Symposium on Algebra and Coding Theory

organised by

Sudhir R. Ghorpade, IIT Bombay

at the

Indian Science Congress, Tirupati, January 3-7, 2017

List of Speakers and Affiliations

(in alphabetical order)

- **Mrinmoy Datta**, Technical University of Denmark, Copenhagen
- **N. S. Narasimha Sastry**, Indian Statistical Institute, Bangalore
- **Anuradha Sharma**, IIIT Delhi
- **P. Vijay Kumar**, Indian Institute of Science, Bangalore

Schedule

January 5, 2017

- 2.00 pm – 2.05 am *Opening Remarks* by **Tarun K. Das**, Sectional President, Mathematical Sciences, ISC-2017
- 2.05 pm - 2.40 pm **P. Vijay Kumar**, *The Evolution of Coding Theory to Ensure Reliable Distributed Storage*
- 2.40 pm - 3.15 pm **N. S. Narasimha Sastry**, *Binary Codes from Projective Geometries*
- 3.15 pm - 3.50 pm **Anuradha Sharma**, *Enumeration of complementary-dual cyclic additive codes*
- 3.55 pm - 4.30 pm **Mrinmoy Datta**, *Maximum Number of Rational Points on Varieties over Finite Fields and Higher Weights of Projective Reed-Muller Codes*

Titles and Abstracts of Talks

(in alphabetical order of the names of speakers)

Title: *Maximum Number of Rational Points on Varieties over Finite Fields and Higher Weights of Projective Reed-Muller Codes*

Speaker: Mrinmoy Datta

Abstract: For a prime power q, let $\mathbb{F}_q$ denote the finite field with q elements. For positive integers m and d, let $\mathbb{P}^m$ denote the projective space of dimension m over $\mathbb{F}_q$ and let R_d denote the $\mathbb{F}_q$-vector space generated by all the homogeneous polynomials of degree d in $m+1$ variables $x_0, x_1, \ldots, x_m$ with coefficients in $\mathbb{F}_q$. For $1 \leq r \leq \binom{m+d}{d}$, let $e_r(d,m)$ denote the maximum number of common zeroes that r linearly independent elements of R_d can have in $\mathbb{P}^m$.

In this talk, we will discuss the open problem of determining $e_r(d,m)$. In particular, we will outline some recent progress that has been made in determining $e_r(d,m)$ for $r \leq \binom{m+2}{2}$ and $d < q$ in a joint work with Peter Beelen and Sudhir Ghorpade. We will also discuss applications to explicit determination of the generalized Hamming weights of projective Reed-Muller codes.

Title: *Binary Codes from Projective Geometries*

Speaker: N. S. Narasimha Sastry

Abstract: An ovoid in a projective 3-space over a field k is a maximal set of points, no three on a line. Elliptic quadrics are the generic examples of ovoids and are the only ovoids if k is a finite field of odd order. If the number of elements of k is 2^{2n+1}, $n > 1$, Tits constructed an ovoid for each n, not equivalent to an elliptic quadric, as the set of absolute points of a polarity of a symmetric generalised quadrangle. Classification and distribution of ovoids in a projective 3- space over a finite field of even characteristic is a fundamental problem in incidence geometry in view of the appearance of ovoids in many geometric and combinatorial structures. We discuss the applications of coding theory in understanding some of the issues regarding this question.

Title: *Enumeration of complementary-dual cyclic additive codes*

Speaker: Anuradha Sharma

Abstract: Let $\mathbb{F}_q$ denote the finite field of order q and characteristic p, n be a positive integer coprime to q and $t \geq 2$ be an integer. A cyclic additive code $\mathcal{C}$ of length n is defined as an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^t}^n$ satisfying the following property: $(c_0, c_1, c_2, \cdots, c_{n-1}) \in \mathcal{C}$ implies

that $(c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in \mathcal{C}$. These codes form an important class of error-correcting codes due to their rich algebraic structure and have nice connections with quantum stabilizer codes. Many authors studied their dual codes with respect to the ordinary and Hermitian trace inner products on $\mathbb{F}_{q^t}^n$.

For any integer $t \geq 2$ satisfying $t \not\equiv 1 (\mathrm{mod}\ p)$, we place a new trace bilinear form on $\mathbb{F}_{q^t}^n$, which is called the $*$ trace bilinear form and is a generalization of the Hermitian trace inner product on $\mathbb{F}_{q^t}^n$ when q is even and $t = 2$. We observe that it is a non-degenerate, symmetric bilinear form on $\mathbb{F}_{q^t}^n$ for any prime power q and is alternating when q is even. We study dual codes of cyclic additive codes of length n with respect to this bilinear form. We further study and enumerate all the complementary-dual cyclic additive codes of length n by placing $*$, ordinary and Hermitian trace bilinear forms on $\mathbb{F}_{q^t}^n$.

Title: *The Evolution of Coding Theory Towards Reliable Distributed Storage*

Speaker: P. Vijay Kumar

Abstract: There has been an evolution in coding theory over the past 7+ years, to address problems associated with the distributed storage of 'Big Data'. In distributed storage, data pertaining to a single file is stored in redundant fashion across nodes of a storage network. A node could correspond to a hard disk or a server and the nodes are assumed to fail independently.

From an application point of view, the problem is one of dealing efficiently with the failure of individual nodes. From a coding-theoretic viewpoint, the challenge is one of partial data recovery. Two new classes of codes, known respectively as regenerating codes and codes with locality have arisen to address this challenge. We will in this talk present an accessible overview of these exciting recent developments.
