Véges geometria és Hermit-kódok

Korchmáros Gábor

Potenza, Olaszország

Abstract

Véges geometria néhány olyan problémájával foglalkozunk, melyeket Hermit-görbén definiált AG (algebrai geometria) hibajavító kódok aktuális kutatása hozott felszínre.

Finite geometry and Hermitian codes

Gábor Korchmáros

Potenza, Italy

Abstract

We deal with some problems in Finite geometry arising from current research on AG (algebraic-geometry) error correcting codes defined over the Hermitian curve.

In $PG(2, q^2)$, let $\mathcal{H}$ be the Hermitian curve. For a fixed positive integer d, let $\mathbf{S}_d$ be the family of all degree d plane algebraic curves (possibly singular or reducible) defined over $\mathbf{F}_{q^2}$ which do not have $\mathcal{H}$ as a component. A natural question in Finite geometry is to ask for the maximum number $N(d)$ of common points in $PG(2, q^2)$ of $\mathcal{H}$ with $\mathcal{S}$ where $\mathcal{S}$ ranges over $\mathbf{S}_d$. From Bézout's theorem, $N(d) \leq d(q + 1)$. The problem of finding better upper bounds on $N(d)$ for certain families of curves $\mathbf{S}$ is motivated by the "minimum distance problem" for AG-codes.

A family of curves which play role in the study of Hermitian codes is defined as follows:

Let β be a Baer involution of $PG(2, q^2)$ which preserves $\mathcal{H}$. The set of points of $\mathcal{H}$ which are fixed by β has size $q + 1$ and it is the complete intersection $\mathcal{H} \cap \mathcal{C}^2$ of $\mathcal{H}$ with an irreducible conic $\mathcal{C}^2$. For a positive integer m less than $q + 1$, define D to be the set of all points of $\mathcal{H}$ other than those in U, together with the divisor (formal sum) G of points on $\mathcal{H}$:

$$\mathsf{G} := m \sum_{\mathcal{H}\cap\mathcal{C}^2} P.$$

The functional AG-code $C_L(\mathsf{G}, D)$ is obtained taking the rational functions with pole numbers at most m at any point in $\mathcal{H} \cap \mathcal{C}^2$ and evaluating them at the points of D.

For m even, the minimum distance problem for $C_L(D, G)$ is equivalent to the problem of determining the maximum number of points on $\mathcal{H} \cap \mathcal{S}$ with $\mathcal{S} \in \mathbf{S}_m$.

For m odd, let $\mathbf{T}_{m+1}$ be the subfamily of $\mathbf{S}_d$ consisting of all curves $\mathcal{T}$ of degree $m + 1$ which contain all points in D. The minimum distance problem for $C_L(D, G)$ is equivalent to the problem of determining the maximum number of points on $\mathcal{H} \cap \mathcal{T}$ with $\mathcal{T} \in \mathbf{T}_{m+1}$.

The automorphism group of $C_L(D, G)$ is isomorphic to $G \cong P\Gamma L(2, q)$

We address the above problems using tools from Finite geometry.