Workshop on Polynomials over Finite Fields: Functional and Algebraic Properties
19-24 May 2014

SCHEDULE

Monday

10:00–11:00 Jean-Charles Faugere, On the complexity of solving polynomial systems over finite fields
11:00–11:30 Coffee Break
11:30–12:05 Omran Ahmadi, Sets with many pairs of orthogonal vectors over finite fields
12:05–12:40 Antonio Rojas Leon, Rational points on curves with many automorphisms
12:40–13:15 Arne Winterhof, Generalizations of complete mappings of finite fields
13:30–15:00 Lunch
15:00– Afternoon session, in smaller groups
19:00– Welcome reception

Tuesday

10:00–11:00 Brigitte Vallée, Probabilistic analysis of gcd algorithms: Introduction of a dynamical point of view, and comparison between polynomials and integers
11:00–11:30 Coffee Break
11:30–12:15 Eric Schost, Constructing finite fields
12:15–13:00 Qiang Wang, On value set of polynomials over finite fields
13:30–15:00 Lunch
15:00– Afternoon session, in smaller groups

Wednesday

10:00–11:00 Pär Kurlberg, Arithmetic geometry applications of cycle lengths mod p
11:00–11:30 Coffee Break
11:30–12:15 Martin Sombra, Modular reduction of systems of polynomial equations
12:15–13:00 Igor Shparlinski, Effective Hilbert’s Nullstellensatz and finite fields
13:30–15:00 Lunch
15:00– Excursion

Thursday

10:00–11:00 Wen-Ching Li, Combinatorial zeta functions
11:00–11:30 Coffee Break
11:30–12:05 Guillermo Matera, On the number of elements in linear families of polynomials with a given factorization pattern
12:05–12:40 Henning Stichtenoth, Recursive towers of curves over finite fields
12:40–13:25 Sudhir Ghorpade, Carlitz-Wan conjecture for permutation polynomials and Weil bound for curves over finite fields
13:30–15:00 Lunch
15:00– Afternoon session, in smaller groups
Friday

10:00–11:00  Gary McGuire, *Recent developments in the Discrete Logarithm Problem in finite fields*
11:00–11:30 Coffee Break
11:30–12:15 Konstantin Ziegler, *Tame decompositions and collisions*
12:15–13:00 Ivelisse Rubio, *Applications of the covering method for computing p-divisibility of exponential sums*
13:30–15:00 Lunch

**ABSTRACTS**

1. **Omran Ahmadi** (Institute for Research in Fundamental Sciences (IPM), Iran)
   
   *Sets with many pairs of orthogonal vectors over finite fields*
   
   Abstract: Let $n$ be a positive integer and $\mathcal{B}$ be a non-degenerate symmetric bilinear form on $\mathbb{F}_q^n$, where $q$ is an odd prime power and $\mathbb{F}_q$ is the finite field with $q$ elements. We determine the largest possible cardinality of a subset $S \subset \mathbb{F}_q^n$ such that $|\{\mathcal{B}(x, y) | x, y \in S \text{ and } x \neq y\}| = 1$.

2. **Jean-Charles Faugere** (INRIA-UPMC-CNRS - LIP6, France)
   
   *On the complexity of solving polynomial systems over finite fields*
   
   Abstract: Solving polynomial systems (PoSSo) is a fundamental problem in Computer Algebra. This problem is NP-Hard and have applications in robotics, mecanism, cryptology, biology, .... The goal of this talk is to show that the complexity of PoSSo can be decreased significantly when the solutions are to be found in a finite field (for instance the cryptanalysis of several modern ciphers reduces to this problem).

   The idea of the algorithm is to combine exhaustive search with Gröbner bases. The efficiency of this method is related to the choice of a trade-off between the two methods. We prove that the optimal trade-off is achieved by fixing a number of variables proportional to the number of variables of the system considered, denoted $n$. Under some natural algebraic assumption, we have been able to quantify the gain provided by this approach compared to a direct Gröbner basis method: for quadratic systems, this gain is exponential in $n$ and is equal to $2^{1.49n}$, where the size of the finite field is big enough.

   In the particular Boolean case we can go even further. Up to now, the best complexity bound was reached by an exhaustive search in $O(2^n)$ operations. Under precise algebraic assumptions on the input system, we exhibit an algorithm that runs in expected complexity $O(2^{0.792n})$. We also give a rough estimate for the actual threshold between our method and exhaustive search, which is as low as 200, and thus very relevant for cryptographic applications.

   *Joint work with M. Bardet, L. Bettale, L. Perret, B. Salvy and P.J. Spaenlehauer.*

3. **Sudhir Ghorpade** (Indian Institute of Technology Bombay, India)
   
   *Carlitz-Wan conjecture for permutation polynomials and Weil bound for curves over finite fields*
   
   Abstract: The Carlitz-Wan conjecture, which is now a theorem, asserts that for any positive integer $n$, there is a constant $C_n$ such that if $q$ is any prime power bigger than $C_n$ with $\text{GCD}(n, q - 1) > 1$, then there is no permutation polynomial of degree $n$ over the finite field with $q$ elements. From the work of von zur Gathen (1991), it is known that one can take $C_n = n^4$. On the other hand, a conjecture of Mullen (1993), which asserts essentially that one can take $C_n = n(n - 2)$ has been shown to be false. We will discuss a precise version of Weil bound for the number of points of affine algebraic curves over finite fields and show how it can be used to obtain a refinement of the result
of von zur Gathen where \( n^4 \) is replaced by a sharper bound. As a corollary, we show that Mullen’s conjecture holds in the affirmative if \( n(n - 2) \) is replaced by \( n^2(n - 2)^2 \).

Joint work with Jasbir Chahal.

4. Pär Kurlberg (KTH Royal Institute of Technology, Sweden)

*Arithmetic geometry applications of cycle lengths mod \( p \)*

Abstract: We will investigate the relationship between periods of iterates of rational maps (reduced modulo \( p \)) and two questions from arithmetic dynamics, namely dynamical analogues of the Mordell-Lang conjecture (an infinite intersection of an orbit with a subvariety implies strong periodicity properties on the subvariety) and the Brauer-Manin problem (an empty intersection of an orbit with a subvariety follows from the adelic orbit closure having empty intersection with the subvariety.)

5. Antonio Rojas Leon (Universidad de Sevilla, Spain)

*Rational points on curves with many automorphisms*

Abstract: Using tools from \( l \)-adic cohomology like Fourier transform, multiplicative convolution of sheaves and partial \( L \) functions, we will show how one can improve the Weil bound for the number of points on curves in certain cases in which the curve has a large abelian group of automorphisms, like the curves defined by polynomials of Artin-Schreier and Kummer type. This is based on earlier joint work with Daqing Wan.

6. Wen-Ching Li (The Pennsylvania State University, USA)

*Combinatorial zeta functions*

Abstract: Combinatorial zeta functions are quotients of polynomials. They are analogous to the zeta functions of varieties defined over finite fields, and share similar properties. In this talk we shall compare these two kinds of zeta functions, and discuss similarities and dissimilarities.

7. Guillermo Matera, (Universidad Nacional General Sarmiento, Argentina)

*On the number of elements in linear families of polynomials with a given factorization pattern*

Abstract: The distribution of factorization patterns on linear families of univariate polynomials of a given degree is considered. Let \( M(n) \) be the set of monic univariate polynomials of degree \( n \) with coefficients in the finite field \( F_q \) of \( q \) elements and let \( L \subseteq M(n) \) be a linear family, namely the set of elements of \( M(n) \) whose coefficients satisfy certain linear relations. Given a factorization pattern \( \lambda \), we shall discuss a methodology which allows us to associate an algebraic variety \( V \) defined over \( F_q \) to the set \( L_\lambda \) of polynomials in \( L \) having such a factorization pattern \( \lambda \). A critical point is that \( V \) is defined by symmetric \( n \)-variate polynomials, namely polynomials which are invariant under any permutation of their variables. This allows us to show that \( V \) satisfies certain geometric conditions, from which we obtain explicit estimates on the number of rational points of \( V \), and thus on the number of elements in \( L_\lambda \). Our results hold for fields of characteristic greater than 2, and imply that \( L \) is uniformly distributed, in the sense of S.D. Cohen. The methodology can also be applied in order to estimate the average value set on any such linear family \( L \).

8. Gary McGuire (University College Dublin, Ireland)

*Recent developments in the Discrete Logarithm Problem in finite fields*

Abstract: This talk will survey recent developments in the DLP index calculus algorithm that have given rise to new world records. We will explain how polynomials of a certain shape are important in the new methods. Based on joint work with Faruk Göloğlu, Robert Granger, and Jens Zumbrägel.

9. Ivelisse Rubio (University of Puerto Rico, Rio Piedras, Puerto Rico)

*Applications of the covering method for computing \( p \)-divisibility of exponential sums*

3
Abstract: The $p$-divisibility of exponential sums of polynomials over finite fields can be used for a variety of applications. A little improvement on the estimation of the $p$-divisibility might be important in some applications. For example, the relation between the 2-divisibility of a Boolean function and certain deformations gives information about cosets of Reed-Muller codes. Moreover, the computation of the exact $p$-divisibility of exponential sums associated to families of systems of polynomials guarantees the solvability of the system and, in the case of a Boolean function, it proves that the functions are not balanced.

In this talk we present the covering method, an elementary method to compute $p$-divisibility of exponential sums and see how it can be used in some applications.

10. **Eric Schost** (University of Western Ontario, Canada)

*Constructing finite fields*

Abstract: Building and computing in arbitrary finite fields is a fundamental task in any computer algebra system. Many questions remain open regarding the complexity of this kind of calculation, some of them very challenging.

If we allow probabilistic algorithms, it is known that one can build and compute in arbitrary finite fields in polynomial time; our goal here is to provide algorithms for computing in an arbitrary finite field in almost linear time. I will describe work in this direction by Shoup, Lenstra, Couveignes and Lercier, as well as recent results obtained with De Feo and Doliskani.

11. **Igor Shparlinski** (The University of New South Wales, Australia)

*Effective Hilbert’s Nullstellensatz and finite fields*

Abstract: We give an overview of recent applications of effective versions of Hilbert’s Nullstellensatz (HN) to various problems in the theory of polynomial dynamical systems over finite fields. In particular, we show applications to the bounds on the period length of orbits of polynomial dynamical systems over finite fields and to orbit intersections of such systems.

We also mention some other application of HN to polynomials over finite fields due to Bombieri-Bourgain-Konyagin (zeros of sparse polynomials) and to Chang (diameter of partial trajectories of polynomial dynamical systems).

*Joint work with Carlos D’Andrea, Alina Ostafe and Martin Sombra.*

12. **Martin Sombra** (University of Barcelona, Spain)

*Modular reduction of systems of polynomial equations*

Abstract: For a large prime $p$, the reduction mod $p$ of a system of polynomial equations with integer coefficients shares many of the properties (dimension, degree) of the original system over the complex numbers. I will show that, using effective versions of Hilbert’s Nullstellensatz, it is possible to give a bound on the size of those prime numbers. These bounds have applications to study of the reduction mod $p$ of dynamical systems.

*Joint work with Carlos D’Andrea, Alina Ostafe and Igor Shparlinski.*

13. **Henning Stichtenoth** (Sabanci University, Turkey)

*Recursive towers of curves over finite fields*

Abstract: For many applications, one needs curves over a finite field having many rational points. A suitable method for constructing such curves is provided by recursive towers of curves. Such towers were first introduced by Feng and Rao (in an attempt to give an elementary approach to the Tsfasman–Vladut–Zink theorem), and they were systematically studied by A. Garcia and H. Stichtenoth. I will introduce the construction of recursive towers, give examples and discuss problems arising in this context.
14. Brigitte Vallée (Laboratoire GREYC, CNRS and Université de Caen, France)

Probabilistic analysis of gcd algorithms: Introduction of a dynamical point of view, and comparison between polynomials and integers

Abstract: Computing gcds is a common operation, perhaps the fifth main arithmetic operation. Indeed, in many symbolic computation systems, a large proportion of the time is devoted to computing gcds on numbers or polynomials in order to keep fractions under an irreducible form. Here, we deal with the case when inputs are either integers or polynomials over a finite field \( \mathbb{F}_q \). When there are only two inputs (polynomials or integers), various methods have been designed to compute gcds. The Euclid Algorithm or its variants play a central role here, and Knuth writes that the Euclid algorithm can be called “the granddaddy of all algorithms, because it is the oldest nontrivial algorithm that has survived to the present day”.

Here, we are concerned by the case when the gcd of \( \ell \) inputs \( x_1, \ldots, x_\ell \), with \( \ell \geq 2 \) has to be computed. The most straightforward algorithm, described in Knuth’s book, is a sequence of \( \ell - 1 \) gcd computations on two entries: one lets \( y_1 := x_1 \), then, for \( k \in [2, \ell] \), one successively computes \( y_k := \text{gcd}(x_k, y_{k-1}) = \text{gcd}(x_1, x_2, \ldots, x_k) \). The “total” gcd is \( y_\ell := \text{gcd}(x_1, x_2, \ldots, x_\ell) \), and it is obtained after \( \ell - 1 \) phases. We call it the plain \( \ell \)-Euclid algorithm. Knuth wrote: “In most cases, the length of the partial gcd decreases rapidly during the first few phases of the calculation, and this will make the remainder of the computation quite fast”. However, to the best of our knowledge, the plain \( \ell \)-Euclid algorithm has not been yet analyzed (It was proposed as an exercise in Knuth’s book). The situation contrasts with the case \( \ell = 2 \), where the classical Euclid algorithm and its main variants running on integers or on polynomials are now precisely analyzed.

The talk has three main aims:
(a) We first perform a precise probabilistic analysis of the plain algorithm, and we make more precise the phenomenon which was remarked by Knuth: in most cases, “almost all the calculation” is done during the first phase. This will make possible to compare the \( \ell \)-Euclid algorithm to another strategies.
(b) As usual, the results are similar in the two cases (polynomials and integers), even though the analysis is much more difficult in the integer case. We first explain the differences between the two analyses: In the polynomial case, classical tools of analytic combinatorics, described in the book of Flajolet and Sedgewick, may be used, whereas the analysis in the integer case is based on a methodology which mixes analytic combinatorics and dynamical systems and was introduced by the author.
(c) We finally describe a common dynamical framework for the two analyses.

15. Qiang Wang (Carleton University, Canada)

On value set of polynomials over finite fields

Abstract: Let \( \mathbb{F}_q \) be a finite field of \( q \) elements with characteristic \( p \). The value set of a polynomial \( f \) over \( \mathbb{F}_q \) is the set \( V_f \) of images when we view \( f \) as a mapping from \( \mathbb{F}_q \) to itself. Clearly \( f \) is a permutation polynomial (PP) of \( \mathbb{F}_q \) if and only if the cardinality \( |V_f| \) of the value set of \( f \) is \( q \).
It was conjectured by Mullen and then first proved by Wan that if \( f \) is not a PP over \( \mathbb{F}_q \) then \( |V_f| \leq q - \lceil (q - 1)/d \rceil \), where \( d \) is the degree of the polynomial. In general, let \( f : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n \) be a polynomial map in \( n \) variables defined over \( \mathbb{F}_q \), where \( n \) is a positive integer. Denote by \( |V_f| \) the number of distinct values taken by \( f(x_1, \ldots, x_n) \) as \( (x_1, \ldots, x_n) \) runs over \( \mathbb{F}_q^n \). In this talk, we first give an upper bound of \( |V_f| \) in terms of the total degree of the multivariate polynomial \( f \) over \( \mathbb{F}_q \) following the approach of studying value set problems in terms of the degree of a polynomial. Secondly, we introduce a new approach to obtain an index upper bound by studying the index of a polynomial. In particular, this answers an open problem raised by Lipton in his computer science blog.

Joint work with Gary L. Mullen and Daqing Wan.

16. Arne Winterhof (RICAM, Austrian Academy of Sciences, Austria)
**Generalizations of complete mappings of finite fields**

**Abstract:** Let \( f(X) \in \mathbb{F}_q[X] \) be a permutation polynomial over \( \mathbb{F}_q \). For \( k = 0, 1, \ldots \) we define the \( k \)-th iteration \( f^{(k)}(X) \) of \( f(X) \) by the recurrence relation
\[
    f^{(0)}(X) = X, \quad f^{(k)}(X) = f(f^{(k-1)}(X)), \quad k = 1, 2, \ldots.
\]

For a finite set of \( s \) positive integers \( \mathcal{K} = \{k_1, \ldots, k_s\} \) we call \( f(X) \) a \( \mathcal{K} \)-complete mapping if
\[
    F_{\mathcal{K}}(X) = X + \sum_{k \in \mathcal{K}} f^{(k)}(X)
\]
is also a permutation polynomial. The concept of \( \mathcal{K} \)-complete mappings unifies several kinds of mappings studied before in view of applications to cryptography, coding theory, and combinatorics. For \( \mathcal{K} = \{1\} \), that is, \( f(X) \) and \( X + f(X) \) are both permutation polynomials we get complete mappings as a first special case.

A permutation polynomial \( f(X) \) is called an orthomorphism if \( -X + f(X) \) is also a permutation polynomial. Note that \( f(X) \) is an orthomorphism whenever \( -f(X) \) is a complete mapping and both terms coincide in characteristic 2. In analogy to \( \mathcal{K} \)-complete mappings we define a \( \mathcal{K} \)-orthomorphism as a permutation polynomial such that
\[
    \tilde{F}_{\mathcal{K}}(X) = -X + \sum_{k \in \mathcal{K}} f^{(k)}(X)
\]
is also a permutation.

It is easy to see that \( f(X) = aX \) is a \( \mathcal{K} \)-complete mapping or a \( \mathcal{K} \)-orthomorphism whenever \( \sum_{k \in \mathcal{K}} a^k \neq -1 \) or \( \neq 1 \), respectively.

In the first part of the talk we recall some known applications of these permutations including check digit systems.

In the second part of this paper we study the problem if certain classes of polynomials contain \( \mathcal{K} \)-complete mappings or \( \mathcal{K} \)-orthomorphisms for certain types of \( \mathcal{K} \). These classes are linear polynomials, polynomials of degree 3, monomials, and cyclotomic mapping polynomials of order 2.

17. **Konstantin Ziegler** (Bonn-Aachen International Center for Information Technology, Germany)

**Tame decompositions and collisions**

**Abstract:** A univariate polynomial \( f \) over a field is decomposable if \( f = g \circ h = g(h) \) for nonlinear polynomials \( g \) and \( h \). It is intuitively clear that the decomposable polynomials form a small minority among all polynomials over a finite field. The tame case, where the characteristic of \( \mathbb{F}_q \) does not divide \( n = \deg f \), is fairly well-understood, and we have reasonable bounds on the number of decomposables of degree \( n \). Nevertheless, no exact formula is known if \( n \) has more than two prime factors. In order to count the decomposables, one wants to know, under a suitable normalization, the number of collisions, where essentially different components \( (g, h) \) yield the same \( f \). In the tame case, Ritts Second Theorem classifies all collisions of two such pairs.

We present a normal form for collisions of any number of decompositions with any number of components and describe exactly the (non)uniqueness of the parameters in the tame case. This yields an efficiently computable formula for the exact number of such collisions over a finite field. We conclude with an efficient algorithm for the exact number of decomposable polynomials of degree \( n \) over a finite field \( \mathbb{F}_q \) of characteristic coprime to \( n \).