Hyperovals in finite projective planes

Kai-Uwe Schmidt

Paderborn University, Germany

Let q be a power of two and let $\mathbb{F}_q$ be the finite field with q elements. An *arc* in the projective plane $\mathbb{P}^2(\mathbb{F}_q)$ is a set of points of $\mathbb{P}^2(\mathbb{F}_q)$ with the property that no three of them are collinear. The maximum number of points in an arc in $\mathbb{P}^2(\mathbb{F}_q)$ is $q+2$, and in case of equality the arc is called a *hyperoval*. Hyperovals have applications in statistics, cryptography, and coding theory and have been studied extensively by finite geometers since the 1950s with the ultimate goal of establishing a complete classification. In spite of this, classification results for hyperovals were rather scarce until recently.

It is well known that hyperovals in $\mathbb{P}^2(\mathbb{F}_q)$ are in one-to-one correspondence to polynomials with certain properties, called *o-polynomials of* $\mathbb{F}_q$. This provides a powerful approach to study hyperovals and brings in methods from algebraic geometry. In this talk, I will describe the history of the hyperoval classification problem, survey prior results, and discuss a recent advance, which gives a complete classification of o-polynomials of $\mathbb{F}_q$ whose degree is sufficiently small compared to q.