Abstract

Long codes are judged on the basis of their parameters (δ, R) where δ is the relative minimum distance and R is the code rate i.e. if $[N, K, D_{min}]$ are the length, dimension and minimum distance of the code respectively, then

$$\delta = \frac{D_{min}}{N} \quad \text{and} \quad R = \frac{K}{N}$$

The best long codes lie in the region defined by the GilbertŋVarshamov lower bound and the McEliece, Rodemich, Rumsey and Welch upper bound. One of the challenges in coding theory has been the construction of codes with symbol alphabet size fixed at r and growing length whose performance exceeds that of the G-V bound.

Around 1980, V. D. Goppa used the theory of algebraic curves to construct a new family of codes, now referred to as algebraic geometric (AG) codes. The length N of an AG code defined over a curve of genus g, is roughly equal to the number of rational points on the curve. The performance of an AG code of length N is governed by the equation

$$R \geq 1 - \delta - \frac{g}{N}.$$

Good codes result when the ratio g/N is small. However, the Drinfeld-Vladut (D-V) bound states that this ratio cannnot be too small:

$$\liminf_{g \to \infty} \frac{g}{N} \geq \frac{1}{\sqrt{r} - 1}.$$

In 1982, Tsfasman, Vladut and Zink showed for the case r is a perfect square, the existence of curves over $\mathbb{F}_r$, known as modular curves, whose g/N ratio achieves the D-V bound. However, the modular curves in did not have a simple explicit description.

In a major step forward in 1996, Garcia and Stichtenoth showed that two explicitly described towers of function fields also achieve the D-V bound. For an explicit description of AG codes based on these function fields one requires the determination of a basis for the vector space $\mathcal{L}(mP)$, which comprise functions having poles only at a specified place P, with pole order bounded by m.

In the main part of my dissertation I describe a new approach for construction of an algorithm for explicit description a basis of the vector space $\mathcal{L}(mP)$ in the second tower of Garcia and Stichtenoth.

I examine also automorphisms of this function fields and present a new proof for the fact that the first tower of Garcia and Stichtenoth achieves the D-V bound.

Keywords

AG codes, algebraic geometric codes, function field tower, Gilbert-Varshamov bound, integral basis.