On algorithms for finding the missing functions

Ruud Pellikaan

Let $X$ be curve defined over a finite field $\mathbb{F}_q$. Let $Q$ be an $\mathbb{F}_q$-rational point of $X$. Let $\mathbb{F}_q(X)$ be the function field of rational functions on $X$, and $\mathbb{F}_q(X, Q)$ the ring of rational functions on $X$ that are regular outside $Q$.

In the construction of one-point algebraic geometric codes and their decoding according to Feng-Rao the ring $\mathbb{F}_q(X, Q)$ plays a crucial role. Therefore we are looking for an "easy" and "explicit" description of this ring.

Suppose that the curve $X$ is given by an affine part $X_0$ in affine space $\mathbb{A}^m$ as the zero set of the equations $F_1 = \cdots = F_l = 0$. Then the coordinate ring of $X_0$ is given by

$$R := \mathbb{F}_q[X_1, \ldots, X_m]/(F_1, \ldots, F_l).$$

Suppose that $Q_1, \ldots, Q_l$ are the points at infinity and $Q = Q_1$. Then $\mathbb{F}_q(X, Q) \subseteq R$. Let $S$ be the vector space over $\mathbb{F}_q$ generated by the monomials in $X_1, \ldots, X_m$ that are elements of $\mathbb{F}_q(X, Q)$. Then $S$ is in fact a subring of $\mathbb{F}_q(X, Q)$. Suppose that $\mathbb{F}_q(X, Q)$ is a finite dimensional extension of $S$ over $\mathbb{F}_q$, then $\mathbb{F}_q(X, Q)$ is the integral closure of $S$ in $R$. A basis of this extension is called a basis of missing functions.

In this lecture I have reported on the computation of a basis of missing functions in the work of:

1. Aleshnikov, Deolalikar, Kumar, Shum and Stichtenoth, on asymptotically good towers of function fields (curves),

2. Peter Beelen, on plane curves of type II,

3. Leonard, on the $q$-th power algorithm to compute the normalization (integral closure), and its generalization.