Cyclically Permutable Codes Specified by Roots of the Generator Polynomial

J. S. Lemos-Neto

and

V. C. da Rocha Jr.

Communications Research Group - CODEC
Department of Electronics and Systems
Federal University of Pernambuco
Recife, BRAZIL

Campinas, January 2015

Introduction

Objective:

- The goal of the theory in this work is the construction of cyclically permutable codes (CPC).

Definition:

- A CPC is a binary code the codewords of which are cyclically distinct and have full cyclic order.

Theorem 1: full cyclic order for all nonzero codewords

- Let $\mathcal{C}$ be a linear q-ary cyclic (n, k, d) and let n be a divisor of $q^m - 1$;
- If and only if the set of roots of $g(x)$ includes all roots of $x^n - 1$ which have multiplicative order less than n.

Construction of Cyclically Permutable Codes

Theorem 2: CPC constructed by means of cyclic codes

- Let $\mathcal{C}$ be a linear q-ary cyclic (n, k, d) and let $n = q^m - 1$;
- generator polynomial $g(x)$ whose roots satisfy Theorem 1;
- $c(x) = g(x)[1 + s_i(x)m_i(x)] \prod_{j=1}^{i-1} s_j(x) \mod x^n - 1$;
- The number of cyclic equivalence classes generated is precisely $(q^k - 1)/n$ (optimal in this sense).

That's all folks!

Thank you!