Polynomials over Finite Fields and Applications

Ian F. Blake (University of Toronto, ifblake@comm.utoronto.ca)
Stephen D. Cohen (University of Glasgow, sdc@maths.gla.ac.uk)
Gary L. Mullen (Pennsylvania State University, mullen@math.psu.edu)
Daniel Panario (Carleton University, daniel@math.carleton.ca)

November 18–23, 2006

1 Introduction

Finite fields are discrete mathematical objects satisfying all the axioms of a field, much as for the real or complex numbers, except for their finiteness. They are also referred to as Galois fields after the French mathematician Evariste Galois who was one of the first to show interest in them. It is easy to show that such objects exist only when the number of their elements is a power of a prime number and that any two finite fields with the same number of elements are isomorphic. Fundamental to the study of finite fields is the study of polynomials over finite fields which is the focus of this workshop.

The properties of finite fields and polynomials over them are of interest in their own right as they play a central role in many areas of pure mathematics. However it is perhaps the fundamental role they play in applications that propels them to such prominence and is the central interest of this workshop. These applications include such areas as:

Error correcting codes: Such codes are fundamental to many digital communication and storage systems, to improve the error performance over noisy channels. First proposed in the seminal work of Claude Shannon, they are now ubiquitous and included even in consumer electronic systems such as compact disc players and many others. Virtually all such error correcting codes and their decoding algorithms depend on the structure and properties of finite fields and polynomials over finite fields.

Cryptography: The advent of public key cryptography in the 1970's has generated innumerable security protocols which find widespread application in securing digital communications, electronic funds transfer, email, internet transactions and the like. Most of these schemes use either the integers or finite fields as the domain of computation to achieve their goals. More recent systems use elliptic curves, hyperelliptic curves and Abelian varieties over finite fields and these are assuming ever greater importance in applications and depend crucially on properties of finite fields for their study and implementation.

Sequences: Pseudorandom sequences i.e. deterministic sequences with random-like properties, are needed in a great many applications, including such areas as cryptography where random-like seeds are required. In addition, the design of sequences, mainly binary, for low correlation are central to such cell phone technology as CDMA. Most such systems require application of various finite field properties, including polynomials over finite fields.

While many of the talks of this workshop found their motivation in the above and related areas, such as combinatorics and design theory, many other talks addressed questions of fundamental importance to the theory of finite fields and their relationship to other areas of mathematics such as algebraic geometry and number theory.

2 Press Release

World's top experts on finite field theory meet at BIRS: Finite fields are finite sets of objects which have an arithmetic that allows the usual operations of addition, subtraction, multiplication, and division, except that contrary to the real numbers, the set contains only a finite number of distinct elements. Some of the best finite field researchers from around the world will converge on The Banff Centre during the period Nov. 18-23, 2006, where the Banff International Research Station will be hosting a workshop on recent developments in the theory of polynomials over finite fields. This event is co-organized by Professors Ian Blake of the University of Toronto, Stephen Cohen from the University of Glasgow, Gary Mullen from The Pennsylvania State University and Daniel Panario of Carleton University.

The workshop will focus on new results and methods in the study of various kinds of polynomials over finite fields. Finite fields are not only of deep mathematical interest in their own right but also play a critical role in modern information theory including algebraic coding theory for the error-free transmission of information and cryptology for the secure transmission of information. Polynomials over finite fields play an essential role in these and other very practical and important technologies; thus the emphasis of the workshop on various aspects related to polynomials with coefficients in finite fields.

3 Overview of the Field and Objectives of the Workshop

Polynomials over finite fields have been studied since the time of Gauss and Galois. The determination of special types of polynomials such as irreducible, primitive, and permutation polynomials, is a long standing and well studied problem in the theory and application of finite fields.

On the other hand, in recent years there has been intensive use of special polynomials in many areas including algebraic coding theory for the error-free transmission of information, cryptography for the secure transmission of information, and combinatorics, especially design theory. Polynomials over finite fields are the key ingredient in the construction of error-correcting codes such as BCH, Goppa, Reed-Solomon, and Reed-Muller codes, among others. Moreover, polynomials also play a key role in other areas of coding theory such as the determination of weight enumerators, the study of distance distributions, and decoding algorithms.

Large extensions of finite fields (especially over the two-element field) are important in cryptography. Elements in these extension fields can be represented by polynomials over the prime subfield. Thus, constructions of extension fields and fast arithmetic of polynomials are important practical questions. Moreover, many central problems in cryptography such as the discrete logarithm problem can be immediately translated into problems involving polynomials over finite fields.

Polynomials over finite fields appear very naturally in several areas of combinatorics. First, due to the finite number of elements, the enumeration of various special kinds of polynomials over finite fields is an interesting and extremely important research area in combinatorics. In design theory, polynomials are used to construct and describe cyclic difference sets and special types of designs such as group divisible designs. Divisibility conditions on trinomials over finite fields have been shown to produce orthogonal arrays with certain strengths, and bivariate and multivariate polynomials can be used to represent and study latin squares and sets of orthogonal latin squares and hypercubes of prime power orders.

In addition, polynomials over finite fields are important in engineering applications. Linear recurrence relations over finite fields produce sequences of field elements. Linear feedback shift registers are used to implement these recurrences. Characteristic polynomials over finite fields are one of the main tools when dealing with shift registers. In particular, primitive characteristic polynomials produce sequences with large periods, and thus have found many applications in areas such as random number generation.

As an example of an important theoretical problem involving polynomials over a finite field F_q is the study of the value set $\{f(a)|a \in F_q\}$ of a polynomial f. Polynomials with maximal value sets are permutation polynomials which have applications in various areas of combinatorics such as the study of sets of orthogonal latin squares, as well as in cryptography. Can one characterize the polynomials of degree n which have maximal value sets; minimal value sets, value sets of cardinality k with $1 \leq k \leq q$? What is the number of such polynomials? These are fundamental theoretical problems which are not only worthy of study in their own right, but also because of their applications.

This workshop addressed new theoretical results about polynomials over finite fields as well as the ways in which polynomials are used in algebraic coding theory, cryptography, and design theory. Given the increasing number of relevant research papers, as can be seen by checking recent issues of journals such as *Finite Fields and Their Applications*, *Designs, Codes and Cryptography*, and the *IEEE Transactions on Information Theory*, along with other journals such as the *J. Combinatorial Theory Series A*, *J. Number Theory*, and *Discrete Mathematics* which regularly publish papers dealing with finite fields and their applications, we believe the time has come to summarize these achievements and formulate new challenges in this very important area.

The purpose of the workshop was to establish links between the community of researchers working on polynomials over finite fields and researchers and practitioners working in various areas of application. The workshop brought together researchers from finite fields, coding theory, cryptography, combinatorics, number theory and engineering. As a result of this interaction researchers became acquainted with recent techniques and results dealing with various theoretical properties of polynomials over finite fields. The diversity of the attendees stimulated joint works and fostered work across fields, leading to new mathematics and to the solution of interesting applied problems.

A balanced group of talks in each of the areas of focus of the workshop was presented. These areas included theoretical properties of polynomials over finite fields, connections to algebraic coding theory, combinatorial design theory, and cryptography.

4 Recent Developments

We enumerate some important recent developments discussed at the meeting.

In 1992 Hansen and Mullen conjectured that with only a few necessary exceptions for very small values of q and small degrees n, there is always at least one primitive polynomial of degree n over $\mathbb{F}_q$ with the coefficient of any power of x specified in advance. More precisely, given $a \in \mathbb{F}_q$ and j with $1 \leq j \leq n-1$, there is always at least one primitive polynomial of degree n over $\mathbb{F}_q$ where a is the coefficient of x^j. This conjecture led to a lot of research establishing various related results, but the Banff Workshop talk by M. Presern completed the proof that the Hansen/Mullen Conjecture was indeed true.

The computation of modular polynomials is crucial for many applications, including the problem of counting points on elliptic curves over finite fields. Enge's presentation centered on recent algorithmic developments that allow modular polynomial computation in essentially linear time in the output size. This algorithm has been used to establish new records for elliptic curve point counting.

Lenstra's talk focused on a very recent new algorithm (due to himself and Carl Pomerance) for the construction of irreducible polynomials over finite fields. Irreducible polynomials are normally used for constructing elements in finite field extensions. This algorithm comes as a by-product of their version of a new polynomial time primality test.

In recent years, there has been considerable progress in the constructions of algebraic curves with many rational points. The main leaders of these developments are Arnaldo Garcia and Henning Stichtenoth. This area has applications to coding theory (which for years was its main driving motivation). Garcia's talk focused on new results for certain type of towers (Artin-Schreier) recently studied in collaboration with Stichtenoth.

An important class of polynomials over finite fields are the polynomials that permute the elements in the field, the so-called *permutation polynomials*. Permutation polynomials have been largely studied since Hermite but even the simple case of characterizing permutation binomials remains vastly open. Masuda's talk concentrated on characterizing and counting permutation binomials over certain special finite fields.

Counting special type of polynomials is a classical problem in finite fields. Precise formulas exist for the number of univariate irreducible polynomials over a finite field and several related quantities such as squarefree (and in general, k-free) polynomials, and so on. The equivalent problem of counting polynomials in several variables has been less studied, although some results from the 1960's exist mostly due to Carlitz and Cohen. Von zur Gathen's talk presented new counting estimates for some classes of special bivariate polynomials such as reducible, the so-called "exceptional" and "singular" polynomials.

Many properties of integers have been considered for polynomials over finite fields. For example, questions about the factorization of integers can be easily translated into questions about the decomposition of polynomials in irreducibles; famous number theoretic problems such as the twin primes and the Goldbach

conjectures have been studied over finite fields. Mullen's talk presented results dealing with a polynomial analogue of the famous unsolved 3n+1 problem.

On Monday evening there was a very active two hour problem session moderated by Gary Mullen during which numerous open problems relating to polynomials over finite fields were discussed. While we will not try to describe these problems here, it was clear that the problems generated considerable interest. Moreover, later in the week many participants continued to discuss some of these problems. We are confident that further discussion will continue long after the conference is over and that some related results will be published.

5 Participants

A total 41 participants from thirteen countries attended the workshop:

1. Ahmadi, Omran (University of Toronto, Canada)
2. Arikushi, Karin (Carleton University, Canada)
3. Bernstein, Dan (University of Illinois, Chicago, USA)
4. Blake, Ian (University of Toronto, Canada)
5. Bluher, Antonia (National Security Agency, USA)
6. Car, Mireille (Universite Paul Cezanne, Aix-Marseille III, France)
7. Coulter, Robert (University of Delaware, USA)
8. Dewar, Michael (University of Illinois, Urbana-Champaign, USA)
9. Dillon, John (National Security Agency, USA)
10. Enge, Andreas (Ecole polytechnique, Paris, France)
11. Gallardo, Luis (L'Universite de Bretagne Occidentale, France)
12. Gao, Shuhong (Clemson University, USA)
13. Garcia, Arnaldo (IMPA, Brazil)
14. Garefalakis, Theo (University of Crete, Greece)
15. von zur Gathen, Joachim (University of Bonn, Germany)
16. Gong, Guang (University of Waterloo, Canada)
17. Hirschfeld, James (University of Sussex, England)
18. Huczynska, Sophie (University of St Andrews, Scotland)
19. Lange, Tanja (Technische Universiteit Eindhoven, the Netherlands)
20. Lenstra, Hendrik W. (University of Leiden, the Netherlands)
21. Li, Winnie (Pennsylvania State University, USA)
22. Lisonek, Petr (Simon Fraser University, Canada)
23. Masuda, Ariane (Carleton University, Canada)
24. McGuire, Gary (University College Dublin, Ireland)
25. Mills, Don (Rose-Hulman Institute of Technology, USA)

26. Moisio, Marko (University of Vaasa, Finland)
27. Mullen, Gary (Pennsylvania State University, USA)
28. Panario, Daniel (Carleton University, Canada)
29. Park, Jang-Woo (Clemson University, USA)
30. Presern, Mateja (University of Glasgow, Scotland)
31. Ranto, Kalle (University of Turku, Finland)
32. Ruskey, Frank (University of Victoria, Canada)
33. Semaev, Igor (University of Bergen, Norway)
34. Shparlinski, Igor (Macquarie University, Australia)
35. Tapia-Recillas, Horacio (Universidad Autonoma Metropolitana-Iztapalapa, Mexico)
36. Thomson, David (Carleton University, Canada)
37. Voloch, Jose (University of Texas at Austin, USA)
38. Wan, Daqing (University of Calirfornia, Irvine, USA)
39. Wang, Qiang (Carleton University, Canada)
40. Yucas, Joe (Southern Illinois University, USA)
41. Zieve, Michael (IDA Center for Communications Research, USA)

6 Titles and Abstracts

Speaker: **Omran Ahmadi** (University of Toronto)
Title: *Quadratic transformation of irreducible polynomials over finite fields*

Abstract: Self-reciprocal irreducible monic (srim) polynomials over finite fields have been studied in the past. These polynomials can be studied in the context of quadratic transformation of irreducible polynomials over finite fields. In this talk we present the generalization of some of the results known about srim polynomials to polynomials obtained by quadratic transformation of irreducible polynomials over finite fields.

Speaker: **Dan Bernstein** (University of Illinois at Chicago)
Title: *Faster factorization into coprimes*
Abstract: How quickly can we factor a set of univariate polynomials into coprimes? See `http://cr.yp.to/coprimes.html` for examples and applications. Bach, Driscoll, and Shallit achieved time $n^{(2+o(1))}$ in 1990, where n is the number of input coefficients; I achieved time $n(\lg n)^{(O(1))}$ in 1995; much more recently I achieved time $n(\lg n)^{(4+o(1))}$.

Speaker: **Antonia Bluher** (National Security Agency)
Title: *Hyperquadratic elements of degree 4*
Abstract: I will describe joint work with Alain Lasjaunias about the construction of degree-4 polynomials over fields K of char p whose roots α have a Frobenius property:

$$\alpha^q = \frac{A\alpha + B}{C\alpha + D},$$

where $A, B, C, D \in K$, $AD - BC$ is nonzero, and q is a power of p.

The case of interest is when K is a function field and α has a Laurent series expansion. It is conjectured that in such a case, α might have interesting patterns in its continued fraction expansion, such as those found by Buck and Robbins for a root of the polynomial $X^4 + X^2 - TX + 1 \in \mathbb{F}_{13}(T)[X]$.

Speaker: **Mireille Car** (Universite Paul Cezanne (Aix-Marseille III))
Title: *Ternary Quadratic forms that represent 0, the function field case*

Abstract: Let K be a global function field with field of constants a finite field k with q elements and odd characteristic. Let S be a finite set of $s > 0$ places of K and let R_S denote the set of S-integers of K. For s-tuples of rational integers $\mathbf{m} = (m_v)_{v\in S}$ and $\mathbf{n} = (n_v)_{v\in S}$, let $Q_S(\mathbf{m}, \mathbf{n})$ denote the number of pairs (a, b) of integers of R_S such that $v(a) = m_v, v(b) = n_v$ for all $v \in S$, and such that the quadratic form

$$(f_{a,b}) \qquad X^2 - aY^2 - bZ^2$$

represents 0 over the field K. We give an asymptotic estimate for the number $Q_S(\mathbf{m}, \mathbf{n})$ for s-tuples $\mathbf{m}$ and $\mathbf{n}$ such that the numbers

$$\|\mathbf{m}\| = -\sum_{v\in S} f_v m_v, \qquad \|\mathbf{n}\| = -\sum_{v\in S} f_v n_v$$

tend to $+\infty$, f_v denoting the degree of the place v.

In a previous work, we dealt with these questions in the case of a rational function-field. (Indeed, if $K = k(T)$, the rational function field, the polynomial ring $k[T]$ is the ring $R_{\{\infty\}}$ with ∞ the $\frac{1}{T}$-place, and if m and n are positive integers, if $(\mathbf{m}, \mathbf{n}) = ((-m), (-n))$, the number $Q_{\{\infty\}}(\mathbf{m}, \mathbf{n})$ is equal to the number $H(m, n)$ of polynomials a and b in $k[T]$ of degree m and n respectively, such that the quadratic form $(f_{a,b})$ represents 0 over the field $k(T)$.) The case of the rational function-field was a polynomial analogue of questions asked by Serre and solved by Hooley and Guo about the size of the number $H(x)$ of pairs $(a, b) \in \mathbb{Z}^2$, such that $|a| \leq x$, $|b| \leq x$ and such that the ternary quadratic form

$$X^2 + aY^2 + bZ^2$$

represents 0 over the field $\mathbb{Q}$. Presently now, no number field analogue of the theorems proved in what follows is known.

Speaker: **Michael Dewar** (University of Illinois, Urbana-Champaign)
Title: *When do pentanomials divide trinomials over $\mathbb{F}_2$?*
Abstract: Over $\mathbb{F}_2$, up to reciprocals, no pentanomial of degree m divides a trinomial of degree at most $2m$ except for 25 specific exceptions, all with degree $m < 14$, and one infinite family of pentanomials. A careful case analysis reveals that for large degree the coefficients cancel in a "staircase"-like manner. This divisibility property allows the construction of orthogonal arrays of strength 3.

[This is a joint work with L. Moura, D. Panario, B. Stevens and Q. Wang.]

Speaker: **John Dillon** (National Security Agency)
Title: *APN polynomials and related codes*
Abstract: A map $f : \mathrm{GF}(2^m) \to \mathrm{GF}(2^m)$ is APN (*almost perfect nonlinear*) if $x \mapsto f(x + a) - f(x)$ is 2-to-1 for all nonzero a in GF(2^m). Equivalently, the binary code of length $2^m - 1$ with parity-check matrix

$$H := \begin{bmatrix} \cdots & \omega^j & \cdots \\ \cdots & f(\omega^j) & \cdots \end{bmatrix}$$

is double-error-correcting, where ω is primitive in GF(2^m) and we may, without loss of generality, assume that $f(0) = 0$.

We give a brief review of these maps and their polynomials; and we present some new examples along with some related codes and designs which serve as invariants for their equivalence classes.

Speaker: **Andreas Enge** (Ecole polytechnique, Paris)
Title: *Asymptotically optimal computation of modular polynomials*

Abstract: Modular polynomials play an essential role in the Schoof-Elkies-Atkin algorithm for point counting on elliptic curves over finite fields, and they occur in several algorithms for constructing elliptic curves with prescribed complex multiplication. I present an algorithm based on floating point evaluation and interpolation that computes several flavours of modular polynomials in essentially linear time in the output size, and that has enabled us to set the recent records for elliptic curve point counting.

Speaker: **Luis H. Gallardo** (L'Universite de Bretagne Occidentale)
Title: *Sums of biquadrates in $\mathbb{F}_q[t]$*
Abstract: For most q's, it is known that every polynomial $P \in \mathbb{F}_q[t]$ that is a sum of biquadrates in $\mathbb{F}_q[t]$ is a strict sum, (i.e., if $P = A^4 + \ldots$ then $\deg(A^4) < \deg(P) + 4$), of 16 biquadrates.

Here we explain how we may reduce this to 11 biquadrates. Essentially this is done by using a new formula (that was discovered recently) to write t as a sum of 4 biquadrates when -1 is not a biquadrate in $\mathbb{F}_q$. (Its proof uses Jacobi sums). [This is joint work with Mireille Car.]

Speaker: **Shuhong Gao** (Clemson University)
Title: *Primary decomposition of zero-dimensional ideals over finite fields*
Abstract: A new algorithm is presented for computing primary decomposition of zero-dimensional ideals over finite fields. Like Berlekamp's algorithm for univariate polynomials, the new method is based on the kernel of the Frobenius map acting on the quotient algebra. The dimension of the kernel equals the number of primary components, and a basis of the kernel yields a complete decomposition. Unlike previous approaches for multivariate polynomial systems, the new method needs no generic projections but reduces the problem directly to root finding of univariate polynomials over the ground field. If time permits, we shall show how Gröbner basis structure can be used to get partial primary components without root finding. [Joint work with Daqing Wan and Mingsheng Wang.]

Speaker: **Arnaldo Garcia** (IMPA)
Title: *Some Artin-Schreier towers are easy*
Abstract: Towers of function fields (resp. of algebraic curves) over finite fields with positive limit, for the ratios of numbers of rational places over the genera, provide examples of curves with large genus having many rational points over a finite field. It is in general a difficult task to calculate the limit of a tower. In this talk we present a simple method how to calculate the genus of certain Artin-Schreier towers. As an illustration of our method we obtain a very simple and unified proof for the limits of some towers which attain the Drinfeld-Vladut bound or the Zink bound.The limits of their Galois closures can also be obtained similarly. The method computes the limit of certain towers avoiding the hard computations involved in the determination of the individual genus of each function field in the tower.

Speaker: **Joachim von zur Gathen** (University of Bonn)
Title: *Counting bivariate polynomials: reducible, exceptional, and singular ones*
Abstract: Among the bivariate polynomials over a finite field, most are irreducible. We count some classes of special polynomials, namely the reducible ones, those with a square factor, the "exceptional" ones which are irreducible but factor over an extension field, and the singular ones, which have a root at which both partial derivatives vanish.

Speaker: **Guang Gong** (University of Waterloo)
Title: *Two-level Autocorrelation Sequences, Polynomials, and Exponential Sum Equalities*
Abstract: In this presentation, first, I will provide a survey of all the known constructions of (ideal) 2-level autocorrelation sequences with period $p^n - 1$ over a finite field $GF(p)$ where p is a prime and n is a positive integer. These sequences have important applications in code division multiple access (CDMA) communications. Any sequence over $GF(p)$ with period dividing $p^n - 1$ can be represented by a sum of multiple trace terms, which corresponds to a polynomial function from $GF(p^n)$ to $GF(p)$. Then I will present some conjectures on ternary sequences with 2-level autocorrelation, their trace representations, and some extremely surprising exponential sum equalities obtaining by iteratively applying the two operations of decimation and Hadamard transform.

Speaker: **James Hirschfeld** (University of Sussex)
Title: *Non-isomorphic maximal curves over a finite field*
Abstract: A *maximal curve* $\mathcal{F}$ over the finite field $\mathbf{F}_q$ is an algebraic curve attaining the Hasse–Weil upper bound,

$$q + 1 + 2g\sqrt{q},$$

where g is the genus of $\mathcal{F}$ and q is necessarily a square.

The genus of $\mathcal{F}$ satisfies the inequality,

$$g \leq \tfrac{1}{2}(q - \sqrt{q}),$$

where equality is achieved if and only if $\mathcal{F}$ is isomorphic to the Hermitian curve $\mathcal{H}_q$, given by the form,

$$X_0^{\sqrt{q}+1} + X_1^{\sqrt{q}+1} + X_2^{\sqrt{q}+1}.$$

If a curve is a quotient of $\mathcal{H}_q$, then it is maximal. It is conjectured that every maximal curve is a quotient of $\mathcal{H}_q$.

A family of quotient curves of $\mathcal{H}_q$ with genus $\sqrt{q} - 1$ is considered. The members of the family have many similar properties but provide many non-isomorphic maximal curves.

[Joint work with M. Giulietti, G. Korchmáros and F. Torres.]

Speaker: **Sophie Huczynska** (University of St Andrews)
Title: *The Strong Primitive Normal Basis Theorem*
Abstract: An element α of the extension E of degree n over the finite field $F = GF(q)$ is called free over F if $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a (normal) basis for E/F. The Primitive Normal Basis, first established in full by Lenstra and Schoof (1987), asserts that for any such extension E/F, there exists an element $\alpha \in E$ which is simultaneously primitive (generates the multiplicative group of E) and free over F (equivalently, there exists a primitive free polynomial). in this talk, I will discuss the following strengthening of this theorem: aside from four specific extensions E/F, there exists an element $\alpha \in E$ such that both α and α^{-1} are simultaneously primitive and free over F (equivalent to the existence of a pair of reciprocal primitive free polynomials).

[This is joint work with S.D.Cohen (Glasgow).]

Speaker: **Hendrik W. Lenstra** (University of Leiden)
Title: *Constructing finite fields*
Abstract: We shall describe an algorithm that, given a prime number p and an integer D with $D > (\log p)^{46/25}$, produces an irreducible polynomial f over $\mathbf{Z}/p\mathbf{Z}$ with $D \leq \deg f < 4D$. It is a particularly attractive feature of the algorithm that its run time is essentially linear in terms of the length of the output; that is, it runs in time at most $(d \log p) \cdot (2 + \log d + \log\log p)^c$, where c is some universal constant. The algorithm was developed jointly with Carl Pomerance, as a byproduct of a new primality test.

Speaker: **Winnie Li** (Pennsylvania State University)
Title: *Characterizations of pseudo-codewords of a parity-check code*
Abstract: In this survey talk we shall explain how pseudo-codewords of a parity-check code arise, the role they play in the fast decoding algorithms, and give two ways to characterize them.

Speaker: **Petr Lisonek** (Simon Fraser University)
Title: *Caps and highly nonlinear functions on finite fields*
Abstract: We consider functions on binary vector spaces which are far from linear functions in different senses. Three well studied classes of such functions are crooked (CR) functions, almost bent (AB) functions and almost perfect nonlinear (APN) functions. In the binary case all known constructions of such functions arise from certain monomial functions on GF(2^n). In 2003 van Dam and Fon-Der-Flaass obtained a combinatorial characterization of all AB functions in terms of the number of solutions to a certain system of equations. We study a similar characterization for certain classes of APN functions. We discuss an application of this characterization in the study of caps in the finite projective spaces over GF(2).

Speaker: **Ariane Masuda** (Carleton University)
Title: *Permutation binomials over $\mathbb{F}_{2^k p+1}$ where p and $2^k p+1$ are primes*
Abstract: In this talk we present results on the characterization of permutation binomials over $\mathbb{F}_{2^k p+1}$ where $k \geq 1$, p and $2^k p+1$ are primes. We also give a formula for the number of permutation binomials of degree smaller than $q-1$ when $k=1$ and 2.

[This is joint work with Daniel Panario and Steven Wang.]

Speaker: **Marko Moisio** (University of Vaasa)
Title: *Kloosterman curves, their fibre products, and explicit enumeration of irreducible polynomials with two coefficients prescribed, I*
Abstract: Let $\mathbb{F}_q$ be a finite field with $q=p^r$ and let $c \in \mathbb{F}_q$. In this talk some preliminaries for an explicit enumeration of the irreducible polynomials

$$x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$$

with $a_{m-1}=0$ and $a_1=c$, are given.

First, for $a, b \in \mathbb{F}_q^*$ ($a \neq b$), the number of rational places of the function field $\mathbb{F}_{q^m}(x,y,z)$ with $y^q - y = x + ax^{-1}$, $z^q - z = x + bx^{-1}$, is given in terms of moments of Kloosterman sums over $\mathbb{F}_q$. Secondly, evaluation of moments in cases $p=2,3$ is considered. More precisely, the moments are connected by Pless's power moment identity to the weight distribution of Melas codes, which opens up a possibility to evaluate moments by using explicit weight formulae obtained by Schoof, van der Vlugt, and van der Geer.

We illustrate the method by giving explicitly the number of rational places of $\mathbb{F}_{q^m}(x,y,z)$ for $m = 1, \ldots, 10$.

Speaker: **Gary Mullen** (Pennsylvania State University)
Title: *A polynomial analogue of the $3n+1$ problem*
Abstract: The integer $3n+1$ problem is a well studied but still open problem. In particular, if n is an even positive integer, then one divides by 2 while if n is odd, one calculates $3n+1$. The process is repeated and the $3n+1$ problem conjectures that after a finite number of iterations, one always ends at the value 1.

I will discuss a polynomial analogue of this problem which was first motivated by considering polynomials over the binary field $\mathbb{F}_2$. We will consider an even more general version over any field. The interesting point is that after a finite number of iterations, our algorithm for monic polynomials over a field always ends at 1. We will also discuss several related open problems which arise in the case of the binary field $\mathbb{F}_2$.

Speaker: **Jang-Woo Park** (Clemson University)
Title: *Monomial dynamics over finite fields*
Abstract: Let k be a finite field and $f : k^n \to k^n$ a map defined by polynomials. It is an important problem to study the dynamics of f, particularly its fixed points and cycles of various lengths. This problem is well understood for linear functions, but wide open for nonlinear functions. In this talk, we present our recent work on dynamics defined by monomials.

Speaker: **Mateja Presern** (University of Glasgow)
Title: *Completing the Hansen-Mullen primitivity conjecture*
Abstract: The Hansen-Mullen Primitivity Conjecture (1992) is that, generally, there exists a primitive polynomial of degree n over a finite field $\mathbb{F}_q$ with any coefficient arbitrarily prescribed. This was proved by S. D. Cohen for $n \leq 3$ and $n \geq 9$ and S. D. Cohen and M. Prešern for $n=4$. We present refinements of these ideas which yield the facts that the 3rd or 4th (or $(n-3)$rd or $(n-4)$th) coefficient can be prescribed, thus completing the proof of the Hansen-Mullen Primitivity Conjecture. We particularly focus on primitive polynomials of degree 8. A very small amount of computation is needed.

[This is joint work with S. D. Cohen.]

Speaker: **Kalle Ranto** (University of Turku)
Title: *Kloosterman curves, their fibre products, and explicit enumeration of irreducible polynomials with two coefficients prescribed, II*
Abstract: Let $\mathbb{F}_q$ be a finite field with $q=p^r$ and let $c \in \mathbb{F}_q$. We show how the number of irreducible

polynomials $x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in \mathbb{F}_q[x]$ with $a_{m-1} = 0$ and $a_1 = c$ is connected to the number of rational places of the function field $\mathbb{F}_{q^m}(x, y, z)$ with $y^q - y = x + ax^{-1}$, $z^q - z = x + bx^{-1}$, $a, b \in \mathbb{F}_q^*$, and $a \neq b$. The number of these rational places in cases $p = 2, 3$ were recently obtained by Marko Moisio, and this enables us to give the number of irreducible polynomials in question when $m = 1, ..., 10$.

Speaker: **Frank Ruskey** (University of Victoria)
Title: *Exhaustive generation of irreducible polynomials over small finite fields*
Abstract: We have exhaustively generated all irreducible polynomials over GF(2), GF(3), GF(4), GF(5), GF(7), and GF(8) for "reasonable" values of n. Reasonable means that they will fit on a single CD after compression. For example, over GF(3) we generate up to degree $n = 20$, and there are 174,342,216 such polynomials. We also generate one million primitive polynomials for each degree $n \leq 64$. The basic technique is to generate Lyndon strings and convert each string to a polynomial using a shift and add technique on computer words. The optimization of the crucial add routine leads to interesting questions in circuit optimization that are addressed in the latest drafts of Knuth Volume IV.

Using the data we have produced tables computing various statistics of the polynomials and will present several conjectures based on those statistics.

[This research done together with my Ph.D. student Gilbert Lee.]

Speaker: **Igor Semaev** (University of Bergen)
Title: *On solving sparse algebraic equations over finite fields*
Abstract: A system of algebraic equations over a finite field is called sparse if each equation depends on a small number of variables. In this talk new deterministic algorithms for solving such equations are presented. The mathematical expectation of their running time is derived. These estimates are at present the best theoretical bounds on the complexity of solving average instances of the above problem.

Speaker: **Igor Shparlinski** (Macquarie University)
Title: *On the Sato-Tate conjecture on average*
Abstract: We obtain asymptotic formulae for the number elliptic curves $E_{a,b} : Y^2 = X^3 + aX + b$ over a field $\mathbb{F}_p$ where p is prime, satisfying certain "natural" properties. We consider the cases when:

- a and b are fixed but p is chosen at random with $p \leq x$,
- p is fixed but a and b are chosen at random with $|a| \leq A$ and $|b| \leq B$,
- a, b and p are chosen at random with $|a| \leq A$, $|b| \leq B$ and $p \leq x$.

Specifically, we investigate the behavior of such curves with respect to the Sato-Tate conjecture, cyclicity and divisibility of the number of points by a fixed integer m.

[Joint work with Bill Banks.]

Speaker: **Horacio Tapia-Recillas** (Universidad Autonoma Metropolitana-Iztapalapa)
Title: *The simplex code over finite chain rings*
Abstract: Codes over finite rings have been studied since the early seventies, particularly over the ring $\mathbb{Z}_m$ of integer modulo m. Recently the ring $\mathbb{Z}_4$ has been of particular interest after the work of Nechaev and later, Hammond et al. These authors show that certain non-linear binary codes with good parameters, including the Kerdock and Preparata codes, are the image of $\mathbb{Z}_4$ linear codes under the Gray isometry between $(\mathbb{Z}_4^n, d_L)$ and $(\mathbb{Z}_2^{2n}, d_H)$, (here d_L and d_H are the Lee and Hamming distance respectively). This result has motivated the study of several types of codes over finite rings and their image under the (generalized) Gray isometry. These rings include $\mathbb{Z}_{p^s}$ where p is a prime and s a positive integer, Galois rings, finite chain rings and Frobenious rings, to mention some of them. Recently the simplex code over the ring $\mathbb{Z}_{2^s}$ has been introduced and some of its properties studied. Since this ring, and, more generally, the ring $\mathbb{Z}_{p^s}$ where p is a prime and s a positive integer, is a particular case of a Galois ring and the latter is an example of a finite chain ring, it is natural to ask if it is possible to extend some of the results previously given for the (linear) simplex code over the ring $\mathbb{Z}_{2^s}$ to the case of finite chain rings. Also, the Gray isometry for codes over a finite chain ring has been introduced; thus, one can ask if the image under the Gray isometry of the (linear) simplex code defined over a finite chain ring is still linear. In this talk the simplex code over a finite chain ring is defined and its

homogeneous weight distribution is determined. Furthermore, it is shown with an example that the image of this simplex code under the Gray isometry is not linear in general.

Speaker: **Felipe Voloch** (University of Texas at Austin)
Title: *Symmetric Cryptography and Algebraic Curves*
Abstract: The S-boxes of symmetric cryptography can be viewed as polynomials over finite fields (of characteristic two). Their non-linearity properties, which are important for their use in cryptography, translate into properties of certain algebraic curves. I will explain these facts and present some results obtained along these lines.

Speaker: **Daqing Wan** (University of Calirfornia, Irvine)
Title: *Counting rational points on varieties over finite fields*
Abstract: This is an expository lecture on both complexity and algorithms for counting the number of rational points on a hypersurface over a finite field, with an emphasis on modular reduction via p-adic methods.

Speaker: **Qiang (Steven) Wang** (Carleton University)
Title: *Permutation polynomials and sequences over finite fields*
Abstract: A polynomial over a finite field is called a permutation polynomial if it induces a bijective map from the finite field to itself. Permutation polynomials were first investigated by Hermite, and since then, many studies concerning them have been devoted. Recently there has been a revival in the interest for permutation polynomials, in part due to their applications in coding theory, combinatorics, and cryptography. In this talk I will describe some new classes of permutation polynomials of finite fields in terms of sequences over finite fields. I will also explain the tight connections between permutation behaviors of binomials and the periodicity of certain class of sequences.

Speaker: **Joseph L. Yucas** (Southern Illinois University)
Title: *Generalized reciprocals and factors of Dickson polynomials*
Abstract: We discuss recent results on Dickson polynomials. In particular we give new descriptions of the factors of Dickson polynomials over finite fields in terms of cyclotomic factors. To do this generalized reciprocal polynomials are introduced and characterized.

[This is joint work with Robert W. Fitzgerald.]

Speaker: **Michael Zieve** (IDA Center for Communications Research)
Title: *Polynomial decomposition*
Abstract: Consider the operation of composition on polynomials over a field K, namely $(f \circ g)(x) = f(g(x))$. A polynomial of degree at least 2 is called indecomposable if it cannot be written as the composition of polynomials of strictly lower degree. Every polynomial f of degree at least 2 can be written as the composition of indecomposable polynomials, but this decomposition need not be unique. However, if K has characteristic zero, then results of Ritt, Levi, Engstrom, and Schinzel provide a complete theory of polynomial decomposition – for instance, any two decompositions of f must have the same length, and it is known how to produce all decompositions of f from any single decomposition.

I will present several results and examples about the analogous problem in fields of positive characteristic. Along the way I will present new examples of indecomposable polynomials which decompose over an extension field; new types of reducible 'variables separated' polynomials $f(x) - g(y)$; and various results on computing the intersection of two subfields of $K(x)$.

7 Outcome of the Meeting

A great deal of collaboration between participants at the workshop was in evidence, either on previously discussed problems or initial work on new problems. Many of the participants commented favorably to the organizers how the setting and the format of the workshop was conducive to such cooperation. Indeed the only negative comments received, from two prominent researchers, was that there should have been fewer talks and that some of the talks should have been shorter in order to allow more time for such collaboration.

We briefly comment on some new results obtained during the workshop. It is very likely that more results will come up in the future from discussions that happened in Banff. Indeed, we are aware that other papers by participants are in various stages of preparation.

Boolean functions with small Fourier spectrum have been widely studied in recent years. They are interesting not only from a pure standpoint but also they are used nowadays in applications in areas such as communications, cryptography and information theory. The study of bent functions, that is boolean functions where the Fourier spectrum contains only the two values $\{\pm 2^{n/2}\}$, has been at the center of the research in this area. The classification of all bent functions seems to be a very hard problem. Some boolean functions of interest are the well-known Kasami-Welch functions: $\mathrm{Tr}(x^d)$, for certain exponent d. John Dillon and Gary McGuire's collaboration at the Banff meeting focus on finite fields of the form $\mathbb{F}_{2^n}$ where n is not divisible by 3. They show that in this case and when the Kasami-Welch exponent is $d = 4^k - 2^k + 1$, where $n = 3k \pm 1$, then $\mathrm{Tr}(x^d)$ is bent when restricted to the hyperplane formed by the trace 0 elements in $\mathbb{F}_{2^n}$.

Gao and Lenstra have characterized, in a fundamental paper, when optimal normal elements exist. Normal elements are vastly used in practice, specially for exponentiation in finite fields, a basic operation in cryptography. However, as Gao and Lenstra have shown, optimal normal elements do not exist for every finite field extension of a finite field. The question of finding low complexity normal elements when optimal elements do not exist remains wide open. At the BIRS meeting, Theo Garefalakis, Daniel Panario and David Thomson (later joined by Maria Christopoulou), teamed up to study whether one could obtain normal elements with guaranteed low complexity. They were able to construct such elements by studying traces of optimal normal elements.

The talk by Masuda on permutation binomials over certain finite fields triggered the collaboration, during the workshop, between her and Michael Zieve. As a consequence of this collaboration, they have now submitted a paper where some conjectures on Masuda's previous work are solved. In particular, this new work establishes the nonexistence of binomials for a larger class of finite fields than previously known, or even conjectured.

In recent years many results towards the enumeration of classes of univariate irreducible polynomials with certain characteristics have appeared in the literature. Marko Moisio and Kalle Ranto's collaboration in Banff centered on the study of irreducible polynomials with two prescribed coefficients. This problem is quite hard and only very basic results are known. For example, Carlitz has studied the case when the two fixed coefficients are the trace and the independent term of the polynomial. Using properties of Kloosterman sums and enumeration of the number of rational points on some super-singular curves, Moisio and Ranto obtain explicit counting formulas for the number of irreducible polynomials with two prescribed coefficients, for some new special cases.

Related to the Hansen/Mullen conjecture about primitive polynomials with prescribed coefficients, Gary Mullen and Frank Ruskey are considering various possible refinements of the conjecture for primitive and irreducible polynomials over finite fields.

(**Please note:** the references in the section below are for papers which either previously existed and were used in the talks or for work which was initiated or contributed to during the workshop.)

References

[1] Amir Akbary and Qiang Wang, A generalized Lucas sequence and permutation binomials, *Proceedings of the American Mathematical Society*, 134 (2006), no 1, 15-22.

[2] Amir Akbary and Qiang Wang, On some permutation polynomials over finite fields, *International Journal of Mathematics and Mathematical Sciences*, 16 (2005), 2631-2640.

[3] Antonia Bluher and Alain Lasjaunias, "Hyperquadratic Power Series of Degree Four", *Acta Arithmetica*, 124 (2006), 257-268.

[4] Mireille Car and Louis Gallardo, Waring's problem for polynomial biquadrates over a finite field of odd characteristic, to appear in *Functiones et Approximation*.

[5] Maria Christopoulou, Theo Garefalakis, Daniel Panario and David Thomson, The trace of an optimal normal element and low complexity normal bases, preprint, contributed to during the workshop.

[6] Stephen D. Cohen and Mateja Presern, The Hansen-Mullen primitivity conjecture: completion of proof, to appear in the *Proceedings volume for the Number Theory and Polynomials conference*, Bristol, UK, April 2006 (to be published by the LMS).

[7] John Dillon and Gary McGuire, Kasami-Welch functions on hyperplane, in preparation (initiated during BIRS meeting).

[8] Andreas Enge, Computing modular polynomials in quasi-linear time, available at http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/modcomp.pdf

[9] Arnaldo Garcia and Henning Stichtenoth, Some Artin-Schreier towers are easy, *Moscow Math. J.*, 5 (2005), 767-774.

[10] Kenneth Hicks, Gary L. Mullen, Joseph L. Yucas and Ryan Zavislak, A polynomial analogue of the 3N + 1 problem, preprint.

[11] Ralf Koetter, Winnie Li, Pascal Vontobel, and Judy Walker, Characterizations of pseudo-codewords of (low-density) parity-check codes, to appear in *Advances in Mathematics*.

[12] Hendrik K. Lenstra and Carl Pomerance, Primality testing with Gaussian periods, to be submitted.

[13] Ariane Masuda and Michael Zieve, Nonexistence of permutation binomials of certain shapes, preprint.

[14] Ariane Masuda and Michael Zieve, Rational functions with linear relations, preprint.

[15] Ariane Masuda and Michael Zieve, Permutation binomials over finite fields, preprint.

[16] Marko Moisio and Kalle Ranto, Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed, preprint, contributed to during workshop.