planetmath.org

Math for the people, by the people.

cyclic code

Canonical name	CyclicCode
Date of creation	2013-03-22 15:12:56
Last modified on	2013-03-22 15:12:56
Owner	GrafZahl (9234)
Last modified by	GrafZahl (9234)
Numerical id	6
Author	GrafZahl (9234)
Entry type	Definition
Classification	msc 94B15
Related topic	LinearCode
Related topic	Code

Let C be a linear code over a finite field A of block length n. C is called a *cyclic code*, if for every codeword $c = (c_1, \ldots, c_n)$ from C, the word $(c_n, c_1, \ldots, c_{n-1}) \in A^n$ obtained by a right shift of is also a codeword from C.

Sometimes, C is called *the c*-cyclic code, if C is the smallest cyclic code containing c, or, in other words, C is the linear code generated by c and all codewords obtained by shifts of its .

For example, if $A = \mathbb{F}_2$ and $n = 3$, the codewords contained in the $(1, 1, 0)$-cyclic code are precisely

$$(0, 0, 0), (1, 1, 0), (0, 1, 1) \text{ and } (1, 0, 1).$$

Trivial examples of cyclic codes are A^n itself and the code containing only the zero codeword.