

On equidistant binary codes of length $n=4k+1$ with distance $d=2k$

Citation for published version (APA):

van Lint, J. H. (1984). On equidistant binary codes of length $n=4k+1$ with distance $d=2k$. *Combinatorica*, 4(4), 321-323. <https://doi.org/10.1007/BF02579143>

DOI:

[10.1007/BF02579143](https://doi.org/10.1007/BF02579143)

Document status and date:

Published: 01/01/1984

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

ON EQUIDISTANT BINARY CODES OF LENGTH
 $n=4k+1$ WITH DISTANCE $d=2k$

J. H. van LINT

Received 2 February 1984

The aim of this paper is to provide a short proof of the main result (Theorem 2.12) of [3], using standard methods from the theory of combinatorial designs.

We consider a binary alphabet F with symbols $+1$ and -1 . Let C be a code over F with wordlength $n=4k+1$ such that any two words have Hamming distance $d=2k$. Let $m:=|C|$.

We define the matrix A of size m by $4k+1$ by taking the words of C as the rows of A . Then the properties of C are described by

$$(1) \quad AA^T = 4kI + J.$$

Just as in the proof of Fisher's inequality (cf. [2] §10.2) it follows from (1) that A has rank m , i.e., $m \leq 4k+1$. We are interested in the case where $|C|$ is maximal, i.e., $m=4k+1$. Let $c_1, c_2, \dots, c_{4k+1}$ be the column sums of A . In other words $c = A^T j$. We define the matrix X by $X := A^T A$.

Then we have

$$Xc = A^T A A^T j = A^T (4kI + J) j = (8k+1) A^T j = (8k+1) c.$$

i.e., c is eigenvector of X with eigenvalue $8k+1$. Let u be an eigenvector of X with $Xu = \lambda u$ and $u^T c = 0$ (note that X is symmetric). From (2) we find

$$X^2 = A^T (4kI + J) A = 4kX + cc^T,$$

and hence

$$\lambda^2 u = X^2 u = (4kX + cc^T) u = 4k\lambda u,$$

i.e., $\lambda=4k$. We have proved the following fact:

$$(2) \quad X \text{ has eigenvalue } 8k+1 \text{ with multiplicity } 1 \text{ and eigenvalue } 4k \text{ with multiplicity } 4k.$$

This paper was submitted to *Combinatorica* at the request of the editors.
 AMS subject classification (1980): 05 B 05, 05 B 20

We now define a matrix $Y=(y_{ij})$ by $Y:=X-4kI$. Clearly all the entries y_{ij} are *odd* integers. We have

$$\sum_{i,j} (y_{ij}^2-1) = \text{tr}(Y^2)-(4k+1)^2$$

and by (2) the right-hand side is equal to 0. Therefore we have established the following fact:

(3) *The off-diagonal elements of $A^T A$ are equal to 1 or -1 .*

Consider any three columns of A (number them 1, 2, 3) and normalize the first in the usual way to j . We use the familiar Hadamard matrix counting argument cf. [2] §14.1). Let $+++$ occur α times in the three columns, $++-$ β times, $+-+$ γ times, $+- -$ δ times. Let ε_{ij} ($i, j=1, 2, 3$) denote the inner product of column i with column j .

Then

$$\alpha + \beta + \gamma + \delta = 4k + 1$$

$$\alpha + \beta - \gamma - \delta = \varepsilon_{12}$$

$$\alpha - \beta + \gamma - \delta = \varepsilon_{13}$$

$$\alpha - \beta - \gamma + \delta = \varepsilon_{23}$$

from which we find

$$4\alpha = 4k + 1 + \varepsilon_{12} + \varepsilon_{13} + \varepsilon_{23}.$$

This implies that either all the ε_{ij} are equal to 1 or exactly one of them is 1, the other two being -1 . This means that if we call two columns of A related if their inner product is not -1 , then this relation is an equivalence relation and furthermore we see that the columns of A can be partitioned into two equivalence classes, say of size t and $4k+1-t$, such that after a reordering of the columns we have

$$(4) \quad A^T A = \begin{pmatrix} 4kI+J & -J \\ -J & 4kI+J \end{pmatrix},$$

where the matrices on the diagonal have size t resp. $4k+1-t$. W.l. o. g. we may assume that the first row of A is j^T . It follows that all other rows of A have $2k+1$ entries $+1$ and $2k$ entries -1 . Therefore

$$j^T A^T A j = (4k+1)^2 + 4k.$$

On the other hand (4) implies that

$$j^T A^T A j = t(2t-1) + (4k+1-t)(8k-2t+1).$$

Combining these two equations we find

$$t = \frac{1}{2} (4k+1 \pm \sqrt{8k+1}).$$

Since t is an integer, $8k+1$ must be the square of an odd integer, i.e.,

$$(5) \quad k = \frac{1}{2}(u^2+u) \text{ and } t = u^2 \text{ or } t = (u+1)^2, \quad (u \in \mathbf{Z}).$$

We shall now show that the existence of the equidistant code C of size $4k+1$ implies the existence of a certain block design and vice versa. In order to do this we define the matrix

$$B := A \begin{pmatrix} -I & 0 \\ 0 & I \end{pmatrix}.$$

By (4) and the fact that C is equidistant we have

$$(6) \quad BB^T = B^T B = 4kI + J.$$

Note that (6) implies that

$$BB^T B = 4kB + JB = 4kB + BJ,$$

so $BJ = JB = \gamma J$ and hence $\gamma^2 = 4k + (4k+1) = (2u+1)^2$. It follows that B is the ± 1 incidence matrix of a $2 - ((2u^2+2u+1), u^2, 1/2(u^2-u))$ design. Conversely, if such a design exists, the rows of its incidence matrix are the words of the equidistant code C . Therefore the following theorem has been proved (cf. [3]):

Theorem. *An equidistant binary code with wordlength $n=4k+1$ and distance $d=2k$ exists if and only if $k=1/2(u^2+u)$ and there exists a $2 - (2u^2+2u+1, u^2, 1/2(u^2-u))$ design. ■*

Remark. It is known that such designs exist if u is a prime power. They were constructed independently by R. M. Wilson (unpublished) and A. E. Brouwer [1].

References

- [1] A. E. BROUWER, An infinite series of symmetric designs, *to appear*.
- [2] M. HALL, JR., *Combinatorial Theory*, Blaisdell Publ. Co., Waltham, Mass. 1967.
- [3] D. R. STINSON and G. H. J. VAN REES, The equivalence of certain equidistant binary codes and symmetric BIBDs, *Combinatorica* 4 (1984), 357—362.

J. H. van Lint

*Department of Mathematics and Comp. Sci.
University of Technology
Den Dolech 2
P.O.B. 513
5600 MB Eindhoven
The Netherlands*