# *Automated Deduction in Algebraic Geometry*

William McCune
(work with R. Padmanabhan)

Mathematics and Computer Science Division
Argonne National Laboratory

March 1995

## *An Inference Rule for Cubic Curves*

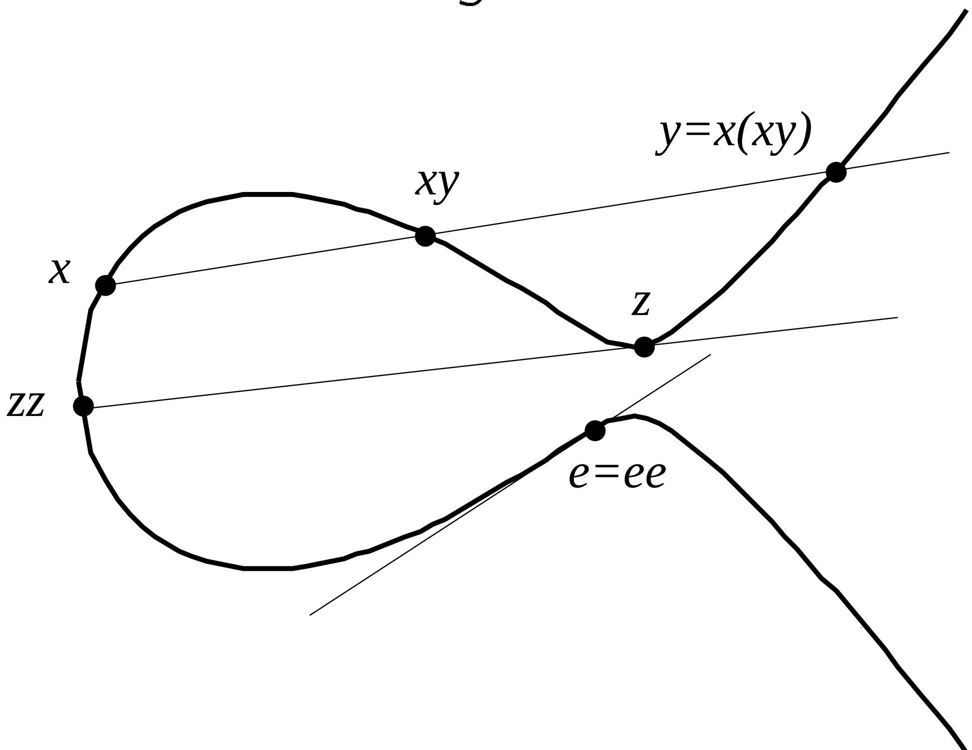
- A "basic" theorem in algebraic geometry:

  > *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 $y \in Y$.* [Shafarevich, p.152]

- Padmanabhan devised a first-order equational inference rule $=(gL)\Rightarrow$ that captures the above theorem for the algebra of cubic curves.

- $=(gL)\Rightarrow$ allows one to prove, in equational logic, some incidence theorems and configuration theorems on projective curves without reference to the underlying geometry or topology of the curves.

## *The Chord-Tangent Construction*




Consider a nonsingular cubic curve in the complex projective plane. Define a binary operation on the points of the curve.

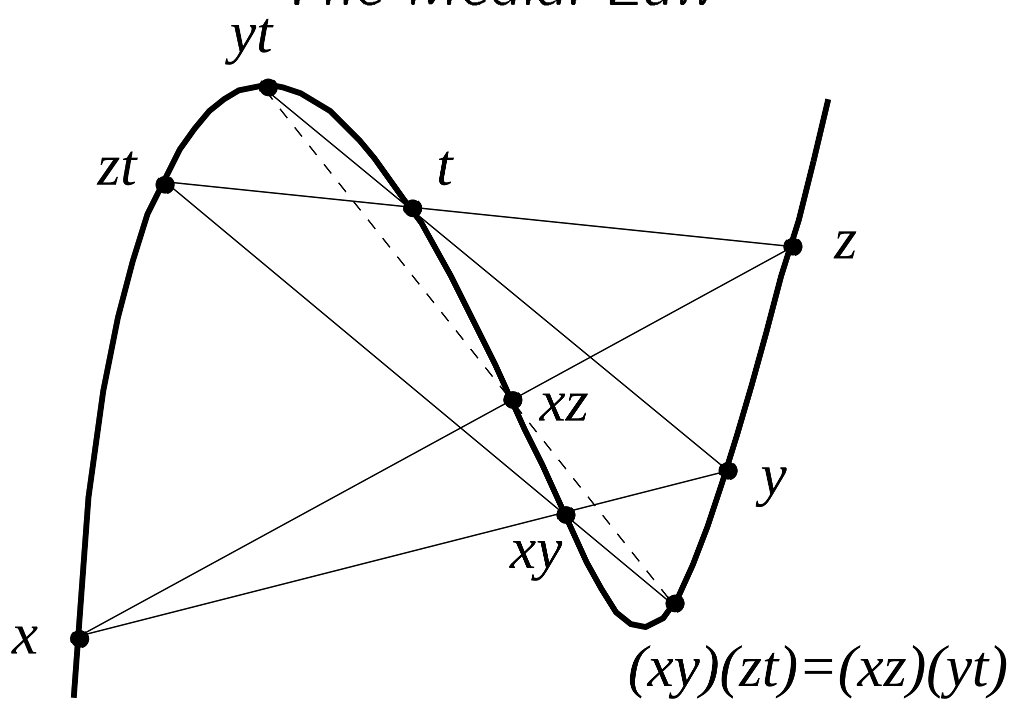
– If a line intersects the curve in 3 points, the product of any two points is the third point.

– $zz$ is the point where the tangent at $z$ intersects the curve.

– Inflection points are idempotent elements ($ee = e$).

– The operation is commutative, and the Steiner law, $x(yx) = y$, holds.

## *The Medial Law*



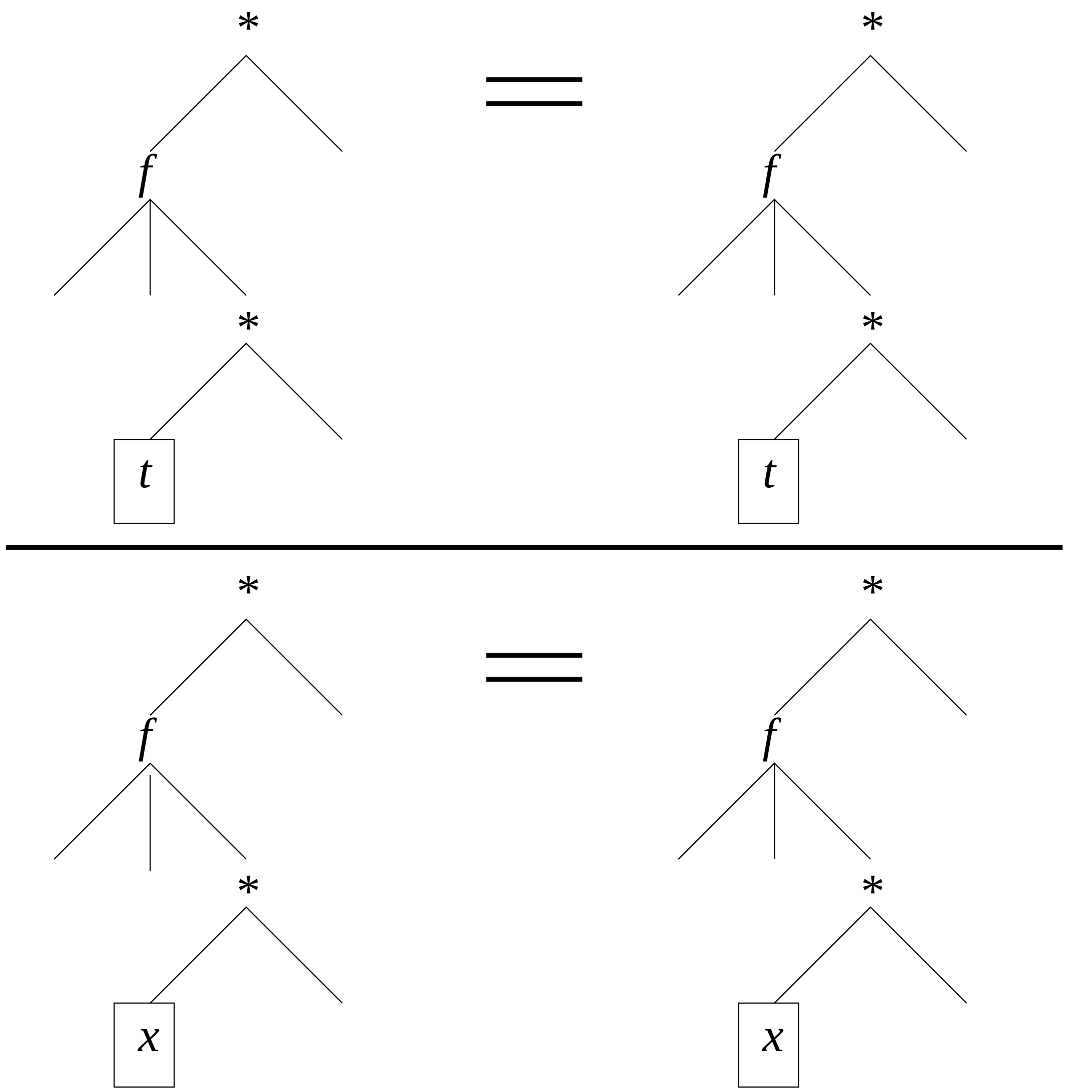

$$\{x(yx) = y\} \overset{(gL)}{\Longrightarrow} \{(xy)(zu) = (xz)(yu)\}.$$

*Proof* (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 | $(w \cdot (y \cdot x)) \cdot (z \cdot y) = (w \cdot z) \cdot x$ | [gL 38] |
| 333 | $(w \cdot x) \cdot (z \cdot y) = (w \cdot z) \cdot (x \cdot y)$ | [2 $\to$ 331] |

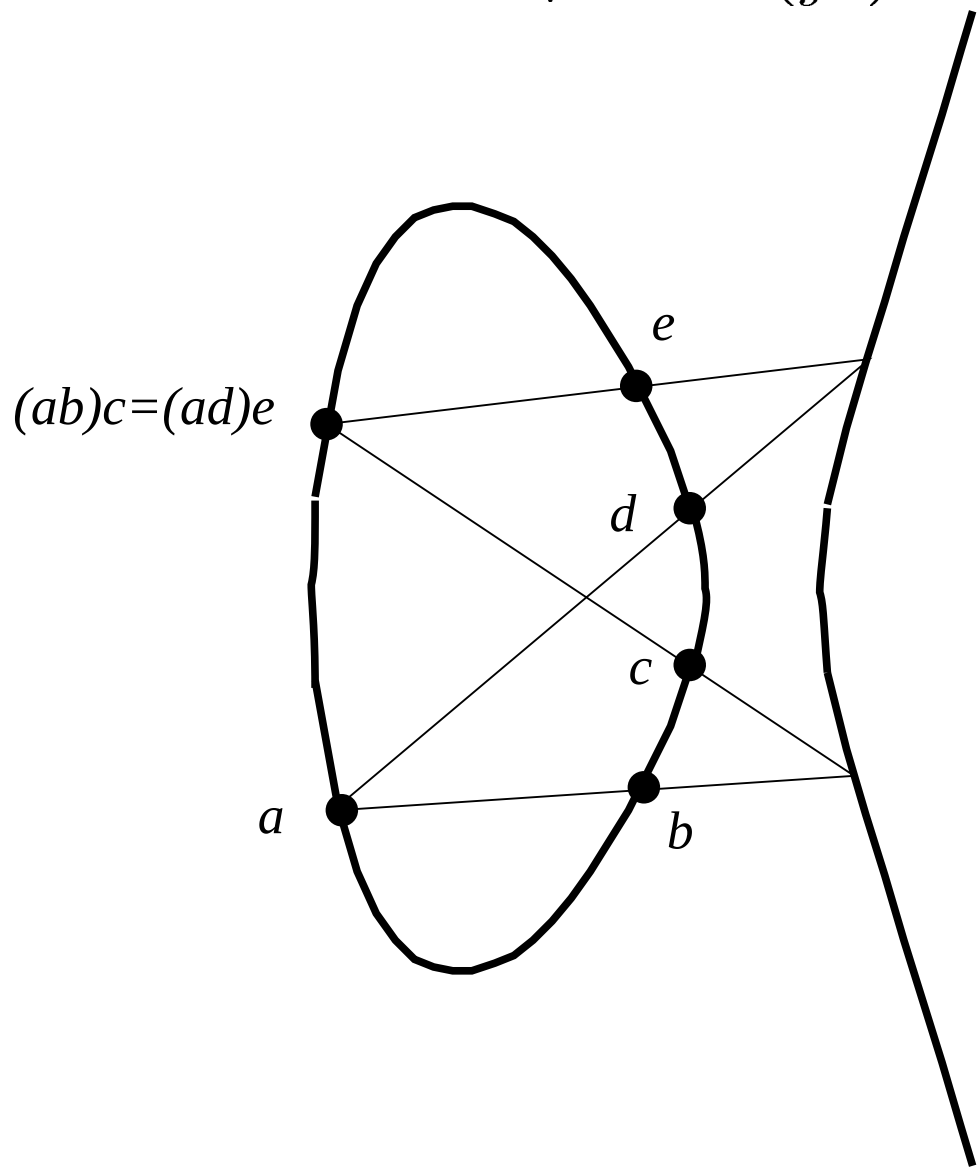
- The proof ordinarily involves high-level concepts (the Bezout theorem, the Riemann-Roch theorem, or Weierstrass elliptic functions).

## *The Rule* $=(gL)\Rightarrow$




- Given an equality, if identical terms ($t$) occur in corresponding positions, and in the same nest of function symbols, replace both occurrences with a new variable ($x$).

## *A Geometric Example of* $=\!\!(gL)\!\!\Rightarrow$




- $[(ab)c = (ad)e] \;=\!\!(gL)\!\!\Rightarrow\; [\forall x\ (xb)c = (xd)e]$.
- Select a point $x$ and see if it works.

## *Implementation of* $=(gL)\Rightarrow$ *(in Otter)*

As an inference rule, with unification:

29. $f(x, y, f(z, u, v, w), v) = f(x, y, v_6, f(z, u, v_6, w))$
119. $f(x, y, v_0, v) = f(x, y, v_0, f(z, u, f(z, u, v, w), w))$
[gL 29]

As a rewrite rule, applied to identical terms (usually before ordinary rewriting):

6. $f(e, y, f(e, e, y)) = e$
12. $f(x, y_1, f(z, u, y_1)) = f(x, y_2, f(z, u, y_2))$
[6 $\rightarrow$ 6: gL, gL, gL]

- Note that we paramodulate from the *right* side of 6 into the *right* side of 6.

## *Strategies for* $=\!\!(gL)\!\!\Rightarrow$ *(A)*

- For ordinary equational problems, we usually use rewrite-based strategies.
- However, $=\!\!(gL)\!\!\Rightarrow$ appears to be incompatible with rewrite-based strategies
  - $=\!\!(gL)\!\!\Rightarrow$ frequently must be applied to *simplifiable* terms, so we cannot always rewrite.
  - We must paramodulate from smaller sides into smaller sides.
  - We must paramodulate from variables and into variables.
- We must relax the rewrite-based strategy.

$$\{ex = xe = x\} \;=\!\!(gL)\!\!\Rightarrow\; \{xy = yx\}.$$

*Proof* (Otter 3.0.3+ on gyro at 31.16 seconds).

| | | |
|---|---|---|
| 2 | $e \cdot x = x$ | |
| 3 | $x \cdot e = x$ | |
| 5 | $(e \cdot e) \cdot x = x$ | [2 → 2] |
| 7 | $(x \cdot e) \cdot e = x$ | [3 → 3] |
| 79 | $(x \cdot y) \cdot e = (e \cdot y) \cdot x$ | [5 → 7 :gL] |
| 355 | $(e \cdot x) \cdot y = y \cdot x$ | [3 → 79, flip] |
| 814 | $x \cdot y = y \cdot x$ | [2 → 355] |

## *Strategies for* $=\!(gL)\!\Rightarrow$ *(B)*

In some cases, we can rewrite everything.

$$\left\{ \begin{array}{l} x(yx) = y \\ ex = xe \\ ee = e \end{array} \right\} =\!(gL)\!\Rightarrow \{(x((z(xy))(ey)))(ee) = z\}$$

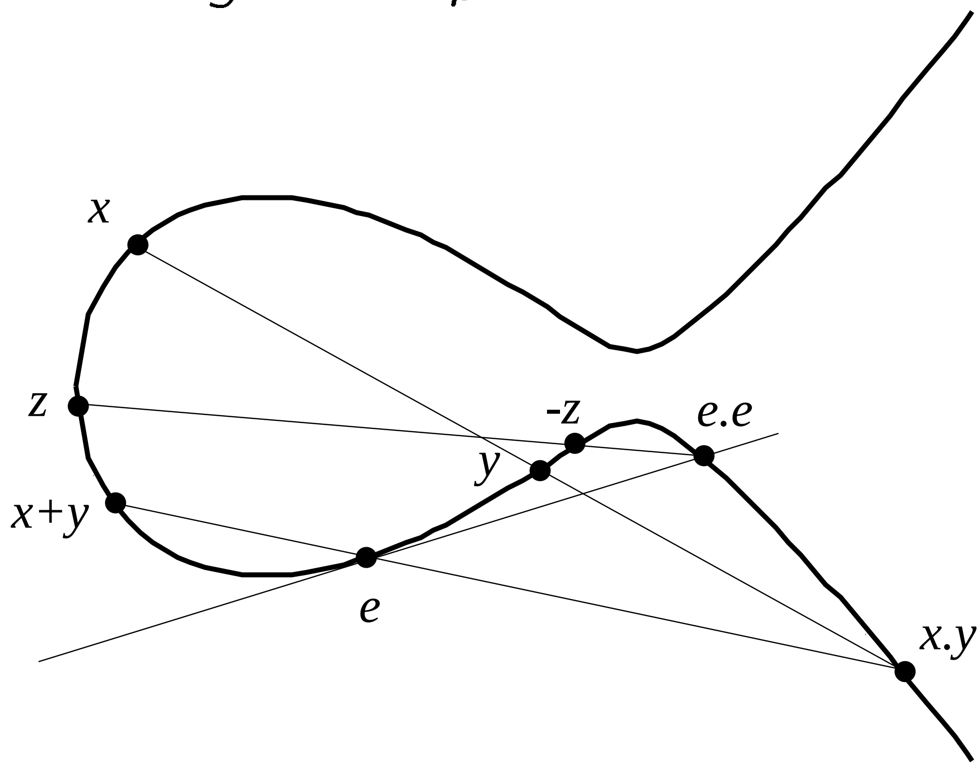
*Proof* (Otter 3.0.3+ on gyro at 10.12 seconds).

| | | |
|---|---|---|
| 1 | $x = x$ | |
| 3,2 | $e \cdot e = e$ | |
| 4 | $e \cdot x = x \cdot e$ | |
| 6,5 | $x \cdot (y \cdot x) = y$ | |
| 7 | $(A \cdot ((C \cdot (A \cdot B)) \cdot (e \cdot B))) \cdot (e \cdot e) \neq C$ | |
| 8 | $(A \cdot ((C \cdot (A \cdot B)) \cdot (e \cdot B))) \cdot e \neq C$ | [copy,7 :3] |
| 18,17 | $(x \cdot y) \cdot x = y$ | [5 $\rightarrow$ 5] |
| 20,19 | $e \cdot (e \cdot x) = x$ | [4 $\rightarrow$ 5] |
| 21 | $x \cdot (x \cdot e) = e$ | [4 $\rightarrow$ 5] |
| 34 | $x \cdot (x \cdot y) = y$ | [19 $\rightarrow$ 21 :gL, 20] |
| 41,40 | $(x \cdot y) \cdot y = x$ | [17 $\rightarrow$ 34] |
| 42 | $x \cdot y = y \cdot x$ | [5 $\rightarrow$ 34] |
| 46 | $(x \cdot y) \cdot z = z \cdot (y \cdot x)$ | [42 $\rightarrow$ 42] |
| 53 | $(A \cdot ((C \cdot (B \cdot A)) \cdot (e \cdot B))) \cdot e \neq C$ | [42 $\rightarrow$ 8] |
| 114 | $(x \cdot y) \cdot (z \cdot u) = (u \cdot z) \cdot (y \cdot x)$ | [42 $\rightarrow$ 46] |
| 204 | $(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$ | [gL 114] |
| 231 | $C \neq C$ | [204 $\rightarrow$ 53 :18,6,41] |
| 232 | $\square$ | [231,1] |

## *Strategies for $=\!(gL)\!\Rightarrow$ (C)*

- The current meta-strategy for $=\!(gL)\!\Rightarrow$ .
  - Start with unconstrained paramodulation (from and into variables, from and into both sides), orient equalities, and make all orientable equalities into rewrite rules.
  - If that fails, successively constrain rewriting by being more selective about adding rewrite rules.
  - Adjust the strategy until a "well behaved" search is achieved.
- There is a lot of room for work on $=\!(gL)\!\Rightarrow$ strategies.
  - Keep several versions at various stages of simplification.
  - Bidirectional search (including a backward $=\!(gL)\!\Rightarrow$ rule).
  - Linked or hyper inference rules.

## *Defining a Group on a Cubic Curve*




- '·' is the operation of chord-tangent construction.
- Select any point as the identity $e$.
- Define $x + y$ as $(x \cdot y) \cdot e$.
- Define $-x$ as $(e \cdot e) \cdot x$.

With a given identity, the group is unique.

## *Uniqueness of Inversive Groupoids (A)*

$$\left\{\begin{array}{ll} f(e,x)=x, & F(e,x)=x \\ f(x,e)=x, & F(x,e)=x \\ f(g(x),x)=e, & F(G(x),x)=e \\ f(x,g(x))=e, & F(x,G(x))=e \end{array}\right\} \overset{(gL)}{\Longrightarrow}$$

$$\left\{\begin{array}{l} f(x,y)=F(x,y) \\ g(x)=G(x) \end{array}\right\}.$$

- A rewrite strategy that works for this problem.
  - Do not use input equations as rewrite rules.
  - Use instances of input equations and some lemmas as rewrite rules:

    $$f(e,e)=e, \quad F(e,e)=e, \quad g(e)=e, \quad G(e)=e$$

  - Make orientable derived equations into rewrite rules.
  - Paramodulate from both sides into both sides.
  - Paramodulate from variables but not into variables.

## *Uniqueness of Inversive Groupoids (B)*

*Proof* (Otter 3.0.3e on gyro at 11.77 seconds).

| | | |
|---|---|---|
| 2 | $f(e,x) = x$ | |
| 3 | $f(x,e) = x$ | |
| 4 | $f(g(x),x) = e$ | |
| 6 | $F(e,x) = x$ | |
| 7 | $F(x,e) = x$ | |
| 9 | $F(x,G(x)) = e$ | |
| 10 | $f(A,B) = F(A,B),\ g(A) = G(A) \ \rightarrow \ \Box$ | |
| 18,17 | $f(f(x,e),e) = x$ | [3 → 3] |
| 21 | $f(f(e,x),e) = x$ | [3 → 2] |
| 26,25 | $f(F(e,x),e) = x$ | [3 → 6] |
| 38,37 | $f(F(x,e),e) = x$ | [3 → 7] |
| 47 | $f(F(g(x),e),x) = e$ | [7 → 4] |
| 49 | $f(F(e,g(x)),x) = e$ | [6 → 4] |
| 53 | $f(f(e,g(x)),x) = e$ | [2 → 4] |
| 63 | $f(g(x),x) = f(g(y),y)$ | [4 → 4] |
| 71,70 | $f(f(g(x),x),y) = y$ | [4 → 2] |
| 154,153 | $f(F(x,G(x)),y) = y$ | [9 → 2] |
| 163 | $f(F(g(x),y),x) = y$ | [37 → 47 :gL, 26] |
| 173 | $G(g(x)) = f(e,x)$ | [9 → 163, flip] |
| 199 | $f(F(x,g(y)),y) = x$ | [37 → 49 :gL, 38] |
| 294 | $f(f(x,g(y)),y) = x$ | [21 → 53 :gL, 18] |
| 307 | $F(x,g(g(y))) = f(x,y)$ | [199 → 294, flip] |
| 335,334 | $g(g(x)) = x$ | [63 → 294 :71, flip] |
| 337 | $f(x,y) = F(x,y)$ | [307 :335, flip] |
| 604 | $G(g(x)) = x$ | [9 → 173 :154] |
| 608 | $g(x) = G(x)$ | [334 → 604, flip] |
| 627 | $\Box$ | [608,10,337] |

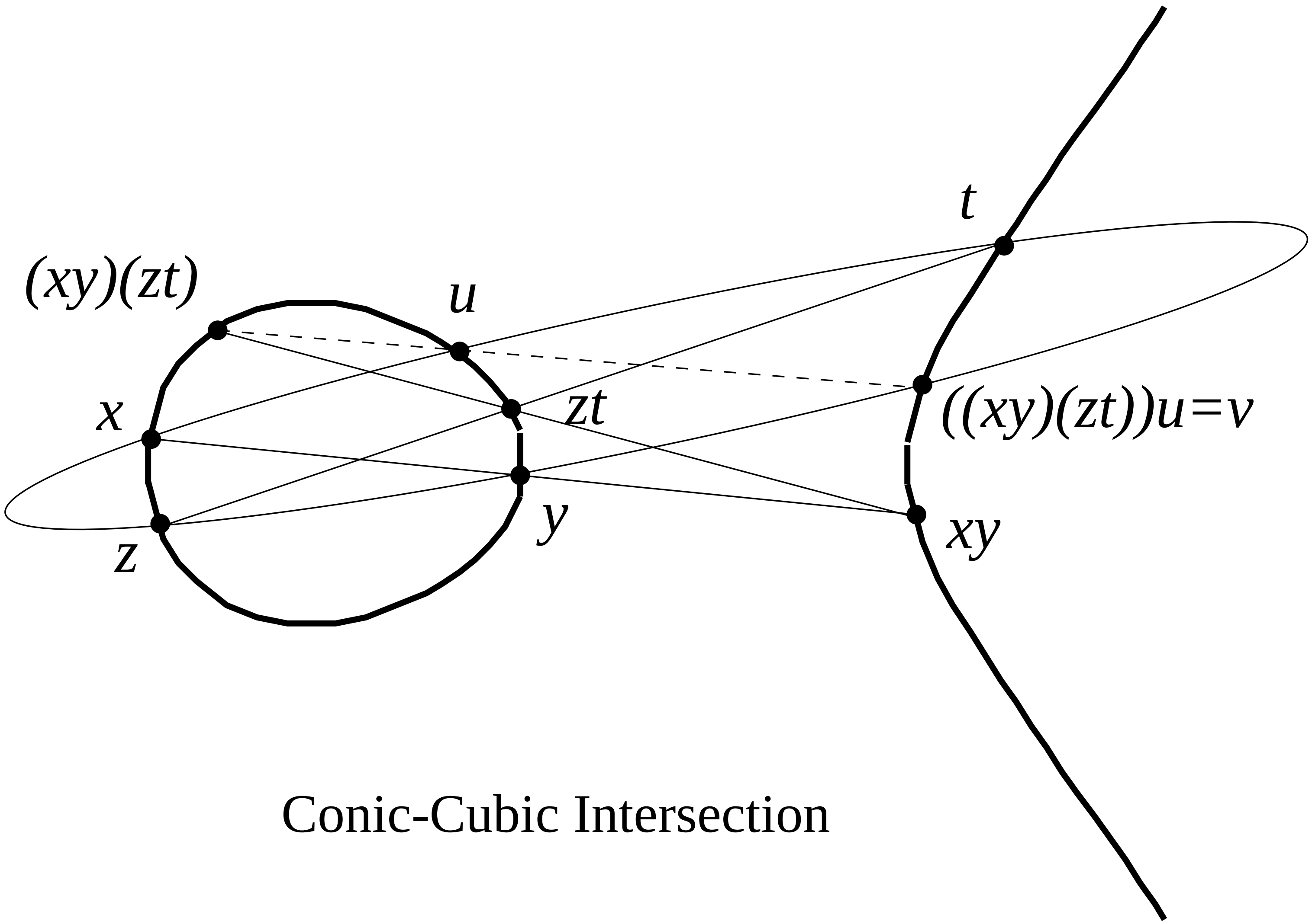
## *New Results with* $=(gL)\Rightarrow$ *(A)*

- General exploration of $=(gL)\Rightarrow$ algebras.
- A cancellative semigroup on a cubic curve must be commutative.
- Uniqueness of the 5-ary Steiner Law:

$$\left\{\begin{array}{l} \text{full permutability of } f \\ f(e,e,e,e,e) = e \\ f(e,e,e,x,f(e,e,e,x,y)) = y \\ \text{full permutability of } g \\ g(e,e,e,e,e) = e \\ g(e,e,e,x,g(e,e,e,x,y)) = y \end{array}\right\} =(gL)\Rightarrow$$

$$g(x,y,z,u,v) = f(x,y,z,u,v).$$

A corollary: given 5 points of intersection of a cubic and a conic, the sixth point can be found be a simple ruler construction.




Conic-Cubic Intersection

## *Summary*

- $=(gL)\Rightarrow$ is unnatural for humans, but useful in programs.

- Strategy for $=(gL)\Rightarrow$ needs a lot of work.

- References


  - R. Padmanabhan and W. McCune, "Automated Reasoning about Cubic Curves", *Computers and Mathematics with Applications*, 29(2), 17–26 (1995).
  - W. McCune and R. Padmanabhan, "Uniqueness of the 5-ary Steiner Law on Elliptic Curves", Preprint.
  - W. McCune and R. Padmanabhan, "Automated Equational Deduction with Otter", In preparation.
  - R. Padmanabhan, "Logic of Equality in Geometry", *Discrete Mathematics* 15, 319–331 (1982).
  - I. R. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag (1977).