On algorithms for finding the missing functions

Ruud Pellikaan

Let $\mathcal{X}$ be curve defined over a finite field $\mathbf{F}_q$. Let Q be an $\mathbf{F}_q$-rational point of $\mathcal{X}$. Let $\mathbf{F}_q(\mathcal{X})$ be the function field of rational functions on $\mathcal{X}$, and $\mathbf{F}_q(\mathcal{X}, Q)$ the ring of rational functions on $\mathcal{X}$ that are regular outside Q.
In the construction of one-point algebraic geometric codes and their decoding according to Feng-Rao the ring $\mathbf{F}_q(\mathcal{X}, Q)$ plays a crucial role. Therefore we are looking for an "easy" and "explicit" description of this ring.

Suppose that the curve $\mathcal{X}$ is given by an affine part $\mathcal{X}_0$ in affine space $\mathbf{A}^m$ as the zero set of the equations $F_1 = \cdots = F_l = 0$. Then the coordinate ring of $\mathcal{X}_0$ is given by

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

Suppose that $Q_1, \ldots, Q_t$ are the points at infinity and $Q = Q_1$. Then $\mathbf{F}_q(\mathcal{X}, Q) \subseteq R$. Let S be the vector space over $\mathbf{F}_q$ generated by the monomials in $X_1, \ldots, X_m$ that are elements of $\mathbf{F}_q(\mathcal{X}, Q)$. Then S is in fact a subring of $\mathbf{F}_q(\mathcal{X}, Q)$. Suppose that $\mathbf{F}_q(\mathcal{X}, Q)$ is a finite dimensional extension of S over $\mathbf{F}_q$, then $\mathbf{F}_q(\mathcal{X}, Q)$ 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.