Workshop on

Algebraic Curves Over Finite Fields

November 11-15, 2013

as part of the

Radon Special Semester 2013 on

Applications of Algebra and Number Theory

ÖAW
Austrian Academy
of Sciences

RICAM
JOHANN·RADON·INSTITUTE
FOR COMPUTATIONAL AND APPLIED MATHEMATICS

"*On the zeta function of curves over finite fields*"
Nurdagül Anbar Sabanci University Istanbul, Turkey

Abstract

Let $L(t) = 1 + a_1 t + \cdots + a_{2g} t^{2g}$ be the numerator of the zeta function of an algebraic curve $\mathcal{C}$ defined over the finite field $\mathbb{F}_q$ of genus g. We show that the coefficients a_r of $L(t)$ satisfy certain inequalities. Conversely, for any integers $a_1, \ldots, a_m$ satisfying these inequalities and all sufficiently large integers g there exist curves of genus g, whose L-polynomial satisfies the following congruence.

$$L(t) \equiv 1 + a_1 t + \cdots + a_m t^m \pmod{t^{m+1}}.$$

In fact, this result is equivalent to the following statement: for any non-negative integers $b_1, \ldots, b_m$ and all sufficiently large integers g there exist curves of genus g having exactly b_j points of degree j, for $1 \leq j \leq m$.
This is a joint work with Henning Stichtenoth.

Reference. N. Anbar, H. Stichtenoth, *Curves of every genus with a prescribed number of rational points*, Bulletin of the Brazilian Mathematical Society, **44** (2013), 173–193.

"*Obtaining towers using Drinfeld modules*"
Peter Beelen Technical University of Denmark

Abstract

In this talk, an overview will be given of known and new techniques on how one can obtain explicit equations for candidates of good towers of function fields. The techniques are founded in modular theory (both the classical modular theory and the Drinfeld modular theory). In the classical modular setup, optimal towers can be obtained, while in the Drinfeld modular setup, good towers over any non-prime field may be found. We illustrate the theory with several examples, thus explaining some known towers as well as giving new examples of good explicitly defined towers of function fields.

"*Bounds for the number of rational points on curves over finite fields.*"
Herivelto Borges
Universidade de São Paulo - São Carlos, Brazil.

Abstract

Let $\mathcal{X}$ be a projective irreducible nonsingular curve defined over a finite field K. Considering certain linear series on $\mathcal{X}$, we establish new upper bounds for the number of rational points defined on some extensions of K. The method is based on the theory of Stöhr-Voloch, and it can be considered as a variation thereof. Some examples using the Veronese morphism will be presented and discussed. We will see that, in certain cases, the bounds obtained are effective improvements of the Stöhr-Voloch, Hasse-Weil and Ihara bounds.

This is joint work with Nazar Arakelian.

"*Weierstrass semigroups at several points, total inflection points on curves and coding theory*"
Cícero Carvalho Universidade Federal de Uberlândia, Brazil

Abstract

Let $\mathcal{X}$ be a smooth curve of genus g defined over a finite field $\mathbb{F}$ which is the full field of constants of $\mathbb{F}(\mathcal{X})$. Let $P_1, \ldots, P_m$ be rational points of $\mathcal{X}$, denote by $\mathbb{N}_0$ the set of nonnegative integers and by $\operatorname{div}_\infty(f)$ the pole divisor of $f \in \mathbb{F}(\mathcal{X})$. The *Weierstrass semigroup at* $P_1, \ldots, P_m$ is defined as

$$H(P_1, \ldots, P_m) := \{(\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m \mid \exists f \in \mathbb{F}(\mathcal{X}) \text{ with } \operatorname{div}_\infty(f) = \sum_{i=1}^{m} \alpha_i P_i\}.$$

This semigroup has been studied by several authors in the past decades and we would like to start this talk by presenting some of its properties and also the following application to coding theory which was discovered by Homma and Kim and further developed by Carvalho and Torres. The set $\mathbb{N}_0^m \setminus H(P_1, \ldots, P_m)$ is called *the set of gaps* of the semigroup, the above mentioned authors proved that by choosing special points in the set of gaps one can construct algebraic geometry codes which have a better bound for the minimum distance than the Goppa bound. All of these results could be stated in the language of function fields of one variable, without reference to curves, yet we will present results by Carvalho and Kato which describe how an extrinsic geometry property of curves, namely, the existence of total inflection points on a smooth plane curve, can determine the existence of these special gaps in certain Weierstrass semigroups.

"*Asymptotics of arithmetic codices and towers of function fields*"
Ignacio Cascudo CWI Amsterdam, The Netherlands

Abstract

Multiplicative secret sharing schemes are a cryptographic notion which is useful in the area of secure multiparty computation. In recent years, asymptotics of multiplicative secret sharing schemes have become important due to interesting applications in communication efficient two-party computation.

Roughly, we are interested in linear codes C over a finite field where both the dual of C and some "power" of C have good minimum distance. We can consider a more general concept (which we dubbed arithmetic codex) which also encompasses the notion of bilinear multiplication algorithm from algebraic complexity.

Towers of algebraic function fields with many rational points are currently the only known resource for the construction of families of codices with the asymptotic properties we are interested in. A notion we called the torsion limit of the tower is of great interest.

I will survey recent results in the area, which are mainly joint work with Ronald Cramer (CWI) and Chaoping Xing (NTU Singapore).

"*Maximal Fermat varieties*"
Iwan Duursma University of Illinois at Urbana-Champaign, USA

Abstract

We classify all hypersurfaces $X_0^d + \cdots + X_r^d = 0$ of degree d in projective $r-$space over a finite field that attain the Weil-Deligne upper bound or lower bound for the number of rational points.

"*Smooth models for the Suzuki and Ree curves*"
Abdulla Eid University of Illinois at Urbana-Champaign, USA

Abstract

The Hermitian, Suzuki and Ree curves form three special families of curves with unique properties. They arise as the Deligne-Lusztig varieties of dimension one and their automorphism groups are the algebraic groups of type 2A2, 2B2 and 2G2, respectively. The Hermitian curve has a smooth model as plane curve. For the Suzuki and Ree curves we give defining equations for smooth models in projective 4-space and projective 13-space, respectively.

Part 1: The algebraic groups 2A2, 2B2 and 2G2, the function fields for the Suzuki and Ree curves, their Weierstrass semigroups.

Part 2: The Deligne-Lusztig construction of the Suzuki and Ree curves, very ample divisors on the curves, smooth models and their equations, comparison with invariant embeddings by Kane using a recent description of the Ree group by Wilson.

“*On curves over finite fields*”

Arnaldo Garcia IMPA Rio de Janeiro, Brazil

Abstract

The investigation of curves over finite fields has a long history, the main result being Weil‘s Theorem bounding the number of rational points (equivalent to the validity of Riemann‘s Hypothesis in this context). Ihara has shown that Weil‘s bound was weak for high genus curves, and he then considered a certain constant (the so-called Ihara‘s constant) that measures the asymptotic behaviour, as the genus goes to infinity, of the ratios (number of rational points)/ genus. To deal with Ihara‘s constant we introduce towers of curves and their limits. The aim is to present a new tower over nonprime finite fields with a very remarkable limit, improving a lot former results. This tower was obtained together with Alp Bassa, Peter Beelen and Henning Stichtenoth.

“*Affine variety codes are better than their reputation*”

Olav Geil Aalborg University, Denmark

Abstract

In this joint work with Stefano Martin we present two new methods for estimating the minimum distance of affine variety codes. Namely one for dual codes and one for primary codes. Our bound for dual codes improves previous results by Salazar et. al., whereas our bound for primary codes is completely new. As becomes clear from the bounds, affine variety codes can be very good, also in the cases where they are not one-point algebraic geometric codes in disguise.

“*Good covering codes from algebraic curves*”

Massimo Giulietti Università degli Studi di Perugia, Italy

Abstract

The covering radius of a linear $[n, k, d]_q$-code C is the minimum integer R for which the spheres of radius R centered in codewords cover the whole space $\mathbb{F}_q^n$. An $[n, k, d]_q$-code with covering radius R is sometimes called an $[n, k, d]_q R$-code. One of the parameters characterizing the covering quality of an $[n, k, d]_q R$-code is its covering density, that is the average number of codewords at distance less than or equal to R from a vector in $\mathbb{F}_q^n$. For fixed codimension and covering radius, the shorter the code the better its covering density. This is why one of the central problems concerning covering codes is that of constructing *short* linear codes for fixed codimension r, order q, minimum distance d, and covering radius R.

It is easily seen that the covering density of a code is greater than or equal to 1. When equality is attained - or, equivalently, when $R = \lfloor (d-1)/2 \rfloor$ - the code is said to be perfect. A classical result from Coding Theory is the classification of linear perfect codes: apart from trivial examples, the only possibilities are Hamming codes and the two sporadic Golay codes.

In this talk we deal with both $[n, n-r, 4]_q 2$-codes and $[n, n-r, r+1]_q (r-1)$ codes. Interestingly, the former are *quasi-perfect* codes, that is codes for which $R = \lfloor (d-1)/2 \rfloor + 1$ holds, whereas the latter are MDS codes. The geometrical counterparts of these objects are *complete n-caps* and *complete n-arcs* in $\mathbb{P}^{r-1}(\mathbb{F}_q)$, the projective Galois space of dimension $r-1$ over $\mathbb{F}_q$. An n-cap in $\mathbb{P}^{r-1}(\mathbb{F}_q)$ is a set of n points no three of which are collinear, whereas an n-arc is a set of n points every r of which are linearly independent; if an n-cap, or an n-arc, is maximal with respect to set theoretical inclusion then it is said to be complete.

Our aim is to provide a survey on the state of the art of the research on short $[n, n-r, 4]_q 2$-codes and $[n, n-r, r+1]_q (r-1)$ codes, with particular emphasis on recent developments. In the last decade a number of new results have appeared, and new notions have emerged as powerful tools in dealing with the covering problem, including bicovering arcs and translation caps. Although caps and arcs are rather combinatorial objects, constructions and proofs sometimes heavily rely on concepts and results from Algebraic Geometry in positive characteristic. In particular, new examples of complete n-arcs are obtained from the set of $\mathbb{F}_q$-rational points of certain elliptic curves in $\mathbb{P}^{r-1}(\mathbb{F}_q)$.

"*Symmetric digit sets for elliptic curve scalar multiplication*"

Clemens Heuberger Alpen-Adria-Universität Klagenfurt, Austria

Abstract

One way for efficient scalar multiplication in abelian groups is to use appropriate digit expansions such as the classical binary double-and-add method. Generalisations may use larger digit sets—thus requiring precomputation of some multiples—and other bases which can be implemented more efficiently than doubling.

In the setting of an elliptic curve defined over the ground field $\mathbb{F}_p$, the Frobenius endomorphism sending elements to their pth powers corresponds to an imaginary quadratic integer base. For suitable choices of curves, roots of unity also act on the curve in a computationally inexpensive way. Using those, the precomputation effort can be decreased.

Choosing the digit set as the elements of some multiplicative group which can be factored into few cyclic groups further decreases the precomputation effort while not significantly increasing the running time of the scalar multiplication itself.

We give examples of curves in various characteristics where these ideas lead to efficient scalar multiplication algorithms.

This is joint work with Michela Mazzoli.

"*Galois module structure of polydifferentials of Mumford Curves*"

Aristides Kontogeorgis Athens, Greece

Abstract

We study the Galois-module structure of polydifferentials on Mumford curves, defined over a field of positive charactersitic. The identification of these spaces to spaces of Harmonic cocycles will be used and the structure of polydifferentials is reduced to a problem of cohomology of groups. As an example the Galois module structure of the curves $(y^p - y)(x^p - x) = c$ will be discussed.

This is a joint work with Janne Kool (Utrecht) and Fumiharu Kato (Kumamoto).

"*Garden of curves with many automorphisms*"

Gábor Korchmáros Università degli Studi della Basilicata Potenza, Italy

Abstract

This is a joint work with M. Giulietti.

Let $\mathcal{X}$ be a (projective, geometrically irreducible, non-singular) algebraic curve defined over an algebraically closed field $\mathbb{K}$ of characteristic $p \geq 0$. Let $\mathbb{K}(\mathcal{X})$ be the field of rational functions (the function field of transcendency degree one over $\mathbb{K}$) of $\mathcal{X}$. The $\mathbb{K}$–automorphism group $\mathrm{Aut}(\mathcal{X})$ of $\mathcal{X}$ is defined to be the automorphism group $\mathrm{Aut}(\mathbb{K}(\mathcal{X}))$ consisting of those automorphisms of $\mathbb{K}(\mathcal{X})$ which fix each element of $\mathbb{K}$. $\mathrm{Aut}(\mathcal{X})$ has a faithful action on the set of points of $\mathcal{X}$.

By a classical result, $\mathrm{Aut}(\mathcal{X})$ is finite if the genus $\mathfrak{g}$ of $\mathcal{X}$ is at least two.

It has been known for a long time that every finite group occurs in this way, since for any ground field $\mathbb{K}$ and any finite group G, there exists $\mathcal{X}$ such that $\mathrm{Aut}(\mathcal{X}) \cong G$,

This result raised a general problem for groups and curves: Determine the finite groups that can be realized as the $\mathbb{K}$-automorphism group of some curve with a given invariant. The most important such invariant is the genus $\mathfrak{g}$ of the curve, and there is a long history of results on the interaction between the automorphism group of a curve and its genus.

In positive characteristic, another important invariant is the p-rank of the curve (also called the Hasse-Witt invariant), which is the integer γ so that the Jacobian of $\mathcal{X}$ has p^γ points of order p. It is known that $0 \leq \gamma \leq \mathfrak{g}$.

In this survey we focus on the following issues:

(i) Upper bounds on the size of G depending on $\mathfrak{g}$.

(ii) Examples of curves defined over a finite field with very large automorphism groups.

(iii) The possibilities for G when the p-rank is 0.

(iv) Upper bounds on the size of the p-subgroups of G depending on the p-rank.

The study of the automorphism group of an algebraic curve is mostly carried out by using Galois theory, via the fundamental group of the curve. Here, we adopt a different approach in order to exploit the potential of finite group theory.

"*Typical size and cancellations among coefficients of modular forms*"
Florian Luca UNAM, Juriquilla, Mexico

Abstract

We obtain a nontrivial upper bound for almost all elements of the sequences of real numbers which are multiplicative and at the prime indices are distributed according to the Sato-Tate density. Examples of such sequences come from coefficients of several L-functions of elliptic curves and modular forms. In particular, we show that $|\tau(n)| \leq n^{11/2}(\log n)^{-1/2+o(1)})$ for a set of n of asymptotic density 1, where $\tau(n)$ is the Ramanujan τ function. In comparison, the standard argument, based on the estimate for the number of prime divisors of a typical integer n, only leads to the bound $|\tau(n)| \leq n^{11/2}(\log n)^{\log 2+o(1)}$ for almost all n.

This is joint work with Igor Shparlinski.

"*Superspecial rank of supersingular curves*"
Rachel Pries Colorado State University, USA

Abstract

A curve X of genus g defined over a finite field is *supersingular* if the Newton polygon of the L-polynomial of X is a line segment of slope 1/2. Equivalently, X is supersingular if and only if the Jacobian $\mathrm{Jac}(X)$ is isogenous to a product of supersingular elliptic curves. Only in rare cases is $\mathrm{Jac}(X)$ isomorphic to a product of supersingular elliptic curves, in which case X is called *superspecial.*

In this talk, I will define the *superspecial rank*, which is an invariant of the Dieudonné module or Ekedahl-Oort type of a principally polarized abelian variety. If X is a supersingular curve, then the superspecial rank determines the number of elliptic factors in the decomposition of $\mathrm{Jac}(X)$ up to isomorphism. As examples, we compute the superspecial rank of Hermitian curves and Suzuki curves. I will describe results about the superspecial rank of curves in characteristic 2. If time permits, I will talk about the superspecial rank on the supersingular locus of the moduli space $\mathcal{A}_g$.

"*Weierstrass points on cyclic extensions*"
Luciane Quoos Universidade Federal do Rio de Janeiro, Brazil

Abstract

For Kummer extensions $y^m = f(x)$ we discuss conditions for an integer be a Weierstrass gap at a point P. For the totally ramified points, the conditions will be necessary and sufficient. As a consequence, we extend independent results of Hasse, Valentini-Madan, Leopoldt and Towse. This is a joint work with Miriam Abdon(UFF) and Herivelto Borges(USP).

"*Distribution of genus* 3 *curves over finite fields according to their trace*"
Christophe Ritzenthaler IRMAR, Rennes, France

Abstract

Presenting some numerical evidences, we would like to convince the audience that there seem to be new phenomenas structuring the distribution, with respect to the trace of their Frobenius endomorphism, of isomorphism classes of genus 3 curves over finite fields. These observations can be interpreted as fluctuations in Katz-Sarnak theory and contain important information about the maximal number of points of genus 3 curves, $N_q(3)$. In order to do that, we will need better normal models to describe all strata of smooth quartics with a given automorphism group. This is joint work with Reynald Lercier, Florent Rovetta, Jeroen Sijsling and Ben Smith.

"*Analogue of the Kronecker–Weber Theorem in positive characteristic*"

Gabriel Villa–Salvador Centro de Investigación y de Estudios Avanzados del I.P.N., Mexico

Abstract

The classical Kronecker–Weber Theorem establishes that the maximal abelian extension of the field of rational numbers is the union of all cyclotomic number fields. In 1974, D. Hayes proved the analogue in characteristic $p > 0$. Hayes' result says that the maximal abelian extension of the rational function field $\mathbb{F}_q(T)$ is the composite of three pairwise linearly disjoint extensions. The first one is the union of all cyclotomic function fields relative to the infinite prime, the pole divisor of T, introduced by L. Carlitz. The second one is the union of all cyclotomic function fields relative to the zero divisor of T and where the infinite prime is totally wildly ramified and is the only ramified prime. Finally, the third one is the union of all constant extensions. The proof of Hayes is based on the Reciprocity Law. In this work we describe another approach to Hayes' analogue of the Kronecker–Weber Theorem that uses tools from the classical case as well as the ramification theory of Artin–Schreier extensions and the arithmetic of Witt vectors developed by H. Schmid.

"*Optimal rate algebraic list decoding using narrow ray class fields*"

Chaoping Xing Nanyang Technological University, Singapore

Abstract

We use class field theory, specifically Drinfeld modules of rank 1, to construct a family of asymptotically good algebraic-geometric (AG) codes over fixed alphabets. Over a field of size ℓ^2, these codes are within $2/(\sqrt{\ell}-1)$ of the Singleton bound. The functions fields underlying these codes are subfields with a cyclic Galois group of the narrow ray class field of certain function fields. The resulting codes are "folded" using a generator of the Galois group. Using the Chebotarev density theorem, we argue the abundance of inert places of large degree in our cyclic extension, and use this to devise a linear-algebraic algorithm to list decode these folded codes up to an error fraction approaching $1 - R$ where R is the rate. The list decoding can be performed in polynomial time given polynomial amount of pre-processed information about the function field.

Our construction yields algebraic codes over constant-sized alphabets that can be list decoded up to the Singleton bound — specifically, for any desired rate $R \in (0, 1)$ and constant $\epsilon > 0$, we get codes over an alphabet size $(1/\epsilon)^{O(1/\epsilon^2)}$ that can be list decoded up to error fraction $1 - R - \epsilon$ confining close-by messages to a subspace with $N^{O(1/\epsilon^2)}$ elements. Previous results for list decoding up to error-fraction $1 - R - \epsilon$ over constant-sized alphabets were either based on concatenation or involved taking a carefully sampled subcode of algebraic-geometric codes. In contrast, our result shows that these folded algebraic-geometric codes *themselves* have the claimed list decoding property.

This is joint work with Venkatesan Guruswami.

"*Zeta functions of towers of function fields*"

Alexey Zaytsev Kaliningrad, Russia

Abstract

Let $\mathcal{T} = (T_n)_{n\geq 1}$ be a tower of function fields over a finite field. Then there exists a sequence of zeta functions (or L-polynomials) $(Z_n(t))_{n\geq 1}$ (or $(L_n(t))_{n\geq 1}$) attached to it. It is well know that L-polynomial $L_n(t)$ is a polynomial of degree $2g$, where g is genus of T_n. It turns out that if a tower is recursive then we can attach a certain graph to it. Using this graph we can express the first few coefficients of L-polynomials of function field T_n as functions in n explicitly. We also formulate some conjecture on coefficients of L-polynomial for particular example of towers.