PROGRAMME and ABSTRACTS

24 September

OPENING : Welcoming session by

· V. Nesi, as Director of Mathematics Department

· C. Procesi, as Dean of Algebra

· F. Flaminio, as member of Scientific Committe

MORNING

Chairlady: D. Ghinelli

10.20-11.10	F. de Clerck: "Small is beautiful.... "
11.10-11.40	Coffe Break
11.40-12.20	J. W.P. Hirschfeld: "Curves of genus 3"
12.30-12.50	A. Sonnino: "The Gale transform in finite geometry and coding theory"
13.00	Lunch

AFTERNOON

15.00-15.50	V. Jha :"Fractional Dimensional Semifields"
15.50-16.20	Coffe Break
16.20-17.10	F. Mazzocca: "BLOCKING SET: Una panoramica di risultati e alcune recenti direzioni di ricerca"
17.20-17.40	C. Cerroni:"Some models of geometries after Hilbert's Grundlagen"

25 September

MORNING

Chairman: A. D'Andrea

10.00-10.50	S. Magliveras: "Cryptanalysis of the Tillich-Zemor hash function"
10.50-11.20	Coffe Break
11.20-12.10	L. Bader: "Spreads of $PG(3,q)$ and Ovoids of $H(3,q^2)$"
12.20-12.40	D. Iacono: "A new look at the BTT-Theorem"
13.00	Lunch

AFTERNOON

Chairman: A. Machì

15.00-15.20	G. Bini: "Some Remarks on Calabi-Yau Manifolds"
15.30-15.50	M. Avitabile: "Thin Lie algebras"
15.50-16.20	Coffe Break
16.20-17.10	D. Jungnickel: "Characterizing Geometric Designs"

CLOSING: Greeting session by

· Ernest A. Ruet d'Auteuil, Institute of Combinatorics and Its Applications

· M. Monsurró

· C. Colasanti

ABSTRACTS

24 SEPTEMBER

Small is beautiful....

F. de Clerck

Abstract. Quite often constructions or characterization theorems of finite incidence structures are based on some experiments (with or without the use of the computer) with structures having small parameters. In this talk we will discuss a few examples of such small incidence structures in projective and polar spaces, that have lead to a more general theory.

Curves of genus 3

J.W.P. Hirschfeld

Abstract. Over any field, there is a classical connection between curves of genus 3 and cubic surfaces. There is the question of how many points such a curve can have over a finite field. This is reviewed for curves of this genus as well as those of genus 1 and genus 2.

The Gale transform in finite geometry and coding theory

A. Sonnino

Abstract. The Gale transform is an involution on sets of points in a projective space. It plays a crucial role in several different subjects such as algebraic geometry, optimization, coding theory, etc. Sometimes in the literature the Gale transform is used implicitly, without mentioning it as such. We give a short account of the algebraic and geometrical implicatons that the Gale transform has when it is applied to sets of points in finite projective spaces. Further, we give some geometric constructions of linear codes admitting a prescribed automorphism group obtained by means of the Gale transform.

Fractional Dimensional Semifields

V. Jha

Abstract. Let D be a finite semifield. Then the dimension of D relative to a subsemifield E is $log|D|/log|E|$: so for fields the dimension is an integer. I shall consider the situation when D has non-integer dimension relative to some E. Such cases are known to arise in several cases when D has even order 2^n. The aim of this talk is to show that fractional semifields arise even for semifields of odd order.

BLOCKING SET: Una panoramica di risultati e alcune recenti direzioni di ricerca

F. Mazzocca

Abstract. Verranno esposti alcuni risultati fondamentali della teoria dei blocking set e alcune recenti direzioni di ricerca.

Some models of geometries after Hilbert's Grundlagen

C. Cerroni

Abstract. In 1899, David Hilbert published the *Grundlagen der Geometrie*, a book that opened up research in the foundations of geometry. In fact, the *Grundlagen* took the axiomatic method both as a culmination of geometry and as the beginning of a new phase of research. In that new phase, the links between the postulates were not seen as the cold expression of their logical relations or interdependence, but as the creation of new geometries having equal importance at the research level.

We will investigate the contribution of Max Dehn to the development of non-Archimedean geometries and the contribution of his student Ruth Moufang to the development of non-Desarguesian geometries. We will see that it is possible to construct some models of non-Archimedean geometries to prove the independence of the continuity axiom and we will study the interrelations between Archimedes' axiom and Legendre's theorems. Moreover, we will study the model of non-Desarguesian geometry of Ruth Moufang and we will see that a geometric model became a complicated interrelation between algebra and geometry.

25 SEPTEMBER

Cryptanalysis of the Tillich-Zemor hash function

S. Magliveras

Abstract. Cryptographic (one-way) hash functions have many information security applications, particularly in *digital signatures*, *data integrity*, *message authentication codes* (MAC's), and other types of authentication. At CRYPTO'94, Tillich and Zémor proposed a hash function, based on the family groups $SL_2(\mathbb{F}_q)$, $q = 2^n$. We have recently compromised the hash function by showing it is not collision resistant. In fact we can construct efficiently *short* collisions, independently of the choice of the irreducible polynomial in the definition of $\mathbb{F}_q$. Our approach also yields collisions for related proposals by Petit et al. from ICECS'08 and CT-RSA'09. The attack is afforded by using a 1987 result of Mesirov and Sweet on the existence of maximal length chains in the execution of the Euclidean algorithm over a field of even characteristic. More specifically, the approach is constructive and we present an algorithm to compute collisions for any choice of parameters. The applicability of the attack is demonstrated by producing, in a few seconds, short palindromic collisions for all recently proposed specific parameters, using a computer algebra system on a standard PC.

The talk is based on joint work with my student Ivana Ilić (CCIS, Florida Atlantic University), and our colleagues, Rainer Steinwandt (CCIS, Florida Atlantic University) and Markus Grassl (CQT, National University of Singapore).

Keywords: cryptographic hash function, cryptanalysis, special linear group

Spreads of $PG(3, q)$ and Ovoids of $H(3, q^2)$

L. Bader

Abstract. We review some results on ovoids and spreads of finite polar spaces, focusing on the ovoids $H(3, q^2)$ arising from spreads of $PG(3, q)$ via indicator sets and Shult embedding.

A new look at the BTT-Theorem

D. Iacono

Abstract. We give a completely algebraic proof of the Bogomolov-Tian-Todorov theorem. More precisely, we shall prove that if X is a smooth projective variety with trivial canonical bundle defined over an algebraically closed field of characteristic 0, then the L_∞-algebra controlling infinitesimal deformations of X is quasi-isomorphic to an abelian differential graded Lie algebra.

Some Remarks on Calabi-Yau Manifolds

G. Bini

Abstract. After recalling some classical examples, we will go over some constructions which might yield - hopefully - new examples of Calabi-Yau manifolds

Thin Lie algebras

M. Avitabile

Abstract.

Characterizing Geometric Designs

D. Jungnickel

Abstract. We conjecture that the classical geometric 2-designs $PG_d(n, q)$ formed by the points and d-dimensional subspaces of the projective space of dimension n over the field with q elements, where $2 \leq d \leq n-1$, are characterized among all designs with the same parameters as those having line size $q+1$. The conjecture is known to hold for the case $d = n-1$ (the Dembowski-Wagner theorem) and also for $d = 2$ (a recent result established by Tonchev and the present author). Here we extend this result to the cases $d = 3$ and $d = 4$. The general case remains open and appears to be difficult.