CONTRIBUTIONS TO BOOLEAN GEOMETRY OF p-RINGS

ROBERT A. MELTER

1. Introduction. In a paper in this journal [7], J. L. Zemmer proposed two problems relating to the geometry of the Boolean metric space of a p-ring. (A p-ring is a ring R in which $px = 0$ and $x^p = x$ for some positive prime p, and all $x \in R$. The axioms of a p-ring imply its commutativity.) The first problem asked for necessary and sufficient conditions in order that a subset of such a space (hereafter called a p-space) be a metric basis; the second problem was the determination of congruence indices for p-spaces, with respect to the class of Boolean metric spaces. The present paper contains solutions to these questions as well as a brief discussion of certain properties of the group of motions of a p-space, and an introduction to analytic geometry in a p-space. The reader is referred to Zemmer's paper for definitions not contained herein.

2. Metric bases for p-spaces. Let us recall the following definition.

DEFINITION 2.1. A subset S of a Boolean metric space M is called a *metric basis*, if and only if x, y in M and $d(x, s) = d(y, s)$ for all $s \in S$ imply $x = y$.

Let R be a p-space and B its Boolean ring of idempotents. It is well known that B is a subdirect sum of $GF(2)$ [6]. Denote by B^* the complete direct sum of these same rings.

Associate with every subset S of R a subset $\bar{S}$ of B^* defined as follows:

Let $S_{j,k}$ be the subring of B^* consisting of those elements z of B^* having the property

$$z \subseteq \bigcap_{s \in S} (s - j)^{p-1}(s - k)^{p-1}$$

for $j, k = 0, 1, 2, \cdots, p - 1,\ j \neq k$.

Let

$$\bar{S} = \bigcup_{set} S_{j,k}[j < k;\ j, k = 0, 1, 2, \cdots, p - 1] .$$

THEOREM 2.1. *Let R be a p-space with Boolean ring of idempotents B. If S is a subset of R then S is a metric basis for R if*

Received August 12, 1963. The contents of this paper formed a part of the author's University of Missouri Doctoral Dissertation, written under the direction of Professor Joseph L. Zemmer.

and only if $\bar{S} \cap B = 0$, *where* $\cap$ *indicates set intersection.*

Proof. A sequence of lemmas will be established, followed by the demonstration of the theorem itself.

LEMMA 2.2. *Let* w, s, b, d *be elements of a p-ring such that* $w^2 = w$, *and* $w \subseteqq (s-b)^{p-1} \cap (s-d)^{p-1}$, *then* $(s-dw)^{p-1} = (s-bw)^{p-1}$.

Proof. By the binomial expansion

$$
\begin{aligned}
&(s-dw)^{p-1} \\
&\quad = s^{p-1} - (p-1)s^{p-2}dw + \frac{(p-1)(p-2)}{2}s^{p-3}d^2w^2 + \cdots + d^{p-1}w^{p-1} \\
&\quad = s^{p-1} - (p-1)s^{p-2}dw + \frac{(p-1)(p-2)}{2}d^2ws^{p-3} + \cdots + d^{p-1}w \\
&\quad = w(s-d)^{p-1} - ws^{p-1} + s^{p-1}\,.
\end{aligned}
$$

Similarly $(s-bw)^{p-1} = w(s-b)^{p-1} - ws^{p-1} + s^{p-1}$. Hence $(s-dw)^{p-1} - (s-bw)^{p-1} = w[(s-d)^{p-1} - (s-b)^{p-1}]$. But $w \subseteqq (s-b)^{p-1} \cap (s-d)^{p-1}$ implies $w(s-b)^{p-1} = w(s-d)^{p-1} = w$ and hence $w[(s-b)^{p-1} - (s-d)^{p-1}] = w - w = 0$, and thus $(s-dw)^{p-1} = (s-bw)^{p-1}$, which establishes the lemma.

LEMMA 2.3. *Let* x, y, s, f, g *be elements of a p-ring such that* $(x-s)^{p-1} = (y-s)^{p-1}$, *and* $(f-g)^{p-1} = 1$, *then* $\overline{(x-f)^{p-1}}\,\overline{(y-g)^{p-1}} \subseteqq (s-f)^{p-1}(s-g)^{p-1}$ *where the bar over an idempotent indicates its complement in the Boolean ring of idempotents.*

Proof. Let

$$
\begin{aligned}
a &= (x-s)^{p-1} \qquad & t &= (y-g)^{p-1} \\
b &= (y-s)^{p-1} \qquad & u &= (s-f)^{p-1} \\
r &= (x-f)^{p-1} \qquad & v &= (s-g)^{p-1}
\end{aligned}
$$

and recall that $1 = (f-g)^{p-1}$. By hypothesis $a = b$ and using the fact that the mapping $x \to x^{p-1}$ is a strong Boolean valuation the following inequalities are obtained:

$$
\begin{aligned}
&a \subseteqq r \cup u \qquad && b = a \subseteqq t \cup v \qquad && 1 \subseteqq u \cup v \\
&u \subseteqq r \cup a \qquad && v \subseteqq b \cup t = a \cup t
\end{aligned}
$$

but $1 \subseteqq u \cup v$ implies $u \cup v = 1$, or equivalently

$$
* \qquad\qquad u + v + uv = 1\,,
$$

the addition taking place in the Boolean ring of idempotents.

But then,

$$1 = u \cup v \subseteqq r \cup a \cup t = 1$$
$$1 = u \cup v \subseteqq r \cup t \cup v = 1$$
$$1 = u \cup v \subseteqq r \cup t \cup u = 1 .$$

Let $c = (r \cup t)$, then $c \cup u = 1$ and $c \cup v = 1$ or $c + u + uc = 1$ and $c + v + cv = 1$. Adding the two last equalities it follows that $(u + v)(1 + c) = 0$, $(u + v)(1 + r + t + rt) = 0$, or $(u + v)(1 + r)(1 + t) = 0$. But by * $(u + v) = (1 + uv)$ so that $(1 + uv)(1 + r)(1 + t) = 0$, and in turn $(1 + uv)\bar{r}\bar{t} = 0$ or $\bar{r}\bar{t}uv = \bar{r}\bar{t}$. Returning to the original symbols, this is equivalent to

$$\overline{(x - f)^{p-1}}\overline{(y - g)^{p-1}} \subseteqq (s - f)^{p-1}(s - g)^{p-1}$$

which establishes the lemma.

LEMMA 2.4. *Let x, y be elements of a p-ring such that $(x - y)^{p-1} \neq 0$. Then elements f, g, can be selected from the summands of the identity, $0, 1, 2, \cdots, p - 1$ such that*

(i) $(f - g)^{p-1} = 1$, *and*

(ii) $\overline{(x - f)^{p-1}}\overline{(y - g)^{p-1}} \neq 0$.

Proof. From the hypothesis it is clear that $x \neq y$. If the p-ring is considered as a subring of the ring of all functions on a set X with values in $GF(p)$, then there is some element t_0 of X such that $x(t_0) \neq y(t_0)$. Let f and g correspond to the functions $f(t) \equiv x(t_0)$ for all $t \in X$ and $g(t) \equiv y(t_0)$ for all $t \in X$. It will be shown that f and g satisfy the conditions set forth by the conclusion of the lemma. Clearly f and g are distinct for every t, and hence $(f - g)^{p-1} = 1$. But $(x - f)(t_0) = (y - g)(t_0) = 0$, so that $\overline{(x - f)^{p-1}}(t_0) = \overline{(y - g)^{p-1}}(t_0) = 1$, and $\overline{(x - f)^{p-1}}\overline{(y - g)^{p-1}} \neq 0$.

Proof of Theorem 2.1.

Necessity. Suppose S is a metric basis and $\bar{S} \cap B \ni w \neq 0$. Then w is an element of some $S_{j,k}$, say $S_{b,d}$. Consider bw and dw. Since b and d are distinct and at least one is a unit in the p-ring, $bw \neq dw$. But then by Lemma 2.2 $(s - dw)^{p-1} = (s - bw)^{p-1}$, that is bw and dw have the same distances from every element of S contradicting the assertion that S was a metric basis.

Sufficiency. Suppose $\bar{S} \cap B = 0$ and S is not a metric basis. Then there are elements x, y, of R such that $d(x, s) = d(y, s)$ for all $s \in S$, and $x \neq y$. By Lemma 2.4 there are summands of the identity f, g,

such that

$$(f-g)^{p-1}=1 \qquad \text{and} \qquad \overline{(x-f)^{p-1}}\,\overline{(y-g)^{p-1}} \neq 0 .$$

But by Lemma 2.3

$$\overline{(x-f)^{p-1}}\,\overline{(y-g)^{p-1}} = w \subseteqq (s-f)^{p-1}(s-g)^{p-1}$$

for all $s \in S$, that is $w \in S_{f,g}$ or $w \in \bar{S}$, so that $0 \neq w \in \bar{S} \cap B$. This contradiction terminates the proof of Theorem 2.1.

An examination of the proof of Theorem 2.1 reveals that the role played by the set of summands of the identity can be taken by any equilateral p-tuple with side 1. Further, if $\bar{S} \cap B = 0$ with respect to a given equilateral p-tuple with side 1, then $\bar{S} \cap B = 0$ with respect to every equilateral p-tuple with side 1.

A restatement of the theorem can be given which exposes its content of a metric characterization of metric bases.

THEOREM 2.5. *Let R be a p-space with distance algebra B. A subset S of R is a metric basis for R if and only if there exists an equilateral p-tuple with side* 1, $\{v_1, v_2, \cdots, v_p\}$, *such that the distance algebra does not contain a nonzero element w such that* $w \subseteqq \bigcap_S d(s, v_i)d(s, v_j)$ $[i \neq j, i, j = 1, 2, \cdots, p]$. *(The intersection is to be formed in the Boolean completion of the distance algebra).*

The statement of Theorem 2.5 can be somewhat simplified in a p-space for which the distance algebra is a complete Boolean algebra.

THEOREM 2.6. *Let R be a p-space with complete distance algebra B. A subset S of R is a metric basis for R if and only if there exists an equilateral p-tuple with side* 1, $\{v_1, v_2, \cdots, v_p\}$, *such that* $\bigcap_S d(s, v_i)d(s, v_j) = 0$, $i \neq j$.

A similar result obtains if S is any finite subset of an arbitrary p-space.

THEOREM 2.7. *Let R be a p-space and S a finite subset. Then S is a metric basis for R if and only if there exists an equilateral p-tuple with side* 1, $\{v_1, v_2, \cdots, v_p\}$ *such that* $\bigcap_S d(s, v_i)d(s, v_j) = 0$ $[i \neq j]$.

A useful algebraic interpretation of Theorem 2.7 is incorporated in the following Theorem 2.8.

THEOREM 2.8. *Let R be a p-space. Consider the p-ring R as a subdirect sum of $GF(p)$, that is as a set of "sequences" with terms*

in $GF(p)$. Then if S is a finite subset of R, S is a metric basis for R if and only if the set of kth terms of elements of S contains at least $p-1$ distinct elements of $GF(p)$, for every k.

COROLLARY 1. *A set of $p-1$ elements of a p-space forms a metric basis if and only if it is equilateral of side* 1.

COROLLARY 2. *A metric basis for a p-space contains at least $p-1$ elements.*

COROLLARY 3. *Every element of an autometrized Boolean algebra forms a metric basis.*

Corollary 3 was originally discovered by Ellis [1].

Ellis [2] quotes a conjecture due to J. Gaddum that in a metric space any equilateral set containing the maximal number of elements forms a metric base provided the space is complete and convex.

In a p-space the maximal equilateral sets have exactly p-elements. These sets are metric bases if and only if they have side 1, that is that they are maximal with respect both to number of sides and to common distance.

It is interesting to note that in a p-space even though every metric basis must contain at least $p-1$ points, there are *infinite minimal metric bases*, that is infinite metric bases such that no proper subset is also a metric basis. The following example illustrates such a case.

Example 2.1. Let R be a 3-space in which the distance algebra B is the complete direct sum of countably many copies of $GF(2)$. Let S be the set of atoms in B. Then S is a metric basis for R, but no proper subset of S has this property.

We concluded this section with a brief study of superposability properties of metric bases in p-spaces.

It is known that every congruence between two finite subsets of a p-space can be extended to a motion. The following example illustrates that this conclusion cannot be extended to metric bases.

EXAMPLE 2.2. Let $[0, 1)$ be the right open interval on the real line. Let B denote the class of all subsets of $[0, 1)$ that are unions of finitely many right open intervals $[a, b)$, $0 \leqq a \leqq 1$, $0 \leqq b \leqq 1$, where a and b are *rational* numbers. Then B is an atom-free Boolean algebra whose Boolean operations are the usual set operations [4]. Furthermore, B is not a complete Boolean algebra. For example, the set X

of open intervals of the form $[0, a)$ where $a < \frac{\sqrt{2}}{2}$ has no least upper bound.

Represent this Boolean algebra as "sequences" of zeros and ones indexed by the continuum from 0 to 1. Then a typical element of X will appear as follows:

$$\left(1, 1, 1, 1, \cdots 1, \cdot\cdot 0, 0, 0, 0, 0, \cdot\cdot \frac{\sqrt{2}}{2} \cdot\cdot 0, 0, 0, 0, 0, \cdots\right).$$

A typical element of the set X^* of upper bounds of X will appear as

$$\left(1, 1, 1, 1, 1, \cdots\cdots 1, 1, 1, \cdot\cdot \frac{\sqrt{2}}{2} \cdot\cdot 1, 1, 0, 0, 0, \cdots\right).$$

and a typical element of the set Y of complements of elements of X^* will appear as

$$\left(0, 0, 0, \cdots\cdots\cdots 0, 0, \cdot\cdot \frac{\sqrt{2}}{2} \cdot\cdot 0, 0, 1, 1, 1, \cdots\right).$$

It is clear that the sets X and Y have the same cardinality since they are both infinite subsets of a countable set.

Let $x \rightarrow f(x)$ be any one-to-one correspondence between X and Y. Zemmer [7] has shown that in a p-space with B as Boolean algebra of idempotents there is a congruence which cannot be extended to a motion, between the sets A and C defined as follows: A contains 0, and for each x in X the element $x + f(x)$. C contains 0, and for each x in X the element $x + 2f(x)$. The congruence F between A and C takes 0 into 0 and $x + f(x)$ into $x + 2f(x)$. It will be shown, moreover, that in the 3-ring with B as Boolean algebra of idempotents the sets A and B are metric bases. Theorem 2.1 can be applied. Since $0 \in A$, it is clear that $\bigcap_{a \in A} d(a, 0)d(a, 2)$ and $\bigcap_{a \in A} d(a, 0)d(a, 1)$ are both equal to zero. However, since for any coordinate less than the $\sqrt{2}/2$th there is a 1 in x for some x in X and for any coordinate greater than the $\sqrt{2}/2$th there is a 1 in some y in Y and since $xy = 0$, $\bigcap_{a \in A} d(a, 1)$ (in the complete direct sum) is the atom with a 1 in the $\sqrt{2}/2$th coordinate, but since B itself is atom free, this implies that there are no elements z of B such that $z \subseteq \bigcap_{a \in A} d(a, 1)d(a, 2)$ and hence by Theorem 2.1 A is a metric basis. A similar argument shows that C is also a metric basis, which establishes the example.

3. Imbedding and characterization theorems.

DEFINITION 3.1. Let $\{S\}$ be a class of Boolean metric spaces. Then a Boolean metric space R is said to have *congruence indices*

(n, k) with respect to $\{S\}$ provided evey member of $\{S\}$ containing more than $n + k$ distinct points, is congruently imbeddable in R, whenever every n of its poinits are imbeddable in R.

DEFINITION 3.2. A space R is said to have *congruence order* n with respect to $\{S\}$ provided it has congruence indices $(n, 0)$ with respect to $\{S\}$.

(It is understood that the distance algebras of members of the comparison class are isomorphic with the distance algebra of the space R.)

The following series of theorems will establish that a p-space with Boolean algebra of idempotents B where B is a complete direct sum of $GF(2)$ has best congruence order $p + 1$ with respect to the class of all Boolean metric spaces (S, B, d). Theorem 3.4 generalizes a theorem due to Ellis [1].

LEMMA 3.1. *If A and B are congruent metric bases for a Boolean metric p-space R and if $f: A \to B$ is a congruence between the two sets, which can be extended to a motion, then the extension is unique.*

Proof. Suppose f and g are distinct motions which agree on A; then there is an $x \in R$ such that $f(x) \neq g(x)$. But for all $a \in A$,

$$\begin{aligned} d(f(x), f(a)) = d(x, a) &= d(g(x), g(a)) , \\ &= d(g(x), f(a)) , \end{aligned}$$

which contradicts the assumption that B is a metric basis.

LEMMA 3.2. *If A is a metric basis, for a Boolean metric p-space, and A and B are superposable then B is also a metric basis.*

Proof. Let f be a motion which takes A onto B. Suppose B is not a metric basis, then there are elements x, y, of R such that $x \neq y$, and $d(x, b) = d(y, b)$ for all $b \in B$. But then $d(f^{-1}(x), f^{-1}(b)) = d(f^{-1}(y), f^{-1}(b))$ for all $f^{-1}(b)$ in A, and since f^{-1} is, in particular, one-to-one, this contradicts the assertion that A is a metric basis.

COROLLARY. *If A is a finite metric basis for a Boolean metric p-space, and A and B are congruent, then B is also a metric basis.*

Proof. This follows immediately from the lemma and the corollary to Theorem 5 of [7].

If $\{S_1, S_2, \cdots, S_k\}$ and $\{t_1, t_2, \cdots, t_k\}$ are subsets of a Boolean metric space the statement

$S_1, S_2, \cdots, S_k \approx t_1, t_2, \cdots, t_k$ is to indicate that the mapping which takes S_i into t_i $(i = 1, 2, \cdots, k)$ is a congruence.

LEMMA 3.3. *If* $\{r'_1, r'_2, \cdots, r'_{p-1}\}$ *is a metric basis for a Boolean metric space and*

$$r'''_1, r'''_2, \cdots, r'''_{p-1}, x''' \approx r'_1, r'_2, \cdots, r'_{p-1}, x'$$
$$r'''_1, r'''_2, \cdots, r'''_{p-1}, y''' \approx r'_1, r'_2, \cdots, r'_{p-1}, y'$$

then

$$r'''_1, r'''_2, r'''_3, \cdots, r'''_{p-1}, x''', y''' \approx r'_1, r'_2, r'_3, \cdots, r'_{p-1}, x'y' .$$

Proof. Consider the unique motion which takes

$$\{r'_1, r'_2, \cdots, r'_{p-1}, x'\} \quad \text{into} \quad \{r'''_1, r'''_2, \cdots, r'''_{p-1}, x'''\} .$$

Such a motion exists since by the corollary to Theorem 5 of [7] any congruence between two finite sets can be extended to a motion. If $A \subset B$ and A is a metric basis, then B is also a metric basis. Hence $\{r'_1, r'_2, \cdots, r'_{p-1}, x'\}$ and $\{r'''_1, r'''_2, \cdots, r'''_{p-1}, x'''\}$ are superposable, and by the corollary to Lemma 3.2, $\{r'''_1, r'''_2, \cdots, r'''_{p-1}, x'''\}$ also forms a metric basis and then by Lemma 3.2 the congruence

$$r'''_1, r'''_2, \cdots, r'''_{p-1}, \cdots, x''' \approx r'_1, r'_2, \cdots, r'_{p-1}, x'$$

can be uniquely extended to a motion. Suppose that this motion takes y' into y^* where $y^* \neq y'''$. Then

$$r'''_1, r'''_2, r'''_{p-1}, y''' \approx r'''_1, r'''_2, \cdots, r'''_{p-1}, y^*$$

which contradicts the fact that $\{r'''_1, r'''_2, \cdots, r'''_{p-1}\}$, being congruent to a metric basis are themselves a metric basis by the corollary to Lemma 3.2.

THOREM 3.4. *A Boolean metric space S with distance algebra B is congruently imbeddable in the p-space R with Boolean algebra of idempotents B if*:

(i) *S contains $p - 1$ points congruent with a metric basis of R,*

(ii) *Every $p + 1$ points of S are congruently imbeddable in R.*

Proof. Let $\{\rho_1, \rho_2, \cdots, \rho_{p-1}\}$ be a $p - 1$ tuple of S congruent with $\{r_1, r_2, \cdots, r_{p-1}\}$ a metric basis in R, that is

$$\rho_1, \rho_2, \cdots, \rho_{p-1} \approx r_1, r_2, \cdots, r_{p-1} . \tag{1}$$

Let ρ_p be another point of S. Then there exists $\{r'_1, r'_2, \cdots, r'_{p-1}, r'_p\}$ in S, such that

$$(2) \qquad \rho_1, \rho_2, \rho_3, \cdots, \rho_p \approx r'_1, r'_2, \cdots, r'_p$$

and by the corollary to Lemma 3.2 $\{r'_1, r'_2, \cdots, r'_{p-1}\}$ is a metric basis.

Let $\zeta \in S$. Then again there exists $\{r''_1, r''_2, \cdots, r''_p, x''\} \in R$ such that

$$(3) \qquad \rho_1, \rho_2, \cdots, \rho_p, \zeta \approx r''_1, r''_2, \cdots, r''_p, x''$$

and therefore

$$(4) \qquad r'_1, r'_2, \cdots, r'_p \approx r''_1, r''_2, \cdots, r''_p \ .$$

Let x' be the image of x'' under the unique motion which preserves congruence (4). Thus there is defined a single-valued mapping $x' = x'(\zeta)$ of S into R, and

$$(5) \qquad \rho_1, \rho_2, \cdots, \rho_p, \zeta \approx r'_1, r'_2, \cdots, r'_p, x' \ .$$

It remains to show that distances are preserved.

Let $\zeta, \eta \in S$ and let x, y be the corresponding elements in R. Now

$$(6) \qquad \rho_1, \rho_2, \cdots, \rho_{p-1}, \zeta, \eta \approx r'''_1, r'''_2, \cdots, r'''_{p-1}, x''', y''' \in R$$

for some $p+1$ tuple $\{r'''_1, r'''_2, \cdots, r'''_{p-1}, x''', y'''\} \in R$. Then using Lemma 3.3, (5), (6) and the fact that $r'_1, r'_2, \cdots, r'_p, y' \approx \rho_1, \rho_2, \cdots, \rho_p, \eta$ it follows that

$$\rho_1, \rho_2, \cdots, \rho_{p-1}, \zeta, \eta \approx r'''_1, r'''_2, \cdots, r'''_{p-1}, x''', y''' \approx r'_1, r'_2, \cdots, r'_{p-1}x', y'$$

and hence $d(\zeta, \eta) = d(x', y')$.

THEOREM 3.5. *Let S be a Boolean metric space with distance algebra B, then every p-tuple of S is imbeddable in the p-space R with Boolean ring of idempotents B.*

COROLLARY. *Every finite Boolean metric space is imbeddable in a p-space, for some prime p.*

Proof. Let $\{s_1, s_2, \cdots, s_p\}$ be a p-tuple in S. Let q_{ij} denote $d(s_i, s_j)$. Consider the following set of $p-1$-tuples of elements of B:

$$s'_1 = (0, 0, \cdots, 0)$$
$$s'_2 = (q_{12}, 0, \cdots, 0)$$
$$s'_3 = (q_{13}\overline{q_{24}}, q_{13}q_{23}, 0, \cdots, 0)$$
$$s'_4 = (q_{14}\overline{q_{24}}, q_{14}q_{24}\overline{q_{34}}, q_{14}q_{24}q_{34}, 0, \cdots, 0)$$
$$s'_j = (q_{1j}\overline{q_{2j}}, q_{1j}q_{2j}\overline{q_{3j}}, q_{1j}q_{2j}q_{3j}\overline{q_{4j}}, \cdots, q_jq_{2j}\cdots\overline{q_{j-1,j}}, q_{1j}q_{2j}\cdots q_{j-1,j}, 0, \cdots, 0)$$
$$s'_p = (q_{1p}\overline{q_{2p}}, q_{1p}q_{2p}\overline{q_{3p}}, \cdots, q_{1p}q_{2p}\cdots\overline{q_{p-1,p}}, q_{1p}q_{2p}\cdots q_{p-1,p}) \ .$$

It is clear that the s_i' are $p-1$-tuples of pairwise orthogonal elements of B and therefore by Theorem 1 of [7] correspond to elements of R. It remains to show that the mapping $\lambda: s_i \rightarrow s_i'$ is an isometry. Let $q_{ij}' = d(s_i', s_j')$.

Consider the rings B and R in their subdirect sum representations. In order to show that λ is an isometry it is sufficient to show that q_{ij}' has a zero in a given component if and only if q_{ij} has a zero in that same component. Let Q_{ij} and Q_{ij}' represent the αth component of q_{ij} and q_{ij}', respectively. Let $\bar{S}_j$ represent the entry in the αth component of the subdirect sum representation of s_j'.

Assertion. $Q_{ij} = 0$ if and only if $Q_{ij}' = 0$.

It is clear that $Q_{1j} = 0$ if and only if $Q_{1j}' = 0$, $[j = 1, 2, \cdots, p]$. Suppose, therefore, that $i, j \neq 1$.

Suppose that $Q_{ij} = 0$ and assume without loss of generality that i is less than j. Then $\bar{S}_j$ is equal to x where $0 \leqq x \leqq i-1$. But if $\bar{S}_j = x-1$ where $1 < x < i$ then $Q_{tj} = 1$ for $t = 1, 2, \cdots, x-1$, and $Q_{xj} = 0$ which implies that $Q_{ni} = 1$ for $n = 1, 2, \cdots, x-1$. (For if $Q_{ni} = 0$ for some n, $[n = 1, 2, \cdots, x-1]$ then by the triangle inequality $Q_{ni} = 0$, $Q_{ij} = 0$ imply $Q_{nj} = 0$ which is a contradiction.) But then since $Q_{xj} = 0$, $Q_{ij} = 0$ imply $Q_{xi} = 0$, $\bar{S}_i = x-1$, and $Q_{ij}' = 0$.

Now, still under the hypothesis that $Q_{ij} = 0$ it remains to show, in order to complete the proof of the necessity of the assertion that if $S_j = 0$, then $\bar{S}_i = 0$. But if $\bar{S}_j = 0$, $Q_{1j} = 0$. (For suppose $\bar{S}_j = 0$ and $Q_{1j} = 1$, then there must be an r, $[r = 2, 3, \cdots, j-1]$ such that $Q_{rj} = 0$. But then by examining the term in s_j' involving Q_{rj} it is seen that there must be a v strictly less than r such that $Q_{vj} = 0$, and proceeding by induction $Q_{1j} = 0$, contrary to hypothesis). But $Q_{1j} = 0$ and $Q_{ij} = 0$ imply by the triangle inequality that $Q_{1i} = 0$ and hence $\bar{S}_i = 0$ which completes the proof of the necessity of the assertion.

To demonstrate the sufficiency of the assertion it must be shown that if $Q_{ij}' = 0$, then $Q_{ij} = 0$.

If $Q_{ij} = 0$, then $\bar{S}_i = \bar{S}_j = x$, where x is an integer mod p. Assume without loss of generality that $i < j$ and suppose $x \neq 0$, $i-1$. Then $Q_{x-1,j} = 0$, $Q_{x-1,i} = 0$ which together imply that $Q_{ij} = 0$. If $x = i-1$, it is clear from examining the term in S_j involving $\overline{Q_{ij}}$ that $Q_{ij} = 0$, and lastly if $x = 0$, $Q_{1j} = 0$, and $Q_{1i} = 0$; hence by the triangle inequality $Q_{ij} = 0$. This completes the proof of the theorem.

To clarify the proof, it seems worthwhile to establish the theorem without using the subdirect sum formulation, in a particular instance. Thus let $\{s_1, s_2, s_3\}$ be a Boolean metric triple. Then

$$s_1' = (0, 0) ,$$
$$s_2' = (q_{12}, 0) ,$$
$$s_3' = (q_{13}\overline{q_{23}}, q_{13}q_{23}) .$$

Since the sum of the coordinates in a Boolean vector representation is the distance from the origin it is clear that $q_{12} = q_{12}'$. By the same token

$$q_{13}' = q_{13}(q_{23} + \overline{q_{23}}) = q_{13} .$$

Lastly $q_{23}' = d(s_3' - s_2', 0)$. The Boolean vector representation of $s_3' - s_2'$ is (a_1, a_2) where

$$a_1 = q_{12}q_{13}q_{23} + q_{13}\overline{q_{23}}\,\overline{q_{12}}$$
$$a_2 = q_{12}q_{13}q_{23} + q_{12}\overline{q_{12}\overline{q_{23}}} + q_{13}q_{23}$$

so that $q_{23}' = a_1 + a_2$, which upon simplification gives

$$q_{23}' = q_{12} + q_{13} + q_{12}q_{13}q_{23}$$
$$= q_{23}$$

since in any Boolean metric space the product of the lengths of the sides of a triangle is equal to their sum.

Before indicating the procedure for imbedding $p + 1$-tuples, a definition of a chain of integers and some lemmas concerning these chains will be presented.

DEFINITION 3.3. Let i, j be positive integers such that $i \leqq j$. An (i, j) chain is any finite sequence of positive integers such that

(1) The sequence has exactly j terms,

(2) The first element in the sequence is 1, and the last is i,

(3) The terms in the sequence are selected from the integers $1, 2, \cdots, j$,

(4) If r and s are integers which occur in the sequence and r is less than s, then the first occurrence of r precedes the first occurrence of s. Every integer between r and s must occur if r and s occur.

Let $x_1, x_2, \cdots, x_j$ be an (i, j) chain. Define a metric on this chain by letting $d(x_a, x_b) = r_{ab} = 1$ if $x_a \neq x_b$ and $d(x_a, x_b) = r_{ab} = 0$ if $x_a = x_b$.

LEMMA 3.6. *Let $s_1, s_2, \cdots, s_v$ be a v-tuple in a Boolean metric space. Let $t_{ij} = d(s_i, s_j)$ and let T_{ij} denote the αth component in the subdirect sum representation of t_{ij}. Then there exists a unique (i, v) chain Γ such that $r_{ab} = T_{ab}$, $a, b = 1, 2, \cdots, v$.*

Proof. By induction on v. For $v = 1$ the theorem is trivially satisfied. Suppose then that $\{s_1, s_2, \cdots, s_k\}$ is a Boolean metric k tuple and $x_1, x_2, \cdots, x_k$ is the unique chain such that $r_{ab} = T_{ab}$. If $T_{w,k+1} = 1$ for $w = 1, 2, \cdots, k$, let x_{k+1} be the next integer not already used in the chain. This integer is uniquely determined and $r_{ab} = T_{ab}$ $a, b = 1, 2, \cdots, k+1$. On the other hand if $T_{\bar{w},k+1} = 0$ where $1 \leqq \bar{w} \leqq k+1$, let $x_{k+1} = x_{\bar{w}}$. x_{k+1} is uniquely determined, for if $T_{\bar{w},k+1} = 0$ and $T_{\bar{\bar{w}},k+1} = 0$, then by the triangle inequality $T_{\bar{w},\bar{\bar{w}}} = 0$ and so $x_{\bar{w}} = x_{\bar{\bar{w}}} = x_{k+1}$ and hence $r_{\bar{\bar{w}},k+1} = 0$. If $r_{a,k+1} = 0$, then $x_a = x_{k+1} = x_{\bar{w}}$, hence, $T_{a,\bar{w}} = 0$, which with the hypothesis $T_{\bar{w},k+1} = 0$, yields $T_{a,k+1} = 0$, which completes the proof.

DEFINITION 3.4. Let $\{p_1, p_2, \cdots, p_k\}$ be a finite subset of a Boolean metric space. Then the *distance product* of this subset is defined to be

$$\prod_{i \neq j} d(p_i, p_j) .$$

THEOREM 3.7. *Let S be a Boolean metric space with distance algebra B. Ap + 1-tuple K of S is imbeddable in the p-space R with Boolean ring of idempotents B if and only if the distance product of K is zero.*

Proof. The necessity is easily established. Let $\{t_1, t_2, \cdots, t_{p+1}\}$ be points of a p-space. In the αth component of the subdirect sum representation, each of the t_r must contain one of the elements of $GF(p)$. Thus in this αth component, for some c, d, t_c and t_d have the same element of $GF(p)$, and hence the distance product has a zero in the αth component. Since this is true for every α, the distance product of $\{t_1, t_2, \cdots, t_{p+1}\}$ is zero.

To establish the sufficiency of the condition, let $\{s_1, s_2, \cdots, s_j\}$ be a Boolean metric j-tuple and let C_{ij} be an arbitrary (i, j) chain. Denote by q_{ab} the distance $d(s_a, s_b)$ and let $C^*_{i\,j}$ be the product

$$\prod_{a,b \leqq j} g(q_{ab})$$

where $g(q_{ab}) = \overline{q_{ab}}$, if the ath and bth terms in C_{ij} are identical; $g(q_{ab}) = q_{ab}$, if the ath and bth terms in C_{ij} differ. Let $\{s_1, s_2, s_3, \cdots, s_{p+1}\}$ be a Boolean metric $p+1$ tuple with distance product zero. Define a set of $p-1$-tuples of B as follows:

$$t_J = (t_J^1, t_J^2, \cdots, t_J^I, \cdots, t_J^{P-1}) \qquad (J = 1, 2, \cdots, p+1)$$

where t_J^I is equal to zero if $I > J - 1$, otherwise t_J^I is the Boolean algebra union of all the elements of B of the form $C^*_{I+1,J}$.

Let T_J^I denote the αth component in the subdirect sum representation of t_J^I.

In order to show that the mapping $s_J \to t_J$ is a mapping into a p-ring, it is sufficient to establish that $T_J^n T_J^m = 0$, if $n \neq m$. But this follows at once from the fact that $T_J^n = 1$ if and only if there is an $(n+1, J)$ chain $x_1, x_2, \cdots, x_J$ such that the αth component of $d(s_a, s_b)$ is equal to $d(x_a, x_b)$ $[a, b = 1, 2, \cdots, J]$, for it follows from Lemma 3.6 that two (i, j) chains are isometric if and only if they are identical.

Since $T_J^I = 1$ if and only if t_J has an I in the αth component and also if and only if $\{s_1, s_2, \cdots, s_J\}$ is such that for a unique $(I+1, J)$ chain $y_1, y_2, \cdots, y_J$, $d(y_a, y_b)$ is equal to the αth component of $d(s_a, s_b)$, $(a, b = 1, 2, \cdots, J)$, it follows that $\{R_1 + 1, R_2 + 1, \cdots, R_{p+1} + 1\}$, where R_k is the αth component of t_k, is the unique chain such that $d(R_m + 1, R_n + 1)$ is equal to the αth component of $d(s_m, s_n)$ $(m, n = 1, 2, \cdots, p+1)$ and hence the αth component of $d(t_a, t_b) = 0$ if and only if the αth component of $d(s_a, s_b) = 0$. This completes the proof of the theorem.

Recall that if B is a Boolean ring, B^* designates the complete direct sum of those $GF(2)$ used in the subdirect sum representation of B.

LEMMA 3.8. *Let S be Boolean metric space with distance algebra B, in which the distance product of every $p+1$ points is zero. Then S is congruent with a subset of a Boolean metric space S^* with distance algebra B^*, such that B is isomorphic with a subalgebra of B^*, the distance product of every $p+1$ points of S^* is zero, and S^* contains an equilateral $p-1$-tuple of side 1.*

Proof. Let $\{t_1, t_2, \cdots, t_n\}$ be a maximal equilateral set of side 1 in S. If $n \geqq p-1$, no further proof is needed. If $n < p-1$, consider B in its subdirect sum representation and let B^* be the complete direct sum of the $GF(2)$ used to represent B. Let S^* be the set union of S and an element σ. Define a distance d' in S^* as follows: if $x, y \in S$, $d'(x, y) = d(x, y)$, $d'(\sigma, \sigma) = 0$. For $x \in s$, define $d'(x, \sigma) = q'_{x\sigma}$ by giving its αth component $Q'_{x\sigma}$ as follows: If for all $w \in S$, the αth component of $d(w, t_i) = 0$ for some $i = 1, 2, \cdots, n$ then $Q'_{x\sigma} = 1$ for all $x \in S$. If there is a w_α such that the αth component of $d(w_\alpha, t_i) = 1$ for all $i = 1, 2, \cdots, n$, then let $Q'_{x\sigma} = 0$ if and only if $d(x, w_\alpha)$ has a zero in the αth component.

To show that S^* is a Boolean metric space, observe that it is clear that if r, s are elements of S^*, with $r = s$, then $d'(r, s) = 0$. If $d'(r, s) = 0$, it is evident that $r = s$ if r and s are both elements of S. Suppose then that $d'(x, \sigma) = 0$ where $x \in S$. But then in the αth component $d(x, w_\alpha)$ has a zero, where w_α is such that the αth

component of $d(w_\alpha, t_i) = 1$ for $i = 1, 2, \cdots, n$, by the triangle inequality. Since this is true for every α, $\{t_1, t_2, \cdots, t_n, x\}$ is an equilateral set of side 1, contrary to hypothesis. The symmetry of d' follows at once from its definition. For the triangle inequality the only triples which need be studied are those of the form (x, y, σ). But, referring now to the αth component, if $d(x, y) = 0$, $d(y, \sigma) = 0$ then $d(y, w_\alpha) = 0$, hence $d(x, w_\alpha) = 0$ and $d(x, \sigma) = 0$ and if $d(x, \sigma) = 0$, $d(y, \sigma) = 0$ then $d(x, w_\alpha) = 0$, $d(y, w_\alpha) = 0$, and $d(x, y) = 0$. In all other cases $d(x, y)$, $d(x, \sigma)$, $d(y, \sigma)$ clearly form a metric triple, because x, y, σ, is a Boolean metric triple unless in some component two of $d(x, \sigma), d(y, \sigma), d(x, y)$ are equal to zero and the third is equal to one.

To show that $\{t_1, t_2, \cdots, t_n\}$ form an equilateral set of side 1, suppose this is not the case, then in some αth component, for some i, $d(\sigma, t_i) = 0$, but then $d(\sigma, w_\alpha) = 0$, hence $d(w_\alpha, t_i) = 0$, contrary to the definition of w_α.

In verifying that the distance product of every $p + 1$ points of S^* is zero, it is sufficient to consider $p + 1$ tuples $\{r_1, r_2, \cdots, r_p, \sigma\}$, $[r_i \in S]$ where in some αth component, the distance products of the r's is one. But if the αth component of $d'(r_i, \sigma)$ is one for $i = 1, 2, \cdots, p$, then either there is for every i, a j, $[j = 1, 2, \cdots, n]$ where $n < p - 1$, such that $d'(r_i, t_j)$ has a zero in the αth component (which implies that for some i, j, k, $d'(r_i, t_k)$, $d'(r_j, t_k)$ have zeros in the αth component and so $d'(r_i, r_j)$ has a zero in the αth component, contrary to hypothesis). On the other hand, if there exists a w_α such that in the αth component $d'(w_\alpha, t_j) = 1$ for all j, $[j = 1, 2, \cdots, n]$, and $d'(\sigma, r_i)$ has a 1 in the αth component, then $d'(w_\alpha, r_i)$ has a 1 in the αth component. But then $\{r_1, r_2, \cdots, r_p, w_\alpha\}$ is a $p + 1$ tuple in S with distance product different from zero.

Continuing in this manner a space containing an equilateral $p - 1$ tuple of side 1 is obtained.

THEOREM 3.9. *Let S be a Boolean metric space with distance algebra B and let R^* be the p-space with Boolean ring of idempotents B^*. The space S is congruently imbeddable in R^* if and only if the distance product of every $p + 1$ points of S is equal to zero.*

Proof. By hypothesis the distance product of every $p + 1$ points of S is zero. Then by Lemma 3.8, S is congruently contained in a Boolean metric space S^*, with distance algebra B^*, containing an equilateral $p - 1$ tuple of side 1, and in which the distance product of every $p + 1$ points is zero. By Lemma 3.7, every $p + 1$ points of S are imbeddable in R^*, and by Theorem 3.4, S^* is congruently imbeddable in R^*, and hence S is congruently imbeddable in R^*. This establishes the sufficiency of the condition and the necessity follows

immediately from Theorem 3.7.

COROLLARY 1. *S is congruently imbeddable in R^* if and only if every $p+1$ points of S are congruently imbeddable in the p-space R, with Boolean ring of idempotents B.*

COROLLARY 2. *R^* has congruence order $p+1$ with respect to the class of all Boolean metric spaces (S, B^*, d).*

LEMMA 3.10. *A p-space does not have congruence order p.*

Proof. Let M be a Boolean metric space of any cardinality in which the distance of every two distinct points is one. Then M has every p points imbeddable in a given p-space, but M itself need not be.

THEOREM 3.11. *A p-space R^*, with distance algebra B^* has best congruence order $p+1$ with respect to the class of all Boolean metric spaces.*

Proof. By Corollary 2 of Theorem 3.9 the best congruence order of R^* is less than or equal to $p+1$, but by Lemma 3.10 the congruence order is greater than p.

Another topic of interest in distance geometry is psuedo sets.

DEFINITION 3.5. A $p+1$ tuple T in a Boolean metric space is said to be a *pseudo-p-space $p+1$ tuple* if every p points of T are imbeddable in a p-space but T is not.

THEOREM 3.12. *A Boolean metric $p+1$ tuple is either imbeddable in a p-space or is a pseudo-p-space $p+1$ tuple.*

Theorem 3.9 gives a solution to the congruent imbedding problem of determining necessary and sufficient conditions in order that a Boolean metric space be isometric with a subspace of a p-space. In order to obtain a characterization of Boolean metric spaces themselves one method is to first categorize those subspaces of a given p-space which are themselves p-spaces among the class of all subspaces of the p-space. This is accomplished in the following two theorems.

THEOREM 3.13. *Let R be a Boolean metric p-space with distance algebra B. Let S be a subspace of R. Then a necessary and sufficient condition that S be a p-space is that:*

(1) *There exists a subalgebra $\bar{B}$ of B such that S contains an equilateral $p-1$ tuple with side 1 of $\bar{B}$: $\{t_1, t_2, \cdots, t_{p-1}\}$,*

(2) *There is a one-to-one correspondence between the elements of* S, *and the set of pairwise orthogonal* $p-1$ *tuples*: $\{c_1, c_2, \cdots, c_{p-1}\}$ *of elements of* $\bar{B}$, *such that for* $x \in S$, $d(x, t_i) = \overline{c_i}$.

Proof. The necessity is clear, since for any sub-p-space, $\{t_1, t_2, \cdots, t_{p-1}\}$ can be taken as summands of the identity and the c_i are then the "coordinates" in a Boolean vector representation.

Sufficiency. If the conditions of the theorem are satisfied the set of $p-1$ tuples of c's form a p-ring, which is a subring of the original ring.

THEOREM 3.14. *Let* S *be a Boolean metric space with distance algebra* B. *A necssary and sufficient condition that* S *be a* p*-space is that*:

(1) *The distance product of every* $p+1$ *points of* S *is zero and for some subalgebra* $\bar{B}$ *of* B

(2) S *contains an equilateral* $p-1$ *tuple of side* 1 *in* $\bar{B}$

(3) *There is a one-to-one correspondence between the elements of* S, *and the set of pairwise orthogonal* $p-1$ *tuples*: $\{c_1, c_2, \cdots, c_{p-1}\}$ *of elements of* $\bar{B}$, *such that for* $x \in S$, $d(x, t_i) = \overline{c_i}$.

Proof. By Theorem 3.9, S is a subspace of a p-space, but by Theorem 3.13, S is then a p-space.

4. **Properties of the group of motions.** This section is devoted to developing certain properties of the group of motion of p-spaces.

THEOREM 4.1. *In a* p*-space every rotation about the origin is a product of a finite number of involutions.*

Proof. Let R be a p-space and B its distance algebra. Let $x \to f(x)$ be a rotation about the origin on R, and M the matrix corresponding to f. Then $M = (a_{ij})$ is a $(p-1) \times (p-1)$ matrix with elements in B satisfying $a_{ik}a_{ij} = 0$, $j \neq k$, and $a_{ij}a_{kj} = 0$, $i \neq k$, and $MM' \neq I$, where $a_{ij} \in B$.

For $b \in B$, denote by b^r, the rth component of b in the subdirect sum representation of B, and define $M^{(r)} = (a_{ij}^r)$.

Then the set $\{M^{(r)}\}$, $r \in \mathscr{R}$, consists of at most $(p-1)!$ different matrices each of which is a permutation matrix. Clearly

$$M^{(r)} = M_1^{(r)} \cdot M_2^{(r)} \cdot \cdots M_{p-2}^{(r)}$$

where the elements on the right are transposition matrices.

Whence $M^{(r)}$ can be transformed into $M_k^{(r)}$ by a certain permutation of its columns.

Let M_{rk} be the matrix which results from applying these same column operations to M.

Let Z_r be the product of those elements in M corresponding to the 1's in $M^{(r)}$. Let $Z_r^{(s)}$ be the sth component of Z_r, and note that $Z_r^{(s)} = 1$ if and only if $M^{(r)} = M^{(s)}$.

Let M_{rk}^* be the matrix obtained from M_{rk} by multiplying every element by z_r and then adding $\bar{Z}_r$ to the elements along the main diagonal, i.e., $M_{rk}^* = Z_r M_{rk} + \bar{Z}_r I$.

Denote the matrix of tth components of M_{rk}^* by $M_{rk}^{*(t)}$.

It follows that:

$$M_{rk}^{*(t)} = M_k^{(r)} \quad \text{if} \quad M^{(r)} = M^{(t)}$$
$$M_{rk}^{*(t)} = I \quad \text{if} \quad M^r \neq M^t .$$

(From the definition of M_{rk}^*, if $M^{(r)} = M^{(t)}$, $M_{rk}^{*(t)} = M_{rk}^{(t)}$, and from the definition of M_{rk}, $M_{rk}^{(t)} = M_{rk}^{(r)}$, which is equal to $M_k^{(r)}$ by the definition of $M_k^{(r)}$, that is, $M_{rk}^{*(t)} = M_k^{(r)}$).

Thus

$$\prod_k M_{rk}^{*(t)} = M^{(r)} \quad \text{if} \quad M^{(r)} = M^{(t)}$$
$$\prod_k M_{rk}^{*(t)} = I \quad \text{if} \quad M^{(r)} \neq M^{(t)} \qquad (k = 1, 2, \cdots, p-2) .$$

Now select a minimal set of $r's$, $L = (r_1, r_2, \cdots, r_m)$ such that each $M^{(r)} = M^{r_j}$ for some $r_j \in L$. Then

$$M = \prod M_{r_j k}^* \qquad (k = 1, 2, \cdots, p-2, r_j \in L) .$$

To show this, observe that

$$M^{(\lambda)} = \prod M_{r_j k}^{*(\lambda)} \qquad (k = 1, 2, \cdots, p-2, r_j \in L) .$$

Let $r_\beta \in L$ be such that $M^{(\lambda)} = M^{(r_\beta)}$. Then

$$\begin{aligned} \prod M_{r_j k}^{*(\lambda)} &= (\prod M_{r_\beta k}^{*(\lambda)})(\prod_{j \neq \beta} M_{r_j k}^{*(\lambda)}) \\ &= M^{(r_\beta)} \cdot I \\ &= M^{(r_\beta)} = M^{(\lambda)} . \end{aligned}$$

COROLLARY. *Every motion which leaves zero fixed in a 3-space is a reflection. Every reflection in a 3-space therefore has determinant equal to* -1.

The proof of Theorem 4.1. suggests that there is a close relationship between the group of motions of a p-space, and permutation groups. Indeed it is the case that the group of motions is a subgroup

of the direct product of permutation groups on $p-1$ letters. This will be made precise in the following two theorems.

DEFINITION 4.1. Let B be a Boolean ring. Consider B as a subdirect sum of $GF(2)$. Let φ be a group of permutations on p-symbols and G_φ the full direct product of φ of the same cardinality and number of summands as B. For $b \in B$, and $P \in \varphi$, let $g(P, b)$ be the element of G_φ, which effects the permutation P where b has 1's and the identity permutation elsewhere. Denote by $G_\varphi(B)$ the subgroup of G_φ generated by the set of elements $g(P, b)$, $P \in \varphi$, $b \in B$.

THEOREM 4.2. *Let R be a p-space with Boolean ring of idempotents B. Then the group of motions of R which leave zero fixed is $G_T(B)$ where T is the symmetric group on $p-1$ symbols.*

Proof. Let M be a motion matrix for R. In the proof of Theorem 4.1 it was shown that M can be written as a product of matrices $M^*_{r_jk}$, but these matrices correspond to motions of the form $g(t, b)$ where t is a transposition.

COROLLARY. *Let R be a p-space. Then the group of motions of R is $G_S(B)$, where S is the group of permutations on p symbols.*

Proof. Let $f(x)$ be a motion, then $f(x) = xM + b$. It has been shown in the theorem that the rotation is an element of $G_T(B)$ and hence of $G_S(B)$. Consider now the translation $t(x) = x + t$. It can be written as the product of translations as $t_1(x) \cdot t_2(x) \cdot \cdots, \cdot t_{p-1}(x)$ where $t_i(x) = x + i(1 - (t - i))^{p-1}$ which are elements of $G_S(B)$.

On the other hand it must be shown that every element of $G_S B$ is a motion. It suffices to show that every $g(P, b)$ is a motion. Thus let $g(P, b)$ be given. If P fixes zero, the result follows from the theorem. If P does not fix zero, let $0'$ be the image of zero under P. Consider the permutation q: $x \to x - 0'$ of the integers mod p. Then $g(pq, b)$ is a motion and has a matrix M, and $f(x) = xM + 0'b$ corresponds to $g(p, b)$.

THEOREM 4.3. *Let R be a 3-space with Boolean ring of idempotents B. Then every motion f on R which leaves 0 fixed is of the form $f(x) = ax$ where a is a unit in the 3-ring.*

Proof. It follows from Theorem 4 of [7] that $f(x) = xM$ where $M = (a_{ij})$ $i, j = 1, 2$, and $a_{ij} \in B$. Further

$$M = \begin{pmatrix} a & 1 + a \\ 1 + a & a \end{pmatrix}$$

Suppose then that $x = (x_1, x_2)$, and so

$$f(x) = (ax_1 + (1 + a)x_2, (1 + a)x_1 + ax_2)$$
$$= (x_1, x_2)\cdot(a, 1 + a)$$

where $(a, 1 + a)(a, 1 + a) = (1, 0) = 1$.

5. **Analytic geometry in p-spaces.** If a rectangular coordinate system is introduced in a Euclidean plane E, a point P can be represented as a pair (x, y) of real numbers. One then seeks to describe geometrically the loci of equations of the form $y = f(x)$, and conversely, given a geometric description of a plane set, to find the equation of which it is the corresponding locus. But a point P in the Euclidean plane may also be considered to be represented by the single complex number $z = x + iy$. Here the question is not so much the investigation of the loci of equations of the from $f(z) = 0$; a study is rather made of the way in which geometric properties change or remain invariant under transformations $w = f(z)$ of the plane into itself. It is the purpose of the following remarks to exhibit theorems which illustrate that an analytic geometry for p-spaces may be developed in a manner analogous with both of the methods discussed above for Euclidean plane geometry.

Suppose, therefore, that R is a p-space. Since the elements of the p-ring R are in one-to-one correspondence with the points of the p-space R, every function $f(x)$ defined for all x in the p-ring R and having values in the p-ring R induces a mapping of the p-space R into itself. This mapping need not of course preserve distances, and in general will not even be one-to-one. Theorem 5.2 establishes necessary and sufficient conditions that a polynomial function defined on a p-ring R induce a motion on the corresponding p-space.

The following theorem, which was first established in 1882 is needed for the proof.

THEOREM 5.1. *Raussnitz* [6]. *Let* $f(x) = a_{-1}x^{p-1} + a_0x^{p-2} + a_1x^{p-3} + \cdots + a_{p-2}$ *be a polynomial where* $a_i \in GF(p)$, $(i = -1, 0, 1, 2, \cdots, p-1)$. *Then a necessary and sufficient condition that* $f(0), f(1), \cdots, f(p-1)$ *be distinct is that* (i) *the determinant* $R(k)$ *be equal to zero for* $k = 0, 1, \cdots, a_{p-2} - 1, a_{p-2} + 1, \cdots, p - 1$ *where*

$$R(k) = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_{p-3} & a_{p-2} - k \\ a_1 & a_2 & a_2 & & a_{p-2} - k & a_0 \\ \cdots\cdots & & & & & \\ \cdots\cdots & & & & & \\ a_{p-2} - k & a_0 & a_1 & & a_{p-4} & a_{p-3} \end{vmatrix}$$

and (ii) $a_{-1} = 0$.

THEOREM 5.2. *Let R be a p-space. Then a necessary and sufficient condition that the polynomial*

$$P(x) = a_{-1}x^{p-1} + a_0x^{p-2} + a_1x^{p-3} + \cdots + a_{p-2},$$

where the a_i $(i = -1, 0, 1, \cdots, p-1)$ are elements of the p-ring R, induce a motion on the p-space R is that

(i) $a_{-1} = 0$

and

(ii) $\bar{R}(c_k) = 0$ $(k = 0, 1, 2, \cdots, p-1)$ *where*

$$\bar{R}(c_k) = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_{p-3} & a_{p-2} - c_k \\ a_1 & a_2 & a_3 & & a_{p-2} - c_k & a_0 \\ \cdots\cdots & & & & & \\ \cdots\cdots & & & & & \\ a_{p-2} - c_k & a_0 & a_1 & & a_{p-4} & a_{p-3} \end{vmatrix}$$

and $c_k = -(a_{p-2} - k)^{p-1} + k + 1$. (Note that $R(k)$ has integer arguments whereas the arguments of $\bar{R}(c_k)$ are elements of a p-ring).

Proof. Suppose that the polynomial $P(x)$ corresponds to a motion M on the p-space R, and consider the p-ring R as a subdirect sum of $GF(p)$. Then the elements of R may be represented as $(r_1, r_2, \cdots, r_t, \cdots)$ where the $r_t \in GF(p)$. Clearly M induces a permutation p_t on the components r_t, for every t. If for $x_1 \in R$ and $x_2 \in R$, $r_t^1 = r_t^2$ and $M(r_t^1) \neq M(r_t^2)$, then $d(x_1, x_2)$ will have a zero in its tth component while $d(M(x_1), M(x_2))$ will have a one in the tth component contradicting the assumption that M is distance preserving. The uniqueness of p_t is a consequence of the fact that the motion M is a well defined mapping. Let $a_{j,t}$ be the tth component of a_j in the subdirect sum representation of R. Then the polynomial

$$P_t(x) = a_{-1,t}x^{p-1} + a_{0,t}x^{p-2} + a_{1,t}x^{p-3} + \cdots + a_{p-2,t}$$

must represent the permutation p_t on the elements of $GF(p)$. Hence by Theorem 5.1, $a_{-1,t} = 0$, for all t, so that $a_{-1} = 0$. Also, $R(k_t) = 0$ for all t, and $k = 0, 1, 2, \cdots, a_{p-2} - 1, a_{p-2,t} + 1, \cdots, p-1$. Notice however that $c_{k,t}$ ranges over $0, 1, 2, \cdots, a_{p-2,t} - 1,, a_{p-2,t} + 1, \cdots, p-1$ as k takes on the values $0, 1, \cdots, p-1$. Thus $\bar{R}(c_k) = 0$, for $k = 0, 1, 2, \cdots, p-1$, and the necessity of conditions (i) and (ii) is established.

On the other hand, suppose that conditions (i) and (ii) are satisfied by $P(x)$. It will first be shown that the polynomial $P^*(x)$ where

$P^*(x) = P(x) - a_{p-2}$ also satisfies conditions (i) and (ii). For each t, the polynomial $P_t(x)$ satisfies the conditions of Theorem 5.1 and hence $P(x)$ induces a permutation p_t on the tth component of the subdirect sum representation of the p-ring R. But in each component $P^*(x)$ also induces a permutation and since conditions (i) and (ii) of Theorem 5.1 are necessary conditions, $P^*(x)$ satisfies conditions (i) and (ii) of Theorem 5.2. It is clear that if $P^*(x)$ is a motion, so also is $P(x)$, and thus it is sufficient to consider polynomials $P(x)$ for which $a_{p-2} = 0$.

Since there are only a finite number of different permutations on the elements of $GF(p)$, it is possible to choose a finite set of distinct permutations

$$\{q_1, q_2, \cdots, q_s\} = \Gamma$$

in such a way that for each t, p_t is equal to one of the q_j. Note that $1 \leqq s \leqq p!$. Now, with each permutation q_j, there is associated at most a finite number of polynomials

$$Q_{jk}(x) = i_{0,k}^{(j)}x^{p-2} + i_{1,k}^{(j)}x^{p-3} + \cdots + i_{p-2,k}^{(j)}x \qquad [k = 1, 2, \cdots, w_j]$$

in $GF(p)$ $[x]$ which satisfy the conditions of Theorem 5.1 and such that $q_j(i) = Q_{jk}(i)$, $i = 0, 1, \cdots, p-1$, $k = 1, 2, \cdots, w_j$.

Define b_{j_k}, an element in the Boolean ring of idempotents, as follows:

$$b_{j_k} = (a_0 - i_{0,k}^{(j)})^{p-1} \cup (a_1 - i_{1,k}^{(j)})^{p-1} \cup \cdots \cup (a_{p-3} - i_{p-3,k}^{(j)})^{p-1} .$$

This element has a zero in those components t of the subdirect sum representation of the Boolean ring of idempotents, where

$$a_{h,t} = i_{h,k}^{(j)} \qquad [h = 0, 1, \cdots, p-3]$$

and has a 1 in the other components. Let

$$b_j = 1 + \prod_{k=1}^{w_j} b_{j_k} ,$$

and note that b_j has a 1 in those components t where the permutation $q_j = p_t$ and zeros elsewhere.

Define a matrix $M = (m_{ij})$ as follows:

$$m_{ij} = b_{j_1} + b_{j_2} + \cdots + b_{j_v}$$

where $q_{j_1}, q_{j_2}, \cdots, q_{j_r}, \cdots, q_{j_v}$ are those elements of Γ which satisfy $q_{j_r}(i) = j$, and $m_{ij} = 0$ if there are no such permutations in Γ. It can be seen that m_{ij} has a 1 in the tth component if and only if $P_t(i) = j$. Since the b_j are pairwise orthogonal and a permutation is a one-to-one onto map, it is clear that M satisfies the conditions for a motion matrix and $P(x) \equiv xM$.

To illustrate the second point of view in analytic geometry reference will be made to the particular instance of a 3-space, although similar results could be obtained for larger primes.

It follows from the Boolean vector representation of p-rings that a 3-ring can be represented as the set of all pairwise orthogonal ordered pairs (x, y) of elements from its Boolean ring of idempotents. Thus the pair (x, y) can be considered as coordinates for points in the 3-space. The locus of all points of the 3-space, whose coordinates satisfy an equation of the form $Ax + By + C = 0$, where $A \cup B = 1$, is called a *linear set*. (The indicated operations are those of the Boolean ring of idempotents).

THEOREM 5.3. *A linear set is a circle of radius* $A + B + C$.

Proof. Denote by Ω the linear set associated with the equation $Ax + By + C = 0$. Then if $(x, y) \in \Omega$,

$$d[(x, y), (1 + B, 1 + A)] = A + B + C .$$

For

$$\begin{aligned} d[(x, y), (1 + B, 1 + A)] &= d[((1 + B, 1 + A) - (x, y)), 0] \\ &= d[(c, d), 0] = c + d \end{aligned}$$

where

$$\begin{aligned} c &= (1 + A)x + y(1 + A + 1 + B + 1) + (1 + B)(1 + x + y) \\ d &= (1 + B)y + x(1 + A + 1 + B + 1) + (1 + A)(1 + x + y) \end{aligned}$$

hence

$$c + d = Ax + By + A + B = A + B + C .$$

Also if $d[(1 + B, 1 + A), (x, y)] = A + B + C$ then from the above

$$[d(x, y), (1 + B, 1 + A)] = Ax + By + A + B$$

and hence $Ax + By + C = 0$.

COROLLARY. *The form* $A + B + C$ *is a complete set of invariants for linear sets under motions.*

The following theorem illustrates a connection between the geometry of a p-space and the geometry of its Boolean ring of idempotents.

THEOREM 5.4. *If* R *is a* p*-space and* B *the corresponding Boolean ring of idempotents, then* B *itself is a Boolean metric space and is isometric to the set of idempotents of* R*, considered as a sub-*

space of R. Further, any motion on B, can be extended to a motion on R.

Proof. In an autometrized Boolean ring, the distance between two elements is the ring sum. But if x and y are idempotents in a ring their sum in the Boolean ring of idempotents is $x + y - 2xy$. But it is easy to see that if x and y are idempotents in a p-ring $x + y - 2xy = (x - y)^{p-1}$. Hence the distance between two idempotents is the same, whether the set of idempotents is considered as a subspace of the p-space, or as forming a Boolean ring itself.

If f is a motion on B, then the motion $f^*(x) = xM + f(0)$ is a motion on R which coincides with f on B, where the matrix $M = (m_{ij})$ is defined as:

$$m_{11} = m_{p-1,p-1} = \overline{f(0)}\,, \qquad m_{1,p-1} = m_{p-1,1} = f(0)\,,$$

$m_{ii} = 1$ for $i \neq 1, p-1$, and all other elements in the matrix equal to zero.

REFERENCES

1. David Ellis, *Autometrized Boolean algebras I, II*, Canadian J. Math. **3** (1951), 87-93 and 145-147.

2. ———, *Geometry in abstract distance spaces*, Mathematical Publications (Debrecen), (1951), 1-25.

3. R. F. Keller, *A lattice valuation for simple and semi-simple algebras*, Doctoral Dissertation, University of Missouri (1962).

4. C. J. Penning, *Boolean Metric spaces*, Doctoral Thesis, Technische Hogeschool te Delft, (1960).

5. G. Raussnitz, *Zur theorie der congruenzen hoheren grades*, Mathematische und Naturwissenschaftliche Berichte aus Ungarn, **I** (1882-1883), 266-278.

6. M. H. Stone, *The theory of representations for Boolean algebras*, Trans. Amer. Math. Soc. **40** (1936), 37-111.

7. J. L. Zemmer, *Some remarks on p-rings and their Boolean geometry*, Pacific J. Math., **6** (1956), 193-208.

UNIVERSITY OF RHODE ISLAND