Abstract

In a communication system, data are transmitted from a sender to a receiver via a channel. This channel is often affected by many sources of noise and interference, which may damage the data during transmission. It is not always possible to get rid of this problem by simply improving the quality of communication channel. To overcome this situation, error-correcting codes are helpful upto a great extent to detect and even correct errors that occur when data are transmitted across some noisy channel. Linear codes have been in use in communication systems and data storage in daily life. We are interested in codes with high error-correcting capacity and minimum redundancy; in other words, we want to find codes with large minimum "Hamming distance" and small "length". High minimum distance and small length are controversial goals for the optimization of codes. A linear code C is called distance optimal if there exists no linear code with higher minimum distance (than that of C) but with the same code length and the same code size (as that of C). A distance optimal code has the highest possible error-correcting capacity for a given code length and code size.

Secret sharing schemes are becoming essential nowadays; in fact, these are used heavily in electronic voting systems, cryptographic protocols, banking systems, etc. "Minimal linear codes" have interesting applications in secret sharing schemes and secure two-party computation. "LCD codes" are important linear codes due to their use in implementations against side-channel attacks and fault injection attacks. Thus, it is of great interest to construct and investigate linear codes which have many applications, for instance, LCD codes, minimal codes and distance optimal codes.

In this thesis, we construct linear codes over certain finite fields and finite rings and study their algebraic structures. The non-unital rings I, E and F (notation is due to Fine [26]) are used as code alphabets. We use the mathematical object called simplicial complex in this construction. Using these linear codes, we obtain two types of binary linear codes. The first one (called subfield or subfield-like codes) is obtained with the help of certain linear functionals (for instance, the trace map) and

the other one is obtained with the help of certain isomorphisms of vector spaces (called Gray maps). The weight distributions of all these codes are computed. Most of these binary codes are few-weight minimal linear codes. With respect to the "Griesmer bound", a few classes of distance optimal codes are obtained. Sufficient conditions for these binary linear codes to be self-orthogonal are obtained. This is the first attempt to study the structure of linear codes over non-unital rings using simplicial complexes.

The hull of a linear code is the intersection of the code with its dual. We construct linear codes over finite fields using multiplicative characters of other finite fields and study their hull. We discuss certain sufficient conditions under which these are either linear complementary dual (in short, LCD) codes or linear codes with one-dimensional hull. General Gauss sums are used heavily to achieve these results. Finally, we show that if the base field is of characteristic 2, these codes are isodual. An additive complementary dual (in short, ACD) code is a generalization (in fact, an exact analogue) of an LCD code in the class of additive codes. ACD codes are considered over the ring $\mathbb{Z}_2\mathscr{R}$, where $\mathscr{R} = \frac{\mathbb{Z}_2[u]}{\langle u^4 \rangle}$. We investigate free "self-dual codes" over $\mathscr{R}$. A condition that ensures an additive code to be an ACD code is established. Furthermore, for a separable additive code to be an ACD code, a necessary and sufficient condition is established. We consider a Gray map under which certain additive codes become binary LCD codes. We also present a few optimal (or almost optimal) binary LCD codes. Moreover, a number of weight enumerators are computed and the corresponding MacWilliams identities are discussed.