PROCEEDINGS OF 2002 IEEE INFORMATION THEORY WORKSHOP
20–25TH October 2002.
Indian Institute of Science, Banglore
Bangalore, KA
India

MULTI-COVERING RADII OF CODES WITH RANK-METRIC

W.B.Vasantha Kandasamy and R.S.Selvaraj

The notion of multi-covering Radius, a generalization of the covering radius, was defined for codes with Hamming metric over GF(2) to study the existence of stream ciphers secure against a large class of attacks. If m is a positive integer, then the m-covering radius $t_m(C)$ of a block code C of length n is the smallest positive integer t such that every set of m vectors in $[GF(2)]^n$ is contained in at least one ball of radius t around a codeword in C.

Let V^n be n-dimensional vector space over $GF(2^N)$ ($\leq$ N and N > 1). An RD code [1] is a subspace of V^n wherein the weight (norm) of each vector $x = (x_1, x_2, \ldots, x_n) \in V^n$ (denoted by r(x) or wt(x)) is defined to be the maximum number of its coordinates xi that are linearly independent over GF(2). This norm induces a rank metric on V^n: $d(x, y) = r(x + y)$, for $x, y \in V^n$. For $S \subseteq V^n$, the weight of a set S is $wt(S) = \max\{wt(x) / x \in S\}$. Let $cov(x, S) = \max\{d(x, y)/y \in S\}$ and $cov(C, S) = \min\{cov(c, S) /c \in C\}$. Then $t_m(C) = \max\{cov(C, S) / S \subseteq Vn$ and $|S| = m\}$. Denote (u | v) as concatenation of vectors u and v; $t_m[n, k]$ as smallest m-covering radius among all [n, k] codes.

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