XII. Antalya Cebir Günleri

19–22 Mayıs 2009
Contents

Invited talks 4
1. Alp Bassa .......................... 4
2. Alexandre Borovik .................. 4
3. Pascale Charpin ...................... 5
4. Wilfrid Hodges ...................... 6
5. Franz-Viktor Kuhlmann ............... 6
6. Mahmut Kuzucuoğlu .................. 8
7. Ömer Küçüksakallı ................... 9
8. James D. Lewis ....................... 9
9. Christian Lomp ....................... 10
10. Gary McGuire ....................... 11
11. Ferruh Özbudak ..................... 11
12. Daniel Panario ..................... 12
13. Alexander Pott ..................... 13
14. Peter Roquette ...................... 14
15. Hans-Georg Rück ..................... 14
16. Amin Shokrollahi .................... 15
17. Patrick F. Smith .................... 15
18. Wolfgang Willens ................... 16
19. Arne Winterhof ...................... 16

Contributed Talks 18
1. Ahmet Arıkan ....................... 18
2. A. O. Asar .......................... 18
3. Tengiz Bokelavadze .................. 19
4. Inês Borges .......................... 20
5. Engin Büyükaşık .................... 20
6. Yasemin Çengellenmiş ................ 21
7. Ahmet Sinan Çevik ................... 22
8. Ömür Deveci ......................... 23
9. Yılmaz Durgun ....................... 24
10. Betül Gezer ........................ 25
11. Pedro A. Guil Asensio ............... 26
12. Ayşe Dilek Güngör .................. 26
13. Serpil Güngör ....................... 27
14. Erhan Gürel ........................ 28
15. Murat Güzeltepe ..................... 28
16. Sevgi Harman ....................... 29
17. Eylem Güzel Karpuz .................. 30
18. Tariel Kemoklidze ................... 31

19. Fatih Koyuncu ....................... 32
20. V. M. Levchuk ........................ 32
21. Engin Mermet ....................... 34
22. Figen Öke ........................... 35
23. Hakan Özadam ....................... 36
24. Dilek Pusat-Yılmaz .................. 36
25. Ashkan Sezgin ....................... 37
26. Ebru Solak ........................... 38
27. Vedat Şiap ........................... 38
28. Funda Taşdemir ..................... 39
29. Yasemin Taşyurdu .................... 40
30. S. Eylem Toksoy ..................... 40

Posters 42
1. Akleyelek & Cenk .................... 42
2. Esen Aksoy .......................... 43
3. Nurdagül Anbar ...................... 43
4. Vural Cam ........................... 44
5. Murat Cenk ........................... 44
6. Münever Çelik ....................... 44
7. Ayça Çesmelioglu .................... 45
8. Şükrü Uğur Efem ..................... 45
9. Mehmet İnan Karakuş ................ 46
10. Dilber Koçak ......................... 46
11. Azadeh Neman ....................... 48
12. Mehmet Özdemir ..................... 49
13. Buket Özkaya ....................... 50
14. David Pierce ......................... 51
15. Ata Firat Pir ......................... 52
16. Elif Saygı ........................... 52
17. Zülfükar Saygı ....................... 53
18. Seher Tutdere ....................... 53
19. İnan Utku Türkmen ................... 54

Participants 55
Personnel 58
Acknowledgements 58
Short talks 59
Timetable 60
It is a pleasure to welcome you to Antalya Algebra Days XII.

Having begun as an informal meeting of approximately 40 mathematicians in 1999, Antalya Algebra Days have evolved into meetings that most algebraists and number theorists in Turkey look forward to each year.

For those of us who have been involved in organization since the beginning, this year’s meeting is a sad occasion. We lost one of the founders, and a great friend, Professor Cemal Koç. He passed away on 1 April 2010. We remember him very dearly.

One of the main aims of AAD has been to provide a platform for enabling and strengthening national as well as international collaboration in various topics in algebra. The participation of guests from abroad greatly helps in realizing this goal. We deeply thank them for their contribution.

All of the organizers of this meeting have put in a lot of effort, but Ayşe, David, and Henning join me in expressing our gratitude to Cem for his dedication and extremely hard work.

Special thanks go to Tamer Koç and Şükran Demir of Tivrona Tours who have been able to meet our endless wishes.

TÜBİTAK (the Scientific and Technological Research Council of Turkey), Sabancı University, and the Turkish Mathematical Society have provided financial support; Middle Eastern Technical University hosts the website. We thank them all.

We hope that you will have a wonderful time here.

Alev Topuzoğlu
For the Organizers of AAD XII
Invited talks

**Towers of algebraic function fields and their applications**

Alp Bassa

In this talk I will introduce towers of algebraic functions fields and outline some of their applications. I will discuss some of the questions about towers, which emerge naturally from these applications.

*Centrum Wiskunde & Informatica, Amsterdam*

Alp.Bassa@cwi.nl

**Pseudofinite groups and groups of finite Morley rank: proof of concept**

Alexandre Borovik

The talk will discuss recent progress in a joint project with PınarUGHURULU and Şükri YALÇNKAYA.

Our project looks at relations between two major conjectures in the theory of groups of finite Morley rank, a modern chapter of model theoretic algebra. One conjecture, the famous the Cherlin-Zilber Algebraicity Conjecture formulated in 1970-s states that infinite simple groups of finite Morley rank are isomorphic to simple algebraic groups over algebraically closed fields. The other conjecture, due to Hrushovski and more recent, states that a generic automorphism of a simple group of finite Morley rank has pseudofinite group of fixed points. Hrushovski showed that the Cherlin-Zilber Conjecture implies his conjecture. Proving Hrushovski’s Conjecture and reversing the implication would provide a new efficient approach to proof of Cherlin-Zilber Conjecture.

Meanwhile, the machinery already developed for work at the pseudofinite/finite Morley rank interface yields an interesting and powerful result: an alternative proof of the Larsen-Pink Theorem (the latter says, roughly speaking, that “large” finite simple groups of matrices are Chevalley groups over finite fields):

**Theorem** (Larsen and Pink [1]). *For any finite simple group G possessing a faithful linear or projective representation of dimension n over a field k we have either*

(a) |G| is bounded by a function which depends only on n, or

(b) \(p := \text{char}(k)\) is positive and G is a group of Lie type in characteristic p.

This alternative proof is based on ideas from the classification theory of groups of finite Morley rank; it does not use the classification of finite simple groups and can be seen as “proof of concept” for our research programme.
Permutations with small differential uniformity

Pascale Charpin

Differential cryptanalysis is the first statistical attack proposed for breaking iterated block ciphers. Its presentation then gave rise to numerous works which investigate the security offered by different types of functions with respect to differential attacks. This security is quantified by the so-called differential uniformity of the Substitution box used in the cipher. The study of algebraic properties of functions over finite fields (most important are the finite fields of order 2), replaced in this context, is a major topic for the last fifteen years. Although the purpose is to obtain new efficient designs for block ciphers, the theoretical aspects of this research are of great interest.

Monomial permutations, form a class of suitable candidates since they usually have a lower implementation cost in hardware. Moreover, their properties regarding differential attacks can be studied more easily since they are related to the weight enumerators of some cyclic codes with two zeroes. However, using power permutations which are optimal for differential cryptanalysis might not be suitable in a cryptographic context: Such permutations on $\mathbb{F}_{2^n}$ are generally not known for even $n$ and optimal functions usually correspond to extremal objects, which possess very strong algebraic structures.

For all these reasons, it is important to find some permutations which have an almost optimal low differential uniformity, and a sparse polynomial expression. Also, other properties appear as necessary, because of the active research on other statistical attacks.

In this context, we first investigate the differential properties, namely the whole differential spectrum, of power permutations which have a low differential uniformity. Further, we present recent results on polynomials in $\mathbb{F}_{2^n}[X]$ of the shape

$$G(X) + \lambda Tr(H(X)),$$

$G(X), H(X) \in \mathbb{F}_{2^n}[X], \quad \lambda \in \mathbb{F}_{2^n}.$

We notably identify such permutations when $G$ and $H$ are monomials.

INRIA, B.P. 105, 78153 Le Chesnay Cedex, France
Pascale.Charpin@inria.fr
http://www-rocq.inria.fr/secret/Pascale.Charpin/index.html
Definability versus definability-up-to-isomorphism, in groups and fields

Wilfrid Hodges

Many algebraic constructions $F$, where $F(A)$ is a structure built on the structure $A$, are defined up to isomorphism over $A$. (A typical example is algebraic closure, where $F(A)$ is the algebraic closure of a field $A$.) Suppose we ask whether such a construction $F$ can be defined outright and not just up to isomorphism. In general the answer calls on some interactions of cohomology and set theory. The talk will survey examples from groups and fields, and will mention recent joint work with Saharon Shelah.

Herons Brook, Sticklepath, Okehampton EX20 2PY, England

wilfrid.hodges@btinternet.com

http://wilfridhodges.co.uk

The structure of valued function fields in positive characteristic: known results and open problems

Franz-Viktor Kuhlmann

The structure theory of valued function fields has important applications in many areas, two of the most prominent being local uniformization (i.e., local resolution of singularities) and the model theory of valued fields. In positive characteristic, these two areas offer deep open problems: neither resolution of singularities nor local uniformization have been proved, and the question whether Laurent series fields over finite fields have a decidable theory has not been answered. I will show how these problems are connected with the structure theory of valued function fields and its open problems. One of these problems is the elimination of ramification, a necessary but not sufficient step towards local uniformization. In positive characteristic, one phenomenon we have to struggle with is the defect of valued field extensions (which is connected with wild ramification). I will present two main theorems that deal with the defect in valued function fields, and their application to local uniformization and the model theory of so-called tame valued fields.
Using a purely valuation-theoretical proof, I have shown that local uniformization is always possible after a separable extension of the function field of the algebraic variety (separable "alteration"). Local uniformization by alteration also follows from de Jong’s resolution by alteration, but our result gives more detailed information on the extension of the function field. Recently, Michael Temkin has proved local uniformization by purely inseparable alteration. However, a classification of Artin-Schreier extensions with non-trivial defect shows that separable alteration and purely inseparable alteration are just two ways to eliminate particularly malicious defects. So the existence of these two seemingly "orthogonal" local uniformization results does not necessarily indicate that local uniformization without alteration is possible.

The structure theory of valued function fields in positive characteristic and the theory of the defect offer many deep and exciting questions, with applications to important open problems. My goal is to attract more young mathematicians to this particular area of research.

References


Department of Mathematics and Statistics, University of Saskatchewan, 106 Wiggins Road, Saskatoon, Saskatchewan, Canada S7N 5E6
fvk@math.usask.ca
http://math.usask.ca/~fvk
Universal groups
Mahmut Kuzucuoğlu

A group is called a **locally finite group** if every finitely generated subgroup is a finite group. A locally finite group \( U \) is called **universal** if
1. every finite group can be embedded into \( U \),
2. any two isomorphic finite subgroups of \( U \) are conjugate in \( U \).

Existence and basic properties of countable universal locally finite groups are given by P. Hall in [2] see also in [3]. For any given uncountable cardinality \( \kappa \), existence of \( 2^\kappa \) non-isomorphic universal locally finite groups of cardinality \( \kappa \) is given by S. Shelah and A. J. Macintyre in [5].

We are interested in centralizers of finite subgroups in simple non-linear locally finite groups. In particular the following question. Is the centralizer of every finite subgroup in a non-linear locally finite simple group infinite? We answer this question for direct limit of finite alternating groups. Particular case gives an answer to the centralizers of finite subgroups in universal groups.

**Theorem 1.** (Ersoy-Kuzucuoğlu) Let \( G \) be a simple locally finite group which is a direct limit of finite alternating groups, and \( F \) be a finite subgroup of \( G \). Then \( C_G(F) \) contains an abelian subgroup \( A \) which is isomorphic to \( \mathbb{Z}_p \) for some prime \( p \).

We also mention universal groups that are not necessarily locally finite groups constructed by O. H. Kegel in [4]. We will discuss basic properties of this regular limit group \( S_\lambda \) of symmetric groups. We also discuss the following result.

**Lemma 2.** (O. H. Kegel, M. Kuzucuoğlu) Let \( B \) be a bounded subgroup of a regular limit group \( S_\lambda \) with trivial center. Then \( C_{S_\lambda}(B) \) is isomorphic to \( S_\lambda \).

**References**

[1] Ersoy, K; Kuzucuoğlu M. Centralizers of subgroups in simple locally finite groups, Submitted.

Middle East Technical University, Department of Mathematics, 06531 Ankara, TURKEY
matmah@metu.edu.tr
metu.edu.tr/~matmah
Computing class numbers via elliptic units

Ömer Küçüksakallı

The class number is a powerful invariant in algebraic number theory which can be used to investigate the integer solutions of polynomials, such as Fermat’s Equation. It can be computed for extensions with small degree and discriminant, however computations take a very long time for higher extensions. In this talk, we will describe a heuristic method to compute the class numbers of some abelian extensions of imaginary quadratic fields. This is the elliptic analogue of an algorithm of Schoof used for cyclotomic fields. We will use elliptic units analytically constructed by Stark and the Galois action on them given by Shimura’s reciprocity. In the end we will give a counter-example to Vandiver’s conjecture in the elliptic curve case.

References


Middle East Technical University, Department of Mathematics, 06531 Ankara Turkey
komer@metu.edu.tr
www.metu.edu.tr/~komer/

The Bloch–Kato theorem and Hodge type conjectures

James D. Lewis

The Bloch–Kato conjecture was recently proven by V. Voevodsky and his collaborators. It is a generalization of the Merkurjev–Suslin theorem and the Milnor conjecture [theorem]. This conjecture [theorem] turns out to be under the same general umbrella as the Hodge conjecture and its generalizations (due to Beilinson). We will explain the Bloch–Kato theorem and its connection to the Hodge type conjectures.

University of Alberta
lewisjd@gpu.srv.ualberta.ca
http://www.math.ualberta.ca/Lewis_JD.html
Injective hulls of simple modules over down-up algebras

Christian Lomp

The module theoretical properties of indecomposable injective modules over a Noetherian ring $R$ are important for the structure theory of $R$. For a commutative Noetherian ring $R$, Eben Matlis showed in [1] that any injective hull of a simple $R$-module is Artinian, a property that, in general does not hold for non-commutative rings. However Randall Dahlberg showed in [2] that injective hulls of simple modules over $U(\mathfrak{sl}_2)$ are locally Artinian. The enveloping algebra $U(\mathfrak{sl}_2)$ is an instance of a larger class of Noetherian domains, the Down-Up algebras, introduced by Georgia Benkart and Tom Roby in [3]. The Down-Up algebras $A(\alpha, \beta, \gamma)$ form a three parameter family of associative algebras. For any parameter set $(\alpha, \beta, \gamma) \in \mathbb{C}^3$ one defines a $\mathbb{C}$-algebra, denoted by $A(\alpha, \beta, \gamma)$, generated by two elements $u$ and $d$ subject to the relations
\[
\begin{align*}
    d^2 u &= \alpha dud + \beta ud^2 + \gamma d \\
    du^2 &= \alpha ud + \beta u^2 d + \gamma u
\end{align*}
\]
which is a Noetherian domain if and only if $\beta \neq 0$. In particular $A(2, 1, 1) = U(\mathfrak{sl}_2)$ holds.

During the X. Antalya Algebra Days, Patrick Smith asked in a private conversation with Paula Carvalho, which Noetherian Down-Up algebras satisfy the condition that their injective hulls of simple modules are locally Artinian.

I will present the findings on Patrick’s question from our joint work [4] with Paula Carvalho and Dilek Pusat-Yilmaz, namely that a Noetherian Down-Up algebra $A(\alpha, \beta, \gamma)$ has the desired property if the roots of the polynomial $X^2 - \alpha X - \beta$ are distinct roots of unity or both equal to 1. If time permits I will also report on the progress made by Paula Carvalho and Ian Musson in [5].

References


University of Porto
clomp@fc.up.pt
www.fc.up.pt/mp/clomp
Introduction to APN functions and related topics
Gary McGuire

In this talk we will introduce PN (perfect nonlinear) and APN (almost perfect nonlinear) functions. Without assuming any previous knowledge, we present and discuss the definitions, applications, and connections to areas like coding theory and cryptography. We will also discuss the Fourier transforms of such functions.

University College Dublin
gmg2010@gmail.com
http://mathsci.ucd.ie/~gmg/

Quadratic forms of codimension 2 over finite fields containing $\mathbb{F}_4$ and Artin-Schreier type curves
Ferruh Özbudak

Let $F_q$ be a finite field containing $\mathbb{F}_4$. Let $k \geq 2$ be an integer. We give a full classification of quadratic forms over $F_{q^k}$ of codimension 2 provided that certain three coefficients are from $\mathbb{F}_4$. As an application of this we obtain new results on the classification of maximal and minimal curves over $F_{q^k}$. We also give some nonexistence results on certain systems of equations over $F_{q^k}$.

This is a joint work with Elif Saygî and Zülfükar Saygî.

Middle East Technical University
ozbudak@metu.edu.tr
Normal bases in finite fields

Daniel Panario

This talk surveys normal bases and normal elements in finite fields. These concepts were defined, and their existence proved, 150 years ago. However, due to their many recent applications, they have been vastly studied in the last 20 years.

Let $q$ be a prime power. An element $\alpha$ in a finite field $\mathbb{F}_{q^n}$ is called normal if $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this case, the basis $N$ is called a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

First we briefly give an account of basic properties and results of normal elements including existence and number of normal elements.

Then we focus on how to operate with normal basis. As Hensel noted, in a normal basis $q$th powers are for free. This can be exploited to have fast exponentiation algorithms. As a consequence, normal elements are important in cryptographic applications where exponentiation and discrete logarithm computations are employed.

Next we discuss how to find normal elements. It turns out that not all normal elements behave in the same way, the so called optimal normal elements being preferable for most computations with normal elements. These special elements are directly related to Gauss periods in finite fields and have been characterized by Gao and Lenstra. Unfortunately, optimal normal elements only exist for some extension fields. This makes the study of low complexity normal elements relevant. We comment on several old and new results to produce low complexity normal elements. We conclude giving some open problems.

Carleton University, Canada

daniel@math.carleton.ca

http://www.math.carleton.ca/~daniel/
**APN and PN functions: Differences and Similarities**

Alexander Pott

Motivated by cryptography, one is interested in functions

\[ f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n \]

such that the equations (given \( a \neq 0 \) and \( b \))

\[ f(x + a) - f(x) = b \]

have only a few solutions \( \delta(a, b) \). More precisely, the maximum value of all the numbers \( |\delta(a, b)| \) should be small. It is easy to see that the maximum is 2 if \( p = 2 \), and it is 1 if \( p \) is odd. In the case \( p = 2 \), functions which achieve this minimum are called **almost perfect nonlinear** (APN), in the case \( p \) odd **perfect nonlinear** (PN).

Both for the PN and the APN case, some (but not too many) examples are known: infinite families as well as sporadic examples. It seems that there are more APN functions known since the defining property for APN functions is less restrictive: Some of the \( \delta(a, b) \) are 0, some are 2. In the PN case, all these numbers must be 1. Similarly, the absolute values of the Walsh coefficients in the APN case are not determined by the APN property, but they are determined in the PN case.

Another important difference seems to be the underlying algebraic structure: Quadratic PN functions (and all PN functions except those constructed by Coulter and Matthews are quadratic) give rise to a strong algebraic structure (semifields). Nothing comparable seems to be true for quadratic APN functions.

PN functions can be used to construct finite projective planes. APN functions also describe certain incidence structures, but these have, in general, less structure than projective planes.

However, there are also similarities between APN and PN functions: Some constructions, described in terms of polynomials in \( \mathbb{F}_p^n \), work both for the PN and the APN case. Moreover, a switching construction which has been shown to be quite powerful in the APN case has the potential to be useful also in the PN case.

In my talk, I will discuss these similarities and differences between APN and PN functions. In particular, I will cover the following topics:

- Incidence structures defined by PN and APN functions.
- Automorphism groups of these incidence structures.
- Semifields and the equivalence of functions.
- The switching construction of PN and APN functions.

*Otto-von-Guericke-University Magdeburg*

alexander.pott@ovgu.de

http://fma2.math.uni-magdeburg.de/~pott/
News on the Arf invariant

Peter Roquette

The 10-Lira note of Turkish currency carries the portrait of the mathematician Cahit Arf, accompanied with a formula for the Arf invariant of a quadratic form. I shall explain the notion of Arf invariant and its place within the general theory of quadratic forms. The talk is relying not only on published papers but also on letters and other documents of Arf’s time. Recently it has turned out that some of Arf’s results have to be modified.

References


University of Heidelberg, Germany
roquette@uni-hd.de
roquette.uni-hd.de

Elliptic curves and Drinfeld modules

Hans-Georg Rück

This is an introductory talk to the theory of Drinfeld modules. We want to explain how Drinfeld modules can be defined analogously to elliptic curves, following the path from an analytic torus to an algebraic structure.

References


Universität Kassel, Germany
rueck@mathematik.uni-kassel.de
http://www.mathematik.uni-kassel.de/~rueck
**Efficiency of random matrices over finite fields**

Amin Shokrollahi

A “random” \( m \times n \) matrix over a field \( K \) is a matrix sampled from some probability distribution over the space of such matrices. In this talk, we will investigate properties of such matrices over finite fields using several interesting probability distributions. The final goal is to construct matrices that behave like uniform random matrices (where the probability distribution is uniform) as far as their rank properties are concerned, and at the same time allow for very fast algorithms for solving systems of linear equations. Such matrices are used in the design of state of the art codes which allow for recovery of data in the face of data erasures.

*École Polytechnique Fédérale de Lausanne (EPFL) - ALGO*

amin.shokrollahi@epfl.ch

http://algo.epfl.ch/

**Homological properties and chain conditions**

Patrick F. Smith

There are many results linking homological properties of rings and modules with other properties, in particular chain conditions. The famous Auslander-Buchsbaum-Serre Theorem is one such. We shall investigate some of these results starting with the Auslander-Buchsbaum-Serre Theorem and including the work of Cohn on free ideal rings and more generally hereditary rings. Cohn’s work is related to a theorem of Schreier on free groups.

*University of Glasgow*

pfs@maths.gla.ac.uk

**New construction of \( \tilde{D}_5 \)-singularities**

Meral Tosun

For a given pair of special elements in the Lie algebra \( \mathfrak{sl}(2, \mathbb{C}) + \mathfrak{sl}(2, \mathbb{C}) \), we can define a slice whose intersection with the nilpotent subvariety is a \( \tilde{D}_5 \)-singularity. Here by special element we mean an element in the Lie algebra which has semi-simple component and nilpotent component simultaneously. We also calculated the \( j \)-function of the exceptional curves in the minimal resolutions of \( \tilde{D}_5 \)-singularities by using pairs of special elements. This is one of analogies of Grothendieck–Brieskorn theory.

This is joint work with K. Nakamoto.

*Galatasaray University*

mrltosun@gmail.com
Groups, representations and codes

Wolfgang Willems

Extremal self-dual doubly-even codes are for several reasons of particular interest. However only for small lengths \( n \) such codes have been constructed. The largest one has length \( n = 136 \). On the other hand, by a result of Zhang, we know that such codes might exist up to \( n = 3928 \). Thus there is a large gap between the bound and what we have constructed so far. In order to find larger examples ‘symmetries’ or in other words ‘non-trivial automorphisms’ may be helpful. In this spirit the talk deals with automorphisms of putative extremal self-dual doubly-even codes which induce a module structure of the ambient space. The known examples and what we can prove about the primes which do not occur in the order of the automorphism groups lead to interesting conjectures. On the way we classify all extremal doubly-even extended quadratic residue and quadratic double circulant codes. The results are joint work with Stefka Bouyuklieva (Veliko Tarnovo) and Anton Malevich (Magdeburg).

Otto-von-Guericke-Universität Magdeburg
willems@ovgu.de
http://fma2.math.uni-magdeburg.de/~willems/

Exponential sums and linear complexity of nonlinear pseudorandom number generators

Arne Winterhof

Let \( p \) be a prime, \( r \) a positive integer, \( q = p^r \) and denote by \( \mathbb{F}_q \) the finite field of \( q \) elements. Given a polynomial \( f(X) \in \mathbb{F}_q[X] \) of degree \( d \geq 2 \), we define the nonlinear pseudorandom number generator \((\mu_n)\) by the recurrence relation

\[
\mu_{n+1} = f(\mu_n), \quad n = 0, 1, \ldots, \quad (*)
\]

with \( \mu_0 \in \mathbb{F}_q \) such that \((\mu_n)\) is purely periodic with period \( T \leq q \).
Niederreiter and Shparlinski developed a method to study the exponential sums

\[ S_{a,N}(f) = \sum_{n=0}^{N-1} \chi \left( \sum_{j=0}^{s-1} \alpha_j \mu_{n+j} \right), \quad 1 \leq N \leq T, \]

where \( \chi \) is a nontrivial additive character of \( \mathbb{F}_q \) and \( a = (\alpha_0, \ldots, \alpha_{s-1}) \in \mathbb{F}_q^s \setminus \{0\} \), see also the survey [2]. In general this method leads only to a nontrivial bound if \( d = q^{o(1)} \).

For a nonnegative integer we define its \( p \)-weight as

\[ \sigma \left( \sum_{i=0}^{l} n_i p^i \right) = \sum_{i=0}^{l} n_i \quad \text{if } 0 \leq n_i < p. \]

For \( 0 \neq f(X) = \sum_{i=0}^{d} \gamma_i X^i \in \mathbb{F}_q[X] \) we define its \( p \)-weight degree as

\[ w(f) = \max \{ \sigma(i) \mid \gamma_i \neq 0, \ 0 \leq i \leq d \}. \]

Therefore, \( w(f) \leq \deg(f) \). Under certain restrictions on \( f(X) \) we proved in [1] a bound on \( S_{a,N}(f) \) which is nontrivial if \( w(f) \) is small enough but the degree can be large.

We also use the \( p \)-weight to bound the \( N \)th linear complexity of the sequence defined in \((*)\). The linear complexity is a measure for the unpredictability and thus suitability in cryptography.

References


Austrian Academy of Sciences (Linz)

arne.winterhof@oeaw.ac.at

http://www.ricam.oeaw.ac.at/people/page.cgi?firstn=Arne;lastn=Winterhof
Contributed Talks

Some progress on minimal non $X$-groups
Ahmet Arıkan

Let $X$ be a class of groups. A group $G$ is called a minimal non-$X$-group if every proper subgroup of $G$ is an $X$-group but $G$ itself is not.

We consider certain classes like “minimal non-solvable groups”, “minimal non-Baer groups” and some others here, and give some recent results relevant to them.

Infinite perfect groups will be under consideration and the results will be displayed mostly in Fitting $p$-group case.

References


Gazi University
arikan@gazi.edu.tr
http://websitem.gazi.edu.tr/~arikan

Barely transitivity and hypercentrality in locally finite $p$-Groups
A. O. Asar

In this work it is shown that if there exists a perfect locally finite barely transitive $p$-group, then it has a finite subgroup whose centralizer has finite exponent. As an application of this result it follows that there does not exist a totally imprimitive $p$-subgroup of $FSym(\Omega)$ which is a minimal non-$FC$-group, where $\Omega$ is infinite. This result together with the earlier results answers the following question in the negative: Does there exist a perfect locally finite minimal non-$FC$-group? Of course an imperfect locally finite minimal non-$FC$-group exist. It is an extension of its commutator subgroup which is a divisible abelian $q$-group of finite rank by a cyclic $p$-group. Furthermore it is shown
that the existence of a perfect locally finite minimal non-hypercentral $p$-group satisfying certain properties implies the existence of a perfect locally finite barely transitive $p$-group. Finally a sufficient condition is given for a perfect locally finite countable minimal non-hypercentral and non-(residually finite) group to contain a finite subgroup whose centralizer has finite exponent.

Varieties of power groups

Tengiz Bokelavadze

A. Myasnikov and V. Remeslennikov refined in his paper [1] the notion of a power series due to Lindon by introducing one more additional axiom, by which all abelian subgroups of a power group are ordinary modules. This refinement is the identical generalization of a module to the non-commutative case. In [1], the basic notions of the theory of power series are introduced and also the tensor completion construction, which is a key construction in the category of power groups, is defined. The papers [1-4] marked the beginning of a systematic study of the category of power groups in the sense of Myasnikov.

The present paper continues the series of the papers [1], [2], [3] and is dedicated to the construction of basic principles of the theory of power series varieties and tensor completions of groups in a variety. We study the relationship between free groups of a given variety for various rings of scalars. Varieties of abelian power groups are described. Besides, in the category of power groups we give various analogues of the notion of an $n$-step nilpotent group and prove their coincidence for $n = 1; 2$. It is shown that the tensor completion of a 2-step nilpotent group is also 2-step nilpotent.

This is joint work with Mikheil Amaglobeli, mikheil.amaglobeli@tsu.ge.

References


Faculty of Exact and Natural Sciences, A. Tsereteli State University, 59, Tamar Mepe St., Kutaisi, 4600, Georgia

bokele71@yahoo.com
Irreducible actions of Hopf algebras
Inês Margarida Rodrigues Pais da Silva Borges

A theorem by Bergen, Cohen and Fishman states that if a Hopf algebra \( H \) acts finitely on a module algebra \( A \) with finite Goldie dimension, such that \( A \) is a simple \( A\#H \)-module, then \( A \) has finite vector space dimension over \( A^H \). At the heart of its proof is the Jacobson’s Density Theorem. In this talk we extend this theorem to certain operator algebras using Julius Zelmanowitz’ density theorems.

ISCAC, Coimbra
iborges@iscac.pt

Rings over which flat covers of simple modules are projective
Engin Büyükaşik

Throughout, \( R \) is a ring with a unit element and all modules are unital right \( R \)-modules. In [3] L. Bican et al. proved that all modules have flat covers over arbitrary rings. It is known that, a ring \( R \) is right perfect if and only if flat cover of any right \( R \)-module is projective. The rings over which flat covers of finitely generated modules are projective are characterized in [1] and [2].

The aim of this talk is to introduce and give several characterization of the rings \( R \) over which flat covers of simple right \( R \)-modules are projective. A ring \( R \) is said to be right \( B \)-perfect if \( \text{Hom}(F, R) \to \text{Hom}(F, R/I) \) is an epimorphism for every flat right module \( F \) and maximal right ideal \( I \) of \( R \).

Theorem 1. For a ring \( R \) the following are equivalent.
1. \( R \) is right \( B \)-perfect.
2. Flat covers of simple modules are projective.
3. \( R \) is semiperfect and flat covers of simple modules are local.

Theorem 2. For a ring \( R \) the following are equivalent.
1. \( R \) is right \( B \)-perfect.
2. Every right ideal of \( R \) containing \( J(R) \) is cotorsion.
3. \( R \) is semilocal and \( J(R) \) is right cotorsion.

References
A characterization of the codes over $F_3$

Yaşemin Çengellenmiş

It is introduced $\nu$-cyclic and cyclic codes over the ring $F_3 + \nu F_3$ where $\nu^2 = 1, F_3 = \{0, 1, 2\}$. It is proved that the Gray image of the linear $\nu$-cyclic code over the commutative ring $F_3 + \nu F_3$ of length $n$ is a distance invariant ternary linear cyclic code and it is proved that if $n$ is odd, then every code over $F_3$ which is the Gray image of a linear cyclic code over $F_3 + \nu F_3$ of length $n$ is permutation equivalent to a linear cyclic code.

References


Department of Mathematics, Faculty of Science, Trakya University, 22030 Edirne, Turkey
ycengellenmis@yahoo.com
Subgroup separability and efficiency

Ahmet Sinan Çevik

Let $G$ be a group and let $H$ be a subgroup of $G$. Then $G$ is said to be $H$-separable if, for each $x \in G - H$, there exists $N \triangleleft G$ with finite index such that $x \notin NH$. Moreover $G$ is called subgroup separable if $G$ is $H$-separable for all finitely generated subgroups $H$ of $G$. The newest known results about subgroup separability can be found, for instance, in a joint paper “(Cyclic) Subgroup Separability of HNN and Split Extensions” written by Ateş and Çevik (published in Math. Slovaca, Vol 57(1) (2007), 33-40). Furthermore let $S$ be a generating set for $G$. We also recall that the Cayley graph of $G$, denoted by $\Gamma_G$, with respect to $S$ has a vertex for every element of $G$, with an edge $g$ to $gs$ for all elements $g \in G$ and $s \in S$. Thus the initial vertex of the edge is $g$ and the terminal is $gs$. Finally we let remind the definition of “efficiency” on finitely presented groups. So let us suppose that $G$ is such a group with a finite presentation $\mathcal{P}_G = \langle X; R \rangle$. Then the Euler characteristic of $\mathcal{P}_G$ is defined by $\chi(\mathcal{P}) = 1 - |X| + |R|$, where $|.|$ denotes the number of elements in the related set. Also there exists an upper bound $\delta(G) = 1 - rk_\mathbb{Z}(H_1(G)) + d(H_2(G))$, where $rk_\mathbb{Z}(.)$ denotes the $\mathbb{Z}$-rank of the torsion-free part and $d(.)$ denotes the minimal number of generators. In fact, by a paper written by Epstein in 1961, it always true that $\chi(\mathcal{P}_G) \geq \delta(G)$. We then define $\chi(G) = \min\{\chi(\mathcal{P}) : \mathcal{P} \text{ is a finite presentation for } G\}$. Hence the presentation $\mathcal{P}_G$ is called efficient if $\chi(\mathcal{P}_G) = \delta(G)$. In addition, $G$ is called efficient if $\chi(G) = \delta(G)$.

In this talk we are mainly interested in separability and efficiency on groups under standard wreath products. To do that we will first give a new geometric way to get a presentation for the standard wreath product in terms of Cayley graphs. Then we will express the first result of the talk about efficiency. Moreover, by considering the standard wreath product $G$ of any finite groups $B$ by $A$, we will give the relationship between $B$-separability and efficiency on $G$ as another result of the talk. We note that these two results have been obtained by Çevik and Ateş in a joint work which was published in the Rocky Mountain J. Math. 38(3) (2008), 779-800.

References


Selcuk University, Konya-Turkey
sinan.cevik@selcuk.edu.tr
On the basic k-nacci sequences in the direct product $D_n \times \mathbb{Z}_{2^i}$

Ömür Deveci

In this work, defining basic $k$-nacci sequences and the basic periods of these sequences in finite groups then we obtain the basic periods of basic $k$-nacci sequences and the periods of $k$-nacci sequences in the direct product $D_n \times \mathbb{Z}_{2^i}$.

This is joint work with Erdal Karaduman, eduman@atauni.edu.tr.

Department of Mathematics, Faculty of Science and Letters, Kafkas University, 36100 Kars, TURKEY
odeveci36@hotmail.com

Euclid alone has looked on beauty bare

Edna St. Vincent Millay, 1892–1950

Euclid alone has looked on Beauty bare.
Let all who prate of Beauty hold their peace,
And lay them prone upon the earth and cease
To ponder on themselves, the while they stare
At nothing, intricately drawn nowhere
In shapes of shifting lineage; let geese
Gabble and hiss, but heroes seek release
From dusty bondage into luminous air.

O blinding hour, O holy, terrible day,
When first the shaft into his vision shone
Of light anatomized! Euclid alone
Has looked on Beauty bare. Fortunate they
Who, though once only and then but far away,
Have heard her massive sandal set on stone.
The least proper class containing weak supplements

Yılmaz Durgun

This study deals with the classes Small, $S$, and $WS$ of short exact sequence of $R$-modules determined by small, supplement and weak supplement submodules respectively, and the class $\overline{WS}$ which is the least proper class contain all of them over a hereditary ring $R$. Small is the class of all short exact sequences $0 \to A \xrightarrow{\alpha} B \to C \to 0$ where $\text{Im}(\alpha) \ll B$, WS is the class of all short exact sequences $0 \to A \xrightarrow{\alpha} B \to C \to 0$ where $\text{Im}(\alpha)$ has a weak supplement in $B$. $S$ is the class of all short exact sequence $0 \to A \xrightarrow{\alpha} B \to C \to 0$ where $\text{Im}(\alpha)$ has a supplement in $B$ defined by Zöschinger in [4].

The classes are different from each other, in general. On the other hand the proper classes generated by these classes, that is the least proper classes containing these classes are equivalent: $\langle \text{Small} \rangle = \langle S \rangle = \langle WS \rangle$ (The least proper class containing a class $A$ is denoted by $\langle A \rangle$ see [3]). WS-elements are preserved under $\text{Ext}(g, f) : \text{Ext}(C, A) \to \text{Ext}(C', A')$ with respect to the second variable, they are not preserved with respect to the first variable. We extend the class $WS$ to the class $\overline{WS}$, which consists of all images of WS-elements of $\text{Ext}(C, A')$ under $\text{Ext}(f, 1_A) : \text{Ext}(C', A) \to \text{Ext}(C, A)$ for all homomorphism $f : C \to C'$.

To prove that $\overline{WS}$ is a proper class we will use the result of [2] that states that a class $P$ of short exact sequences is proper if $\text{Ext}_P(C, A)$ is a subfunctor of $\text{Ext}_R(C, A)$, then $\text{Ext}_P(C, A)$ is a subgroup of $\text{Ext}_R(C, A)$ for every $R$-modules $A, C$ and the composition of two $P$-monomorphism (epimorphism) is a $P$-monomorphism (epimorphism). We obtain the following results:

**Lemma 1.** If $f : A \to A'$, then $f_* : \text{Ext}(C, A) \to \text{Ext}(C, A')$ preserves WS-elements.

**Lemma 2.** If $g : C' \to C$, then $g^* : \text{Ext}(C, A) \to \text{Ext}(C', A)$ preserves WS-elements.

**Corollary 3.** The WS-elements of $\text{Ext}(C, A)$ form a subgroup.

**Lemma 4.** Let $R$ be hereditary ring. For a $\overline{WS}$ class of short exact sequences of $R$ modules, the composition of an Small-epimorphism and a $\overline{WS}$-epimorphism is a $\overline{WS}$-epimorphism.

**Lemma 5.** Let $R$ be hereditary ring. For a $\overline{WS}$ class of short exact sequences of $R$ modules, the composition of two $\overline{WS}$ monomorphism is a $\overline{WS}$ monomorphism.

**Theorem 6.** If $R$ is a hereditary ring, $\overline{WS}$ is a proper class.

**Corollary 7.** If $R$ is hereditary ring, then $\langle \text{Small} \rangle = \langle S \rangle = \langle WS \rangle = \overline{WS}$.

Joint work with: Prof. Rafail Alizade.

**References**

Squares and cubes in elliptic divisibility sequences

Betül Gezer

Elliptic divisibility sequences (EDSs) are generalizations of a class of integer divisibility sequences called Lucas sequences. There has been much interest in cases where the terms of Lucas sequences are squares and cubes. But the question of when a term of an EDS can be a square has not been answered yet. We answer this question by using the general terms of these sequences. In this work, we give the general terms of the elliptic divisibility sequences with zero terms and then we determine which terms of these are squares and cubes.

This is joint work with Osman Bizim, obizim@uludag.edu.tr.

References


Uludag University, Faculty of Science, Department of Mathematics, Göürükle 16059, Bursa, TÜRKİYE

betulgezer@uludag.edu.tr
Model category structures arising from Drinfeld vector bundles

Pedro A. Guil Asensio

We present a general construction of model category structures on the category

\[ \mathbb{C}(\mathcal{Qco}(X)) \]

of unbounded chain complexes of quasi-coherent sheaves on a semi-separated scheme \( X \). This construction is based on making compatible the filtrations of individual modules of sections at open affine subsets of \( X \). We apply this to describe the homotopy category \( \mathbb{K}(\mathbb{C}(\mathcal{Qco}(X))) \) via various model structures on \( \mathbb{C}(\mathcal{Qco}(X)) \). As particular instances, we recover recent results on the flat model structure for quasi-coherent sheaves. Our approach also includes the case of (infinite-dimensional) vector bundles, and of restricted flat Mittag-Leffler quasi-coherent sheaves, as introduced by Drinfeld. However, we show that the unrestricted case does not induce a model category structure as above.

University of Murcia, Spain
paguay@um.es

The bounds for distance Estrada index

Ayşe Dilek Güngör

Let \( G \) be a connected graph on \( n \) vertices, and let \( \mu_1, \mu_2, \ldots, \mu_n \) be the \( D \)-eigenvalues of its distance matrix \( D \). In this talk, we will present the definition and some properties of the distance Estrada index

\[ \text{DEE} = \text{DEE}(G) = \sum_{i=1}^{n} e^{\mu_i} \]

of the graph \( G \) (see [3]). We further present lower and upper bounds for \( \text{DEE}(G) \) and relations between \( \text{DEE}(G) \) and the distance energy.

References

Co-coatomically supplemented modules

Serpil Güngör

$M$ will mean an $R$-module where $R$ is an arbitrary ring with identity. A module $M$ is called coatomic if every submodule is contained in a maximal submodule of $M$. A proper submodule $N$ of $M$ is called co-coatomic if $M/N$ is coatomic. A module $M$ is co-coatomically supplemented if every co-coatomic submodule $U$ of $M$ has a supplement $V$, i.e. $V$ is minimal in the collection of submodules $L$ of $M$ such that $M = N + L$.

We have the following results.

**Proposition 1.** Let $M$ be a co-coatomically supplemented module. Then $M/N$ is co-coatomically supplemented.

**Proposition 2.** Let $M$ be a co-coatomically supplemented $R$-module. Then every co-coatomic submodule of the module $M/Rad(M)$ is a direct summand.

**Theorem 3.** Let $R$ be any ring. The following are equivalent for an $R$-module $M$.
1. Every co-coatomic submodule of $M$ is a direct summand of $M$.
2. Every maximal submodule of $M$ is a direct summand of $M$.
3. $M/Soc(M)$ does not contain a maximal submodule.

Joint work with Prof. Dr. Rafail Alizade

**References**


A note on the products \((1^\mu + 1)(2^\mu + 1) \ldots (n^\mu + 1)\)

Erhan Gürel

Let \(\Omega_\mu(n) = (1^\mu + 1)(2^\mu + 1) \ldots (n^\mu + 1)\) where \(\mu \geq 2\) is an integer. We prove that \(\Omega_3(n)\) is never squarefull, and in particular never a square, using arguments similar to those in [2], where Cilleruelo proves that \(\Omega_2(n)\) is not a square for \(n \neq 3\). In [1], among many other results, Amdeberhan, Medina and Moll claim that \(\Omega_\mu(n)\) is not a square if \(\mu\) is an odd prime and \(n > 12\). However, we have found a gap in the proof of this statement in [1], which we illustrate by giving counterexamples.

References


Nonbinary quantum stabilizer codes from codes over Gaussian integers

Murat Güzeltepe

There has been a great deal of work on trying to create efficient codes since Shor and Steane showed that it was possible to create quantum error-correcting codes [1-2]. The most successful technique to date for constructing binary quantum codes is the additive or stabilizer construction [3]. This construction takes a classical binary code, self-orthogonal under a certain symplectic inner product, and produces a quantum code, with the minimum distance determined from the classical code. Later, some results were generalized to the case of nonbinary stabilizer codes [4-7], but the theory is not nearly as complete as in the binary case. In [7], comprehensive theory of nonbinary stabilizer codes was submitted. In this paper, we obtain some nonbinary quantum stabilizer codes using classical codes over Gaussian integers. Some of these codes are MDS.

This is joint work with Mehmet ÖZEN (ozen@sakarya.edu.tr, www.mehmetozen.com) and is supported by Sakarya University Research funds as a Research Project with Project number 2009-50-02-001.

References

Finite generation of ideals in rings of finite character

Sevgi Harman

A ring $R$ is said to be of finite character if each nonzero element of it is contained in only finitely many maximal ideals. Let $R$ be a ring and $I$ an ideal of $R$. Then by the $J$-radical of the ideal $I$ we mean the intersection of all maximal ideals of $R$ containing $I$, and the $J_{\text{max}}$-radical of $I$ the intersection of all maximal ideals of $R$ of maximal height that contains $I$. It is shown that over a finite dimensional integral domain $R$ of finite character, each maximal ideal of $R[X]$ of maximal height is the $J$-radical of an ideal generated by three elements and $J_{\text{max}}$-radical of an ideal generated by two elements. We also show that over a one dimensional $S$-domain $R$ of finite character each prime ideal of $R[X]$ that does not contract to the zero ideal of $R$ is the radical of an ideal generated by at most two elements.

References


Istanbul Technical University
harman@itu.edu.tr
Generalized Bruck-Reilly $*$-extension of monoids

Eylem Güzel Karpuz

This is a joint work with Firat Ateş and Ahmet Sinan Çevik. Let $M$ be a monoid and $\theta : M \to M$ be an endomorphism. Then the Bruck-Reilly extension $BR(M, \theta)$ is the set

\[ \mathbb{N}^0 \times M \times \mathbb{N}^0 = \{(p, m, q) : p, q \geq 0, m \in M\} \]

with multiplication

\[
(p_1, m_1, q_1)(p_2, m_2, q_2) = (p_1 - q_1 + t, (m_1 \theta^{t-q_1})(m_2 \theta^{t-p_2}), q_2 - p_2 + t),
\]

where $t = \max(q_1, p_2)$. $BR(M, \theta)$ is a monoid with identity $(0, 1_M, 0)$. If $M$ is defined by the presentation $<A; R>$, then $BR(M, \theta)$ is defined by

\[ <A, b, c ; R, bc = 1, ba = (a\theta)b, ac = c(a\theta) (a \in A)> , \]

in terms of generators $(0, a, 0) (a \in A)$, $(0, 1_M, 1)$ and $(1, 1_M, 0)$ [2]. This extension is considered a fundamental construction in the theory of semigroups. In [1], the author defined a monoid, namely generalized Bruck-Reilly $*$-extension and studied some Green’s relations on it.

In this talk, we give a presentation for generalized Bruck-Reilly $*$-extension of monoids and then by using Bruck-Reilly and this generalized Bruck-Reilly $*$-extensions we answer the following question negatively.

**Question.** Does the group of units of a finitely presented monoid have to be finitely generated?

References


Balikesir University
eguzel@balikesir.edu.tr
http://w3.balikesir.edu.tr/~eguzel/
The lattice of fully invariant subgroups of a cotorsion hull

Tariel Kemoklidze

The report deals with the questions of abelian group theory and the term group always means an additively written abelian group. The notation and terms used in the talk are taken from the monographs [1], [2].

$p$—denotes a fixed prime number. $\mathbb{Z}$ and $\mathbb{Q}$ respectively the groups of integer and rational numbers. The investigation of the lattice of fully invariant subgroups of a group is an important task of the theory of groups. This question is a less studied for cotorsion groups. A group $A$ is called cotorsion if any extension of $A$ by a torsion-free group $C$ splits, i. e. $\text{Ext}(C, A) = 0$. The importance of the class of cotorsion groups is related to two facts (see [1, §§54, 55]): for any groups $A, B$ the group $\text{Ext}(A, B)$ is a cotorsion group; any reduced group $G$ is isomorphically embeddable into the group $G^\bullet = \text{Ext}(\mathbb{Q}/\mathbb{Z}, G)$ called the cotorsion hull of the group $G$. If $G$ is a torsion-complete $p$—group or a direct sum of cyclic $p$—groups or a countable direct sum of torsion-complete $p$—groups, then the lattice of fully invariant subgroups of group $G^\bullet$ was studied respectively in the works [3],[4],[5]. In this work the mentioned points is studied in case when $G$ is any direct sum of torsion-complete $p$—groups. With the help of projections and indicators (see [2, §65]) every element of the group $G^\bullet$ is corresponded to infinite matrix, with the help of their necessary properties semilattice $\Omega$ is built. The lattice of fully invariant subgroups of the group $G^\bullet$ is isomorphic to the lattice of filters of semilattice $\Omega$.

References


A. Tsereteli State University, 59, Tamar Mepe st., Kutaisi, 4600, Georgia
kemoklidze@gmail.com
Polytope method over rings containing non zero-divisors
Fatih Koyuncu

For any field $F$, there is a relation between the factorization of a polynomial $f \in F[x_1, ..., x_n]$ and the integral decomposition, with respect to Minkowski sum, of the Newton polytope of $f$. We extended this result to polynomial rings $R[x_1, ..., x_n]$ for an arbitrary ring $R$ containing non zero-divisors.

References

Muğla University, Department of Mathematics
fatih@mu.edu.tr

Locally derivations and locally isomorphisms of matrix rings
V. M. Levchuk

A bijective linear map $\psi$ of an arbitrary algebra $A$ is said to be a local isomorphism if it acts on each element $v \in A$ as a suitable isomorphism of $A$. Also $\psi$ is said to be a proper local isomorphism if is an isomorphism of $A$. Similarly we define local automorphisms and local derivations of algebras and rings, see [1], [2], [3]. For the algebra of certain triangular complex $3 \times 3$ matrices R. Crist [4] constructed examples of a proper local automorphisms.

Let $K$ be an associative ring with the identity and $\Gamma$ be an arbitrary linear ordered set. We study local derivations and local isomorphisms of certain rings of finitary $\Gamma$-matrices $\| a_{ij} \|_{i,j \in \Gamma}$ over $K$ (in particularly see [5], [6]) and also for the associated Lie and Jordan rings.

The work is supported by the Russian Foundation for Basic Research (grant 09-01-00717).

References
The undertaking

John Donne (1572–1631)

I HAVE done one braver thing
Than all the Worthies did;
And yet a braver thence doth spring,
Which is, to keep that hid.

It were but madness now to impart
The skill of specular stone,
When he, which can have learn’d the art
To cut it, can find none.

So, if I now should utter this,
Others—because no more
Such stuff to work upon, there is—
Would love but as before.

But he who loveliness within
Hath found, all outward loathes,
For he who color loves, and skin,
Loves but their oldest clothes.

If, as I have, you also do
Virtue in woman see,
And dare love that, and say so too,
And forget the He and She;

And if this love, though placèd so,
From profane men you hide,
Which will no faith on this bestow,
Or, if they do, deride;

Then you have done a braver thing
Than all the Worthies did;
And a braver thence will spring,
Which is, to keep that hid.
\textbf{$\mathcal{P}$-pure submodules and its relation with neat and coneat submodules}

Engin Mermut

Let $R$ be an arbitrary ring with unity. Take all modules to be \textit{left} $R$-modules.

A subgroup $A$ of an abelian group $B$ is said to be a neat subgroup if $A \cap pB = pA$ for all prime numbers $p$ ([3], [1, p. 131]). This is a weakening of the condition for being a pure subgroup. There are several reasonable ways to generalize this concept to modules.

Following Stenström ([6, 9.6] and [5, §3]), we say that a submodule $A$ of an $R$-module $B$ is neat in $B$ if for every simple module $S$, the sequence $\text{Hom}(S, B) \to \text{Hom}(S, B/A) \to 0$ obtained by applying the functor $\text{Hom}(S, -)$ to the canonical epimorphism $B \to B/A$ is exact.

Another natural generalization of neat subgroups is what is called $\mathcal{P}$-purity. Denote by $\mathcal{P}$ the collection of all \textit{left primitive ideals} of the ring $R$. We say that a submodule $A$ of an $R$-module $B$ is $\mathcal{P}$-pure in $B$ if $A \cap PB = PA$ for all $P \in \mathcal{P}$. In [4], the relation of $\mathcal{P}$-purity with complements and supplements have been used to describe the structure of $c$-injective modules over Dedekind domains.

A natural question to ask is when neatness and $\mathcal{P}$-purity coincide. Suppose that the ring $R$ is commutative. Then $\mathcal{P}$ is the collection of all \textit{maximal ideals} of $R$. Recently Fuchs ([2]) has characterized the commutative domains for which these two notions coincide. Fuchs calls a ring $R$ to be an $N$-domain if $R$ is a commutative domain such that neatness and $\mathcal{P}$-purity coincide. Unlike expected, Fuchs shows that $N$-domains are not just Dedekind domains. For a commutative domain $R$, Fuchs proves that $R$ is an $N$-domain if and only if all maximal ideals of $R$ are projective (and so all maximal ideals are invertible ideals and finitely generated). We slightly generalize this result by taking instead of domains commutative rings $R$ such that every maximal ideal contains a regular element so that the ideals of $R$ that are invertible in the total quotient ring of $R$ will be just projective ones as in the case of commutative domains. On the way, we also obtain some properties for a dual concept to neat: coneat submodules. A monomorphism $f : K \to L$ is called coneat if each module $M$ with $\text{Rad } M = 0$ is injective with respect to it, that is, the hom sequence $\text{Hom}(L, M) \to \text{Hom}(K, M) \to 0$ obtained by applying the functor $\text{Hom}(-, M)$ to the monomorphism $f : K \to L$ is exact. We use a description of coneat short exact sequences to show that over commutative \textit{small rings} (these are the rings such that the radical of every injective module is itself), the splitting of every coneat short exact sequence ending with a simple module implies that all simple modules have projective dimension $\leq 1$ (that is every maximal ideal is projective).

\textbf{References}


On extensions of a valuation on $K$ to $K(x)$

Figen Öke

Let $v$ be a valuation of a field $K$, $G_v$ its value group and $k_v$ its residue field and $w$ be an extension of $v$ to $K(x)$. $w$ is called residual transcendental extension of $v$ if $k_w/k_v$ is a transcendental extension and $w$ is called residual algebraic extension of $v$ if $k_w/k_v$ is an algebraic extension. In this study residual transcendental and residual algebraic extensions of $v$ to $K(x)$ are represented.

References


Trakya University, Department of Mathematics, 22030 Edirne, TURKEY
figenoke@gmail.com
An application of strong Groebner basis to coding theory
Hakan Özadam

Let $GR(p^a, m)$ be the Galois ring with characteristic $p^a$ and cardinality $p^{am}$. Since $GR(p^a, m)[x]$ is not a principal ideal ring, the study of the ideal structure of $\frac{GR(p^a, m)[x]}{(x^N-1)}$, and therefore the study of cyclic codes of length $N$ over $GR(p^a, m)$, is much more complicated compared to the case of cyclic codes over finite fields. This motivates applying the theory of Groebner basis to cyclic codes over Galois rings. It is well-known that the classical theory of Groebner basis can be extended to the theory of Groebner basis over rings. In [1], the authors introduce a special type of Groebner basis over principal ideal rings which they call strong Groebner basis. Given a cyclic code of length $N$ over $GR(p^a, m)$, which is an ideal of $\frac{GR(p^a, m)[x]}{(x^N-1)}$, it has been explained in [2] and [3] how to determine the minimum Hamming distance of $C$, using strong Groebner basis. Recently, Lopez-Permouth, Özadam, Özbudak and Szabo determined the minimum Hamming distance of certain constacyclic codes of length $np^s$ over $GR(p^a, m)$ via strong Groebner basis in [4]. In this talk, I will give an overview of this result.

References

Middle East Technical University
ozhakan@metu.edu.tr

Cotorsion modules and pure-injectivity
Dilek Pusat-Yılmaz

A module $C$ is called cotorsion if $\text{Ext}^1(F,C) = 0$ for any flat module $F$. We show that any cotorsion module satisfies a compactness condition on certain finite definition subgroups. Namely, those associated to divisibility conditions on pp-formulae in the First Order Logic of Modules. Using this characterization, we obtain a new proof of the fact that the endomorphism ring of any flat cotorsion module is f-semiperfect and idempotents
We apply these results to the particular case of hereditary rings and obtain conditions that force a hereditary ring to be semiperfect in terms of the presentation of its cotorsion envelope.

Joint work with Deniz Erdemirci and Pedro Guil Asensio.

References


Izmir Institute of Technology
dilekyilmaz@iyte.edu.tr

Soft near-rings

Aslıhan Sezgin

This is a joint work with Akın Osman Atagün. Soft set theory, which can be used as a new mathematical tool for dealing with uncertainty was introduced by Molodtsov. In this paper, we indicate the study of soft near-rings by using Molodtsov’s definition of the soft sets. The notions of soft near-rings, soft subnear-rings, soft (left, right) ideals, (left, right) idealistic soft near-rings and soft near-ring homomorphisms are introduced. Moreover, several related properties are investigated and illustrated by a great deal of examples.

Department of Mathematics, Bozok University, 66100, Yozgat, Turkey
aslihan.sezgin@bozok.edu.tr
Decomposability of \((1, 2)\)-Groups

Ebru Solak

A torsion free abelian group of finite rank is called almost completely decomposable if it has a completely decomposable subgroup of finite index. A \(p\)-local, \(p\)-reduced almost completely decomposable group of type \((1, 2)\) is briefly called a \((1, 2)\)-group. Almost completely decomposable groups can be represented by matrices over the ring \(\mathbb{Z}_h = \mathbb{Z}/h\mathbb{Z}\), where \(h\) is the exponent of the regulator quotient. This particular choice of representation allows for a better investigation of the decomposability of the group. Arnold and Dugas showed in several of their works that \((1, 2)\)-groups with regulator quotient of exponent at least \(p^7\) allow infinitely many isomorphism types of indecomposable groups. It is not known if the exponent 7 is minimal.

References


Middle East Technical University, Department of Mathematics, 06531 Ankara, Turkey
esolak@metu.edu.tr
www.metu.edu.tr/~esolak/

MacWilliams identity for M-spotty weight enumerators of linear codes over the finite fields \(GF(q)\)

Vedat Şiap

Some of the error control codes applies to high-speed memory systems using RAM chips with either 1-bit I/O data \((b = 1)\) or either 4-bit I/O data \((b = 4)\). However, modern large-capacity memory systems use RAM chips with 8, 16, or 32 bits of I/O data. A new class of codes called m-spotty byte error codes provides good source for correcting / detecting in those memory systems that use high density RAM chips with wide I/O data (e.g. 8, 16, or 32 bits). The MacWilliams identity provides the relation of weight distribution of a code and that of its dual code. This paper presents the MacWilliams identity for m-spotty weight enumerators of linear codes over the finite fields \(GF(q)\).

This is a joint work with M. ÖZEN ozen@sakarya.du.tr.
References


Sakarya University Arts and Science Faculty Department of Mathematics 54187 Esentepe Campus Serdivan/SAKARYA
vsiap@sakarya.edu.tr

Equiprime ideals of near-ring modules

Funda Taşdemir

This is a joint work with Akın Osman Atagün and Hüseyin Altındiş. In this paper we introduce the notion of equiprime $N$-ideals (ideals of near-ring modules) where $N$ is a near-ring. We consider the interconnections of equiprime, 3-prime and completely prime $N$-ideals. The relationship between an equiprime $N$-ideal $P$ of an $N$-group $\Gamma$ and the ideal $(P : \Gamma)$ of the near-ring $N$ is also investigated.

Department of Mathematics, Bozok University, 66100, Yozgat, Turkey
funda.tasdemir@bozok.edu.tr
On the relationship between Fibonacci length of its extensions and dicyclic group

Yasemin Taşyurdu

This paper is concerned with the relationship between $\text{Dic}_n$ dicyclic group and Fibonacci lengths of the cyclic groups which are extension of $\text{Dic}_n$ dicyclic group for $n = 2^k$. Also, we showed that $\text{LEN}(C_m + 1) = \text{LEN}(C_m)$ for $m = p^s$, $p$ is prime ; $s \in \mathbb{Z}^+$

This is joint work with İnci GÜLTEKİN.

References


Atatürk University, Science Faculty, Department of Mathematics, 25240 Erzurum, Turkey
yasemintasyurdu@hotmail.com.tr

On cofinitely supplemented lattices

S. Eylem Toksoy

$L$ will mean a complete modular lattice with smallest element $0$ and greatest element $1$. A lattice $L$ is said to be supplemented if every element $a$ of $L$ has a supplement in $L$, i.e. an element $b$ such that $a \lor b = 1$ and $a \land b \ll b/0$. An element $c$ of a complete lattice $L$ is said to be compact if for every subset $X$ of $L$ with $c \leq \lor X$ there exists a finite subset $F$ of $X$ such that $c \leq \lor F$. A lattice $L$ is called a compact lattice if $1$ is compact and a compactly generated lattice if each of its elements is a join of compact elements. An element $a$ of a lattice $L$ is said to be cofinite in $L$ if the quotient sublattice $1/a$ is compact. A lattice $L$ is called a cofinitely supplemented lattice if every cofinite element of $L$ has a supplement in $L$.

For compactly generated compact lattices a supplement of an element is compact (see [2, Proposition 12.2 (2)]). In the following proposition we show that for an arbitrary lattice $L$ a supplement of a cofinite element is compact.
Proposition 1. Let $a$ be a cofinite element of a lattice $L$ and $b$ be a supplement of $a$. Then $b/0$ is compact.

Theorem 2. (cf. [3, Theorem 5.3.33]) A lattice $L$ is a cofinitely supplemented lattice if and only if every maximal element of $L$ has a supplement in $L$.

Theorem 1 is used in the proof of the following theorem which gives a new result for modules.

Theorem 3. If $a/0$ is a cofinitely supplemented sublattice of $L$ and $1/a$ has no maximal element, then $L$ is also a cofinitely supplemented lattice.

Corollary 4. Let $M$ be a module, $N$ be a cofinitely supplemented submodule of $M$. If $\text{Rad}(M/N) = M/N$, then $M$ is cofinitely supplemented.

Joint work with: Refail Alizade, İzmir Institute of Technology
e-mail: rafailalizade@iyte.edu.tr

References


İzmir Institute of Technology
eylemtoksoy@iyte.edu.tr
www.iyte.edu.tr/~eylemtoksoy
Posters

Speeding up Montgomery modular multiplication for prime fields
Sedat Akleylek, Murat Cenk

We give faster versions of Montgomery modular multiplication algorithm without precomputational phase for $GF(p^m)$, where $p$ is prime and $m > 1$, which can be considered as a generalization of [1], [2] and [3]. We propose sets of moduli which can be used in public key cryptographic applications. We eliminate pre-computational phase with proposed sets of moduli. We show that these methods are easy to implement for hardware.

References


Middle East Technical University and Ondokuz Mayıs University
akleylek@metu.edu.tr

Middle East Technical University
mcenk@metu.edu.tr
Pseudorandom sequences over finite fields

Esen Aksoy

We consider the permutation polynomial $P_n(x) = (x^{q-2} + a_1)^{q-2} + a_2)^{q-2} + \cdots + a_n(x^{q-2} + a_n$ of $\mathbb{F}_q$, where $P_0(x) = x$, $P_{n+1}(x) = P_n(x)^{q-2} + a_{n+1}$ for $n \geq 0$ as in [1] and define a sequence $(u_n)_{n \geq 0}$ with $u_n = P_n(u_0)$. If the sequence $(a_n)$ is periodic and $\text{per}(a_n) = t$, then $\text{per}(u_n)$ depends on the cycle structure of $P_t(x)$, and the starting value $u_0$. In particular, if $P_t$ has full cycle structure, then the sequence $(u_n)$ is balanced and $\text{per}(u_n) = pt$ for all initial values $u_0 \in \mathbb{F}_q$.

References


Sabancı University
eaksoy@sabanciuniv.edu

On ramification in extensions of rational function fields

Nurdagül Anbar

Let $K(x)$ be a rational function field, which is a finite separable extension of the rational function field $K(z)$. In the first part, we have studied the number of ramified places of $K(x)$ in $K(x)/K(z)$. Then we have given a formula for the ramification index and the different exponent in the extension $F(x)$ over a function field $F$, where $x$ satisfies an equation $f(x) = z$ for some $z \in F$ and separable polynomial $f(x) \in K[x]$. In fact, this generalizes the well-known formulas for Kummer and Artin-Schreier extensions.

References


Sabancı University
nurdagul@sabanciuniv.edu
Drinfeld modular curves with many rational points over finite fields

Vural Cam

For some kinds of reasons one is interested to construct curves which have many rational points over a finite field. Drinfeld modular curves can be used to construct that kinds of curves over a finite field. In my work I am using reductions of the Drinfeld modular curves $X_0(n)$ with suitable primes to get such nice curves. The main idea is to divide the Drinfeld modular curves by an Atkin-Lehner involution which has many fixed points to obtain a quotient with a better ratio \(\text{number of rational points}/\text{genus}\).

Metu
cvural@metu.edu.tr

Polynomial multiplication over finite fields

Murat Cenk

Let $q$ be a prime power and $\mathbb{F}_q$ be the finite field with $q$ elements. Let $n$ and $\ell$ be positive integers and $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ such that $\ell \deg(f(x)) < 2n - 1$. We obtain an effective upper bound for the multiplication complexity of $n$-term polynomials modulo $f(x)^\ell$. This upper bound allows a better selection of the moduli when Chinese Remainder Theorem is used for polynomial multiplication over $\mathbb{F}_q$. We give improved formulas to multiply polynomials of small degree over $\mathbb{F}_2$ and $\mathbb{F}_3$. In particular, we improve the best known multiplication complexities over $\mathbb{F}_2$ and $\mathbb{F}_3$ in the literature in some cases.

Middle East Technical University
mcenk@metu.edu.tr

Quantum groups

Münevver Çelik

$R$-matrices are solutions of the Yang-Baxter equation. They give rise to link invariants. $R$-matrices are derived from a special kind of Hopf algebra, namely quantum group. In this work, I will define quantum groups and present the way to derive link invariants from $R$-matrices.

METU
mucelik@metu.edu.tr
A remark on permutations with full cycle
Ayça Çeşmelioğlu

For $q > 2$, Carlitz proved in [1] that the group of permutation polynomials (PPs) over $\mathbb{F}_q$ is generated by the linear polynomials and $x^{q-2}$. Based on this result, we point out a simple method for representing all PPs with full cycle over the prime field $\mathbb{F}_p$, where $p$ is an odd prime. We use the isomorphism between the symmetric group $S_p$ of $p$ elements and the group of PPs over $\mathbb{F}_p$, and the well-known fact that permutations in $S_p$ have the same cycle structure if and only if are conjugate.

References


Sabancı Üniversitesi
cesmelioglu@sabanciuniv.edu
http://myweb.sabanciuniv.edu/acesmelioglu

On o-minimal structures
Şükrü Uğur Efem

A linearly ordered structure is said to be o-minimal if every definable subset of it is a finite union of intervals and points. The motivating example is the ordered field of reals. The notion of o-minimality was implicitly introduced in the eighties by Lou van den Dries who observed that many non-trivial properties of semi-algebraic sets follow from those simple axioms, and then developed further by Pillay and Steinhorn. In this poster we survey some known results and applications of o-minimality.

References


Sabancı Üniversitesi
suefem@sabanciuniv.edu
Maximal subgroups in Hall universal groups

Mehmet İnan Karakuş

In an infinite group, it is a difficult task to decide whether a maximal subgroup exist or not. It is a well known trivial example that the p-quasicyclic group (or Prüfer p-group, or $C_p^\infty$) has no maximal subgroup. A locally finite group $G$ is called a universal group (see [2]) if

1. Every finite group can be embedded in $G$
2. Any two isomorphic finite subgroups of $G$ are conjugate in $G$

We discuss the existence of maximal subgroups in locally finite universal groups. In particular there is a construction of a maximal p-subgroup which is also maximal subgroup of the group. The construction is due to M. Dalle Molle (see [1])

References


Middle East Technical University

minan@metu.edu.tr

Classification of finitary linear simple locally finite groups

Dilber Koçak

A group is called locally finite if every finitely generated subgroup is a finite group. $G$ is called a linear group if it is a subgroup of $GL(n, F)$ for some field $F$.

The classification of simple locally finite linear groups is completed independently by Belyaev, Borovik, Hartley-Shute and Thomas. They have proved:

**Theorem 1.** (*BBHST: Belyaev, Borovik, Hartley, Shute, and Thomas* [1], [2], [4] and [5]). Each locally finite simple group that is not finite but has a faithful representation as a linear group in finite dimension over a field is isomorphic to a Lie type group $\Phi(K)$, where $K$ is an infinite, locally finite field, that is, an infinite subfield of $\mathbb{F}_p$, for some prime $p$. 
A group of linear transformations is called finitary if each element minus the identity is an endomorphism of finite rank. Then observe that every linear locally finite simple group is a finitary linear simple locally finite group. Recently the classification of finitary simple locally finite groups are completed by J. I. Hall in [3].

**Theorem 2.** (Hall). A locally finite simple group that has a faithful representation as a finitary linear group is isomorphic to one of:

1. a linear group in finite dimension;
2. an alternating group $\text{Alt}(\Omega)$ with $\Omega$ infinite;
3. a finitary symplectic group $F\text{Sp}_K(V,s);$
4. a finitary special unitary group $F\text{SU}_K(V,u);$
5. a finitary orthogonal group $F\Omega_K(V,q);$
6. a finitary special linear group $F\text{SL}_K(V,W,m).$

Here $K$ is a (possibly finite) subfield of $\mathbb{F}_p$, the algebraic closure of the prime subfield $\mathbb{F}_p$. The forms $s,u,$ and $q$ are nondegenerate on the infinite dimensional $K$-space $V$; and $m$ is a nondegenerate pairing of the infinite dimensional $K$-spaces $V$ and $W$. Conversely, each group in (2)-(6) is locally finite, simple, and finitary but not linear in finite dimension.

**References**


*METU*

dilber@metu.edu.tr
On stability of free products in bounded balls

Azadeh Neman

In a series of papers, Z. Sela proved that free groups, and more generally torsion-free hyperbolic groups, have a stable first-order theory. It has been conjectured by E. Jaligot [2] that the free product of two arbitrary stable groups is stable. However, a full answer seems to become a very large project of generalization, from free groups to free products, of the famous articles of Sela. Until this monumental task is done, we provide a very preliminary result in the direction of the stability of free products of stable groups, restricting ourselves to quantifer-free definable sets and to bounded balls of free products and including finite amalgamation.

References

[1] A. Neman. Stability and bounded balls of free products, Accepted


[3] W. Magnus, A. Karrass and D. Solitar Combinatorial group theory. Presentations of groups in terms of generators and relations

Istanbul Bilgi University

azadeh.neman@gmail.com
Automorphism groups of generalized Giulietti–Korchmaros curves

Mehmet Özdemir

Giuletti and Korchmaros introduced a new example of a maximal curve which is not covered by the Hermitian curve [1]. Their curve is defined over $GF(q^6)$ for some prime power $q$. Later, Garcia, Güneri and Stichtenoth introduced a family of maximal curves over $GL(q^{2n})$ for a prime $q$ and an odd integer $n \geq 3$ [3]. Amongst these curves the one with $n = 3$ coincides with the curve of Giuletti and Korchmaros, and for $n > 3$ it is not known yet whether these curves are covered by the Hermitian curve. The automorphism group of Giuletti-Korchmaros curve is known, and Fanali and Giuletti found some subfields of this curve corresponding to some subgroups of its automorphism group [2]. The question is what is the automorphism group of Generalized Giuletti-Korchmaros curves for $n > 3$ and how to find subfields of these curves corresponding to subgroups of their automorphism groups and what are the genera of these subfields.

References


Sabancı University
mehmetozdemir@su.sabanciuniv.edu
Low-density-parity-check codes

Buket Özkaya

Low-density-parity-check (LDPC) codes were first proposed in the PhD thesis of Gallager at MIT, in 1962. They remained largely neglected for over 35 years due to the computational difficulties at that time, which didn’t allow to discover their elegant properties. After their rediscovery in 1996, they became one of the most popular research topics of coding and information theory, which also yield many applications in the fields like telecommunication, signal processing, statistical physics etc. The aim of my work was to survey the main concerning approaches and to express them in an unified mathematical language, which would let the subject not only to be understood in a systematic way, but also to be a brief collective tutorial about LDPC codes. After a summary of the most important tasks of coding and information theory, various techniques of LDPC-code constructions are presented in matrix and graph representations, following the historical progression. Their properties are explained in algebraic and combinatorial terms such as their minimal distance can achieve Gilbert-Varshamow bound exponentially and with an optimal decoding the code rate approaches the channel capacity, which provides a constructive proof to the Shannon’s theorem. The decoding algorithms used for LDPC codes belong to the class of message passing algorithms. They are iterative and rely on binary or probabilistic decisions about the bit values of the codeword which is sent through a noisy channel. The analysis of the algorithm is carried out by the process called density evolution, which intends to determine a threshold of channel noise for a given LDPC-code ensemble so that the message passing decoder is able to correct the possible errors successfully.

References


Sabancı University

buketo@sabanciuniv.edu
Numbers and sets

David Pierce

This is about an analogy between numbers and sets that is highlighted when one generalizes both.

Dedekind [1] identified the properties that determine the set \( \mathbb{N} \) of natural numbers as an algebraic structure, \((\mathbb{N}, 1, S)\):

1. There is a distinguished initial natural number \( 1 \);
2. Each natural number \( n \) has a successor, \( S(n) \);
3. \( 1 \) is not a successor;
4. No two numbers have the same successor;
5. Proof by induction is possible.

These properties are often named for Peano [2], perhaps because he gave them a symbolic formulation; but his understanding of them was apparently less profound than Dedekind’s. In any case, their import is that \( \mathbb{N} \) is a free algebra in the signature \( \{1, S\} \).

Von Neumann [3] gave a set-theoretic definition of the class \( \text{ON} \) of ordinal numbers. This class is well-ordered by membership (\( \in \)); it can also be understood as an algebraic structure, \( (\text{ON}, \emptyset, x \mapsto x \cup \{x\}) \); this has the substructure \( (\omega, \emptyset, x \mapsto x \cup \{x\}) \), which is isomorphic to \( (\mathbb{N}, 1, S) \). The isomorphism suggests an analogy:

There are two kinds of numbers: 1 and the successors.
There are two kinds of sets: empty and not.
The operation of succession takes a single argument.
Sets contain their elements in only one way.

If one allows sets to have various “types” (beyond “empty” and “nonempty”), and one allows sets to have various “grades” of elements, then, in any algebraic signature, there is a set-theoretic construction of a free algebra analogous to \( \omega \); this is embedded in an ordered class analogous to \( \text{ON} \).

References


METU
dpierce@metu.edu.tr
http://metu.edu.tr/~dpierce/
Monomial Gotzmann sets in a quotient by a pure power
Ata Fırat Pir

We study Gotzmann sets in a quotient $R = F[x_1, \ldots, x_n]/(x_1^a)$ of a polynomial ring over a field $F$. These are monomial sets whose sizes grow minimally when multiplied with the variables. We partition the set of monomials in a Gotzmann set with respect to the multiplicity of $x_1$ and show that if the size of a component in a partition is sufficiently large, then this component is a multiple of a Gotzmann set in $F[x_2, \ldots, x_n]$. Otherwise we derive lower bounds on the size of a component depending on neighboring components.

For $n = 3$, we classify all Gotzmann sets in $R$ and for a given degree, we compute all integers $j$ such that the only Gotzmann set in that degree is the lexsegment set of size $j$. We also note down adoptions of some properties concerning the minimal growth of the Hilbert function in $F[x_1, \ldots, x_n]$ to $R$.

Bilkent University
pir@fen.bilkent.edu.tr

On the number of Boolean functions satisfying strict avalanche criteria
Elif Saygı

Boolean functions play an important role in the design of both block and stream ciphers. In this work, the number of Boolean functions satisfying strict avalanche criteria are considered. Also, the number of functions with particular difference distribution vectors is studied. The exact formula for a special case is given. Results of some statistical observations are compared to the exact values.

This is a joint work with Ali Doğanaksoy and Zülfükar Saygı.

Hacettepe University
esaygi@hacettepe.edu.tr
Quadratic feedback shift registers and maximum length sequences
Zülfükar Saygı

In this work, the properties of the quadratic feedback shift registers generating maximum length sequences are considered. Some necessary conditions for a quadratic feedback function $f$ of a feedback shift register to generate a maximum length sequence is given. Also a method generalizing this condition is presented. Instead of searching all the sequence, looking at the algebraic normal form of the function $f$ one can understand if the corresponding shift register generates a sequence having short period.

This is a joint work with Elif Saygı and Ali Doğanaksoy.

TOBB University of Economics and Technology
zsaygi@etu.edu.tr
http://zsaygi.etu.edu.tr/

Recursive towers of function fields over finite fields
Seher Tutdere

In 1995 Garcia and Stichtenoth gave explicit constructions of towers of function fields over the finite field $\mathbb{F}_q$. Moreover, in the case that $q = p^k$ (for $k \geq 2$ and $p$ is a prime) they have given some examples of towers having positive limit which are called asymptotically good and optimal towers (see [1, 2]). Now we deal with the following problem: Are there any such towers of function fields over the prime fields $\mathbb{F}_p$ for any prime $p$? If so, then how to define polynomials which give such nice towers?

References

Sabancı University
sehertutdere@su.sabanciuniv.edu
Regulators on $K_1$ of product of elliptic curves
İnan Utku Türkmen

Spencer Bloch defined and studied the properties of higher Chow groups, $CH^\bullet(X, m)$, in his seminal work [Blo] and established the relation between these groups and higher K theory which is known as Bloch’s version of Grothendieck Reimann Roch theorem;

$$K_m(X) \otimes \mathbb{Q} \simeq CH^\bullet(X, m) \otimes \mathbb{Q}.$$ 

Both higher K groups and higher Chow groups are complicated objects and it is hard to compute them, so they are studied by mappings to more computable cohomology theories. These maps are named regulators.

In this work, we are going to give a brief introduction to subject, defining the basic objects and methods in the literature and present our results on higher Chow groups of sufficiently general product of elliptic curves and regulator maps to Deligne cohomology.

This work has been carried out under the supervision of Prof. James D. Lewis from University of Alberta.

References


Bilkent University

turkmen@fen.bilkent.edu.tr
Participants

1. Sedat Akleylek akleylek@metu.edu.tr
2. Esen Aksoy eaksoy@su.sabanciuniv.edu
3. Emine Albaş emine.albas@ege.edu.tr
4. Tüna Altınel altinel@math.univ-lyon1.fr
5. Nurdağül Anbar
6. Nurcan Argaç nurcan.argac@ege.edu.tr
7. Ahmet Arıkan arikan@gazi.edu.tr
8. Ayşen Arkan
9. Ali Osman Asar
10. Fırat Ateş firat@balikesir.edu.tr
11. Alp Bassa Alp.Bassa@cwi.nl
12. Oleg Belegradek obolegradek@rambler.ru
13. Ayşe Berkman mehpare@metu.edu.tr
14. Mehpare Bilhan
15. Tengiz Bokelavadze boke171@yahoo.com
16. Ines Borges iborges@isac.pt
17. Alexandre Borovik borovik@manchester.ac.uk
18. Ayşe Büte ayse.bute@stu.edu.tr
19. Engin Büyükaşık enginbuyukasik@iyte.edu.tr
20. Vural Cam cvural@metu.edu.tr
21. Murat Cenk mcenk@metu.edu.tr
22. Pascale Charpin Pascale.Charpin@inria.fr
23. Kutay Cingiz
24. Şermim Çam mucelik@metu.edu.tr
25. Münever Çelik
26. Fatih Çelik
27. Türkü Özlim Çelik
28. Yasemin Çengellenmiş ycengellenmis@yahoo.com
29. Ayça Çesmeoğlu cesmelioglu@sabanciuniv.edu
30. Ahmet Sinan Çevik sinan.cevik@selcuk.edu.tr
31. Gülens Çevik gulencevik@gmail.com
32. Büşra Çınar e147988@metu.edu.tr
33. Derya Çıray
34. Ömür Deveci odeveci36@hotmail.com
35. Uğur Doğan sdogruoz@adu.edu.tr
36. Semra Doğruöz yilmazdurgun@iyte.edu.tr
37. Yılmaz Durğun suefem@sabanciuniv.edu
38. Şükrü Uğur Efem oejder@ku.edu.tr
39. Özlem Ejder
40. Ceyhun Erdel erdogdu@itu.edu.tr
41. Vahap Erdoğan garcia@impa.br
42. Arnaldo García
<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>87</td>
<td>Buket Özkaya</td>
<td><a href="mailto:buketo@sabanciuniv.edu">buketo@sabanciuniv.edu</a></td>
</tr>
<tr>
<td>88</td>
<td>Neslihan Ayşen Özkirişçi</td>
<td><a href="mailto:aysen.1007@gmail.com">aysen.1007@gmail.com</a></td>
</tr>
<tr>
<td>89</td>
<td>Daniel Panario</td>
<td>daniel.math.carleton.ca</td>
</tr>
<tr>
<td>90</td>
<td>David Pierce</td>
<td><a href="mailto:dpierce@metu.edu.tr">dpierce@metu.edu.tr</a></td>
</tr>
<tr>
<td>91</td>
<td>Ata Furat Pir</td>
<td><a href="mailto:atafirat@gmail.com">atafirat@gmail.com</a></td>
</tr>
<tr>
<td>92</td>
<td>Övgür Deniz Polat</td>
<td><a href="mailto:polat@su.sabanciuniv.edu">polat@su.sabanciuniv.edu</a></td>
</tr>
<tr>
<td>93</td>
<td>Alexander Pott</td>
<td><a href="mailto:alexander.pott@ovgu.de">alexander.pott@ovgu.de</a></td>
</tr>
<tr>
<td>94</td>
<td>Peter Roquette</td>
<td><a href="mailto:rueck@mathematik.uni-kassel.de">rueck@mathematik.uni-kassel.de</a></td>
</tr>
<tr>
<td>95</td>
<td>Hans-Georg Rück</td>
<td><a href="mailto:mathematicianesen@gmail.com">mathematicianesen@gmail.com</a></td>
</tr>
<tr>
<td>96</td>
<td>Esengül Saltürk</td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>Mehmet Sariyüce</td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>Zülfükar Saygı</td>
<td><a href="mailto:sariyuce@sabanciuniv.edu">sariyuce@sabanciuniv.edu</a></td>
</tr>
<tr>
<td>99</td>
<td>Elif Saygı</td>
<td><a href="mailto:zsaygi@etu.edu.tr">zsaygi@etu.edu.tr</a></td>
</tr>
<tr>
<td>100</td>
<td>Ali Sinan Sertöz</td>
<td><a href="mailto:sertoz@bilkent.edu.tr">sertoz@bilkent.edu.tr</a></td>
</tr>
<tr>
<td>101</td>
<td>Sezgin Sezer</td>
<td><a href="mailto:sezer@fen.bilkent.edu.tr">sezer@fen.bilkent.edu.tr</a></td>
</tr>
<tr>
<td>102</td>
<td>Müfit Sezer</td>
<td><a href="mailto:sezer@bilkent.edu.tr">sezer@bilkent.edu.tr</a></td>
</tr>
<tr>
<td>103</td>
<td>Ashlan Sezgin</td>
<td><a href="mailto:sezgin@bilkent.edu.tr">sezgin@bilkent.edu.tr</a></td>
</tr>
<tr>
<td>104</td>
<td>Amin Shokrollahi</td>
<td><a href="mailto:sezgin.nearring@hotmail.com">sezgin.nearring@hotmail.com</a></td>
</tr>
<tr>
<td>105</td>
<td>Patrick Smith</td>
<td><a href="mailto:amin.shokrollahi@epfl.ch">amin.shokrollahi@epfl.ch</a></td>
</tr>
<tr>
<td>106</td>
<td>Ebru Solak</td>
<td><a href="mailto:p.smith@maths.gla.ac.uk">p.smith@maths.gla.ac.uk</a></td>
</tr>
<tr>
<td>107</td>
<td>Henning Stichtenoth</td>
<td><a href="mailto:esolak@metu.edu.tr">esolak@metu.edu.tr</a></td>
</tr>
<tr>
<td>108</td>
<td>Vedat Şiap</td>
<td><a href="mailto:henning@sabanciuniv.edu">henning@sabanciuniv.edu</a></td>
</tr>
<tr>
<td>109</td>
<td>Funda Taşdemir</td>
<td><a href="mailto:vsiap@sakarya.edu.tr">vsiap@sakarya.edu.tr</a></td>
</tr>
<tr>
<td>110</td>
<td>Yasemin Taşıyurdu</td>
<td><a href="mailto:funda.tasdemir@bozok.edu.tr">funda.tasdemir@bozok.edu.tr</a></td>
</tr>
<tr>
<td>111</td>
<td>Kadiyie Dilek Tefenilii</td>
<td><a href="mailto:yasemintasyurdu@hotmail.com">yasemintasyurdu@hotmail.com</a></td>
</tr>
<tr>
<td>112</td>
<td>Eylem Toksoy</td>
<td><a href="mailto:eylemtoksoy@iyte.edu.tr">eylemtoksoy@iyte.edu.tr</a></td>
</tr>
<tr>
<td>113</td>
<td>Alev Topuzoğlu</td>
<td><a href="mailto:alev@sabanciuniv.edu">alev@sabanciuniv.edu</a></td>
</tr>
<tr>
<td>114</td>
<td>Meral Tosun</td>
<td><a href="mailto:mtosun@gsu.edu.tr">mtosun@gsu.edu.tr</a></td>
</tr>
<tr>
<td>115</td>
<td>Nesrin Tutas</td>
<td><a href="mailto:ntutas@akdeniz.edu.tr">ntutas@akdeniz.edu.tr</a></td>
</tr>
<tr>
<td>116</td>
<td>Seher Tutdere</td>
<td><a href="mailto:sehertutdere@sabanciuniv.edu">sehertutdere@sabanciuniv.edu</a></td>
</tr>
<tr>
<td>117</td>
<td>Erkan Murat Türkcan</td>
<td><a href="mailto:turkmen@fen.bilkent.edu.tr">turkmen@fen.bilkent.edu.tr</a></td>
</tr>
<tr>
<td>118</td>
<td>İnan Utku Türkmen</td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>Özte Ülkem</td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>Wolfgang Willems</td>
<td><a href="mailto:willems@ovgu.de">willems@ovgu.de</a></td>
</tr>
<tr>
<td>121</td>
<td>Arne Winterhof</td>
<td><a href="mailto:arne.winterhof@oeaw.ac.at">arne.winterhof@oeaw.ac.at</a></td>
</tr>
<tr>
<td>122</td>
<td>Firat Yaşar</td>
<td><a href="mailto:hyazarli@cumhuriyet.edu.tr">hyazarli@cumhuriyet.edu.tr</a></td>
</tr>
<tr>
<td>123</td>
<td>Hasret Yazarlı</td>
<td><a href="mailto:dilekylimaz@iyte.edu.tr">dilekylimaz@iyte.edu.tr</a></td>
</tr>
<tr>
<td>124</td>
<td>Dilek Pusat Yılmaz</td>
<td><a href="mailto:sergey.zyubin@gmail.com">sergey.zyubin@gmail.com</a></td>
</tr>
<tr>
<td>125</td>
<td>Sergey Zyubin</td>
<td></td>
</tr>
</tbody>
</table>
Personnel

**Meeting coordinator** Alev Topuzoğlu (Sabancı)

**Scientific committee** Mahmut Kuzucuoğlu (METU), Ali Nesin (Bilgi), Sinan Sertöz (Bilkent), Henning Stichtenoth (Sabancı), Simon Thomas (Rutgers)

**Organizing committee** Ayşe Berkman (METU), Cem Güneri (Sabancı), David Pierce (METU), Henning Stichtenoth (Sabancı)

**Booklet editor** David Pierce

Acknowledgements

**Hospitality** Tivrona Tours

**Venue** Antalya Oteli, Lara Yolu, Antalya

**Financial support** TÜBİTAK (the Scientific and Technological Research Council of Turkey), the Turkish Mathematical Association, Sabancı University

**Website** [http://aad.metu.edu.tr/](http://aad.metu.edu.tr/)
### Short talks

#### Wednesday

<table>
<thead>
<tr>
<th>Time</th>
<th>Session I</th>
<th>Session II</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:50</td>
<td>Gürel</td>
<td>Asar</td>
</tr>
<tr>
<td>17:10</td>
<td>Öke</td>
<td></td>
</tr>
<tr>
<td>17:30</td>
<td>Özadam</td>
<td>Levchuk</td>
</tr>
<tr>
<td>17:50</td>
<td>Guil Asensio</td>
<td></td>
</tr>
</tbody>
</table>

#### Thursday

<table>
<thead>
<tr>
<th>Time</th>
<th>Session I</th>
<th>Session II</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:20</td>
<td>Sezgin</td>
<td>Güzeltepe</td>
</tr>
<tr>
<td>14:40</td>
<td>Taşdemir</td>
<td>Çengellenmiş</td>
</tr>
<tr>
<td>15:00</td>
<td>Durğun</td>
<td>Şiap</td>
</tr>
<tr>
<td>16:50</td>
<td>Bokelavadze</td>
<td>Gezer</td>
</tr>
<tr>
<td>17:10</td>
<td>Çevik</td>
<td>S. Güngör</td>
</tr>
<tr>
<td>17:30</td>
<td>Solak</td>
<td>Büyükaşık</td>
</tr>
<tr>
<td>17:50</td>
<td>Zyubin</td>
<td>Toksoy</td>
</tr>
</tbody>
</table>

#### Saturday

<table>
<thead>
<tr>
<th>Time</th>
<th>Session I</th>
<th>Session II</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:20</td>
<td>A. D. Güngör</td>
<td>Taşyurdu</td>
</tr>
<tr>
<td>14:40</td>
<td>Pusat-Yılmaz</td>
<td>Koyuncu</td>
</tr>
<tr>
<td>15:00</td>
<td>Karpuz</td>
<td></td>
</tr>
</tbody>
</table>