van Lint, Jacobus H.; **Wilson, Richard M.**
On the minimum distance of cyclic codes. (English) Zbl 0616.94012
IEEE Trans. Inf. Theory 32, 23-40 (1986).

A new lower bound for the minimum distance of cyclic codes is given that includes the earlier BCH, Hartmann-Tzeng and Roos bounds. For n-vectors $\underline{a}$ and $\underline{b}$ let $\underline{a}^*\underline{b}$ be the Hadamard product. For an $m \times n$ matrix $\underline{A}$ and $k \times n$ matrix $\underline{B}$, $\underline{A}^*\underline{B}$ is the matrix that has as rows all the products $\underline{a}^*\underline{b}$ where $\underline{a}$ is a row of $\underline{A}$ and $\underline{b}$ is a row of $\underline{B}$. For $I \subset \{1, 2, ..., n\}$ let $\underline{M}_I$ be the submatrix of a matrix of $\underline{M}$ consisting of the columns designated by I. One of the main tools used in the work is the following Theorem: Let $\underline{A}$ and $\underline{B}$ be matrices with entries from the field F and let $\underline{A}^*\underline{B}$ be a parity check matrix for the code C over F. If I is the support of a codeword in C, then $\text{rank}(\underline{A}_I) + rank(\underline{B}_I) \leq |I|$. In particular, C has minimum distance $\geq \delta$ if $\text{rank}(\underline{A}_I) + rank(\underline{B}_I) \leq |I|$ for every subset I of { 1,2,...,n} for which $|I| < \delta$.

If α is a primitive nth root of unity in an extension field F_{q^m} over F_q, the set $A = \{\alpha^{i_1}, ..., \alpha^{i_\ell}\}$ is called a defining set of a code C iff $c(\xi) = 0$ for all $\xi \in A$ and for all c(x)$\in C$. The matrix $\underline{M}$(A) is the $\ell \times n$ matrix whose jth row is $(1, \alpha^{i_j}, ..., \alpha^{(n-1)i_j})$. The results of the paper are obtained by applying the theorem to matrices of the form $\underline{M}$(A). For all binary cyclic codes of length less than or equal to 63, with wo exceptions, the methods obtained yield the true minimum distance. Some results for longer length codes are also given.

Reviewer: I.F.Blake

MSC:

94B15 Cyclic codes
05B20 Combinatorial aspects of matrices (incidence, Hadamard, etc.)

Cited in **4** Reviews
Cited in **35** Documents

Keywords:

code bounds; lower bound for the minimum distance of cyclic codes

Full Text: DOI

Edited by FIZ Karlsruhe, the European Mathematical Society and the Heidelberg Academy of Sciences and Humanities
© 2021 FIZ Karlsruhe GmbH