Some Results on Theorem Proving In Geometry over Finite Fields

Dongdai Lin,Zhuojun Liu
Mathematics-Mechanization Research Center
Institute of Systems Science, Academia Sinica, Beijing,100080

Abstract. In this paper, we discuss Wu's well ordering principle and theorem proving over finite fields, try to prove some theorems in the geometry over finite fields.

1 Introduction

Automated reasoning and/or theorem-proving by machine(abbr. TPM) is an attractive research field. Even before the computer appeared, many research works in this field had been done. For the history of development of TPM, see [1].

It is very interesting that almost all the people doing TPM, try to prove some geometry theorems by their method. However, before 1970s, there were not any astonishing results for geometry theorem proving by machine, although Tarski, in 1949 presented a decidable method for elementary geometry. In 1978, Prof. Wu Wentsün, in his well known paper [9,10], gave a new (algebraic) method and lay a foundation for geometry theorem proving by machine. The more than 500 theorems proved by Wu's method in [2], many of them are even difficult for man to prove, show that Wu's method is very powerful in elementary geometry theorem proving. In recent years, Wu's method has been well developed, now it can be used not only in the elementary geometry theorem proving but also in the differiential geometry theorem proving [3,5,8,11] and automated derivation between some physical laws [12]. However, we have not find the works on TPM in finite geometry so far.

ACM-ISSAC '93-7/93/Kiev, Ukraine
© 1993 ACM 0-89791-604-2/93/0007/0292...$1.50

Finite geometry is one that contains a finite number of points. It has many applications in coding theory, cryptogrphy,block design and so on. Undoubtedly, automated derivation of some geometry relations and the theorem proving by machine in finite geometry will be helpful to its development.

Unlike in the ordinary geometry, the discussion of geometric statements in the geometry over finite fields is not restricted to a fixed base field, in fact, when we talk about the geometric statements in the geometry over finite fields, we don't clearly indicate which finite field we discuss over, even its characteristic. It might raise the degree of difficulties of geometry theorem proving over finite field.

In this paper, we discuss the TPM in projective plane over finite field, show that, after some minor revision, the Wu's method can be used in TPM over finite fields and try to prove some theorems by Wu's method. Like TPM in elementary geometry, in this paper, we only consider the theorems whose hypotheses and conclusions can be expressed by polynomial equations.

In next section, we will give some fundamental knowledge on projective plane over finite fields. In section 3, the Wu's well-ordering principle over finite field will be discussed. And in the last section, we will give some theorems proved by machine as examples.

2 Basic concepts of Finite Geometry

In this section, we will give a survey of projective plane over finite fields and the knowledge of translating geometry statements into polynomial equations. For more details, see [7].

Let $V_3(\mathbf{F}_q)$ be the 3-dimensional row vector space over $\mathbf{F}_q$, $\mathcal{P}$ be set of all the 1-dimensional vector subspaces of $V_3(\mathbf{F}_q)$, $\mathcal{L}$ be the set of all 2-dimensional vector subspaces of $V_3(\mathbf{F}_q)$, $\mathcal{I}$ be a relation, called incidence, between the elements of $\mathcal{P}$ and the elements of $\mathcal{L}$ such that for any $p \in \mathcal{P}$, $l \in \mathcal{L}$, p is incident with l if and only if p as a subspace of $V_3(\mathbf{F}_q)$ is contained in l as a subspace of $V_3(\mathbf{F}_q)$. Then if we treat the elements of $\mathcal{P}$ as points, the elements of $\mathcal{L}$ as lines, $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ becomes a finite projective plane, i.e. it satisfies the following axioms:

P1 every pair of distinct lines is incident with a unique point called intersection.

P2 every pair of distinct points is incident with a unique line.

P3 there exist four points such that no three of them are incident with a single line.

The above finite projective plane is denoted by $PG(2,\mathbf{F}_q)$.

Example. The simplest finite projective plane is $PG(2,\mathbf{F}_2)$ called *Fano plane*. There are precisely three lines through each point and three points on each line. Altogather there are 7 points and 7 lines in the plane. This projective plane may be illustrated as in Figure 2.1. The points are A, B, C, D, E, F and G, and the lines are ADC, AGE, AFB, CGF, CEB and DEF. The line DEF in this plane shows that straightness is no longer meaningful in a finite projective plane.

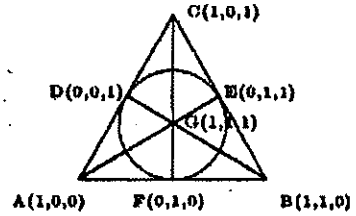

Figure 2.1

To be concrete, let us introduce the coordinate description of $PG(2,\mathbf{F}_q)$. Let P be a point of $PG(2,\mathbf{F}_q)$, that is , P is a 1-dimensional vector subspace of $V_3(\mathbf{F}_q)$. Let (x_0, x_1, x_2) be a non-zero vector in P, then

$$P = \{(\lambda x_0, \lambda x_1, \lambda x_2) | \lambda \in \mathbf{F}_q\}.$$

For any non-zero $\lambda \in \mathbf{F}_q$, we shall call the non-zero vector $(\lambda x_0, \lambda x_1, \lambda x_2)$ the coordinates of the point P, we also say that $(\lambda x_0, \lambda x_1, \lambda x_2)$ is the point P. Clearly the coordinate of a point P is uniquely determined up to a non-zero constant multiple of $\mathbf{F}_q$.

Let l be a line in $PG(2,\mathbf{F}_q)$, that is, l is a 2-dimensional vector subspace of $V_3(\mathbf{F}_q)$. Clearly, we can choose $a_0, a_1, a_2 \in \mathbf{F}_q$, not all zero, such that the subspace of solutions of the homogeneous equation

$$a_0 y_0 + a_1 y_1 + a_2 x_2 = 0 \qquad (1)$$

is just l. Conversely, for any homogeneous equation like (1), the subspace of solutions is a 2-dimensional vector subspace of $V_3(\mathbf{F}_q)$, i.e. is line in $PG(2,\mathbf{F}_q)$. Hence we can use homogeneous equation (1) to denote a line of $PG(2,\mathbf{F}_q)$ and the points on this line are just those points whose coordinates satisfy the (1).

The following two propositions is very important for us to translate the relation between points and lines into polynomial equations.

Proposition 2.1 Three points (a_0, a_1, a_2), (b_0, b_1, b_2), (c_0, c_1, c_2) are collinear, i.e. lie on the same line, if and only if the discriminate

$$\begin{vmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \\ c_0 & c_1 & c_2 \end{vmatrix} = 0$$

Proposition 2.2 Three lines

$$\begin{aligned} a_0 x_0 + a_1 x_1 + a_2 x_2 &= 0 \\ b_0 x_0 + b_1 x_1 + b_2 x_2 &= 0 \\ c_0 x_0 + c_1 x_1 + c_2 x_2 &= 0 \end{aligned}$$

are concurrent, i.e. intersect in a common point, if and only if the discriminate

$$\begin{vmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \\ c_0 & c_1 & c_2 \end{vmatrix} = 0$$

Any $T \in GL_3(\mathbf{F}_q)$ defines a point to point transformation of $PG(2,\mathbf{F}_q)$ in the following way:

$$PG(2,\mathbf{F}_q) \to PG(2,\mathbf{F}_q)$$

$$(x_0, x_1, x_2) \to (x_0, x_1, x_2)T \qquad (2)$$

This is well-defined. The tranformation (2) is called a *projective transformation* of $PG(2,\mathbf{F}_q)$, and denoted by $\overline{T}$.

The set of points (x_0, x_1, x_2) of $PG(2, \mathbf{F}_q)$ which satisfy a quadratic homogeneous equation

$$\sum_{0 \le i \le k \le 2} a_{ik} x_i x_k = 0, \tag{3}$$

where a_{ik} $(0 \le i \le k \le 2)$ are elements of $\mathbf{F}_q$ and not all a_{ik} are zero, is called a quadric in $PG(2, \mathbf{F}_q)$ and the quadratic equation (3) is called its equation.

The quadric is said to be *non-degenerate*, if its equation cannot be tranformed into an equation with less than 3 varibles under projective transformations.

By a *conic* in $PG(2, \mathbf{F}_q)$ we mean a non-degenerate quadric in $PG(2, \mathbf{F}_q)$.

Proposition 2.3 The equation of any conic can be carried by projective transformations into the following form

$$x_0^2 + x_1 x_2 = 0. \tag{4}$$

A line is called the tangent of a conic if it meets the conic in exactly one point, and it is called a tangent at this point.

Proposition 2.4. Let $A = (x_0, y_0, z_0)$ be a point on the conic $X^2 + YZ = 0$, then the tangent line of the conic at A has equation:

$$2x_0 X + z_0 Y + y_0 Z = 0. \tag{5}$$

3 Wu's Well-Ordering Principle over Finite Fields

Let the hypotheses of a theorem have been expressed as a finite set of polynomial equations over a field K:

$$\begin{aligned} PS: \quad & h_1(x_1, x_2, ..., x_n) = 0, \\ & h_2(x_1, x_2, ..., x_n) = 0, \\ & ... \\ & h_m(x_1, x_2, ..., x_n) = 0, \end{aligned} \tag{6}$$

and conclusion as a polynomial equation $g(x_1, \cdots, x_n) = 0$. We wish to find a method to decide when and under what conditions we can derive $g(x_1, \cdots, x_n) = 0$ from (6).

For the case that K is a field of characteristic 0, Prof. Wu Wentsün has presented a method (called well-ordering principle) by which we can get another set of polynomials CS and a polynomial J such that

$$Zero(CS/J) \subset Zero(PS) \subset Zero(CS)$$

and decide whether

$$Zero(CS/J) \subset Zero(g),$$

where $Zero(CS/J) = Zero(CS) \setminus Zero(J)$.

What about the case that K is a finite field. In this section, we will discuss the Wu's method over finite field. We shall learn late that, after some minor revision, Wu's method can also be used over finite field.

Let $\mathbf{F}_q$ be a finite field, $x_1, x_2, \cdots, x_n$ be a fixed number of indeterminates with order $x_1 < x_2 < \cdots < x_n$. Similar to the case of characteristic 0, we can also introduce the concepts of class, rank, initial, ascending chain and so on for the polynomials in $\mathbf{F}_q[x_1, x_2, \cdots, x_n]$.

Let $f \in \mathbf{F}_q[x_1, x_2, \cdots, x_n]$ be a polynomial. We define the *class* of f (denoted by $cls(f)$) be the smallest positive integer c, if any, such that $f \in \mathbf{F}_q[x_1, \cdots, x_c]$, otherwise 0. The degree of f in varible x_i is denoted by $deg(f, x_i)$.

Now consider f as a polynomial in x_c $(c = cls(f) \neq 0)$, then f can be put into the form:

$$f = I \cdot x_c^d + \text{ lower degree term in } x_c,$$

where $d = deg(f, x_c)$. The coefficient I is called the *initial* of f and to be denoted by $Init(f)$. A polynomial g is said to be reduced with respect to a polynomial f if $c(= cls(f)) = 0$ or $c \neq 0$ and $deg(f, x_c) > deg(g, x_c)$.

Let $f \in \mathbf{F}_q[x_1, \cdots, x_n]$ with $Init(f) = I$ and $cls(f) = c > 0$. If a polynomial g is not reduced with respect to f, then we can find a smallest positive integer s and polynomials q and r such that

$$I^s \cdot g = q \cdot f + r \text{ and r is reduced w.r.t. f.}$$

In fact, r and q are uniquely determined by f and g. We denote r by $prem(g, f)$ and call it *pseudo-remainder* of g with respect to f. The procedure obtaining r from f and g is called *pseudo division*. Pseudo division is the most important operation in Wu's method.

Definition 3.1. Let $AS: f_1, f_2, ..., f_r$ be a finite sequance of polynomials in $F_q[x_1, x_2, ..., x_n]$. We call it an ascending chain if either $r = 1$ and $f_1 \neq 0$ or $r > 1$, $0 < class(f_1) < class(f_2) < ... < class(f_r)$ and f_j is reduced with respect to f_i for any $i < j$.

Given a ascending chain $AS: f_1, f_2, ..., f_r$ with $class(f_1) > 0$ and a polynomial g, we define the pseudo remainder of g with respect to AS inductively as

$$\mathrm{prem}(\mathrm{g}, \mathrm{f}_1, \mathrm{f}_2, \cdots, \mathrm{f}_r) = \mathrm{prem}(\mathrm{prem}(\mathrm{g}, \mathrm{f}_2, \cdots, \mathrm{f}_r), \mathrm{f}_1). \tag{7}$$

By examine the well-ordering procedure of [10] carefully, we can find that all the operations needed are addition, substraction, multiplication and psuedo division of polynoimals. Obviously, all these computations can be done over finite fields, hence, we have

Theorem 3.2. Let $\mathbf{F}_q$ be a fixed finite field. Then there is an mechanical algorithm, for any finite set PS of polynomials in $\mathbf{F}_q[x_1, x_2, ..., x_n]$ we can get, in finite steps, either a non-zero constant $c \in \mathbf{F}_q$ or an ascending chain CS such that for any $f_i \in PS$

$$prem(f_i, CS) = 0.$$

and

$$Zero(CS/I_1 I_2 \cdots I_r) \subset Zero(PS) \subset Zero(CS)$$
$$\mathrm{Zero(PS)} = \mathrm{Zero(CS/I_1 \cdots I_r)} + \sum_{\mathrm{i}=1}^{\mathrm{r}} \mathrm{Zero(PS, I_i)} \tag{8}$$

Prof. Wu called the mechanical procedure obtaining CS from PS well ordering of PS. The polynomial set CS in Theorem 3.2 is called a characteristic set of PS.

Above theorem shows that Wu's well-ordering priciple is also efficient over a fixed finite field and there is no special difference from the case over a field of characteristic 0. But in practice, we would face some problems such as the expression and operations of polynomials over finite fields. Many packages such as REDUCE do not supply the operations of polynomials over finite fields, but only the ability of manipulating polynomials whose coefficients are computed modulo a given prime number. Hence we have to find a method that permits us to compute the characteristic set of a polynomial set over finite field. To be concurrent with Wu's method, we suggest using polynomials to denote the elements of a field.

Let $\mathbf{F}_q$ be a finite filed with characteristic p, $q = p^m$, $f_0(x_0)$ be an irreducible polynomial of degree m over $\mathbf{F}_p$, then $\mathbf{F}_q$ is isomorphism to the quotient field $\mathbf{F}_q[x_0]/ < f_0(x_0) >$, hence the elements of $\mathbf{F}_q$ can be expressed as polynomials in x_0 with degree $\leq m$. The polynomial f_0 is called generating polynomial of $\mathbf{F}_q$.

Theorem 3.3. Let $\mathbf{F}_q$ be a fixed finite field with characteristic p, f_0 be a generating polynomial of $\mathbf{F}_q$, PS a polynomial set over $\mathbf{F}_q$. Then $PS \subset \mathbf{F}_p[x_0, x_1, \cdots, x_n]$. If $CS' = \{f_0, c_1, \cdots, c_r\}$ is the characteristic set of $PS \cup \{f_0\}$, under modular p and order $x_0 < x_1 < \cdots < x_n$, then $CS = \{c_1, \cdots, c_r\}$ is the characteristic set of PS over $\mathbf{F}_q$ and the pseudo-remainder of a polynomial g with respect to CS over $\mathbf{F}_q$ can be computed by $prem(g, CS')$ under modular p.

The above theorem describes a method to compute the characteristic set of a polynomial set over finite field. It seems that we are ready to prove geometry theorems over finite fields. But it is wrong. Usually, when we talk about geometry statement in geometry over finite field , we don't clearly indicate which finite field we discuss over, even its characteristic, i.e. the finite field may be $\mathbf{F}_2, \mathbf{F}_3, \mathbf{F}_{2^6}$ and so on. So Theorem 3.2 and 3.3 are not enough to prove geometry theorems since it is imposible to use them to prove a geometry statement for every possible finite fields. Fortunately, in this case, all the polynomials we encountered are polynomials with integer coefficients which could be regarded as polynomials over any finite field as well as the rational field Q.

Theorem 3.4. Let p be a prime number, PS be a finite set of polynomials over the integer ring $\mathbf{Z}$, $[CS, p]$ the characteristic set of PS under modular p. Then over any finite field $\mathbf{F}_q$ with characteristic p, we have

$$Zero([CS, p]/J) \subset Zero(PS) \subset Zero([CS, p])$$
$$\mathrm{Zero(PS)} = \mathrm{Zero([CS, p]/J)} + \sum_{\mathrm{i}=1}^{\mathrm{r}} \mathrm{Zero(PS, I_i)} \tag{9}$$

where I_i's are initials of the polynomials in $[CS, p]$, J is the product of I_i's.

Theorem 3.5. Let PS be a finite set of polynomials over $\mathbf{Z}$, $[CS, 0] = \{p_1, \cdots, p_r\}$ be the char-

acteristic set of PS over a field of characteristic 0. Write the initials of the polynomials of $[CS,0]$ as

$$Init(p_1) = n_1 I_1'$$
$$Init(p_2) = n_2 I_2'$$
$$\cdots$$
$$Init(p_r) = n_r I_r'$$

where n_i are the integer factor of $Init(p_i)$. Then over any finite field with characteristic not a prime factor of $n_1 n_2 \cdots n_r$ we have

$$Zero([CS,0]/J) \subset Zero(PS) \subset Zero([CS,0])$$
$$\text{Zero(PS)} = \text{Zero([CS,0]/J)} + \sum_{i=1}^{r} \text{Zero(PS, I}_i\text{)} \quad (10)$$

where $J = I_1' \cdots I_r'$.

To summarize the discussion above, we have

Theorem 3.6. There is a mechanical algorithm, for any finite polynomial set PS over $\mathbf{Z}$, we can find a polynomial set CS over $\mathbf{Z}$, an integer n and a polynomial J such that

$$Zero(CS/J) \subset Zero(PS) \subset Zero(CS)$$

over any finite field of characteristic not a prime factor of n.

Now we have been in the position to give a procedure for TPM in projective plane over finite fields. If the field we work on is a fixed finite field or its characteristic has been given, then we can do the TPM by Theorem 3.3 and 3.4. otherwise, we can follow the following steps to decide in which finite field and under what conditions the theorem is true.

Step 1: Express the hypotheses of theorem by polynomial set PS, the conclusion by polynomial g. Then these polynomials would be polynomials over $\mathbf{Z}$.

Step 2: Compute the characteristic chain CS of PS over $\mathbf{Z}$ or a field of characteristic 0, and compute the integer n and polynomial J of Theorem 3.6.

Step 3: Compute the pseudo remainder $prem(g,CS)$ of g with respect to CS. Then

1. If $prem(g,CS) = 0$, then over any finite field of characteristic not a prime factor of n, the theorem is true under non-degenerate condition $J \neq 0$.
2. If $prem(g,CS) \neq 0$, we can write $prem(g,CS) = m \cdot p$, where m is the integer factor of $prem(g,CS)$. Then over any field of characteristic which is a prime factor of m but not a prime factor of n, the theorem is true under non-degenerate condition $J \neq 0$.

If we want to know the theorem is true or false in the exceptions, we can use the theorems of this section repeatedly.

Remark 3.7. In this section, we don't present the procedure of computing the characteristic set of a polynomial set, since it is the same as that in the case of characteristic 0. In fact, all the techniques used in proving theorems over a field of characteristic 0 can be used here.

In the next section, we will prove some theorems of projective plane over finite fields by Wu's method.

4 Examples

Two triangles $\triangle A_1B_1C_1$ and $\triangle A_2B_2C_2$ are said to be in *perspective* from a point O if the lines A_1A_2, B_1B_2 and C_1C_2 pass through O.

Example 4.1 (Desargue's Theorem). If $\triangle A_1B_1C_1$ and $\triangle A_2B_2C_2$ are in perspective from O, then the intersections of the lines A_1B_1 and A_2B_2, of A_1C_1 and A_2C_2, and of B_1C_1 and B_2C_2, are collinear (Figure 4.1).

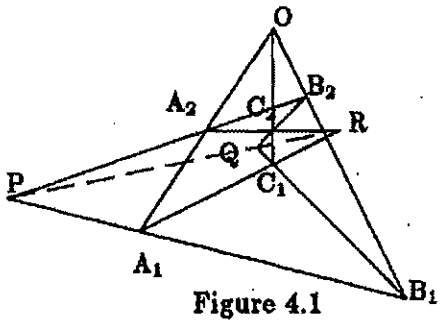

Figure 4.1

Proof: Take $O = (0,0,1)$, $A_1 = (x_1,x_2,x_3)$, $B_1 = (x_4,x_5,x_6)$, $C_1 = (x_7,x_8,x_9)$, $A_2 = (x_{10},x_{11},x_{12})$, $B_2 = (x_{13},x_{14},x_{15})$, $C_2 = (x_{16},x_{17},x_{18})$, $Q = (x_{19},x_{20},x_{21})$, $P = (x_{22},x_{23},x_{24})$, $R = (x_{25},x_{26},x_{27})$. Then the hypotheses of the theo-

rem can be expressed by

$$
\begin{aligned}
P_1 =& x_{11}x_1 - x_{10}x_2\\
P_2 =& x_{14}x_4 - x_{13}x_5\\
P_3 =& 2x_{17}x_7 - x_{16}x_8\\
P_4 =& x_{21}x_8x_4 - x_{21}x_7x_5 - x_{20}x_9x_4\\
&+x_{20}x_7x_6 + x_{19}x_9x_5 - x_{19}x_8x_6\\
P_5 =& x_{21}x_{17}x_{13} - x_{21}x_{16}x_{14} - x_{20}x_{18}x_{13}\\
&+x_{20}x_{16}x_{15} + x_{19}x_{18}x_{14} - x_{19}x_{17}x_{15}\\
P_6 =& x_{27}x_8x_1 - x_{27}x_7x_2 - x_{26}x_9x_1\\
&+x_{26}x_7x_3 + x_{25}x_9x_2 - x_{25}x_8x_3\\
P_7 =& x_{27}x_{17}x_{10} - x_{27}x_{16}x_{11} - x_{26}x_{18}x_{10}\\
&+x_{26}x_{16}x_{12} + x_{25}x_{18}x_{11} - x_{25}x_{17}x_{12}\\
P_8 =& x_{24}x_5x_1 - x_{24}x_4x_2 - x_2{}^3x_6x_1\\
&+x_2{}^3x_4x_3 + x_{22}x_6x_2 - x_{22}x_5x_3\\
P_9 =& x_{24}x_{14}x_{10} - x_{24}x_{13}x_{11} - x_2{}^3x_{15}x_{10}\\
&+x_2{}^3x_{13}x_{12} + x_{22}x_{15}x_{11} - x_{22}x_{14}x_{12}
\end{aligned}
$$

The conclusion can be expressed by

$$
\begin{aligned}
P_{10} =\ & x_{27}x_2{}^3x_{19} - x_{27}x_{22}x_{20} - x_{26}x_{24}x_{19}\\
&+x_{26}x_{22}x_{21} + x_{25}x_{24}x_{20} - x_{25}x_2{}^3x_{21}
\end{aligned}
$$

By computations over $\mathbf{Z}$, we get the characteristic set $[CS, 0]$ of the first nine polynomials as

$$
\begin{aligned}
P_{11} =& x_{11}x_1 - x_{10}x_2,\\
P_{12} =& x_{14}x_4 - x_{13}x_5,\\
P_{13} =& x_{17}x_7 - x_{16}x_8,\\
P_{14} =& (x_8x_4 - x_7x_5)(x_{20}x_{18}x_{13}x_7x_4 - x_{20}x_{16}x_{15}x_7x_4\\
&-x_{20}x_{16}x_{13}x_9x_4 + x_{20}x_{16}x_{13}x_7x_6\\
&-x_{19}x_{18}x_{13}x_7x_5 + x_{19}x_{16}x_{15}x_8x_4\\
&+x_{19}x_{16}x_{13}x_9x_5 - x_{19}x_{16}x_{13}x_8x_6),\\
P_{15} =& x_{13}x_{16}(x_8x_4 - x_7x_5)^2(x_{21}x_{18}x_{13}x_7x_4\\
&-x_{21}x_{16}x_{15}x_7x_4 - x_{21}x_{16}x_{13}x_9x_4\\
&+x_{21}x_{16}x_{13}x_7x_6 - x_{19}x_{18}x_{13}x_7x_6\\
&+x_{19}x_{16}x_{15}x_9x_4),\\
P_{16} =& (x_6x_1 - x_4x_2)(x_{23}x_{15}x_{10}x_4x_1 - x_{23}x_{13}x_{12}x_4x_1\\
&-x_{23}x_{13}x_{10}x_6x_1 + x_{23}x_{13}x_{10}x_4x_3\\
&-x_{22}x_{15}x_{10}x_4x_2 + x_{22}x_{13}x_{12}x_5x_1\\
&+x_{22}x_{13}x_{10}x_6x_2 - x_{22}x_{13}x_{10}x_5x_3),\\
P_{17} =& x_{10}x_{13}(x_5x_1 - x_4x_2)^2(x_{24}x_{15}x_{10}x_4x_1\\
&-x_{24}x_{13}x_{12}x_4x_1 - x_{24}x_{13}x_{10}x_6x_1\\
&+x_{24}x_{13}x_{10}x_4x_3 - x_{22}x_{15}x_{10}x_4x_3\\
&+x_{22}x_{13}x_{12}x_6x_1),\\
P_{18} =& (x_8x_1 - x_7x_2)(x_{26}x_{18}x_{10}x_7x_1 - x_{26}x_{16}x_{12}x_7x_1\\
&-x_{26}x_{16}x_{10}x_9x_1 + x_{26}x_{16}x_{10}x_7x_3\\
&-x_{25}x_{18}x_{10}x_7x_2 + x_{25}x_{16}x_{12}x_8x_1\\
&+x_{25}x_{16}x_{10}x_9x_2 - x_{25}x_{16}x_{10}x_8x_3),
\end{aligned}
$$

$$
\begin{aligned}
P_{19} =& x_{10}x_{16}(x_8x_1 - x_7x_2)^2(x_{27}x_{18}x_{10}x_7x_1\\
&-x_{27}x_{16}x_{12}x_7x_1 - x_{27}x_{16}x_{10}x_9x_1\\
&+x_{27}x_{16}x_{10}x_7x_3 - x_{25}x_{18}x_{10}x_7x_3\\
&+x_{25}x_{16}x_{12}x_9x_1),
\end{aligned}
$$

and the pseudo-remainder of P_{10} with respect to CS is zero. Hence the theorem is true under non-degenerate condition

$$
\begin{aligned}
J =& x_1x_4x_7x_{13}x_{16}x_{10}(x_8x_4 - x_7x_5)(x_{18}x_{13}x_7x_4\\
&-x_{16}x_{15}x_7x_4 - x_{16}x_{13}x_9x_4 + x_{16}x_{13}x_7x_6)(x_6x_1\\
&-x_4x_2)(x_{15}x_{10}x_4x_1 - x_{13}x_{12}x_4x_1 - x_{13}x_{10}x_6x_1\\
&+x_{13}x_{10}x_4x_3)(x_8x_1 - x_7x_2)(x_{18}x_{10}x_7x_1\\
&-x_{16}x_{12}x_7x_1 - x_{16}x_{10}x_9x_1 + x_{16}x_{10}x_7x_3).
\end{aligned}
$$

By further computations, we can assert that the theorem is true except the case $(x_8x_1 - x_7x_2)(x_5x_1 - x_4x_2)(x_8x_4 - x_7x_5) = 0$ which means that A_1B_1 and A_2B_2, or A_1C_1 and A_2C_2, or B_1C_1 and B_2C_2 are coincide.

A projective plane in which Desargue's theorem holds is called Desarguesian. Hence the projective plane $PG(2, \mathbf{F}_q)$ is Desarguesian.

Example 4.2 (Theorem of Pappus). If A_1, B_1, C_1 are points of a lines and A_2, B_2, C_2 are points of another line in the the same plane, and if A_1B_2 and A_2B_1 intersect in P, A_1C_2 and A_2C_1 intersect in Q, and B_1C_2 and B_2C_1 intersect in R, then P, Q, and R are collinear (Figure 4.2).

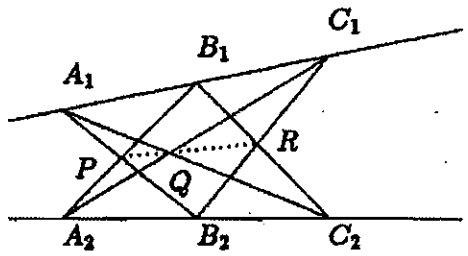

Figure 4.2

This is an important theorem in finite projective plane. It has also been proved by Wu's method on machine. The proof of this theorem is omitted here because there is no special technique used in the proof.

A *complete quadrangle* in the projective plane is a configuration consisting of (i) four points, no three of them are collinear, and (ii) six lines, each of them joining a pair of the points. the four points of a complete quadrangle are called its *verteces*, and the six lines are called its *diagonal*, the intersection

of any two diagonals is called a diagonal points of the complete quadrangle. For example, in Figure 2.1, $CDGE$ is a complete quadrangle with diagonal points A, F, B.

Example 4.3. The diagonal points of a complete quadrangle in $PG(2,\mathbf{F}_q)$ are collinear if q is even.

Proof: Let A, B, C, and D be the four verteces of a complete quadrangle, E, F, and G be the intersections of AC and BD, of AB and CD, and of AD and BC respectively. Without loss of generality, we may suppose $A=(0,0,1)$, $B=(x_1,x_2,x_3)$, $C=(x_4,x_5,x_6)$, $D=(x_7,x_8,x_9)$, $E=(x_{10},x_{11},x_{12})$, $F=(x_{13},x_{14},x_{15})$, and $G=(x_{16},x_{17},x_{18})$. Then the conditions of the theorem can be expressed as polynomials:

$$\begin{aligned}
P_1 &= x_{14}x_1 - x_{13}x_2,\\
P_2 &= x_{17}x_7 - x_{16}x_8,\\
P_3 &= x_{11}x_4 - x_{10}x_5,\\
P_4 &= x_{12}x_8x_1 - x_{12}x_7x_2 - x_{11}x_9x_1 + x_{11}x_7x_3\\
&\quad + x_{10}x_9x_2 - x_{10}x_8x_3,\\
P_5 &= x_{18}x_5x_1 - x_{18}x_4x_2 - x_{17}x_6x_1\\
&\quad + x_{17}x_4x_3 + x_{16}x_6x_2 - x_{16}x_5x_3,\\
P_6 &= x_{15}x_8x_4 - x_{15}x_7x_5 - x_{14}x_9x_4\\
&\quad + x_{14}x_7x_6 + x_{13}x_9x_5 - x_{13}x_8x_6,
\end{aligned}$$

and the conclusion can be expressed as polynomial:

$$\begin{aligned}
P_7 = {} & x_{18}x_{14}x_{10} - x_{18}x_{13}x_{11} - x_{17}x_{15}x_{10}\\
& + x_{17}x_{13}x_{12} + x_{16}x_{15}x_{11} - x_{16}x_{14}x_{12}.
\end{aligned}$$

The characteristic set $[CS,0]$ of $\{P_1,P_2,\cdots,P_6\}$ contains

$$\begin{aligned}
P_8 &= x_{18}x_7x_5x_1 - x_{18}x_7x_4x_2 - x_{16}x_8x_6x_1\\
&\quad + x_{16}x_8x_4x_3 + x_{16}x_7x_6x_2 - x_{16}x_7x_5x_3,\\
P_9 &= x_{17}x_7 - x_{16}x_8,\\
P_{10} &= x_{15}x_8x_4x_1 - x_{15}x_7x_5x_1 + x_{13}x_9x_5x_1\\
&\quad - x_{13}x_9x_4x_2 - x_{13}x_8x_6x_1 + x_{13}x_7x_6x_2,\\
P_{11} &= x_{14}x_1 - x_{13}x_2,\\
P_{12} &= x_{12}x_8x_4x_1 - x_{12}x_7x_4x_2 - x_{10}x_9x_5x_1\\
&\quad + x_{10}x_9x_4x_2 - x_{10}x_8x_4x_3 + x_{10}x_7x_5x_3,\\
P_{13} &= x_{11}x_4 - x_{10}x_5,
\end{aligned}$$

and the pseudo-remainder P_{14} of polynomial P_7 w.r.t. $[CS,0]$ is

$$\begin{aligned}
P_{14} = {} & 2x_{16}x_{13}x_{10}x_7x_4x_1(x_5x_1 - x_4x_2)(x_8x_4\\
& - x_7x_5)(x_8x_1 - x_7x_2)(x_9x_5x_1 - x_9x_4x_2\\
& - x_8x_6x_1 + x_8x_4x_3 + x_7x_6x_2 - x_7x_5x_3),
\end{aligned}$$

so the conclusion is true under condition q is even and

$$\begin{aligned}
J = {} & x_7^2x_4^2x_1^2(x_8x_1 - x_7x_2)(x_8x_4 - x_7x_5)(x_5x_1\\
& - x_4x_2) \neq 0,
\end{aligned}$$

i.e. theorem is true under non-degenerate condition $J\neq 0$. In fact, $(x_8x_1 - x_7x_2)(x_8x_4 - x_7x_5)(x_5x_1 - x_4x_2)\neq 0$ is always true for a complete quadrangle and only one of the three variables x_1, x_4 and x_7 can be zero. By further computations, we can assert that theorem is also true even if one of x_1, x_4 and x_7 are zero. Therefore, theorem is always true.

Theorem 4.4. Any three distinct points on a conic are not collinear.

Proof: Without loss of generality, we may suppose the conic has equation

$$X^2 + YZ = 0. \tag{11}$$

Let $A=(x_1,x_2,x_3)$, $B=(x_4,x_5,x_6)$, $C=(x_7,x_8,x_9)$ be three points on the conic. Then the theorem is equivalent to that provided A, B and C are collinear, then two of them are coincide. The condition polynomials are

$$\begin{aligned}
\text{A on conic: } P_1 &= x_3x_2 + x_1^2,\\
\text{B on conic: } P_2 &= x_6x_5 + x_4^2,\\
\text{C on conic: } P_3 &= x_9x_8 + x_7^2,
\end{aligned}$$

A, B, and C are collinear:

$$\begin{aligned}
P_4 = {} & x_9x_5x_1 - x_9x_4x_2 - x_8x_6x_1\\
& + x_8x_4x_3 + x_7x_6x_2 - x_7x_5x_3
\end{aligned}$$

and conclusion polynomials are:

$$\begin{aligned}
\text{A=B: } & p_5 = x_5x_1 - x_4x_2,\\
& P_6 = x_6x_1 - x_4x_3\\
& P_7 = x_2x_6 - x_5x_3\\
\text{A=C: } & P_8 = x_8x_1 - x_7x_2,\\
& P_9 = x_9x_1 - x_7x_3\\
& P_{10} = x_2x_9 - x_3x_8\\
\text{B=C: } & P_{11} = x_8x_4 - x_7x_5,\\
& P_{12} = x_9x_4 - x_7x_6\\
& P_{13} = x_5x_9 - x_8x_6.
\end{aligned}$$

The characteristic set of the set of condition polynomials contains:

$$\begin{aligned}
P_{14} &= x_3x_2 + x_1^2,\\
P_{15} &= x_6x_5 + x_4^2,\\
P_{16} &= x_8^2x_5x_4x_1^2 - x_8^2x_4^2x_2x_1 - x_8x_7x_5^2x_1^2\\
&\quad + x_8x_7x_4^2x_2^2 + x_7^2x_5^2x_2x_1 - x_7^2x_5x_4x_2^2,\\
P_{17} &= x_9x_8 + x_7^2
\end{aligned}$$

and the non-degenerate polynomial are

$$J = x_8x_5x_4x_2x_1(x_5x_1 - x_4x_2).$$

Factorize P_{16} as

$$\begin{aligned} P_{16} =& (x_5x_1 - x_4x_2)(x_8x_4 - x_7x_5)(x_8x_1 - x_7x_2) \\ =& P_{16}^{(1)}P_{16}^{(2)}P_{16}^{(6)}, \end{aligned}$$

then we can check that $P_{16}^{(1)}$ is a factor of J and the pseudo remainders of P_8, P_9 and P_{10}, and of P_{11}, P_{12} and P_{13} are zero polynomials with respect to $\{P_{14}, P_{15}, P_{16}^{(2)}, P_{17}\}$ and $\{P_{14}, P_{15}, P_{16}^{(3)}, P_{17}\}$ respectively. Hence the theorem is true under condition

$$J = x_8x_5x_4x_2x_1(x_5x_1 - x_4x_2) \neq 0$$

In fact, we can check that the theorem is also true even if $J = 0$.

Theorem 4.5. If q is odd, then any three distinct tangents of a conic are not concurrent.

Proof: Without loss of generality, we may suppose the equation of the conic is (11). The theorem is equivalent to that for any three points A, B and C, if the three tangents at A, B and C meet at a point O, then two of the three points A, B and C must be coincide.

Suppose $A = (x_1, x_2, x_3)$, $B = (x_4, x_5, x_6)$ and $C = (x_7, x_8, x_9)$. Then the equations of the tangents at A, B and C are

$$\begin{aligned} &\text{Tangent } l_1 \text{ at A:} \quad 2x_1X + x_3Y + x_2Z = 0 \\ &\text{Tangent } l_2 \text{ at B:} \quad 2x_4X + x_6Y + x_5Z = 0 \\ &\text{Tangent } l_3 \text{ at C:} \quad 2x_7X + x_9Y + x_8Z = 0 \end{aligned}$$

So the hypotheses can be expressed by

$$\begin{aligned} &\text{A on the conic:} \quad P_1 = x_3x_2 + x_1^2 \\ &\text{B on the conic:} \quad P_2 = x_6x_5 + x_4^2 \\ &\text{C on the conic:} \quad P_3 = x_9x_8 + x_7^2 \end{aligned}$$

l_1, l_2, l_3 are concurrent:

$$\begin{aligned} P_4 = \; & -2(x_9x_5x_1 - x_9x_4x_2 - x_8x_6x_1 \\ & + x_8x_4x_3 + x_7x_6x_2 - x_7x_5x_3) \end{aligned}$$

and the conclusion polynomials are:

$$\begin{aligned} \text{A=B:} \quad & p_5 = x_5x_1 - x_4x_2, \\ & P_6 = x_6x_1 - x_4x_3 \\ & P_7 = x_2x_6 - x_5x_3 \\ \text{A=C:} \quad & P_8 = x_8x_1 - x_7x_2, \\ & P_9 = x_9x_1 - x_7x_3 \\ & P_{10} = x_2x_9 - x_8x_8 \\ \text{B=C:} \quad & P_{11} = x_8x_4 - x_7x_5, \\ & P_{12} = x_9x_4 - x_7x_6 \\ & P_{13} = x_5x_9 - x_8x_6 \end{aligned}$$

Working on $\mathbb{Z}$ we get the characteristic set $[CS, 0]$ of $\{P_1, P_2, P_3, P_4\}$ as

$$\begin{aligned} P_{14} = \; & x_9x_8 + x_7^2, \\ P_{15} = \; & 2(x_8^2x_5x_4x_1^2 - x_8^2x_4^2x_2x_1 - x_8x_7x_5^2x_1^2 \\ & + x_8x_7x_4^2x_2^2 + x_7^2x_5^2x_2x_1 \\ & - x_7^2x_5x_4x_2^2), \\ P_{16} = \; & x_6x_5 + x_4^2, \\ P_{17} = \; & x_3x_2 + x_1^2 \end{aligned}$$

Factorize P_{15} as

$$\begin{aligned} P_{15} \; & = 2(x_8x_4 - x_7x_5)(x_8x_1 - x_7x_2)(x_5x_1 \\ & - x_4x_2) = P_{15}^{(1)}P_{15}^{(2)}P_{15}^{(3)} \end{aligned}$$

It is easy to check that the conclusion is true under condition:

$$2 \not| q \text{ and } J = x_8x_5x_4x_2x_1(x_5x_1 - x_4x_2) \neq 0$$

In fact, provided $2 \not| q$, the conclusion is also true even if $J = 0$.

Theroem 4.6. If q is even, then all the tangents of a conic meet in a single point.

Proof: Without loss of generality, we may suppose the equation of the conic is (11). Let $A = (x_1, x_2, x_3)$, $B = (x_4, x_5, x_6)$, $C = (x_7, x_8, x_9)$ be any three distinct points on the conic, $O = (x_{10}, x_{11}, x_{12})$ be the intersection of the tangents at A and B. Then the theorem is to say that the tangent at C pass through O. Hence the hypotheses are

$$\begin{aligned} & P_1 = x_3x_2 + x_1^2, \\ & P_2 = x_6x_5 + x_4^2, \\ & P_3 = x_9x_8 + x_7^2, \\ & P_4 = x_{12}x_2 + x_{11}x_3 + 2x_{10}x_1, \\ & P_5 = x_{12}x_5 + x_{11}x_6 + 2x_{10}x_4 \end{aligned}$$

the conclusion is

$$P_6 = x_{12}x_8 + x_{11}x_9 + 2x_{10}x_7$$

Working modulo 2 we get the characteristic set $[CS, 2]$ of the first five polynomials as

$$\begin{aligned} P_7 &= x_{12}x_6^2(x_5x_1 - x_4x_2)^2 \\ P_8 &= x_{11}(x_5x_1 - x_4x_2)^2, \\ P_9 &= x_9x_8 + x_7^2, \\ P_{10} &= x_6x_5 + x_4^2, \\ P_{11} &= x_3x_2 + x_1^2 \end{aligned}$$

and the pseudo-remainder of P_6 w.r.t. $[CS, 2]$ is 0. Hence the conclusion is true under condition

$$J = x_8x_5^3x_2(x_5x_1 - x_4x_2)^4 \neq 0.$$

In fact, the conclusion is always true except the case $x_5 = x_2 = 0$. In this case, we would get $A = B$, a contradiction to the the hypotheses. Hence theorem is true.

References

1. Bledsoe, W. W. and Loveland, D. W.(ed.), Automated Theorem proving, after 25 years, Amer. Math. Soc.,(1984)
2. Chou, S. C. , Mechanical Geometry Theorem Proving, D. Reidel Publishing Company, 1988.
3. Chou, S.C. and Gao, X.S., Theorem proved automatically using Wu's method — part on differential geometry and mechanics. MM Research preprints, No. 6(1991), 37-55.
4. Hall, M., Jr., Combinatorial Theory (2nd edition). A Wiley-Interscience Publication, 1986.
5. Li, Z. M., Mechanical theorem proving of the local theory of surfaces. MM Research preprints, No. 6(1991), 102-120.
6. Lidl, R. and Niederreiter, H., Finite fields. Addison-Wesley Publishing Company, 1983.
7. Wan, Zhe-xian, Geometry of Classical Group over Finite Fields, to be published by Studentlitteratur, 1993.
8. Wu, Wentsün, Mechanical Theorem proving of differential geometry and some of applications in mechanics, MM Research preprints, No. 6(1991), 1-22.
9. ———, On the decision problem and the mechanization of theorem-proving in elementary geometry, Scientia Sinica, 21(1978), 159-172.
10. ———, Basic priciple of mechanical theorem proving in elementary geometry. J. Sys. Sci. & Math. Sci., No. 4(1984), 207-235. Republished in J. Automated Reasoning, 2(1986), 221-252.
11. ———, On the Foundation of Algebraic Differential Geometry. J. Sys. & Math. Sci., Vol. 2, No. 4(1989), 290-312.
12. ———, Automated Derivation of Newton's Gravitational Laws from Kepler's Laws. To appear in New Trends in Automated Mathematical Reasoning, Eds. A. Ferro et al.