Stephen Cohen, University of Glasgow

Methods for primitive and normal polynomials

Primitive and normal polynomials over a finite field are, of course, particular examples of irreducible polynomials over the field. Now, many techniques for studying irreducible polynomials as such are related, admittedly sometimes distantly, to the analytic treatment of primes in classical number theory. Such techniques can be less effective when applied to primitive and normal polynomials because these are intrinsically less number-theoretic in nature. We will survey some ideas which have been more successful in dealing with existence questions on primitive and/or normal polynomials. For example, the problem of whether there exists a primitive normal polynomial (of any degree) whose reciprocal polynomial is also primitive has been completely resolved for any field, [1], as has the existence question for primitive polynomials of any degree with an arbitrary prescribed coefficient, [2]. In a formidable development of this last question, the existence of primitive normal polynomials with a prescribed coefficient has been settled at least for degrees $n \geq 15$, [3], and claimed, in an $\mathbb{F}_q9$ abstract, for $n \geq 11$. Some interwoven techniques to be surveyed include:

- character-sum expressions/estimates over finite fields and Galois rings
- the use of sieving techniques, both additive and multiplicative
- p-adic methods for overcoming characteristic obstacles
- specifying conditions to determine individual coefficients

Much work remains in this area. Can the degree bound in the "primitive, normal, specified coefficient question" be reduced, or even a complete answer obtained (hard)? Can conditions on different coefficients be profitably combined to yield answers to further questions? Can the theory be put on a formal systematic basis? Can results like Zsigmondy's theorem (on the existence of particular primes dividing $q^n - 1$) be used to generate alternative existence results on (merely) irreducible polynomials?

References

[1] S. D. Cohen and S. Huczynska, The strong primitive normal basis theorem, *Acta Arith.*, to appear (arXiv:math/0610400v2[math.NT]).

[2] S. D. Cohen, Primitive polynomials with a prescribed coefficient, *Finite Fields Appl.* 12 (2006), 425–491

[3] S. Fan and X. Wang, Primitive normal polynomials with a prescribed coefficient, *Finite Fields Appl.* 15 (2009), 682–730.

Theo Garefalakis, University of Crete

Self-reciprocal irreducible polynomials with prescribed coefficients

We prove estimates for the number of self-reciprocal monic irreducible polynomials over a finite field of odd characteristic, that have the t lower degree coefficients fixed to given values. Our estimates imply that one may specify up to $m/2-\log_q(2m)-1$ values in the field and a self-reciprocal monic irreducible polynomial of degree $2m$ exists with its low degree coefficients fixed to those values.

Guang Gong, University of Waterloo

Multi-valued Sequences with 2-Level Autocorrelation from Iterative Decimation Hadamard Transform

The sequences with 2-level autocorrelation have important applications in code division multiple access (CDMA) systems. Those sequences correspond the so-called orthogonal spreading sequences. Recently, orthogonal spreading sequences are introduced to orthogonal frequency division multiplexing (OFDM) systems by spreading the data symbols across a set of subcarriers for achieving frequency diversity and relieving the high peak-to-average power ratio (PAPR). In this talk, first I will give a survey on multi-valued sequences with 2-level autocorrelation by applying the iterative decimation Hadamard transform (DHT) to a single m-sequence over $GF(p)$, a finite field with p elements where p is prime. In 2002, Gong and Golomb proposed the iterative decimation Hadamard transform for searching for new sequences with idea 2-level autocorrelation functions. Starting from single m-sequence with period 2^n-1, using this iterative DHT, all known binary sequences with ideal 2-level autocorrelation are found for all odd n up to 17. Recently, Yu and Gong extended this transform to a general case, called multiplexing DHT, and they completed the search for n even case. A remarkable observation is that any of those sequences constructed from applying the iterative DHT to a p-ary m-sequence is a multi-valued sequence (could be an integer sequence for $p = 2$ or complex sequence for $p > 2$), which has two-level autocorrelation. Secondly, I will present a new construction for ternary sequences whose terms are taken from the alphabetic set $\{-1, 0, 2\}$ from the second order DFT. Some open problems on 2-level autocorrelation sequences will be addressed by the end of the talk.

The new construction is from a joint work with Honggang Hu.

Gary McGuire, University College Dublin

Computing Fourier Spectra

Many important properties of functions on finite fields can be read from the Fourier transform. Some of these properties are relevant to cryptography, such as the nonlinearity. We will discuss techniques for computing the Fourier spectrum of functions on finite fields. The main idea of this talk is to survey some standard methods, which we will discuss and illustrate, assuming no prior knowledge. We may also discuss functions on finite rings, and other finite algebraic structures, if time permits.

Gary Mullen, Pennsylvania State University

How are irreducible and primitive polynomials distributed over finite fields?

We will discuss the distribution of irreducible and primitive polynomials over finite fields. In particular, we will discuss the Hansen/Mullen conjecture which led to a lot of work by various authors. We will also discuss some other conjectures as well some explicit formulas for the number of irreducibles satisfying various conditions. The talk will focus on conjectures and various results, rather than going into detail on the various methods used to prove the results.

Some basic results concerning permutation polynomials over finite fields

In this talk we will focus our discussion on permutation polynomials over finite fields; i.e. on polynomials whose sets of distinct values are the entire field. We will also discuss some results concerning the cardinalities of the value sets of some specific polynomials. In particular, we will discuss some results concerning Dickson polynomials and reversed Dickson polynomials over finite fields. We will also discuss some connections to topics like APN functions.

Arne Winterhof, Austrian Academy of Sciences

Mini-course on pseudorandom Sequences

Arne Winterhof
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69, 4040 Linz, Austria
E-Mail: arne.winterhof@oeaw.ac.at

Part I: Linear Complexity and Related Complexity Measures

The linear complexity of a sequence is not only a measure for the unpredictability and thus suitability for cryptography but also of interest in information theory because of its close relation to the Kolmogorov complexity. However, in contrast to the Kolmogorov complexity the linear complexity is computable and so of practical significance.
It is also linked to low correlation sequence design and coding theory. On the one hand the linear complexity of a sequence can be estimated in terms of its correlation and there are also strong ties to the theory of error-correcting codes. On the other hand the linear complexity can be calculated with the Berlekamp-Massey algorithm which was initially introduced for decoding BCH-codes.
This talk surveys several mainly number theoretic methods for the theoretical analysis of the linear complexity and related complexity measures and describes several classes of particularly interesting sequences with high linear complexity.

Part II: Exponential Sums and Uniform Distribution

Uniform distribution is a desirable feature for sequences used in quasi-Monte Carlo methods. The Erdős-Turán inequality reduces the problem of studying uniform distribution to the problem of estimating certain exponential sums. We describe some standard techniques for estimating exponential sums as well as we give an overview of recent research results on nonlinear pseudorandom sequences.

Part III: Measures of Pseudorandomness for Binary and Quaternary Sequences

Binary and quaternary sequences are the most important sequences in view of many practical applications. Mauduit and Sarközy introduced several measures of pseudorandomness for these sequences. We first give an overview of these measures and sequences where good bounds are known. Moreover, any quaternary sequence can be decomposed into two binary sequences and any two binary sequences can be combined into a quaternary sequence. We analyze the relation between the measures of pseudorandomness for the two binary sequences and the measures for the corresponding quaternary sequences. Our results show that each 'pseudorandom' quaternary sequence corresponds to two 'pseudorandom' binary sequences which are 'uncorrelated'.

Reference: Topuzoğlu, Alev; Winterhof, Arne Pseudorandom sequences. Topics in geometry, coding theory and cryptography, 135–166, Algebr. Appl., 6, Springer, Dordrecht, 2007.

Qing Xiang, University of Delaware

Strongly Regular Cayley Graphs: Constructions and Problems

Qing Xiang

Department of Mathematical Sciences
University of Delaware
Newark, DE 19716, USA
xiang@math.udel.edu

A *strongly regular graph srg* (v, k, λ, μ) is a graph with v vertices that is regular of valency k and that has the following properties:

(i) For any two adjacent vertices x, y, there are exactly λ vertices adjacent to both x and y.

(ii) For any two nonadjacent vertices x, y, there are exactly μ vertices adjacent to both x and y.

For example, a 5-cycle is a $(5, 2, 0, 1)$-srg, and the Petersen graph is a $(10, 3, 0, 1)$-srg. An srg (v, k, λ, μ) with a regular automorphism group G is equivalent to a (v,k,λ,μ) *partial difference set* in G, and can be obtained by a Cayley graph construction.

We discuss recent constructions of strongly regular Cayley graphs (equivalently, partial difference sets) by using semifields, weakly regular p-ary bent functions, quadratic forms and cyclotomy. Some open problems related to these constructions will be mentioned.

Joe Yucas, University of Southern Illinois Urbandale

Dickson Polynomials over Finite Fields

We let $\mathbb{F}_q$ denote the finite field of characteristic p containing q elements. Let n be a positive integer and write $t = \lfloor n/2 \rfloor$. In his 1897 PhD Thesis, Dickson introduced a family of polynomials

$$D_n(x) = \sum_{i=0}^{t} \frac{n}{n-i} \binom{n-i}{i} x^{n-2i}.$$

These are the unique polynomials satisfying Waring's identity

$$D_n(x + x^{-1}) = x^n + x^{-n}.$$

In recent years these polynomials have received an extensive examination. They have become known as the *Dickson polynomials* (of the first kind). In this talk we present some results and refinements which lead to new questions and new directions.