A METRIZATION FOR POWER-SETS WITH APPLICATIONS TO COMBINATORIAL ANALYSIS

ROBERT SILVERMAN

1. Introduction. Combinatorial configurations may generally be phrased in terms of arrangements of objects into sets subject to certain conditions. In view of this, the question arises as to whether given a set S and its power-set U_S (the class of all subsets of S), it might be possible to structure U_S in a combinatorially significant manner. This paper proposes and investigates one such structuring achieved by defining a distance function over U_S.

Given A, B in U_S, define their *distance* by

$$d(A, B) = N([A \cup B] - [A \cap B])/2,$$

where $N(E)$ denotes the number of elements in E, $+ \infty$ being an admissible value. One readily verifies that the distance function satisfies the metric postulates $d(A, B) = 0$ if and only if $A = B$, and $d(A, B) \leqslant d(A, C) + d(B, C)$ for all A, B, C in U_S **(15)**. More generally, we may define a higher dimensional metric by associating with every r-tuple $E_1, \ldots, E_r$ of elements of U_S, the number $d(E_1, \ldots, E_r) = N(\cup A_i - \cap A_i)/r$. Although it appears that this will be necessary in order to obtain metric characterizations of, for example, the theorem of Desargues, only the ordinary metric is studied here.

Given the sets $S_1, \ldots, S_k$, denote by

$$\pi S_i = S_1 \times S_2 \times \ldots \times S_k = \{(s_1, \ldots, s_k); s_i \in S_i\},$$

their Cartesian product of ordered k-tuples. Since πS_i may be viewed as a subclass of an appropriate power-set by identifying the *element* $(s_1, \ldots, s_k)$ with the *set* $\{(1, s_1), \ldots, (k, s_k)\}$, the above definition also yields a metrization for Cartesian products which may be restated: For x, y in πS_i, $x = (x_1, \ldots, x_k)$, $y = (y_1, \ldots, y_k)$, $d(x, y)$ is the number of subscripts i for which $x_i \neq y_i$, $i = 1, \ldots, k$.

Section 3 gives metric characterizations of some of the classical configurations and their generalizations, such as balanced incomplete block designs (and, in particular, v, k, λ configurations and projective planes) and orthogonal Latin squares and cubes. Section 4 sets forth some theorems for metrized Cartesian product spaces.

2. Definitions and notation. In order to reduce to a minimum the introduction of new terminology, wherever feasible the author has adopted

that used by Blumenthal **(4; 5)**, whose excellent books also nourished several interesting trains of thought. In the following, M denotes an abstract metric space, and E a subspace of M. Wherever applicable, $+ \infty$ is regarded as an admissible value.

DEFINITION 1. If $M = \{a_1, a_2, \ldots,\}$ is countable, it may be completely specified by the symmetric *distance matrix*

$$A = [a_{ij}], a_{ij} = d(a_i, a_j).$$

DEFINITION 2. For a in M, $r > 0$, the *open sphere* and *closed sphere with centre a, radius r* are defined, respectively, by

$$s(a, r) = \{x; x \text{ in } M, d(x, a) < r\},$$

$$c(a, r) = \{x; x \text{ in } M, d(x, a) \leqslant r\}.$$

Note that in general a sphere need not have a unique centre or radius.

DEFINITION 3. For x in M, the *distance of x from E* is given by $d(x, E) = $ g.l.b. $d(x, y)$ for y in E.

DEFINITION 4. Two metric spaces M and M' are *isometric* provided there exists a mapping α from M onto M' such that $d(x, y) = d(\alpha(x), \alpha(y))$ for all x, y in M. We write $M \sim M'$. Note that α is biunique since $\alpha(x) = \alpha(y)$ implies $d(\alpha(x), \alpha(y)) = d(x, y) = 0$. If $M = M'$, the isometry is termed a *motion*. Two subsets of M are *superposable* provided a motion exists that maps one onto the other.

DEFINITION 5. E is a *metric basis* of M provided each point of M is uniquely determined by its distances from the points of E.

DEFINITION 6. The *major diameter* $\Delta(E)$, of E, and the *minor diameter* $\delta(E)$, of E are defined by

$$\Delta(E) = \text{l.u.b. } d(x, y) \text{ for } x, y \text{ in } E,$$

$$\delta(E) = \text{g.l.b. } d(x, y) \text{ for } x, y \text{ in } E, x \neq y.$$

If E contains fewer than two points, define $\delta(E) = 0$.

Combinatorial configurations generally are highly symmetric in various aspects of their structure. Searching for a means of obtaining some sort of "symmetrizing" condition in U_S, it was discovered that one way of achieving this is to require that U_S contain a "large" number of elements mutually "far apart." These considerations motivate the next definition.

DEFINITION 7. The *t-extent* of E, $e(E, t)$, is the greatest integer m such that E contains m distinct points with minor diameter greater than t. If no two points of E have distance greater than t, set $e(E, t) = 1$, while if for n arbitrarily large there are n points of E with minor diameter exceeding t, define $e(E, t) = + \infty$.

As we shall see in the next section, the concept of t-extent enables us to give simple metric characterizations of the various configurations examined there.

Let $S(n)$ denote a set of n elements $(n > 1)$, and $S^k(n)$ $(k \geqslant 1)$ the k-fold Cartesian product of $S(n)$,

$$S^k(n) = \{(x_1, \ldots, x_k); x_i \in S(n)\}.$$

Assume that $S^k(n)$ has been metrized as in the preceding section, so that for x, y in $S^k(n)$, $x = (x_1, \ldots, x_k)$, $y = (y_1, \ldots, y_k)$, $d(x, y)$ is the number of subscripts i for which $x_i \neq y_i$, $i = 1, \ldots, k$. For $0 \leqslant r \leqslant k$, every set of $n^r + 1$ elements of $S^k(n)$ has minor diameter at most $k - r$. Hence the $k - r$ extent of every subspace E of $S^k(n)$ satisfies $e(E, k - r) \leqslant n^r$. We next define terms to describe subspaces which attain this maximum extent.

DEFINITION 8. A subspace E of $S^k(n)$ is *r-orthogonal*, $0 \leqslant r \leqslant k$, provided $e(E, k - r) = n^r$. If in addition E contains precisely n^r elements, E is termed an $L(n, k, r)$ space. (Thus E is r-orthogonal if and only if E contains an $L(n, k, r)$ space.)

For a given subspace E, r-orthogonality does not imply $(r - 1)$-orthogonality. $S^k(n)$ always has orthogonality 0, 1, and k. Indeed, any point constitutes an $L(n, k, 0)$ space; the points $(i, i, \ldots, i)$, $i = 1, \ldots, n$ comprise an $L(n, k, 1)$ space, and $S^k(n)$ is itself an $L(n, k, k)$ space. For values between 1 and k the property becomes non-trivial, and, as we shall see in the following section, is related to some of the classical unsolved problems in combinatorial analysis.

3. Metric characterizations of some combinatorial configurations.

(a) *Latin squares and cubes.* A *Latin square of order n*, $A = [a_{ij}]$, is an $n \times n$ matrix whose entries are from a set of n distinct symbols and such that each symbol appears exactly once in each row and column. Thus a Latin square of order n is essentially the multiplication table of a loop of order n. Two Latin squares $A = [a_{ij}]$, $B = [b_{ij}]$ of order n are *Graeco-Latin* provided the n^2 ordered pairs (a_{ij}, b_{ij}) are all distinct. A set of Latin squares of order n, $A_1, A_2, \ldots, A_m$, is *orthogonal* provided A_i and A_j are Graeco-Latin for all $i \neq j$. In this event, one readily shows that $m \leqslant n - 1$. An orthogonal set is *complete* provided $m = n - 1$.

A *Latin cube of order n*, $A = [a_{ijk}]$, i sa cubical array of n^3 cells (in n row-planes, n column-planes, and n layers) whose entries are from a set of n distinct symbols and such that whenever $a_{rst} = a_{uvw}$ and at least two of the equalities $r = u$, $s = v$, $t = w$ hold, then the third also holds. Note that this condition holds if and only if each row-plane, column-plane, and layer is a Latin square of order n. Two Latin cubes of order n are *Graeco-Latin* provided every pair of corresponding row-planes, column-planes, and layers is a Graeco-Latin square. Three Latin cubes, $A = [a_{ijk}]$, $B = [b_{ijk}]$, $C = [c_{ijk}]$,

of order n are *strongly Eulerian* provided each pair is Graeco-Latin and the n^3 ordered triples $(a_{ijk}, b_{ijk}, c_{ijk},)$ are all distinct. (These conditions are stronger than those of Ball **(2)**.) A set of pairwise Graeco-Latin cubes of order n, $A_1, \ldots, A_m$, is *orthogonal* provided A_i, A_j, A_k are strongly Eulerian for all i, j, k pairwise distinct. Again one readily shows that $m \leqslant n - 1$, and an orthogonal set is termed *complete* provided $m = n - 1$.

There exists a fairly extensive literature on Latin squares. (In this connection, see the fine historical review by Norton **(19)**.) Euler conjectured that for $n = 4k + 2$, Graeco-Latin squares of order n do not exist, and Tarry **(25)** verified this for $n = 6$. Aside from $n = 6$ ($n = 2$ is, in a sense, vacuous since a complete set consists of a single square), the question of the validity of the conjecture has resisted all determined onslaught (although Mann **(17)** has ruled out certain candidates, among these being the group multiplication tables). The case $n = 10$ remains the first undecided instance.[1] MacNeish **(16)** seems to have been the first to establish the existence of complete sets of orthogonal Latin squares of prime power order. The interest in orthogonal Latin squares and finite projective planes was mutually enhanced when Bose **(6)** and Levi **(14)** independently showed the equivalence of complete sets of such squares to the planes.

Given a set of orthogonal Latin squares $A_1, \ldots, A_m$, of order n, construct the associated n^2 k-tuples ($k = m + 2$) in the usual manner. (Here the k-tuple $(i_1, \ldots, i_k)$ is admitted if and only if i_j is in row i_{k-1}, column i_k of $A_j, j = 1, \ldots, k - 2$.) One readily verifies that these n^2 elements actually comprise an $L(n, k, 2)$ space, since any pair of the elements having at least two corresponding components equal would violate either the Latin condition on rows or columns, or the orthogonality condition. Thus the minor diameter of the n^2 elements exceeds $k - 2$. Conversely, given an $L(n, k, 2)$ space, we may reverse the process and obtain $k - 2$ orthogonal Latin squares of side n. The same procedure may be employed to show the equivalence of $L(n, k, 3)$ spaces and sets of $k - 3$ orthogonal Latin cubes.

(b) *Finite nets.* For k, n positive integers with $k \geqslant 3$, Bruck **(9)** defines a (finite) net N of degree k, order n, as "a system of undefined objects called 'points' and 'lines' together with an incidence relationship ('point is on line' or 'line passes through point') such that:

(i) N contains k (non-empty) classes of lines.

(ii) Two lines a, b of N belonging to distinct classes, have a unique common point P.

(iii) Each point P of N is on exactly one line of each class.

(iv) Some line of N has exactly n distinct points.

"A finite affine plane with n points on each line, $n \geqslant 2$, is simply a net of degree $n + 1$, order n **(13)**. A loop of order n is essentially a net of degree 3, order n **(1; 3)**. More generally, for $3 \leqslant k \leqslant n + 1$, a set of $k - 2$ mutually

---

[1]See the addendum for recent developments.

orthogonal $n \times n$ Latin squares may be used to define a net of degree k, order n (and conversely) by paralleling Bose's correspondence **(6)** between affine planes and complete sets of orthogonal Latin squares.''

For $k > r > 1$ we may generalize Bruck's configuration to a finite net of degree k, order n, and dimension r by replacing (ii) and (iv) with

(ii') Every r lines $l_1, \ldots, l_r$ of N belonging to pairwise distinct classes have a unique common point P.

(iv') Some line of N has exactly n^{r-1} points.

As immediate consequences of the axioms we have

(1) Every class contains n lines.

(2) Every line has exactly n^{r-1} points.

(3) N contains n^r points.

For let $A_1, \ldots, A_r, A_{r+1}, \ldots, A_k$ be the k classes of lines of N, and suppose A_i contains m_i lines, and N contains m points. One readily shows m_i and m to be finite. Then from (ii') and (iii) we obtain the system of $r + 1$ equations $\pi m_j = m (j = 1, \ldots, r + 1, j \neq i; i = 1, \ldots, r + 1)$ which have the unique solution $m_i = m^{1/r}$, $i = 1, \ldots, r + 1$, and since we may replace A_{r+1} by any other A_j, we obtain $m_i = m^{1/r}$, $i = 1, \ldots, k$. If we next consider any fixed line of A_1 together with the classes $A_2, \ldots, A_r$, then (ii') and (iii) imply that the line passes through $m^{(r-1)/r}$ points, and this together with (iv') implies $m = n^r$.

Now let us co-ordinatize N by assigning to the point P the co-ordinates $(i_1, \ldots, i_k)$ provided P is on the i_jth line of the jth class. Then (ii') and (iii) imply that there is a 1-1 correspondence between points and co-ordinates, and that as elements of $S^k(n)$ any two of these ordered k-tuples have distance exceeding $k - r$. Since there are n^r distinct such k-tuples, and each component of a k-tuple can assume n values, the n^r k-tuples comprise an $L(n, k, r)$ space. Conversely, one may reverse the above process, and we thus have a correspondence between $L(n, k, r)$ spaces with $1 < r < k$ and finite nets of degree k, order n, dimension r. In particular then, an $L(n, 3, 2)$ space is essentially a loop of order n, an $L(n, n + 1, 2)$ space defines a finite affine plane with n points on each line $(n \geqslant 2)$, and from an $L(n, k, 2)$ space we may construct a system of $k - 2$ orthogonal Latin squares of side n.

(c) *Hypercubes and orthogonal arrays.* Rao **(21)** defines a hypercube of strength d as follows: "Let there be m factors $A_1, A_2, \ldots, A_m$ each of which can assume s different values. We define an ordered set $(i_1, i_2, \ldots, i_m)$ as a combination of m factors obtained by the selection of i_1th, i_2th $\ldots$ values of the first, second, $\ldots$, factors respectively. There are s^m such combinations of which a subset of s^t combinations may be called a (m, s, t) array. An (m, s, t) array is said to be of strength d if all combinations of any d of the m factors occur in equal number (s^{t-d}) of times. An array of strength d represented by (m, s, t, d) is, alternatively, called a hypercube of strength d." For $t = d$, these hypercubes correspond to $L(n, k, r)$ spaces with $n = s$, $r = d$, and conversely.

Bose and Bush **(7, 8)** weakened the condition of s^t combinations to $N = \lambda s^d$ combinations, to obtain an orthogonal array of strength d, size N, index λ, k constraints, and s levels which they define as "a $k \times N$ matrix A, with entries from a set Σ of $s \geqslant 2$ elements . . . [such that] each $d \times N$ submatrix of A contains all possible $d \times 1$ column vectors with the same frequency λ." For $\lambda = 1$ it is clear that the column vectors of A comprise an $L(n, k, r)$ space, and conversely.

(d) *A configuration.* Let v elements be arranged into $v + 1$ sets $T_1, \ldots,$ T_{v+1} such that for $i \neq j$, the number of elements which are in either T_i or T_j but not in both is k. We may co-ordinatize the *sets* of the configuration by assigning to a set the co-ordinates $(i_1, \ldots, i_v)$, where $i_j = 1$ if the jth element is in the set, and $i_j = 0$ otherwise. If $x_1, \ldots, x_{v+1}$ are the co-ordinates of $T_1, \ldots, T_{v+1}$, respectively, then the x_i comprise a subspace of $S^v(2)$, $S(2)$ $= \{0, 1\}$, satisfying $d(x_i, x_j) = k$, for all $i \neq j$. We will discuss this configuration further in the next example.

As an illustration, for $k = 4$, $v = 7$, consider

$$T_1 = \{1, 2\} \qquad T_4 = \{1, 3, 6, 7\} \qquad T_7 = \{2, 4, 6, 7\}$$

$$T_2 = \{3, 4\} \qquad T_5 = \{1, 4, 5, 7\} \qquad T_8 = \{1, 2, 3, 4, 5, 6\}.$$

$$T_3 = \{5, 6\} \qquad T_6 = \{2, 3, 5, 7\}$$

(e) *The v, k, λ configuration.* Consider next the now classic v, k, λ configuration defined in Chowla and Ryser **(11)** as an arrangement of v elements into v sets such that every set contains exactly k distinct elements and such that every pair of sets has exactly λ elements in common, $0 < \lambda < k < v$. In statistics these configurations are termed symmetrical balanced incomplete block designs. For $\lambda = 1$ and $k = n + 1$, $n \geqslant 2$, the configuration reduces to a projective plane with $n + 1$ points per line, and for $v = 4m - 1$, $k = 2m - 1$, $\lambda = m - 1$, it is equivalent to a Hadamard matrix of order $N = 4m$ **(20)** (these are the ± 1 matrices H satisfying $HH^T = NI$, where H is of order N and I is the identity matrix). For a comprehensive summary of results see Ryser **(22)**. With the v, k, λ configuration we may associate its characterizing $v \times v$ incidence matrix $A = [a_{ij}]$, where $a_{ij} = 1$ if the jth element is in the ith set, and 0 otherwise. Actually, constructing the incidence matrix is equivalent to co-ordinatizing the sets of the configuration, the ith row representing the co-ordinates of the ith set. It is apparent that the v sets of co-ordinates so obtained comprise v elements of $S^v(2)$, $S(2) = \{0, 1\}$, satisfying:

(i) If $s = (0, 0, \ldots, 0)$, and the v elements are $x_1, \ldots, x_v$, then $d(x_i, s) = k$ for $i = 1, \ldots, v$.

(ii) $d(x_i, x_j) = 2(k - \lambda)$, $i \neq j$.

That the metric characterization of v, k, λ tends toward the heart of the matter is suggested in (ii) by the fact that the value $k - \lambda$ which appears in both the v, k, λ design and its complementary design (the design obtained

by replacing each set by its complement) and plays such a critical role in the non-existence theorems, occurs explicitly.

Also of interest is the fact that the "strong" converse of the above holds. That is, given $v + 1$ elements s', x_1', ..., x_v' of $S^v(2)$ satisfying

(i') $d(x_i', s') = k$ for $i = 1, ..., v$

(ii) $d(x_i', x_j') = 2(k - \lambda)$, $i \neq j$, $0 < \lambda < k < v$,

we may construct v elements $x_1, ..., x_v$ satisfying (i) and (ii) and hence constituting a v, k, λ configuration. This may be seen as follows. If in the jth components of $x_1', ..., x_v', s'$ we replace 0's by 1's and 1's by 0's, we clearly obtain an isometric space. Now perform this replacement in the jth components if and only if the jth component of s' is 1. Then we obtain an isometric space with $s = (0, 0, ..., 0)$ as the image of s'.

Consider again the configuration in (d). Though, at least on the surface, the relation of this configuration to the v, k, λ configuration is somewhat obscure, by relating both to their metric characterizations, it is immediately apparent that for $0 < 2\lambda = k < v$, they are essentially equivalent.

(f) *Balanced incomplete block designs.* Let $T = \{s_1, ..., s_v\}$, and consider the configuration $C = \{T_1, ..., T_b\}$, where the T_i are subsets of T. Then the *dual* configuration consists of the subsets $A_1, ..., A_v$ of the set $A = \{t_1, ..., t_b\}$, where t_i is in A_j if and only if a_j is in T_i; and the *complementary* configuration consists of the sets $\bar{T}_1, ..., \bar{T}_b$, where $\bar{T}_i$ denotes the complement of T_i.

Given the set $S(b)$ of b elements, let E_r denote the class of all subsets of $S(b)$ containing r elements. Then E_r is a subspace of the metric space $U_{S(b)}$. We will show that for $0 < \lambda < r < b$, the existence of a balanced incomplete block design BIBD **(26)** with parameters b, v, k, r, λ is equivalent to having $e(E_r, r - \lambda - 1) = (r - \lambda)b/(r^2 - \lambda b)$ with $r^2 - \lambda b > 0$.

THEOREM 3.1. *If $r^2 - \lambda b > 0$ (λ integral and $0 \leqslant \lambda \leqslant r$), then*

(a) $e(E_r, r - \lambda - 1) \leqslant v$, *where $v = (r - \lambda)b/(r^2 - \lambda b)$.*

(b) *Equality holds in* (a) *if and only if there exist v elements $x_1, ..., x_r$ in E_r such that $d(x_i, x_j) = r - \lambda$, for all $i \neq j$.*

Proof. Let $e(E_r, r - \lambda - 1) = m$. Then since λ is integral there exist $x_1, ..., x_m$ in E_r with $d(x_i, x_j) \geqslant r - \lambda$ for all $i \neq j$. Denote by k_i the number of sets x_j containing the ith element of $S(b)$, $i = 1, ..., b$. Comparing total occurrences we obtain

(1) $$\sum k_i = rm.$$

Comparing contributions to all

$$\binom{m}{2}$$

set intersections, we obtain

(2) $$\sum \binom{k_i}{2} = \sum_{i<j} N(x_i \cap x_j) = \sum_{i<j} [r - d(x_i, x_j)].$$

But then $d(x_i, x_j) \geqslant r - \lambda$ implies

(3)
$$\sum \binom{k_i}{2} \leqslant \lambda \binom{m}{2}.$$

Now from Lemma 1 (§ 4) and (1), (3) follows

(4)
$$L = b \binom{rm/b}{2} \leqslant M = \sum \binom{k_i}{2} \leqslant R = \lambda \binom{m}{2}.$$

Using $r^2 - \lambda b > 0$, we find from elementary calculations that $L \leqslant R$ is equivalent to $m \leqslant v$, and $L = R$ if and only if $m = v$. Thus conclusion (a) is established. Finally, if $m = v$, from $L = M = R$ and (2) it follows that

$$\sum [r - d(x_i, x_j)] = \lambda \binom{m}{2},$$

and thus $d(x_i, x_j) \geqslant r - \lambda$ implies $r - d(x_i, x_j) = \lambda$. Hence $d(x_i, x_j) = r - \lambda$, completing the proof of the theorem.

COROLLARY 1. For $0 < \lambda < r < b$, the configuration $x_1, \ldots, x_v$ is the dual of a BIBD with parameters b, v, k, r, λ, where $k = rv/b$. Conversely, given the BIBD and considering its dual configuration as a subspace of E_r, one obtains $e(E_r, r - \lambda - 1) = v$, $r^2 - \lambda b > 0$, and $v = (r - \lambda)b/(r^2 - \lambda b)$.

Proof. In the proof of the above theorem, from $m = v$ we obtain $L = M$. This together with Lemma 1 (§ 4) and (1), gives $k_i = rv/b = k$, for $i = 1, \ldots, b$. Thus every element of $S(b)$ occurs in k of the sets $x_1, \ldots, x_v$. Further, note that $d(x_i, x_j) = r - \lambda$ for all $i \neq j$ implies that every pair of distinct sets intersect in exactly λ elements. Thus the first conclusion follows. Conversely, given the BIBD and considering its dual configuration as a subspace of E_r, one obtains $e(E_r, r - \lambda - 1) \geqslant v$. Further, from $0 < \lambda < r < b$, and the well-known conditions $rv = bk$, $\lambda(v - 1) = r(k - 1)$, it follows that $r^2 - \lambda b > 0$ and $v = (r - \lambda)b/(r^2 - \lambda b)$. But then from conclusion (a) of the theorem, we have $e(E_r, r - \lambda - 1) = v$.

Specializing to v, k, λ configurations, one obtains the interesting result:

COROLLARY 2. *If v elements are arranged in $v' \geqslant v$ sets of k elements each, such that every pair of distinct sets has at most λ elements in common, where $\lambda < k^2/v$ is a non-negative integer, then $\lambda \geqslant k(k - 1)/(v - 1)$. If equality holds, then $v' = v$ and every pair of distinct sets has exactly λ elements in common.*

Thus for $1 < k < v$, the arrangement constitutes a v, k, λ configuration. (In this event, it is interesting to note that from Corollary 1 one also obtains directly that each element occurs in exactly k sets.)

Proof. From conclusion (a) of the theorem we have that if $k^2 - \lambda v > 0$, then $v \leqslant v' \leqslant e(E_k, k - \lambda - 1) \leqslant (k - \lambda)v/(k^2 - \lambda v)$. But $v \leqslant (k - \lambda)v/(k^2 - \lambda v)$ is equivalent to $\lambda \geqslant k(k - 1)/(v - 1)$, and equality hold sin both expressions or neither. Finally, apply the proof of (b).

4. Some theorems for metrized Cartesian product spaces. Let E_i denote a subspace of the metric space $S^k(n_i)$, $i = 1, \ldots, t$. For $x_i = (a_{i1}, \ldots, a_{ik})$ in E_i, $i = 1, \ldots, t$, let $x_1 x_2 \ldots x_t = \pi x_i = (b_1, \ldots, b_k)$, where $b_j = (a_{1j}, \ldots, a_{tj})$, $j = 1, \ldots, k$. If $\pi x_i = (b_1, \ldots, b_k)$, $\pi y_i = (c_1, \ldots, c_k)$, x_i and y_i in E_i, define $d(\pi x_i, \pi y_i)$ in the usual manner as the number of subscripts j for which $b_j \neq c_j$, $j = 1, \ldots, k$.

Definition 9. The metric space

$$E_1 \dot{x} E_2 \dot{x} \ldots \dot{x} E_t = \dot{\pi} E_i = \{\pi x_i; x_i \in E_i\}$$

is termed the *direct product* of the E_i. Note the distinction between the *direct* product $\dot{\pi} E_i$ and the *Cartesian* product πE_i.

From the above definition, it is clear that any biunique mapping from $\pi S(n_i)$ onto $S(\pi n_i)$ induces an isometry between $\dot{\pi} S^k(n_i)$ and $S^k(\pi n_i)$. For convenience we simply write $\dot{\pi} S^k(n_i) = S^k(\pi n_i)$. With this understanding, $\dot{\pi} E_i$ is a subspace of $S^k(\pi n_i)$. Note that the direct product is independent of the order of the factors. That is, if $i(1), \ldots, i(t)$ is a permutation of $1, 2, \ldots, t$, then $\dot{\pi} E_j$ is isometric to $\dot{\pi} E_{i(j)}$ under the mapping $\pi x_j \rightarrow \pi x_{i(j)}$. Next note that if $t_1 < t_2 < \ldots < t_r = t$, then $\dot{\pi} E_{i(1)} \dot{x} \dot{\pi} E_{i(2)} \dot{x} \ldots \dot{x} \dot{\pi} E_{i(r)}$ is isometric to $\dot{\pi} E_j$, where $i(j) = t_{j-1} + 1, \ldots, t_j$ $(t_0 = 0)$. In particular it follows that $(E_1 \dot{x} E_2) \dot{x} E_3$ and $E_1 \dot{x} (E_2 \dot{x} E_3)$ are isometric since each is isometric to $E_1 \dot{x} E_2 \dot{x} E_3$. Thus, relative to isometry, the direct product operation is associative and commutative.

THEOREM 4.1. *For x_i and y_i in E_i,*

$$\max[d(x_i, y_i)] \leqslant d(\pi x_i, \pi y_i) \leqslant \sum d(x_i, y_i).$$

Proof. From the definition it is clear that if x_r and y_r have distinct jth components, then so do πx_i and πy_i. Hence $d(x_r, y_r) \leqslant d(\pi x_i, \pi y_i)$ and the first inequality follows. Next suppose πx_i and πy_i have distinct jth components. Then so do at least one pair x_t, y_t, and from this it is clear that the second inequality must hold.

COROLLARY 1. *The major and minor diameters Δ, δ satisfy*

$$\max(\delta(E_i)) \leqslant \delta(\dot{\pi} E_i) \leqslant \Delta(\dot{\pi} E_i) \leqslant \Sigma \Delta(E_i).$$

Proof. From the definitions and the theorem we have

$$\delta(E_i) \leqslant d(x_i, y_i) \leqslant \max d(x_i, y_i) \leqslant d(\pi x_i, \pi y_i),$$

which implies $\max \delta(E_i) \leqslant \delta(\dot{\pi} E_i)$. Also

$$d(\pi x_i, \pi y_i) \leqslant \sum d(x_i, y_i) \leqslant \sum \Delta(E_i)$$

implies that $\Delta(\dot{\pi} E_i) \leqslant \sum \Delta(E_i)$.

COROLLARY 2. *If $S^k(n_1)$ and $S^k(n_2)$ are r-orthogonal, then so is $S^k(n_1 n_2)$.*

Proof. Let L_i be an $L(n_i, k, r)$ space of $S^k(n_i)$, $i = 1, 2$. Then $L = L_1 \dot{x} L_2$ is an $L(n_1 n_2, k, r)$ space of $S^k(n_1 n_2)$, since

$$\delta(L) \geqslant \max[\delta(L_1), \delta(L_2)] > k - r,$$

and L contains exactly $(n_1 n_2)^r$ elements.

By identifying the element $(a_1, \ldots, a_k)$ with the set $\{(1, a_1), \ldots, (k, a_k)\}$, we can apply Theorem 3.1 and its first corollary to the metric space $S^k(n)$. We then obtain immediately

THEOREM 4.2. *If $k > (r - 1)n$ (r integral, $2 \leqslant r$, $n > 1$), then*
(a) $e(S^k(n), k - r) \leqslant v$, where $v = n[k - (r - 1)]/[k - n(r - 1)]$.
(b) *If equality holds in* (a) *there exist v elements $x_1, \ldots, x_v$ in $S^k(n)$ such that $d(x_i, x_j) = k - (r - 1)$, for all $i \neq j$. In this event, each element of $S(n)$ occurs as a jth component of exactly $t = [k - (r - 1)]/[k - n(r - 1)]$ of the x_i's, $j = 1, \ldots, k$. Further, from $x_1, \ldots, x_v$ we can construct a BIBD with parameters b', v', k', r', λ' ($0 < \lambda' < r' < b'$), where $b' = kn$, $v' = v$, $k' = t$, $r' = k$, $\lambda' = r - 1$.*

This BIBD has the special property that its b' blocks can be partitioned into k pairwise disjoint classes of n blocks each, such that every variety occurs in exactly one block from each class. Conversely, given such a BIBD, one can construct v elements of $S^k(n)$ with mutual distances exceeding $k - r$, and the elementary conditions on its parameters will imply $k > (r-1)n$.

From Cauchy's inequality we obtain

LEMMA 1. *For the real numbers $a_1, \ldots, a_n$,*

$$n \binom{a}{2} \leqslant \sum \binom{a_i}{2},$$

where

$$\binom{a_i}{2} = a_i(a_i - 1)/2$$

and $a = (\sum a_i)/n$. Further, equality holds if and only if $a_i = a$ for all i.

LEMMA 2. *Let $i(1), \ldots, i(t)$, $t \leqslant r$, be any t distinct integers from among $1, \ldots, k$, and let $a_{i(j)}$ be in $S(n)$. Then in the $L(n, k, r)$ space, L, there are precisely n^{r-t} elements with $i(j)$th component equal to $a_{i(j)}$, $j = 1, \ldots, t$.*

Proof. The proof is evident from the fact that L contains n^r elements, any two distinct elements agree in at most $r - 1$ corresponding components, and over $S(n)$ every t-tuple can be completed to an r-tuple in exactly n^{r-t} ways.

LEMMA 3. *If $S^k(n)$ is r-orthogonal, then $S^{k-1}(n)$ is $(r - 1)$-orthogonal.*

Proof. Let L be an $L(n, k, r)$ space of $S^k(n)$. By Lemma 2 there are n^{r-1} elements in L having the same kth component. If their kth components are dropped, it is easy to see that the n^{r-1} elements so obtained constitute an $L(n, k - 1, r - 1)$ space.

LEMMA 4. *If $S^k(n)$ is r-orthogonal, then so is $S^t(n)$, $t < k$.*

Proof. This is clear from the fact that if the last $k - t$ components of the elements in an $L(n, k, r)$ space are dropped, the resulting elements comprise an $L(n, t, r)$ space.

LEMMA 5. *If $S^k(n)$ is r-orthogonal, $r \geqslant 2$, then $k \leqslant n + r - 1$.*

Proof. Let L be an $L(n, k, r)$ space in $S^k(n)$. For a in $S(n)$, by Lemma 2 there are n elements $x_1, \ldots, x_n$ in L with first $r - 1$ components equal to a, and an element x_{n+1} distinct from these and having its first $r - 2$ components equal to a. Thus from $d(x_i, x_j) > k - r$ for all $i \neq j$, it follows that $n \geqslant k - r + 1$.

LEMMA 6. *For x and y in the $L(n, n + r - 1, r)$ space, L, $d(x, y) \leqslant n + 1$ implies $d(x, y) = n$.*

Proof. Let $x = (a_1, \ldots, a_k)$, $y = (b_1, \ldots, b_k)$, $k = n + r - 1$. Suppose $d(x, y) \leqslant n + 1$. Then $a_i = b_i$ for at least $r - 2$ subscripts i. With no loss of generality, suppose $a_i = b_i$, $i = 1, \ldots, r - 2$. Now by Lemma 2 there are exactly $n^2 - 1$ elements in $L(n, k, r)$ which are different from x and have ith component equal to a_i, $i = 1, \ldots, r - 2$. Let A_j denote the subset of these $n^2 - 1$ elements having jth component equal to a_j, $j = r - 1, \ldots, k$. Then again by Lemma 2, A_j contains precisely $n - 1$ elements. Also, $A_i \cap A_j = \phi$ for $i \neq j$, and so $\cup A_j$ contains precisely $(n - 1)(n + 1) = n^2 - 1$ elements. Thus every element in L having ith component equal to a_i, $i = 1, \ldots, r - 2$, has its jth component equal to a_j for precisely one value of j, $r - 1 \leqslant j \leqslant k$, and so has distance n from x. In particular, $d(x, y) = n$.

LEMMA 7. *Given a $k \times r$ matrix, A, over a field F, having all its r-rowed minors non-singular, we can construct a $k \times (k - r)$ matrix with all $(k - r)$-rowed minors non-singular.*

Proof. Let A_1 denote the $r \times r$ matrix consisting of the first r rows of A, and let A_2 denote the $(k - r) \times r$ matrix consisting of the remaining $k - r$ rows, so that

$$A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}.$$

By hypothesis A_1 is non-singular, so by elementary operations on the columns of A we can obtain

$$A' = \begin{bmatrix} I \\ A_2' \end{bmatrix},$$

where I is the $r \times r$ identity matrix. Since the elementary operations have been performed only on the *columns* of A, A' also has all r-rowed minors non-singular. Now using the Laplace expansion, one sees that every minor determinant of A_2' occurs as a factor of some r-rowed minor determinant of A', and hence is not zero. Again applying the Laplace expansion, one verifies that every $(k - r)$-rowed minor determinant of the $(k - r) \times k$ matrix $[A_2', I]$ either equals unity or has the same absolute value as some minor determinant of A_2' (here I is the $(k - r)$-rowed identity matrix). Hence $[A_2', I]$ has all $(k - r)$-rowed minors non-singular. Taking the transpose, we have the required result.

THEOREM 4.3. *Given a $k \times r$ matrix $A = [a_{ij}]$ over $GF(p^m)$ having all r-rowed minors non-singular, we can construct an $L(n, k, r)$ and an $L(n, k, k - r)$ space, $n = p^m$.*

Proof. Denote the row vectors of A by $\alpha_1, \ldots, \alpha_k$. Let $L = \{Ax\}$, where x ranges over the n^r r-place column vectors over $GF(p^m)$. Then L is an $L(n, k, r)$ space, for suppose $Ax, Ay, x \neq y$, have as many as r components the same, say $i(1), \ldots, i(r)$. Then the submatrix B of A consisting of the row vectors $\alpha_{i(1)}, \ldots, \alpha_{i(r)}$ satisfies $Bx = By$. But by hypothesis B is non-singular, so $x = y$ contradicting our choice of x and y. Hence $d(Ax, Ay) > k - r$, and L is an $L(n, k, r)$ space. Finally, by Lemma 7, from A we can construct a $k \times (k - r)$ matrix with all r-rowed minors non-singular, and applying the above proof we obtain an $L(n, k, k - r)$ space.

The first part of the above theorem corresponds to that of Bose and Bush (**7**, Theorem 5A, p. 521) with index one. They employ a similar proof.

LEMMA 8. *For $n = p^m$, p a prime,*
(1) $S^k(n)$ *is r-orthogonal for $k \leqslant n + 1$.*
(2) $S^k(n)$ *is 3-orthogonal for $k \leqslant n + 2$ and $p = 2$.*
(3) $S^k(n)$ *is r-orthogonal for $k \leqslant r + 1$.*

Proof. Letting $a_1, \ldots, a_{n-1}$ denote the non-zero elements of $GF(p^m)$, one readily verifies that the matrix

$$\begin{bmatrix} B \\ 1\ 0 \ldots 0\ 0 \\ 0\ 0 \ldots 0\ 1 \end{bmatrix}$$

where $B = [b_{ij}]$ is an $(n - 1) \times r$ matrix with $b_{ij} = a_i{}^j$, $j = 0, \ldots, r - 1$, has all r-rowed minors non-singular, since their determinants all reduce to the Vandermonde type. For the special case $p = 2$, $r = 3$, we may adjoin to A as an $(n + 2)$th row the vector $(0, 1, 0)$ and again verify that A has all 3-rowed minors non-singular. Conclusions (1) and (2) now follow from Theorem 4.3 and Lemma 4. Finally, consider (3). For $k = r$, the result is trivial. For $k = r + 1$, the matrix obtained by adjoining the row vector

$(1, 1, \ldots, 1)$ to the $r \times r$ identity matrix has all r-rowed minors non-singular, and (3) follows from Theorem 4.3.

Conclusions (1) and (2) of the above lemma correspond to the theorem of Bush (8, p. 431), who obtains the construction by employing polynomials over $GF(p^m)$.

From Lemmas 4 and 8 and Corollary 2 of Theorem 4.1, we obtain

THEOREM 4.4. *If* $n = \pi p_i{}^{e_i}$ *is the decomposition of* n *into distinct prime powers, then*

(1) $S^k(n)$ *is* r-*orthogonal for* $k \leqslant \min(p_i{}^{e_i} + 1)$.
(2) $S^k(n)$ *is* 3-*orthogonal for* $k \leqslant 2^m + 2$ *if* $\min(p_i{}^{e_i} + 1) = 2^m + 1$.
(3) $S^k(n)$ *is* r-*orthogonal for arbitrary* n *whenever* $k \leqslant r + 1$.

From the relation between orthogonal Latin squares and $L(n, k, 2)$ spaces, for $r = 2$ we obtain the theorem proved in Mann's book (18, Theorem 8.8, p. 105) (other construction methods may be found in (16, Theorem 12.1)):

COROLLARY. *There exist at least* $\min(p_i{}^{e_i} - 1)$ *orthogonal Latin squares of side* $n = \pi p_i{}^{e_i}$.

(It is of interest to note here that in a yet unpublished paper, E. T. Parker has, by an elegant construction, succeeded in exceeding the minimum given in the above corollary for certain values of n. The author believes this to be the first such successful attempt.)

THEOREM 4.5. *Let* L *be an* $L(n, k, r)$ *space,* $r \geqslant n - 1$, $k \geqslant r + 2$. *Then* $r = n - 1$, *and for every* x *in* $S^k(n)$, $d(x, L) < k - r$.

Proof. Let $x = (x_1, \ldots, x_k)$, and applying Lemma 2 with $t = r$, let $y = (a_1, \ldots, a_k)$ be the unique element of L having $a_i = x_i$, $i = 1, \ldots, r$. Let $y' = (a_1, \ldots, a_r)$, and in $S^r(n)$ consider the unit closed sphere $c(y', 1)$. The sphere contains $r(n - 1)$ elements $y_1', \ldots, y_{r(n-1)}'$ different from y', and by the triangle inequality, $d(y_i', y_j') \leqslant 2$, $i \neq j$. Again by Lemma 2, to each $y_i' = (b_{i1}, \ldots, b_{ir})$ there corresponds a unique element y_i in L, $y_i = (b_{i1}, \ldots, b_{ir}, u_i, v_i, \ldots,)$. Now $d(y, y_i) > k - r$ and $d(y', y_i') = 1$ imply $u_i \neq a_{r+1}$, $v_i \neq a_{r+2}$. Also, for $i \neq j$, $d(y_i, y_j) > k - r$ and $d(y_i', y_j') \leqslant 2$ imply that the ordered pairs (u_i, v_i) and (u_j, v_j) are distinct. Thus there are $r(n - 1)$ distinct ordered pairs (u_i, v_i) for which $u_i \neq a_{r+1}$ and $v_i \neq a_{r+2}$. But since the total number of such pairs is $(n - 1)^2$, we must have $r(n - 1) \leqslant (n - 1)^2$ or $r \leqslant n - 1$. Hence $r = n - 1$.

We now prove the second part of the theorem. If $x_i = a_i$ for either $i = r + 1$ or $r + 2$, we are done. So assume $x_i \neq a_i$, $i = r + 1$, $r + 2$. But then (x_{r+1}, x_{r+2}) must be one of the pairs (u_i, v_i), and the conclusion follows.

As an immediate corollary, we obtain the equivalent of the theorem of Bush (8, p. 427):

COROLLARY 1. *If* $S^k(n)$ *is* r-*orthogonal, then* $r \geqslant n$ *implies* $k \leqslant r + 1$.

(Thus there are no Graeco-Latin squares of order 2, no Graeco-Latin cubes of order 3, etc.)

Lemma 5 and the above corollary give

COROLLARY 2. *For $1 < r < k - 1$ and $k \geqslant 2n - 1$, $S^k(n)$ is not r-orthogonal.*

THEOREM 4.6. *If $S^k(n)$ is r-orthogonal for $r \geqslant 2$ and $k = n + r - 1$, then*

$$\binom{n + t - 3}{t - 2} \equiv 0 \bmod (t - 1) \ for \ t = 2, 3, \ldots, r.$$

Proof. The proof is by induction on r. For $r = 2$ the theorem is trivial. Assume the theorem holds for $r - 1, r \geqslant 3$. Let L be an $L(n, k, r)$ space, and let $x = (a_1, \ldots, a_k)$ be in L, $k = n + r - 1$. By Lemma 2, L contains n^{r-2} elements $y_j, j = 1, \ldots, n^{r-2}$, with first and second components b_1 and b_2, respectively, $b_1 \neq a_1$, $b_2 \neq a_2$. Also, for every set $i_1, \ldots, i_{r-2}$ of $r - 2$ distinct integers from among $3, 4, \ldots, n + r - 1$, there is a unique element $y(i_1, \ldots, i_{r-2})$ among the y_j's with i_jth component equal to $a_{t(j)}(i(j) = i_j), j = 1, \ldots, r - 2$. But then by Lemma 6, the distance of this element from x is n, and so among the last $n + r - 3$ components, $y(i_1, \ldots, i_{r-2})$ has $r - 1$ components equal to the corresponding components of x. Hence there are

$$\binom{r - 1}{r - 2} = r - 1$$

distinct sets $\{j_1, \ldots, j_{r-2}\}$ associated with the same element $y(i_1, \ldots, i_{r-2})$. Further, since x and $y(i_1, \ldots, i_{r-2})$ agree in at most $r - 1$ corresponding components, there can be no more than $r - 1$ such sets associated with $y(i_1, \ldots, i_{r-2})$. Thus the

$$\binom{n + r - 3}{r - 2}$$

sets are divided into classes of $r - 1$ sets each, and we must have

$$\binom{n + r - 3}{r - 2} \equiv 0 \bmod (r - 1).$$

Applying the induction hypothesis and Lemma 3, we obtain the theorem.

From $t = 3$ in the above, one obtains the theorem of Bush (**8**, p. 430):

COROLLARY. *For n odd, $r \geqslant 3$, an $L(n, k, r)$ space satisfies $k \leqslant n + r - 2$.*

Relative to our previous remarks (§ 3, Example (a)), from the above theorem and Lemma 8 it follows that complete sets of orthogonal Latin cubes always exist for n a power of 2, and never exist for n odd. However, for n an odd prime power $\geqslant 5$, we can always construct a complete set less one.

THEOREM 4.7. *If $S^n(n)$ is 2-orthogonal, then so is $S^{n+1}(n)$.*

Proof. Let L be an $L(n, n, 2)$ space in $S^n(n)$, where $S(n) = \{a_1, \ldots, a_n\}$. Denote by $x_1, \ldots, x_n$ the n elements of L having first component equal to a_1 (Lemma 2). Let x_i' in $S^{n+1}(n)$ be the element obtained by adjoining a_i as an $(n + 1)$th component to x_i, $i = 1, \ldots, n$. Let y in L be different from the x_i's. Then since $d(x_i, x_j) = n - 1$ for all $i \neq j$, each a_j occurs exactly once as a tth component of the x_i's for $t = 2, \ldots, n$. Hence $d(x_i, y) > n - 2$ for $i = 1, \ldots, n$ implies that there is a unique subscript m for which $d(x_m, y) = n$. Let y' in $S^{n+1}(n)$ be the element obtained by adjoining a_m as an $(n + 1)$th component to y. Now repeat the above process for all y in L different from the x_i's, and denote by L' the set of n^2 elements of $S^{n+1}(n)$ which are thus obtained. By construction it is clear that x_i' has distance n from each of the other elements of L'. Let y_1' and y_2' be any two distinct elements of L' different from the x_i''s. If $d(y_1, y_2) = n$, then $d(y_1', y_2') \geqslant n$. If y_1 and y_2 have the same first component $b \neq a_1$, let $y_3, \ldots, y_n$ denote the remaining elements of L with first component b. Then applying the argument used above to the y_i, for each x_i there is a unique subscript m for which $d(y_m, x_i) = n$. Hence, by construction, no two of the y_i''s have the same $(n + 1)$th component, and so in particular, $d(y_1', y_2') = n$. Finally, if y_1 and y_2 have the same jth component b, $2 \leqslant j \leqslant n$, let $y_3, \ldots, y_{n-1}, x_t$ denote the remaining elements of L with jth component b. Again applying the above argument, we obtain $d(y_1', y_2') = n$. Hence $d(x', y') \geqslant n$ for all x', y' in L', and so L' is an $L(n, n + 1, 2)$ space and $S^{n+1}(n)$ is 2-orthogonal.

The above theorem is equivalent to saying that every set of $n - 2$ orthogonal Latin squares of side n may be completed to a full set of $n - 1$ orthogonal Latin squares. From our remarks following Theorem 4.7, it is interesting to note that the corresponding theorem for cubes is false.

From Lemma 3, Theorem 4.7, the Bruck-Ryser non-existence theorem **(10)** and the relations among orthogonal Latin squares, projective planes, and $L(n, k, r)$ spaces, we obtain immediately:

THEOREM 4.8. *If $n \equiv 1$ or 2 (mod 4) and the square-free part of n is divisible by a prime of the form $4k + 3$, then $S^k(n)$ is not r-orthogonal for $k \geqslant n + r - 2$, $r \geqslant 2$.*

THEOREM 4.9. *If $S^k(n)$ is r-orthogonal, then it admits of a partitioning into pairwise disjoint, superposable $L(n, k, r)$ spaces.*

Proof. Suppose $S^k(n)$ is r-orthogonal, and let L denote an $L(n, k, r)$ space of $S^k(n)$. Let $A_1, \ldots, A_{k-r}$ be $k - r$ Latin squares of side n, and denote by $\alpha(i, j)$ the permutation $t \to a_t$, $t = 1, \ldots, n$, where $(a_1, a_2, \ldots, a_n)$ is the ith row vector of A_j. Finally, let $\omega = \omega(i_1, \ldots, i_{k-r})$ denote the mapping of $S^k(n)$ into itself generated by performing the permutation $\alpha(i_j, j)$ upon the jth components of the elements of $S^k(n)$, $j = 1, \ldots, k - r$. It is clear that ω is indeed a motion (Definition 4), and so under ω, L is carried into a superposable $L(n, k, r)$ space, $L(i_1, \ldots, i_{k-r})$. Further, from Lemma 2 with $t = r$,

it is easy to see that if $(i_1, \ldots, i_{k-r})$ and $(j_1, \ldots, j_{k-r})$ are distinct as vectors, then $L(i_1, \ldots, i_{k-r})$ and $L(j_1, \ldots, j_{k-r})$ are disjoint. Finally, since $L(i_1, \ldots, i_{k-r})$ consists of n^r elements, and there are n^{k-r} distinct vectors $(i_1, \ldots, i_{k-r})$, it is clear that these spaces exhaust $S^k(n)$.

THEOREM 4.10. *For $r > 1$, $L(n, k, r)$ is a metric basis for $S^k(n)$.*

Proof. The theorem is trivial for $k = r$, so assume $k > r$. Let x and y be arbitrary in $S^k(n)$, $x = (a_1, \ldots, a_k)$, $y = (b_1, \ldots, b_k)$, $x \neq y$. The theorem will be proved if it can be shown that (C): there exists z in $L(n, k, r)$ such that $d(x, z) < d(y, z)$. Proof is by induction on r. Consider first $L(n, k, 2)$. Suppose, say, $a_1 \neq b_1$. Let $z_1, \ldots, z_n$ be the n elements of $L(n, k, 2)$ with first component equal to a_1. If for some z_i, $d(y, z_i) = k$, we are done since $d(x, z_i) \leqslant k - 1$. So suppose $d(y, z_i) < k$ for $i = 1, \ldots, n$. Then since $L(n, k, 2)$ has minor diameter $\geqslant k - 1$, by Lemma 5 we must have $k = n + 1$, and hence $d(y, z_i) = k - 1$, $i = 1, \ldots, n$. Now let z_t be the unique element among the z_i (Lemma 2) with second component equal to a_2. Then $d(y, z_t) = k - 1$ and $d(x, z_t) \leqslant k - 2$. This completes the proof for $r = 2$. Now suppose that (C) holds for $r - 1$ ($r \geqslant 3$) and all k, and consider $L(n, k, r)$. If $d(x, y) \leqslant r$, then by Lemma 2, we can always find a z in $L(n, k, r)$ such that $d(x, z) < d(y, z)$. So suppose $d(x, y) > r \geqslant 3$. Select the n^{r-1} elements in $L(n, k, r)$ with kth component equal to a_k. Denote these elements by $z_1, \ldots, z_t$, $t = n^{r-1}$, and let $z_1', \ldots, z_t'$ be the corresponding elements of $S^{k-1}(n)$ obtained by dropping the kth components of the z_i. By the proof of Lemma 3, the z_j''s constitute an $L(n, k - 1, r - 1)$ space, and by the induction hypothesis there exists z_i' in $L(n, k - 1, r - 1)$ with $d(x', z_i') < d(y', z_i')$, where $x' = (a_1, \ldots, a_{k-1})$, $y' = (b_1, \ldots, b_{k-1})$. But $d(x', z_i') = d(x, z_i)$, and $d(y', z_i') \leqslant d(y, z_i)$. Hence $d(x, z_i) < d(y, z_i)$.

5. Concluding remarks. The investigation of the metric properties of $S^k(n)$ and, in general, of power-sets has, of course, only its beginnings in the present paper. One of the initial problems is the discovery of further significant concepts (such as "extent" appears to be, for example), since many of the classical metric concepts apparently will have limited value, and topological concepts become completely trivial for the finite spaces. High on the list of desiderata would be a development of the basic theory to the point where the elements, say, of $S^k(n)$ could be treated abstractly, making it unnecessary to deal with their internal structure each time a new result is under scrutiny. For it is precisely at the point where internal combinatorial structure becomes too complex for the mind to grasp as a totality that our efforts fail.

A line of attack which has been neglected in the present paper and which may prove to be fruitful, is an examination of the distance matrix. One may readily obtain an indication of the manner in which some of the properties of $S^k(n)$ are reflected in its distance matrix A by going through the definitions

and theorems and rephrasing them in terms of A. Of course, one of the critical questions in this regard is whether these and other significant properties of A lend themselves to matric methods and theory. Also of value may be an investigation of the behaviour of subspaces of $S^k(n)$ under motions of $S^k(n)$. (Any circle of radius 1, $C = C(a, 1) = \{x; d(x, a) = 1\}$, is a metric basis for $S^k(n)$. Considering such a circle, it is not difficult to show that the group of motions of $S^k(n)$ is the semi-direct product of A by B, where A is the direct product of k symmetric groups on n letters, and B is the symmetric group on k letters.) For example, what can be said about the group of motions which carries an $L(n, k, r)$ space into itself?

In addition to these metric spaces being objects of interest in their own right, the results thus far obtained offer hope that this type of approach may provide a useful common orientation for a wide class of combinatorial problems.

Addendum. Since the submission of this paper, there have been several developments in the field. The work of Bose, Parker, and Shrikhande has annihilated the Euler conjecture. It is now known that pairs of orthogonal Latin squares ($L(n, 4, 2)$ spaces) exist for all orders except $n = 2, 6$. It will be interesting to see to what extent their construction techniques can be extended to general $L(n, k, r)$ spaces. Remaining related problems are in a state of flux. Also, in a recent conversation the author learned from Professor Bose that the metric space $S^k(2)$ has been studied in connection with error correcting codes. (The metric space $S^k(2)$ is, of course, isometric with the set of vertices of a k-dimensional Euclidean hypercube of unit side, where the distance between vertices is taken as the square of the Euclidean distance. Also, $S^k(n)$ can be essentially embedded in $S^{kn}(2)$ in a trivial manner.) The elements are termed k-place messages and the metric is termed the Hamming distance. It is important in the theory of symmetric binary codes to determine the t-extent of $S^k(2)$. Discussion of this problem and additional bibliography can be found in **(28)**, along with an excellent summary of the status of the existence problem for Hadamard matrices. One of the main results in the above paper is that if we consider $(4t - 1)$-place messages having all mutual distances greater than or equal to $2t$, then the existence of the maximum number, $4t$, of such messages is equivalent to the existence of a symmetric BIBD with parameters $v = b = 4t - 1$, $r = k = 2t - 1$, $\lambda = t - 1$ (or

equivalently, to the existence of a Hadamard matrix of order $4t$). This result may also be obtained as a corollary to Theorem 4.2 of the present paper by taking $n = 2$, $k = 4t - 1$ and $r = 2t$. The design derived from the resolvable BIBD of the theorem by deleting one variety and all blocks not containing it, is precisely the symmetric BIBD obtained by Bose and Shrikhande. More generally, for $n = 2$, Theorem 4.2 may be rephrased: If we consider m-place messages having all mutual distances greater than or equal to d, then for $d + 1 \leqslant m < 2d$, the maximum number of such messages is less than or equal to $2d/(2d - m)$, and equality is attained if and only if there exists a BIBD with parameters

$$b = m, \quad v = \frac{m}{2d - m}, \quad r = m - d, \quad k = \frac{m - d}{2d - m}, \quad \lambda = \frac{2m - 3d}{2}.$$

REFERENCES

1. Reinhold Baer, *Nets and groups*, Trans. Amer. Math. Soc., *46* (1939), 110–141.
2. W. W. Rouse Ball, *Mathematical Recreations and Essays* (New York, 1947).
3. Grace E. Bates, *Free loops and nets and their generalizations*, Amer. J. Math., *69* (1947), 499–550.
4. Leonard M. Blumenthal, *Distance geometries*, University of Missouri Studies, vol. 13, no. 2 (1938).
5. ———— *Theory and applications of distance geometry* (New York, 1953).
6. R. C. Bose, *On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares*, Sankhya, *3* (1938), 323–338.
7. R. C. Bose and K. A. Bush, *Orthogonal arrays of strength two and three*, Ann. Math. Stat., *23* (1952), 508–524.
8. K. A. Bush, *Orthogonal arrays of index unity*, Ann. Math. Stat., *23* (1952), 426–434.
9. R. H. Bruck, *Finite nets, I. Numerical invariants*, Can. J. Math., *3* (1951), 94–107.
10. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Can. J. Math., *1* (1949), 88–93.
11. S. Chowla and H. J. Ryser, *Combinatorial problems*, Can. J. Math., *2* (1950), 93–99.
12. Leonard Euler, *Recherches sur une nouvelle espèce de quarrés magiques*, Commentationes Algebraicae, Opera Omnia, series prima, *7* (1923).
12.1 R. A. Fisher and F. Yates, *Statistical tables for Biological, agricultural, and medical research* (1st ed., Oliver and Boyd, 1938).
13. Marshall Hall, Jr., *Projective planes*, Trans. Amer. Math. Soc., *54* (1943), 229–277.
14. F. W. Levi, *Finite geometrical systems* (University of Calcutta, 1942).
15. A. Lindenbaum, *Contributions à l'étude de l'espèce métrique*, I Fund. Math., *8* 1926), 209–222.
16. H. F. MacNeish, *Euler squares*, Ann. Math., *23* (1921), 221–227.
17. H. B. Mann, *On orthogonal Latin squares*, Bull. Amer. Math. Soc., *50* (1944), 249–257.
18. ———— *Analysis and design of experiments* (New York, 1949).
19. H. W. Norton, *The 7 × 7 squares*, Ann. Eugen., *9* (1939), 269–307.
20. R. E. A. C. Paley, *On orthogonal matrices*, J. Math. and Phys., *12* (1933), 311–320.
21. C. R. Rao, *Hypercubes of strength d leading to confounded designs in factorial experiments*, Bull. Calcutta Math. Soc., *38* (1946) 67–78.
22. H. J. Ryser, *Geometries and incidence matrices*, Amer. Math. Monthly, *62* (1955), 25–31.
23. Esther Seiden, *On the problem of construction of orthogonal arrays*, Ann. Math. Stat., *25* (1954), 151–156.

24. W. L. Stevens, *The completely orthogonalized Latin square*, Ann. Eugen., *9* (1939), 82–93.

25. G. Tarry, *Le problème de 36 officiers*, Mathesis, *20* (1901).

26. F. Yates, *Incomplete randomized blocks*, Ann. Eugen., *7* (1936), 121–140.

Added in proof

27. R. C. Bose and S. S. Shrikhande, *On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order 4t + 2*, Proc. N. A. S., *45* (1959), 734–737.

28. ——— *A note on a result in the theory of code construction*, Inform. and Control, *2* (1959), 183–194.

29. ——— *On the falsity of Euler's conjecture for all orders exceeding 26*, Amer. Math. Soc. Notices, *6* (1959), 379.

30. R. W. Hamming, *Error detecting and error correcting codes*, Bell System Tech. J., *29* (1950), 147–160.

31. E. T. Parker, *Construction of some sets of pairwise orthogonal Latin squares*, Amer. Math. Soc. Notices, *5* (1958), 815.

32. ——— *Orthogonal Latin squares*, Proc. Nat. Acad. Sci., *45* (1959), 859–862.

33. ——— *Completion of disproof of Euler's conjecture*, Am. Math. Soc. Notices, *6* (1959), 391.

34. M. Plotkin, *Binary codes with specified minimum distance*, Research Div. Rept. 51–20, University of Pennsylvania.

35. R. R. Varsamov, *The evaluation of signals in codes with correction of errors*, Math. Rev., *20* (1959), 262.

Ohio State University
and
The National Bureau of Standards