Linear Cellular Automata over Fields and Factorization of Polynomials

Ehler Lange

It was shown by v. Haeseler, Peitgen, Skordev that the self-similar evolution patterns of so-called Fermat-Cellular Automata can be completely decoded by means of substitutions or hierarchical iterated function systems. Furthermore, they provided a simple algorithm for setting up these substitutions. Linear CA over finite fields clearly belong to the class of Fermat-CA and results concerning the algebraic properties of the induced substitutions are presented in the talk. Also we describe a remarkable relationship between such substitutions and the factorization algorithms of Berlekamp and Niederreiter for polynomials over finite fields. We finally obtain a new approach to both of these factorization methods.

References

[1] E. R. Berlekamp: Factoring Polynomials Over Finite Fields, Bell System Tech. J. 46:1853-1859 (1967)

[2] F. v. Haeseler, H.-O. Peitgen, G. Skordev: Linear cellular automata, substitutions, hierarchical iterated function systems and attractors, Univ. Bremen, Inst.Dyn.Syst., Rep. 254 (1991); in: Fractal geometry and computer graphics, ed. J.L. Encarnacao et al, Springer 1992

[3] E. Lange: Cellular Automata, Substitutions, and Factorization of Polynomials Over Finite Fields, in: S. D. Cohen, H. Niederreiter eds, Proceedings of the 3rd International Conference on Finite Fields and Applications 1995 (to appear)

[4] H. Niederreiter: Factorization of Polynomials and some Linear-Algebra Problems Over Finite Fields, Linear Algebra Appl. 192:301-328 (1993)