Can. J. Math., Vol. XXXVIII, No. 3, 1986, pp. 672-696

THE GEOMETRY OF $GF(q^3)$

F. A. SHERK

1. Introduction. Inversive geometry involves as basic entities points and circles [**2**, p. 83; **4**, p. 252]. The best known examples of inversive planes (the Miquelian planes) are constructed from a field K which is a quadratic extension of some other field F. Thus the complex numbers yield the Real Inversive Plane, while the Galois field $GF(q^2)(q = p^e, p$ prime) yields the Miquelian inversive plane $M(q)$ [**2**, chapter 9; **4**, p. 257]. The purpose of this paper is to describe an analogous geometry of $M(q)$ which derives from $GF(q^3)$, the cubic extension of $GF(q)$.

The resulting space, $\mathscr{A}$, is three-dimensional, involving a class $\{\mathscr{S}\}$ of surfaces which include planes, some quadric surfaces, and some cubic surfaces. We explore these surfaces, giving particular attention to the number of points they contain, and their intersections with lines and planes of the space $\mathscr{A}$.

It should be noted that this geometry is radically different from three dimensional real inversive geometry, in which spheres are preserved by the automorphism group of the space. The geometry developed here is much more closely related to the "circle geometry" of Bruck [**1**]. The automorphism groups are almost the same (Bruck's is slightly larger), and some results on the nature of these groups are common to both papers. But the invariants studied in [**1**] are the "circles" (which are not necessarily circles in the classical sense, i.e., plane conics), whereas the invariants in this paper are surfaces, including planes, quadric cones, hyperboloids, and some cubic surfaces. Some of these surfaces appear in [**1**] as "covers" of the circle geometry, but otherwise they are not considered. In this paper the emphasis is entirely on the surfaces. There is also a considerable difference in the methods used in [**1**] as compared to the present paper. In [**1**] the proofs are largely group-theoretical in nature, with little use of combinatorial arguments. Since the scope includes infinite spaces, this is not surprising. On the other hand this paper is restricted to finite spaces, and makes much use of counting arguments.

An examination of the quadric cones involved leads, in Section 6, to the discovery of a set of $q^2 + q + 1$ conics in the plane $PG(2, q)$ with the property that any two are mutually tangent. The same set of conics, in a somewhat wider context, was discovered by Jungnickel and Vedder by

Received May 11, 1984, and in revised form July 11, 1985. This research was supported by NSERC Grant No. A4827 (Canada). This paper was written while the author held a visiting appointment at Clemson University, Clemson, South Carolina.

the use of difference sets [7]. A few of the properties of these conics, which we call cells, are noted.

In Section 7 we study the cubic surfaces from the set $\{\mathscr{S}\}$. Our main object here is to locate any planes of $\mathscr{A}$ which fail to meet any given cubic $\mathscr{S}$. We find some cubics which are met by every plane in $\mathscr{A}$. For others, we find an exterior plane, which we conjecture to be unique.

We propose to show in a future paper that the surfaces $\{\mathscr{S}\}$ are useful in the study of finite translation planes of order q^3. In particular, semifield planes of order q^3 can be conveniently classified in the context of cubic surfaces from the set $\{\mathscr{S}\}$.

Throughout the paper, some more or less standard notation will be used without comment. We shall denote the cardinality of a finite set S by $|S|$, and occasionally also use the same symbol, "| |", to denote a determinant. The symbol $\langle A, B, C, \ldots \rangle$ will denote the group generated by $A, B, C, \ldots$ and the remainder of a set S when a subset T has been removed will be denoted either by $S - T$ or by $S \backslash T$.

2. The spaces $\mathscr{A}$ and $\bar{\mathscr{A}}$. Let F denote the field $GF(q)$ ($q = p^e$, p prime). Let K be a cubic extension of F, so that $K \cong GF(q^3)$. We shall denote the elements of K by capital Latin letters; A, B, X, Y, etc., and the elements of F by lower case Greek; $\alpha, \beta, \lambda, \mu$, etc. The zero and unit elements will be denoted by 0 and 1 respectively.

Any mapping $X \to X^{p^n}$ is an automorphism of K; in particular, if $n = e$, then $X \to X^q$ is of period 3 and fixes every element of F. Also, $K^* = K - \{0\}$, the multiplicative group of K, is cyclic; $K^* = \langle W \rangle$, where W is a primitive element of K. $F^* = F - \{0\}$ is generated by $\epsilon = W^{1+q+q^2}$.

There are three functions in K with range in F that are of importance in this context:

(i) $N(X) = X^{1+q+q^2}$. $N(X)$ is usually called the *norm* of X. It is easy to show that for any $\lambda \in F$, $\lambda \neq 0$, there are exactly $q^2 + q + 1$ elements Z in K^* such that $N(Z) = \lambda$.

(ii) $T(X) = X + X^q + X^{q^2}$. $T(X)$ is usually called the *trace* of X.

(iii) $B(X) = X^{1+q} + X^{q+q^2} + X^{q^2+1}$. We shall call $B(X)$ the *bitrace* of X.

The field K is usually denoted either as $\{0\} \cup \langle W \rangle$ or as a vector space $\mathscr{V}$ of dimension 3 over F. In the latter description, let $\{1, R, S\}$ be a basis for $\mathscr{V}$. Then any element X of K has a unique representation $X = \theta_1 + \theta_2 R + \theta_3 S$, where $\theta_1, \theta_2, \theta_3 \in F$. Multiplication is polynomial multiplication, and the products R^2, S^2, RS all have unique expression in the basis $\{1, R, S\}$.

In a natural fashion [4, pp. 27, 28], $\mathscr{V}$ defines a three-dimensional affine space $\mathscr{A} \cong AG(3, q)$, where the points of $\mathscr{A}$ are the elements of $\mathscr{V}$ (i.e., the elements of K) and the lines and planes are respectively translates of

the one- and two-dimensional subspaces of $\mathscr{V}$. Thus K is interpreted geometrically as the points of $\mathscr{A}$.

In the above interpretation the norm, trace, and bitrace functions induce familiar surfaces:

THEOREM 2.1. *$T(X) = \alpha$, $B(X) = \beta$, $N(X) = \gamma$ define respectively a plane, a quadric surface, and a cubic surface in $\mathscr{A}$.*

Proof. With fixed basis $\{1, R, S\}$ of $\mathscr{V}$,

$$X = \theta_1 + \theta_2 R + \theta_3 S,\ X^q = \theta_1 + \theta_2 R^q + \theta_3 S^q, \text{ and}$$
$$X^{q^2} = \theta_1 + \theta_2 R^{q^2} + \theta_3 S^{q^2}.$$

Now

$$T(X) = X + X^q + X^{q^2} = 3\theta_1 + T(R)\theta_2 + T(S)\theta_3.$$

Thus $T(X) = \alpha$ is a linear equation over F, defining a plane in $\mathscr{A}$. Similarly,

$$\begin{aligned} B(X) &= X^{1+q} + X^{q+q^2} + X^{q^2+1} \\ &= 3\theta_1^2 + B(R)\theta_2^2 + B(S)\theta_3^2 + 2T(R)\theta_1\theta_2 \\ &\quad + 2T(S)\theta_1\theta_3 + T(RS^q + R^qS)\theta_2\theta_3; \end{aligned}$$

so $B(X) = \beta$ is a quadratic equation in $\theta_1, \theta_2, \theta_3$ over F, defining a quadric surface. A similar calculation shows that $N(X) = \gamma$ is a cubic equation in $\theta_1, \theta_2, \theta_3$ over F, which therefore defines a cubic surface in $\mathscr{A}$.

Our further study of the geometry of K will involve point to point mappings in $\mathscr{A}$. Some of these will be collineations of $\mathscr{A}$, but others (analogous to inversions in an inversive plane) will not even be bijections unless the space $\mathscr{A}$ is enlarged. Anticipating this difficulty, we augment $\mathscr{A}$ by adding a single ideal point, which we denote by ∞. Just as in the development of Inversive Geometry, the particular properties of ∞ will be specified by the mappings that make it necessary. We denote $\{\infty\} \cup \mathscr{A}$ by $\bar{\mathscr{A}}$.

3. The permutation groups of $\bar{\mathscr{A}}$. Translations are familiar collineations of $\mathscr{A}$. Identifying points of $\mathscr{A}$ with elements of K, as we now consistently do, we describe any translation as $X \to A + X$, where A is some fixed element of K. We shall denote this translation by τ_A. Thus for each of the q^3 possible values for A, we have a translation τ_A; τ_0 is, of course, the identity, 1.

Another important collineation, which has no counterpart in real geometry, is $\Gamma: X \to WX$, where W is the generator of K^* introduced in Section 2. Since Γ^i is $X \to W^iX$ $(0 \leqq i < q^3 - 1)$, Γ has period $q^3 - 1$, and Γ^{q^2+q+1} is the central dilatation $X \to \epsilon X$.

The automorphism $\Sigma: X \to X^q$ is also a collineation of $\mathscr{A}$. In $\bar{\mathscr{A}}$, τ_A, Γ, and Σ all fix ∞.

We now define a mapping Δ in $\bar{\mathscr{I}}$ which we call the *inversion in* 0. Under Δ, $X \to X^{-1}$ where $X \neq 0$, and Δ interchanges 0 and ∞. Thus Δ is a bijection and $\Delta^2 = 1$. No confusion should arise if we describe Δ simply as $X \to X^{-1}$, even allowing X to be 0. A similar convention is used in the statement of the following theorem (cf. [**1**, pp. 153, 154]):

THEOREM 3.1. (i) Γ, $\{\tau_R\}(R \in K)$ *and* Δ *generate the group* G:

$$\left\{X \to (A + BX)^{-1}(C + DX) \mid A, B, C, D \in K, \begin{vmatrix} AC \\ BD \end{vmatrix} \neq 0\right\}$$

(ii) $G \cong PGL(2, q^3)$

(iii) Γ, $\{\tau_R\}(R \in K)$, Δ, *and* Σ *generate the larger group* $\bar{G}$:

$$\left\{X \to (A + BX^{q^i})^{-1}(C + DX^{q^i}) \mid A, B, C, D \in K, \begin{vmatrix} AC \\ BD \end{vmatrix} \neq 0, i = 0, 1, 2\right\},$$

which contains G *as a subgroup of index 3.*

Proof. Let $B = 0$ and choose $A \neq 0$, $D \neq 0$ such that $A^{-1}D = W^j$. Then under the product $\Gamma^j \tau_{A^{-1}C}$:

$$X \xrightarrow{\Gamma^j} A^{-1}DX \xrightarrow{\tau_{A^{-1}C}} A^{-1}C + A^{-1}DX = A^{-1}(C + DX).$$

If $B \neq 0$, then $B = W^i$ for some i. Let A, D be any elements of K. Then under the product $\Gamma^i \tau_A \Delta \tau_{B^{-1}D}$:

$$X \xrightarrow{\Gamma^i} BX \xrightarrow{\tau_A} A + BX \xrightarrow{\Delta} (A + BX)^{-1} \xrightarrow{\tau_{B^{-1}D}} B^{-1}D + (A + BX)^{-1}$$
$$= (A + BX)^{-1}(C + DX),$$

where $C = 1 + AB^{-1}D$. We note that

$$\begin{vmatrix} AC \\ BD \end{vmatrix} = AD - BC = -B \neq 0.$$

By convention,

$$-B^{-1}A \xrightarrow{\Gamma^i} -A \xrightarrow{\tau_A} 0 \xrightarrow{\Delta} \infty \xrightarrow{\tau_{B^{-1}D}} \infty \quad \text{and}$$

$$\infty \xrightarrow{\Gamma^i} \infty \xrightarrow{\tau_A} \infty \xrightarrow{\Delta} 0 \xrightarrow{\tau_{B^{-1}D}} B^{-1}D;$$

thus ∞ has a unique image and pre-image. This proves (i).

To prove (ii) we note that any element of G is given by the matrix

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

$$M = \begin{pmatrix} AC \\ BD \end{pmatrix},$$

with the understanding that $\lambda M(\lambda \in F, \lambda \neq 0)$ gives the same element as M does. Also, we find by easy calculation that if $g, g_1 \in G$ are given by M, M_1 respectively, then gg_1 is given by MM_1. This establishes an isomorphism between G and $PGL(2, q^3)$.

(iii) It is easy to show that $\Delta\Sigma$, $\Gamma\Sigma$, and $\tau_R\Sigma$ all have the form

$$X \to (A + BX^q)^{-1}(C + DX^q),$$

which is also the form of $\Sigma\Delta$, $\Sigma\Gamma$, and $\Sigma\tau_R$. Therefore Σ normalizes G. A complete set of coset representatives of G in $\bar{G}$ is $\{1, \Sigma, \Sigma^2\}$, so that G has index 3 in $\bar{G}$.

Using the nomenclature for Möbius transformations, we call G the group of *homographies* in $\bar{\mathscr{A}}$, and $\bar{G} - G$ the set of *antihomographies* [**2**, pp. 145-147]. If $q = p^e$ with $e > 1$, it would be possible, by adjoining the collineation induced by the automorphism $X \to X^p$, to get an even larger group of transformations on $\bar{\mathscr{A}}$, but this generalization does not seem to enhance our study. Indeed, even the antihomographies are less important to us than the homographies; for this reason we concentrate on G rather than $\bar{G}$ in subsequent sections.

As a useful observation, we have

COROLLARY 3.1. *Any collineation in G fixes ∞ and has the form $X \to C + DX$.*

4. The surfaces $\mathscr{S}(\theta, K, L, \phi)$. As an important generalization of the surfaces in $\mathscr{A}$ arising from the norm, trace, and bitrace functions, we introduce the surface

$$\mathscr{S} = \mathscr{S}(\theta, K, L, \phi),$$

where $\theta, \phi \in F$ and $K, L \in K$ (θ, ϕ, K, L not all 0). (No confusion should arise by using the same symbol K both for the field K and for an element of K.) $\mathscr{S}$ is the set of points in $\bar{\mathscr{A}}$ corresponding to solutions of the equation

$$\theta X^{1+q+q^2} + (KX^{1+q} + K^q X^{q+q^2} + K^{q^2} X^{q^2+1}) + (LX + L^q X^q + L^{q^2} X^{q^2}) + \phi = 0. \tag{4.1}$$

Note that if $\lambda \in F, \lambda \neq 0$, then

$$\mathscr{S}(\lambda\theta, \lambda K, \lambda L, \lambda\phi) = \mathscr{S}(\theta, K, L, \phi).$$

Similar calculations to those in the proof of Theorem 2.1 yield the proof of

THEOREM 4.1. *If $\theta \neq 0$ then $\mathscr{S}$ is a cubic surface in $\mathscr{A}$. If $\theta = 0$, $k \neq 0$, then $\mathscr{S}$ is a quadric surface. If $\theta = K = 0$, $L \neq 0$, then $\mathscr{S}$ is a plane.*

The importance of the surfaces $\{\mathscr{S}\}$ is that they are invariants under $\bar{G}$, and thus are basic to the geometry:

THEOREM 4.2. *The group $\bar{G}$ of homographies and antihomographies preserves the class of surfaces $\{\mathscr{S}\}$.*

Proof. We need only to show that the generators of $\bar{G}$:Σ, Γ, τ_R $(R \in F)$, and Δ, take $\mathscr{S} = \mathscr{S}(\theta, K, L, \phi)$ onto some surface

$$\mathscr{S}' = \mathscr{S}(\theta', K', L', \phi').$$

This is a matter of straightforward calculation, which is included here for future reference since similar calculations are often needed later:

(i) Under $\Sigma: X \to X^q$,

$$\begin{aligned}\phi X^{1+q+q^2} &+ (KX^{1+q} + K^q X^{q+q^2} + K^{q^2} X^{q^2+1}) \\ &+ (LX + L^q X^q + L^{q^2} X^{q^2}) + \phi = 0 \\ &\to \theta(X^{q^2})^{1+q+q^2} + [K(X^{q^2})^{1+q} + \dots] \\ &+ [L(X^{q^2}) + \dots] + \phi = 0,\end{aligned}$$

i.e.,

$$\theta X^{1+q+q^2} + (K^q X^{1+q} + \dots) + (L^q X + \dots) + \phi = 0.$$

Thus

$$\mathscr{S}(\theta, K, L, \phi) \xrightarrow{\Sigma} \mathscr{S}(\theta, K^q, L^q, \phi). \tag{4.2}$$

(ii) Under $\Gamma^i: X \to W^i X$,

$$\begin{aligned}\theta X^{1+q+q^2} &+ (KX^{1+q} + \dots) + (LX + \dots) + \phi = 0 \\ &\to \theta(W^{-i}X)^{1+q+q^2} + [K(W^{-i}X)^{1+q} + \dots] \\ &+ [L(W^{-i}X) + \dots] + \phi = 0,\end{aligned}$$

i.e.,

$$\begin{aligned}\theta X^{1+q+q^2} &+ (KW^{iq^2} X^{1+q} + \dots) + (LW^{i(q+q^2)} X + \dots) \\ &+ \phi W^{i(1+q+q^2)} = 0.\end{aligned}$$

Thus

$$\mathscr{S}(\theta, K, L, \phi) \xrightarrow{\Gamma^i} \mathscr{S}(\theta, KW^{iq^2}, LW^{i(q+q^2)}, \phi W^{i(1+q+q^2)}). \tag{4.3}$$

(iii) Under $\tau_R: X \to R + X$,

$$\begin{aligned}\theta X^{1+q+q^2} &+ (KX^{1+q} + \dots) + (LX + \dots) + \phi = 0 \\ &\to \theta(X - R)^{1+q+q^2} + [K(X - R)^{1+q} + \dots]\end{aligned}$$

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

$$+ [L(X - R) + \dots] + \phi = 0,$$

i.e.,

$$\theta X^{1+q+q^2} + [(K - \theta R^{q^2})X^{1+q} + \dots] + [(L + \theta R^{q+q^2} - KR^q - K^{q^2}R^{q^2})X + \dots] + \phi - \theta R^{1+q+q^2} + (KR^{1+q} + \dots) - (LR + \dots).$$

Thus

$$(4.4)\quad \mathscr{S}(\theta, K, L, \phi) \xrightarrow{\tau_R} \mathscr{S}(\theta, K - \theta R^{q^2}, L + \theta R^{q+q^2} - KR^q - K^{q^2}R^{q^2}, \phi - \theta R^{1+q+q^2} + T(KR^{1+q}) - T(LR)).$$

(iv) Under $\Delta: X \to X^{-1}$,

$$\theta X^{1+q+q^2} + (KX^{1+q} + \dots) + (LX + \dots) + \phi = 0 \to \theta X^{-1-q-q^2} + (KX^{-1-q} + \dots) + (LX^{-1} + \dots) + \phi = 0,$$

i.e.,

$$\theta + (KX^{q^2} + \dots) + (LX^{q+q^2} + \dots) + \phi X^{1+q+q^2} = 0.$$

Thus

$$(4.5)\quad \mathscr{S}(\theta, K, L, \phi) \xrightarrow{\Delta} \mathscr{S}(\phi, L^{q^2}, K^q, \theta).$$

Among the four types of transformations, the effect of Δ is the most interesting. For whereas Σ, Γ, and τ_R preserve subclasses of cubics, quadrics and planes, the inversion Δ does not necessarily do so. For example, Δ carries the cubic $\mathscr{S}(1, K, L, 0)$ $(K \neq 0)$ onto $\mathscr{S}(0, L^{q^2}, K^q, 1)$, which is either a plane or a quadric, depending on whether or not $L = 0$.

Since $\bar{G}$ is a permutation group on the surfaces $\{\mathscr{S}\}$, it is pertinent to determine the number and nature of orbits involved. We shall say that two surfaces are *equivalent* if they belong to the same orbit under the action of $\bar{G}$. Noting that $S(1, 0, 0, 0)$ is the single point $\{0\}$ and that $\bar{G}$ is transitive on the $q^3 + 1$ points of $\mathscr{A}$, we see that one orbit consists of these points (including ∞); we may call this the *trivial* orbit. There are at least two other orbits, since there must be at least one containing planes, which have $q^2 + 1$ points (including ∞), and another containing $\mathscr{S}(1, 0, 0, 1)$, which has $q^2 + q + 1$ points. We shall find that there are in fact four orbits (Theorem 5.5). As a first step towards this goal, we prove

LEMMA 4.1. *Any surface $\mathscr{S}(\theta, K, L, \phi)$ which contains more than a single point is equivalent to a quadric surface or to a plane.*

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

Proof. Let $\mathscr{S}$ be a surface containing more than a single point, and let $\mathscr{A}$ be a point of $\mathscr{S}$. Under $\tau - A$, $\mathscr{S} \to \mathscr{S}'$ where $\mathscr{S}' \ni 0$, and therefore

$$\mathscr{S}' = \mathscr{S}(\theta, K, L, 0) \quad \text{for some } \theta, K, L.$$

Since $\mathscr{S}'$ contains more than one point, K and L are not both $= 0$. Under Δ,

$$\mathscr{S}' \to \mathscr{S}(0, L^{q^2}, K^q, \theta)$$

(cf. (4.5)), which is either a quadric surface or a plane (Theorem 4.1).

LEMMA 4.2. *Every plane in $\mathscr{A}$ is a surface $\mathscr{S}(0, 0, L, \phi)$ for some L, ϕ. Any two planes are equivalent.*

Proof. A plane Π through 0 is determined by 0 and two other points A and $B \neq \lambda A$. Π then is the set of points $\{\alpha A + \beta B\}$ $(\alpha, \beta \in F)$. Consider the equations

$$AZ + A^q Z^q + A^{q^2} Z^{q^2} = 0 \tag{4.6}$$

$$BZ + B^q Z^q + B^{q^2} X^{q^2} = 0. \tag{4.7}$$

By Theorem 4.1, the above are equations of planes through 0, which therefore contain a common line (also through 0). Thus there is an element $L \neq 0$ of K which is a solution to equations (4.6) and (4.7); the equation

$$LX + L^q X^q + L^{q^2} Z^{q^2} = 0,$$

being satisfied by all elements of the set $\{\alpha A + \beta B\}$, is the equation of Π. Therefore Π is the surface $\mathscr{S}(0, 0, L, 0)$.

If Π' is a plane not through 0, it is parallel to some plane Π through 0 and hence there is a translation τR taking Π onto Π'. If Π is $\mathscr{S}(0, 0, L, 0)$, then from (4.4), Π' is $\mathscr{S}(0, 0, L, \phi)$, where $\phi = -T(LR)$.

From (4.3) we see that

$$\mathscr{S}(0, 0, 1, 0) \xrightarrow{\Gamma} \mathscr{S}(0, 0, W^{-1}, 0);$$

therefore $\langle \Gamma \rangle$ is transitive on planes through 0. (By a slightly more detailed argument it can also be shown that $\langle \Gamma \rangle$ is sharply transitive on the $q^3 - 1$ planes not through 0.) Thus, by virtue of $\langle \Gamma \rangle$ and appropriate translations, any two planes are equivalent.

COROLLARY 4.2. *Given $L \in K$, $(L \neq 0)$, and $\phi \in F$, there are exactly q^2 elements $X \in K$ such that*

$$LX + L^q X^q + L^{q^2} X^{q^2} + \phi = 0.$$

Proof. The q^2 elements are the q^2 points of $\mathscr{A}$ on the plane $\mathscr{S}(0, 0, L, \phi)$.

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

While Lemma 4.2 assures us that all planes lie in one orbit, there are other surfaces in that orbit. For example the orbit also contains $\mathscr{S}(0, 1, 0, 0)$, the inverse of $\mathscr{S}(0, 0, 1, 0)$. We shall see in Theorem 5.2 that $\mathscr{S}(0, 1, 0, 0)$ is a non-degenerate quadric, and therefore is not a plane.

Since $\mathscr{S}(0, 1, 0, 0)$ is a quadric (Theorem 2.1), we can strengthen Lemma 4.1 to

LEMMA 4.1′. *Every orbit that consists of surfaces having more than one point contains a quadric surface.*

Thus we need only to analyse the quadrics $\mathscr{S}(0, K, L, \phi)$ $(K \neq 0)$ in order to determine the orbits of $\{\mathscr{S}\}$ under $\bar{G}$.

5. Analysis of the quadrics. In this section we think of surfaces $\mathscr{S}(0, K, L, \phi)$ as being in the affine space $\mathscr{A}$, rather than in $\bar{\mathscr{A}}$. We seek canonical forms for the quadrics; as a first step, we prove:

THEOREM 5.1. *Any quadric* $\mathscr{Q} = \mathscr{S}(0, K, L, \phi)$ $(K \neq 0)$ *is equivalent to one of the following*:

(a) *For q odd*: $\mathscr{Q}_0 = \mathscr{S}(0, 1, 0, 0), \mathscr{Q}_1 = \mathscr{S}(0, 1, 0, 1)$, *or* $\mathscr{Q}_\nu = \mathscr{S}(0, 1, 0, \nu)$, *where* ν *is a given non-square in F.*

(b) *For q even*: $\mathscr{Q}_0 = \mathscr{S}(0, 1, 0, 0)$, $\bar{\mathscr{Q}}_1 = \mathscr{S}(0, 1, 1, 0)$, *or* $\bar{\mathscr{Q}}_\sigma = \mathscr{S}(0, 1, 1, \sigma)$, *where* σ *is a given element of F with the property that the equation* $x^2 + x + \sigma = 0$ *is irreducible over F.*

Proof. Since $\langle \Gamma \rangle$ is transitive on all points $\neq 0$ of $\mathscr{A}$, there is an integer i such that

$$1 \xrightarrow{\Gamma^i} K^{-q}.$$

Thus $W^i = K^{-q}$, $W^{iq^2} = K^{-1}$ and

$$\mathscr{S}(0, K, L, \phi) \xrightarrow{\Gamma^i} \mathscr{S}(0, 1, L_1, \phi_1)$$

for some L_1, ϕ_1 (cf (4.3)). Also (from 4.4)),

$$\mathscr{S}(0, 1, L_1, \phi_1) \xrightarrow{\tau_A} \mathscr{S}(0, 1, L_1 - A^q - A^{q^2}, \phi_1 + B(A) - T(L_1 A)),$$

where A is any point of $\mathscr{A}$. Now suppose that

$$A^q + A^{q^2} = A_1^q + A_1^{q^2} \quad \text{for some } A_1 \in \mathscr{A}.$$

Then

$$A_1^q - A^q = -(A_1^{q^2} - A^{q^2}),$$

from which it follows that

$$(A_1 - A) = -(A_1 - A)^q.$$

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

Thus either $A_1 = A$ or else $A_1 - A = Z \neq 0$ where $Z^{q-1} = -1$. In the latter case,

$$1 = Z^{q^3-1} = Z^{(q-1)(q^2+q+1)} = -1,$$

and so F is of characteristic 2, i.e., q is even. We deduce that if q is odd, then $A^q + A^{q^2}$ assumes different values for different A; in particular there is one value of A such that

$$A^q + A^{q^2} = L_1,$$

and therefore

$$\mathscr{S}(0, 1, L_1, \phi_1) \overset{\tau_A}{\to} \mathscr{S}(0, 1, 0, \beta) \quad \text{for some } \beta \in F.$$

On the other hand, if q is even then

$$(A + \mu)^q + (A + \mu)^{q^2} = A^q + A^{q^2} \quad \text{for all } \mu \in F,$$

and so $A^q + A^{q^2}$ assumes only q^2 distinct values. Moreover,

$$A_1^q + A_1^{q^2} + \lambda_1 = A^q + A^{q^2} + \lambda$$

implies

$$(A_1 + A)^{q^2} + (A_1 + A)^q = \lambda_1 + \lambda = (A_1 + A) + (A_1 + A)^{q^2},$$

which implies $(A_1 + A)^q = (A_1 + A)$. Hence

$$\lambda_1 + \lambda = (A_1 + A) + (A_1 + A) = 0,$$

and $\lambda_1 = \lambda$. Thus to every $L_1 \in K$, there exists $A \in K$ and $\lambda \in F$ such that

$$L_1 = A^q + A^{q^2} + \lambda;$$

therefore

$$\mathscr{S}(0, 1, L_1, \phi_1) \overset{\tau_A}{\to} \mathscr{S}(0, 1, \lambda, \beta) \quad \text{for some } \beta \in F.$$

To finish the proof we separate into two cases:

(a) q odd. Then $\mathscr{Q}$ is equivalent to $\mathscr{S}(0, 1, 0, \beta)$ ($\beta \in F$). Now

$$W^{q^2+q+1} = \epsilon,$$

a primitive element of F. Thus

$$\mathscr{S}(0, 1, 0, \beta) \xrightarrow{\Gamma^{q^2+q+1}} \mathscr{S}(0, \epsilon, 0, \beta\epsilon^3)$$

(cf (4.3))

$$= \mathscr{S}(0, 1, 0, \beta\epsilon^2).$$

It follows that $\mathscr{S}(0, 1, 0, \epsilon^{2i})$ and $S(0, 1, 0, \nu\epsilon^{2i})$ are equivalent to

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

$S(0, 1, 0, 1)$ and $S(0, 1, 0, \nu)$ respectively.

(b) q even. Then $\mathscr{Q}$ is equivalent to $S(0, 1, \lambda, \beta)$ ($\lambda, \beta \in F$). As in (a),

$$\epsilon = W^{q^2+q+1} \quad \text{and}$$

$$\mathscr{S}(0, 1, \lambda, \beta) \xrightarrow{\Gamma^{q^2+q+1}} \mathscr{S}(0, \epsilon, \lambda\epsilon^2, \beta\epsilon^3) = \mathscr{S}(0, 1, \lambda\epsilon, \beta\epsilon^2).$$

It follows that if $\lambda \neq 0$, then $\mathscr{S}(0, 1, \lambda, \beta)$ is equivalent to $\mathscr{S}(0, 1, 1, \beta_1)$ for some $\beta_1 \in F$. Since q is even, every element of F is a square. Therefore

$$\mathscr{S}(0, 1, 0, \beta) \xrightarrow{\tau_{\sqrt{\beta}}} \mathscr{S}(0, 1, 0, 0)$$

(cf (4.4)), and so $\mathscr{S}(0, 1, 0, \beta)$ is equivalent to $\mathscr{S}(0, 1, 0, 0)$. Finally,

$$\mathscr{S}(0, 1, 1, \beta_1) \xrightarrow{\tau_\rho} \mathscr{S}(0, 1, 1, \beta_1 + \rho^2 + \rho),$$

$\rho_1^2 + \rho_1 = \rho^2 + \rho$ if and only if $\rho_1 = \rho$ or $\rho + 1$. Thus $\rho^2 + \rho$ assumes $q/2$ distinct values for the q values of ρ. So given β_1, there exists $\rho \in F$ such that $\rho^2 + \rho + \beta_1 = 0$ or σ, where σ is any element of F which cannot be expressed in the form $\rho^2 + \rho$. Hence $\beta_1 = \rho^2 + \rho$ or else $\beta_1 = \rho^2 + \rho + \sigma$, and $\mathscr{S}(0, 1, 1, \beta_1)$ is equivalent to $\mathscr{S}(0, 1, 1, 0)$ or $\mathscr{S}(0, 1, 1, \sigma)$. This completes the proof of Theorem 5.1.

We now investigate $\mathscr{Q}_\beta = \mathscr{S}(0, 1, 0, \beta)$. Before doing so, it is necessary to review the types of quadric surfaces possible in $\mathscr{A} = AG(3, q)$, and this is best done by considering $\mathscr{P} \cong PG(3, q)$, the projective extension of $\mathscr{A}$. To obtain $\mathscr{P}$ from $\mathscr{A}$, we adjoin to each parallel class of lines in $\mathscr{A}$ a unique ideal point, stipulating that the ideal points associated with any parallel class of planes are collinear (in an ideal line) and that all ideal points and lines lie in a single ideal plane, which we denote by π_∞. Thus

$$\mathscr{P} = \mathscr{A} \cup \pi_\infty \quad \text{and} \quad \pi_\infty \cong PG(2, q).$$

Any quadric surface $\bar{\mathscr{Q}}$ in $\mathscr{P}$ is one of four types, namely:

(a) Ruled quadrics. A ruled quadric $\bar{\mathscr{Q}}$ consists of a regulus $\mathscr{R}$ of $q + 1$ mutually skew lines, and an opposite regulus $\mathscr{R}'$ with the property that every line of $\mathscr{R}'$ intersects every line of $\mathscr{R}$. $\bar{\mathscr{Q}}$ thus contains $(q + 1)^2$ points and $2(q + 1)$ lines. Any plane of $\mathscr{P}$ intersects $\bar{\mathscr{Q}}$, either in two lines (one from each regulus) or in a non-degenerate conic [**4**, p. 221].

(b) Non-ruled quadrics. In this case, $\bar{\mathscr{Q}}$ is an ovoid [**4**, p. 48], and contains $q^2 + 1$ points. Any plane of $\mathscr{P}$ is either a tangent to $\bar{\mathscr{Q}}$ or a secant.

(c) Cones. Here $\bar{\mathscr{Q}}$ consists of $q + 1$ lines, called *generators*, concurrent in a point A, called the *apex* of $\bar{\mathscr{Q}}$. Thus

$$|\bar{\mathscr{Q}}| = q(q + 1) + 1 = q^2 + q + 1.$$

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

Any plane of $\mathscr{P}$ meets $\bar{\mathscr{Q}}$ in A alone, in one generator, two generators, or in a conic.

(d) Degenerate quadrics. In this case, $\bar{\mathscr{Q}}$ is either two distinct planes or two coincident planes; therefore

$$|\bar{\mathscr{Q}}| = 2(q^2 + q + 1) \quad \text{or} \quad q^2 + q + 1$$

respectively.

In $\mathscr{A} = \mathscr{P} \backslash \pi_\infty$, $\mathscr{Q} = \bar{\mathscr{Q}} - (\bar{\mathscr{Q}} \cap \pi_\infty)$ has several forms; we are interested in the following:

(a) Ruled hyperboloids. Here, $\bar{\mathscr{Q}}$ is a ruled quadric, and $\bar{\mathscr{Q}} \cap \pi_\infty$ is a conic, so that $\mathscr{Q}$ contains $2(q + 1)$ lines, and

$$|\mathscr{Q}| = (q + 1)^2 - (q + 1) = q^2 + q.$$

(b) Non-ruled hyperboloids. In this case, $\bar{\mathscr{Q}}$ is a non-ruled quadric, $\bar{\mathscr{Q}} \cap \pi_\infty$ is a conic, and

$$|\mathscr{Q}| = q^2 + 1 - (q + 1) = q^2 - q.$$

(c) (i) Cones. $\bar{\mathscr{Q}}$ is a cone whose apex A is not on π_∞.

$$|\mathscr{Q}| = q^2 + q + 1 - (q + 1) = q^2.$$

(ii) Cylinders. Again, $\bar{\mathscr{Q}}$ is a cone, but now $A \in \pi_\infty$. Thus $\mathscr{Q}$ consists of $q + 1$, q, or $q - 1$ parallel lines, depending on whether π_∞ meets $\bar{\mathscr{Q}}$ in A alone, in one, or in two generators respectively. Following common nomenclature, we call $\mathscr{Q}$ an elliptic, parabolic, or hyperbolic cylinder respectively. Also, $|\mathscr{Q}| = q^2 + q$, q^2, or $q^2 - q$ respectively.

(d) One or two planes. In this case, $|\mathscr{Q}| = q^2$, $2q^2$, or $2q^2 - q$.

THEOREM 5.2. *$\mathscr{Q} = \mathscr{S}(0, K, 0, 0)$ $(K \neq 0)$ is a cone with apex 0.*

Proof. Under Δ,

$$\mathscr{Q} \to \mathscr{S}(0, 0, K^q, 0) = \pi,$$

a plane through 0. Therefore $|\mathscr{Q}| = |\pi| = q^2$. Moreover, $Z \in \mathscr{Q}$ if and only if $\lambda Z \in \mathscr{Q}$ $(\lambda \in F)$, and so $\mathscr{Q}$ consists of $q + 1$ lines through 0. Hence $\mathscr{Q}$ is either a cone with apex 0 or a plane through 0.

Assume $\mathscr{Q}$ is a plane through 0. Since $\bar{G}$ is transitive on the planes through 0 (Lemma 4.2), we may assume without loss of generality that $\mathscr{Q} \ni 1$ and W. Now

$$1, W \xrightarrow{\Delta} 1, W^{-1},$$

and so $\pi = \{\lambda + \mu W^{-1}\}$ $(\lambda, \mu \in F)$. Therefore

$$\mathscr{Q} = \{(\lambda + \mu W^{-1})^{-1}\},$$

and in particular

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

$$\mathcal{Q} \ni \{1, W, (I + W^{-1})^{-1}\}.$$

Since $\mathcal{Q}$ is assumed to be a plane through 0, there exist $\alpha, \beta \in F$ such that

$$(1 + W^{-1})^{-1} = \alpha + \beta W.$$

Re-arranging, we have the equation

$$\beta W^2 + (\alpha + \beta - 1)W + \alpha = 0. \tag{5.1}$$

But W is a primitive root of K; therefore W has period $q^3 - 1$, from which it follows that 1, W, W^2, as vectors, are linearly independent. Referring to (5.1), this implies that $\alpha = \beta = 0$, $\alpha + \beta = 1$, yielding the inconsistency $0 = 1$. Therefore $\mathcal{Q}$ cannot be a plane through 0.

We have from Theorem 5.2 that $\mathcal{Q}_0 = \mathcal{S}(0, 1, 0, 0)$ is a cone with apex 0. We now investigate $\mathcal{Q}_\beta = \mathcal{S}(0, 1, 0, \beta)$ for any value of $\beta \in F$.

THEOREM 5.3. (a) *If q is odd and $\beta \neq 0$, then $\mathcal{Q}_\beta$ is either a ruled or a non-ruled hyperboloid, depending on whether $|\mathcal{Q}_\beta| = q^2 + q$ or $q^2 - q$.*

(b) *If q is even, then $\mathcal{Q}_\beta$ is a cone with apex 0.*

Proof. (a) By Lemma 4.2 and Theorem 5.1 there is some $\beta_1 \neq 0$ such that $\mathcal{Q}_{\beta_1}$ is equivalent to $\mathcal{S}(1, 0, 0, 1)$, which, as noted in Section 2, contains $q^2 + q + 1$ points. Hence

$$|\mathcal{Q}_{\beta_1}| = q^2 + q.$$

Also, the $(q - 1)/2$ quadrics $\mathcal{Q}_{\lambda^2\beta_1} (\lambda \in F, \lambda \neq 0)$ are equivalent to $\mathcal{Q}_{\beta_1}$, while $\mathcal{Q}_{\lambda^2\beta_1\nu}$ is equivalent to $\mathcal{Q}_{\beta_1\nu}$. Observing that

$$\mathcal{Q}_\beta \cap \mathcal{Q}_{\beta'} = \emptyset \quad \text{for } \beta' \neq \beta,$$

and letting $n = |\mathcal{Q}_{\beta_1\nu}|$, we count the total number of points in $\mathcal{A}$:

$$q^3 = |\mathcal{Q}_0| + \frac{q - 1}{2}[\,|\mathcal{Q}_{\beta_1}| + |\mathcal{Q}_{\beta_1\nu}|\,]$$

$$= q^2 + \frac{q - 1}{2}(q^2 + q + n).$$

Solving this equation, we have $n = q^2 - q$. We now have

$$|\mathcal{Q}_{\beta_1}| = q^2 + q \quad \text{and} \quad |\mathcal{Q}_{\beta_1\nu}| = q^2 - q.$$

From our analysis of quadrics in $\mathcal{A}$, it follows that $\mathcal{Q}_{\beta_1}$ is either a ruled hyperboloid or an elliptic cylinder, while $\mathcal{Q}_{\beta_1\nu}$ is either a non-ruled hyperboloid or a hyperbolic cylinder. Suppose that $\mathcal{Q}_\beta (\beta = \beta_1 \text{ or } \beta_1\nu)$ is a cylinder. By means of

$$\Gamma^i : X \to W^i X \quad \text{for some } i,$$

we take $\mathcal{Q}_\beta$ onto some cylinder $\mathcal{Q}'_\beta$, whose generators are parallel to the line

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

$0I$, where I is the point 1. $\mathcal{Q}'_\beta$ has equation

$$KX^{1+q} + K^qX^{q+q^2} + K^{q^2}X^{q^2+1} + \gamma = 0,$$

where

$$K = W^{iq^2} \quad \text{and} \quad \gamma = \beta W^{i(1+q+q^2)}.$$

Since the generators of $\mathcal{Q}'_\beta$ are parallel to $0I$, $Z \in \mathcal{Q}'_\beta$ if and only if

$$\lambda + Z \in \mathcal{Q}'_\beta \quad \text{for all } \lambda \in F.$$

Therefore the equation

$$\begin{aligned} 0 &= K(\lambda + Z)^{1+q} + \ldots + \gamma \\ &= T(K)\lambda^2 + [(K + K^{q^2})Z + \ldots.]\lambda + (KZ^{1+q} + \ldots) + \gamma \\ &= \{T(K)\lambda + [(K + K^{q^2})Z + (K^q + K)Z^q + (K^{q^2} + K^q)Z]\}\lambda \end{aligned}$$

is true for all λ, and so

$$T(K) = (K + K^{q^2})Z + \ldots = 0.$$

In other words, $T(K) = 0$ and Z lies in the plane

$$\pi = \mathcal{S}(0, 0, K + K^{q^2}, 0).$$

Therefore every generator of $\mathcal{Q}'_\beta$ lies in π. But π can contain at most two generators of the quadric cylinder $\mathcal{Q}'_\beta$. It follows that

$$q^2 - q \leqq |\mathcal{Q}_\beta| = |\mathcal{Q}'_\beta| \leqq 2q,$$

from which we have $q \leqq 3$. Therefore, if $q > 3$, $\mathcal{Q}_\beta$ is not a cylinder. By direct computation in the case $q = 3$ we can show that here too $\mathcal{Q}_\beta$ is not a cylinder. This completes the proof of (a).

To prove (b) we simply note, as in the proof of Theorem 5.1, that

$$\mathcal{Q}_\beta \xrightarrow{\tau_{\sqrt{\beta}}} \mathcal{Q}_0,$$

and invoke Theorem 5.2.

THEOREM 5.4. *If q is even, then $\bar{\mathcal{Q}}_\beta = \mathcal{S}(0, 1, 1, \beta)$ is either a ruled or a non-ruled hyperboloid, depending on whether $|\bar{\mathcal{Q}}_\beta| = q^2 + q$ or $q^2 - q$.*

Proof. Assume $q > 2$. Since

$$S(1, 0, 0, 1) \xrightarrow{\tau_1} S(1, 1, 1, 0) \xrightarrow{\Delta} \mathcal{S}(0, 1, 1, 1) = \bar{\mathcal{Q}}_1,$$

$|\bar{\mathcal{Q}}_1| = q^2 + q$. Let $\bar{\mathcal{Q}}_\theta$ belong to the other orbit to $\bar{\mathcal{Q}}_1$ as determined by Theorem 5.1, and let $|\bar{\mathcal{Q}}_\theta| = n$. Since the quadrics $S(0, 1, 1, \beta)$ break up into two orbits, and since

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

$$\mathscr{S}(0, 1, 1, \beta) \cup \mathscr{S}(0, 1, 1, \beta') = \emptyset \quad \text{for } \beta \neq \beta',$$

we count points of $\mathscr{A}$ to get the equation

$$q^3 = \frac{q}{2}[\,|\bar{\mathscr{Q}}_1| + |\bar{\mathscr{Q}}_\theta|\,] = \frac{q}{2}(q^2 + q + n).$$

Solving, we have $n = q^2 - q$. Turning again to our analysis of the quadrics of $\mathscr{A}$, we find that $\bar{\mathscr{Q}}_1$ is either a ruled hyperboloid or an elliptic cylinder, while $\bar{\mathscr{Q}}_\theta$ is either a non-ruled hyperboloid or a hyperbolic cylinder.

Suppose that $\bar{\mathscr{Q}}_1$ or $\bar{\mathscr{Q}}_\theta$ is a cylinder. By exactly the same argument used in the proof of Theorem 5.3, we conclude that every generator lies in a plane π and that therefore $q \leqq 3$. But $q > 2$ and q is even, so neither $\bar{\mathscr{Q}}_1$ nor $\bar{\mathscr{Q}}_\theta$ can be a cylinder. This completes the proof of Theorem 5.4 for $q > 2$. The case $q = 2$ is verified by direct computation.

As a corollary to Theorems 5.1-5.4, we have

THEOREM 5.5. *In the extended space $\bar{\mathscr{A}} = \mathscr{A} \cup \{\infty\}$, $\bar{G}$ divides the class of surfaces $\mathscr{S}(\theta, K, L, \phi)$ into four orbits, which are characterized by the number N of points in any element of the orbit. The orbits are*:

$O_1 = \{P\}$, *where P is any point of $\bar{\mathscr{A}}$. $N = 1$.*

O_2: $N = q^2 + q + 1$. *O_2 contains a ruled hyperboloid of $\mathscr{A}$.*

O_3: $N = q^2$. *O_3 contains the cone $\mathscr{Q}_0 = \mathscr{S}(0, 1, 0, 0)$ and all planes of $\mathscr{A}$.*

O_4: $N = q^2 - q + 1$. *O_4 contains a non-ruled hyperboloid of $\mathscr{A}$.*

6. Cells in π_∞. A closer examination of the cones of the set $\{\mathscr{S}\}$ in $\mathscr{A}$ leads to the discovery of a set of $q^2 + q + 1$ conics in $\pi_\infty = \mathscr{P} - \mathscr{A}$. Of course $\pi_\infty \cong PG(2, q)$.

Definition. A *cell* of π_∞ is the intersection $\mathscr{C} \cap \pi_\infty$, where $\mathscr{C}$ is a cone of $\{\mathscr{S}\}$.

To be precise, $\mathscr{C}$ is the extension of a cone when $\mathscr{A}$ is projectively extended to $\mathscr{P}$. If $\mathscr{C}$ is any cone of $\{\mathscr{S}\}$, we let $\mathscr{C}$ also denote the cell defined by $\mathscr{C}$.

LEMMA 6.1. *There is a one to one correspondence between the set $\{\mathscr{C}\}$ of cells in π_∞ and the set of cones in $\{\mathscr{S}\}$ with apex 0.*

Proof. Using the translation

$$\tau_{-A}: X \to -A + X,$$

we take a cone with apex A onto a cone with apex 0. Since τ_{-A} fixes π_∞ pointwise, the cell defined by the first cone is identical to the cell defined by the second.

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

THEOREM 6.1. *The set* $\{\mathscr{C}\}$ *of cells in* π_∞ *has the following properties*:
(a) *Any cell is a non-degenerate conic.*
(b) $|\{\mathscr{C}\}| = q^2 + q + 1$.
(c) *Any cell contains* $q + 1$ *points.*
(d) *Every point lies on* $q + 1$ *cells.*
(e) *Any two distinct points lie on one and only one cell.*
(f) *Any two cells are tangent to one another.*

Proof. Since any cell is the intersection of the plane π_∞ with a quadric surface, it must be a conic. By Theorem 5.2, the cell is a non-degenerate conic since it is the intersection of π_∞ with a cone which does not degenerate into a plane.

By Lemma 6.1, any cell is determined by a cone $\mathscr{S}(0, K, 0, 0)$. Under

$$\Delta: X \to X^{-1},$$

$\mathscr{S}(0, K, 0, 0)$ inverts into $\mathscr{S}(0, 0, K^{q^2}, 0)$, which is a plane of $\mathscr{A}$ through 0. Properties (b)-(f) now follow from the well-known properties of lines in π_∞, which of course are the intersections of π_∞ with planes of $\mathscr{P}$ through 0. For example, (f) follows from the fact that any two distinct lines in a projective plane intersect. Since any two planes through 0 have exactly one common line, so also do the two cones which are their inverses; in other words, the two cells defined by these cones share a single point of π_∞.

The subgroups of G and $\bar{G}$ which are collineations in $\mathscr{A}$ induce collineations in π_∞. Thus $\Gamma: X \to WX$ induces a Singer cycle [**4**, p. 34, **5**, **8**] which cyclically permutes points, lines or cells, and $\Sigma: X \to X^q$ induces a collineation of period 3. The inversion Δ in $\mathscr{A}$ induces a bijection Δ in π_∞ which fixes the point 1 and interchanges the points Z and Z^{-1}. Δ is not a collineation; in fact Δ interchanges the set of lines with the set of cells. We shall call Δ an *inversion* of π_∞.

Since π_∞ is exhibited as a cyclic plane [**5**, p. 1080; **8**] and its points are $\{W^i\}$ $(0 \leqq i \leqq q^2 + q)$, the $q + 1$ points $\{W^{i_0}, W^{i_1}, \ldots, W^{i_q}\}$ are collinear only if $\{i_0, i_1, \ldots, i_q\}$ is a perfect difference set (mod $q^2 + q + 1$).

If we apply the inversion Δ to the line represented by the difference set

$$D = \{i_0, i_1, \ldots, i_q\},$$

we get a cell represented by

$$-D = \{-i_0, -i_1, \ldots, -i_q\}.$$

This is the approach of Jungnickel and Vedder [**7**]. Using difference set arguments, several interesting properties of the set of cells can be proved [**7**, pp. 144, 145]. In particular:

THEOREM 6.2. *Any two distinct cells have one and only one common tangent.*

THEOREM 6.3. *Consider the following incidence structure* Π:
(i) *the points of* Π *are the cells of* Π_∞;
(ii) *the lines of* Π *are the lines of* Π_∞;
(iii) *a point* $\mathscr{C}$ *and a line* l *are incident if and only if* l *is a tangent to* $\mathscr{C}$;
Then Π *is a finite projective plane isomorphic to* Π_∞. *Moreover,* Δ *is a polarity in* Π.

Since the above results are either explicitly proved in [7] or easily deduced therefrom, we offer no proofs here.

7. Cubic surfaces $\mathscr{S}(\theta, K, L, \phi)$. It remains only to consider the cubic surfaces $\mathscr{S}(\theta, K, L, \phi)$ $(\theta \neq 0)$. Since

$$\mathscr{S}(\theta, K, L, \phi) = \mathscr{S}(1, \theta^{-1}K, \theta^{-1}L, \theta^{-1}\phi),$$

we shall henceforth take $\theta = 1$ and consider $\mathscr{S} = \mathscr{S}(1, K, L, \phi)$. Excluding the trivial case $\mathscr{S} = \mathscr{S}(1, 0, 0, 0) = \{0\}$ and its images under $\bar{G}$, we have from Theorem 5.5 that $\mathscr{S}$ is one of three types, according to the orbit to which it belongs:

I. $\mathscr{S} \in O_2 \cdot |\mathscr{S}| = q^2 + q + 1$
II. $\mathscr{S} \in O_3 \cdot |\mathscr{S}| = q^2 + 1$
III. $\mathscr{S} \in O_4 \cdot |\mathscr{S}| = q^2 - q + 1.$

It is easy to see that cubics of each type exist, since an example is obtained by inverting any quadric which does not contain 0. It is also easy to see that $\mathscr{S}$ does not contain ∞, since

$$\mathscr{S}^\Delta = \mathscr{S}(\phi, L^{q^2}, K^q, 1)$$

does not contain 0. Our particular interest in this study of $\mathscr{S}$ will be the intersection of $\mathscr{S}$ with lines and planes of $\mathscr{A}$.

Definition. An *exterior* line (plane) to $\mathscr{S}$ is a line (plane) that contains no point of $\mathscr{S}$.

It will be helpful to have simpler forms for the cubic surfaces $\mathscr{S}$:

LEMMA 7.1. *Any cubic* $\mathscr{S} = \mathscr{S}(1, K, L, \phi)$ *is equivalent under collineations of* $\mathscr{A}$ *to* $\mathscr{S}(1, 0, \rho, \sigma)$ *for some* $\rho, \sigma \in F$.

Proof.

$$\mathscr{S}(1, K, L, \phi) \xrightarrow{\tau_K q} \mathscr{S}(1, 0, L_1, \phi_1) \quad \text{for some } L_1, \phi_1$$

(cf. (4.4)). Now $L_1 = \lambda W^i$ for some $\lambda \in F$, $W^i \in K$, and

$$\mathscr{S}(1, 0, L_1, \phi_1) \xrightarrow{\Gamma^i} S(1, 0, \lambda W^{i(1+q+q^2)}, \phi_1 W^{i(1+q+q^2)})$$

(cf (4.3))

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

$$= S(1, 0, \rho, \sigma) \quad \text{for some } \rho, \sigma \in F.$$

By application of appropriate elements of $\langle \Gamma \rangle$ we can get even simpler forms for $\mathscr{S}$. Thus if

$$\sigma = \epsilon^j = W^{j(1+q+q^2)},$$

then

$$\mathscr{S}(1, 0, 0, \sigma) \overset{\Gamma^{-j}}{\rightarrow} \mathscr{S}(1, 0, 0, 1),$$

and so $\mathscr{S}(1, 0, 0, 1)$ is a canonical form for $\mathscr{S}(1, 0, 0, \sigma)$ $(\sigma \neq 0)$. To obtain the three canonical forms for $\mathscr{S}$ would require a more thorough analysis, involving the use of Δ. However, since we are interested in the relationship of $\mathscr{S}$ to lines and planes, which are not preserved by Δ, it is inappropriate to restrict attention to canonical forms.

We first consider $\mathscr{S}(1, 0, 0, \sigma)$ $(\sigma \neq 0)$, which we denote by $\mathscr{S}_\sigma$. Clearly,

$$\mathscr{S}_\sigma = \{X | N(X) = -\sigma\}.$$

Since K has $q^2 + q + 1$ elements of norm $-\sigma$, $\mathscr{S}_\sigma$ is a cubic of type I.

LEMMA 7.2. *Let*

$$\Gamma' = \Gamma^{q-1}: X \rightarrow W^{q-1}X.$$

Then $\langle \Gamma' \rangle$ *is sharply transitive on the points of* $\mathscr{S}_\sigma$.

Proof. Letting $U = W^{q-1}$, we note that

$$N(U) = U^{q^2+q+1} = W^{q^3-1} = 1.$$

Under the action of Γ',

$$X^{1+q+q^2} + \sigma = 0 \rightarrow U^{-(1+q+q^2)}X^{1+q+q^2} + \sigma = 0.$$

Thus Γ' fixes $\mathscr{S}_\sigma$ since $N(U) = 1$. Since

$$|\langle \Gamma' \rangle| = q^2 + q + 1 = |\mathscr{S}_\sigma|,$$

and only the identity fixes a point, $\langle \Gamma' \rangle$ is sharply transitive on $\mathscr{S}_\sigma$.

Since $\mathscr{S}_\sigma$ is a cubic surface, some lines of $\mathscr{A}$ may meet $\mathscr{S}_\sigma$ in three points. Thus if $q \leqq 3$ a line may lie entirely within $\mathscr{S}_\sigma$. However:

LEMMA 7.3. $\mathscr{S}_\sigma$ *contains no line of* $\mathscr{A}$ *if* $q > 3$.

Proof. Any plane intersects $\mathscr{S}_\sigma$ in a cubic curve. A plane cubic curve could consist of 3 distinct lines, but not $n > 3$, since it would then be described in Cartesian coordinates by an equation having n linear factors, and thus be of degree greater than 3.

Now suppose that $\mathscr{S}_\sigma$ contains a line l. Then l contains q points of $\mathscr{S}_\sigma$. Let

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

A be a fixed point of l and let X be any other point of l. Because $\langle \Gamma' \rangle$ is transitive on the points of $\mathscr{S}_\sigma$, there is an element of $\langle \Gamma' \rangle$ taking X into A. However, this element, γ say, does not fix l, since if it did it would also fix the line through 0 parallel to l; in that case γ would be a central dilatation $X \to \lambda X$, which fixes only lines through 0. Since l is assumed to lie on $\mathscr{S}_\sigma$, it cannot contain 0, and therefore is not fixed by γ.

It follows that through A there are q lines which lie on $\mathscr{S}_\sigma$. Since this is true for every point A on l, we have $q(q-1)$ distinct lines lying on $\mathscr{S}_\sigma$, each of which contains one point of l. Counting l, we now have $q^2 - q + 1$ lines lying on $\mathscr{S}_\sigma$, and also lying on the $q+1$ planes through l. Therefore, the number of lines of $\mathscr{S}_\sigma$ lying on one of these planes is at least

$$1 + (q^2 - q)/(q+1) = q - 1 + 2/(q+1).$$

That is, some plane through l contains at least q lines which lie completely in $\mathscr{S}_\sigma$. But no plane can contain more than 3 lines of $\mathscr{S}_\sigma$, so $q \leqq 3$.

Let P be any point of $\mathscr{S}_\sigma$, and let X be any point $\neq P$ of $\mathscr{S}_\sigma$. For $q > 2$ the lines PX are of two different types: some lines contain exactly 3 points of $\mathscr{S}_\sigma$ (counting P), and others contain only two. We say that there are k of the first type and d of the second. Since $\langle \Gamma' \rangle$ is transitive on the points of $\mathscr{S}_\sigma$, k and d are independent of the choice of P.

LEMMA 7.4. *The number of lines which contain at least one point of* $\mathscr{S}_\sigma$ *is*

$$(7.1) \quad (q^2 + q + 1)[(q^2 + q + 2)/2 + k/3].$$

Proof. Given a point P of $\mathscr{S}_\sigma$, the number of ordered pairs (P, X) $(X \in \mathscr{S}_\sigma, X \neq P)$ is $q^2 + q$, or in terms of k and d, $2k + d$. Thus

$$(7.2) \quad 2k + d = q^2 + q.$$

Summing over all points of $\mathscr{S}_\sigma$, the number of lines containing 3 points of $\mathscr{S}_\sigma$ is $(q^2 + q + 1)k/3$, and the number containing 2 is $(q^2 + q + 1)d/2$. The total number of lines containing at least one point of $\mathscr{S}_\sigma$ is therefore

$$(q^2 + q + 1)[k/3 + d/2 + q^2 + q + 1 - k - d].$$

Using (7.2) to substitute for d, and simplifying, we get (7.1).

We wish to show now that every plane of $\mathscr{A}$ contains at least one point of $\mathscr{S}_\sigma$. We begin by investigating planes through 0.

If Z is any point of $\mathscr{A}(Z \neq 0)$, then $\{\lambda Z\}(\lambda \in F)$ is the line OZ. Now

$$N(\lambda Z) = \lambda^3 N(Z).$$

Hence if $q \equiv 1 \pmod 3$, so that F contains all 3 cube roots of unity, OZ contains 5 points of norm $N(Z)$. But if $q \not\equiv 1 \pmod 3$, then OZ contains one and only one point of norm $N(Z)$. In this case, any line through 0

contains exactly one point of $\mathscr{S}_\sigma$; therefore every plane through 0 contains exactly $q + 1$ points of $\mathscr{S}_\sigma$ if $q \not\equiv 1 \pmod 3$.

Now suppose $q \equiv 1 \pmod 3$. As above, F contains all 3 cube roots of unity: ω, ω^2, and 1. Also, any line OZ contains 3 points with norm $N(Z)$, namely Z, ωZ, and $\omega^2 Z$. Moreover,

$$N(\lambda Z)/N(Z) = \lambda^3,$$

from which it follows that the lines through 0 are partitioned into three mutually exclusive classes:

(i) lines each containing 3 points of norm 1,
(ii) lines each containing 3 points of norm ω,
(iii) lines each containing 3 points of norm ω^2.

Let Π be a plane through 0, and let Π contain x, y and z lines of class (i), (ii) and (iii) respectively. Then

$$x + y + z = q + 1. \tag{7.3}$$

LEMMA 7.5. *x, y, z, are all positive integers.*

Proof. Since $q \equiv 1 \pmod 3$, $\langle \Gamma' \rangle$ contains

$$W^{(q^3-1)/3} = \omega.$$

Therefore $\langle \Gamma' \rangle$ partitions both the lines and the planes through 0 into three orbits of length $(q^2 + q + 1)/3$ each. The orbits themselves are permuted by $\Gamma: X \to WX$ since $\langle \Gamma \rangle$ is transitive on lines (and planes) through 0. Consider the plane Π through 0, mentioned above, which contains x, y, and z lines of class (i), (ii), and (iii) respectively. Π lies in one of the three orbits. Now Γ permutes classes (i), (ii) and (iii) as well as orbits, while $\langle \Gamma' \rangle$ is transitive on the planes in any orbit. Therefore, in one orbit the planes each contain $3x$ points of norm 1, in another, $3y$, and in the third $3z$. Let OP be a line through 0 containing (three) points of norm 1. In virtue of the transitivity of $\langle \Gamma' \rangle$ on points of norm 1, OP lies on a plane through 0 containing $3x$ points of norm 1. Moreover, since $\langle \Gamma' \rangle$ contains a collineation that will take any line of Π through 0 containing points of norm 1 onto OP, it follows that there are at least x planes through OP, each of which contains $3x$ points of norm 1. By similar reasoning with respect to y and z, we conclude that the $q + 1$ planes through OP consist of x from one orbit, y from a second, and z from the third.

If we now count the $q^2 + q + 1$ points of norm 1 by observing their incidences with the $q + 1$ planes through OP, we get the equation

$$3 + 3x(x - 1) + 3y(y - 1) + 3z(z - 1) = q^2 + q + 1,$$

which, simplified, is

$$x^2 + y^2 + z^2 - (x + y + z) = (q^2 + q - 2)/3.$$

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

Applying (7.3), we have

$$(7.4)\quad x^2 + y^2 + z^2 = (q^2 + 4q + 1)/3.$$

Equations (7.3) and (7.4) are two simultaneous Diophantine equations, symmetric in x, y, and z. Eliminating z, we have

$$x^2 + y^2 + (q + 1 - x - y)^2 = (q^2 + 4q + 1)/3.$$

Re-arranged, this is

$$(7.5)\quad y^2 - (q + 1 - x)y + x^2 - (q + 1)x + (q^2 + q + 1)/3 = 0.$$

As a quadratic in y, (7.5) has discriminant

$$\begin{aligned} D &= (q + 1 - x)^2 - 4x^2 + 4(q + 1)x - 4(q^2 + q + 1)/3 \\ &= -[9x^2 - 6(q + 1)x + (q - 1)^2]/3 \\ &= -\{[3x - (q + 1)]^2 - 4q\}/3. \end{aligned}$$

Since $D \geqq 0$ for a solution to (7.5),

$$[3x - (q + 1)]^2 \leqq 4q.$$

Thus

$$-2\sqrt{q} \leqq 3x - (q + 1) \leqq 2\sqrt{q},$$

i.e.,

$$(7.6)\quad (\sqrt{q} - 1)^2 \leqq 3x \leqq (\sqrt{q} + 1)^2$$

(cf [**6**, p. 311]). In particular, (7.6) shows that $x > 0$. Since (7.3) and (7.4) are symmetric in x, y, and z, we also have $y > 0$ and $z > 0$, proving Lemma 7.5.

THEOREM 7.1. *Every plane of $\mathscr{A}$ contains at least one point of $\mathscr{S}_\sigma$.*

Proof. If $q \not\equiv 1 \pmod 3$, then every line through 0 contains a point of $\mathscr{S}_\sigma$, and therefore every plane through 0 contains $q + 1$ points of $\mathscr{S}_\sigma$. If $q \equiv 1 \pmod 3$, it is an immediate corollary of Lemma 7.5 that any plane through 0 meets $\mathscr{S}_\sigma$. Thus, regardless of the value of q, every plane through 0 contains at least one point of $\mathscr{S}_\sigma$.

Now suppose that there is a plane π not through 0 and exterior to $\mathscr{S}_\sigma$. Under the action of $\langle \Gamma' \rangle$, which fixes $\mathscr{S}_\sigma$, we get a set S of $q^2 + q + 1$ distinct planes, including π, each of which is exterior to $\mathscr{S}_\sigma$. We count the number of lines which lie on at least one plane of S:

For each $i (2 \leqq i \leqq r \leqq q^2 + q + 1)$ there are $n_i \geqq 0$ lines of π, each of which is the common intersection of i planes of S. Counting multiplicities, the total number of intersections of planes of $S \backslash \pi$ with π is

$$n_2 + 2n_3 + 3n_4 + \ldots + (r - 1)n_r \leqq q^2 + q.$$

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

We note for future reference that

$$\begin{aligned} & n_2/2 + 2n_3/3 + \ldots + (r-1)n_r/r \\ & \leqq [n_2 + 2n_3 + 3n_4 + \ldots + (r-1)n_r]/2 \\ & \leqq (q^2+q)/2. \end{aligned}$$

If a line of π is the common intersection of i planes of S, and if we apply $\langle \Gamma' \rangle$ to this line, we get $q^2 + q + 1$ exterior lines; i of these, including the original line itself, are on π. Hence the total number of lines in $\mathscr{A}$, each of which is the intersection of i planes of S, is

$$(q^2 + q + 1)n_i/i.$$

The total number of lines that lie on at least one plane of S is therefore

$$\begin{aligned} & (q^2+q+1)[n_2/2 + n_3/3 + \ldots + n_r/r + q^2 + q \\ & \qquad - (n_2 + n_3 + \ldots + n_r)] \\ & = (q^2+q+1)[q^2 + q - (n_2/2 + 2n_3/3 \\ & \qquad + \ldots + (r-1)n_r/r)] \\ & \geqq (q^2+q+1)[q^2 + q - (q^2+q)/2] \end{aligned}$$

(by the above note)

$$= (q^2+q+1)(q^2+q)/2.$$

Thus the number of exterior lines to $\mathscr{S}_\sigma$ is at least

$$(q^2+q+1)(q^2+q)/2.$$

But by Lemma 7.4, the number of lines containing at least one point of $\mathscr{S}_\sigma$ is greater than

$$(q^2+q+1)(q^2+q)/2.$$

Therefore the total number of lines in $\mathscr{A}$ is greater than

$$(q^2+q+1)(q^2+q).$$

This is a contradiction; there are only $(q^2+q+1)q^2$ lines in $\mathscr{A}$. Therefore every plane of $\mathscr{A}$ contains at least one point of $\mathscr{S}_\sigma$.

We are now ready to consider the more general surface

$$\mathscr{S} = \mathscr{S}(1, 0, \rho, \sigma) \quad (\rho, \sigma \in F).$$

We exclude only the trivial case $\rho = \sigma = 0$, in which $\mathscr{S} = \{0\}$.

THEOREM 7.2. *If* $\rho\sigma \neq 0$, *then the plane* $\mathscr{S}(0, 0, \rho, \sigma)$ *is exterior to* $\mathscr{S}$.

Proof. Suppose to the contrary that there is a point Z in $\mathscr{S} \cap \mathscr{S}(0, 0, \rho, \sigma)$. Substituting

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

$$\rho(Z + Z^q + Z^{q^2}) + \sigma = 0$$

into the equation of $\mathscr{S}$:

$$X^{1+q+q^2} + \rho(X + X^q + X^{q^2}) + \sigma = 0, \tag{7.7}$$

with $X = Z$, and simplifying we have

$$Z^{1+q+q^2} = 0,$$

i.e., $Z = 0$. But if $\sigma \neq 0$, then 0 does not lie on $\mathscr{S}(0, 0, \rho, \sigma)$.

As a companion to Theorem 7.2, we have:

THEOREM 7.3. *Every plane* $\pi_\alpha = \mathscr{S}(0, 0, 1, \alpha)$, *except* $\pi_{\sigma/\rho}$ *when* $\rho\sigma \neq 0$, *contains at least one point of* $\mathscr{S}$.

Proof. If $\rho = 0$ then $\mathscr{S} = \mathscr{S}_\sigma$ and the result follows from Theorem 7.1. If $\sigma = 0$, then substitution of

$$Z + Z^q + Z^{q^2} + \alpha = 0$$

into (7.7), with $Z = X$ and $\sigma = 0$, yields

$$Z^{1+q+q^2} = \rho\alpha,$$

and we know from Theorem 7.1 that π_α contains a point of the surface $\mathscr{S}_{-\rho\alpha}$. Any point Z that is in $\mathscr{S}_{-\rho\alpha} \cap \pi_\alpha$ must also lie in the surface with equation

$$X^{1+q+q^2} + \rho(X + X^q + X^{q^2}) + \rho\alpha - \rho\alpha = 0,$$

which is $\mathscr{S}(1, 0, \rho, 0)$. By similar reasoning, if $\rho\sigma \neq 0$ and $\alpha \neq \rho$, then substitution of

$$Z + Z^q + Z^{q^2} + \alpha = 0$$

into (7.7) with $Z = X$ yields

$$Z^{1+q+q^2} = \rho\alpha - \sigma \neq 0.$$

Once again, Theorem 7.1 assures that π_α contains a point of the surface $\mathscr{S}_{\sigma-\rho\alpha}$, and therefore also contains a point of $\mathscr{S}$.

To generalize Lemma 7.3 we have

THEOREM 7.4. $\mathscr{S}$ *contains no line if* $q > 3$.

Proof. If $\rho = 0$, then by Lemma 7.3, $\mathscr{S} = \mathscr{S}_\sigma$ contains no line for $q > 3$. If $\rho\sigma \neq 0$ and there is a line l lying on $\mathscr{S}$, then by Theorem 7.2, l cannot intersect $\pi' = \mathscr{S}(0, 0, \rho, \sigma)$. Thus l lies in a plane $\pi_\alpha = \mathscr{S}(0, 0, 1, \alpha)$ which is parallel to π'. Substituting

$$Z + Z^q + Z^{q^2} + \alpha = 0$$

https://doi.org/10.4153/CJM-1986-035-2 Published online by Cambridge University Press

into (7.7) with $Z = X$, we have

$$Z^{1+q+q^2} = \rho\alpha - \sigma \neq 0.$$

Thus any point Z of l is also a point of $\mathscr{S}_{\sigma-\rho\alpha}$. But this implies $q \leqq 3$ by Lemma 7.3.

The only case not yet considered is $\sigma = 0$, $\rho \neq 0$. In this case it is easily seen that

$$\pi_0 \cap \mathscr{S} = \{0\},$$

where $\pi_0 = \mathscr{S}(0, 0, 1, 0)$; therefore any line l lying entirely in $\mathscr{S}$ either contains 0 or lies in a plane $\pi_\alpha(\alpha \neq 0)$ parallel to π_0. If the latter holds, then a duplicate argument to the above yields $q \leqq 3$. If l contains 0, then

$$l = \{\lambda Z\} \quad (\lambda \in F, Z \neq 0),$$

where

$$(7.8) \quad Z^{1+q+q^2} + \rho(Z + Z^q + Z^{q^2}) = 0.$$

Since by assumption $\lambda Z \in \mathscr{S}$ for all $\lambda \in F$,

$$(7.9) \quad \lambda^3 Z^{1+q+q^2} + \rho\lambda(Z + Z^q + Z^{q^2}) = 0.$$

Solving (7.8) and (7.9) simultaneously, we have $\lambda^3 - \lambda = 0$. Thus $\lambda = 0$, 1, or -1. But (7.9) is true for all $\lambda \in F$ and neither Z^{1+q+q^2} nor $Z + Z^q + Z^{q^2}$ is zero. Therefore

$$|\{\lambda\}| = |F| = q \leqq 3.$$

Theorems 7.1-7.3 contribute to, but do not complete, the solution of the following problem:

Given a cubic surface $\mathscr{S} = \mathscr{S}(1, 0, \rho, \sigma)$, find all exterior planes to $\mathscr{S}$.

We know from Theorem 7.1 that $\mathscr{S}_\sigma = \mathscr{S}(1, 0, 0, \sigma)$ $(\sigma \neq 0)$ has no exterior planes, and $\mathscr{S}_\sigma$ is a cubic of type I. But it is not hard to show that for $q > 2$, $\mathscr{S}_\sigma$ is equivalent to a cubic $\mathscr{S}(1, 0, \rho, \sigma)$ with $\rho\sigma \neq 0$, which by Theorem 7.2 has an exterior plane. Thus we cannot conclude that all cubics of type I have no exterior planes. Moreover, we can show by direct computation for any given value of $q \geqq 2$ that there are cubics of each type with form $\mathscr{S}(1, 0, \rho, \sigma)$ where $\rho\sigma \neq 0$; therefore there are cubics of each type with at least one exterior plane.

References

1. R. H. Bruck, *Circle geometry in higher dimensions II*, Geom. Ded. *2* (1973), 133-188.
2. H. S. M. Coxeter, *Introduction to geometry* (Wiley, New York, 1969).
3. ——— *Projective geometry* (Blaisdell, Waltham, Mass., 1964).
4. P. Dembowski, *Finite geometries* (Springer-Verlag, Berlin, 1968).
5. M. Hall, Jr., *Cyclic projective planes*, Duke Math. J. *14* (1947), 1079-1090.

6. J. W. P. Hirschfeld, *Projective geometries over finite fields* (Clarendon Press, Oxford, 1979).
7. D. Jungnickel and K. Vedder, *On the geometry of planar difference sets*, Europ. J. Combinatorics *5* (1984), 143-148.
8. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. *43* (1938), 377-385.

University of Toronto,
Toronto, Ontario