Counting decompositions of additive polynomials

Mark Giesbrecht

July 26, 2011

Cheriton School of Computer Science, University of Waterloo, Waterloo, Canada
(joint work with Joachim von zur Gathen, B-IT, Universität Bonn, Germany)

We consider the problem of counting decompositions of r-additive (or linearized) polynomials over a finite field $\mathbb{F}_q$, for q a power of a prime power r. The r-additive polynomials in $\mathbb{F}_q[x]$ have the form $f = \sum_{0 \le i \le d} f_i x^{r^i}$. We count the number of distinct functional decompositions of r-additive polynomials with a right component of degree r (all such components must be r-additive):

$$C(f) = \#\left\{a \in \mathbb{F}_q : \ f = g \circ (x^r + ax)\right\},$$
$$R(d) = \left\{C(f) : f \in \mathbb{F}_q[x] \text{ monic, squarefree, } r\text{-additive of degree } r^d\right\}.$$

For f as above, $C(f)$ also equals the number of roots in $\mathbb{F}_q$ of the (generalized) projective polynomial $\sum_{0 \le i \le d} f_i x^{(r^i-1)/(r-1)}$ (Abhyankar, 1997). We determine $R(d)$ for all d, and in particular $R(2) = \{0, 1, 2, r+1\}$ and $R(3) = \{0, 1, 2, 3, r+1, r+2, r^2+r+1\}$. This result for $R(2)$ is consistent with the work of Bluher (2004), who also considers the inverse problem of finding formulas for the number of polynomials in each class. I.e., for given d find

$$A_i^{(d)} = \#\left\{f \in \mathbb{F}_q[x] \text{ monic, squarefree, } r\text{-additive of degree } r^d, \ C(f) = i\right\}.$$

Bluher gives formulas for $d = 2$. Using elementary and explicit methods, we demonstrate analogous formulae for $d = 3$ as follows:

$$A_0^{(3)} = \frac{\left(q^3-1\right)(r+1)\,r}{3(r^2+r+1)}, \qquad A_{r+1}^{(3)} = \frac{q\,(q-1)\,(q-r)}{r^3\,(r-1)},$$
$$A_1^{(3)} = \frac{(q-1)\left(q^2r^3 - r^3 + 2q^2r + 2q^2\right)}{2r^2\,(r+1)}, \qquad A_{r+2}^{(3)} = \frac{(q-1)^2\,(q-r)\,(r-2)}{r\,(r^2-1)\,(r-1)},$$
$$A_2^{(3)} = \frac{q\,(q-1)^2\,(r-2)}{r\,(r-1)}, \qquad A_{r^2+r+1}^{(3)} = \frac{\left(q-r^2\right)(q-r)\,(q-1)}{r^3\,(r-1)\,(r^2-1)\,(r^2+r+1)},$$
$$A_3^{(3)} = \frac{(q-1)^3\,(r-2)\,(r-3)}{6\,(r-1)^2}, \qquad A_i^{(3)} = 0 \ \text{ otherwise.}$$

We then discuss the inverse problem for more general d. For all these problems we provide computable constructions and fast algorithms (requiring time polynomial in d and $\log q$).