Thematic Seminar: “Algebraic Geometry, Coding and Computing”

Universidad de Valladolid - E. U. Informática, Segovia
October 8-10th, 2007

Abstracts:

Monday, October 8th 2007

- **09:10-10:10- J.W.P. Hirschfeld (Sussex University): “Curves over a finite field with many points and some applications”.**

  The number N_1 of rational points on an algebraic curve $\mathcal{F}$ of genus g over the finite field $\mathbf{F}_q$ satisfies the Hasse–Weil bound,

  $$N_1 \leq q + 1 + 2g\sqrt{q}.$$

  When q is odd and $\mathcal{F}$ is a plane curve of degree d with a finite number of inflexions, then

  $$N_1 \leq \tfrac{1}{2}d(d+q-1).$$

  The latter is the Stöhr–Voloch bound in a particular case.

  These and other bounds on curves can be applied to obtain bounds on the length of maximum distance separable codes and on the size of arcs in a finite Desarguesian plane.

  A survey of results is presented.

- **10:15-11:15- S. Ball (Universitat Politècnica de Catalunya): “Punctured Combinatorial Nullstellensatzen and some Applications to Geometry and Codes”.**

  Let $\mathbb{F}$ be a field and let f be a polynomial in $\mathbb{F}[X_1, X_2, \ldots, X_n]$. Suppose that $S_1, S_2, \ldots, S_n$ are arbitrary non-empty finite subsets of $\mathbb{F}$ and define

  $$g_i(X_i) = \prod_{s_i \in S_i} (X_i - s_i).$$

  Alon’s Combinatorial Nullstellensatz states that if f vanishes over all the common zeros of $g_1, g_2, \ldots, g_n$, in other words $f(s_1, s_2, \ldots, s_n) = 0$ for all $s_i \in S_i$, then there are polynomials $h_1, h_2, \ldots, h_n \in \mathbb{F}[X_1, X_2, \ldots, X_n]$ satisfying $deg(h_i) \leq deg(f) - deg(g_i)$ with the property that

  $$f = \sum_{i=1}^{n} h_i g_i.$$

  In this talk I shall present a punctured version of Alon’s Nullstellensatz which states that if f vanishes at nearly all, but not all, of the common zeros of some polynomials $g_1(X_1), \ldots, g_n(X_n)$ then every representative of f in the ideal $\langle g_1, \ldots, g_n \rangle$ has a large degree.

  We shall look at some applications of the punctured Nullstellensatz to projective a nd affine geometries over an arbitrary field which, in the case that the field is finite, will lead to some bounds related to linear codes containing the all one vector.

- **11:45-12:45- G. Korchmaros (University of Basilicata), M. Giulietti (University of Perugia): "Automorphism groups of algebraic curves with p-rank zero".**

  Let $\mathcal{X}$ be a (projective, geometrically irreducible, non-singular) algebraic curve defined over an algebraically closed basefield $\mathbb{K}$ of characteristic $p \geq 0$. By a classical result, the automorphism group $\mathrm{Aut}(\mathcal{X})$ of $\mathcal{X}$ is finite provided that the genus g of $\mathcal{X}$ is at least two. It is known that every finite group occurs in this way, since for any groundfield $\mathbb{K}$ and for any finite group G, there exists $\mathcal{X}$ such that $\mathrm{Aut}(\mathcal{X}) \cong G$. This raises a general problem for groups and curves: Determine the finite groups that can be realized as the automorphism group of some curve with a given invariant, such as genus g, p-rank (for $p > 0$) or number of $\mathbb{F}_q$-rational places (for $\mathbb{K} = \mathbb{F}_q$), where $\mathbb{F}_q$ stands for the finite field of order q. In this talk we deal with zero p-rank curves and their automorphism groups.

- **13:00-14:00- O. Geil (Aalborg University): "On Weierstrass semigroups and rational places".**

  It is an important question in algebraic geometry to estimate what is the maximal number $N_q(g)$ such that there exists a function field over $GF(q)$ of genus g having $N_q(g)$ rational places. Recall, that given a Weierstrass semigroup Λ we have $g = \#(\mathbb{N}_0 \backslash \Lambda)$. It is therefore natural to ask in addition to the above question also the following one. Let Λ be a semigroup that can be realized as a Weierstrass semigroup of at least one rational place in at least one function field. What is the maximal number $N_q(\Lambda)$ such that there exists a function field over $GF(q)$ with a rational place having Λ as a Weierstrass semigroup and having $N_q(\Lambda)$ rational places? Lewittes showed that the smallest generator λ_1 of Λ (called the multiplicity) holds information about this in that $N_q(\Lambda) \leq q\lambda_1 + 1$ holds. We generalize Lewittes' bound to take into account all the generators of Λ. This is joint work with Ryutaroh Matsumoto.

- **16:00-17:00- T. Høholdt and J. Justesen (The Technical University of Denmark): "Graph codes with Reed-Solomon component codes".**

  We treat specific cases of codes coming from bipartite graphs. The code symbols are associated with the edges of the graph and the symbols connected to a given node are restricted to be codewords in a Reed-Solomon code. We present results on the parameters of the codes and in the case where the bipartite graph comes from an Euclidean plane we describe the encoding as evaluation. We also analyse an iterative decoder and in the case where the bipartite graph is complete (corresponding to a product code) we use a recent result on random graphs to show that with high probability a large number of errors can be corrected by iterating minmum distance decoding. We present an analysis related to density evolution which gives an exact asymptotic value of the decoding threshold and also provides a closed form approximation to the distribution of errors in each step of the decoding of finite length codes.

- **17:30-18:30- C. Munuera (Universidad de Valladolid): "Error correcting codes and steganography"**.

  We show some relations between error-correcting codes and steganography. These relations can be used to construct new stegocodes, and thus they open a new line of research in the theory of error-correcting codes, in order to study which codes lead to stegocodes having good properties.

Tuesday, October 9th 2007

- **09:10-10:10- R. Pellikaan (Eindhoven University of Technology): "Decoding linear codes with Gröbner bases".**

  In the first part of our lecture we consider bounded distance decoding of arbitrary linear codes with the use of Gröbner bases. The decoding of cyclic codes up to half the BCH distance is well-known by Peterson, Arimoto and Gorenstein-Zierler, by means of the syndromes s_i of a received word and the error-locator polynomial with coefficients σ_i. They satisfy generalized Newton identities. These equations form a system of t linear equations in the unknowns $\sigma_1, \ldots, \sigma_t$ with the known syndromes $s_1, \ldots, s_{2t}$ as coefficients, if the defining set of the cyclic code contains $2t$ consecutive elements. Gaussian elimination solves this system of equations with complexity $\mathcal{O}(n^3)$. This complexity was improved by the algorithm of Berlekamp-Massey and a variant of the Euclidean algorithm due to Sugiyama et al. Both these algorithms are more efficient than solving the system of linear equations, and are basically equivalent but they decode up to the BCH error-correcting capacity, which is often strictly smaller than the true capacity. All these methods do not correct up to the true error-correcting capacity. The Gröbner bases techniques were addressed to remedy this problem. These methods can be divided into the following categories:

  - Unknown syndromes by Berlekamp and Tzeng-Hartmann-Chien,
  - Power sums by Cooper and Chen-Reed-Helleseth-Truong,
  - Newton identities by Augot-Charpin-Sendrier.

  Our method is a generalization of the first one. Recent work on the second method is by Mora-Sala for cyclic codes. The second method was generalized to arbitrary linear codes by Lax-Fitzgerald.

  The theory of Gröbner basis is about solving systems of polynomial equations in several variables and can be viewed as a common generalization of linear algebra that deals with linear systems of equations in several variables and the Euclidean Algorithm that is about polynomial equations of arbitrary degree in one variable. The polynomial equations are linearized by treating the monomials as new variables. In this way the number of variables grows exponentially in the degree of the polynomials. The complexity of computing a Gröbner basis is doubly exponential in general, and exponential in our case of a finite set of solutions. In the second part of our lecture we compare the complexities of several methods. The complexity of our algorithm is exponential and the complexity coefficient is measured under the assumption that the over-determined system of quadratic equations is semi-regular using the results of Bardet et al. applied to algorithm F5 of Faugère. The complexity is compared to existing bounded distance decoding algorithms such as exhaustive search, syndrome decoding and covering set decoding. Our method can be extended to complete and generic decoding, and to finding the minimum distance and the complete weight distribution.

- **10:15-11:15- J.I. Farrán (Universidad de Valladolid): "Computing AG codes".**

  In this talk we analyze the main computational tasks for constructing codes coming from Algebraic Geometry, specially for codes from algebraic curves. We will also show the implementation of such codes in the computer algebra system SINGULAR.

- **11:45-12:45- S. Bulygin (University of Kaiserslautern): "Decoding linear codes with Groebner bases. Part II: Experimental results and comparison of methods".**

  In this talk we continue with the methods of decoding linear codes with the use of Groebner bases introduced in the talk of Ruud Pellikaan. We concentrate now on the computational side of the problem. In paricular, we present some experimental results that enable us to provide comparison between ours and the known methods. We elaborate on which role does the infromation rate and relative error-correcting capacity play in the complexity of proposed algorithms. Special cases of Hermitian and cyclic codes are considered.

- **16:00-17:00- J.P. Hansen (Aarhus Universitet): "Pairings on elliptic and hyperelliptic curves. Applications in cryptography. Effective calculation.".**

  This talk is a survey and a presentation of a new result on the effective calculations of all parings on the Jacobian of hyperelliptic curves. We also talk about some applications in cryptography.

- **17:30-18:30- J.M. Muñoz Porras (Universidad de Salamanca): "Applications of Algebraic Geometry to the theory of Convolutional Codes"**

  We will give an introduction to the theory of Convolutional Codes and some of the relevant problems of the theory. Then we will expose the construction of convolutional codes in terms of the geometry of uniparametric families of algebraic curves.

- **19:30- L. Huguet (Universitat de les Illes Balears): "Comercio electrónico, presente y futuro" (in Spanish).**
  Place: Salón de Actos del Palacio de Mansilla

  Introductory talk about "e-commerce, present and future".

Wednesday, October 10th 2007

- **09:10-10:10- M. Bras-Amorós (Universitat Rovira i Virgili): "On Numerical Semigroups and Their Applications to Algebraic Geometry Codes"**

  A numerical semigroup is a subset of $\mathbb{N}$ containing 0, closed under addition and with finite complement in $\mathbb{N}$. An important example of numerical semigroup is given by the Weierstrass semigroup at one point in a curve. In the theory of algebraic geometry codes, Weierstrass semigroups are crucial for defining bounds on the minimum distance as well as for defining improvements on the dimension of codes. Applications of numerical semigroups can also be found in cryptography, for instance when dealing with a wire-tap channel. We will talk about these applications as well as some theoretical problems related to classification, characterization and counting of numerical semigroups.

- **10:15-11:15- D. Ruano (University of Kaiserslautern): "Conway polynomials and Singular".**

  Conway polinomials are a particular class of irreducible polynomials, one for each finite field. They allow us to map easily objects between two finite fields, with equal characteristic, in a compatible way. We will see some applications to coding theory and as well as the computation of the gcd of two polynomials. Finally, we will introduce the algorithms for computing Conway polynomials and their implementation in the computer algebra system Singular.

- **11:45-12:45- C. Galindo (Universitat Jaume I) and F. Monserrat (Universidad de Valladolid): "δ-Sequences and Evaluation Codes defined by Plane Valuations at Infinity"**

  We introduce the concept of δ-sequence. A δ-sequence Δ generates a well-ordered semigroup S in $\mathbb{Z}^2$ or $\mathbb{R}$. We show how to construct (and compute parameters) for the dual code of any evaluation code associated with a weight function defined by Δ from the polynomial ring in two indeterminates to a semigroup S as above. We prove that this is a simple procedure which can be understood by considering a particular class of valuations of function fields of surfaces, called plane valuations at infinity. We also give algorithms to construct an unlimited number of δ-sequences of the different existing types and so, tools to know and use a new large set of codes are provided.