Uniqueness of Steiner Laws on Cubic Curves

R. Padmanabhan[*]
Department of Mathematics
University of Manitoba
Winnipeg, Manitoba R3T 2N2
Canada
E-mail: padman@cc.umanitoba.ca

W. McCune[†]
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60439-4844
U.S.A.
E-mail: mccune@mcs.anl.gov

Abstract. In this paper we use the Cayley-Bacharach theorem of classical algebraic geometry to construct several universal algebras on algebraic curves using divisors and complete intersection cycles and study the equational identities valid for these synthetic constructions. These results are not necessarily new; in fact, all of them may be "easily" provable by resorting to such powerful tools as the Riemann-Roch theorem, the $\mathcal{P}$-function of Weierstrass, the rigidity lemma, Euler numbers, Lefschetz fixed-point theorem, and so on. However, our equational proofs employ automated reasoning by transforming the Cayley-Bacharach theorem into a formal implication. Besides being elementary, this approach provides new examples for model theorists and computer scientists designing theorem provers and gives new insights and interpretations for these various geometric constructions.

AMS Subject Classification (1991). 14N05, 20N15, 51M15, 68T15.

Key Words and Phrases. Cubic curves, Cayley-Bacharach theorem, n-ary composition laws, Steiner laws, geometric constructions, uniqueness theorems, automated reasoning, Otter, inference rules.

1 Introduction

Let C be a nonsingular cubic curve in the complex projective plane. If a and b are two distinct points on the curve, let $c = a * b$ be the (unique) third point of intersection with C of the line $L(a, b)$ joining a and b. If $b = a$, then we naturally take the line $L(a, b)$ to be the tangent at a. More formally, the set $\{a, b, a * b\}$ is

[*] Supported by an operating grant from NSERC of Canada (OGP8215).

[†] 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.

the complete intersection cycle of the curve C with $L(a,b)$ counting multiplicities. If the ground field k is different from complex numbers, we insist that the points a and b are k-rational points. In that case, the unique third point $a*b$ is obviously k-rational, thus making the cubic curves very interesting. In fact, if e is chosen to be an inflection point (again, k-rational if $k \neq C$), then the composite term $(a*b)*e$ is the classical Poincare group law on C. Clearly, the rational binary operation "$*$" viewed as a mapping from $C \times C$ to C (or from $C(k) \times C(k)$ to $C(k)$ if k is not algebraically closed) satisfies the following universal identities: $x*y = y*x$, $x*(y*x) = y$. This is an example of a binary Steiner law and the idempotents of $*$ are precisely the inflection points of the curve (see Fig. 1). More generally, an n-ary Steiner law $f(x_1, x_2, \ldots, x_n)$ on a projective curve C over k is a totally symmetric rational n-ary function f from C^n to C satisfying the universal identity

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

An element e in C is called an idempotent for f if $f(e, e, ...e) = e$. In this paper, we prove that if f and g are two n-ary Steiner laws on an elliptic curve C sharing a common idempotent, then $f = g$. First, we extract a special case of the inference rule (gL) — indeed, a fragment of the powerful rigidity lemma — from the Cayley-Bacharach theorem of classical algebraic geometry. This rule is implemented in OTTER, a first-order theorem-proving program [6]. Then we use OTTER to automate the proofs of the uniqueness of the 5-ary Steiner laws definable on an elliptic curves. Very much like the binary case, this theorem provides algebraic characterizations of synthetic geometric constructions involving the intersection cycles of cubics with algebraic curves of higher degrees. The well-known theorem of the uniqueness of the group law on such a curve is an extreme special case of this result.

A set P of p points in $PG(2,k)$, a projective plane over a field k, is said to have the Cayley-Bacharach property (CB-property) of degree d if any plane curve of degree d passing through all but one point of P necessarily contains the whole of P. The Cayley-Bacharach theorem of algebraic geometry (see, e.g., [1, 3]) says that if P is a set of mn points that is a complete intersection cycle of two curves of degrees m and n, then P has the CB-property of degree $m+n-3$. This classical result is rife with rich rational universal algebras (i.e., rational constructions that yield unique points). In this paper, we employ the techniques of the Bezout theorem and the CB-theorem to prove that every algebraic curve induces a rational Steiner operation on cubic curves via a complete intersection cycle (see, e.g., Fig. 1 for the binary linear process and Fig. 4 for the 5-ary conic process).

All the proofs in this paper reside completely within the framework of first-order logic with equality. First we show that the Cayley-Bacharach theorem implies the validity of a formal implication that is a fragment of the rule (gL) or the "term condition" — an algebraic avatar of the rigidity lemma of algebraic geometry. Then we exploit this in finding interrelations among various algebraic laws of different arities obtained via the Cayley-Bacharach constructions on algebraic curves. Normally, one would employ the parameters of the elliptic functions of Weierstrass, the group law via the Riemann-Roch theorem or the so-called AF+BG theorem of Max Noether to prove such results in the projective geometry over elliptic curves.

This paper (especially the proof of the basic (gL) implication) was inspired by the excellent survey article [1] which gives a beautiful exposition of the Cayley-

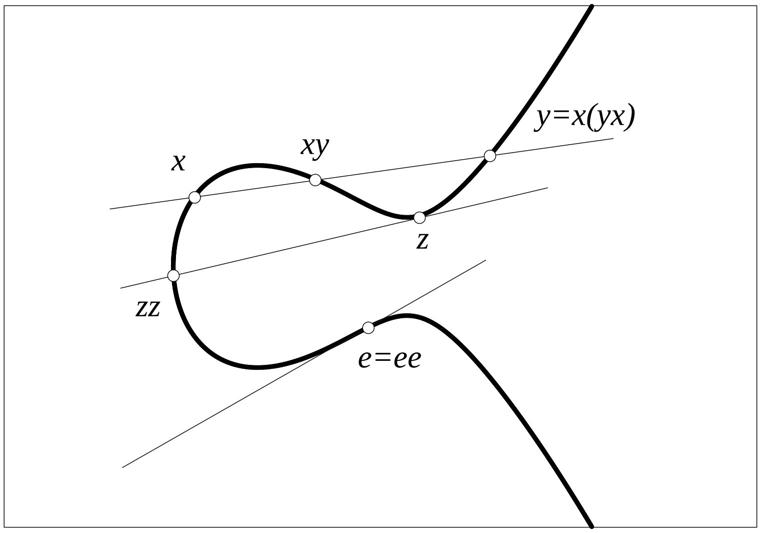

Figure 1: Chord-Tangent Construction

Bacharach theorem, its origins, and modern evolutions.

2 Cayley-Bacharach Theorem Implies the $=\!\!(gL)\!\!\Rightarrow$ Rule for Cubics

Cayley-Bacharach Theorem. *If P is a set of mn points that is a complete intersection cycle of two curves of degrees m and n, then any plane curve of degree $m+n+3$ passing through all but one point of P necessarily contains the whole of P.*

Theorem 1. *Let C be a nonsingular cubic curve over the complex projective plane and let "$*$" be the binary morphism of chord-tangent construction. Then the algebra $\langle C; *\rangle$ satisfies the implication*

$$(a*b)*c = (a*d)*e \quad \Rightarrow \quad (x*b)*c = (x*d)*e.$$

Proof. Let Q_1 be the quartic formed by the four lines $\{1\cup 2\cup 3\cup 4\}$, let Q_2 be the quartic formed by the four lines $\{5\cup 6\cup 7\cup 8\}$, and let C be the given nonsingular cubic curve. See Fig. 2. We have

$$\begin{array}{rcl} C\cap Q_1 & = & \{a, d, a*d, c, a*b, (a*b)*c, e, x*d, (x*d)*e, x, b, x*b\}, \\ C\cap Q_2 & = & \{e, a*d, (a*d)*e, x, d, x*d, a, b, a*b, c, x*b, (x*b)*c\}. \end{array}$$

Hence, if $(a*b)*c = (a*d)*e$, then both Q_1 and Q_2 share 11 common points with the base cubic C. Here both Q_1 and Q_2 are quartics; and so, by the Cayle-Bacharach theorem they must share the 12th common point as well. Thus $(x*b)*c = (x*d)*e$. This completes the proof of the implication

$$(a*b)*c = (a*d)*e \quad \Rightarrow \quad (x*b)*c = (x*d)*e.$$

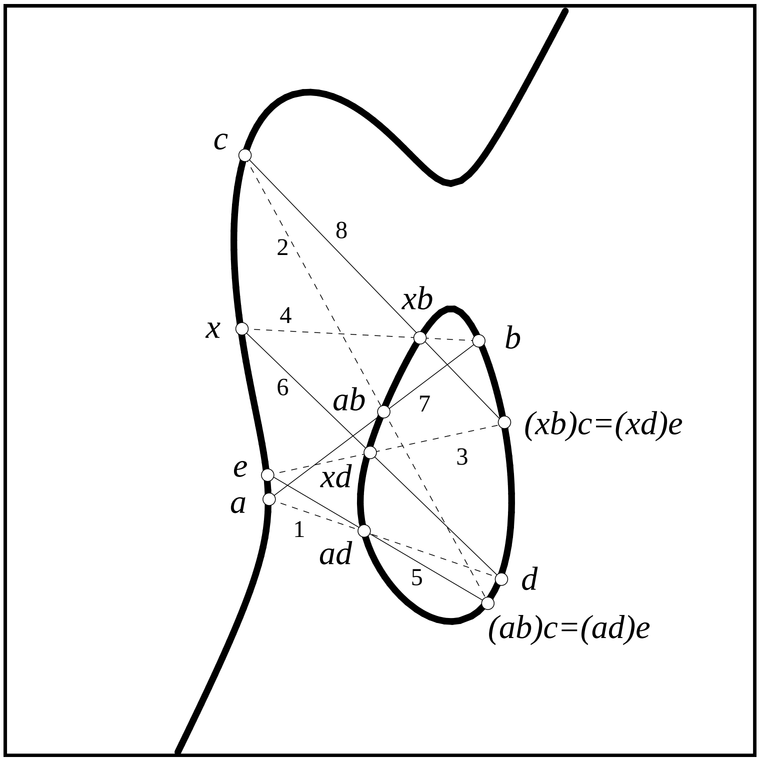

Figure 2: Basic (gL)

In what follows, we call this implication the "basic (gL) rule for cubics" or simply "basic (gL)". This is only a special case of the full version of the rule (gL), which in turn is a modern avatar of the powerful rigidity lemma of complete varieties: $f(x, b) = c \Rightarrow f(x, z) = f(y, z)$ for all terms f in the mathematical structure in question (see [7], page 37 and [11] for more details and references about the related conditions like the term condition).

Theorem 2. *Basic (gL) for cubics* $\Rightarrow$ *the identity* $((u * v) * w) * t = ((t * v) * w) * u$.

Proof. (See the appendix for an Otter proof.) Thanks to the commutative and Steiner laws, we have

$$(w * ((t * v) * w)) * t = (w * ((u * v) * w)) * u$$

because both sides reduce to the variable v. This equality looks like the left hand side of the implication basic (gL) with the following identifications:

$$a = w, b = (t * v) * w, c = t, d = (u * v) * w, e = u.$$

Hence, by the conclusion of the implication basic (gL), we have

$$(x * b) * c = (x * d) * e$$

for all points x on the cubic. In other words, we have

$$(x * ((t * v) * w)) * t = (x * ((u * v) * w)) * u.$$

Substituting $x = t$ and simplifying, we get

$$(t * v) * w) = (t * ((u * v) * w)) * u,$$

which, modulo the commutative and Steiner laws, is the same as

$$((t * v) * w) * u = ((u * v) * w) * t.$$

Theorem 3. *The binary Steiner law $*$ on a nonsingular cubic curve satisfies the medial identity $(x * y) * (z * u) = (x * z) * (y * u)$.* (See Fig. 3.)

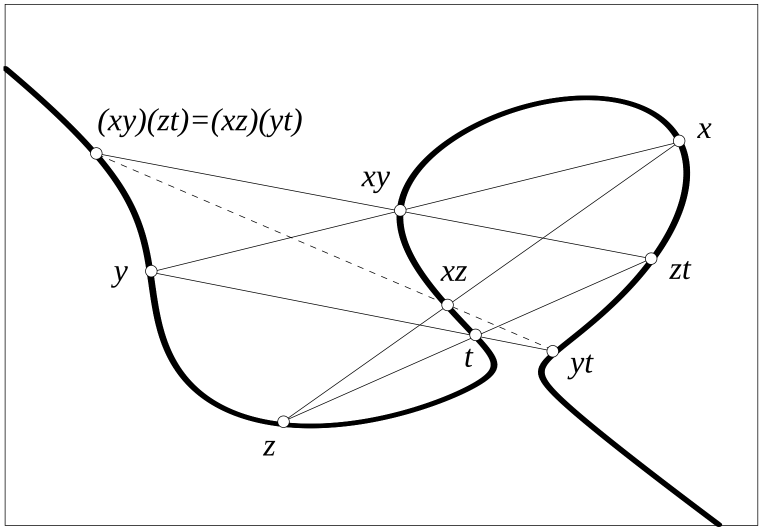

Figure 3: The Medial Identity

Proof. (See the Appendix for an OTTER proof.) It is enough to derive the medial law from the basic (gL). We work backward to show how naturally the implication of basic (gL) works to prove such consequences. We want to derive the identity $(x * y) * (z * u) = (x * z) * (y * u)$. This equality looks exactly like the conclusion of basic (gL) and hence all we need to do is to find a suitable term $a = a(y, z, u)$ such that the relation $(a * y) * (z * u) = (a * z) * (y * u)$. The term $a = y * z$ would do the job because in this case both sides reduce to u.

Historical Remark. The validity of the median law for $*$ was first proved for plane cubics by Etherington [2]. See Knapp [4] for a different and a rather complete proof including the cases where two or more points may coincide. The first automated proof of the median law using the rule (gL) was given in [11] and [12].

To further demonstrate the impact of the Cayley-Bacharach theorem on the geometry of the cubic curves, we show that the formal property of basic (gL) for a binary Steiner law $*$ along with a mild grouplike homomorphism connection with $+$, a binary law of composition, does characterize the $+$ as the (unique) group law. More precisely, we prove the following.

Theorem 4. *Let Σ be*

$$\{x * (y * x) = y, x * y = y * x, e * e = e, (x * e) + (e * y) = x * y\}.$$

Then $\Sigma \;=\!(basic - gL)\!\Rightarrow\; x + y = e * (x * y)$*, where* $+$ *is an Abelian group law.*

Proof. (Found by Otter 3.0.5b in 1.94 seconds; see Sec. 3 for an explanation of the proof notation.)

3	$x * (y * x) = y$	
5	$x * y = y * x$	
6	$e * e = e$	
8	$(x * e) + (e * y) = x * y$	
10	$(x * y) * z = (x * u) * v \;\rightarrow\; (w * y) * z = (w * u) * v$	
11	$(x * y) * x = y$	[3 → 3]
13	$(x * y) * y = x$	[3 → 5, flip]
16,15	$x * (x * y) = y$	[5 → 3]
18,17	$x + (e * y) = (x * e) * y$	[13 → 8]
19	$(x * e) * y = (e * x) * y$	[11 → 8 :18]
26	$(e * x) * y = (x * e) * y$	[flip 19]
27	$x + y = (x * e) * (e * y)$	[15 → 17]
44	$(x * e) * (y * (e * x)) = y$	[3 → 26, flip]
50	$(x * ((y * z) * u)) * y = (x * z) * u$	[10,11]
296	$(x * (e * y)) * e = (x * e) * y$	[6 → 50]
303	$(x * y) * z = (x * e) * (y * (e * z))$	[44 → 50]
349	$(x * e) * (y * (e * z)) = (x * y) * z$	[flip 303]
424,423	$(x * e) * y = e * (x * (e * y))$	[5 → 296, flip]
445,444	$(x * y) * z = e * (x * (e * (y * (e * z))))$	[349 :424, flip]
492	$x + y = e * (x * y)$	[27 :445,16,16]

To complete the proof that $+$ defines a group law, one notices that the associativity is simply the identity of Theorem 2:

$$\begin{aligned} x + (y + z) &= e * (x * (e * (y * z))) \\ &= e * (z * (e * (y * x))) \\ &= z + (y + x), \end{aligned}$$

and hence the binary operation $+$ is both associative and commutative. Clearly, $x + e = x$. Finally, defining x' as $e * x$, we have $x + x' = x + (e * x) = e * (x * (e * x)) = e * e = e$.

Remark. Contrast this with the results in the appendix.

3 Otter and the Implementation of the Rule (gL)

Let us now compare the basic (gL) rule with the rigidity lemma:

Basic (gL) for cubics:	$(a * b) * c = (a * d) * e \Rightarrow (x * b) * c = (x * d) * e.$
Full (gL) for cubics:	$F(a, b) = F(a, c) \Rightarrow F(x, b) = F(x, c)$ for all morphisms F of the curve.
Rigidity for cubics:	$F(x, b) = c \Rightarrow F(x, z) = F(y, z)$ for all morphisms F of the curve.

Thus it is clear that while the basic (gL) for cubics deals only with the single binary operation $*$, the full (gL) — equivalent to the rigidity lemma, see Theorem 3.3 of [7] — involves all possible morphisms and thus provides the necessary glue that binds together these various rational morphisms and gives new and elementary equational proofs to show that all these synthetic operations of higher arities can be obtained by ruler constructions. Unlike the full (gL), the basic (gL) for $*$ is of little use if we assume no further connection between $*$ and other operations (see, for example, the Appendix). Since we discuss the uniqueness of Steiner laws on cubics, we employ the full (gL) as an inference rule as well as a rewrite rule.

Otter [6] 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 full 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 "$m \to n$" indicates paramodulation from m into n; ": $i, j, k, \ldots$" indicates rewriting with the equations $i, j, k, \ldots$; 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.

4 Uniqueness of n-ary Steiner Law on Cubics

In this section, we show that a nonsingular cubic curve admits exactly one n-ary Steiner law for every n congruent to $2 (mod\ 3)$. If $n = 2$, this is the usual chord-tangent process. We give a complete proof for the next case, $n = 5$ (the "conic process"). The proof of the general case is similar and can be proved by induction. Let C be a nonsingular cubic, and let x, y, z, t, u be five points on the curve. Let Q be the unique conic determined by these 5 points. By the celebrated Bezout theorem of classical geometry, we have $|C \cap Q| = 6$, counting multiplicities. Now let $f(x, y, z, t, u)$ be the 5-ary morphism on C defined by the complete intersection cycle

$$C \cap Q = \{x, y, z, t, u, f(x, y, z, t, u)\}.$$

Then the unique sixth point $f(x, y, z, t, u)$ can be found by a simple ruler construction as shown in Fig. 4. A formal proof using the rigidity lemma was given by N. S. Mendelsohn, R. Padmanabhan, and B. Wolk in [8]. Here we would like to characterize the above synthetic geometric process by means of equational identities.

The 5-ary law is totally symmetric in all of its five arguments, and every inflection point is an idempotent for f: $f(e, e, e, e, e) = e$. The geometric reason for this is that the intersection multiplicity at a flex point e is six. Moreover, it satisfies the Steiner identity $f(e, e, e, x, f(e, e, e, x, y)) = y$. We claim that a nonsingular cubic curve over an algebraically closed field admits exactly one such 5-ary morphism.

Lemma 1.

$$\left\{\begin{array}{l} f(x,y,z,u,v) = f(x,y,z,v,u) \\ f(e,e,e,e,e) = e \\ f(e,e,e,x,f(e,e,e,x,y)) = y \end{array}\right\} =\!(gL)\!\Rightarrow \ \{f(u,v,w,x,f(u,v,w,x,y)) = y\}.$$

Proof. (Found by Otter 3.0.5b on soot.mcs.anl.gov in 0.48 seconds, with a specialized search strategy.)

3 $f(x,y,z,u,v) = f(x,y,z,v,u)$

4 $f(e,e,e,e,e) = e$

7,6 $f(e,e,e,x,f(e,e,e,x,y)) = y$

9,8 $f(e,e,e,x,f(e,e,e,y,x)) = y$ [3 → 6]

12 $f(x,y,z,u,f(e,e,e,u,e)) = f(x,y,z,e,e)$ [6 → 4 :(gL) :(gL) :(gL), flip]

21 $f(e,e,e,x,f(y,z,u,f(v,w,v_6,e,e),x)) = f(v,w,v_6,v_7,f(y,z,u,v_7,e))$ [8 → 12 :(gL) :(gL) :(gL), flip]

485 $f(x,y,z,f(x,y,z,e,e),u) = f(e,e,e,e,u)$ [(gL) 21, flip]

533 $f(x,y,z,u,f(x,y,z,u,e)) = e$ [485 → 21 :9, flip]

613 $f(u,v,w,x,f(u,v,w,x,y)) = y$ [6 → 533 :(gL) :7]

Lemma 2.

$$\left\{\begin{array}{l} f(x,y,z,u,v) = f(x,y,z,v,u) \\ g(x,y,z,u,v) = g(x,y,z,v,u) \\ g(u,v,w,x,g(u,v,w,x,y)) = y \\ g(e,e,e,e,e) = e \end{array}\right\} =\!(gL)\!\Rightarrow$$

$$\{f(x,y,z,u,g(v,w,v_6,u,v_7)) = f(x,y,z,v_8,g(v,w,v_6,v_8,v_7))\}$$

Proof. (Found by Otter 3.0.5b on soot.mcs.anl.gov in 0.85 seconds, with a specialized search strategy.)

3 $f(x,y,z,u,v) = f(x,y,z,v,u)$

5 $g(x,y,z,u,v) = g(x,y,z,v,u)$

6 $g(e,e,e,e,e) = e$

7 $g(u,v,w,x,g(u,v,w,x,y)) = y$

9 $f(x,y,z,u,g(e,e,e,e,e)) = f(x,y,z,e,u)$ [6 → 3]

10 $f(x,y,z,e,g(u,v,w,v_6,g(u,v,w,v_6,v_7))) = f(x,y,z,v_7,g(e,e,e,e,e))$ [7 → 9, flip]

13 $f(x,y,z,e,g(u,v,w,v_6,g(u,v,w,v_7,v_6))) = f(x,y,z,v_7,g(e,e,e,e,e))$ [5 → 10]

17 $f(x,y,z,e,g(u,v,w,v_6,g(u,v,w,e,v_7))) = f(x,y,z,v_7,g(e,e,e,v_6,e))$ [(gL) 10]

33 $f(x,y,z,e,g(u,v,w,e,v_6)) = f(x,y,z,v_7,g(u,v,w,v_7,v_6))$
[13 → 17 :(gL) :(gL) :(gL) :(gL)]

40 $f(x,y,z,u,g(v,w,v_6,u,v_7)) = f(x,y,z,v_8,g(v,w,v_6,v_8,v_7))$ [33 → 33]

Theorem 5. *Let S be the set of identities of type (5,5,0) defined by*

$$S = \left\{ \begin{array}{lll} f(e,e,e,e,e) = e, & f \text{ is symmetric}, & f(e,e,e,x,f(e,e,e,x,y)) = y, \\ g(e,e,e,e,e) = e, & g \text{ is symmetric}, & g(e,e,e,x,g(e,e,e,x,y)) = y. \end{array} \right\}$$

Then $S =\!(gL)\!\Rightarrow \{f(x,y,z,u,v) = g(x,y,z,u,v)\}$.

By Lemmas 1 and 2, we assume

$$\begin{array}{l} f(u,v,w,x,f(u,v,w,x,y)) = y, \\ g(u,v,w,x,g(u,v,w,x,y)) = y, \\ f(x,y,z,u,g(v,w,v_6,u,v_7)) = f(x,y,z,v_8,g(v,w,v_6,v_8,v_7)). \end{array}$$

Proof. (Found by Otter 3.0.5b on soot.mcs.anl.gov at 0.34 seconds, with a specialized search strategy.) Full symmetry of the operations causes an explosion in the Otter search space; to constrain the search, we incompletely specify symmetry with deduction rule 2 below.

2 $g(x,y,z,u,v) = f(x,y,z,u,v) \ \rightarrow\ g(y,z,u,v,x) = f(y,z,u,v,x)$

3 $f(e,e,e,e,e) = e$

4 $f(u,v,w,x,f(u,v,w,x,y)) = y$

5 $g(e,e,e,e,e) = e$

6 $g(u,v,w,x,g(u,v,w,x,y)) = y$

7 $f(x,y,z,u,g(v,w,v_6,u,v_7)) = f(x,y,z,v_8,g(v,w,v_6,v_8,v_7))$

10 $f(e,e,e,e,g(e,e,e,e,e)) = e$ [5 → 3]

11 $f(e,e,e,x,g(e,e,e,x,e)) = e$ [7 → 10]

12 $g(e,e,e,x,e) = f(e,e,e,x,e)$ [11 → 4, flip]

13 $g(e,e,x,e,e) = f(e,e,x,e,e)$ [12,2]

15 $f(e,e,x,e,g(e,e,x,e,e)) = e$ [13 → 4]

18 $f(e,e,x,y,g(e,e,x,y,e)) = e$ [7 → 15]

19 $g(e,e,x,y,e) = f(e,e,x,y,e)$ [18 → 4, flip]

20 $g(e,x,y,e,e) = f(e,x,y,e,e)$ [19,2]

22 $f(e,x,y,e,g(e,x,y,e,e)) = e$ [20 → 4]

25 $f(e,x,y,z,g(e,x,y,z,e)) = e$ [7 → 22]

26 $g(e,x,y,z,e) = f(e,x,y,z,e)$ [25 → 4, flip]

27 $g(x,y,z,e,e) = f(x,y,z,e,e)$ [26,2]

29 $f(x,y,z,e,g(x,y,z,e,e)) = e$ [27 → 4]

32	$f(x,y,z,u,g(x,y,z,u,e)) = e$	[7 → 29]
33	$g(x,y,z,u,e) = f(x,y,z,u,e)$	[32 → 4, flip]
34	$g(x,y,z,e,u) = f(x,y,z,e,u)$	[33,2]
36	$f(x,y,z,e,g(x,y,z,e,u)) = u$	[6 → 34, flip]
39	$f(x,y,z,u,g(x,y,z,u,v)) = v$	[7 → 36]
40	$g(x,y,z,u,v) = f(x,y,z,u,v)$	[6 → 39, flip]

Line 40 completes the proof of Theorem 5.

Corollary 1 *$f(x,u,z,t,u) = ((x * y) * (z * t)) * u$, where "$*$" stands for the binary morphism of secant-tangent construction on the cubic.*

Proof. Define $g(x,y,z,t,u) = ((x * y) * (z * t)) * u$. It is clear that g is totally symmetric and that every flex point is an idempotent for g. Moreover, g satisfies the two-variable identity $g(e,e,e,x,g(e,e,e,x,y)) = y$. Hence by Theorem 5, $f = g$.

This gives the well-known ruler construction to locate the unique sixth point $f(x,y,z,t,u)$ on the cubic. See Fig. 4.

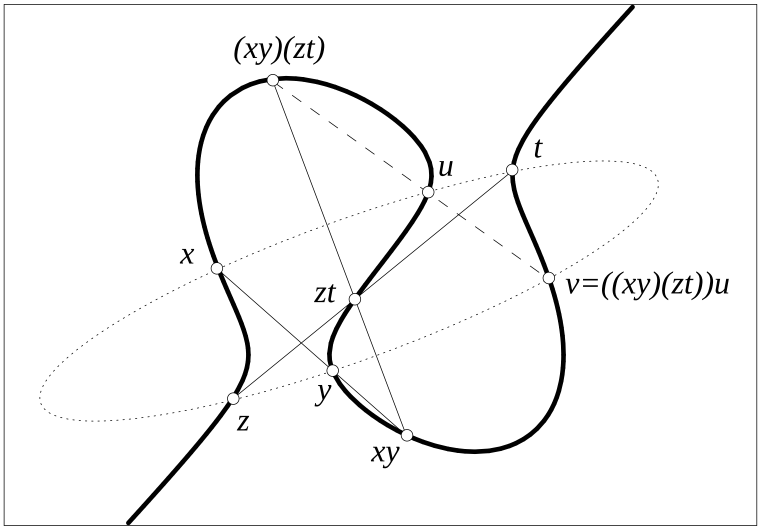

Figure 4: The Sixth Point

Thus, in particular, a nonsingular cubic curve admits exactly one 5-ary totally symmetric Steiner law with flex points as its idempotents. Using similar constructions, one can show that for every $n \equiv 2 (mod\ 3)$, a nonsingular cubic curve admits exactly one totally symmetric n-ary Steiner law with flex points as its idempotents. Indeed, such a Steiner law would be cut on a nonsingular cubic by an algebraic curve of degree $d = (n+1)/3$. Once again, the fact that these operations are well defined follows immediately thanks to the Cayley-Bacharach theorem. Let us quickly illustrate this for, say $n = 11$, the first nontrivial case where the Cayley-Bacharach theorem really applies. If one takes a set of 11 points of general position on a nonsingular cubic curve C, then there exist infinitely many quartic curves passing through these 11 points. If Q is one such quartic curve, it has a 12th common point with the cubic curve, since $|C \cap Q| = 12$ by the Bezout theorem (remember, throughout this paper we are denizens of the complex projective plane). Since this set P of 12 points is the complete intersection cycle of two curves of degrees 3 and 4, respectively, it enjoys the CB-property of degree $3 + 4 - 3 = 4$, meaning that every quartic passing through the initial 11 points must pass through this last point as well! We now have a well-defined universal algebra of arity 11. It is obvious that this is a totally symmetric Steiner law on the cubic. The uniqueness and linear representation follow easily along the previous lines. Indeed, using the full version of (gL), Otter proved the uniqueness of 8-ary Steiner law without much difficulty. Humans can easily prove the uniqueness by induction on the arity.

Theorem 6. *Let $f(x_1, x_2, \ldots, x_{n-1}, x_n)$ and $g(x_1, x_2, \ldots, x_{n-1}, x_n)$ be two n-ary Steiner laws on a nonsingular cubic curve C, and let both f and g share a common idempotent, say e. Then $f = g$.*

Proof. Let f and g be two n-ary Steiner laws on C, and let e be an idempotent element for both f and g. Now specializing $x_n = e$, we do obtain an $(n-1)$-ary Steiner law, since the resulting $(n-1)$-ary law is totally symmetric in all the $n-1$ variables and it is still Steiner and similarly for g. Hence, by the induction hypothesis, we have the universal equality

$$f(x_1, x_2, \ldots, x_{n-1}, e) = g(x_1, x_2, \ldots, x_{n-1}, e).$$

Now form a new n-ary composite function h on the curve C by the rule

$$h(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_{n-1}, x_n) * (e * g(x_1, x_2, \ldots, x_{n-1}, x_n)).$$

Let us substitute $x_n = e$ to obtain $h(x_1, \ldots, x_{n-1}, e) = e$. So the n-ary function h does not depend upon the variable x_n and, by total symmetry, does not depend upon x_i for all $i = 1, 2, \ldots, n$. Hence,

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

In other words $f * (e * g) = e = g * (e * g)$ and hence, by one right cancellation, we obtain the desired equality $f = g$.

Remark. This aspect of formal derivability has been abstracted as the "overlay principle" in [7, p.79].

Appendix

This appendix contains Otter proofs of Theorems 2 and 3, an example of a ternary version of basic (gL), and an example showing that the full (gL) rule is more powerful than the basic (gL) rule.

An Otter proof of Theorem 2

Proof. (Found by Otter 3.0.5b on soot.mcs.anl.gov in 0.58 seconds.)

3	$x * (y * x) = y$	
5	$x * y = y * x$	
6	$(x * y) * z = (x * u) * v \ \rightarrow\ (w * y) * z = (w * u) * v$	
7	$(x * y) * x = y$	[3 → 3]
9	$(x * y) * y = x$	[3 → 5, flip]
14	$(x * ((y * z) * u)) * y = (x * z) * u$	[6,7]
35	$(((x * y) * z) * u) * x = (u * y) * z$	[5 → 14]
1101	$((x * y) * z) * u = ((u * y) * z) * x$	[35 → 9]

An Otter Proof of Theorem 3

Proof. (Found by Otter 3.0.5b on soot.mcs.anl.gov in 0.09 seconds.)

3	$x * (y * x) = y$	
6	$(x * y) * z = (x * u) * v \ \rightarrow\ (w * y) * z = (w * u) * v$	
7	$(x * y) * x = y$	[3 → 3]
14	$(x * ((y * z) * u)) * y = (x * z) * u$	[6,7]
23	$(x * (y * z)) * (u * y) = (x * u) * z$	[7 → 14]
189	$(x * y) * (z * u) = (x * z) * (y * u)$	[3 → 23]

Ternary Basic (gL)

This is an Otter proof of the associativity of the ternary Mal'cev operation using a ternary version of basic (gL).

Theorem 7.

$$\left\{\begin{array}{l} m(x,y,z) = m(x,u,v) \ \rightarrow \\ \qquad\qquad m(w,y,z) = m(w,u,v) \\ m(x,y,y) = x \\ m(x,y,z) = m(z,y,x) \end{array}\right\} \Rightarrow \{m(x,y,m(z,u,v)) = m(m(x,y,z),u,v)\}.$$

Proof. (Found by Otter 3.0.5b on soot.mcs.anl.gov in 0.13 seconds.)

3	$m(x,y,z) = m(x,u,v) \ \rightarrow\ m(w,y,z) = m(w,u,v)$	
4	$m(x,y,y) = x$	
6	$m(x,y,z) = m(z,y,x)$	
7	$m(x,x,y) = y$	[4 → 6, flip]
9	$m(x,y,m(y,z,u)) = m(x,z,u)$	[7,3]
11	$m(x,y,m(z,u,y)) = m(x,u,z)$	[6 → 9]
13	$m(m(x,y,z),x,u) = m(u,y,z)$	[6 → 9]
23	$m(m(x,y,z),u,v) = m(m(v,u,x),y,z)$	[11 → 13]
241	$m(x,y,m(z,u,v)) = m(m(x,y,z),u,v)$	[6 → 23]

Full (gL) vs. Basic (gL)

As we mentioned in Sec. 3, the property of full (gL) — that is Mumford's rigidity lemma of complete varieties (see [10, p.45] or [9, p.104]) — is very powerful and provides the necessary glue to bind the various morphisms definable on a nonsingular cubic curve. In particular, if $m(x, y) : C \times C \longrightarrow C$ is an arbitrary binary composition morphism admitting a two-sided identity, then it must be the usual group law. We produce here a pure first-order proof of this result obtained by Otter using the full (gL) rule:

Theorem 8.

$$\left\{\begin{array}{l} x + e = x \\ e + x = x \\ x * (y * x) = y \\ x * y = y * x \end{array}\right\} \overset{(gL)}{=\!\!\Rightarrow} \; \{x + y = e * (x * y)\}.$$

Proof. (Found by Otter 3.0.5b on soot.mcs.anl.gov in 0.82 seconds.)

2	$x + e = x$	
3	$e + x = x$	
4	$x * (y * x) = y$	
5	$x * y = y * x$	
11	$(e + x) * (y * x) = y$	[3 → 4]
17	$x * (e + (y * x)) = y$	[3 → 4]
28,27	$e + (x * y) = y * x$	[3 → 5]
29	$x * (x * y) = y$	[17 :28]
35	$(x + y) * (z * y) = (x + u) * (z * u)$	[11 → 11 :(gL)]
53	$x * (y * e) = (x + z) * (y * z)$	[2 → 35]
106	$(x + y) * ((x + z) * y) = z$	[35 → 29]
180,179	$(x + y) * (z * y) = x * (e * z)$	[5 → 53, flip]
194	$x * (e * (x + y)) = y$	[106 :180]
225	$e * (x + y) = x * y$	[194 → 29, flip]
231	$x + y = e * (x * y)$	[225 → 29, flip]

As early as 1970, Mumford and Ramanujam proved a rather sweeping and beautiful generalization of this result in the context of complete varieties — not just cubic curves (see [10, p.44]). This single theorem inspired the first author to look into the formal aspects of equational proofs valid on cubic curves.

To show that the corresponding statement is not a theorem in basic (gL) we used MACE [5], a program that looks for small models or counterexamples of first-order statements. The statements

$$\left\{\begin{array}{l} (x * y) * z = (x * u) * v \;\; \rightarrow \;\; (w * y) * z = (w * u) * v \\ x + e = x \\ e + x = x \\ x * (y * x) = y \\ x * y = y * x \\ A + B \neq e * (A * B) \end{array}\right\}$$

have the following model (found by MACE 1.3.2 on ember.mcs.anl.gov in 5.97 seconds).

*	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

+	0	1	2
0	0	1	2
1	1	0	0
2	2	0	0

e:	0
A:	1
B:	1

Web Reference

The programs OTTER and MACE, and the input files that produce the computer proofs in this paper are available on the Web at

`http://www.mcs.anl.gov/~mccune/papers/steiner`.

References

[1] D. Eisenbud, M. Green, and J. Harris. Cayley-Bacharach theorems and conjectures. *Bull Amer. Math. Soc (N.S.)*, 33:295–324, 1996.

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

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

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

[5] W. McCune. Models And Counter-Examples (MACE). `http://www.mcs.anl.gov/AR/mace/`, 1994.

[6] W. McCune. Otter 3.0 Reference Manual and Guide. Tech. Report ANL-94/6, Argonne National Laboratory, Argonne, IL, 1994. Also see `http://www.mcs.anl.gov/AR/otter/`.

[7] W. McCune and R. Padmanabhan. *Automated Deduction in Equational Logic and Cubic Curves*, volume 1095 of *Lecture Notes in Computer Science (AI subseries).* Springer-Verlag, Berlin, 1996.

[8] 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.

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

[10] D. Mumford. *Abelian Varieties.* Oxford University Press, 1985. Tata Institute of Fundamental Research, Bombay.

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

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