DANIEL PANARIO, Carleton University

Divisibility of Polynomials over Finite Fields and Combinatorial Applications

Consider a maximum-length shift-register sequence generated by a primitive polynomial f over a finite field. The set of its subintervals is a linear code whose dual code is formed by all polynomials divisible by f. Since the minimum weight of dual codes is directly related to the strength of the corresponding orthogonal arrays, we can produce orthogonal arrays by studying divisibility of polynomials. Munemasa (Finite Fields Appl., 4(3):252-260, 1998) uses trinomials over $\mathbb{F}_2$ to construct orthogonal arrays of guaranteed strength 2 (and almost strength 3). That result was extended by Dewar, Moura, Panario, Stevens and Wang (Des. Codes Cryptogr., 45:1-17, 2007) to construct orthogonal arrays of guaranteed strength 3 by considering divisibility of trinomials by pentanomials over $\mathbb{F}_2$.

In this talk we review the above results and we comment on extensions of them. First we simplify the requirement in Munemasa's approach that the characteristic polynomial of the sequence be primitive: we show that the method applies even to the much broader class of polynomials with no repeated factors. Then we give characterizations of divisibility for binomials and trinomials over $\mathbb{F}_3$. Some of our results apply to any finite field $\mathbb{F}_q$ with q elements. We briefly comment on the combinatorial applications of these results.

Joint work with Olga Sosnovski, Brett Stevens and Qiang Wang.