Proc. of the National Seminar on Algebra
Bharathidasan University
1993
73-77

ON SOME LINEAR CODES USING SEMIGROUP RINGS

W.B.Vasantha Kandasamy and Suresh Babu

In this note we construct some linear codes using semigroup rings using a special encoding and decoding procedure. It is shown that these codes can be simultaneously used for error correction and authentication.

Throughout this paper $Z_2 = \{0, 1\}$ is the prime field of characteristic two and S a multiplicative semigroup, Z_2S the semigroup ring. Suppose $n > 1$ be the desired length of the code word. Choose a semigroup S of order n and consider the corresponding semigroup ring Z_2S. Let I be a subspace of Z_2S of dimension 'k' I is chosen according to channel requirement. Let $J = \{y \in Z_2 S \mid x.y = 0 \text{ for all } x \in I\}$; J is a subspace of Z_2S. Choose a semigroup T of order 'k' then the space $M = Z_2T$ is called the message space. Let f be a bijection between T and a fixed basis B of I. Now f is called the coding function. The triple {M, f, I} is called a code set. Using the coding function f we encode our message. A procedure for getting the code word is given in this paper.

Suppose A and B are the partners. Each will choose a semigroup of order k say T_A, T_B, respectively. The message spaces for A and B are respectively $Z_2 T_A$ and $Z_2 T_B$. Let f_{AB} be a bijection between $Z_2 T_A$ and $Z_2 T_B$, so each message in $Z_2 T_A$ is equivalent to some message in $Z_2 T_B$. Both A and B

e-mail: vasantha@iitm.ac.in
web: http://mat.iitm.ac.in/~wbv

know each others message set. f_A and f_B be the coding functions for A and B respectively when B receives a word it is decoded by applying f^{-1}_B which he only knows. Since the semigroups T_A and T_B are arbitrary and the message spaces are known only to A and B an intercepter cannot decode any message. Thus the secrecy is preserved.

e-mail: vasantha@iitm.ac.in
web: http://mat.iitm.ac.in/~wbv