XXI CLA - Workshop S07
Finite Fields

S07 - July 28, 15:00 – 15:25

Castle curves and codes

Fernando Torres
IMECC/UNICAMP, Brasil
ftorres@ime.unicamp.br

Algebraic Geometry (AG) Codes were introduced by Goppa around 1980, and since then, there have been quantitative and qualitative advances in Coding Theory. The game is to find families of curves having a reasonable easy handling from which codes with excelent parameters could be construced. For instance, we single out the following type of curves. A nonsigular, projective, geometrically irreducible pointed curve $(\mathcal{X}, P)$ over the finite field $\mathbb{F}$ of order q is called *Castle* if $\#\mathcal{X}(\mathbb{F})$ attains the Lewittes bound, namely $1 + q\rho$, where ρ is the multiplicity of the Weierstrass semigroup $H(P)$ at P with $H(P)$ being symmetric. For instance, Deligne-Lusztig curves (Hermitian, Suzuki, Ree curves) are oustanding examples of such curves; as a matter of fact, many well-known examples of AG codes arise from Castle curves.

Moreover, Euclidian and Hermitian self-orthogonality properties on AG codes based on Castle curves are often easy to describe and handle; thus one can apply the CSS method in order to produce good quantum codes.

Joint work with Carlos Munuera (Universidad de Valladolid, España) and Wanderson Tenório (IMECC/UNICAMP, Brasil).

S07 - July 28, 15:30 – 15:55

The generalized Hamming weights of Castle codes

Wilson Olaya-León
Universidad Industrial de Santander, Colombia
wolaya@uis.edu.co

Castle codes are algebraic geometry one-point codes on Castle curves. This family contains some of the most important algebraic geometry codes among those studied in the literature to date. The generalized Hamming weights of these codes can be bounded by using the orden bound, whose main tools is the notion of well-behaving pairs. This bound is successful and usually gives very good results for the minimum distance (this bound gives the true minimum distance for Hermitian codes) but for weights higher dimension is difficult to compute.

In this talk will present a new way to get the exact value of certain Hamming weights of Castle codes. I will then introduce a notion of regular-behaving pairs and describe your properties in terms of the Weierstrass semigroup associated with the curve. In particular, I will show that for Hermitian codes these Hamming weights are all satisfying the generalized Singleton bound, i.e. are $t-$th rank MDS. Finally, I will propose a new lower bound for the minimum distance of Castle codes.

S07 - July 28, 16:00 – 16:25

On the second lowest Hamming weight of binary projetive Reed-Muller codes

Cicero Carvalho
Universidade Federal de Uberlandia, Brasil
cicero@ufu.br

Projective Reed-Muller codes were introduced by Lachaud, in 1988 and their dimension and minimum distance were determined by Serre and Sorensen in 1991. In coding theory one is also interested in the higher Hamming weights, to study the code performance. Yet, not many values of the higher Hamming weights are known for these codes, not even the second lowest weight (also known as next-to-minimal weight) is completely determined. In this talk we will present all the values of the next-to-minimal weight for the binary projective Reed-Muller codes, and we will also comment on their relation to the next-to-minimal weight of generalized (affine) Reed-Muller codes.

Joint work with Victor G.L. Neumann (Universidade Federal de Uberlandia).

S07 - July 28, 16:30 – 16:55

Some remarks on the asymptotic behavior of cyclic AG-codes

María Chara
Instituto de Matemática Aplicada del Litoral (UNL-CONICET), Argentina
mchara@santafe-conicet.gov.ar

It was proved in [St06] and [B06] that several classes of algebraic geometry codes, such as transitive codes, self-dual codes and quasi transitive codes among others, are asymptotically good over finite fields with square and cubic cardinality. Similar results were proved in [BBGS14] for general non-prime fields. In fact, some of them attain the well known Tsfasman-Vladut-Zink bound and also improvements for another well known bound of Gilbert-Varshamov were given. These results were achieved by considering algebraic geometry codes associated to asymptotically good towers of function fields over suitable finite fields.

Remarkably few things are known, so far, with regard to the asymptotic behavior of the class of cyclic codes. Perhaps the most interesting result in this direction is the one due to Castagnoli who proved in [Ca89] that the class of cyclic codes whose block lengths have prime factors belonging to a fixed finite set of prime numbers is asymptotically bad. This result implies that the construction of cyclic AG-codes in the standard way, would lead to a sequence of codes asymptotically bad.

In this talk we will discuss how different the situation is when dealing with the asymptotic behavior of transitive (or quasi transitive) AG-codes and cyclic AG-codes, which are particular cases of transitive AG-codes, [CPT16]. We will conclude that towers with only totally ramified places in the tower, which are nice candidates for good asymptotic behavior, have to be discarded for the construction of potentially good sequences of cyclic AG-codes, if we want to use all the techniques and results that were successful in the transitive case. All of this, together with Castagnoli's result, provide some good reasons to think that towers of function fields may not be adequate to address the problem of the asymptotic behavior of cyclic codes, as long as the sequence of cyclic AG-codes is constructed using automorphisms of the function fields in the tower. It is clear that the design of new methods to produce cyclic AG-codes is an interesting and challenging problem with potential consequences in the study of the asymptotic behavior of cyclic codes.

References

[B06] A. Bassa. Towers of function fields over cubic fields. Phd Thesis. Duisburg-Essen University. 2006.

[BBGS14] A. Bassa, P. Beelen, A. Garcia, and H. Stichtenoth. An improvement of the gilbert-varshamov bound over nonprime fields. IEEE Trans. Inform. Theory, 60(7):3859–3861, 2014.

[Ca89] G. Castagnoli. On the asymptotic badness of cyclic codes with block-lengths composed from a fixed set of prime factors. Applied algebra, algebraic algorithms and error-correcting codes. Lecture Notes in Comput. Sci., 357:164–168. Springer, Berlin, 1989.

[CPT16] M. Chara, R. Podestá and R. Toledano. Asymptotically good 4-quasi transitive algebraic geometry codes over prime fields. Submitted, arXiv:1603.03398.

[St06] H. Stichtenoth. Transitive and self-dual codes attaining the Tsfasman-Vladut-Zink bound. IEEE Trans. Inform. Theory, 52(5):2218–2224, 2006.

Joint work with Ricardo Podestá (Centro de Investigación y Estudios de la Matemática (UNC-CONICET), Argentina) and Ricardo Toledano (Facultad de Ingeniería Química (UNL), Argentina).

S07 - July 28, 17:30 – 17:55

Estimates for polynomial systems defining irreducible smooth complete intersections

Guillermo Matera
Universidad Nacional de General Sarmiento and CONICET, Argentina
gmatera@ungs.edu.ar

In this talk we shall consider algebraic varieties defined as the set of zeros of a "typical" sequence of multivariate polynomials over a finite field. We shall consider varios types of "nice" varieties: set-theoretic and ideal-theoretic complete intersections, absolutely irreducible one, and nonsingular ones. For these types, we shall present a nonzero "obstruction" polynomial of bounded degree in the coefficients of the sequence that vanishes if its variety is not of the type. This in particular yields bounds on the number of such sequences. Further, we shall show that most sequences (of at least two polynomials) define a degenerate variety, namely an absolutely irreducible nonsingular hypersurface in some linear projective subspace.

Joint work with Joachim von zur Gathen (B-IT, Universität Bonn, Germany).

S07 - July 28, 18:00 – 18:25

The distribution of points on families of curves over finite fields

Matilde Lalín
Université de Montréal, Canada
mlalin@dms.umontreal.ca

We give an overview of a general trend of results that say that the distribution of the number of $\mathbb{F}_q$-points of certain families of curves of genus g is asymptotically given by a sum of $q+1$ independent identically distributed random variables as g goes to infinity. In particular, we discuss the distribution of the number of $\mathbb{F}_q$-points for cyclic ℓ-covers of genus g. This work generalizes previous results in which only connected components of the moduli space were considered.

S07 - July 28, 18:30 – 18:55

Finite Field Constructions of Combinatorial Arrays

Lucia Moura
University of Ottawa, Canada
lucia@eecs.uottawa.ca

Finite fields play a fundamental role in the construction of combinatorial designs. In our article of the same title in Designs, Codes and Cryptography (2016), we survey constructions of combinatorial arrays using finite fields. These combinatorial objects include orthogonal arrays, covering arrays, ordered orthogonal arrays, permutation arrays, frequency permutation arrays, hypercubes and Costas arrays.

In this talk, I briefly discuss finite field constructions of various types of combinatorial arrays. Then, I focus on constructions of orthogonal arrays and related objects such as variable strength orthogonal arrays, ordered orthogonal arrays and covering arrays. An orthogonal array (and its variants) is an array with q^t rows and k columns on an alphabet with q symbols such that its projection into specific t-subsets of columns give subarrays where each t-tuple of the alphabet occurs once as one of its rows. The orthogonal array variants differ in which t-subsets of columns are required to have this "coverage property". A common theme on several of the recent constructions we discuss is the use of linear feedback shift register sequences of maximum period (m-sequences) to build arrays attaining a high number of t-subsets of columns with the "coverage property". The structure of coverage in the arrays built from intervals of length $(q^t-1)/(q-1)$ of these sequences reveal interesting relationships with finite geometry. I will mention different constructions I have worked on with André Castoldi, Sebastian Raaphorst, Daniel Panario, Brett Stevens and Georgios Tzanakis.

Joint work with Gary Mullen and Daniel Panario.

S07 - July 29, 15:00 – 15:25

Galois geometries and Random network coding

Leo Storme
Ghent University, Belgium
ls@cage.ugent.be

Presently, a new direction in coding theory, called Random network coding, receives a lot of attention.

In random network coding, information is transmitted through a network whose topology can vary. A classical example is a wireless network where users come and go.

R. Kotter and F. Kschischang proved in an inspiring article that a very good way of transmission is obtained in networks if subspace codes are used. Here, the codewords are k-dimensional vector subspaces of the n-dimensional vector space $V(n,q)$ over the finite field of order q.

To transmit a codeword, i.e. a k-dimensional vector space, through the network, it is sufficient to transmit a basis of this k-dimensional vector space. But a k-dimensional subspace has different bases. Kotter and Kschischang proved that the transmission can be optimalized if the nodes in the network transmit linear combinations of the incoming basis vectors of the k-dimensional subspace which represents the codeword.

These ideas led to many new interesting problems in coding theory and in Galois geometries. For instance, it leads to the study of sets C of k-dimensional subspaces of $V(n,q)$, where two different k-dimensional subspaces of C pairwise intersect in at most a t-dimensional subspace, for some specified parameter t.

Since the k-dimensional subspaces of $V(n,q)$ define $(k-1)$-dimensional projective subspaces of the projective space $\mathrm{PG}(n-1,q)$, this problem can also be investigated in a projective setting. Hence, Galois geometries can contribute to random network coding.

In this talk, we present a number of geometrical results on random network coding, thereby showing how Galois geometries can contribute to this new area in coding theory.

S07 - July 29, 15:30 – 15:55

Weierstrass semigroup and Automorphism group of the curves $X_{n,r}$

Guilherme Tizziotti
Universidade Federal de Uberlandia, Brasil
guilhermect@ufu.br

In this talk, we determine the Weierstrass semigroup $H(P_\infty)$ and the full automorphism group of a certain family of curves, denoted by $X_{n,r}$, which was recently introduced by H. Borges and R. Conceição.

Joint work with Herivelto Borges (Universidade de Sao Paulo) and Alonso Sepúlveda (Universidade Federal de Uberlandia).

S07 - July 29, 16:00 – 16:25

Asymptotically good 4-quasi transitive AG-codes over prime fields

Ricardo A. Podestá
Universidad Nacional de Córdoba, Argentina
podesta@famaf.unc.edu.ar

It is known, by works of Stichtenoth and Bassa, that several classes of algebraic geometry codes, such as transitive codes, self-dual codes and quasi transitive codes among others, are asymptotically good over finite fields with square and cubic cardinality. Similar results were proved by Bassa, Beelen, Garcia and Stichtenoth for general non-prime fields.

Remarkably, few things are known with respect to the behavior of families of AG-codes over prime fields with some additional structure besides linearity. We will show that there are asymptotically good 4-quasi transitive codes over prime fields $\mathbb{F}_p$ for infinte prime numbers of a given form (for instance of the form $p = 220k + 1$).

Joint work with María Chara (Universidad Nacional del Litoral) and Ricardo Toledano (Universidad Nacional del Litoral).

S07 - July 29, 16:30 – 16:55

A problem of Beelen, Garcia and Stichtenoth on an Artin-Schreier tower

Horacio Navarro
IMAL, Argentina
hnavarro@santafe-conicet.gov.ar

A *tower of function fields* over $\mathbb{F}_q$ is a sequence of algebraic function fields $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ such that for all $i \geq 0$ $F_i \subsetneq F_{i+1}$, F_{i+1}/F_i is a separable finite extension, $\mathbb{F}_q$ is algebraically closed in F_i and there exists F_j with genus greater than one.

A tower $\mathcal{F}$ is called *asymptotically good* if $\gamma(\mathcal{F}) < \infty$ and $\nu(\mathcal{F}) > 0$ where

$$\gamma(\mathcal{F}) := \lim_{i\to\infty} g(F_i)/[F_i : F_0] \quad \text{and} \quad \nu(\mathcal{F}) := \lim_{i\to\infty} N(F_i)/[F_i : F_0],$$

$g(F_i)$ is the genus of F_i and $N(F_i)$ is the number of rational places of F_i. Otherwise, $\mathcal{F}$ is called *asymptotically bad*.

In 2006 Beleen, Garcia and Stichtenoth proved that any recursive tower of function fields over $\mathbb{F}_2$ defined by $g(Y) = f(X)$ with $g(T), f(T) \in \mathbb{F}_2(T)$ and $\deg f = \deg g = 2$ is defined by the Artin-Schreier equation

$$Y^2 + Y = \frac{1}{(1/X)^2 + (1/X) + b} + c, \tag{1}$$

with $b, c \in \mathbb{F}_2$. They checked that all the posible cases were already considered in previous works, except when $b = c = 1$. In fact, they left as an open problem to determine whether or not this tower is asymptotically good over $\mathbb{F}_{2^s}$ for some positive integer s.

In this talk we will show that the recursive tower defined by equation (1) with $b = c = 1$ is asymptotically bad over $\mathbb{F}_{2^s}$ when s is odd and where the main difficulty arises in the study of this tower when s is even.

Joint work with Ricardo Toledano (Universidad Nacional del Litoral-IMAL) and María Chara (Universidad Nacional del Litoral-IMAL).

S07 - July 29, 17:30 – 17:55

Arithmetic Mirror Symmetry of K3 Surfaces and Hypergeometric Functions.

Adriana Salerno
Bates College, USA
asalerno@bates.edu

Mirror symmetry predicts surprising geometric correspondences between distinct families of algebraic varieties. In some cases, these correspondences have arithmetic consequences. Among the arithmetic correspondences predicted by mirror symmetry are correspondences between point counts over finite fields. In particular, we explore closed formulas for the point counts for our alternate mirror families of K3 surfaces, their relation to their Picard-Fuchs equations and hypergeometric functions.

Joint work with Charles Doran (University of Alberta, Canada), Tyler Kelly (University of Cambridge, UK), Steven Sperber (University of Minnesota, USA), John Voight (Dartmouth College, USA) and Ursula Whitcher (University of Wisconsin, Eau Claire, USA).

S07 - July 29, 18:00 – 18:25

Estimates on the average cardinality of the value set of general families of univariate polynomials over a finite field

Melina Privitelli
Instituto de Ciencias, UNGS, Argentina
mprivite@ungs.edu.ar

The aim of this work is to estimate the average cardinality of the value set of a general family of monic univariate polynomials with coefficients in a finite field. This is a classical combinatorial problem with several applications in coding theory, interpolation problems and the analysis of the cost of algorithms for computing $\mathbb{F}_q$-rational zeros of multivariate polynomials with coefficients in a finite field, among others.

Let $\mathbb{F}_q$ be the finite field of $q = p^k$ elements and let $\mathcal{P}_d$ be the set of monic polynomials of degree d with coefficients in $\mathbb{F}_q$. For $f \in \mathcal{P}_d$ we denote by $\mathcal{V}(f) := |\{f(c) : c \in \mathbb{F}_q\}|$ the cardinality of the value set of f. Let $\mathcal{A} \subset \mathcal{P}_d$ be a general family, namely the set of elements of $\mathcal{P}_d$ whose coefficients belong to an $\mathbb{F}_q$–algebraic variety. S. D. Cohen studied the particular case when $\mathcal{A}$ is a linear family and proved that if $p > d$ and $\mathcal{A}$ satisfies certain technical conditions, the average cardinality $\mathcal{V}(\mathcal{A})$ of the value set in $\mathcal{A}$ is

$$\mathcal{V}(\mathcal{A}) = \mu_d q + \mathcal{O}(q^{1/2}),$$

where $\mu_d := \sum_{j=1}^{d} (-1)^{j-1}/j!$.

In our work we significantly generalize this result to rather general (eventually nonlinear) families $\mathcal{A} \subset \mathcal{P}_d$. We establish conditions on $\mathcal{A}$ which allow us to obtain an explicit version of this estimate. Our result provides an expression for the constant underlying the $\mathcal{O}$-notation in terms of d. We obtain a combinatorial expression for $\mathcal{V}(\mathcal{A})$ in terms of certain "interpolating sets" $\mathcal{S}_r^{\mathcal{A}}$ $(1 \leq r \leq d)$ and we associate to each $\mathcal{S}_r^{\mathcal{A}}$ an $\mathbb{F}_q$–algebraic variety Γ_r. We reduce the question to estimate the number of $\mathbb{F}_q$–rational points of Γ_r. We also exhibit linear and non linear families of polynomials which satisfy our requirements. In the particular case of linear families we improve the estimate given by Cohen in several aspects.

Joint work with Guillermo Matera (Instituto del Desarrollo Humano, UNGS, Argentina) and Mariana Pérez (Instituto del Desarrollo Humano, UNGS, Argentina).

S07 - July 29, 18:30 – 18:55

Iterating Redei Functions over Finite Fields

Daniel Panario
Carleton University, Canada
daniel@math.carleton.ca

The dynamics of iterations of polynomials and rational functions over finite fields have attracted much attention in recent years, in part due to their applications in cryptography and integer factorization methods like Pollard rho algorithm. In this talk we study the action of Redei functions over non-binary finite fields. Redei functions have been applied in several areas including pseudorandom number generators and cryptography. They are defined as $R_n(x,a) = \frac{N(x,a)}{D(x,a)}$ over $\mathbb{D}_q^a = \mathbb{P}^1(\mathbb{F}_q) \setminus \{\pm\sqrt{a}\}$, where $\mathbb{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$, $a \in \mathbb{F}_q$, and $N(x,y), D(x,y)$ are given by $(x + \sqrt{y})^n = N(x,y) + D(x,y)\sqrt{y}$. We completely characterize the functional graph of these actions.

For $x_0 \in \mathbb{F}_q$, we define the orbit of x_0 under f to be the sequence $(x_n)_n$ given by $x_n = f(x_{n-1})$, for $n \geq 1$. It is clear that there exists $c, t \geq 0$ such that $x_{c+t} = x_t$; the least such integers are the cycle length and the tail length of x_0, denoted by $c_q(x_0)$ and $t_q(x_0)$, respectively. We obtain average values for $c_q(x) = c_{n,a,q}(x)$ and $t_q(x) = t_{n,a,q}(x)$ over all $x \in \mathbb{D}_q^a$; we denote these quantities by $C(n,a,q)$ and $T(n,a,q)$. We then obtain analogous results for the number of periodic points, that is, for the number of elements $x \in \mathbb{D}_q^a$ such that $t_{n,a,q}(x) = 0$, denoted by $T_0(n,a,q)$, and for the number of cycles of $R_n(x,a)$ as a map over $\mathbb{P}^1(\mathbb{F}_q)$; this is denoted by $N(n,a,p)$.

If time allows, we give asymptotic estimates as N approaches infinity for the average value of $T_0(n,a,p)$ and $T(n,a,p)$ over all prime numbers $p \leq N$; these quantities are denoted $S_0(n,a,N)$ and $S(n,a,N)$, respectively. These latter results follow closely work by Chou and Shparlinski (2004) for iterations of exponentiations.

Joint work with Claudio Qureshi (Unicamp), and with Rodrigo Martins (UTFPR) and Claudio Qureshi (Unicamp).

S07 - Poster

On the Densest Lattices from Number Fields and Division Algebras

Carina Alves
São Paulo State Universtiy - UNESP - Rio Claro, Brasil
carina@rc.unesp.br

Algebraic lattices are lattices obtained via the ring of integers, $\mathcal{O}_{\mathbb{F}}$, of a number field $\mathbb{F}$. They can be constructed considering geometric representations of integral ideals in $\mathcal{O}_{\mathbb{F}}$. This latter method was successfully used by Craig to construct the Leech lattice from a properly chosen integral ideal $\mathcal{I}$ in $\mathbb{Z}[\zeta_{39}]$, the ring of integers of the cyclotomic field $\mathbb{F} = \mathbb{Q}(\zeta_{39})$. In addition to the Leech lattice, Craig showed that the lattices D_4, E_8, K_{12}, and Λ_{16} can all be obtained from properly chosen integral ideals in rings of cyclotomic integers. Bayer-Fluckiger showed that E_8 can be obtained via a ideal $\mathcal{I}$ in $\mathcal{O}_{\mathbb{F}}$, $\mathbb{F} = \mathbb{Q}(\zeta_{15})$, $\mathbb{Q}(\zeta_{20})$, $\mathbb{Q}(\zeta_{24})$. Versions of dense lattices are of interest from the practical viewpoint as they are suitable for data transmission. More recently, the need for higher data transmission has led to consider communication channels using multiple antennas at both transmitter and receiver ends (MIMO). In the case of space-time codes, it is natural to consider a lattice from an ideal of a maximal order of the division algebra. Codewords are usually (in narrow band systems) built over the complex field. However for ultra wideband communication, one needs to design them over the real field. Thus, having the construction of lattices as our goal, in this work we present constructions of dense lattices from maximal orders of the division algebras over a totally real number field.

Joint work with Sueli I.R. Costa (Institute of Mathematics, University of Campinas, Campinas-SP, Brazil, sueli@ime.unicamp.br). and Cintya W. O. Benedito (Institute of Mathematics, University of Campinas, Campinas-SP, Brazil, cwinktc@hotmail.com).

S07 - Poster

New constructions of algebraic lattices

Antonio Aparecido de Andrade
São Paulo State University at São José do Rio Preto, Brasil
andrade@ibilce.unesp.br

In algebraic number theory, it is better known the ring of integers of the cyclotomic field and the ring of integers of their maximal real subfield. An important result of this area, the Kronecker-Weber Theorem, states that every abelian number field is contained in a cyclotomic field. Thinking about this, we can ask ourselves what is the ring of integers of each abelian number field and if this ring of integers has a power basis, this is, if the ring of integers is generated by an element over Z. In this line, to construct lattices in odd dimensions, we can not use cyclotomic fields, but we can use their subfields. Also, the maximal real cyclotomic subfields are not suficient to solve the problem of find algebraic lattices that has better center density. Trying to solve this problem mainly in odd dimensions, we are using abelian number fields. For this task we need the ring of integers of abelian number fields, which is presented by the Leopoldt's Theorem (1959) or its version given by Lettl (1990). In this work, we intend to present the Leopoldt's Theorem in the version of Lettl and elucidate why it can be useful to construct algebraic lattices with better center desnsity.

References.

1. Leopoldt, H.-W. Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. reine angew. Math. 201 (1959), 119-149.

2. Lettl, Günter. The ring of integers of an abelian number field, J. reine angew. Math. 404 (1990), 162-170.

3. Shah, S.I.A., Nakahara, T. Monogenesis of the rings of integers in certain imaginary abelian fields, Nagoya Math. J. Vol. 168 (2002), 85-92.

4. Ribenboim, P. Classical Theory of Algebraic Numbers, Springer Verlag, New York, 2001.

5. Laurent, W. Introduction to cyclotomic fields, Springer Verlag, New York, 1982.

Joint work with Robson Ricardo de Araujo. Department of Mathematics, State University of Campinas, Campinas - SP, Brasil.

S07 - Poster

Gröbner bases for Generalized Hermitian codes.

Federico Fornasiero
UFPE (universidade federal do Pernambuco), Brasile
federico@dmat.ufpe.br

In recent years the theory of Gröbner bases have been largely applied to solve problems in Code Theory. In particular, in 1995 Heegard, Little and Saints found an efficient and interesting decoding method using Gröbner bases, but it has a very high computational cost.
Little, Heegard and Saints found a method to reduce the computational cost and they applied to the Hermitian curve, and then it was applied the same method to the Norm-Trace curve by Farran, Sepulveda, Tizziotti, Torres.
In this talk I want to show how it is possible to extend these results to the curve $x^{q^r+1} = y^q + y$ over the finite field $\mathbb{F}_{q^{2r}}$ (studied by Kondo, Katagiri and Ogihara) and to the curve $x^m = y^q + y$, with $m|q+1$, over the finite field $\mathbb{F}_{q^2}$ (studied by Matthews), determining the so-called Root-Diagram of a curve.

Joint work with This work was supervised by G.Tizziotti and F.Torres.

S07 - Poster

Similarity between the algebraic structure associated with projective space and combinatorial design via Hasse diagram

Leandro Bezzerra de Lima
CPAq/UFMS - FEEC/UNICAMP, Brasil
leandro.lima@ufms.br

Combinatorial design is an important combinatorial structure having a high degree of regularity and which is related to the existence and construction of systems of sets with finite cardinality, [1]. As examples we mention the existing relationship between error-correcting codes in the Hamming space and combinatorial design, where the codewords of weight 3 of the Hamming code form a triple Steiner system STS(7), a projective plane of order 2, known as the Fano plane, [2], as well as q-analogs of a code whose

codewords have constant Hamming weight in the Hamming space, a code belonging to a Grassmannian in the projective space, [3,4]. Projective space of order m over a finite field $\mathbb{F}_p$, denoted by $\mathcal{P}(\mathbb{F}_p^m)$, (note that $\mathbb{F}_{p^m}$ is isomorphic to $\mathbb{F}_p^m$), is the set of all the subspaces in the vector space $\mathbb{F}_p^m$. The projective space endowed with the subspace distance $d(X,Y) = dim(X) + dim(Y) - 2dim(X \cap Y)$ is a metric space. Hence, the subspace code $\mathcal{C}$ with parameters (n, M, d) in the projective space is a subset of $\mathcal{P}(\mathbb{F}_p^m)$ with cardinality M with a subspace distance at least d between any two codewords, [5]. In this paper we show the existing similarity between the Hasse diagram of an Abelian group consisting of the product of multiplicative finite Abelian groups $\mathbb{Z}_p^m$ and the Hasse diagram of the projective space $\mathcal{P}(\mathbb{F}_p^m)$, with the aim to provide the elements that may be useful in the identification and in the construction of good subspaces codes, [6].

[1] - D.R. Stinson, *Combinatorial Designs: Constructions and Analysis*, Springer Verlag, New York, USA, 2004.

[2]-T.Etzion and N. Silberstein, "Error-Correcting codes in projective spaces via rank metric codes and Ferrers diagrams," *IEEE Trans. Inform. Theory*, vol. 55, n.º7, pp.2909-2919, Jul. 2009.

[3]-M.Braun, T. Etzion, P.R.J. Ostergard, A. Vardy, and A. Warssermann, "Existence of q-analogs of Steiner sstems," arxiv.org/abs/1304.1462, Apr. 2013.

[4]-T. Etzion and A. Vardy, "Error-Correcting codes in projective space," *IEEE Intl. Symp. on Inform. Theory - ISIT-08*, pp. 871-875, Toronto, Canada, Jul. 2008.

[5]-A. Khaleghi, D. Silva, and F.R. Kschischang, "Subspace codes," *Lecture Notes in Computer Science*, vol. 5921, pp. 1-21, 2009.

[6]-C.H.A. Costa e M. Guerreiro, "Automorphisms of finite Abelian groups,", MS thesis, Mathematics Dept, UFV, Viçosa, Minas Gerais, 2014. (in Portuguese)

Joint work with Reginaldo Palazzo Jr. (FEEC/UNICAMP) e-mail: palazzo@dt.fee.unicamp.br.

S07 - Poster

Projective Nested Cartesian Codes

Victor Gonzalo Lopez Neumann
Universidade Federal de Uberlândia, Brasil
victor.neumann@ufu.br

In this work we introduce a new type of code, called projective nested cartesian code. It is obtained by the evaluation of homogeneous polynomials of a fixed degree on the set

$$[A_0 \times A_1 \times \cdots \times A_n] := \{(a_0 : \cdots : a_n) | \, a_i \in A_i \text{ for all } i\} \subset \mathbb{P}^n(\mathbb{F}_q),$$

where $A_0, A_1, \ldots, A_n$ is a collection of non-empty subsets of $\mathbb{F}_q$ such that for all $i = 0, \ldots, n$ we have $0 \in A_i$, and for every $i = 1, \ldots, n$ we have $A_j A_{i-1} \subset A_j$ for $j = i, \ldots, n$. These codes may be seen as a generalization of the so-called projective Reed-Muller codes. We calculate the length and the dimension of such codes, a lower bound for the minimum distance and the exact minimum distance in the special case where the sets A_i are subfields of $\mathbb{F}_q$ (so it includes the projective Reed-Muller codes).

Joint work with Cícero Carvalho (Universidade Federal de Uberlândia, Brasil) and Hiram López (Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, México).
