Abstract

The transmission of data in the presence of errors and erasures over random networks, in situations where there is only partial information regarding the underlying network topology, has been interpreted in terms of the transmission and recovery of subspaces of an ambient vector space over a finite field. Under this representation, a random network code is a collection of such subspaces. The present thesis explores several algebraic techniques for constructing constant and non-constant dimension codes for random networks. Orbit codes are constant dimension codes which are orbits of suitable subgroups of the general linear group acting on the subspaces in a Grassmannian. One contribution of the present thesis is to link the construction of Singer cycle orbit codes possessing a given minimum subspace distance with the construction of cyclic difference sets with the appropriate parameters.

In a second contribution, we interpret two constructions of constant dimension codes, namely, the lifting construction and its generalization using Ferrers diagram rank-metric (FDRM) codes, in terms of Plücker coordinates. We show that both constructions can be described via a two-step procedure. In the first step, a set of indices which provides a non-zero Plücker coordinate is identified; in the second, the remaining Plücker coordinates of the lifted subspace are computed by replacing the columns of the original matrix in row-reduced echelon form with those of the matrix to be lifted.

In the existing literature, balls of a given radius cantered at a subspace codeword of a constant dimension code has been interpreted as Schubert systems. We establish that the balls of the same radius cantered at a codeword of the dual subspace code are characterized by the classical dual of the original Schubert system. A method for constructing non-constant dimension subspace codes is proposed, similar to the two-step existing construction with FDRM codes. In the proposed method, the characteristic tuple is used to characterize a Schubert cell. Bounds on the subspace distance and the injection distance among the chosen Schubert cells are obtained in terms of the symmetric distance and a modified symmetric distance between the characteristic tuples. It is shown that our framework is equivalent to the existing construction when FDRM codes are employed.

Based on some modifications of the nearly optimal (5; 3)2 code given by Etzion and Vardy, 4 optimal (5; 3)2 codes are constructed. It is shown that all these sporadic examples fall outside the framework of the recent construction of Honold et al. The radical ideals of a Noetherian commutative ring have unique decomposition as the intersection of prime ideals. This fact is used to construct constant weight codes on the power set of a set of radical ideals. These constant weight codes are suitable for store and- forward (SAF) routing over random networks. Several upper and lower bounds on the sizes of such codes are verified. In this context, the search for codes which achieve a Johnson bound is interpreted as the search for maximal subgraphs in the generalized Johnson graph corresponding to the subset code.

A generalization of the above construction is achieved by considering lattices having irredundant primary decomposition and unique (meet) irreducible decomposition, respectively. The difference between the criteria for these decompositions is established and the primary decomposition in Dedekind domains shown as a common example. In addition, the unique decomposition in lattices in terms of prime elements is formulated in the former case. Construction of constant weight codes for SAF routing is indicated. Finally, the random linear network coding problem has been formulated on the lattice of ideals as well as on the lattice of radical ideals of rings.