THREE-PARAMETER AND FOUR-PARAMETER LINEAR FAMILIES OF CONICS IN THE GALOIS FIELDS OF ORDER 2^n*

BY A. D. CAMPBELL

1. *Three-Parameter Families.* We shall denote a Galois field of order 2^n by the symbol $GF(2^n)$. We define a three-parameter linear family of conics in such a $GF(2^n)$ as the locus of all points whose coordinates x, y, z satisfy an equation of the form

$$\lambda C_1 + \mu C_2 + \nu C_3 + \rho C_4 = 0, \tag{1}$$

where

$$C_i = a_i x^2 + b_i y^2 + c_i z^2 + f_i yz + g_i zx + h_i xy = 0, \quad (i = 1,2,3,4),$$

and where the variables, coefficients, and parameters represent numbers in this domain. The conics $C_1=0, \cdots, C_4=0$ are linearly independent, and are called fundamental conics of this family. In this paper we derive the classes of these families, and we give a typical family for each class. We note that in any $GF(2^n)$ every number is a perfect square with just one square root, and $(\alpha x+\beta y+\gamma z)^2=\alpha^2x^2+\beta^2y^2+\gamma^2z^2$. We note that every such family has at least one double line.

We first divide these families into the following distinct sets.

Set I. Each family contains a net of conics reducible to the form

$$\lambda x^2 + \mu y^2 + \nu z^2 = 0. \tag{2}$$

Set II. Each family contains no net reducible to (2), but does contain a net reducible to the form

$$\lambda x^2 + \mu y^2 + 2\nu xy = 0. \tag{3}$$

* Presented to the Society, December 29, 1923.

Set III. Each family contains at least two double lines, but no net reducible to (2) or (3).

Set IV. Each family contains only one double line, but has also a net reducible to the form

$$(4) \qquad \lambda x^2 + \mu xy + \nu xz = 0.$$

Set V. Each family has none of the preceding properties, but has a pencil reducible to the form

$$(5) \qquad \lambda x^2 + \mu xy = 0.$$

Set VI. Each family has just one double line, but none of the preceding degenerate pencils and nets.

Set I. Such a family can be put in the form

$$\lambda x^2 + \mu y^2 + \nu z^2 + \rho(fyz + gzx + hxy) = 0.$$

We easily get

$$(6) \qquad \text{Class (1)}: \qquad \lambda x^2 + \mu y^2 + \nu z^2 + \rho xy = 0.$$

Set II. We obtain

$$(7) \qquad \text{Class (2)}: \qquad \lambda x^2 + \mu y^2 + \nu xy + \rho(z^2 + zx) = 0.$$

$$(8) \qquad \text{Class (3)}: \qquad \lambda x^2 + \mu y^2 + \nu xy + \rho zx = 0.$$

Any transformation

$$(9) \qquad x = \alpha_1 x' + \beta_1 y' + \gamma_1 z', \quad y = \alpha_2 x' + \beta_2 y' + \gamma_2 z', \quad z = \alpha_3 x' + \beta_3 y' + \gamma_3 z',$$

where $|\alpha_1, \beta_2, \gamma_3| \neq 0$, that is to send (7) into (8) must have $\gamma_1 = \gamma_2 = 0$, $\gamma_3 \neq 0$, since the net $\rho = 0$ of one family must go into that of the other. But (9) then cannot send (7) into a family lacking the term in z^2.

Set III. We can reduce such a family to the form

$$\lambda x^2 + \mu y^2 + \nu xz + \rho(cz^2 + fyz + hxy) = 0.$$

We get the following three classes, according as $cf \neq 0$; or $c = 0$, $f \neq 0$; or $c \neq 0, f = 0$.

(10) Class (4) : $\lambda x^2 + \mu y^2 + \nu zx + \rho(z^2 + yz) = 0.$

(11) Class (5) : $\lambda x^2 + \mu y^2 + \nu zx + \rho yz = 0.$

An argument similar to that used in the study of (7) and (8) shows that (10) and (11) are non-equivalent. Here the pencil $\nu = \rho = 0$ of (10) must go into the similar pencil of (11) by any projectivity (9).

(12) Class (6) : $\lambda x^2 + \mu y^2 + \nu zx + \rho(z^2 + xy) = 0.$

It is easy to prove (12) non-equivalent to (10) or (11).

Set IV. We put (1) in the form

$$\lambda x^2 + \mu xy + \nu xz + \rho(by^2 + cz^2 + fyz) = 0.$$

We get two classes, according as $C_4 = 0$ in the above family is a pair of real or conjugate imaginary lines.

(13) Class (7) : $\lambda x^2 + \mu xy + \nu xz + \rho yz = 0.$

(14) Class (8) : $\lambda x^2 + \mu xy + \nu xz + \rho(y^2 + z^2 + \alpha yz) = 0,$

where $C_4 = 0$ is irreducible. Any transformation (9) that is to send (14) into (13) must have $\beta_1 = \gamma_1 = 0$. But then the conic $C_4 = 0$ of (14) goes into a conic $y'^2(\beta_2^2 + \beta_3^2 + \alpha\beta_2\beta_3) + z'^2(\gamma_2^2 + \gamma_3^2 + \alpha\gamma_2\gamma_3) + \cdots = 0$. So we must have $\beta_2^2 + \beta_3^2 + \alpha\beta_2\beta_3 = 0$, $\gamma_2^2 + \gamma_3^2 + \alpha\gamma_2\gamma_3 = 0$ which give us $\beta_2 = \beta_3 = \gamma_2 = \gamma_3 = 0$ and (9) is singular.

Set V. We can put the family in one of the three following forms:

(A) $\lambda x^2 + \mu xy + \nu(z^2 + zx) + \rho(by^2 + fyz + gzx) = 0;$

(B) $\lambda x^2 + \mu xy + \nu yz + \rho(by^2 + cz^2 + gzx) = 0,$

(C) $\lambda x^2 + \mu xy + \nu(z^2 + yz) + \rho(by^2 + cz^2 + gzx) = 0.$

Case (A) gives us two classes.

(15) Class (9) : $\lambda x^2 + \mu xy + \nu(z^2 + zx) + \rho(y^2 + yz) = 0.$

(16) Class (10) : $\lambda x^2 + \mu xy + \nu(z^2 + zx) + \rho yz = 0.$

Any projectivity (9) that is to send (15) into (16) must have $\beta_1 = \gamma_1 = \gamma_2 = 0$, $\beta_2\gamma_3 \neq 0$. But then $C_3 = 0$ and $C_4 = 0$ of (10) must go separately into conics lacking the term in y^2. This gives us $\beta_3^2=0$, $\beta_2^2+\beta_2\beta_3=0$; hence $\beta_2=0$.

Case (B) gives us two classes.

$$(17)\qquad \text{Class (11)}: \lambda x^2+\mu xy+\nu yz+\rho(y^2+z^2+zx)=0.$$

$$(18)\qquad \text{Class (12)}: \lambda x^2+\mu xy+\nu yz+\rho(y^2+zx)=0.$$

The families (17) and (18) are easily proved to be non-equivalent. They are non-equivalent to families (15) and (16) because of the presence in these two latter families of the degenerate pencil $\lambda x^2+\nu(z^2+zx)=0$.

Case (C) gives us the following class.

$$(19)\qquad \text{Class (13)}: \lambda x^2+\mu xy+\nu(z^2+yz)+\rho(y^2+\alpha z^2+zx)=0.$$

Set VI. We can put the family in one of two forms

$$(\text{A})\qquad \lambda x^2+\mu(y^2+xy)+\nu yz+\rho(by^2+cz^2+gzx)=0,$$

$$(\text{B})\qquad \lambda x^2+\mu yz+\nu(by^2+cz^2+gzx)+\rho(b'y^2+c'z^2+h'xy)=0.$$

Case (A) gives us

(20) Class (14):

$$\lambda x^2+\mu(y^2+xy)+\nu yz+\rho(y^2+\alpha z^2+zx)=0,\quad \alpha\neq 0.$$

Case (B) gives us

(21) Class (15):

$$\lambda x^2+\mu yz+\nu(y^2+\alpha z^2+zx)+\rho(\beta y^2+\gamma z^2+xy)=0,$$

where $\gamma=1$ or $\gamma\neq$ cube, $\gamma/\beta\neq\alpha$. The family (20) has a degenerate pencil $\lambda x^2+\mu(y^2+xy)=0$, which does not occur in (21).

2. *Four-Parameter Families.* We define a four-parameter linear family of conics in a $GF(2^n)$ by the equation

$$(22)\qquad \lambda C_1+\mu C_2+\nu C_3+\rho C_4+\sigma C_5=0,$$

where the details of notation are as indicated in the description of equation (1). It is easy to show that every such family has at least two double lines. First we assume that

(22) has a degenerate net reducible to (2). Then we assume that (22) has no net (2), but a net (3). Then we assume that (22) has neither (2) nor (3).

If (22) has a net (2) we can put the family in the form

$$\lambda x^2 + \mu y^2 + \nu z^2 + \rho xy + \sigma(fyz + gzx) = 0,$$

which gives us

(23) Class (1) : $\lambda x^2 + \mu y^2 + \nu z^2 + \rho xy + \sigma xz = 0.$

If (22) has a net (3), but not a net (2), we get

$$\lambda x^2 + \mu y^2 + \nu xy + \rho xz + \sigma(cz^2 + fyz) = 0,$$

which gives us, according as $c \neq 0$, or $c = 0$,

(24) Class (2) : $\lambda x^2 + \mu y^2 + \nu xy + \rho xz + \sigma(z^2 + yz) = 0,$

(25) Class (3) : $\lambda x^2 + \mu y^2 + \nu xy + \rho xz + \sigma yz = 0.$

If (9) is to send (24) into (25) we must have $\gamma_1 = \gamma_2 = 0$, $\gamma_3 \neq 0$. But such a transformation cannot send (24) into a family lacking the term in z^2.

If (22) has no net (2) and no net (3) we easily reduce the family to the form

(26) Class (4) : $\lambda x^2 + \mu y^2 + \nu xz + \rho yz + \sigma(z^2 + xy) = 0.$

SYRACUSE UNIVERSITY