International Conference
on
Algebraic Geometry and Coding Theory
IIT Bombay, Mumbai, India, December 2-6, 2013

Titles and Abstracts of Talks

(in alphabetical order of the names of speakers)

Title: *On three-valued Weil sums*

Speaker: Yves Aubry

Abstract: Let K be a finite field of characteristic p and order q. Let ψ_K be the canonical additive character of K, that is, $\psi_K(x) = \exp(2i\pi \mathrm{Tr}_{K/\mathbb{F}_p}(x)/p)$ where $\mathrm{Tr}_{K/\mathbb{F}_p}(x)$ is the absolute trace. We are considering character sums of the form

$$W_{K,d}(a) = W_d(a) = \sum_{x \in K} \psi_K(x^d + ax)$$

with $\gcd(d, q-1) = 1$ and $a \in K$.

We are interested to know when Weil sums of this form can be three-valued, and if so, what are the three values they may take.

We prove that if $[K : \mathbb{F}_p]$ is a power of 2 then the set of values assumed by $W_{K,d}(a)$ as a runs through $K^\times$ is not of the form $\{-A, 0, +A\}$ for any A. This generalizes a result of Calderbank-McGuire-Poonen-Rubinstein.

Moreover, we prove that if $[K : \mathbb{F}_p] \equiv 0 (\mathrm{mod}\ 4)$, then the set of values assumed by $W_{K,d}$ as a runs through $K^\times$ is not of the form $\{0, \pm p\sqrt{q}\}$. This generalizes Calderbank-McGuire's proof of Sarwate's Conjecture.

Finally, we prove that if $[K : \mathbb{F}_p]$ is even and if d is a power of p modulo $\sqrt{|K|} - 1$, then $W_{K,d}$ is not three-valued. This generalizes a result of Charpin.

This is a joint work with Daniel Katz and Philippe Langevin

Title: *Rational points on curves over finite fields and Drinfeld modular varieties*

Speaker: Alp Bassa

Abstract: In the past modular curves of various type (classical, Drinfeld, Shimura) have been used successfully to construct high genus curves with many rational points over finite fields of square cardinality. In this talk I will explain how Drinfeld modular varieties can be used similarly to obtain high genus curves with many rational points over any non-prime finite field. This way we obtain lower bounds for the Ihara constant $A(q)$ for all non-prime q, which are better then all previously known bounds.

This is joint work with Beelen, Garcia, Stichtenoth.

Title: *On Polar Grassmann Codes*

Speaker: Ilaria Cardinali

Abstract: Let $V := V(2n+1, q)$ be a $(2n+1)$-dimensional vector space defined over a finite field $\mathbb{F}_q$ equipped with a non-singular quadratic form η. Let $\mathcal{G}_k$ be the k-Grassmannian of $PG(V)$ and Δ_k the k-polar Grassmannian of $PG(V)$ with respect to η $(1 \leq k \leq n)$.

The geometries $\mathcal{G}_k$ and Δ_k are respectively naturally embedded in the projective spaces $PG(W_k)$ and $PG(V_k)$, where $W_k = \bigwedge^k V$, $\dim(W_k) = \binom{2n+1}{k}$, and $V_k \subseteq W_k$ with $dim(V_k) = \binom{2n+1}{k}$ for $char(\mathbb{F}_q) \neq 2$ and $\dim(V_k) = \binom{2n+1}{k} - \binom{2n+1}{k-2}$ for $\mathrm{char}(\mathbb{F}_q) = 2$ ([2], [3]).

The linear codes associated to $\mathcal{G}_k$ are called *Grassmann codes* and have been widely studied in the literature. In this talk, we shall consider the linear codes associated to the polar Grassmannian Δ_k, hence called *polar Grassmann codes* ([1]). We will describe some properties of polar Grassmann codes, focusing our attention on their minimal distance and on the geometric approach to compute it. In the last part of the talk, some open problems will be discussed.

[1] I. Cardinali and L. Giuzzi *Codes and caps from orthogonal Grassmannians.* Finite Fields Appl. 24 (2013), 148–169.

[2] I. Cardinali and A. Pasini, *Grassmann and Weyl Embeddings of Orthogonal Grassmannians*, J. Algebraic Combin. 38 (2013), no. 4, 863–888.

[3] I. Cardinali and A. Pasini, *Veronesean embeddings of dual polar spaces of orthogonal type.* J. Combin. Theory Ser. A 120 (2013), no. 6, 1328–1350.

Title: *Affine variety codes are better than their reputation.*

Speaker: Olav Geil

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, a?ffine variety codes can be very good, also in the cases where they are not one-point algebraic geometric codes in disguise.

Title: *Osculating Spaces of Varieties, Forms and Linear Network Codes*

Speaker: Johan P. Hansen

Abstract: We present a general theory to obtain good linear network codes utilizing the osculating nature of algebraic varieties. In particular, we obtain from

the osculating spaces of Veronese varieties explicit families of equidimensional vector spaces, in which any pair of distinct vector spaces intersect in the same dimension.

Linear network coding transmits information in terms of a basis of a vector space and the information is received as a basis of a possible altered vector space. Ralf Koetter and Frank R. Kschischang introduced a metric on the set of vector spaces and showed that a minimal distance decoder for this metric achieves correct decoding if the dimension of the intersection of the transmitted and received vector space is sufficiently large.

The proposed osculating spaces of Veronese varieties are equidistant in the above metric. The parameters of the resulting linear network codes are determined.

The construction from Veronese varieties is generalized using forms.

Title: *Graph Codes with Reed-Solomon Component Codes*

Speaker: Tom Høholdt

Abstract: We study codes constructed from Reed-Solomon codes and bipartite graphs coming from projective and Euclidean planes. The code symbols are associated with the edges of the graph and symbols connected to a given vertex are restricted to be codewords in the component Reed-Solomon code. We give results on the dimension and minimum distance of the resulting codes.

This is a joint work with J. Justesen and F. Pinero.

Title: *Numbers of points of surfaces in $\mathbb{P}^3$ over $\mathbb{F}_q$.*

Speaker: Masaaki Homma

Abstract: Let S be a surface of degree d in $\mathbb{P}^3$ over $\mathbb{F}_q$ without $\mathbb{F}_q$-plane components, and $N_q(S)$ the number of $\mathbb{F}_q$-points of S.

Recently we established the following theorem.

Theorem 1. *$N_q(S) \leq (d-1)q^2 + dq + 1$, and equality holds if and only if S is projectively equivalent over $\mathbb{F}_q$ to a surface in the following list:*

(i) $X_0X_1 - X_2X_3 = 0$;
(ii) $X_0^{\sqrt{q}+1} + X_1^{\sqrt{q}+1} + X_2^{\sqrt{q}+1} + X_3^{\sqrt{q}+1} = 0$;
(iii) $X_0X_1^q - X_0^qX_1 + X_2X_3^q - X_2^qX_3 = 0$.

I am going to explain some parts of this theorem.

This is a joint work with Seon Jeong Kim.

Title: *Further Results On Exceptional APN Functions*

Speaker: Heeralal Janwa

Abstract: An almost perfect nonlinear (APN) function (necessarily a polynomial function) on a finite field $\mathbb{F}$ is called exceptional APN, if it is also APN on infinitely

many extensions of $\mathbb{F}$. APN functions have many applications in cryptography, coding theory, combinatorics, and finite geometry. In this talk we consider the most studied case of $\mathbb{F} = \mathbb{F}_{2^n}$. A conjecture of Janwa-Wilson and McGuire-Janwa-Wilson (1993/1996) settled in 2011 (Hernando and McGuire) was that the only monomial exceptional APN functions are the monomials x^n, where $n = 2^i + 1$ or $n = 2^{2i} - 2^i + 1$ (the Gold or the Kasami exponents, respectively). A subsequent conjecture by Aubry, McGuire and Rodier states that any exceptional APN function is one of the monomials just described. Several authors obtained partial results. For example, we established that all functions of the form $f(x) = x^{2^k+1} + h(x)$ (for any odd degree $h(x)$, with a mild condition in few cases), are not exceptional APN, extending, to a significant extent, several earlier results towards the resolution of the stated conjecture.

In this talk we will present substantial extensions of these results. One of our results is that most Kasami-Welch degree polynomials of the form $x^{2^{2k}-2^k+1}+h(x)$, where $\deg(h) \equiv 3 \pmod 4$, can not be exceptional APN. In the proofs, we will establish that large classes of hypersurfaces are absolutely irreducible. Our results then follow from the bounds of Lang-Weil, Deligne, and Ghorpade-Lachaud (methods introduced by Janwa-Wilson, Janwa-Wilson-McGuire, and Rodier). These results are of independent interest for algebraic geometric codes.

This is a joint work with Moises Delgado.

Title: *Linear codes and Stanley-Reisner rings associated to matroids*

Speaker: Trygve Johnsen

Abstract: We study properties of linear codes, in particular some algebraic-geometric codes, by studying algebraic and topological properties of the simplicial complexes corresponding to one or more matroids derived from each code. In particular we study various Betti numbers of Stanley-Reisner rings associated to the simplicial complexes. We show how the higher weight hierarchy and other properties of the codes in question can be read off from some of these Betti numbers.

Title: *Generalizations of nonbinary Reed-Muller codes via construction sum of tensor product codes*

Speaker: Grigory Kabatiansky

Abstract: In this talk we will investigate one rather old code construction, which looks very natural from algebraic point of view, and therefore (probably) it was many times rediscovered after the initial Gore's paper, 1973 (the speaker, for instance, did it in 1975).

Consider families of nested linear codes (i.e., linear subspaces)

$$V_{i,1} \subset V_{i,2} \subset \cdots \subset V_{i,s_i} \subseteq \mathbb{F}_q^{n_i} \quad \text{for } i = 1, \ldots, m,$$

and the corresponding tensor product codes

$$\mathbb{V}_{\mathbf{j}} := V_{1,j_1} \otimes V_{2,j_2} \otimes \cdots \otimes V_{m,j_m}$$

of length $n = n_1 \times \cdots \times n_m$, where $\mathbf{j} = (j_1, \ldots, j_m)$. It is obvious and well-known that the minimal Hamming distance (shortly - distance) of the tensor product of codes is equal to the product of their distances, i.e.,

$$d(\mathbb{V}_{\mathbf{j}}) = d(V_{1,j_1}) \otimes \cdots \otimes d(V_{m,j_m}).$$

Surprisingly and it was discovered by Gore, that the minimal Hamming distance of a sum of tensor product codes equals to the minimum of distances of the tensor product code included in that vector subspaces sum, namely,

$$d\left(\sum_{\mathbf{j}\in\mathbf{J}} \mathbb{V}_{\mathbf{j}}\right) = \min_{\mathbf{j}\in\mathbf{J}} d(\mathbb{V}_{\mathbf{j}}).$$

This fact gives, for instance, a natural explanation why Massey, Costello, Justesen codes ("Polynomial weights and code constructions", 1973) should be considered as one more generalization of Reed-Muller codes to nonbinary case. We will discuss how to decode codes, produced by this sum-product construction, including correction of non-standard errors, and relations of this construction with some AG-codes.

Title: *Asymptotic formulae for the number of MDS codes/arcs in Galois geometries*

Speaker: Krishna V, Kaipa

Abstract: The problem of determining exact formulae for the number of q-ary MDS codes of dimension k and length n, is hard and complicated. Exact formulae are known only for $k = 3$, $n < 10$ and $k = 2$, all n. In this talk we present some new asymptotic formulae in q for the number of $[n, k]$ q-ary MDS codes. We obtain these formulae by proving some new results on cardinalities of linear sections of the Grassmann variety over finite fields.

Title: *Jacobi sums and MDS Codes*

Speaker: S. A. Katre

Abstract: There are a number of examples of MDS codes in the literature such as Reed-Soloman codes. In this talk we propose a new method to construct MDS codes using Jacobi sums. The method uses arithmetic characterisation of Jacobi sums of prime order l and we have shown jointly with other co-workers that for $l \leq 19$, for almost all primes $p \equiv 1 \pmod{l}$, we get an MDS $[(l-1, (l-1)/2, (l+1)/2]$-code over $\mathbb{F}_p$. Conjecturally, in this way MDS codes can be obtained for all primes l.

Title: *Asymptotic distribution of the number of points of curves over finite fields*

Speaker: Gilles Lachaud

Abstract: We study the mean value of the number of points of curves over finite fields. Given a random curve of genus g over a finite field, the limit distribution of the normalized Weil polynomial is analogous to the distribution of a random unitary symplectic matrix of order $2g$, with the density defined by the Haar measure. This is linked to the Sato-Tate conjecture, and is based on the results of Katz-Sarnak for universal families of curves. In the case of genus 2, we provide an explicit formula for the asymptotic distribution, the characteristic function and the repartition function, in terms of special functions, namely Legendre and Meijer functions.

Title: *Uniqueness of $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q^2$ and existence of non-extendable $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^4}$ to $\mathbb{F}_q^3$*

Speaker: Ferruh Özbudak

Abstract: Let q be a power of an odd prime. We prove that all $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q^2$ are equivalent. We also give a geometric method to find the corresponding equivalence explicitly [**?**].

The results above imply that any $\mathbb{F}_q$-quadratic perfect nonlinear map from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q^2$ is obtained by restriction of an $\mathbb{F}_q$-quadratic perfect nonlinear map from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q^3$. We also show that there exist $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^4}$ to $\mathbb{F}_q^3$ which cannot be obtained by restriction of any $\mathbb{F}_q$-quadratic perfect nonlinear map from $\mathbb{F}_{q^4}$ to $\mathbb{F}_q^4$. We call such maps *non-extendable* $\mathbb{F}_q$-quadratic perfect nonlinear maps from $\mathbb{F}_{q^4}$ to $\mathbb{F}_q^3$.

Title: *Higher weights of some special Grassmann codes*

Speaker: Arunkumar R. Patil

Abstract: The r-th higher weight of a $[n,k]_q$-linear code is defined as the minimum among the support weights of the r-dimensional subcodes of the given code. The collection of all the higher weights $\{d_r : 1 \leq r \leq k\}$ where k is the dimension of the code, is called the weight hierarchy of the code. The higher weights d_r and d_{k-r} of the $[n,k]_q$- (linear) Grassmann code $C(\ell,m)$ associated with a Grassmannian $G(\ell,m)$ over the finite field $\mathbb{F}_q$ are known for $0 \leq r \leq \mu$, where $\mu = \max\{\ell, m-\ell\}+1$ ([5], [1], [3]) . This is a very small portion of the complete weight hierrachy of these codes. In this talk, we shall demonstrate a method, first outlined in [6], of determining the complete weight hierarchy of some special Grassmann codes, namely, the linear codes associated to $G(2,m)$.

This is a joint work with Sudhir Ghorpade and Harish Pillai.

References

[1] S. R. Ghorpade and G. Lachaud, *Higher weights of Grassmann codes*, Coding Theory, Cryptography and Related Areas (Guanajuato, Mexico, 1998), pp. 122–131, Springer-Verlag, Berlin/Heidelberg, 2000.

[2] S. R. Ghorpade and M. A. Tsfasman, *Schubert varieties, linear codes and enumerative combinatorics*, Finite Fields Appl. **11** (2005), 684–699.

[3] J. P. Hansen, T. Johnsen and K. Ranestad, *Schubert unions in Grassmann varieties*, Finite Fields Appl., **13**, 738-750 (2007).

[4] S. R. Ghorpade, A. R. Patil, H.K. Pillai, *Decomposable subspaces, linear sections of Grassmann varieties, and higher weights of Grassmann codes*, Finite Fields Appl., **15**, 54-68 (2009).

[5] D. Yu. Nogin, *Codes associated to Grassmannians*, Arithmetic, Geometry and Coding Theory (Luminy, 1993), Walter de Gruyter, Berlin/New York, 1996, **pp. 145154**.

[6] A. R. Patil, *Weight hierarchy and generalized spectrum of linear codes associated to Grassmann varieties*, Ph.D. thesis, Indian Institute of Technology Bombay (2008).

Title: *Multisequences, their extensions and applications*

Speaker: Harish K. Pillai

Abstract: Multisequences are vector sequences over a finite field. Periodic multisequences can be associated with certain linear relations. We introduce and explore the concept of an extension of a multisequence. The power of this concept of extensions would then be demonstrated with some examples.

Title: *On linear codes from the Grassmannian and affine Grassmaniannn*

Speaker: Fernando Pinero

Abstract: In this work we present results on the structure of Grassmaniann and Affine Grassmaniann codes. First we determine the minimum weight codewords of the dual codes. This implies that we can give an iterative definition of the linear codes which reflects the recursive nature of the Grassmannian and Affine Grassmannian. Using a Tanner code description of the Affine Grassmaniann Linear Codes we may be able to decode with the bit-flipping algorithm.

Title: *Ovoids in $PG(3, q)$, q even, and related algebraic codes*

Speaker: N.S. Narasimha Sastry

Abstract: We discuss ovoids in $PG(3, q)$, q even, and in the generalized quadrangle $W(q)$ associated with the symplectic group $PSP(4, q)$ and its relation to the binary code $\mathcal{C}$ associated with $W(q)$. We also offer a nondegenerate bilinear form and a polarity on $\mathcal{C}$ when $W(q)$ admits a polarity (equivalently, q an odd power of 2).

Title: *Schubert decomposition for double Grassmannians*

Speaker: Evgeny Smirnov

Abstract: Classical Schubert calculus deals with orbits of a Borel subgroup in $\mathrm{GL}(V)$ acting on a Grassmann variety $\mathrm{Gr}(k, V)$ of k-planes in a finite-dimensional vector space V. These orbits (Schubert cells) and their closures (Schubert varieties) are very well studied both from the combinatorial and the geometric points of view.

One can go one step farther, considering the direct product of two Grassmannians $\mathrm{Gr}(k, V) \times \mathrm{Gr}(l, V)$ and the Borel subgroup in $\mathrm{GL}(V)$ acting diagonally on this variety. In this case, the number of orbits still remains finite, but the combinatorics and geometry of their closures become much more involved. It would be challenging to extend the whole body of Schubert calculus to this situation.

In this talk, I will explain how to index the closures of a Borel subgroup in $\mathrm{Gr}(k, V) \times \mathrm{Gr}(l, V)$ combinatorially, describe the inclusion relations between them, and construct their desingularizations, which are analogous to Bott-Samelson desingularizations for ordinary Schubert varieties. If time allows, I will also try to discuss the relations of this situation with geometry of quiver representations; these relations were recently found by Bobinski and Zwara.

Title: *Points on surfaces*

Speaker: Michael A. Tsfasman

Abstract: Many people work on and quite a lot is known about points on curves over a finite field. Only few papers treat points on surfaces and higher dimensional varieties. I would like to recall some old results to attract attention to the problem.
