ON A NEW CLASS OF BINARY GROUP CODES (*)

G. Dagnino

ABSTRACT - A new class of binary group error-correcting codes is formalized and defined. The codes are generated by irreducible and primitive polynomials over the binary field by an iterative procedure. A general formula for the number of correctible errors related to the length n of the code vectors is given. A method to obtain from a given code a class of subcodes is described. The encoding and decoding (error-detecting, error-correcting) procedures are extremely simple and use linear shift registers. A general formula describing the number of operations involved is given.

1. Introduction.

The purpose of this paper is to show how a class of linear codes can be constructed having some properties typical of the cyclic codes. In fact, as it will be shown in Section 3, the code space is an interconnection of cyclic subspaces. It will be also shown that a given code can be subdivided in « blocks » completely independent from the overall structure, so that subcodes may be formed concatenating such « blocks » (the definition of block is formally given in Section 3). The correction procedure proposed in this paper is concerned not in finding the errors occurred, but in finding an error free « subvector » and from it generate the error free code word (the formal definition of « subvector » is given in Section 3, while the error correcting procedure is given in Section 5).

2. Mathematical Background.

In this paper polynomials (or n-tuples) will be considered with coefficients over the field $\mathbb{Z}_2$ of integers modulo 2. We shall denote the Euclidean ring

(*) This work has been supported by the National Science Foundation under grant number GP-2122 and represents part of the doctoral dissertation.
— Ricevuto il 8-10-1967.
of such polynomials by \( J_2[x] \). Let \( g(x) \) be an irreducible and primitive polynomial such that \( \deg(g(x)) = r \). Since \( g(x) \) is irreducible, \( (g(x)) \) is the maximal ideal generated by \( g(x) \) in \( J_2[x](r) \), hence \( J_2[x]/(g(x)) \) is a Galois field of \( 2^r \) elements, or \( GF(2^r) \). Since \( g(x) \) is primitive, the \( 2^r - 1 \) elements of the multiplicative group of \( GF(2^r) \) will be given as powers of \( x \), where \( x \) is a root of \( g(x) \). The multiplicative group of \( GF(2^r) \) is thus cyclic with the polynomial \( g(x) \) as generator.

Let \( r_0(x) \) be a polynomial of degree \( k - 1 \) (\( k \leq r \))

\[ r_0(x) = a_{k-1} x^{k-1} + a_{k-2} x^{k-2} + \ldots + a_0 x^0. \]

Let \( a_i \in J_2 (i = 0, 1, \ldots, k - 1) \) represent arbitrarily \( n \) information symbols. Using the division algorithm one can say:

\[ \begin{align*}
(2.1) & \quad x^r r_0(x) = q_1(x) g(x) + r_1(x) \\
(2.2) & \quad x^r r_1(x) = q_2(x) g(x) + r_2(x) \\
(2.3) & \quad x^r r_i(x) = q_{i+1}(x) g(x) + r_{i+1}(x)
\end{align*} \]

where \( r_i(x) \in GF(2^r) \). We need the following.

**Theorem 2.1.** If \( \gcd(r, 2^r - 1) = 1 \) then \( x^r r_{2^r - 2}(x) \equiv r_{2^r - 1}(x) \) modulo \( g(x) \), where \( r_{2^r - 1}(x) \equiv r_0(x) \).

**Proof.** Using equations (2.1), (2.2) and (2.3) the following, modulo \( g(x) \), holds:

\[ \begin{align*}
(2.4) & \quad x^r r_0(x) \equiv r_1(x) \\
& \quad x^{2r} r_0(x) \equiv r_2(x) \\
& \quad \ldots \ldots \\
& \quad x^{i \cdot r} r_0(x) \equiv r_i(x).
\end{align*} \]

Since \( x \) is a root of \( g(x) \), then \( x^{2^r - 1} \equiv x^0 \equiv 1 \), and since \( \gcd(r, 2^r - 1) = 1 \), for any integer \( i < 2^r - 1 \), \( x^{ir} \neq x^0 \).