Equidistant point sets

EQUIDISTANT POINT SETS

J. H. VAN LINT

In this talk we shall consider two problems which are both concerned with a set S of points in a metric space (R, d) such that for any 2 distinct points of S the distance d(x, y) is the same. Both problems are connected to several areas of combinatorial theory in the sense that these areas provide examples which often turn out to meet certain bounds which one can derive for these equidistant sets. One other analogy seems to be the fact that we do not really understand these problems yet.

1. Equiangular lines

In our first problem we take R to be elliptic space of dimension r - 1 and d to be elliptic distance. It is more convenient to describe this space by considering the lines through the origin in r-dimensional euclidean space $\mathbf{R}^r$ and defining the distance to be the angle between two such lines.

Definition. (i) $v_\alpha(r)$ is the maximum number of lines in $\mathbf{R}^r$ such that each pair of these lines makes an angle arccos α, $\alpha > 0$.
(ii) $v(r) := \max\{v_\alpha(r) \mid 0 < \alpha \leq 1\}$.

In 1965 Van Lint and Seidel [5] treated this problem for $r \leq 7$. A few months ago a paper by Lemmens and Seidel [3] appeared which extended the results to $r \leq 43$, however with a number of gaps. E. g. the value of v(14) is not known. These results revived my own interest in the problem. It seems worthwhile to point out some of the interesting connections to other areas of combinatorial theory. For a survey of the present state of affairs concerning v(r) we refer to [3].

Let S be a set of v unit vectors spanning $\mathbf{R}^r$ such that any two distinct vectors in S have inner product $\pm\alpha$. If G is the Gram matrix of S, then we write $A := \alpha^{-1}(G - I)$. Then A is a symmetric matrix with zero diagonal and all other entries ±1. Since G has smallest eigenvalue 0 with multiplicity $v - r$ the smallest eigenvalue of A is $-\alpha^{-1}$ with multiplicity $v - r$. In this way the problem of finding equidistant point sets is reduced to finding such (0, +1, -1)-matrices A such that the smallest eigenvalue is ≤ -1 and has a large multiplicity. Any such (0, +1, -1)-matrix A can be interpreted as the adjacency matrix of a graph on vertices $P_1, P_2, \ldots, P_v$ by including the edge $\{P_i, P_j\}$ iff $a_{ij} = -1$. Many good examples are connected to strong graphs which we now define. (We exclude void and complete graphs.)

Definition. Let A be the (0, +1, -1)-adjacency matrix of a graph on the vertices $P_1, P_2, \ldots, P_v$. If there are two integers p_1 and p_2 such that for any two vertices P_i, P_j with $a_{ij} = (-1)^h$ there are exactly p_h points joined by an edge to one, but not both, of P_i and P_j, then the graph is called <u>strong</u>. If the graph is also regular it is called <u>strongly regular.</u>

The following theorem makes it clear why these graphs are interesting for our problem.

Theorem 1 (cf. e. g. [6]). <u>A nonvoid and noncomplete graph of order</u> v <u>is strong if and only if its</u> (0, +1, -1)-<u>adjacency matrix satisfies</u>

$$(A - \rho_1 I)(A - \rho_2 I) = (v - 1 + \rho_1\rho_2)J, \quad (\rho_1 > \rho_2).$$

Clearly A has at most 3 distinct eigenvalues.

In [5] it was shown that $v(5) = 10$. The example was provided by the well known Petersen graph (five eigenvalues -3, five eigenvalues +3).

The following theorem shows how combinatorial designs can be combined to construct equidistant point sets.

Theorem 2. <u>If the projective plane</u> PG(2, q) <u>exists and if a Hadamard matrix of order</u> $q + 2$ <u>exists, then</u> $v(q^2+q+1) \geq (q+2)(q^2+q+1)$.

Proof. Let B be the incidence matrix of the plane. Let H be the Hadamard matrix with the first column consisting of 1's only. Delete the first column to obtain H_0. We replace each row of B by $q + 2$ new rows obtained by leaving the 0's where they are and replacing the 1's by the rows of H_0. We thus obtain a matrix A with $(q+2)(q^2+q+1)$ rows and $q^2 + q + 1$ columns such that any 2 rows have inner product ± 1 and every row is a vector of length $(q+1)^{\frac{1}{2}}$ in $\mathbf{R}^{q^2+q+1}$.

Due to our poor knowledge of projective planes the only example presently known whose order satisfies the conditions of Theorem 2 is $q = 2$ which yields $v(7) \geq 28$ (cf. [5]). Of course we can prove a more general theorem by taking B to be the incidence matrix of any block design with $\lambda = 1$ but this never gives examples near to known bounds. However, the incidence matrix of $PG(2, 2^l)$ in which we replace each line by a Hadamard matrix extended with a column of 1's yields the bound

$$v(2^{2l} + 2^l + 1) \geq 2^l(2^{2l} + 2^l + 1),$$

which is close to the result of Theorem 2.

Recently D. E. Taylor [7] proved that the inequality of Theorem 2 holds if $q + 1$ is a power of an odd prime. The examples obtained by this construction are best possible for small values of the parameter. We describe his construction. Let $q = p^n$ $(p \neq 2)$, (not the same q as above). Let $K = GF(q^2)$, V the 3-dimensional vector space over K and $\mathcal{P}(V)$ the corresponding projective plane. The equation

$$F(x_1, x_2, x_3; y_1, y_2, y_3) = x_1y_3^q + x_2y_2^q + x_3y_1^q = 0$$

defines a unitary polarity of $\mathcal{P}(V)$ (cf. [2]). Let $\mathcal{U}$ be the associated unital (absolute points, nonabsolute lines). Then $\mathcal{U}$ has $q^3 + 1$ points ([2], exercise 2.41). Take the line with equation $x_1 = 0$ as line at infinity and let ∞ be the point $(0, 0, 1)$ of $\mathcal{U}$. Then the q^3 other points of $\mathcal{U}$ are described by affine coordinates x, y. On these $q^3 + 1$ points we define a graph G as follows:

(1) (x, y) is joined to (a, b) if $\begin{cases} F(1, x, y; 1, a, b) \text{ is a square, } q \equiv -1 \pmod 4, \\ F(1, x, y; 1, a, b) \text{ is 0 or a non-square, } q \equiv 1 \pmod 4. \end{cases}$

(ii) ∞ is joined to all other points of $\mathcal{U}$.

Then G turns out to be a strong graph with incidence matrix A satisfying

$(A + qI)(A - q^2 I) = 0.$

Consequently, we have the following theorem.

Theorem 3. If $q = p^n$, $p \neq 2$, p prime, then

$v(q^2 - q + 1) \geq q^3 + 1.$

Since for $\varepsilon > 0$ and r sufficiently large there is a prime power between r and $r(1 + \varepsilon)$ we have

Theorem 4. $\lim_{r\to\infty} r^{-3/2} v(r) \geq 1.$

It is not difficult to show (cf. [3], [7]) that $v(r) \leq \frac{1}{2} r(r + 1)$ but I conjecture that actually $r^{3/2}$ gives the correct order of growth of $v(r)$.

2. Equidistant codes

Now let R be n-dimensional vector space over $GF(q)$ and let d be Hamming distance, defined by $d(\underline{x}, \underline{y}) := |\{i \mid x_i \neq y_i\}|$. We define the weight $w(\underline{x})$ of $\underline{x}$ by $w(\underline{x}) := d(\underline{x}, \underline{0})$.

Definition. An equidistant (m, k)-code is an m-subset S of R such that

$$\forall \underline{x} \in S \, \forall \underline{y} \in S \, [\underline{x} \neq \underline{y} \Rightarrow d(\underline{x}, \underline{y}) = k].$$

If H is a Hadamard matrix of order n then the n rows of $\frac{1}{2}(H + J)$ form an equidistant binary $(n, \frac{1}{2}n)$-code. From now on we take $q = 2$. With an equidistant $(m, 2k)$-code S we associate the matrix C which has as its rows all the code words of S. Each column C of S, interpreted as a binary vector, has a weight. If all these weights are 0, 1, $m - 1$ or m, we call S a trivial equidistant code. E. g. if $C = (I_m I_m \ldots I_m)$, k copies of I_m, then S is trivial with distance $2k$.

Let B be the incidence matrix of $PG(2, k)$ and let J be the $k^2 + k + 1$ by $k - 1$ matrix of 1's. Then

$$C = \left(\begin{array}{ccccc|cccc} 0 & 0 & \ldots & & 0 & 0 & \ldots & & 0 \\ & & B & & & & & J & \end{array} \right)$$

represents an equidistant $(k^2 + k + 2, 2k)$-code which is nontrivial. It was shown by M. Deza [1] that a nontrivial equidistant $(m, 2k)$-code has $m \leq k^2 + k + 2$. We now announce the following theorem ([4]).

Theorem 5. If a nontrivial equidistant $(k^2 + k + 2, 2k)$-code exists, then the projective plane $PG(2, k)$ exists.

Proof. We present a proof here which is shorter than the original proof given in [4]. We first remark that we can choose any row in C and by interchanging 0's and 1's change this row into a row of 0's. Then the other rows of the new matrix C all have weight 2k and any two of them have inner product k. In the following we always assume that C has a 0-row. We again use m for the number of rows of C. If a column of C has weight t then without loss of generality we can take this to be the first column and assume its t 1's are at the top. Let α_i be the number of 1's in the first t positions of column i and let β_i be the number of 1's in the last $m - t$ positions of column i. We define $a_i := \alpha_i/t$, $b_i := \beta_i/(m - t)$. Now we calculate the sum of the distances between respectively the first t rows, the last $(m - t)$ rows and between these two sets. We find

$$\sum a_i(1 - a_i) = k - k/t$$

$$\sum b_i(1 - b_i) = k - k/(m - t)$$

$$\sum \{a_i(1 - b_i) + b_i(1 - a_i)\} = 2k - 1.$$

Hence we have

$$\sum (a_i - b_i)^2 = -1 + \frac{k}{t} + \frac{k}{m - t},$$

i. e.

$$t(m - t) \leq mk.$$

Substituting $m = k^2 + k + 2$ we see that $t \leq k + 1$ or $t \geq k^2 + 1$. In the first case we call the column light, in the second case we call it heavy.

Now suppose there were $k + 2$ heavy columns. If any row had $k + 2$ 1's in these $k + 2$ positions all the others would have at most k

1's in these positions. In the same way there can be no more than $k + 2$ rows having $k + 1$ 1's in these $k + 2$ positions. In both cases the m rows together cannot have $(k + 2)(k^2 + 1)$ 1's in these $k + 2$ positions which contradicts the fact that the columns are heavy.

Now consider any row having q of its 1's in heavy columns. Clearly the sum of the inner products of the other rows with this row is at most $q(k^2 + k) + (2k - q)k$. Since this sum equals $k(k^2 + k)$ we have now shown that there are $k - 1$, k or $k + 1$ heavy columns.

If there are $k + 1$ heavy columns then by the reasoning used above there is a row having 1's in these $k + 1$ positions. Changing this row into the 0-row we find a C with only $k - 1$ heavy columns. If there are k heavy columns and the code is not trivial then there is a row having only $k - 1$ 1's in these heavy columns. Changing this row into the 0-row we find a C with $k + 2$ heavy columns, a contradiction. Therefore, if the equidistant code exists it can be represented by a C with the form

$$C = \begin{pmatrix} 0 & \cdots & 0 & \vdots & 0 & \cdots & 0 \\ & J & & \vdots & & B & \end{pmatrix}$$

where J has $k - 1$ columns. Now each row of B has $k + 1$ 1's and any two distinct rows of B have exactly one 1 in common. Since every column of B has at most $k + 1$ 1's, every column of B must have exactly $k + 1$ 1's. Hence B is the incidence matrix of PG(2, k). This completes the proof.

In the cases where PG(2, k) does not exist, e.g. $k = 6$, we have not been able to find the maximum number of code words in an equidistant code. For $k = 6$ this number is at least 32 since PG(2, 5) exists and at most 43 by Theorem 5. Since EG(2, 6) does not exist we tried to show that an equidistant (m, 12)-code has $m < 37$. By the same methods as used in the proof of Theorem 5 we could show that the existence of an equidistant binary (37, 12)-code implies the existence of an equidistant (29, 6)-code of word length 7 over an alphabet of 6 symbols which seems very unlikely. The work is being continued.

An obvious thing to try when one is looking for equidistant codes is to let C have the same form as above, i. e.

$$C = \begin{pmatrix} C & 0 & \ldots & 0 & \vdots & 0 & 0 & \ldots & 0 \\ & & B & & \vdots & & & J & \end{pmatrix}$$

where B is the v by b point-block incidence matrix of a block design with parameters $(v, k; b, r, \lambda)$ and J is the v by $r - 2\lambda$ matrix of 1's. Then C represents an equidistant $(v + 1, 2(r - \lambda))$-code. That this code cannot have many words is shown as follows.

Let $r - \lambda = d$. From the necessary conditions for v, k, b, r and λ we find (taking $k \leq \frac{1}{2}v$, w. l. o. g.)

$$d = \frac{\lambda(v - 1)}{k - 1} - \lambda = \frac{\lambda(v - k)}{k - 1},$$

i. e.

$$v = \frac{d(k-1)}{\lambda} + k \leq \frac{d(r-1)}{\lambda} + r = \frac{d(d+\lambda-1)}{\lambda} + d + \lambda \leq d^2 + d + 1,$$

where the last inequality is very weak unless $\lambda = 1$. For instance if $d = 6$, then an example yielding more than 32 words would have to have $v \geq 32$, hence $k \geq 6$, i. e. it would be EG(2, 6) which does not exist. It seems likely that a nontrivial equidistant (m, 12)-code has $m \leq 32$.

References

1. M. Deza. Une proprieté extremale des plans projectifs finis dans une classe de codes equidistants. Discrete Math. 6 (1973), 343-52.
2. D. R. Hughes and F. C. Piper. Projective planes. Springer Verlag, New York etc. (1973).
3. P. W. H. Lemmens and J. J. Seidel. Equiangular lines. Journal of Algebra, 24 (1973), 494-512.
4. J. H. van Lint. A theorem on equidistant codes. Discrete Math. 6 (1973), 353-8.
5. J. H. van Lint and J. J. Seidel. Equilateral point sets in elliptic geometry. Proc. Kon. Ned. Akad. v. Wetensch. Ser. A, 69 (1966), 335-48.
6. J. J. Seidel. Strongly regular graphs with (-1, 1, 0) adjacency matrix having eigenvalue 3. Linear Algebra and its Applications, 1 (1968), 281-98.

7. D. E. Taylor. Some topics in the theory of finite groups. Ph. D. thesis, Univ. of Oxford (1971).

Technological University,
Eindhoven, Netherlands