

MATHEMATIKA

A JOURNAL OF PURE AND APPLIED MATHEMATICS

VOL. 19. PART 1.

JUNE, 1972.

No. 37.

THE REALIZATION OF DISTANCES WITHIN SETS IN EUCLIDEAN SPACE

D. G. LARMAN AND C. A. ROGERS

1. *Introduction.* In 1944 and 1945 H. Hadwiger [1, 2] proved the following theorems.

THEOREM A. *Let E^n be covered by $n+1$ closed sets. Then there is one of the sets, within which all distances are realized.*

THEOREM B. *Let E^n be covered by $4n-3$ closed sets that are all mutually congruent. Then all distances are realized within each set.*

Here a distance d is realized within a set S , if there are points x, y in S at distance d apart.

Hadwiger also gives an example of a covering of the plane by a set of seven mutually congruent closed sets, the distance 1 being left unrealized in each.

D. E. Raiskii [3, 4] has recently refined Hadwiger's first theorem by proving

THEOREM C. *Let E^n be covered by $n+1$ sets. Then there is one of the sets, within which all distances are realized.*

Raiskii mentions that S. B. Stechkin has produced a decomposition of the plane into six sets, each of which fails to realize some distance, and he gives a decomposition of his own with this property. In Raiskii's decomposition, and presumably also in Stechkin's, the sets are not closed.

D. R. Woodall [5] has independently proved Theorem C. He also gives an example of a covering of the plane by six closed sets, no one of which realizes all distances.

We understand (private communication from P. Mani) that Hadwiger has long believed that the numbers $n+1$, $4n-3$ occurring in his theorems are not best possible. The main object of this note is to show that Theorem A can be improved for $n \geq 5$. We prove

THEOREM 4. *Let N_n be defined by the table following this theorem.*

(a) *If a measurable set in E^n has upper density exceeding $1/N_n$ then all distances are realized within the set.*

(b) *If E^n is covered by less than N_n sets, then there is a set of the covering within which all distances are realized.*

(c) If E^n is covered by N_n sets (in the case when N_n is an integer) and some point of E^n belongs to two or more of the sets, then there is a set of the covering within which all distances are realized.

TABLE 1

n	N_n	Configuration	Lemma No.
2	$3\frac{1}{2}$	Moser spindle	2
3	$4\frac{2}{3}$	Moser–Raiskii spindle	2
4	$5\frac{1}{4}$	Moser–Raiskii spindle	2
5	8	Half-cube	3
6	$9\frac{3}{8}$	Half-cube spindle	4
7	14	Gosset polytope	6
8, 9, 10	16	Special Gosset spindle	7
11, 12, 13	$17\frac{15}{16}$	Quarter-cube spindle	9
14–22	$\frac{4}{3}n$	3-coordinate configuration	15
23	100	Leech–Conway configuration	11
24–76	102	Special Leech–Conway spindle	12
77–138	$\frac{4}{3}n$	3-coordinate configuration	15
139–	$\frac{n(n-k+1)}{k^3-k^2+1}$	k -coordinate configuration	16

with

$$\frac{1}{2}(k-2)(k-3)2^{k-1} < 2(n-2) \leq \frac{1}{2}(k-1)(k-2)2^k.$$

Our method is based on a simplified version of Raiskii's method, coupled with a considerable study of configurations that are more effective than the Moser–Raiskii spindle used by Raiskii. The reader who is interested in small or large or particular values of n needs to read §2 below together with the relevant part of §3. Note that for n large

$$N_n \sim \frac{n^2}{(\log_2 n)^3}.$$

It seems likely that further improvements can be made for small values of n and that great improvements can be made for large n . In §5 we record two assertions and two conjectures with some sketchy justifications for the assertions and some explanations for the relevance of the conjectures.

We are most grateful to Dr. P. McMullen for drawing our attention to the half-cube in E^5 and the Gosset polytopes in E^6 and E^7 and for so enabling us to extend our results, previously obtained only for $n \geq 14$, to lower values of n .

2. *Configurations; consequences of their existence.* We use the name “configuration” for any finite sequence, $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_M$ of points, not necessarily all distinct. The number of points in the configuration will be M , not in general the number of distinct points in the configuration. We say that a distance d and an integer D are a critical distance and a critical number for the configuration $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_M$, if: whenever a sub-configuration

$$\mathbf{x}_{M(1)}, \mathbf{x}_{M(2)}, \dots, \mathbf{x}_{m(D+1)}, \quad 1 \leq m(1) < m(2) < \dots < m(D+1) \leq M$$

is chosen from the configuration, the distance d is realized in the subconfiguration, and D is the least integer with this property. Many examples of such configurations are given in the next section. It should be noted that, in a given configuration, different critical numbers will be associated with different critical distances.

In this section we prove the following three theorems showing that results of the type summarized in Theorem 4, stated in the introduction, follow from the existence of certain configurations. The first of these theorems is elementary. The second and third depend on a simplified form of Raiskii's method.

THEOREM 1. *Suppose that there is in E^n a configuration of M points with critical distance 1 and critical number D . Then, if a measurable set in E^n has upper density exceeding D/M , all distances are realized within the set.*

THEOREM 2. *Suppose that there is in E^n a configuration of M points with critical distance 1 and critical number D . Then, if E^n is covered by less than M/D sets, then there is a set of the covering within which all distances are realized.*

THEOREM 3. *Suppose that there is in E^n a configuration of M points with critical distance 1 and critical number D with M/D integral. Then, if E^n is covered by M/D sets and some point of E^n belongs to two or more of the sets, there is a set of the covering within which all distances are realized.*

Proof of Theorem 1. Let x_1, x_2, \dots, x_M be a configuration of M points in E^n with critical distance 1 and critical number D . Let S be any Lebesgue measurable set in E^n with upper density exceeding D/M . This means that

$$\limsup_{s \rightarrow \infty} \sup_{s(C)=s} \frac{\mu(S \cap C)}{\mu(C)} > \frac{D}{M}, \tag{1}$$

μ denoting the Lebesgue measure, and the supremum being taken over all cubes C of side $s(C)$ equal to s . Then we can choose $\varepsilon > 0$ and cubes C with arbitrarily large sides and with

$$\frac{\mu(S \cap C)}{\mu(C)} > \frac{D + \varepsilon}{M}. \tag{2}$$

Now let d be a given distance. Provided the side $s(C)$ of C is sufficiently large compared to the maximum distance of the points dx_1, dx_2, \dots, dx_M from the origin we will have

$$\frac{\mu(\{S + dx_i\} \cap C)}{\mu(C)} > \frac{D}{M},$$

for $i = 1, 2, \dots, M$. Then

$$\sum_{i=1}^M \mu(\{S + dx_i\} \cap C) > D\mu(C),$$

and some point, x^* say, of C will necessarily belong to at least $D + 1$ of the sets

$$S + dx_i, \quad i = 1, 2, \dots, M.$$

After some re-naming, we may suppose that $m \geq D + 1$ and that x^* belongs to

$$S + dx_i, \quad i = 1, 2, \dots, m.$$

So the points

$$\mathbf{x}^* - d\mathbf{x}_i, \quad i = 1, 2, \dots, m$$

belong to S . But, by our hypothesis on our configuration, the distance 1 is realized within the sub-configuration $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m$, say between the points $\mathbf{x}_1, \mathbf{x}_2$. Then the points $\mathbf{x}^* - d\mathbf{x}_1, \mathbf{x}^* - d\mathbf{x}_2$ are in S at distance d apart. Thus the distance is realized within S .

This proves the theorem.

Proof of Theorem 2. Let $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_M$ be a configuration in E^n with critical distance 1 and critical number D . Let S_1, S_2, \dots, S_N , with $N < M/D$, be a system of sets covering E^n . We suppose that, for each i with $1 \leq i \leq N$, there is a distance d_i that is not realized in the set S_i , and we seek a contradiction.

We study the configuration of M^N points of the form

$$\sum_{i=1}^N d_i \mathbf{x}_{m(i)}, \quad (3)$$

where m is an arbitrary map from the set $\{1, 2, \dots, N\}$ to the set $\{1, 2, \dots, M\}$. Each point belongs to at least one of the sets S_1, S_2, \dots, S_N . So we can choose an integer, i^* say, so that at least M^N/N of the points lie in the same set S_{i^*} . Now the original system of points can be grouped into M^{N-1} groups

$$d_{i^*} \mathbf{x}_m + \sum_{\substack{i=1 \\ i \neq i^*}}^N d_i \mathbf{x}_{m(i)}, \quad m = 1, 2, \dots, M,$$

of M points each. So at least one of these groups, say the group

$$d_{i^*} \mathbf{x}_m + \sum_{\substack{i=1 \\ i \neq i^*}}^N d_i \mathbf{x}_{m^*(i)}, \quad m = 1, 2, \dots, M,$$

will have at least M/N points in S_{i^*} . As $N < M/D$, we have $M/N > D$, and so there are at least $D + 1$ of these points in S_{i^*} . We write

$$\mathbf{x}^* = \sum_{\substack{i=1 \\ i \neq i^*}}^N d_i \mathbf{x}_{m^*(i)},$$

and we suppose, as we may without loss of generality, that the points

$$d_{i^*} \mathbf{x}_m + \mathbf{x}^*, \quad m = 1, 2, \dots, D + 1,$$

lie in S_{i^*} . But, by our hypothesis on our configuration, the distance 1 is realized within the sub-configuration $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_{D+1}$, say between the points $\mathbf{x}_1, \mathbf{x}_2$. Then the points

$$d_{i^*} \mathbf{x}_1 + \mathbf{x}^*, \quad d_{i^*} \mathbf{x}_2 + \mathbf{x}^*$$

are in S_{i^*} at distance d_{i^*} apart, contrary to our choice of d_{i^*} . This contradiction proves the theorem.

Proof of Theorem 3. It will be sufficient to indicate the modifications to the proof of Theorem 2 that transform it into a proof of Theorem 3. Using the translation invariance of the situation we may start by supposing that \mathbf{x}_1 coincides with the origin \mathbf{o} and also that \mathbf{o} belongs to two at least of the sets S_1, S_2, \dots, S_N , where now

we only know that $N \leq M/D$. This ensures that at least one of the M^N points of the configuration (3) lies in at least two of the sets S_1, S_2, \dots, S_N . So, for a suitable choice of i^* , more than M^N/N of the points of the configuration will lie in S_{i^*} . The argument is now completed as before.

3. *The construction of configurations.* In this section we construct the configurations that, when used in conjunction with Theorems 1, 2 and 3, lead to the proof of Theorem 4. We first describe a process for constructing a configuration in E^{n+1} given a suitable configuration in E^n . This process, which we will call *spindle formation*, is a natural generalization of a process first introduced by Leo Moser and William Moser [6] and later exploited by Raiskii.

LEMMA 1. (Spindle formation). *Let \mathcal{C} be a configuration of M points, lying on an $(n - 1)$ -sphere in E^n , of radius r , and having critical distance d and critical number D . Provided $r \leq \sqrt{\frac{1}{4}}d$, there is a configuration \mathcal{S} , called the spindle on \mathcal{C} , of $M^2 + 2DM - D^2$ points in E^{n+1} with critical distance d and with critical number DM . If $r = \sqrt{\frac{1}{4}}d$, there is a configuration \mathcal{T} , called the special spindle on \mathcal{C} , of $M + 2D$ points in E^{n+1} with critical distance d and with critical number D .*

Proof. Let π_1, π_2 be n -dimensional hyperplanes in E^{n+1} at distances $\sqrt{(d^2 - r^2)}$ and $\sqrt{(4d^2 - 5r^2)}$ from the origin \mathbf{o} . Let $\mathcal{C}_1, \mathcal{C}_2$ be copies of the configuration \mathcal{C} , lying on the $(n - 1)$ -dimensional spheres in these hyperplanes with radius r and with centres at the feet of the perpendiculars from \mathbf{o} to the hyperplanes. Then the points of \mathcal{C}_1 are at distance d from \mathbf{o} and those of \mathcal{C}_2 are at distance $2\sqrt{(d^2 - r^2)}$ from \mathbf{o} .

Let \mathbf{x}^* be the reflection of \mathbf{o} in π_1 . Then \mathbf{x}^* is at distance $2\sqrt{(d^2 - r^2)}$ from \mathbf{o} and at distance d from each point of \mathcal{C}_1 . Let $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_M$ be the points of \mathcal{C}_2 . For each i , with $1 \leq i \leq M$, we can choose an orthogonal transformation Ω_i carrying \mathbf{x}^* to the point \mathbf{x}_i . We can now form the configuration \mathcal{S} by taking the point \mathbf{o} , repeated $D(M - D)$ times, each point of \mathcal{C}_2 repeated D times, and the points of the transformed configurations $\Omega_i \mathcal{C}_1, i = 1, 2, \dots, M$, once each.

Clearly \mathcal{S} has

$$D(M - D) + MD + MM = M^2 + 2MD - D^2$$

points. Let $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_{MD+1}$ be a sequence of $MD + 1$ points of \mathcal{S} , and suppose that the distance d is not realized in this sub-configuration. First suppose that one of $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_{MD+1}$ coincides with \mathbf{o} . Then at most $D(M - D)$ of these points coincide with \mathbf{o} and none can be any point of $\Omega_i \mathcal{C}_1, i = 1, 2, \dots, M$. So at least $D^2 + 1$ of the points are points of the D copies of \mathcal{C}_2 . So at least one of these D copies of \mathcal{C}_2 must contain $D + 1$ of the points $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_{MD+1}$, and so the distance d must be realized in this set, contrary to our supposition.

Now suppose that none of $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_{MD+1}$ coincides with \mathbf{o} . Let the number of the configurations $\Omega_i \mathcal{C}_1, i = 1, 2, \dots, M$ that contain points from $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_{MD+1}$ be r with $0 \leq r \leq M$. We suppose, as we may without loss of generality, that these are the configurations $\Omega_i \mathcal{C}_1, i = 1, 2, \dots, r$. Then, as the distance d is not realized in the subconfiguration, the D copies of the points $\mathbf{x}_i, i = 1, 2, \dots, r$ are not amongst the points $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_{MD+1}$. The number of these points that can occur in each configuration $\Omega_i \mathcal{C}_1, i = 1, 2, \dots, r$ is D ; and so the total number in the sub-configuration is at most

$$rD + (M - r)D = MD,$$

which is contrary to the choice of the sub-configuration. This shows that \mathcal{S} has critical distance d and critical number MD .

Now, in the special case when $r = \sqrt{\left(\frac{3}{4}\right)}d$, the point \mathbf{x}^* is at distance d from \mathbf{o} . It now suffices to form the configuration \mathcal{T} by taking the points \mathbf{o} and \mathbf{x}^* each repeated D times, together with the points of \mathcal{C}_1 . As \mathbf{o} and \mathbf{x}^* are each at distance d from all the other points of the configuration and from each other, it is easy to check that \mathcal{T} has $M + 2D$ points, has critical distance d and has critical number D .

Remark. It is easy to modify this construction to form "mixed" spindles; there is no reason why the configurations \mathcal{C}_1 and \mathcal{C}_2 in the above construction should be copies of the same configuration. We do not give details as we do not have occasion to use such mixed spindles.

LEMMA 2. (The Moser–Raiskii spindle.) *There is a configuration of $n^2 + 2n - 1$ points in E^n with critical distance 1 and with critical number n .*

Proof. The n vertices of a regular simplex of dimension $n - 1$, of edge length 1, lie on an $(n - 2)$ -sphere in E^{n-1} , and trivially form a configuration with critical distance 1 and with critical number 1. As the radius of the $(n - 2)$ -sphere is

$$\sqrt{\left(\frac{n-1}{2n}\right)} < \sqrt{\left(\frac{1}{3}\right)},$$

the required configuration is obtained on application of Lemma 1.

LEMMA 3. (The half-cube.) *There is a configuration of 16 points, lying on a 4-sphere of radius $\sqrt{\left(\frac{5}{8}\right)}$ in E^5 , with critical distance 1 and with critical number 2, and, at the same time, having critical distance $\sqrt{2}$, with critical number 5.*

Proof. In E^5 we consider: the point

$$\mathbf{e}_1 = (1, 1, 1, 1, 1);$$

the point

$$\mathbf{e}_2 = (-1, -1, 1, 1, 1);$$

the points $\mathbf{e}_3, \mathbf{e}_4, \dots, \mathbf{e}_{11}$, obtained by permuting the coordinates of \mathbf{e}_2 ; the point

$$\mathbf{e}_{12} = (-1, -1, -1, -1, 1);$$

and the points $\mathbf{e}_{13}, \mathbf{e}_{14}, \mathbf{e}_{15}, \mathbf{e}_{16}$, obtained by permuting the coordinates of \mathbf{e}_{12} . Clearly the set $\{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{16}\}$ is invariant under the group G of operations consisting of a change of sign of any even number of coordinates, and G is transitive on $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{16}$. All the points are at distance $\sqrt{5}$ from the origin \mathbf{o} ; the distance between two of $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{16}$ is $\sqrt{8}$ if they differ in two of their coordinates and is 4 otherwise.

We first show that given any three points $\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k$ with $1 \leq i < j < k \leq 16$, there is at least one pair from these three points at distance $\sqrt{8}$. As G is transitive, we take $i = 1$, as we may without loss of generality. Then, if $j \leq 11$, we have $\|\mathbf{e}_1 - \mathbf{e}_j\| = \sqrt{8}$, and if $12 \leq j < k \leq 16$, we have $\|\mathbf{e}_j - \mathbf{e}_k\| = \sqrt{8}$. So one of the three distances is $\sqrt{8}$.

We now suppose that $\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_6$ are six points chosen from the points $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{16}$ and show that the distance 4 is necessarily realized in the set $\{\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_6\}$. As G is transitive, we suppose, as we may without loss of generality, that $\mathbf{f}_1 = \mathbf{e}_1$. If any of the points $\mathbf{f}_2, \mathbf{f}_3, \dots, \mathbf{f}_6$ were to coincide with any of the points

$e_{12}, e_{13}, \dots, e_{16}$, the distance 4 would be immediately realized. So we may suppose that f_2, f_3, \dots, f_6 are chosen from the points e_2, e_3, \dots, e_{11} . Now each of the points f_2, f_3, \dots, f_6 have two coordinates with value -1 and three coordinates with value $+1$. Using the invariance of the point e_1 and the set $\{e_2, \dots, e_{11}\}$ under permutation of coordinates, we may suppose that

$$f_2 = e_2 = (-1, -1, 1, 1, 1).$$

Now, among the set $\{e_3, \dots, e_{11}\}$ there are only the three points

$$(-1, 1, -1, 1, 1), (-1, 1, 1, -1, 1), (-1, 1, 1, 1, -1),$$

with first coordinate -1 . So one at least of f_3, f_4, f_5, f_6 must have first coordinate 1. We may take this to be f_3 . Then either $\|f_2 - f_3\| = 4$, or the second coordinate of f_3 is -1 . After permuting the last three coordinates we may suppose that f_3 is the point

$$f_3 = (1, -1, -1, 1, 1).$$

The only further points of our system with a -1 in their second coordinate are now

$$(1, -1, 1, -1, 1) \text{ and } (1, -1, 1, 1, -1).$$

So one of the three points f_4, f_5, f_6 , say f_4 will have 1 for its second coordinate. So, either

$$\|f_2 - f_4\| = 4 \text{ or } \|f_3 - f_4\| = 4,$$

or

$$f_4 = (-1, 1, -1, 1, 1).$$

In this last case we are forced to the conclusion that either

$$\|f_2 - f_5\| = 4, \text{ or } \|f_3 - f_5\| = 4, \text{ or } \|f_4 - f_5\| = 4.$$

Thus 5 is the critical number for the configuration associated with the critical distance 4.

We obtain the configuration we actually require for the lemma on dividing all the coordinates by $2\sqrt{2}$.

LEMMA 4. (The half-cube spindle.) *There is a configuration of 316 points in E^6 with critical distance 1 and critical number 32.*

Proof. As $\sqrt{\frac{5}{8}} < \sqrt{\frac{3}{4}}$ the result follows on applying Lemma 1 to the first configuration in Lemma 3.

LEMMA 5. (The 6-dimensional Gosset polytope.) *There is a configuration of 27 points, lying on a 5-sphere of radius $\sqrt{\frac{3}{2}}$ in E^6 , with critical distance 1 and with critical number 3.*

Proof. We consider the configuration of points in E^8 consisting of the 12 points of the form

$$((2, 0)_p, (2, 0, 0, 0, 0, 0)_{p'}), p \in S_2, p' \in S_6,$$

where we use $(2, 0)_p, (2, 0, 0, 0, 0, 0)_{p'}$ to denote the results of applying permutations p, p' chosen from the symmetric groups S_2, S_6 to the coordinates in the brackets, and the 15 points of the form

$$(1, 1, (-1, -1, 1, 1, 1, 1))_p, p \in S_6,$$

where we use the same convention. These 27 points lie on the 6-dimensional hyperplane with equations,

$$x_1 + x_2 = 2, \quad x_3 + x_4 + x_5 + x_6 + x_7 + x_8 = 2. \quad (4)$$

We take this hyperplane to be our E^6 . The 27 points are all at distance $4/\sqrt{3}$ from the point

$$(1, 1, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}).$$

They, in fact form a representation of the vertices of the 6-dimensional Gosset polytope, see Gosset [7] and Coxeter [8], but we shall not need to appeal to the theory of this polytope.

We introduce the operation T of reflection in the hyperplane with equation

$$x_1 - x_2 - x_3 - x_4 - x_5 + x_6 + x_7 + x_8 = 0. \quad (5)$$

Writing

$$\mathbf{t} = (1, -1, -1, -1, -1, 1, 1, 1),$$

and using the standard scalar product notation this reflection is the transformation

$$T : \mathbf{x} \rightarrow T\mathbf{x} = \mathbf{x} - \frac{1}{4}(\mathbf{t} \cdot \mathbf{x}) \mathbf{t}.$$

It is easy to verify that T leaves invariant the points:

$$\begin{aligned} &(1, 1, (-1, 1, 1)_p, (-1, 1, 1)_{p'}), \quad p, p' \in S_3; \\ &(2, 0, (2, 0, 0)_p, 0, 0, 0), \quad p \in S_3; \\ &(0, 2, 0, 0, 0, (2, 0, 0)_p), \quad p \in S_3; \end{aligned}$$

since all these points lie on the hyperplane with equation (5). Further, for each p in S_3 , T exchanges the two points

$$\begin{aligned} &(2, 0, 0, 0, 0, (2, 0, 0)_p), \\ &(1, 1, 1, 1, 1, (1, -1, -1)_p), \end{aligned}$$

and also the two points

$$\begin{aligned} &(0, 2, (2, 0, 0)_p, 0, 0, 0), \\ &(1, 1, (1, -1, -1)_p, 1, 1, 1). \end{aligned}$$

Thus T is an isometry taking the configuration to itself. It is now easy to see that the group of isometries generated by T , the elements of S_2 acting on the coordinates x_1, x_2 and the elements of S_6 acting on the coordinates x_3, x_4, \dots, x_8 , acts transitively on the points of the configuration.

Now suppose that $\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_m$ is a subset of the configuration that does not realize the distance $2\sqrt{2}$. As the group of isometries of the configuration is transitive on its points, we may, without loss of generality, suppose that \mathbf{z}_1 is the point

$$\mathbf{z}_1 = (2, 0, 2, 0, 0, 0, 0, 0).$$

Then, as the distance $2\sqrt{2}$ is not realized in $\{\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_m\}$, the points $\mathbf{z}_2, \mathbf{z}_3, \dots, \mathbf{z}_m$ cannot be of one of the forms:

$$\begin{aligned} &(2, 0, 0, (2, 0, 0, 0, 0)_p), \quad p \in S_5; \\ &(0, 2, 2, 0, 0, 0, 0, 0); \\ &(1, 1, 1, (-1, -1, 1, 1, 1)_p) \quad p \in S_5; \end{aligned}$$

and so must be of one of the forms:

$$(0, 2, 0, (2, 0, 0, 0)_p), p \in S_5;$$

$$(1, 1, -1, (-1, 1, 1, 1)_p), p \in S_5.$$

Using the permutations of the last five coordinates, all transformations that leave \mathbf{z}_1 invariant, we may suppose, without loss of generality, that \mathbf{z}_2 is either

$$(0, 2, 0, 2, 0, 0, 0, 0)$$

or

$$(1, 1, -1, 1, -1, 1, 1, 1).$$

But these points correspond to each other under the transformation T , which also leaves \mathbf{z}_1 invariant. So we may, without loss of generality take \mathbf{z}_2 to be the point

$$(0, 2, 0, 2, 0, 0, 0, 0).$$

Now the only point of the system, other than $\mathbf{z}_1, \mathbf{z}_2$ that is neither at distance $2\sqrt{2}$ from \mathbf{z}_1 nor at distance $2\sqrt{2}$ from \mathbf{z}_2 is the single point

$$(1, 1, -1, 1, -1, 1, 1, 1).$$

Hence m is at most 3. Thus the distance $2\sqrt{2}$ and the number 3 are critical for the configuration.

The configuration required for the lemma is now obtained by dividing all coordinates by $2\sqrt{2}$.

LEMMA 6. (The 7-dimensional Gosset polytope.) *There is a configuration of 56 points, lying on a 6-sphere of radius $\sqrt{(\frac{3}{2})}$ in E^7 , with critical distance 1 and with critical number 4.*

Proof. We consider in E^8 the configuration of the 28 points of the form

$$((2, 2, 0, 0, 0, 0, 0)_p), p \in S_8, \tag{6}$$

and of the 28 points of the form

$$((-1, -1, 1, 1, 1, 1, 1)_p), p \in S_8. \tag{7}$$

These 56 points lie in the 7-dimensional hyperplane with equation

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 = 4.$$

They are all at distance $\sqrt{6}$ from the point with coordinates

$$(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}),$$

and the operation R of central reflection in this point clearly takes the configuration onto itself, interchanging the corresponding points (6) and (7). It is clear that the group of isometries of the configuration generated by R and by the permutations of the coordinates is transitive on the points of the configuration.

Now suppose that $\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_m$ is a subset of the configuration that does not realize the distance $2\sqrt{2}$. As the group of isometries of the configuration is transitive, we may, without loss of generality, suppose that \mathbf{z}_1 has coordinates

$$\mathbf{z}_1 = (-1, -1, 1, 1, 1, 1, 1).$$

Then $\mathbf{z}_2, \mathbf{z}_3, \dots, \mathbf{z}_m$ cannot be of one of the forms:

$$(0, 0, (2, 2, 0, 0, 0, 0)_p), p \in S_6;$$

$$((-1, 1)_p, (-1, 1, 1, 1, 1, 1)_{p'}), p \in S_2, p' \in S_6;$$

and so must be of one of the forms:

$$(2, 2, 0, 0, 0, 0, 0);$$

$$((2, 0)_p, (2, 0, 0, 0, 0, 0)_{p'}), p \in S_2, p' \in S_6;$$

$$(1, 1, (-1, -1, 1, 1, 1, 1)_p), p \in S_6.$$

If one of $\mathbf{z}_2, \mathbf{z}_3, \dots, \mathbf{z}_m$ is the point

$$(2, 2, 0, 0, 0, 0, 0),$$

there remain no possibilities for any other point and we must have $m \leq 2$. Otherwise $\mathbf{z}_2, \mathbf{z}_3, \dots, \mathbf{z}_m$ are chosen from the points:

$$((2, 0)_p, (2, 0, 0, 0, 0, 0)_{p'}), p \in S_2, p' \in S_6;$$

$$(1, 1, (-1, -1, 1, 1, 1, 1)_p), p \in S_6.$$

As this is just the configuration of points discussed in Lemma 5, it follows immediately from the results, obtained in the proof of that lemma, that $m \leq 4$. So $m \leq 4$ in each case. Thus the distance $2\sqrt{2}$ and the number 4 are critical for our configuration.

The configuration required for the lemma is now obtained by dividing all coordinates by $2\sqrt{2}$.

Remark. The 56 points (6) and (7) used in this configuration are the vertices of a 7-dimensional Gosset polytope, see, for example, Gosset [7] or Coxeter [8].

LEMMA 7. (The special Gosset spindle.) *There is a configuration of 64 points in E^8 with critical distance 1 and critical number 4.*

Proof. The result follows by using Lemma 1 to form a special spindle on the 7-dimensional Gosset polytope described in Lemma 6.

Remark. The points of this configuration can also be obtained from the 8-dimensional Gosset polytope (see [7] or [8]) by the following construction. Take the centre of the polytope repeated four times. Take any vertex of the polytope repeated four times. Take all the vertices of the polytope that are neighbours of this repeated vertex.

LEMMA 8. (The quarter cube.) *There is a configuration of 256 points, lying on a 9-sphere of radius $\sqrt{(\frac{5}{8})}$ in E^{10} , with critical distance 1 and with critical number at most 16.*

Proof. It will be convenient to represent the points of E^{10} , in the natural way, by the use of five complex coordinates. We consider the set of points with complex coordinates.

$$(\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4, \mathbf{z}_5)$$

with

$$\mathbf{z}_t = \pm 1 \text{ or } \pm i, t = 1, 2, 3, 4, 5,$$

subject to the conditions:

- (a) z_t is purely imaginary for an even number of values of t ;
- (b) $z_t = -1$ or $-i$ for an even number of values of t .

If the first four coordinates are chosen freely from $\pm 1, \pm i$, there is just one choice for the fifth coordinate that satisfies the conditions (a) and (b). Hence there are 256 points in the set.

Now let Z be a subset of this system of points and suppose that no two points of Z are at the distance $2\sqrt{2}$ apart. We prove that $|Z| \leq 16$.

We use symbols such as

$$(r, r, r, r, r) \text{ or } (i, r, i, r, r)$$

to indicate the possible patterns of real and purely imaginary coordinates. By the results in the proof of Lemma 3, at most two points of Z can be of any one type. Further, if there are two points of Z of the same type, they differ in the signs of precisely four of their coordinates.

There are just 16 different types; if each type is represented by at most one point in Z we clearly have $|Z| \leq 16$. So we may suppose that at least one type, say the type (r, r, r, r, r) , has two representatives in Z . These two points of Z with real coordinates must differ in the signs of four of their coordinates. We may, without loss of generality, take them to be the points

$$(1, 1, 1, 1, 1) \text{ and } (-1, -1, -1, -1, 1).$$

These two points being in Z , no point of Z can be of any one of the four types

- $(r, i, i, i, i),$
- $(i, r, i, i, i),$
- $(i, i, r, i, i),$
- $(i, i, i, r, i),$

but the type

$$(i, i, i, i, r)$$

is allowed, provided that the last coordinate of the point of this type is -1 .

More generally, if a type has two of its representatives in Z , these two representatives differ in the signs of four of their coordinates, and there is no point of Z in any one of the four types that agree with the first type in the character (real or purely imaginary) of one of these four coordinates, but differ from the first type in the character of their other coordinates.

Now, if just the one type has two representatives in Z , there are four types with no representatives in Z , so that

$$|Z| \leq 1.2 + 4.0 + 11.1 = 13.$$

So we may suppose that there are s types, with $s \geq 2$, each having two representatives in Z . First suppose that two such types differ in the character of just two of their coordinates. We may, without loss of generality take these two types, each with two representatives in Z , to be

$$(r, r, r, r, r),$$

and

$$(i, i, r, r, r).$$

Then four, at least, of the types

$$\begin{aligned} &(r, i, i, i, i), \\ &(i, r, i, i, i), \\ &(i, i, r, i, i), \\ &(i, i, i, r, i), \\ &(i, i, i, i, r), \end{aligned}$$

and four, at least, of the types

$$\begin{aligned} &(i, r, i, i, i), \\ &(r, i, i, i, i), \\ &(r, r, r, i, i), \\ &(r, r, i, r, i), \\ &(r, r, i, i, r), \end{aligned}$$

have no representatives in Z . So in this case six at least of the 16 types have no representative in Z , and

$$|Z| \leq s.2 + 6.0 + (10 - s).1 = 10 + s \leq 16,$$

if $s \leq 6$. But, if $s \geq 6$, it follows from the second half of Lemma 3 that there are two types, each with two representatives in Z , that differ in the character of four of their coordinates.

It now only remains to consider the case when $2 \leq s \leq 16$ and there are two types, each with two representatives in Z , that differ in the character of four of their coordinates. We may, without loss of generality, take these two types to be

$$(r, r, r, r, r) \text{ and } (r, i, i, i, i).$$

Then the types differing from the first in the character of four of their coordinates are distinct from the types differing from the second in the character of four of their coordinates. So there are at least 8 of these 10 types that have no representatives in Z . Hence $s \leq 8$ and

$$|Z| \leq s.2 + 8.0 + (8 - s).1 = 8 + s \leq 16.$$

This shows that, in all cases, Z has at most 16 elements. So the distance $2\sqrt{2}$ and a number less than or equal to number 16 are critical for the configuration. The configuration required for the lemma is now obtained by dividing all coordinates by $2\sqrt{2}$.

LEMMA 9. (The quarter cube spindle.) *There is a configuration of 73,472 points in E^{11} with critical distance 1 and critical number at most 4,096.*

Proof. The result follows on using Lemma 1 to construct a spindle on the configuration of Lemma 8.

LEMMA 10. (Davenport–Hajós Lemma.) *If m points lie on an $(n - 1)$ -sphere of radius 1 in E^n , and the distance between any two of the points is at least $\sqrt{2}$, then $m \leq 2n$.*

Proof. H. Davenport had shown a proof of this to one of us (C.A.R.) by 1949. According to R. A. Rankin, who gives a proof in [9], a proof by Davenport and Hajós was published in *Mat. Lapok*. We have not been able to trace this. But proofs by Sarkadi Károly and Szele Tibor appear in [10], and proofs by Aczél János and Szele Tibor of a closely related result (also proved in Rankin's paper) appear in [11].

LEMMA 11. (The Leech–Conway configuration.) *There is a configuration of 4,600 points, lying on a 22-sphere of radius $\sqrt{(\frac{3}{2})}$ in E^{23} , with critical distance 1 and with critical number at most 46.*

Proof. Let Λ be the Leech lattice in E^{24} , discovered by J. Leech [12, 13] and discussed in detail by J. H. Conway [14]. We use a few of the details of Conway's discussion. The distances between lattice points take the value $4\sqrt{n}$, with $n = 2, 3, \dots$. Let \mathbf{c} be a point of the lattice at distance $4\sqrt{2}$ from its origin \mathbf{o} . Then there are 4,600 points \mathbf{x} of the lattice satisfying the conditions

$$\left. \begin{aligned} \|\mathbf{x}\| &= 4\sqrt{2}, \\ \mathbf{x} \cdot \mathbf{c} &= 16. \end{aligned} \right\} \quad (8)$$

The second condition ensures that the points lie on a 23-dimensional hyperplane; the two conditions, together with the condition $\|\mathbf{c}\| = 4\sqrt{2}$ ensure that

$$\|\mathbf{x} - \frac{1}{2}\mathbf{c}\|^2 = \|\mathbf{x}\|^2 - \mathbf{x} \cdot \mathbf{c} + \frac{1}{4}\|\mathbf{c}\|^2 = 24,$$

so that the points lie on a 22-sphere of radius $2\sqrt{6}$ in this E^{23} .

Now suppose that a subset of this configuration of 4,600 points does not realize the distance $4\sqrt{2}$. As all the points are lattice points, the distance between any two is at least

$$4\sqrt{3} = (2\sqrt{6}) \cdot \sqrt{2}.$$

By the Davenport–Hajós Lemma (Lemma 10) there can be at most 46 points in the subset. Thus the distance $4\sqrt{2}$ and a number less than or equal to 46 are critical for the configuration of 4,600 points.

The configuration required for the lemma is now obtained by dividing all coordinates by $4\sqrt{2}$.

LEMMA 12. (The special Leech–Conway spindle.) *There is a configuration of 4,692 points in E^{24} , with critical distance 1 and with critical number at most 46.*

Proof. The result follows on using Lemma 1 to construct a special spindle on the configuration of Lemma 11.

LEMMA 13. (Hilton and Milner.) *Let A_1, A_2, \dots, A_r be sets, each with k elements chosen from a set A of n elements. Suppose that*

$$A_i \cap A_j \neq \emptyset, \quad 1 \leq i < j \leq r,$$

but that

$$\bigcap_{i=1}^r A_i = \emptyset.$$

Then, provided $2k \leq n$,

$$r \leq 1 + \binom{n-1}{k-1} - \binom{n-k-1}{k-1}.$$

Proof. See A. J. W. Hilton and E. C. Milner [15].

LEMMA 14. (Kleitman.) *Let A_1, A_2, \dots, A_r and B_1, B_2, \dots, B_s be sets, each of k elements chosen from a set A of n elements. Suppose that $2k \leq n$ and*

$$A_i \cap B_j \neq \emptyset, \quad 1 \leq i \leq r, 1 \leq j \leq s.$$

Then

$$\min(r, s) \leq \binom{n-1}{k-1}.$$

Proof. This is a spherical case of the result of D. J. Kleitman [16].

LEMMA 15. (The 3-coordinate configuration.) *If $n \geq 14$ there is a configuration of $\frac{1}{3}n(n-1)(n-2)$ points on an $(n-1)$ -sphere of radius $\sqrt{\frac{1}{2}}$ in E^n with critical distance 1 and critical number at most $(n-1)(n-2)$.*

Proof. We study the set X of

$$\frac{1}{3}n(n-1)(n-2)$$

points

$$\mathbf{x} = (x_1, x_2, \dots, x_n),$$

with

$$x_i = 0, 1 \text{ or } -1, \text{ for } i = 1, 2, \dots, n,$$

and with

$$x_i = \pm 1,$$

for just 3 values of i with $1 \leq i \leq n$. These points lie on the $(n-1)$ -sphere with centre \mathbf{o} and radius $\sqrt{3}$.

Let Z be a subset of X , and suppose that the distance $\sqrt{6}$ is not realized in Z . For each \mathbf{z} in Z , let $\mathcal{N}(\mathbf{z})$ be the set of integers j , with $1 \leq j \leq n$, for which the j -th coordinate of \mathbf{z} is not zero. Then $\mathcal{N}(\mathbf{z})$ is a set of three integers for each \mathbf{z} in Z .

If $\mathbf{z}_1, \mathbf{z}_2 \in Z$ and if we were to have

$$\mathcal{N}(\mathbf{z}_1) \cap \mathcal{N}(\mathbf{z}_2) = \emptyset,$$

we would have $\|\mathbf{z}_1 - \mathbf{z}_2\| = \sqrt{6}$, contrary to the choice of Z . So, for each pair of points $\mathbf{z}_1, \mathbf{z}_2$ in Z we have

$$\mathcal{N}(\mathbf{z}_1) \cap \mathcal{N}(\mathbf{z}_2) \neq \emptyset. \tag{9}$$

We first consider the case when

$$\bigcap_{\mathbf{z} \in Z} \mathcal{N}(\mathbf{z}) = \emptyset. \tag{10}$$

Let \mathcal{S} denote the system of all triples $\mathcal{N}(\mathbf{z})$ obtained as \mathbf{z} varies over Z . Applying Lemma 13 to this system we have

$$|\mathcal{S}| \leq 1 + \binom{n-1}{2} - \binom{n-4}{2} = 3n - 8.$$

We call a triple \mathcal{N} of \mathcal{S} “good”, if there is a second triple \mathcal{M} of \mathcal{S} having just two elements in common with \mathcal{N} . Otherwise \mathcal{N} has just a single element in common with each other triple \mathcal{M} of \mathcal{S} and we call \mathcal{N} “bad”.

Consider a good triple \mathcal{N} of \mathcal{S} . Then there is some other triple \mathcal{M} of \mathcal{S} meeting \mathcal{N} in two elements i, j say. Then $\mathcal{M} = \mathcal{N}(\boldsymbol{\zeta})$ for some $\boldsymbol{\zeta}$ in Z . If $\boldsymbol{\zeta} = (\zeta_1, \zeta_2, \dots, \zeta_n)$ we have $\zeta_i = \pm 1$ and $\zeta_j = \pm 1$. Now, if $\mathbf{z} = (z_1, z_2, \dots, z_n)$ in Z has $\mathcal{N}(\mathbf{z}) = \mathcal{N}$, we have $z_i = \pm 1$ and $z_j = \pm 1$. As $\mathcal{N} \neq \mathcal{M}$, $\boldsymbol{\zeta}, \mathbf{z}$ each have a further non-zero coordinate corresponding to a zero coordinate in the other. Thus, if z_i, z_j were to differ in just one sign from ζ_i, ζ_j , we would have $\|\mathbf{z} - \boldsymbol{\zeta}\| = \sqrt{6}$. Thus \mathbf{z} can only be one of four different vectors if $\mathcal{N}(\mathbf{z}) = \mathcal{N}$, and \mathcal{N} is good.

We now suppose that there are 5 or more bad triples. Without loss of generality we may suppose that $\{1, 2, 3\}$ is a bad triple. Each of the four or more remaining bad triples have just one element in common with $\{1, 2, 3\}$. So one of the integers 1, 2, 3 must belong to two other bad triples. Without loss of generality we may suppose that 1 is this element common to $\{1, 2, 3\}$ and two other bad triples. As these bad

triples can have no other elements in common and can have no other element in common with $\{1, 2, 3\}$, we may suppose, without loss of generality, that they are the triples $\{1, 4, 5\}$ and $\{1, 6, 7\}$. So we have obtained a system of three bad triples:

$$\left. \begin{array}{l} \{1, 2, 3 \\ \{1, \quad 4, 5 \\ \{1, \quad \quad 6, 7. \end{array} \right\} \tag{11}$$

We now study further possible triples, without asking whether they are good or bad. By condition (10) there must be a triple not containing 1. This triple must meet each of the triples (11) and so must be made up of a choice of one element from each of the pairs $\{2, 3\}$, $\{4, 5\}$, $\{6, 7\}$. So, without loss of generality, we may suppose that $\{2, 4, 6\}$ is a triple of \mathcal{S} . The other triples of \mathcal{S} , if any, not containing 1 must be made up in the same way by selecting one element from each of the three pairs. Condition (9) ensures that we can have only one triple from each pair of complementary triples of this type. So can have at most 4 triples not containing 1, in \mathcal{S} . But any triple in \mathcal{S} containing 1 must meet the triple $\{2, 4, 6\}$ and so must have two elements in common with one of the triples (11), contrary to our choice of these triples to be bad triples. Hence \mathcal{S} has at most seven triples as its elements. As at most 8 points \mathbf{z} of Z generate the same triple, and $n \geq 14$, we have

$$|Z| \leq 8|\mathcal{S}| \leq 56 < 4(3n - 4).$$

We remark that in this last paragraph we have used a slight refinement of the proof that a projective plane with just three points on each line has at most seven lines.

Now we may suppose that \mathcal{S} has b bad triples and g good triples with

$$b + g = |\mathcal{S}|, \quad b \leq 4.$$

Hence

$$\begin{aligned} |Z| &\leq 8b + 4g \\ &= 4b + 4|\mathcal{S}| \\ &\leq 4 \cdot 4 + 4(3n - 8) \\ &= 4(3n - 4). \end{aligned}$$

So in these cases, when (10) holds, we have

$$|Z| \leq 4(3n - 4) < (n - 1)(n - 2), \tag{12}$$

as $n \geq 14$.

It remains to consider the case when

$$\bigcap_{\mathbf{z} \in Z} \mathcal{N}(\mathbf{z}) \neq \emptyset.$$

We suppose, as we may without loss of generality, that

$$1 \in \bigcap_{\mathbf{z} \in Z} \mathcal{N}(\mathbf{z}).$$

We now divide the integers j with $2 \leq j \leq n$ into two classes, the ‘‘good’’ integers and the ‘‘bad’’ integers. We say that j is good, if $2 \leq j \leq n$ and j belongs to two distinct triples \mathcal{N} of \mathcal{S} ; otherwise we say that j is bad. Let there be g good integers and b bad ones. Then

$$b + g = n - 1. \tag{13}$$

Let $\mathcal{S}_{g, g}$, $\mathcal{S}_{g, b}$ and $\mathcal{S}_{b, b}$ be the sets of triples of \mathcal{S} that contain, in addition to the integer 1, respectively two good integers, a good integer and a bad integer, and two bad integers. If \mathcal{N} and \mathcal{M} are two triples of $\mathcal{S}_{b, b}$ the bad integers in \mathcal{N} can have no overlap with the bad integers in \mathcal{M} , as otherwise the common integer would be good rather than bad. So the triples \mathcal{N} of $\mathcal{S}_{b, b}$ set up a pairing into disjoint pairs of a subset of the bad integers. Hence

$$|\mathcal{S}_{b, b}| \leq \frac{1}{2}b. \tag{14}$$

Similarly, if \mathcal{N} and \mathcal{M} are triples of $\mathcal{S}_{g, b}$ the bad integer in \mathcal{N} must be distinct from the bad integer in \mathcal{M} . Hence

$$|\mathcal{S}_{g, b}| \leq b. \tag{15}$$

Further

$$|\mathcal{S}_{g, g}| \leq \frac{1}{2}g(g - 1). \tag{16}$$

Now, for any \mathcal{N} in \mathcal{S} , there are at most 8 points \mathbf{z} in Z with $\mathcal{N}(\mathbf{z}) = \mathcal{N}$. But, if $\mathcal{N} \in \mathcal{S}_{g, b}$, we can find a second \mathcal{M} in \mathcal{S} meeting \mathcal{N} in 1 and a second integer, say j . Suppose \mathcal{N} is the triple $\{1, i, j\}$ and \mathcal{M} is the triple $\{1, j, k\}$, with $i \neq k$. Then there is a point, ζ say, in Z with

$$\zeta_1 = \pm 1, \zeta_j = \pm 1, \zeta_k = \pm 1.$$

Now, if \mathbf{z} in Z has $\mathcal{N}(\mathbf{z}) = \mathcal{N}$, the condition $\|\mathbf{z} - \zeta\| \neq \sqrt{6}$ ensures that either

$$z_1 = \zeta_1 \text{ and } z_j = \zeta_j,$$

or

$$z_1 = -\zeta_1 \text{ and } z_j = -\zeta_j.$$

Hence, in this case, there are at most 4 points of \mathbf{z} in Z with $\mathcal{N}(\mathbf{z}) = \mathcal{N}$. Similarly, if $\mathcal{N} \in \mathcal{S}_{g, g}$, and \mathbf{z} in Z has $\mathcal{N}(\mathbf{z}) = \mathcal{N}$, the two remaining non-zero coordinates of \mathbf{z} will be determined, once the first coordinate has been chosen, and so there are only two possibilities for \mathbf{z} .

Combining the results of the last paragraph and then using (14), (15), (16) and (13) we obtain

$$\begin{aligned} |Z| &\leq 8|\mathcal{S}_{b, b}| + 4|\mathcal{S}_{g, b}| + 2|\mathcal{S}_{g, g}| \\ &\leq 4b + 4b + g(g - 1) \\ &= 8(n - 1 - g) + g(g - 1) \\ &= (g - 4\frac{1}{2})^2 - (4\frac{1}{2})^2 + 8(n - 1) \\ &\leq (n - 1 - 4\frac{1}{2})^2 - (4\frac{1}{2})^2 + 8(n - 1) \\ &= (n - 1)(n - 2). \end{aligned}$$

Combining this with (12), we see that the configuration has critical distance $\sqrt{6}$ and critical number at most $(n - 1)(n - 2)$.

The configuration required for the lemma is now obtained by dividing all coordinates by $\sqrt{6}$.

LEMMA 16. (The k -coordinate configuration.) *Suppose that $n \geq 26$ and that k is chosen so that*

$$\frac{1}{2}(k - 2)(k - 3)2^{k-1} < 2(n - 2) \leq \frac{1}{2}(k - 1)(k - 2)2^k. \tag{17}$$

Then

$$k = \log_2 n - (2 + o(1)) \log_2 \log_2 n,$$

as $n \rightarrow \infty$. Further, there is a configuration of

$$2^k \binom{n}{k}$$

points on an $(n - 1)$ -sphere of radius $\sqrt{\binom{n}{2}}$ in E^n with critical distance 1 and critical number not exceeding

$$\frac{k^3 - k^2 + 1}{n(n - k + 1)} 2^k \binom{n}{k}.$$

Proof. We study the set X of

$$2^k \binom{n}{k}$$

points

$$\mathbf{x} = (x_1, x_2, \dots, x_n),$$

with

$$x_i = 0, 1 \text{ or } -1, \text{ for } i = 1, 2, \dots, n,$$

and with

$$x_i = \pm 1,$$

for just k values of i with $1 \leq i \leq n$. These points lie on the $(n - 1)$ -sphere with centre \mathbf{o} and radius \sqrt{k} .

Let Z be a subset of X , and suppose that the distance $\sqrt{(2k)}$ is not realized in Z . As in the proof of Lemma 15, for each \mathbf{z} in Z , we use $\mathcal{N}(\mathbf{z})$ to denote the set of integers j with $1 \leq j \leq n$, for which the j -th coordinate of \mathbf{z} is not zero. In this case $\mathcal{N}(\mathbf{z})$ is a set of k such integers for each \mathbf{z} in Z . As the distance $\sqrt{(2k)}$ is not realised in Z , we have

$$\mathcal{N}(\mathbf{z}_1) \cap \mathcal{N}(\mathbf{z}_2) = \emptyset,$$

for each pair of points $\mathbf{z}_1, \mathbf{z}_2$ of Z .

We first consider the case when

$$\bigcap_{\mathbf{z} \in Z} \mathcal{N}(\mathbf{z}) = \emptyset.$$

Let \mathcal{S} denote the system of all k -tuples $\mathcal{N}(\mathbf{z})$ obtained as \mathbf{z} varies over Z . Applying Lemma 13 to this system we have

$$|\mathcal{S}| \leq 1 + \binom{n-1}{k-1} - \binom{n-k-1}{k-1}.$$

Hence

$$\begin{aligned} |Z| &\leq 2^k |\mathcal{S}| \\ &\leq 2^k \left[1 + \binom{n-1}{k-1} - \binom{n-k-1}{k-1} \right], \end{aligned}$$

and

$$\begin{aligned} \frac{|Z|}{|X|} &\leq \left[1 + \binom{n-1}{k-1} - \binom{n-k-1}{k-1} \right] / \binom{n}{k} \\ &= \frac{k(k-1) \dots 2 \cdot 1}{n(n-1) \dots (n-k+1)} \\ &\quad + \frac{k}{n} \left[1 - \left(1 - \frac{k}{n-1} \right) \left(1 - \frac{k}{n-2} \right) \dots \left(1 - \frac{k}{n-k+1} \right) \right]. \end{aligned}$$

Now the condition $n \geq 26$ and the condition (17) ensure that

$$2k < n - 1$$

so that

$$\frac{|Z|}{|X|} \leq \frac{1}{n(n-k+1)} + \frac{k}{n} \left[1 - \left(1 - \frac{k(k-1)}{n-k+1} \right) \right] = \frac{k^3 - k^2 + 1}{n(n-k+1)}. \tag{18}$$

So we may now suppose that

$$\bigcap_{z \in Z} \mathcal{N}(z) \neq \emptyset.$$

We suppose, as we may without loss of generality, that the integer 1 belongs to all the sets $\mathcal{N}(z)$ with $z \in Z$.

Let Z^+ and Z^- be the subsets of Z whose points have first coordinate 1 and -1 respectively. Further, for $\zeta = \pm 1$, and $2 \leq j \leq n$, let $Z^+(j; \zeta)$ and $Z^-(j; \zeta)$ be the sets of points of Z whose first and j -th coordinates take the values 1, ζ and -1 , ζ respectively. Let $\mathcal{N}^j(z)$ be the set of integers l with

$$1 < l \leq n, \quad l \neq j, \quad z_l = \pm 1.$$

Now suppose that for some z, z' in Z we have

$$z \in Z^+(j; \zeta),$$

$$z' \in Z^+(j; -\zeta),$$

$$\mathcal{N}^j(z) \cap \mathcal{N}^j(z') = \emptyset.$$

Then we would have

$$\|z - z'\|^2 = 2(k-2) + (2\zeta)^2 = 2k,$$

which is excluded by our assumptions. Thus, if

$$z \in Z^+(j; \zeta), \quad z' \in Z^+(j; -\zeta),$$

we have

$$\mathcal{N}^j(z) \cap \mathcal{N}^j(z') \neq \emptyset.$$

So, by Lemma 14, at least one of the families of $(k-2)$ -element sets

$$\mathcal{N}^j(z), \quad z \in Z^+(j; \zeta),$$

$$\mathcal{N}^j(z'), \quad z' \in Z^+(j; -\zeta),$$

has at most

$$\binom{n-3}{k-3}$$

members. Hence, for fixed j , the set $Z^+(j; \zeta)$ can have more than

$$2^{k-2} \binom{n-3}{k-3}$$

members for at most one of the values ± 1 of ζ .

We call a pair $(j; \zeta)$ "good", if

$$|Z^+(j; \zeta)| \leq 2^{k-2} \binom{n-3}{k-3},$$

and “bad”, if

$$|Z^+(j; \zeta)| > 2^{k-2} \binom{n-3}{k-3}.$$

Then we have just shown that for fixed j , at most one of the two values for ζ yields a bad pair $(j; \zeta)$. Let there be g good pairs and b bad pairs. Then

$$g + b = 2(n - 1), \quad b \leq n - 1. \tag{19}$$

We divide Z^+ into two sets Z_g^+ and Z_b^+ . Z_g^+ is the set of “good” elements \mathbf{z} with the property that the pair $(j; z_j)$ is a good pair for at least one j with $2 \leq j \leq n$. Z_b^+ is the set of “bad” elements \mathbf{z} with the property that the pair $(j; z_j)$ is a bad pair for each j with $2 \leq j \leq n$ and $z_j \neq 0$.

If G is the set of good pairs $(j; \zeta)$ we have

$$\begin{aligned} |Z_g^+| &\leq \sum_{(j; \zeta) \in G} |Z^+(j; \zeta)| \\ &\leq |G| \cdot 2^{k-2} \binom{n-3}{k-3} \\ &= g \cdot 2^{k-2} \binom{n-3}{k-3}, \end{aligned}$$

on using the definition of a good pair $(j; \zeta)$.

Now, if $\mathbf{z} \in Z_b^+$, all the pairs $(j; z_j)$ with $z_j \neq 0$ are bad pairs, and there can be no other element \mathbf{z}' in Z_b^+ whose non-zero coordinates fall in the same places. So $|Z_b^+|$ does not exceed the number

$$\binom{b}{k-1}$$

of ways of choosing $k - 1$ positions for the non-zero coordinates, after the first. Hence

$$\begin{aligned} |Z^+| &= |Z_g^+| + |Z_b^+| \\ &\leq g \cdot 2^{k-2} \binom{n-3}{k-3} + \binom{b}{k-1} \\ &= (2n - 2 - b) \cdot 2^{k-2} \binom{n-3}{k-3} + \binom{b}{k-1}. \end{aligned}$$

The righthand side of this inequality is a convex function of b . As $0 \leq b \leq n - 1$, we have

$$\begin{aligned} |Z^+| &\leq \max \left[(2n - 2) \cdot 2^{k-2} \binom{n-3}{k-3}, (n - 1) \cdot 2^{k-2} \binom{n-3}{k-3} + \binom{n-1}{k-1} \right] \\ &= (n - 1) \cdot 2^{k-2} \binom{n-3}{k-3} + \max \left[(n - 1) 2^{k-2} \binom{n-3}{k-3}, \binom{n-1}{k-1} \right] \end{aligned}$$

But

$$\frac{\binom{n-1}{k-1}}{(n-1) 2^{k-2} \binom{n-3}{k-3}} = \frac{2(n-2)}{\frac{1}{2}(k-1)(k-2) 2^k} \leq 1,$$

by our choice of k to satisfy (17). Hence

$$|Z^+| \leq (n - 1) 2^{k-1} \binom{n-3}{k-3}.$$

Similar arguments apply to Z^- . So

$$|Z| = |Z^+| + |Z^-| \leq (n - 1) 2^k \binom{n-3}{k-3},$$

and

$$\begin{aligned} \frac{|Z|}{|X|} &\leq (n - 1) \binom{n-3}{k-3} / \binom{n}{k} \\ &= \frac{k^3 - 3k^2 + 2k}{n(n-2)} \\ &< \frac{k^3 - k^2 + 1}{n(n-k+1)}. \end{aligned}$$

Combining this with (18) we see that the critical number of X associated with the critical distance $\sqrt{(2k)}$ does not exceed

$$\frac{k^3 - k^2 + 1}{n(n-k+1)} \cdot 2^k \binom{n}{k}.$$

The configuration required for the lemma is now obtained from X by dividing all the coordinates of all the points by $\sqrt{(2k)}$.

4. *Proof of Theorem 4.* The result follows on using the results of Lemmas 2, 3, 4, 6, 7, 9, 11, 12, 15 and 16 in Theorems 1, 2 and 3.

5. *The assertions and conjectures.*

Assertion 1. E^n can be covered by a system of

$$[3 + o(1)]^n$$

mutually congruent closed sets, the distance 1 being realized in none of the sets.

Assertion 2. If (as seems likely) a lattice packing of E^n with spherical balls can have density

$$\left[\frac{1}{\sqrt{(2 + o(1))}} \right]^n,$$

then E^n can be covered by a system of

$$[\sqrt{(8 + o(1))}]^n$$

mutually congruent closed sets, the distance 1 being realized in none of the sets.

Conjecture † 1. Suppose that the distance 1 is not realized in a closed subset S of a spherical ball B of radius 1. Then the Lebesgue measure of S is less than $(\frac{1}{2})^n$ times the Lebesgue measure of B .

† Note added in proof. In fact this conjecture was made some years ago by Leo Moser.

Conjecture 2. If n is of the form 2^r (and probably also for many other values of n) any system of m vectors

$$\mathbf{x}^{(\mu)} = (x_1^{(\mu)}, x_2^{(\mu)}, \dots, x_n^{(\mu)}), \mu = 1, 2, \dots, m,$$

with

$$x_i^{(\mu)} = \pm 1, i = 1, 2, \dots, n, \mu = 1, 2, \dots, m,$$

such that none of the scalar products

$$\mathbf{x}^{(\mu)} \cdot \mathbf{x}^{(\nu)}, 1 \leq \mu < \nu \leq m,$$

vanish, necessarily has

$$m = o\left(\frac{2^n}{n^2}\right).$$

Justification of Assertion 1. G. J. Butler in his thesis (London, 1968) and in [17] shows that there exists a lattice Λ in E^n so that the system

$$B + \mathbf{x}, \mathbf{x} \in \Lambda$$

of translates of the unit spherical ball B , by the vectors of Λ forms a packing, and similarly the system

$$\lambda B + \mathbf{x}, \mathbf{x} \in \Lambda,$$

with

$$\lambda = 2 + o(1),$$

forms a covering of E^n . Let π denote the Voronoi polyhedron, centre \mathbf{o} , associated with the packing

$$B + \mathbf{x}, \mathbf{x} \in \Lambda.$$

Then for a suitable δ with

$$0 < \delta = o(1),$$

the distance $4/3$ is not realized within the set

$$E + \bigcup_{\mathbf{x} \in \Lambda} \left\{ \frac{1}{3 + \delta} \pi + \mathbf{x} \right\}$$

which has asymptotic density

$$\left(\frac{1}{3 + \delta} \right)^n.$$

By the method of Erdős and Rogers [18], we can cover E^n by no more than

$$[n \log n + n \log \log n + 4n](3 + \delta)^n = (3 + o(1))^n$$

translates of E . Then the distance $4/3$ remains unrealized in the sets of this cover.

Justification of Assertion 2. If $B + \mathbf{x}, \mathbf{x} \in \Lambda$ is a lattice packing of E^n by unit spherical balls with density

$$\left[\frac{1}{\sqrt{2 + o(1)}} \right]^n,$$

and $0 < \delta = o(1)$, then the distance 1 will not be realized in the set

$$E = \bigcup_{\mathbf{x} \in \Lambda} \left\{ \frac{1}{2 + \delta} B + \mathbf{x} \right\}$$

of asymptotic density

$$\left(\frac{1}{2 + \delta}\right)^n \left[\frac{1}{\sqrt{2 + o(1)}}\right]^n.$$

The justification can be now completed as for Assertion 1.

Remarks on Conjecture 1. If a measurable set E has upper density exceeding $(\frac{1}{2})^n$, then, for each $d > 1$, there will be a spherical ball B of radius d with

$$\frac{\mu(B \cap E)}{\mu(B)} > (\frac{1}{2})^n,$$

and the conjecture would imply that d is realized within $E \cap B$. In the very special case when S is a connected set, its diameter is necessarily less than 1 so that its volume is less than the volume of the spherical ball of diameter 1, which is, of course, $(\frac{1}{2})^n$ times the volume of B , so that the conjecture holds.

Remarks on Conjecture 2. Let $m(n)$ be the maximal number of vectors satisfying the conditions of Conjecture 2. Then if more than $m(n)$ vectors are chosen from 2^n vectors

$$(\pm 1, \pm 1, \dots, \pm 1)$$

one pair at least, say x and y , will have

$$x \cdot y = 0$$

and so

$$\|x - y\| = \sqrt{(2n)}.$$

Thus the distance $\sqrt{(2n)}$ and the number $m(n)$ will be critical for the configuration of 2^n points. This leads to an improvement of Theorem 4 whenever (if ever)

$$m(n) < \frac{2^n}{N_n}.$$

Of course, if n is odd, we have $m(n) = 2^n$ and the configuration is useless. Further, if $n = 2r$ with r odd, we have $m(n) \geq 2^{n-1}$. But, if $n = 4r$ with r integral, it seems likely that $m(n)$ will be rather smaller. If there is a Hadamard matrix of order n , it is easy to show that $m(n) \leq 2^n/n$. On the other hand, if $n = 4r$, it is easy to show that

$$m(n) \geq 2 \sum_{t=0}^r \left(\begin{matrix} 4r \\ r-t \end{matrix} \right) \sim \left(\frac{6}{\pi n} \right)^{\frac{1}{2}} \left(\frac{4}{3^{\frac{1}{2}}} \right)^n,$$

the star indicating that the first term in the sum has to be multiplied by $\frac{1}{2}$. This leaves plenty of scope for improvement of Theorem 4 for large n , as $\frac{4}{3^{\frac{1}{2}}} < 2$.

Note added 25th May, 1972. We are grateful to Dr. P. Erdős for letting us know of an unpublished combinatorial lemma that he and Dr. V. T. Sós had discovered. This result enables us to improve and considerably simplify the above results for $10 \leq n \leq 22$ and $25 \leq n$. We are most grateful to Dr. Erdős and Dr. Sós for allowing us to reproduce their proof here.

The lemma takes the form:

Lemma 17 (P. Erdős and V. T. Sós). Let $n \geq 0$ be an integer and let

$$\begin{aligned} n' &= n, & \text{if } n &\equiv 0 \pmod{4}, \\ n' &= n - 1, & \text{if } n &\equiv 1 \pmod{4}, \\ n' &= n - 2, & \text{if } n &\equiv 2 \text{ or } 3 \pmod{4}. \end{aligned}$$

Then, if more than n' triples are chosen from a set of n distinct objects, at least one pair of triples have exactly one element in common.

Proof. We may take the n objects to be the integers $1, 2, \dots, n$. If $0 \leq n \leq 3$, there is at most one triple to choose and the result is trivial. Suppose then that $n \geq 4$ and that the lemma has been proved for all smaller values of n . Consider any system S of m triples chosen from $\{1, 2, \dots, n\}$ with the property that no two triples from S have exactly one element in common. If no two triples from S have any element in common we must have $3m \leq n$ so that

$$m \leq \frac{1}{3}n = n - \frac{2}{3}n \leq n - \frac{8}{3}$$

and

$$m \leq n - 3 < n'.$$

So we may suppose that S contains a pair of triples that have exactly two elements in common. Without loss of generality we may take these triples to be

$$\{1, 2, 3 \},$$

$$\{1, 2, 4\}.$$

First suppose that r triples, with $r \geq 3$ contain the objects 1, 2. Then these triples may be taken to be

$$\{1, 2, 3 \},$$

$$\{1, 2, 4 \},$$

...

$$\{1, 2, r+2\}.$$

Then no further triple can contain any of the objects $1, 2, \dots, r+2$. Now we can apply our inductive hypothesis to the further triples, if any, of S chosen from the objects $\{r+3, \dots, n\}$, if any. Thus

$$m \leq r + (n - r - 2) = n - 2 \leq n'.$$

Now return to the case when only the two triples

$$\{1, 2, 3 \},$$

$$\{1, 2, 4\},$$

contain both 1 and 2. Then the only triples that can contain any of the elements 1, 2, 3, 4 are the triples

$$\{1, 3, 4\},$$

$$\{2, 3, 4\}.$$

So at most 4 triples have any object from the set $\{1, 2, 3, 4\}$. Applying our inductive hypothesis to the further triples, if any, of S chosen from the $n - 4$ objects $\{5, 6, \dots, n\}$, if any, we again obtain $m \leq n'$. This completes the proof of the lemma.

This enables us to deduce immediately

LEMMA 18. For $n \geq 10$ there is a configuration of $M_n = \frac{1}{8}(n+1)n(n-1)$ points in E^n with critical distance 1 and with critical number $D_n = M_n/N_n'$ with

$$N_n' = \frac{1}{8}(n+1)(n-1), \text{ if } n \equiv 0 \pmod{4},$$

$$N_n' = \frac{1}{8}(n+1)n, \text{ if } n \equiv 1 \text{ or } 2 \pmod{4},$$

$$N_n' = \frac{1}{8}n(n-1), \text{ if } n \equiv 3 \pmod{4}.$$

Proof. We consider the configuration in E^{n+1} of $\frac{1}{6}(n+1)n(n-1)$ points with coordinates obtained by permutation of the coordinates of the point

$$\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0, 0, \dots, 0\right).$$

These points all lie on the n -dimensional hyper-plane with equation

$$x_1 + x_2 + \dots + x_{n+1} = 1\frac{1}{2}.$$

Further two such points are at distance 1 apart when for just one of the coordinates both points have coordinate $\frac{1}{2}$. Applying Lemma 17 the required result follows after some elementary calculations.

Now using Lemma 18 in place of the lemmas of the main text, we may with advantage use N_n' in place of N_n in Theorem 4 for $10 \leq n \leq 22$ and for $n \geq 25$.

References

1. H. Hadwiger, "Ein Überdeckungssätze für den Euklidischen Raum", *Portugaliae Math.*, 4 (1944), 140–144.
2. ———, "Ueberdeckung des Euklidischen Raumes durch Kongruente Mengen", *Portugaliae Math.*, 4 (1945), 238–249.
3. D. E. Raikii, The realisation of all distances in a decomposition of the space R^n into $n+1$ parts (Russian). *Mat. Zametki*, 7 (1970), 319–323.
4. ———, "The realisation of all distances in a decomposition of the space R^n into $n+1$ parts." *Math. Notes*, 7 (1970), 194–196.
5. D. R. Woodall, "Distances realized by sets covering the plane." *J. Combinatorial Theory*, A, to appear.
6. L. Moser and W. Moser, "Problem 10", *Canadian Math. Bull.*, 4 (1961), 187–189.
7. T. Gosset, "On the regular and semi-regular figures in space of n dimensions." *Messenger of Mathematics*, 29 (1900), 43–48.
8. H. S. M. Coxeter, "The pure Archimedean polytopes in six and seven dimensions", *Proc. Camb. Phil. Soc.*, 24 (1927), 1–9.
9. R. A. Rankin, "The closest packing of spherical caps in n dimensions." *Proc. Glasgow Math. Assoc.*, 2 (1955), 139–144.
10. K. Sarkadi and T. Szele, "Feladat 20", *Mat. Lapok*, 2 (1951), 76–77.
11. J. Aczél and T. Szele, "Feladat 35", *Mat. Lapok*, 3 (1952), 94–95.
12. J. Leech, "Some sphere packings in higher space." *Canadian J. Math.*, 16 (1964), 657–682.
13. ———, "Notes on sphere packings." *Canadian J. Math.*, 19 (1967), 251–267.
14. J. H. Conway, "A group of order 8, 315, 553, 613, 086, 720, 000." *Bull. London Math. Soc.*, 1 (1969), 79–88.
15. A. J. W. Hilton and E. C. Milner, "Intersection theorems for systems of finite sets." *Quart. J. Math., Oxford* (2), 18 (1967), 369–384.
16. D. J. Kleitman, "On a conjecture of Milner on k graphs with non-disjoint edges." *J. Combinatorial Theory*, 5 (1968), 153–156.
17. G. J. Butler, "Simultaneous packing and covering in Euclidean space." *Proc. London Math. Soc.*, to appear.
18. P. Erdős and C. A. Rogers, "Covering space with convex bodies." *Acta Arithmetica*, 7 (1962), 281–285.

Department of Mathematics,
University College London.

05B99: Combinatorics; Designs and configurations.

50B99: Geometry; Euclidean Geometry.

(Received on the 31st of January, 1972.)