NEW ALGEBRAIC CONCEPTS AND THEIR APPLICATIONS IN CODING THEORY

During the transmission of data over a communication channel, errors are inevitable. Coding theory aims to design efficient encoding schemes that enable such errors to be detected and, when possible, corrected. Linear codes, and in particular their subclass of cyclic codes, play a fundamental role in modern communication systems and data storage technologies used in everyday life. Determining the distance of a linear code is, in general, a hard problem, even for structured families such as cyclic codes. In particular, maximum distance separable (MDS) codes attain the largest possible distance as determined by the Singleton bound and are therefore distance-optimal. Reed–Solomon codes are the most prominent examples of MDS codes and are widely used in practice. Beyond Reed–Solomon codes, the construction and structural analysis of MDS codes that are not equivalent to Reed–Solomon codes are a challenging and active area of research.

Let $\mathbb{F}$ be a field. A central algebraic tool employed in this thesis is the notion of an $\mathbb{F}$-valued trace on a finite-dimensional commutative $\mathbb{F}$-algebra. A non-zero $\mathbb{F}$-valued $\mathbb{F}$-linear map on a finite-dimensional commutative $\mathbb{F}$-algebra is called an $\mathbb{F}$-valued trace if its kernel contains no non-zero ideals. However, given an $\mathbb{F}$-algebra, such a map may not always exist. In this thesis, we find an infinite class of finite-dimensional commutative $\mathbb{F}$-algebras which admit an $\mathbb{F}$-valued trace. We present a couple of applications of an $\mathbb{F}$-valued trace map to algebraic coding theory.

Using the $\mathbb{F}_2$-valued trace of commutative $\mathbb{F}_2$-algebras $\mathcal{R}_2 := \mathbb{F}_2[x]/\langle x^3 - x\rangle$ and $\mathcal{A}_s := \mathbb{F}_2[x]/\langle x^s\rangle$, for $s \geq 2$, we study the (binary) subfield codes $\mathcal{C}_D^{(2)}$ of simplicial $\mathcal{C}_D$-codes over $\mathcal{R}_2$ and $\mathcal{A}_s$. We explicitly determine the Hamming weight distribution of these subfield codes and derive sufficient conditions under which they are minimal, for various choices of the defining set D constructed via simplicial complexes. To the best of our knowledge, this work constitutes the first systematic study of subfield codes of codes over an $\mathbb{F}_2$-algebra, and in particular, the first instance in which such subfield codes are explicitly computed using an $\mathbb{F}_2$-valued trace.

We next study two families of cyclic codes over $\mathbb{F}_q$ of length n denoted by $\mathcal{C}_n$ and $\mathcal{C}_{n,1}$, which are generated by the n-th cyclotomic polynomial $Q_n(x)$ and the polynomial $Q_n(x)Q_1(x)$, respectively. For each integer $n > 1$, we derive explicit formulae for the distances of $\mathcal{C}_n$ and $\mathcal{C}_{n,1}$, and we also obtain a formula for the distance of their Euclidean duals. Moreover, we show that all these codes are LCD, and several subfamilies are both r-optimal and d-optimal locally recoverable codes.

Lastly, we present a new class of codes called row-column twisted Reed–Solomon codes (abbreviated as RCTRS), motivated by the works of Beelen et al. and Liu et al. We explicitly provide conditions for such codes to be MDS and also ensure their existence. By determining the dimensions of their Schur squares, we prove that these MDS codes are inequivalent to Reed–Solomon codes, thus presenting a new family of non-RS MDS codes.