a cubic and the conic determined the five points $\{x_1, \cdots, x_5\}$.

Corollary 2 *For $n = 2$ (mod 3), let $f(x_1, x_2, \cdots, x_n)$ be an n-ary Steiner law on a non-singular cubic curve and let $f(e, e, ..., e) = e$ for some inflection point e on the curve. Then $f(x_1, x_2, \cdots, x_n) = W(x_1, x_2, \cdots, x_n)$.*

Proof. It is clear that $W(x_1, x_2, \cdots, x_n)$ is totally symmetric and that every inflection point is an idempotent for the n-ary operation W. Moreover, W satisfies the Steiner law $W(W(x, y, .., v), y, u, .., v) = x$. Hence, by the uniqueness theorem, $f = W$.

Since the operation W involves only the methods of chord and tangent, the above corollary actually gives ruler constructions for the various geometric processes involved. It is known that tangents for cubic curves can be drawn using only rulers.

In a similar fashion, we can derive the well-known theorem of the uniqueness of the group law on such a curve is shown to be a consequence of this result.

Corollary 3 *If $x + y$ and $x \cdot y$ are two group law on an elliptic curve, and if $e + e = e \cdot e = e$, where e is an inflection point, then $x + y = x \cdot y$ for all points x, y on the curve.*

Proof. Using the group law $x+y$, define the n-ary Steiner law $f(x, y, z, \cdots, u, v) = -x-y-z-\cdots-u-v$. Similarly, define the n-ary Steiner law $g(x, y, z, \cdots, u, v) = x'y'z' \cdots u'v'$. It is clear that f and g both have the element e as an idempotent. Now verify the n-ary Steiner law for f and g. Conclude $f = g$. Substitute $y = z = u = \cdots = v = e$ to get $-x = x'$. Thus $x + y = xy$.

Appendix A

This section contains a proof, obtained with help from the program OTTER, for the case $n = 8$. The OTTER proofs are the result of specialized search strategies devised by experimenting with smaller arities. Lemma 2 below,

proved with $=(gL)\Rightarrow$, gives us an equation that allows us to insert variables in a particular way. Then OTTER uses the lemma repeatedly to prove Theorem 3.

We then give an alternate proof of the corresponding n-ary theorem, for all n, that was found by extending (by hand) the 8-ary OTTER proofs.

Lemma 2

$$\left\{\begin{array}{l} f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) = f(x_1,x_2,x_3,x_4,x_5,x_6,x_8,x_7) \\ g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) = g(x_1,x_2,x_3,x_4,x_5,x_6,x_8,x_7) \\ g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)) = x_8 \\ g(e,e,e,e,e,e,e,e) = e \end{array}\right\}$$
$$=(gL)\Rightarrow$$
$$\left\{\begin{array}{l} f(x,y,z,u,v,w,x,g(v_7,v_8,v_9,v_{10},v_{11},v_{12},x,v_{13})) = \\ f(x,y,z,u,v,w,y,g(v_7,v_8,v_9,v_{10},v_{11},v_{12},y,v_{13})) \end{array}\right\}$$

Proof (found by Otter 3.0.3i on gyro at 128.46 seconds).

3 $f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) = f(x_1,x_2,x_3,x_4,x_5,x_6,x_8,x_7)$
6 $g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) = g(x_1,x_2,x_3,x_4,x_5,x_6,x_8,x_7)$
7 $g(e,e,e,e,e,e,e,e) = e$
8 $g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)) = x_8$
11 $f(x,y,z,u,v,w,v_6,g(e,e,e,e,e,e,e,e)) = f(x,y,z,u,v,w,e,v_6)$ [7 → 3]
15 $f(x,y,z,u,v,w,e,g(v_6,v_7,v_8,v_9,v_{10},v_{11},v_{12},g(v_6,v_7,v_8,v_9,v_{10},v_{11},v_{12},v_{13}))) =$
$f(x,y,z,u,v,w,v_{13},g(e,e,e,e,e,e,e,e))$ [8 → 11, flip]
24 $f(x,y,z,u,v,w,e,g(v_6,v_7,v_8,v_9,v_{10},v_{11},v_{12},g(v_6,v_7,v_8,v_9,v_{10},v_{11},v_{13},v_{12}))) =$
$f(x,y,z,u,v,w,v_{13},g(e,e,e,e,e,e,e,e))$ [6 → 15]
31 $f(x,y,z,u,v,w,e,g(v_6,v_7,v_8,v_9,v_{10},v_{11},v_{12},g(v_6,v_7,v_8,v_9,v_{10},v_{11},e,v_{13}))) =$
$f(x,y,z,u,v,w,v_{13},g(e,e,e,e,e,e,v_{12},e))$ [(gL) 15]
88 $f(x,y,z,u,v,w,e,g(v_6,v_7,v_8,v_9,v_{10},v_{11},e,v_{12})) =$
$f(x,y,z,u,v,w,v_{13},g(v_6,v_7,v_8,v_9,v_{10},v_{11},v_{13},v_{12}))$
[24 → 31 :(gL) :(gL) :(gL) :(gL) :(gL) :(gL) :(gL)]
95 $f(x,y,z,u,v,w,v_6,g(v_7,v_8,v_9,v_{10},v_{11},v_{12},v_6,v_{13})) =$
$f(x,y,z,u,v,w,v_{14},g(v_7,v_8,v_9,v_{10},v_{11},v_{12},v_{14},v_{13}))$ [88 → 88]

Theorem 3

$$\left\{\begin{array}{l} f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)) = x_8 \\ f(e,e,e,e,e,e,e,e) = e \\ f \textit{ is symmetric} \\ g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)) = x_8 \\ g(e,e,e,e,e,e,e,e) = e \\ g \textit{ is symmetric} \end{array}\right\} \Rightarrow \{f = g\}$$

Proof (found by Otter 3.0.3i on gyro at 13.36 seconds). By Lemma 2, we include equation 7 below. Rule 2 below follows from symmetry of f and g.

2 $g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) = f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8) \rightarrow$
$g(x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_1) = f(x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_1)$
3 $f(e,e,e,e,e,e,e,e) = e$
4 $f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)) = x_8$
5 $g(e,e,e,e,e,e,e,e) = e$
6 $g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)) = x_8$
7 $f(x,y,z,u,v,w,v_6,g(v_7,v_8,v_9,v_{10},v_{11},v_{12},v_6,v_{13})) =$
$f(x,y,z,u,v,w,v_{14},g(v_7,v_8,v_9,v_{10},v_{11},v_{12},v_{14},v_{13}))$
10 $f(e,e,e,e,e,e,e,g(e,e,e,e,e,e,e,e)) = e$ [5 → 3]
11 $f(e,e,e,e,e,e,x,g(e,e,e,e,e,e,x,e)) = e$ [7 → 10]
12 $g(e,e,e,e,e,e,x,e) = f(e,e,e,e,e,e,x,e)$ [11 → 4, flip]
13 $g(e,e,e,e,e,x,e,e) = f(e,e,e,e,e,x,e,e)$ [12,2]
15 $f(e,e,e,e,e,x,e,g(e,e,e,e,e,x,e,e)) = e$ [13 → 4]
18 $f(e,e,e,e,e,x,y,g(e,e,e,e,e,x,y,e)) = e$ [7 → 15]
19 $g(e,e,e,e,e,x,y,e) = f(e,e,e,e,e,x,y,e)$ [18 → 4, flip]
20 $g(e,e,e,e,x,y,e,e) = f(e,e,e,e,x,y,e,e)$ [19,2]
22 $f(e,e,e,e,x,y,e,g(e,e,e,e,x,y,e,e)) = e$ [20 → 4]
25 $f(e,e,e,e,x,y,z,g(e,e,e,e,x,y,z,e)) = e$ [7 → 22]
26 $g(e,e,e,e,x,y,z,e) = f(e,e,e,e,x,y,z,e)$ [25 → 4, flip]
27 $g(e,e,e,x,y,z,e,e) = f(e,e,e,x,y,z,e,e)$ [26,2]
29 $f(e,e,e,x,y,z,e,g(e,e,e,x,y,z,e,e)) = e$ [27 → 4]
32 $f(e,e,e,x,y,z,u,g(e,e,e,x,y,z,u,e)) = e$ [7 → 29]
33 $g(e,e,e,x,y,z,u,e) = f(e,e,e,x,y,z,u,e)$ [32 → 4, flip]
34 $g(e,e,x,y,z,u,e,e) = f(e,e,x,y,z,u,e,e)$ [33,2]
36 $f(e,e,x,y,z,u,e,g(e,e,x,y,z,u,e,e)) = e$ [34 → 4]
39 $f(e,e,x,y,z,u,v,g(e,e,x,y,z,u,v,e)) = e$ [7 → 36]
40 $g(e,e,x,y,z,u,v,e) = f(e,e,x,y,z,u,v,e)$ [39 → 4, flip]
41 $g(e,x,y,z,u,v,e,e) = f(e,x,y,z,u,v,e,e)$ [40,2]
43 $f(e,x,y,z,u,v,e,g(e,x,y,z,u,v,e,e)) = e$ [41 → 4]
46 $f(e,x,y,z,u,v,w,g(e,x,y,z,u,v,w,e)) = e$ [7 → 43]
47 $g(e,x,y,z,u,v,w,e) = f(e,x,y,z,u,v,w,e)$ [46 → 4, flip]
48 $g(x,y,z,u,v,w,e,e) = f(x,y,z,u,v,w,e,e)$ [47,2]
50 $f(x,y,z,u,v,w,e,g(x,y,z,u,v,w,e,e)) = e$ [48 → 4]
53 $f(x,y,z,u,v,w,v_6,g(x,y,z,u,v,w,v_6,e)) = e$ [7 → 50]
54 $g(x,y,z,u,v,w,v_6,e) = f(x,y,z,u,v,w,v_6,e)$ [53 → 4, flip]
55 $g(x,y,z,u,v,w,e,v_6) = f(x,y,z,u,v,w,e,v_6)$ [54,2]
57 $f(x,y,z,u,v,w,e,g(x,y,z,u,v,w,e,v_6)) = v_6$ [6 → 55, flip]
60 $f(x,y,z,u,v,w,v_6,g(x,y,z,u,v,w,v_6,v_7)) = v_7$ [7 → 57]
61 $g(x,y,z,u,v,w,v_6,v_7) = f(x,y,z,u,v,w,v_6,v_7)$ [6 → 60, flip]

Theorem 4 *Uniqueness of the n-ary Steiner law.*

Proof. We show that an equational proof, analogous to the proofs of Lemma 2 and Theorem 3, can be constructed for any n. This proof differs from the proof of Theorem 2 in that here we use the the rule $=\!(gL)\!\Rightarrow$ as implemented in OTTER. We first prove

$$f(v_1, \cdots, v_{n-2}, x, g(z_1, \cdots, z_{n-2}, x, y)) = f(v_1, \cdots, v_{n-2}, w, g(z_1, \cdots, z_{n-2}, w, y)). \tag{1}$$

Consider a proof, for the binary case, of

$$f(x, g(x, y)) = f(w, g(w, y)).$$

With that proof, insert $n-2$ e's at the beginning of each operation to obtain a proof of

$$f(e, \cdots, e, x, g(e, \cdots, e, x, y)) = f(e, \cdots, e, w, g(e, \cdots, e, w, y)).$$

Now apply $=\!(gL)\!\Rightarrow$ to each occurrence of e to obtain (1). (From this point on, we do not use $=\!(gL)\!\Rightarrow$.) We start with

$$f(e, \cdots, e, g(e, \cdots, e, e)) = e,$$

then apply (1) to get

$$f(e, \cdots, e, x, g(e, \cdots, e, x, e)) = e.$$

Use symmetry of f ang g to move variables left one position:

$$f(e, \cdots, e, x, e, g(e, \cdots, e, x, e, e)) = e.$$

Repeat the preceding two steps, introducing new variables, and rotating left, until we get

$$f(x_1, \cdots, x_{n-1}, g(x_1, \cdots, x_{n-1}, e)) = e.$$

Apply the f Steiner law to get

$$f(x_1, \cdots, x_{n-1}, e) = g(x_1, \cdots, x_{n-1}, e).$$

Apply the g Steiner law, obtaining

$$f(x_1, \cdots, x_{n-2}, e, g(x_1, \cdots, x_{n-2}, e, y)) = y.$$

Apply (1), replacing e with z:

$$f(x_1, \cdots, x_{n-2}, z, g(x_1, \cdots, x_{n-2}, z, y)) = y.$$

Apply the g Steiner law to finish the proof:

$$f(x_1, \cdots, x_n) = g(x_1, \cdots, x_n).$$

References

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

[2] P. Griffiths and J. Harris. *Principles of Algebraic Geometry.* Wiley, New York, 1978.

[3] A. Knapp, editor. *Elliptic Curves.* Princeton University Press, 1993.

[4] W. McCune. OTTER 3.0 Reference Manual and Guide. Tech. Report ANL-94/6, Argonne National Laboratory, Argonne, IL, 1994.

[5] W. McCune and R. Padmanabhan. An equational characterization of the conic construction on cubic curves. Preprint ??, Argonne National Laboratory, Argonne, IL, 1995.

[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] D. Mumford. *Algebraic Geometry I, Complex Projective Varieties.* Springer-Verlag, 1970.

[9] Makoto Namba. , *Geometry of Projective Algebraic Curves.* Marcel Dekker, New York, 1984.

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

[11] R. Padmanabhan and W. McCune. Automated reasoning about cubic curves. *Computers and Mathematics with Applications*, 29(2):17–26, 1995.

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

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

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

[15] R. J. Walker. *Algebraic Curves.* Springer-Verlag, New York, 1978.

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