Graduiertenkolleg

Experimentelle und konstruktive Algebra

RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

Einladung zum Mathematischen Kolloquium

Dienstag, 13. Mai 2014, 18:00 Uhr, Hörsaal III, Hauptgebäude

Mark Giesbrecht, University of Waterloo, Canada:

Algorithms and statistics for additive polynomials

The additive or linearized polynomials were introduced by Ore in 1933 as an analogy over finite fields to his theory of difference and difference equations over function fields. The additive polynomials over a finite field $\mathbb{F} = GF(q)$ where $q = p^e$ for some prime p, are those of the form

$$f = f_0 \cdot x + f_1 \cdot x^p + f_2 \cdot x^{(p^2)} + \ldots + f_n \cdot x^{(p^n)}.$$

They form a non-commutative left Euclidean principal ideal domain under the usual addition and functional composition, and possess a rich structure in both their decomposition structures and root geometries. Additive polynomials have been employed in number theory and algebraic geometry, and applied to constructing error-correcting codes and cryptographic protocols. In this talk we will present fast algorithms for decomposing and factoring additive polynomials, and also for counting the number of decompositions with particular degree sequences.

Algebraically, we show how to reduce the problem of decomposing additive polynomials to decomposing a related associative algebra, the eigenring. We give computationally efficient versions of the Jordan-Hölder and Krull-Schmidt theorems in this context to describe all possible factorizations. Geometrically, we show how to compute a representation of the Frobenius operator on the space of roots, and show how its Jordan form can be used to count the number of decompositions. We also describe an inverse theory, from which we can construct and count the number of additive polynomials with specified factorization patterns.

Some of this is joint work with Joachim von zur Gathen (Bonn) and Konstantin Ziegler (Bonn).

Wir laden alle Interessierten herzlich ein.