Can. J. Math., Vol. XXVII, No. 5, 1975, pp. 1141–1148

# SUBREGULAR SPREADS AND INDICATOR SETS

A. BRUEN

**1. Introduction.** In a previous paper [**3**] we introduced indicator sets in order to facilitate the study of partial spreads and spreads in $\Sigma = PG(3, q)$. The idea enabled us to disprove a conjecture in the literature by constructing a spread that contained no regulus. More recently there have been some notable advances in the theory of spreads. One such advance is Denniston's theorem that packings of spreads always exist in $\Sigma$. This result can be very nicely interpreted in terms of indicator sets [**1**]. Another notable advance is the result on subregular spreads due to W. F. Orr [**4**; **5**] which is discussed below. In this note we develop further some ideas on indicator sets in [**3**] and then use these results to give an alternative proof of this result of Orr. Part of our intention also is to show how indicator sets clarify and complement certain details in Orr's work.

As in [**2**; **4**; **5**] we define a *subregular spread* $H$ of $\Sigma$ to be a spread obtainable from a regular spread by a sequence of steps of reversing reguli. The significance of subregular spreads is discussed in Bruck [**2**]. Orr's result [**4**; **5**] is that *$H$ is always obtainable from some regular spread $S$ by reversing a set of disjoint reguli of $S$.* (This theorem follows from another interesting result, namely that no "new" reguli are created unless $H$ is obtained by reversing a linear set of reguli in $S$ – see Theorem 11.) Because of the connection (see [**3**]) between deriving certain translation planes (and in particular those of order $p^2$ with $p$ a prime) and reversing reguli in the corresponding spread, Orr's theorem also settles the analagous outstanding question for translation planes of order $p^2$ (T. G. Ostrom has posed the question in this form in [**6**]).

As stated earlier, our purpose is to develop the theory of indicator sets and then to give an alternative proof of Orr's theorem. Our proof makes use of a new result which is of interest in its own right (Theorem 6) concerning a partitioning of a finite field $K$ that uses additive translates of certain multiplicative subgroups of $K$. In Section 4 it is shown that our proof of Orr's theorem also ties in nicely with an even stronger result which has been proved by J. Thas for $q$ even and which has been shown in the case of $q$ odd by Orr. The result is that a complete set of $q - 1$ disjoint reguli in a regular spread is linear. As is pointed out in [**4**, p. 5] this actually implies Orr's theorem above on subregular spreads. The proof of the stronger result for $q$ even (due to Thas) is quite short, but the proof for the case of $q$ odd (due to Orr [**5**]) is long and appears quite complicated.

---

Received August 9, 1974 and in revised form, October 15, 1974. This research was supported by NRC Grant A-8726.

**2. Finite fields.** Let $F \subset K$ with $F = GF(q)$, $K = GF(q^2)$. We denote by $\sigma$ the involutory automorphism of $K$ fixing $F$. For each element $x$ of $K$ we define the *norm* $M(x)$ of $x$ by $M(x) = xx^\sigma$. Set $N_1 = \{x \in K | M(x) = 1\}$. Then $N_1$ is a subgroup of $K^*$ (the multiplicative group of non-zero elements of $K$) of order $q + 1$. The cosets $N_1, N_2, \ldots, N_{q-1}$ of $N_1$ in $K^*$ will be referred to as *norm sets* (*classes*).

*Notation.* Greek letters and subscripted Greek letters will always denote elements of $F$ throughout. If $A$, $B$ are arbitrary sets then $A - B$ means those elements of $A$ which are not in $B$. The cardinality of the set $X$ will be denoted by $|X|$.

LEMMA 1. *Let $t \in K - F$ with $M(t) = \gamma \in F$. Then the irreducible quadratic over $F$ which is satisfied by $t$ is of the form $x^2 = \alpha_1 x + \alpha_2$ where $0 \neq \alpha_2 = -\gamma$. If $q$ is even $\alpha_1 \neq 0$.*

*Proof.* $K$ is a quadratic extension of $F$, so $t$ satisfies a unique monic irreducible quadratic over $F$, say $t^2 = \alpha_1 t + \alpha_2$. Then $(t^\sigma)^2 = \alpha_1 t^\sigma + \alpha_2$. Since $t \neq t^\sigma$, $t^\sigma = \alpha_1 - t$. Thus $\gamma = M(t) = tt^\sigma = -t^2 + \alpha_1 t = -\alpha_2$. Finally, if $q$ is even, every element of $F$ has a square root in $F$ so $\alpha_1 \neq 0$ in this case.

COROLLARY 2. *Let $N$ be any norm class, and assume that $q \geqq 4$. Let $\delta$ be any element of $F = GF(q)$. Then there exists at least one $t \in N$ with $t \in K - F$ such that $\lambda_1\lambda_2^{-1} \neq \delta$ where the irreducible quadratic satisfied by $t$ over $F$ is given by $t^2 = \lambda_1 t + \lambda_2$.*

*Proof.* Let $N = \{x | M(x) = \gamma\}$. Put $L = (K - F) \cap N$ and let $u \in L$. Then $u$ satisfies $u^2 = \lambda_1 u + \lambda_2$ say where, by Lemma 1, $\lambda_2 = -\gamma$. Suppose that $\lambda_1\lambda_2^{-1} = \delta$. There is at most one other element, say $v$, in $L$ satisfying the same quadratic as $u$ and having $\lambda_1\lambda_2^{-1} = \delta$. Since $|L| \geqq q - 1$, $|L - \{u, v\}| \geqq q - 3 \geqq 1$ since $q \geqq 4$. Then any element $t$ in the set $L - \{u, v\}$ has the desired property.

LEMMA 3. *Let $q$ be even. Assume there exists an element $d \in K$ and a norm class $N$ such that the $q - 1$ sets $\gamma(N + d) = \{\gamma(n + d) | n \in N\}$ with $0 \neq \gamma \in F$ form a partition of $K^*$. Then $d \in F$.*

*Proof.* Because of the partitioning, the set $T = N + d$ must contain a unique element $\beta \in F^*$. Thus there exists a unique $v \in N$ with $v + d = \beta$. Suppose $v \notin F$. Then, as in Lemma 1, $v^\sigma = v + \alpha_1$ with $0 \neq \alpha_1 \in F$. Clearly $M(v) = M(v^\sigma)$, so $v^\sigma \in N$. Now $v^\sigma + d = (v + d) + \alpha_1 \in F$. We are given a partitioning of non-zero elements, and $v$ is unique. We conclude that $v \in F$. Since $d = v + \beta$ we have $d \in F$.

LEMMA 4. *With the hypotheses of Lemma 3 we have $d = 0$.*

*Proof.* By Lemma 3, $d \in F$. We show that if $d \neq 0$ then $N + d$ contains two distinct elements denoted by $s$, $t$ such that $(s + d)(t + d)^{-1} \in F$. Then

Lemma 4 will immediately follow. Choose any element $t \in (K - F) \cap N$. Let $N = \{x | M(x) = \rho\}$. Then $t$ satisfies $t^2 = t\lambda_1 + \lambda_2$ say, with $\lambda_1$, $\lambda_2$ in $F$. Since $q$ is even we have from Lemma 1 that $\lambda_1 \neq 0$ and $\lambda_2 = \rho$. Set $s = t\alpha + \beta$ with $\alpha$, $\beta$ to be determined in $F$. Then, as in Lemma 1, $s \in N$ if and only if

(1) $\lambda_2\alpha^2 + \lambda_1\alpha\beta + \beta^2 = \lambda_2$.

Since $\lambda_1 \neq 0$, $(s + d)(t + d)^{-1} \in F$ if and only if

(2) $\beta + d = \alpha d$.

Since $d \in F$ and since $x^2 = x\lambda_1 + \lambda_2$ is irreducible over $F$, $d$ cannot satisfy it. Solving the simultaneous equations (1), (2) we find that apart from the trivial solution $\alpha = 1$, $\beta = 0$ there is one other solution, namely $\alpha = (d^2 + \lambda_2)(d^2 + d\lambda_1 + \lambda_2)^{-1}$, $\beta = d^2\lambda_1(d^2 + d\lambda_1 + \lambda_2)^{-1}$. This yields the desired element $s = t\alpha + \beta$ such that $(s + d)(t + d)^{-1} \in F$ proving the lemma.

LEMMA 5. *Let $q$ be odd. Then there does not exist an element $d \in K$ and a norm class $N$ such that the $q - 1$ sets $\gamma(N + d)$ with $0 \neq \gamma \in F$ partition $K^*$.*

*Proof.* For any given $N$, $d$, we produce elements $s$, $t$ in $N$ with $t \in K - F$ such that $(s + d)(t + d)^{-1} \in F$, and this will establish the result. As before, set $N = \{x | M(x) = \rho\}$. Choose any $t \in (K - F) \cap N$, and let $t^2 = t\lambda_1 + \lambda_2$, with $\lambda_1, \lambda_2 \in F$. By Lemma 1, $\lambda_2 = -\rho$. Since $t \in K - F$, every element of $K$ can be written in the form $t\gamma_1 + \gamma_2$ for unique elements $\gamma_1, \gamma_2 \in F$. In particular, we may write $d = t\omega_1 + \omega_2$. As in Lemma 4, set $s = t\alpha + \beta$ with $\alpha, \beta$ (to be determined) in $F$. Now $s \in N$ if and only if

(1) $\lambda_2\alpha^2 - \lambda_1\alpha\beta - \beta^2 = \lambda_2$.

The lemma is clear if any element of $N + d$ is zero. Thus we may assume that $t + d \neq 0$. Then $(s + d)(t + d)^{-1} \in F$ if and only if

(2) $\alpha\omega_2 - \beta(1 + \omega_1) - \omega_2 = 0$.

We seek an ordered pair $(\alpha, \beta) \neq (1, 0)$ satisfying both (1) and (2). If $\omega_2 = 0$ the pair $(-1, 0)$ will satisfy. Assume $\omega_2 \neq 0$. Then from (2) we obtain $\alpha = 1 + \theta\beta$, where $\theta = (1 + \omega_1)\omega_2^{-1} \in F$. Since the quadratic $g(x) = x^2 - \lambda_1 x - \lambda_2$ is irreducible over $F$, we have $g(\theta\lambda_2) \neq 0$. Substituting $\alpha = 1 + \theta\beta$ in (2) we obtain a solution pair $(\alpha, \beta)$ with $\beta = \lambda_2^2(\lambda_1\lambda_2^{-1} - 2\theta)[g(\theta\lambda_2)]^{-1}$ and $\alpha = 1 + \theta\beta$.

Also, $(\alpha, \beta) \neq (1, 0)$ unless $\lambda_1\lambda_2^{-1} = 2\theta$. But by Corollary 2, we can choose $t$ to avoid the case $\lambda_1\lambda_2^{-1} = 2\theta$ if $q \geqq 4$. The case $q = 3$ is easily handled separately. This proves Lemma 5.

Combining Lemmas 4 and 5 we obtain

THEOREM 6. *There exists an element $d \in K$ and a norm set $N$ such that the sets $\gamma(N + d)$ (with $0 \neq \gamma \in F$) partition $K^*$ if and only if $q$ is even and $d = 0$.*

*Proof.* If $q$ is even, the elements of $F^*$ form a complete set of coset representatives for the subgroup $N_1$ of $K^*$. This proves the "if" part. The "only if" part follows from Lemmas 4 and 5.

**3. Background.** We use the ideas on indicator sets etc. as discussed in [**3**] and we will try to combine our notation with that of Orr [**4**]. We have $\Sigma \subset \Sigma^*$

where $\Sigma = PG(3, F) = PG(3, q)$ and $\Sigma^* = PG(3, K) = PG(3, q^2)$. We use homogeneous coordinates in describing $\Sigma(\Sigma^*)$ in terms of a 4-dimensional vector space over $F(K)$. The *indicator plane* $\pi(l)$ is the plane spanned by the vectors $e_1$, $e_2$, $te_3 + e_4$ where $\{e_1, e_2, e_3, e_4\}$ form a basis for $\Sigma(\Sigma^*)$ over $F(K)$ and $t$ is an element of $K - F$. *Here $l$ is the line of $\pi(l)$ spanned by $e_1$, $e_2$ and given by* $l = \langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle$. Through each point of $\pi(l) - l$, that is, through each *affine point* of $\pi(l)$ there passes, by [**3**, Lemma 2.1], a *unique line* of $\Sigma$. Let $u$, $v$ be the unique lines of $\Sigma$ through the affine points $U$, $V$ respectively. Then by [**3**, Theorem 2.4] *$u$ and $v$ are skew if and only if the line $UV$ meets $l$ in a point of $\Sigma^* - \Sigma$*. We say that $U(V)$ *indicates* $u(v)$. Each affine point of $\pi(l)$ has (homogeneous) coordinates of the form $(x, y, t, 1)$. *In particular the affine point* $(0, 0, t, 1)$ *indicates the line* $m = \langle e_3, e_4\rangle$ *given by* $m = \langle(0, 0, 1, 0), (0, 0, 0, 1)\rangle$.

A *regular spread* $S$ of $\Sigma$ has the characteristic property that if $x$ is any line of $\Sigma - S$ *then the* $q + 1$ *lines of $S$ meeting $x$ form a regulus denoted by* $R_S(x)$ *or, if no confusion can arise, simply by* $R(x)$. The set of points on an affine line of $\pi(l)$ (whose slope is in $K - F$) indicates a partial spread $U$ such that $U \cup l$ is a *regular spread* of $\Sigma$. If $W$ denotes a family of disjoint reguli in $S$ then $S^W$ denotes the subregular spread obtained from $S$ by reversing each regulus of $W$. For the isomorphism between a regular spread, with its lines and reguli, and the inversive plane over $GF(q)$ with its points and circles we refer to [**3**, p. 536; **4**, p. 4; and **2**, Theorem 4.5]. In particular, if $R$ is a regulus of $\Sigma$ containing $l$ then $R - l$ is indicated by a set $L$ of $q$ affine collinear points of $\pi(l)$ which are contained in a *chain* or *projective subline* in $\pi(l)$ (see [**3**, Lemma 3.3] and [**3**, p. 536]). If this set $L$ contains $(0, 0, t, 1)$, and say, $(x, y, t, 1)$ then $L = \{(\gamma x, \gamma y, t, 1)|\gamma \in F\}$.

**4. The main result.** We refer to [**2**, p. 437] for an account of the following results.

LEMMA 7. *The projective linear group $PL(\Sigma)$ of $\Sigma = PG(3, q)$ is transitive on the regular spreads of $\Sigma$.*

LEMMA 8. *Let $S$ be a regular spread of $\Sigma$ and let $G$ be the subgroup of $PL(\Sigma)$ mapping $S$ upon $S$. Then $G$ is transitive on the ordered triples of lines in $S$.*

Much of the following lemma is implicit in the work of Bruck [**2**] but for the sake of completeness and compactness we discuss it here.

LEMMA 9. *Let $S$ be a regular spread of $\Sigma$ consisting of* $l = \langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle$ *together with those lines of $\Sigma$ indicated by the set $y = xt$, that is, the lines indicated by* $\{(x, xt, t, 1)|x \in K\}$. *Suppose $N$ is a norm set in $K$. Then*

(i) *Each subset of the form* $\{(x + d, (x + d)t, t, 1)|x \in N\}$ *indicates a regulus $R(d)$ of $S$. If $R'(d)$ denotes the lines indicated by*

$$\{(x + d, xt^{\sigma} + dt, t, 1)|x \in N\}$$

*then $R'(d)$ is the opposite regulus of $R(d)$.*

(ii) *Any regulus of $S$ not containing $l$ is equal to $R(d)$ for some choice of $N$, $d$.*

(iii) *For a fixed $d$ and varying $N$, the $q - 1$ reguli $R(d)$ form a complete linear set $H(d)$ of reguli in $S$. In particular, if $d = 0$, this linear set $H(0)$ has the lines $m$, $l$ for common conjugate lines where*

$$m = \langle (0, 0, 1, 0), (0, 0, 0, 1) \rangle, \quad l = \langle (1, 0, 0, 0), (0, 1, 0, 0) \rangle.$$

(iv) *Set $S' = S^{H(0)}$. Then $S'$ is a regular spread, $S \cap S' = \{l, m\}$ and $S' - \{l\}$ is indicated by the line $y = xt^\sigma$ that is, by the set $\{(x, xt^\sigma, t, 1) | x \in K\}$. Moreover, if $x$ is any line of $S' - \{l, m\}$ indicated by the point $(x, xt^\sigma, t, 1)$ then $x$ lies in the reverse of a unique regulus $R_S(x)$ of $S$. This regulus is a regulus of $H(0)$ indicated by $\{(y, yt, t, 1) | y \in N\}$ with $N$ being the norm class of $K$ containing $x$.*

*Proof.* (i) can be seen from the following argument. Let $A$ be the point $(y + d, (y + d)t, t, 1)$ with $y \in N$. Let $B$ be the point $(z + d, zt^\sigma + dt, t, 1)$ with $z \in N$. Then the line $AB$ meets $l$ in a point of $\Sigma$, namely $(1, \gamma, 0, 0)$ where $\gamma = (zt^\sigma - yt)(z - y)^{-1} \in F$. Thus (Section 3) the lines $a$, $b$ indicated by $A$ and $B$ intersect. Letting $x$ vary over $N$ we obtain $q + 1$ distinct lines $a$ which, being contained in $S$, are pairwise skew. From the above, each of these $q + 1$ pairwise skew lines in $R(d)$ intersects each line of $R'(d)$. Thus, $R'(d)$ is contained in a regulus, and since $|R'(d)| = q + 1$, we have that $R'(d)$ is a regulus, with opposite regulus $R(d)$.

(ii) is easily established by counting.

For (iii) see Bruck [**2**, p. 509].

Part (iv) is proved in a manner similar to (i), using the fact that a linear indicator set yields a regular spread minus the line $l$.

*Comment.* If we think of the real inversive plane most of the above results become rather clear. For example, (ii) says that every circle (regulus) not passing through the point at infinity has a centre (at $d$) and a radius (corresponding to the norm class $N$).

We proceed to the main result (Theorem 11). One of the major differences between our approach and that of Orr [**4**] occurs in the proof of the following result which corresponds approximately to Lemma 2 in [**4**].

LEMMA 10. *Let $U = S^W$ where $S$ is a regular spread and $W = \}R_1, R_2, \ldots, R_{q-1}\}$ is a set of $q - 1$ disjoint reguli of $S$. Suppose $R$ is a regulus of $S^W$ with $|R \cap R_i'| = 1$, $1 \leqq i \leqq q - 1$. Then $q$ is even and $W$ is a complete linear set.*

*Proof.* Let $S \cap S^W = \{u, v\}$ say, where $S - \bigcup_i R_i = \{u, v\}$. Then $R \cap S = \{u, v\}$. The property of being a complete linear set is invariant under collineations of $\Sigma$. Using Lemma 7, we can thus assume that $S$ is the regular spread of Lemma 9 consisting of $l = \langle e_1, e_2 \rangle$ together with the lines of $\Sigma$ indicated by $y = xt$. Using Lemma 8 we can also assume that $u = l$ above and $v = m = \langle e_3, e_4 \rangle$. Thus $R$ contains $l$, $m$. Furthermore, $R_i \cap \{l, m\} = \emptyset$, $1 \leqq i \leqq q - 1$. Let $R \cap R_1' = b$. By 9 (ii) the regulus $R_1$, being disjoint from $l$, is equal to

https://doi.org/10.4153/CJM-1975-119-4 Published online by Cambridge University Press

$R(d)$ for some choice of $N$, $d$. By 9 (i), $R_1'$ is indicated by

$$\{(x + d, xt^\sigma + dt, t, 1) | x \in N\}.$$

In particular, $b$ is indicated by $(x_0 + d, x_0t^\sigma + dt, t, 1)$ for some $x_0 \in N$. Since $R$ contains $l$ and also $\{m, b\}$, $R - l$ is indicated by a projective subline (see Section 3) containing the two points indicating $m, b$. Thus $R - \{l, m\}$ is indicated by

$$\{(\gamma(x_0 + d), \gamma(x_0t^\sigma + dt), t, 1) | \gamma \in F^*\}.$$

We now find $R \cap R_i'$. By 9 (i) and 9 (ii), $R_i'$ is indicated by

$$\{(z + d_i, zt^\sigma + d_it, t, 1) | z \in N_i\}$$

where $N_i$ is some norm class. Since $|R \cap R_i'| = 1$ there must be a unique $\gamma_0 \in F^*$ such that

$$z + d_i = \gamma_0(x_0 + d)$$
$$zt^\sigma + d_it = \gamma_0(x_0t^\sigma + dt).$$

Since $t^\sigma \neq t$, we have $d_i = \gamma_0 d$, $z = \gamma_0 x_0$. Thus *one line* in $R_i'$, call it $p$, is indicated by $(\gamma_0(x_0 + d), \gamma_0x_0t^\sigma + \gamma_0dt, t, 1)$. A virtue of indicator sets is that we can now easily determine $R_i$ from this as follows. We have $p \in R_i'$. Thus $R_i$ will be the *unique* regulus of the regular spread $S$ whose $q + 1$ lines pass through the $q + 1$ points of $p$ (in terms of the notation of Section 3, $R_i = R_S(p)$). Thus, to find $R_i$, we look for a regulus in $S$ all of whose lines intersect $p$. Since $0 \neq \gamma_0$ is fixed and the norm function is multiplicative, the set $\gamma_0N = \{\gamma_0x | x \in N\}$ is a norm class. Also $d$ is fixed. By 9 (i) the set

$$T = \{(\gamma_0(x + d), \gamma_0(x + d)t, t, 1) | x \in N\}$$

is a regulus of $S$. Since $x_0 \in N$, the line $p$ is in the opposite regulus $T'$ by 9 (ii). Thus $T$ is a regulus of $S$, and $p$ meets each line of $T$. Therefore $T = R_i$. (We note that different values of $i$ yield different values of $\gamma_0$.) Now for $x \in K^*$, the point $(x, xt, t, 1)$ indicates a line $\neq l, m$ of $S$ which must be contained in some $R_i$, since $\bigcup_i R_i = S - \{l, m\}$. Thus the $q - 1$ sets $\gamma(N + d)$ with $\gamma \in F^*$ partition $K^*$. By Theorem 6, $q$ is even and $d$ is zero. In this case, by Lemma 9 (iii), the $R_i$ form a complete linear set. This completes the proof of Lemma 10.

We now come to the main result. The proof is similar to that in [**4**], although it is somewhat more streamlined, and is simplified, we feel, by the use of indicator sets.

THEOREM 11. *Let $S^W$ be a subregular spread in $\Sigma = PG(3, q)$ obtained from a regular spread $S$ by reversing a non-linear set $W = \{R_1, R_2, \ldots, R_k\}$ of pairwise disjoint reguli of $S$. Then every regulus $R$ contained in $S^W$ is either*

(i) *a regulus in $S$, or*

(ii) *the reverse of some $R_i$, $1 \leqq i \leqq k$.*

*Proof*. Any two disjoint reguli of $S$ are extendable to a complete linear set. Thus since $W$ is non-linear we have $k \geqq 3$. The maximum number of disjoint reguli in $S$ is $q - 1$. Thus, $3 \leqq k \leqq q - 1$, so $q \geqq 4$. Suppose that $R \subset S^W$ is neither in class (i) or (ii) of the theorem. Then $|R \cap S| \leqq 2$, since $S$ is regular, and $|R \cap R_i'| \leqq 2$ for $1 \leqq i \leqq k$. Since $q \geqq 4$ this implies that $R$ contains lines from at least two of the reguli $R_i'$.

First we claim that $|R \cap R_i'| \leqq 1, 1 \leqq i \leqq k$. For suppose that $|R \cap R_1'| = 2$, say. $R$ contains lines from at least one more of the $R_i'$, say $R_2'$, so that $|R \cap R_2'| \geqq 1$. The pair $R_1$, $R_2$ extend to a complete linear set $J$ in $S$ with common conjugate lines $u, v$. By Lemmas 7 and 8 we may assume that $u = l = \langle e_1, e_2 \rangle$, $v = m = \langle e_3, e_4 \rangle$, and that $S - l$ is indicated by $y = xt$. Since $J$ can be recovered from $\{l, m\}$ we have by 9 (iii) that $J = H(0) = H$ say. Set $S' = S^J$. *Then $S'$ is regular*, with $S \cap S' = \{l, m\}$. Since $S'$ contains $R_1'$, $R'_2$, $|R \cap S'| \geqq 3$. So $R \subset S'$. Put $T = R - \{l, m\}$. As in 9 (iv), each line $x \in T$ is in the reverse of a *unique* regulus $R_S(x)$ of $S$. Now, since $x \in R$, $x \in S'$. Also $x \neq l, m$. By definition, each line of $S'$ apart from $\{l, m\}$ lies in (exactly) one of the reguli $R_i'$. In particular, $x$ lies in one of the reguli $R_i'$, say $x \in R_a'$. Since $R_a$ is in fact a regulus of $S$, we see that $R_S(x) = R_a$ and, by 9 (iv), $R_S(x) \in H$. Since $|R \cap R_i'| \leqq 2$, it follows that the number $n$ of reguli $R_1, R_2, \ldots, R_n$ that are also reguli of $H$ is at least $\frac{1}{2}|T|$. Also, $|T| \geqq q - 1$. Thus $n \geqq \frac{1}{2}(q - 1)$. Since $W$ is nonlinear, there exists at least one regulus $R_j \in W$ with $R_j \notin J$. Then each line of $R_j$ is either $l$, $m$ or a line of the $q - 1 - n$ reguli of $J$ that are contained in $J - \{R_1, R_2, \ldots, R_n\}$; moreover, $R_j$ has at most two lines in common with any of these last reguli. This yields that

$$2(q - 1 - n) + 2 \geqq q + 1,$$

so that $n \leqq \frac{1}{2}(q - 1)$. From the above we see that $n = \frac{1}{2}(q - 1)$. On the one hand this implies that $\{l, m\} \subset R$ and, on the other hand, that $\{l, m\} \subset R_j$. Now since $R_j' \subset S^W$, and $\{l, m\} \subset R_j$ neither $l$ nor $m$ is in $S^W$. However, from the above, $\{l, m\} \subset R \subset S^W$. This is a contradiction, and we conclude that $|R \cap R_i'| \leqq 1, 1 \leqq i \leqq k$.

Finally, since $|R| = q + 1$ and $|R \cap S| \leqq 2$ we obtain $k = q - 1$ and $|R \cap R_i'| = 1, 1 \leqq i \leqq q - 1$. An appeal to Lemma 10 completes the proof.

*Comment*. Theorem 11 shows that by reversing the reguli of a non-linear disjoint set in the regular spread $S$ we cannot obtain any "new" reguli.

Finally, we sketch a proof of the following result, the details of which may be found in [**4**].

COROLLARY 12. *Every subregular spread in $\Sigma = PG(3, q)$ is obtainable from some regular spread $S$ by reversing a set of disjoint reguli of $S$.*

*Outline of proof.* Let $U$ be a subregular spread obtained from the regular spread $S$ by a sequence of steps of reversing reguli. That is, there is a sequence $S = S_0, S_1, \ldots, S_k$ of spreads such that $S_i = (S_{i-1})^{R_i}$ for some regulus $R_i$ in

$S_{i-1}$, $1 \leqq i \leqq k$. We proceed by induction. Clearly $S_1$ is obtainable from $S = S_0$ by reversing a (singleton) set of reguli. For $1 \leqq i < k$, suppose that $S_i$ is obtainable from some regular spread $S^*$ by reversing a set $L$ of disjoint reguli in $S^*$, so that $S_i = (S^*)^L$. If $L$ is non-linear we may exploit Theorem 11. Now suppose $L$ is linear. Then $L$ is extendable to a complete linear set $H$ in $S$. If $q > 3$ and if $R_{i+1}$ is not in $S^*$, then, as in the proof of Theorem 11, $R_{i+1}$ is contained in the regular spread $(S^*)^H$. For each regulus $R$ in $H - L$, $R_{i+1}$ is disjoint from $R$ and $R'$ the opposite regulus of $R$. The set $W$ of the regular spread $(S^*)^H$ consisting of $R_{i+1}$ and each $R'$ (where $R \in H - L$) is a set of disjoint reguli, and moreover, $S_{i+1} = ((S^*)^H)^W$. Thus the corollary holds for $S_{i+1}$ and, by induction, for $S_k$ provided $q > 3$. For $q \leqq 3$ we can use the known structure of spreads of $PG(3, q)$ to prove the result also in these cases.

*Remark.* Let us suppose that $W$ is a complete set of $q - 1$ disjoint reguli of the regular spread $S$. Denote by $u, v$ the two lines "left over". It has been shown by J. Thas [**7**] that for $q$ even, $W$ is linear with common conjugate lines $u$, $v$. Subsequently this result has also been shown for $q$ odd by W. Orr. By a collineation (Lemma 7) we assume that $S$ is indicated by $y = xt$ and (Lemma 8) that $u = l$, $v = m$. Using the ideas in this section we can then see that the above result of Thas (for $q$ even) and of Orr (for $q$ odd) is equivalent to the following statement.

COROLLARY 13. *Let there be given a partition of $K^*$ by $q - 1$ sets of the form $N_i + a_i$, with $N_i$ being a norm set in $K$ and $a_i \in K$. Then each $a_i$ is zero, and $N_i \cap N_j = \emptyset$ if $i \neq j$ so that each norm set in $K^*$ is equal to one of the sets $N_i$, $1 \leqq i \leqq q - 1$.*

## REFERENCES


**1.** A. Beutelspacher, *On parallelisms in 3-dimensional finite projective spaces*, to appear, Geometriae Dedicata.

**2.** R. H. Bruck, *Construction problems of finite projective planes*, Proceedings of the Conference in Combinatorics held at the University of North Carolina at Chapel Hill, April 10–14, 1967 (University of North Carolina Press, 1969), 426–514.

**3.** A. Bruen, *Spreads and a conjecture of Bruck and Bose*, J. Algebra *23* (1972), 519–537.

**4.** W. F. Orr, *A characterization of subregular spreads in finite 3-space*, text of lecture presented to the American Mathematical Society at the Annual Meeting in Dallas, Texas, January 25–29, 1973. (See abstract no. 351, A. M. S. Notices, January 1973.)

**5.** ——— *The miquelian inversive plane $IP(q)$ and the associated projective planes*, Doctoral Dissertation, University of Wisconsin, 1973.

**6.** T. G. Ostrom, *Translation planes*, Proc. Conf. on Combinatorial Mathematics and its Applications, Chapel Hill, April 1967 (University of North Carolina Press, Chapel Hill, North Carolina, 1969).

**7.** J. Thas, *Flocks of finite egglike inversive planes;* in *Finite geometric structures and their applications*, C.I.M.E. II ciclo 1972, Ed. Cremonese, Rome, 1973, pp. 189–191.



*University of Western Ontario,*
*London, Ontario*