Joachim von zur Gathen (2011). Census of Polynomials. Plenary talk. Joint work with Raoul Blankertz, Mark Giesbrecht, Alfredo Viola, and Konstantin Ziegler. In *Fq10 - The Tenth International Conference on Finite Fields and Their Applications*, p.8.

Census of polynomials

Joachim von zur Gathen

1 June 2011

B-IT, Universität Bonn
D-53113 Bonn, Germany
joint with:
Raoul Blankertz, Mark Giesbrecht, Alfredo Viola, Konstantin Ziegler

The Prime Number Theorem and a well-known result of Gauß count (approximately or exactly) the number of prime (or irreducible) elements in $\mathbb{Z}$ or $\mathbb{F}_q[x]$. Leonard Carlitz, Stephen Cohen, and others considered multivariate polynomials. We now have an exact formula for their number, and similarly for squareful und relatively irreducible (irreducible and not absolutely irreducible) polynomials, and approximations for the decomposable ones.

This talks' report results on univariate decomposable polynomials $f = g \circ h = g(h) \in \mathbb{F}_q[x]$. The *tame case*, where the characteristic p of $\mathbb{F}_q$ does not divide $n = \deg f$, is fairly well-understood, and we obtain closely matching upper and lower on the number of decomposable polynomials. In the opposite *wild case*, the bounds are less satisfactory.

The care of this talk deals with the easiest instance of the tame case, where $n = p^2$. We may assume g and h to have degree p and to be monic and original, that is, with constant coefficient 0.

Besides the trivial case of pth power, the additive polynomials $f = x^{p^2} + ax^p + bx$ are of interest. Mark Giesbrecht's talk reports on these. We now assume f to be not of this form.

Any (g, h) yields a decomposable $f = g \circ h$, and the crux of the matter is to count the number of *collisions*, where different (g, h) yield the same f. Abhyankar introduced the *projective polynomial* $\psi = y^{p+1} - uy + u$. There is an intimate connection between collisions and the roots of ψ. As an example, suppose that $l \mid p-1$, $m = (p-1)/l$ and $t \in \mathbb{F}_q^\times$ is a root of ψ. Then

$$\begin{aligned} f = x(x^{l(p+1)} - ux^l + u) &= (x(x^l - ut^{-1})) \circ (x(x^l - t)^m) \\ &= g \circ h. \end{aligned}$$

While g and h depend on t, f does not. Thus two distinct roots of ψ yield a collision.

There is another, similar, type of collision from different roots of ψ. The main result is that these are all possibilities.

Work in progress is to simplify the current proof of this result which relies on the ramification theory of function fields, and to determine exactly the number of such collisions.

References

[1]