2017 Gaeta Fq13

The 13th International Conference on Finite Fields and their Applications

June 4–10, 2017

Hotel Serapo, Gaeta (It)

This online version of the book of abstract has been last updated on 25th June 2017. We invite all the participants to check that their data are correct and up to date.

Contents

Overview

Overview

Presentation

The 13th International Conference on Finite Fields and their applications takes place at Hotel Serapo in Gaeta, Italy, during the weed of June 4–10, 2017. The present booklet contains the list of the participants and the abstracts of the presentations which will be given during the conference.

Topics of interest include, but are not limited to:

- **Theory**: structure of finite fields, primitive elements, normal bases, polynomials, number-theoretic aspects of finite fields, character sums, function fields, APN functions.
- **Computation**: algorithms and complexity, polynomial factorization, decomposition and irreducibility testing, sequences and functions.
- **Applications**: algebraic coding theory, cryptography, algebraic geometry over finite fields, finite incidence geometry, designs, combinatorics, quantum information science.

Plenary speakers

- Massimo Giulietti -University of Perugia (IT)
- Daniel Katz -California State University (USA)
- Kristin Lauter -Microsoft Research (USA)
- Alev Topuzoğlu -Sabancı Üniversitesi (TR)
- Qiang Wang -Carleton University (CAN)
- Julia Wolf -University of Bristol (UK)
- Chao Ping Xing -Nanyang Technological University (SG)

Scientific committee

- Anne Canteaut (France)
- Gove Effinger (USA)
- Sophie Huczynska (UK)
- Guglielmo Lunardon (Italy, Chair)
- Gary Mullen (USA)
- Harald Niederreiter (Austria)
- Daniel Panario (Canada)
- Alexander Pott (Germany)
- Massimiliano Sala (Italy)
- Henning Stichtenoth (Turkey)
- Leo Storme (Belgium)

Organizing committee

- Francesco Belardo
- Giorgio Donati
- Nicola Durante
- Luca Giuzzi (webmaster)
- Giuseppe Marino
- Rocco Trombetti

Travel advice

- Gaeta is located on a peninsula about 58 miles north of Naples; for information about the local attractions and events we refer to the site of Proloco Gaeta.
- The closest train station to Gaeta is located in Formia and it is named Forma-Gaeta. It is reached by trains either from Rome or from Naples. For further information and tickets, we refer to the web site of trenitalia.
- There is a city bus running from Formia to Gaeta approximately every half an hour from 4.30am till 10.00pm; see the page of the operator. Observe that on sundays ("Festivi") the scheduled times are less frequent than on work-days ("Feriali").
- There are several licensed taxis connecting from Formia train station to the city of Gaeta; some operators are *Formia Taxi Service*, *Taxi Formia NCC*. It takes approximately 30 minutes by car to travel from the station to the hotel.
- A possible alternative is driving from Rome or Naples. Gaeta can be reached from Rome by Autostrada `A1/E45` (exit: Frosinone) and from Naples by Autostrada `A1/E45` (exit: Capua) and Strada Statale 7 via Appia.
- The closest international airports to Gaeta are in Naples and Rome.

Contacts

Email: `fq13@unina.it`

Rocco Trombetti (for the organizing committee)
Dipartimento di Matematica e Applicazioni "Renato Caccioppoli"
Università degli Studi di Napoli "Federico II"
Via Cintia, Monte S. Angelo
I-80126 Napoli (IT)

Programme

Sunday 4 June

17:30 – 20:00 Registration

Monday 5 June

Plenary talks

10:00 – 10:55 Kristin Lauter: "*How to Keep your Secrets in a Post-Quantum World*"

11:00 *Coffee Break*

11:35 – 12:30 Chaoping Xing: "*Three Combinatorial Problems in Theoretical Computer Science*"

13:00 *Lunch Break*

Contributed talks

	Session A	Session B
15:30 – 15:50	Gábor Korchmáros: "*Curves with large automorphism groups in positive characteristic*"	Roberto Civino: "*Generalised Round Functions for Block Ciphers*"
15:55 – 16:15	Daniele Bartoli: "*AG codes from the GK and the GGS curves*"	Domingo Gomez-Perez: "*On the expansion complexity and i-expansion complexity*"
16:20 – 16:40	Matteo Bonini: "*Minimal weight codewords of some codes from the GK curve*"	Sihem Mesnager: "*On the nonlinearity of Boolean functions with restricted input*"

16:40 *Coffee Break*

Contributed talks

	Session A	Session B
17:10 – 17:30	Jan De Beule: "*Blocking sets of Hall planes and value sets of polynomials over finite fields*"	Ariane Masuda: "*Collision-free bounds for the BSV hash*"
17:35 – 17:55	Francesco Pavese: "*Ovoids of $\mathcal{H}(3, q^2)$, q odd, admitting a group of order $\frac{(q+1)^3}{2}$*"	Yves Aubry: "*Second order differential uniformity*"
18:00 – 18:20	Maarten De Boeck: "*New families of KM-arcs*"	Violetta Weger: "*Weight Two Masking in the McEliece System*"

Tuesday 6 June

Plenary talks

09:00 – 9:55 Massimo Giulietti: "*Maximal Curves over Finite Fields*"

Contributed talks

	Session A	Session B
10:00 – 10:20	Giovanni Longobardi: "*Pre-sympletic semifields*"	Beatriz Motta: "*P-Chain Codes*"
10:25 – 10:45	Valentina Pepe: "*Symplectic semifield spreads of $PG(5, q)$, q even*"	Martino Borello: "*Symmetries of weight enumerators*"
10:50 – 11:10	Sam Mattheus: "*The (weak) cylinder conjecture and its reduction to a weight function in $AG(2, p)$*"	Leyla Ateş: "*On short vectors in function field lattices*"
11:15	*Coffee Break*	

Contributed talks

	Session A	Session B
11:40 – 12:00	Pietro Speziali: "*Automorphisms of even genus ordinary curves*"	Ka Hin Leung: "*Structure of Group Invariant Weighing Matrices of Small Weight*"
12:05 – 12:25	Maria Montanucci: "*$\mathbb{F}_{p^2}$-maximal curves with many automorphisms are Galois-covered by the Hermitian curve*"	Robert Granger: "*On the Enumeration of Irreducible Polynomials over $GF(q)$ with Prescribed Coefficients*"
12:30 – 12:50	Giovanni Zini: "*Generalized Artin-Mumford curves and their automorphisms*"	Christian Günther: "*L^α norms of polynomials derived from characters of finite fields*"
13:00	*Lunch Break*	

Tuesday 6 June

Contributed talks

	Session A	Session B
15:30 – 15:50	Simeon Ball: "*Arcs and the $\sqrt{q}$ conjecture*"	Megha Kolhekar: "*On Permutation Polynomial Representatives, their Matrices and their Inverses*"
15:55 – 16:15	Heriveldo Borges: "*Slices of Fermat Surfaces over Finite Fields and Curves with Many Points*"	Daniel Panario: "*The Graph Structure of Chebyshev Polynomials over Finite Fields*"
16:20 – 16:40	Luca Giuzzi: "*Hermitian Line Polar Grassmann Codes*"	Simone Ugolini: "*On some iterative constructions of irreducible polynomials over finite fields*"
16:40	*Coffee Break*	

Contributed talks

	Session A	Session B
17:10 – 17:30	Gábor P. Nagy: "*On the computer algebra implementation of Hermitian codes*"	Longjiang Qu: "*New Constructions of Permutation Polynomials with the Form of $xh\left(x^{q-1}\right)$ over $\mathbb{F}_{q^2}$*"
17:35 – 17:55	Mark Pankov: "*Isometric embeddings of Johnson graphs in Grassmann graphs and generalized arcs*"	Arne Winterhof: "*Carlitz rank and index of permutation polynomials*"
18:00 – 18:20	Angela Aguglia: "*On singular quasi-Hermitian varieties*"	Giacomo Michelin: "*Regular patterns of irreducible polynomials* "
18:25 – 18:45	Angelo Sonnino: "*Inherited unitals in Moulton planes of odd order*"	Marc Munsch: "*On the minimal number of small elements generating finite prime fields*"

Wednesday 7 June

Plenary talks

9:00 – 9:55 Julia Wolf: "*Additive combinatorics over Finite Fields: recent progress and open problems*"

Contributed talks

	Session A	Session B
10:00 – 10:20	Jürgen Bierbrauer: "*Additive quaternary codes*"	Anurag Bishnoi: "*The cage problem and finite geometry*"
10:25 – 10:45	Petr Lisoněk: "*On a family of APN quadrinomials*"	Anna-Lena Horlemann-Trautmann: "*A Complete Classification of Partial-MDS (Maximally Recoverable) Codes Correcting one Additional Erasure*"
10:50 – 11:10	Valentin Suder: "*A Note on Complete Mappings over $\mathbb{F}_{2^n}$*"	Mariusz Kwiatkowski: "*SR-construction of linear codes and application to the simplex codes*"

11:15 *Coffee Break*

Contributed talks

	Session A	Session B
11:40 – 12:00	Sébastien Duval: "*On a generalisation of Dillon's APN permutation*"	Jonathan Jedwab: "*Costas cubes*"
12:05 – 12:25	Wilfried Meidl: "*Bent function generalizations and their transforms*"	Jordy Vanpoucke: "*General Properties of Costas Permutations and Graphs from Hops and Alternating Runs*"
12:30 – 12:55	Kanat Abdukhalikov: "*Bent functions, ovals and line ovals*"	Giorgos Kapetanakis: "*On a conjecture of Morgan and Mullen*"

13:00 *Lunch Break*

15:00 *Excursion to* Grotta di Tiberio

Thursday 8 June

Plenary talks

9:00 – 9:55 Alev Topuzoğlu: "*On permutation polynomials over finite fields*"

10:00 – 10:55 Daniel Katz: "*Character Sums, Correlation and Nonlinearity*"

11:00 *Coffee Break*

Contributed talks

	Session A	Session B
11:30 – 11:50	Marco Buratti: "*Combinatorial designs over finite fields*"	Nurdagül Anbar: "*On the difference of permutation polynomials*"
11:55 – 12:15	Oktay Olmez: "*Binary three-weight linear codes from partial geometric difference sets*"	Rainer Göttfert: "*Entropy Extraction via Decimation*"
12:20 – 12:40	Jim Davis: "*Constructions of Partial Geometric Difference Sets*"	László Mérai: "*On the pseudorandomness of automatic sequences*"

13:00 *Lunch Break*

Contributed talks

	Session A	Session B
15:30 – 15:50	Leo Storme: "*On the geometrical sunflower bound*"	Augustine Musukwa: "*Counting Extended Irreducible Binary Goppa Codes of Degree $2p$ and Length $2^n + 1$*"
15:55 – 16:15	Relinde Jurrius: "*A q-analogue of perfect matroid designs*"	Avaz Naghipour: "*Construction of binary quantum codes on closed orientable surfaces*"
16:20 – 16:40	Kai-Uwe Schmidt: "*On the number of inequivalent MRD codes*"	Elif Saçikara: "*Concatenated Structure and a Minimum Distance Bound for Generalized Quasi-Cyclic Codes*"

16:40 *Coffee Break*

Contributed talks

	Session A	Session B
17:10 – 17:30	Hiroaki Taniguchi: "*Dual hyperovals from three or more semifields*"	Cathy Swaenepoel: "*Digits in finite fields*"
17:35 – 17:55	Ferruh Özbudak: "*Self-duality of generalized twisted Gabidulin codes*"	P.L. Sharma: "*Existence of normal elements with prescribed trace vectors over finite fields*"
18:00 – 18:20	John Sheekey: "*An algebraic construction for new MRD codes and new semifields*"	David Thomson: "*Towards primitive k-normality*"
18:25 – 18:45	Alessandro Siciliano: "*Puncturing maximum rank distance codes*"	Mahmood Alizadeh: "*On the k-normal elements over finite fields*"

20:00 *Social dinner*

Programme

Friday 9 June

Plenary talks

9:00 – 9:55 Qiang Wang: "*Polynomials over finite fields: an index approach*"

Contributed talks

	Session A	Session B
10:00 – 10:20	Iván Blanco-Chacón: "*Rank metric codes and Zeta functions: bounds, functional equations and conjectures*"	Buket Özkaya: "*Some Recent Results on LCD Codes*"
10:25 – 10:45	Eimear Byrne: "*Puncturing, Shortening and the Rank Metric Zeta Function*"	Horacio Tapia-Recillas: "*On constacyclic codes over a class of finite local non-chain Frobenius rings*"
10:50	*Coffee Break*	
11:25 – 11:45	Sascha Kurz: "*Upper bounds for partial spreads from divisible codes*"	Assia Rousseva: "*On Arcs with High Divisibility Related to Linear Codes*"
11:50 – 12:10	Alessandro Neri: "*On linear Generalized Twisted Gabidulin codes and the existence of new MRD codes*"	Maosheng Xiong: "*Cyclic codes of composite length and the minimum distance*"
12:15 – 12:35	Lucas Reis: "*On the factorization of polynomials of the form $f(x^n)$ over finite fields*"	Nurdagül Anbar: "*Spectra and Equivalence of Boolean Functions*"
13:00	*Lunch Break*	
15:30 – 15:50	Gohar Kyureghyan: "*On permutation polynomials of shape $X^k + \gamma\, Tr_{q^n/q}(X^d)$*"	Stiofáin Fordham: "*On the height of the formal group of a smooth projective hypersurface*"
15:55 – 16:15	Ömer Küçüksakalli: "*Bivariate polynomial mappings associated with simple complex Lie algebras*"	Satoru Fukasawa: "*A birational embedding of an algebraic curve into a projective plane with two Galois points*"
16:20 – 16:40	Lisa Nicklasson: "*The Lefschetz properties of monomial algebras over finite fields*"	Seon Jeong Kim: "*Number of points of a nonsingular hypersurface in an odd-dimensional projective space*"
16:40	*Coffee Break*	
17:10 – 17:30	Ivan Landjev: "*On Homogeneous Arcs and Linear Codes over Finite Chain Rings*"	Emrah Sercan Yilmaz: "*Counting Points on Curves and Irreducible Polynomials over Finite Fields*"
17:35 – 17:55	Todd Mateer: "*Improved decoding of Quick Response (QR) codes*"	Nazar Arakelian: "*Number of rational points of a singular plane curve over a finite field*"

List of Participants

List of Participants

A

Kanat Abdukhalikov
UAE University (UAE)
e-mail: abdukhalik@uaeu.ac.ae

Angela Aguglia
Politecnico di Bari (Italy)
e-mail: angela.aguglia@poliba.it

Nurdagul Anbar
RICAM (Austria)
e-mail: nurdagulanbar2@gmail.com

Riccardo Aragona
University of Trento (Italy)
e-mail: ric.aragona@gmail.com

Nazar Arakelian
Universidade Federal Doi ABC (Brazil)
e-mail: n_arakelian@hotmail.com

Leyla Ateş
Sabancı University (Turkey)
e-mail: leylaparlar@sabanciuniv.edu

Yves Aubry
IMATH - Université de Toulon and I2M-AMU (France)
e-mail: yves.aubry@univ-amu.fr

B

Simeon Ball
Universitat Politècnica de catalunya (Spain)
e-mail: simeon@ma4.upc.edu

Daniele Bartoli
Università degli Studi di Perugia (Italy)
e-mail: daniele.bartoli@unipg.it

Francesco Belardo
Università di Napoli "Federico II" (Italy)
e-mail: fbelardo@gmail.com

Clark Benson
Department of Defense (USA)
e-mail: clark_t_benson@yahoo.com

Elena Berardini
Aix-Marseille University (France)
e-mail: elena.berardini@univ-amu.fr

Jürgen Bierbrauer
Michigan Technological University (USA)
e-mail: jbierbra@mtu.edu

Anurag Bishnoi
University of Ghent (Belgium)
e-mail: anurag.2357@gmail.com

Iván Blanco Chacón
University College Dublin (Ireland)
e-mail: ivanblanco@gmail.com

Matteo Bonini
University of Trento (Italy)
e-mail: matteo.bonini@unitn.it

Martino Borello
University of Paris (France)
e-mail: martino.borello@univ-paris8.fr

Herivelto Borges
Univesidade de são Paulo (Brazil)
e-mail: h.borges@icmc.usp.br

Marco Bucci
Infineon Technologies AG (Germany)
e-mail:

Marco Buratti
Università di Perugia (Italy)
e-mail: buratti@dmi.unipg.it

Eimear Byrne
University College of Dublin (Ireland)
e-mail: ebyrne@ucd.ie

List of Participants

C

Anne Canteaut
Inria (France)
e-mail: anne-canteaut@inria.fr

Ilaria Cardinali
University of Siena (Italy)
e-mail: ilaria.cardinali@unisi.it

Michela Ceria
University of Trento (Italy)
e-mail: michela-ceria@unitn.it

Pascale Charpin
Inria (France)
e-mail: pascale.charpin@inria.fr

Enju Cheon
Gyeongsang National University (South Korea)
e-mail: enju1000@naver.com

Gloria Chong Shuen
( )
e-mail:

Roberto Civino
University of Trento (Italy)
e-mail: robcivino@gmail.com

Mariana Coutinho
Universitade de são Paulo (Brasil)
e-mail: mariananerey@usp.br

D

James Davis
University of Richmond (USA)
e-mail: jdavis@richmond.edu

Jan De Beule
Vrije Universiteit Brussel (Belgium)
e-mail: Jan.De.Beule@vub.ac.be

Maarten De Boeck
University of Ghent (Belgium)
e-mail: maarten.deboeck@ugent.be

Lilian Batista De Oliveira
Federal University of Minas Gerais (Brazil)
e-mail:

Giorgio Donati
Università di Napoli "Federico II" (Italy)
e-mail: giorgio.donati@unina.it

Nicola Durante
Università di Napoli "Federico II" (Italy)
e-mail: ndurante@unina.it

Sébastien Duval
Inria (France)
e-mail: sebastian.duval@inria.fr

E

Gove Effinger
Skidmore College (USA)
e-mail: effinger@skidmore.edu

Michele Elia
Politecnico di Torino (Italy)
e-mail: michele.elia@polito.it

F

Andrea Ferraguti
University of Cambridge (United Kingdom)
e-mail: af612@cam.ac.uk

Stiofáin Fordham
University College Dublin (Ireland)
e-mail: stiofan.fordham@ucdconnect.ie

Satoru Fukasawa
Yamagata University (Japan)
e-mail: s.fukasawa@sci.kj.yamagata-u.ac.jp

List of Participants

G

Daniel Gerike
Otto-von-Guericke Universität (Germany)
e-mail: daniel.gerike@gmail.com

Alejandreo Jose Giangreco Maidana
Aix-Marseille University (France)
e-mail: ajgiangreco@gmail.com

Massimo Giulietti
Università di Perugia (Italy)
e-mail: giuliet@dipmat.unipg.it

Luca Giuzzi
University of Brescia (Italy)
e-mail: luca.giuzzi@unibs.it

Domingo Gómez Pérez
University of Cantabria (Spain)
e-mail:

Rainer Göttfert
Infineon Technologies AG (Germany)
e-mail: rainer.goettfert@infineon.com

Robert Granger
EPFL (Switzerland)
e-mail: robert.granger@epfl.ch

Cem Güneri
Sabancı University (Turkey)
e-mail: guneri@sabanciuniv.edu

Burçin Güneş
Sabancı University (Turkey)
e-mail: bgunes@sabanciuniv.edu

Christian Günther
Paderborn University (Germany)
e-mail: chriguen@math.upb.de

H

James Hirschfeld
University of Sussex (United Kingdom)
e-mail: jwph@sussex.ac.uk

Masaaki Homma
Kanagawa University (Japan)
e-mail: homma@kanagawa-u.ac.jp

Anna-Lena Horlemann
University of St. Gallen (Switzerland)
e-mail: anna-lena.horlemann@unisg.ch

I

Annamaria Iezzi
Institut de Mathématiques de Marseille (France)
e-mail: annamaria.iezzi@univ-amu.fr

J

Jonathan Jedwab
Simon Fraser University (Canada)
e-mail: jed@sfu.ca

Lingfei Jin
Fudan University (China)
e-mail: lfjin@fudan.edu.cn

Relinde Jurrius
University of Neuchâtel (Switzerland)
e-mail: relinde.jurrius@unine.ch

K

Giorgos Kapetanakis
Sabancı University (Turkey)
e-mail: gnkapet@gmail.com

Canan Kaşıkçı
Sabancı University (Turkey)
e-mail: canank@sabanciuniv.edu

Daniel Katz
California State University, Northridge (USA)
e-mail: daniel.katz@csun.edu

List of Participants

Motoko Kawakita
Shiga University of Medical Science (Japan)
e-mail: kawakita@belle.shiga-med.ac.jp

Seon Jeong Kim
Gyeongsang National University (South Korea)
e-mail: skim@gnu.ac.kr

Megah Kolhekar
Indian Institute of Tecnology Bombay (India)
e-mail: megakolhekar@ee.iitt.ac.in

Gábor Korchmáros
Università della Basilicata (Italy)
e-mail: gabor.korchmaros@unibas.it

Ömer Küçüksakalli
Middle East Technical University (Turkey)
e-mail: komer@metu.edu.tr

Selda Küçükçifçi
Koç University (Turkey)
e-mail: skucukcifci@ku.edu.tr

Sacha Kurz
University of Bayreuth (Germany)
e-mail: sascha.kurz@uni-bayreuth.de

Gohar Kyureghyan
University of Rostock (Germany)
e-mail: gohar.kyureghyan@uni-rostock.de

Mariusz Kwiatkowski
University of Warmia and Mazury (Poland)
e-mail: mkw@matman.uwm.edu.pl

L

Ivan Landjev
New Bulgarian University (Bulgaria)
e-mail: i.landjev@nbu.bg

Kristin Lauter
Microsoft (USA)
e-mail: klauter@microsoft.com

Kahin Leung
National University of Singapore (Singapore)
e-mail: matlkh@nus.edu.sg

Kangquan Li
National University of Defense Technology (China)
e-mail: likangquan11@nudt.edu.cn

Petr Lisoněk
Simon Fraser University (Canada)
e-mail: plisonek@sfu.ca

Giovanni Longobardi
Università di Napoli "Federico II" (Italy)
e-mail: giovanni.longobardi@unina.it

Guglielmo Lunardon
Università di Napoli "Federico II" (Italy)
e-mail: lunardon@unina.it

M

Giuseppe Marino
Università degli Studi della Campania "Luigi Vanvitelli" (Italy)
e-mail: giuseppe.marino@unicampania.it

Carla Mascia
University of Trento (Italy)
e-mail: carla.mascia@unitn.it

Ariane Masuda
New York City College of Technology (USA)
e-mail: ariane.masuda@gmail.com

Todd Mateer
Department of Defense (USA)
e-mail: tmateer@howardcc.edu

Sam Mattheus
Vrije Universiteit Brussel (Belgium)
e-mail: sam.mattheus@vub.ac.be

Francesco Mazzocca
Università degli Studi della Campania "Luigi Vanvitelli" (Italy)
e-mail: francesco.mazzocca@unicampania.it

Wilfred Meidl
RICAM (Austria)
e-mail: meidlwilfred@gmail.com

List of Participants

László Mérai
Austrian Academy of Sciences (Austria)
e-mail: laszlo.merai@oeaw.ac.at

Francesca Merola
Università degli Studi Roma Tre (Italy)
e-mail: merola@uniroma3.it

Sihem Mesnager
Université Paris 8 Vincennes Saint-Denis (France)
e-mail: smesnager@univ-paris8.fr

Giacomo Micheli
University of Oxford (United Kingdom)
e-mail: giacomo.micheli@maths.ox.ac.uk

Maria Montanucci
Università degli Studi della Basilicata (Italy)
e-mail: maria.montanucci@unibas.it

Marc Munsch
Technische Universität Graz (Austria)
e-mail: munsch@math.tugraz.at

Augustine Musukwa
University of Trento (Italy)
e-mail: augustine.musukwa@unitr.it

N

Avaz Naghipour
University College of Nabi Akram (Iran)
e-mail: a_naghipour@tabrizu.ac.ir

Gábor Nagy
University of Szeged (Hungary)
e-mail: nagyg@math.u-szeged.hu

Zoltán Lóránt Nagy
Eötvös Loránd University Budapest (Hungary)
e-mail: nagyzoli@cs.elte.hu

Vito Napolitano
Università degli Studi della Campania "Luigi Vanvitelli" (Italy)
e-mail: vito.napolitano@unicampania.it

Alessandro Neri
University of Zürich (Switzerland)
e-mail: alessandro.neri@math.uzh.ch

Lisa Nicklasson
Stockholm University (Sweden)
e-mail: lisan@math.su.sc

O

Oktay Ölmez
Ankara University (Ankara)
e-mail: olmezoktay@gmail.com

Ferruh Özbudak
Middle East Technical University (Ankara)
e-mail: ozbudak@metu.edu.tf

Buket Özkaya
Sabancı University (Turkey)
e-mail: buketozkaya@sabanciuniv.edu

P

Nicola Pace
Technical University of Munich (Germny)
e-mail: nicolaonline@libero.it

Daniel Panario
Carleton University (Canada)
e-mail: daniel@math.carleton.ca

Mark Pankov
University of Warmia and Mazury (Poland)
e-mail: pankov@matman.uwm.edu.pl

Francesco Pavese
Politecnico di Bari (Italy)
e-mail: francesco.pavese@unibas.it

Valentina Pepe
"La Sapienza" - University of Rome (Italy)
e-mail: valepepe@sbai.uniroma1.it

Rachel Petrik
University of Kentucky (USA)
e-mail: rachel.petrik@uky.edu

List of Participants

Olga Polverino
Università degli Studi della Campania "Luigi Vanvitelli" (Italy)
e-mail: olga.polverino@unicampania.it

Alexander Pott
Otto-von-Guericke Universität (Germany)
e-mail: alexander.pott@ovgu.de

Q

Longjiang Qu
National University of Defense Technology (China)
e-mail: ljqu@hotmail.com

R

Lucas Reis
Federal University of Minas Gerais (Brazil)
e-mail: lucasreismat@gmail.com

Joachim Rosenthal
University of Zürich (Switzerland)
e-mail: rosenthal@math.uzh.ch

Assia Rousseva
Sofia University "St. Kl. Ohridski" (Bulgaria)
e-mail: assia@fmi.uni-sofia.bg

S

Elif Saçikara Kariksiz
Sabancı University (Turkey)
e-mail: elifsacikara@sabanciuniv.edu

Giordano Santilli
University of Trento (Italy)
e-mail: giordano.santilli

Kai-Uwe Schmidt
Universität Paderborn (Germany)
e-mail: kus@math.upb.de

P L Sharma
(India)
e-mail: plsharma1964@gmail.com

John Sheekey
University College Dublin (Irland)
e-mail: johnsheekey@gmail.com

Alessandro Siciliano
Università degli Studi della Basilicata (Italy)
e-mail: alessandro.siciliano@unibas.it

Angelo Sonnino
Università degli Studi della Basilicata (Italy)
e-mail: angelo.sonnino@unibas.it

Pietro Speziali
Università degli Studi della Basilicata (Italy)
e-mail: pietro.speziali@unibas.it

Henning Stichtenoth
Sabancı University (Turkey)
e-mail: henning@sabanciuniv.edu

Leo Storme
Ghent University (Belgium)
e-mail: leo.storme@ugent

Valentin Suder
University of Versailles St. Quentin (France)
e-mail: valentin@suder.xyz

Cathy Swaenepoel
Aix-Marseille Université (France)
e-mail: cathy.swaenepoel@univ-amu.fr

Péter Sziklai
Eötvös Loránd University Budapest (Hungary)
e-mail: sziklai@cs.elte.hu

Tamás Szőnyi
Eötvös Loránd University / Ghent University (Hungary)
e-mail: szonyi@cs.elte.hu

List of Participants

T

Hiroaki Taniguchi
Kagawa National College of Technology (Japan)
e-mail: taniguchi@t.kagawa-nct.ac.jp

Horacio Tapia-Recillas
Universidad Autonoma Metropolitana-I (Mexico)
e-mail:

Daniele Taufer
University of Trento (Italy)
e-mail: daniele.taufer@unitn.it

David Thomson
Carleton University (Canada)
e-mail: dthomson@math.carleton.ca

Alev Topuzoğlu
Sabancı University (Turkey)
e-mail: alev@sabanciuniv.edu

Rocco Trombetti
Università di Napoli "Federico II" (Italy)
e-mail: rtrombet@unina.it

U

Simone Ugolini
University of Trento (Italy)
e-mail: sugolini@gmail.com

V

Jordy Vanpoucke
Vrije Universiteit Brussel (Belgium)
e-mail: jvpoucke@vub.ac.be

W

Qiang Wang
Carleton University (Canada)
e-mail: wang@math.carleton.ac

Kenneth Austin Ward
American University (USA)
e-mail: kward@american.edu

Violetta Weger
University of Zürich (Switzerland)
e-mail: violetta.weger@math.uzh.ch

Zsuzsa Weiner
Eötvös Loránd University (Hungary)
e-mail: weiner@cs.elte.hu

Arne Winterhof
Austrian Academy of Sciences (Austria)
e-mail: arne.winterhof@oeaw.ac.at

Julia Wolf
University of Bristol (United Kingdom)
e-mail: julia.wolf@bristol.ac.uk

X

Chao Ping Xing
Nanyang Techonoligical University (Singapore)
e-mail: xingcp@ntu.edu.sg

Maosheng Xiong
Hong Kong University of Science and Technology (China)
e-mail: mamsxiong@ust.hk

Y

Emrah Sercan Yilmaz
University College Dublin (Ireland)
e-mail: emrahsercan@gmail.com

Z

Corrado Zanella
Università degli Studi di Padova (Italy)
e-mail: corrado.zanella@unipd.it

Giovanni Zini
Università di Firenze (Italy)
e-mail: gzini@math.unifi.it

Invited talks

Invited talks

Maximal curves over finite fields

Massimo Giulietti

University of Perugia

Abstract

Algebraic curves over a finite field $\mathbb{F}_q$ with q elements have intrinsic interest as well as many applications to coding theory and cryptography. In the late seventies V. D. Goppa came up with a brilliant idea of constructing error correcting codes by means of algebraic curves over finite fields. The key point of Goppa's construction is that the code parameters are essentially expressed in terms of geometric and arithmetic features of the curve, such as the number N_q of $\mathbb{F}_q$-rational points and the genus g.

Goppa codes with good parameters are constructed from curves with large N_q with respect to their genus g. Given a smooth projective, algebraic curve of genus g over $\mathbb{F}_q$, an upper bound for N_q is a corollary to the celebrated Hasse-Weil Theorem,

$$N_q \leq q + 1 + 2g\sqrt{q}.$$

Curves attaining this bound are called $\mathbb{F}_q$-maximal. The Hermitian curve $\mathcal{H}$, that is, the plane projective curve with equation

$$X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}+1} = 0,$$

is a key example of an $\mathbb{F}_q$-maximal curve, as it is the unique curve, up to isomorphism, attaining the maximum possible genus $\frac{1}{2}\sqrt{q}(\sqrt{q}-1)$ of an $\mathbb{F}_q$-maximal curve. Other important examples of maximal curves are the Suzuki and the Ree curves.

It is a result commonly attributed to Serre that any curve which is $\mathbb{F}_q$-covered by an $\mathbb{F}_q$-maximal curve is still $\mathbb{F}_q$-maximal. In particular, quotient curves of $\mathbb{F}_q$-maximal curves are $\mathbb{F}_q$-maximal. Many examples of $\mathbb{F}_q$-maximal curves have been constructed as quotient curves $\mathcal{X}/G$ of the Hermitian/Ree/Suzuki curve $\mathcal{X}$ under the action of subgroups G of the full automorphism group of $\mathcal{X}$.

The first example $\tilde{\mathcal{H}}_q$ of an $\mathbb{F}_\ell$-maximal curve which is not covered by the Hermitian curve was constructed in 2009 by Giulietti and Korchmáros and it is commonly referred to as the GK curve. Let q_0 be any prime power and $q = q_0^2$. The curve $\tilde{\mathcal{H}}_q$ can be defined by the affine equations

$$\tilde{\mathcal{H}}_q : \begin{cases} t^m = x^q - x \\ x^{q_0+1} = y^{q_0} + y \end{cases},$$

where $m = q - q_0 + 1$. The curve $\tilde{\mathcal{H}}_q$ is $\mathbb{F}_{q^3}$-maximal and by construction is a Galois cover of the $\mathbb{F}_{q_0^2}$-maximal Hermitian curve $\mathcal{H}_{q_0} : x^{q_0+1} = y^{q_0} + y$. Garcia, Güneri and Stichtenoth extended this to a larger class by proving that the curve is maximal over q^n for n odd if the exponent for t is replaced by $(q_0^n + 1)/(q_0 + 1)$.

Recently, Skabelund constructed analogous Galois covers of the Suzuki and Ree curves as follows. Let $q_0 = 2^s$ with $s \geq 1$ and $q = 2q_0^2$ and let $\mathcal{S}_q : y^q + y = x^{q_0}(x^q + x)$ be the Suzuki curve. The curve

$$\tilde{\mathcal{S}}_q : \begin{cases} t^m = x^q + x \\ y^q + y = x^{q_0}\,(x^q + x) \end{cases},$$

where $m = q - 2q_0 + 1$, is maximal over the field $\mathbb{F}_{q^4}$.

Let $q_0 = 3^s$ with $s \geq 1$ and $q = 3q_0^2$ and let $\mathcal{R}_q : y^q - y = x^{q_0}(x^q - x), z^q - z = x^{2q_0}(x^q - x)$ be the Ree curve. The curve

$$\tilde{\mathcal{R}}_q : \begin{cases} t^m = x^q - x \\ z^q - z = x^{2q_0}(x^q - x) \\ y^q - y = x^{q_0}(x^q - x) \end{cases},$$

where $m = q - 3q_0 + 1$, is $\mathbb{F}_{q^6}$-maximal.

In this talk we will discuss the following topics:

1. further examples of $\mathbb{F}_q$-maximal curves that are not quotient curves of $\mathcal{H}$;
2. determination of the possible genera of $\mathbb{F}_q$-maximal curves, especially quotients of (generalized) GK curves and Skabelund curves;
3. $\mathbb{F}_q$-maximal curves with a large automorphism group.

Keywords: Curves over finite fields, Maximal curves, Automorphism of curves

Character Sums, Correlation, and Nonlinearity

Daniel J. Katz

California State University, Northridge

Abstract

Many of the pseudorandom objects used in digital sequence design, cryptography, and coding theory take their origin from constructions involving finite fields. To evaluate the performance of these objects, one must calculate their properties, such as correlation spectrum, nonlinearity, and weight distribution. Character sums lie at the heart of these calculations, and our ability to determine correlation or nonlinearity often hinges on our understanding of the underlying sums. We shall survey both past and recent advances in our knowledge of these character sums, and what they tell us about nonlinearity of functions and correlation of sequences of interest in cryptography and communications. On the way, we shall see the wide range of algebraic, analytic, arithmetic, and combinatorial techniques used to evaluate and estimate (using both archimedean and p-adic valuations) the complete and incomplete character sums that govern correlation and nonlinearity. We shall also discuss conjectures and open problems.

Keywords: character sums, correlation, nonlinearity, pseudorandom, sequences

How to Keep your Secrets in a Post-Quantum World

Kristin E. Lauter

Microsoft Research

Abstract

This talk will give an overview of the history of various hard problems in number theory involving finite fields which are used as the basis for cryptosystems. I will discuss the upcoming NIST international competition to standardize new cryptographic schemes for a post-quantum world and present some current proposals for post-quantum systems based on supersingular isogeny graphs of elliptic curves and lattice-based cryptosystems in cyclotomic number fields.

Keywords: Cryptography, Post-Quantum Cryptography, Supersingular Isogeny Graphs, Lattice-based Cryptography

On permutation polynomials over finite fields

Alev Topuzoğlu

Sabanci University, Istanbul

Abstract

Carlitz rank of a permutation polynomial is a simple concept that was introduced in the last decade. One of the assets of classifying permutation polynomials with respect to their Carlitz ranks is that a polynomial of small Carlitz rank can be approximated by a linear fractional transformation. This feature helps to analyze permutation polynomials, and provides methods of constructing those with favourable properties.

We will describe some recent results obtained by the use of this notion and indicate several applications.

This work is partially supported by TUBITAK project 114F432.

Keywords: permutation polynomial, Carlitz rank, complete mapping, cycle structure, iterations, value set

Polynomials over finite fields: an index approach

Qiang Wang

Carleton University

Abstract

The degree of a polynomial is an important parameter to study many problems on polynomials over finite fields. Recently, a new notion of the index of a polynomial over a finite field is introduced to study the distribution of permutation polynomials over finite fields. This parameter also turns out to be very useful in studying value set size bounds, character sum bounds, among others. In this talk I will introduce this new index approach and report some recent results on polynomials over finite fields mentioned above.

Keywords: index, polynomials, permutation polynomials, value set, character sum

Additive combinatorics over finite fields: recent progress and open problems

Julia Wolf

University of Bristol

Abstract

The use of high-dimensional vector spaces over finite fields as a toy model for tackling additive problems concerning the integers has only gained in popularity over the past decade. A recent high-profile breakthrough on one such toy problem, the so-called cap set problem, has called the effectiveness of the traditionally used Fourier-analytic techniques into question. We shall survey some of the developments surrounding this breakthrough, and its implications for some of the remaining open problems in the area.

Three Combinatorial Problems in Theoretical Computer Science

Chaoping Xing

Nanyang Technological University, Singapore

(Joint work with R. Cramer, V. Guruwami, C. Padró and C. Yuan)

Abstract

In recent years, some well-known combinatorial problems have found interesting applications in theoretical computer science (TCS). At the meanwhile, some new combinatorial structures arise due to need of applications in TCS. In this talk, we survey a few new combinatorial problems that arose from applications to theoretical computer science in the last few years. These combinatorial structures include algebraic manipulation detection codes, evasive subsets, subspace design. We will survey their current status and present some open problems.

Keywords: Algebraic manipulation detection codes, Evasive subspace subset, Subspace design

Contributed talks

List of contributors

Bent functions, ovals and line ovals

Kanat Abdukhalikov

UAE University

Abstract

We consider Niho bent functions (they are equivalent to bent functions which are linear on the elements of a Desarguesian spread). We show that Niho bent functions are in one-to-one correspondence with line ovals in an affine plane, and the zeroes of the dual function of a Niho bent function are exactly the points of the line oval. Furthermore, Niho bent functions are in one-to-one correspondence with ovals (in a projective plane) with nucleus at a fixed point. Similar statements are true for bent functions which are linear on the elements of an arbitrary spread.

Keywords: Bent functions, Niho bent functions, ovals, line ovals, affine planes, projective planes

On singular quasi-Hermitian varieties

Angela Aguglia

Politecnico di Bari

Abstract

A *quasi-Hermitian variety* $\mathcal{V}$ in $PG(r,q^2)$ is a generalization of the non-singular Hermitian variety $H(r,q^2)$ so that $\mathcal{V}$ and $H(r,q^2)$ have the same size and the same intersection numbers with hyperplanes.

Analogously, a *d-singular quasi-Hermitian variety* is a subset of points of $PG(r,q^2)$ having the same number of points and the same intersection sizes with hyperplanes as a singular Hermitian variety with a singular space of dimension d.

We provide some necessary and sufficient conditions for which a singular quasi-Hermitian variety of $PG(3,q^2)$ is a cone with vertex a point and base a Hermitian curve.

Keywords: Hermitian variety, singular space.

On the k-normal elements over finite fields

Mahmood Alizadeh

Department of Mathematics, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran

(Joint work with M. R. Darafsheh, School of Mathematics, University of Tehran, Tehran, Iran)

Abstract

An element $\alpha \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if the set $\{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The k-normal elements over finite fields are defined and characterized by Huczynska, Mullen, Panario and Thomson (2013). For $0 \leq k \leq n-1$, the element $\alpha \in \mathbb{F}_{q^n}$ is called a k-normal element by them, if $gcd(x^n - 1, \sum_{i=0}^{n-1} \alpha^{q^i} x^{n-1-i})$ has degree k. By this mention, a 0-normal element is a normal element. In this paper, a new characterization and construction of k-normal elements over finite fields is given.

Keywords: Finite fields; normal basis; k-normal element.

On the difference of permutation polynomials

Nurdagül Anbar

RICAM, LINZ, AUSTRIA

(Joint work with:
Almasa Odzak–University of Sarajevo, Vandita Patel–University of Warwick,
Luciane Quoos–Universidade Federal do Rio de Janeiro,
Anna Somoza–Universitat Politècnica de Catalunya and Leiden University,
Alev Topuzoğlu–Sabancı University)

Abstract

The well-known Chowla and Zassenhaus conjecture, proven by Cohen in 1990, states that if $p > (d^2 - 3d + 4)^2$, then there is no complete mapping polynomial f in $\mathbb{F}_p[x]$ of degree $d \geq 2$. For arbitrary finite fields $\mathbb{F}_q$, a similar non-existence result is obtained recently by Işık, Topuzoğlu and Winterhof in terms of the Carlitz rank of f, see [2].

Cohen, Mullen and Shiue generalized the Chowla-Zassenhaus-Cohen Theorem significantly in 1995, by considering differences of permutation polynomials. More precisely, they showed that if f and $f + g$ are both permutation polynomials of degree $d \geq 2$ over $\mathbb{F}_p$, with $p > (d^2 - 3d + 4)^2$, then the degree k of g satisfies $k \geq 3d/5$, unless g is constant. In recent a work [1], assuming f and $f + g$ are permutation polynomials in $\mathbb{F}_q[x]$, we give lower bounds for k in terms of the Carlitz rank of f and q. Our result generalizes the above mentioned result of Işık et al. In this talk, we briefly describe the idea of the proof of this generalization, which uses methods from Algebraic Geometry.

Keywords: Permutation polynomials, Carlitz rank, Chowla-Zassenhaus-Cohen theorem

References

[1] N. Anbar, A. Odzak, V. Patel, L. Quoos, A. Somoza, A. Topuzoğlu, *On the difference of permutation polynomials*, preprint.

[2] L. Işık, A. Topuzoğlu and A. Winterhof, *Complete mappings and Carlitz rank*, Des. Codes Cryptogr. (2016), DOI 10.1007/s10623-016-0293-5.

Spectra and Equivalence of Boolean Functions

Nurdagül Anbar

RICAM, LINZ, AUSTRIA

(Joint work with Wilfried Meidl–RICAM and Alexander Pott–OvG University of Magdeburg)

Abstract

For $c \in \mathbb{F}_{2^n}$, a c-bent$_4$ function $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$ is a function with a flat spectrum with respect to the unitary transform V_f^c, which is designed to describe the component functions of modified planar functions. In the first part, we generalise the concept of partially bent functions known for the Walsh-Hadamard transform to partially c-bent$_4$ functions for the transforms V_f^c. In particular, we show that any quadratic function is partially c-bent$_4$ for all c and c-bent$_4$ at least three distinct c. By analysing the spectra of a cubic monomial with respect to all transforms V_f^c, we show that non-quadratic functions exhibit a different behaviour.

We call two bent$_4$ functions *equivalent* if their corresponding bent(semibent) functions are EA-equivalent. We call two bent$_4$ functions *difference set equivalent* if their corresponding relative difference sets are equivalent. In the second part, we investigate the equivalence of bent$_4$ functions with respect to these two different aspects and show that two EA-equivalent bent (semibent) functions can induce inequivalent relative difference sets.

Keywords: Boolean functions, c-bent$_4$, difference sets, EA-equivalence, quadratic functions

References

[1] N. Anbar, W. Meidl, *Bent and Bent$_4$ spectra of quadratic functions over $\mathbb{F}_{2^n}$*, Finite Fields and their Applications, **46** (2017), 163–178.

[2] N. Anbar, W. Meidl, A. Pott, *Equivalence of negabent functions and their relative difference sets*, preprint.

Number of rational points of a singular plane curve over a finite field

Nazar Arakelian

Federal University of ABC

Abstract

Let $\mathcal{F}$ be a plane singular curve defined over a finite field $\mathbb{F}_q$. Via the Stöhr-Voloch approach and a variation of it, the linear system of plane curves of a given degree passing through the singularities of $\mathcal{F}$ provide potentially good bounds for the number of points of $\mathcal{F}$. In this talk, the case of a plane curve with two singularities such that the sum of its multiplicities is precisely the degree of the curve is exploited in more depth. In particular, for $q \geq 5$, a curve with a plane model of this type attaining one of the obtained bounds is presented.

Keywords: Algebraic curves, rational points, finite fields

On short vectors in function field lattices

Leyla Ateş

Sabanci University

(Joint work with Henning Stichtenoth — Sabancı University)

Abstract

We will mention lattices Λ associated to function fields over finite fields and discuss some properties such as rank, determinant and kissing number. We will mainly focus on the sublattice $\Delta \subseteq \Lambda$ generated by the shortest vectors in Λ. In the literature, there are examples of well-rounded lattices associated to function fields, i.e., Δ and Λ have the same rank. We will present a large class of function fields, including hyperelliptic function fields, whose associated lattices are not well-rounded.

Keywords: function field lattices, minimum length of a lattice, kissing number, well-roundedness

References

[1] L. Ateş, H. Stichtenoth, *A note on short vectors in lattices from function fields,* Finite Fields Appl., **39** (2016), 264-271.

Second order differential uniformity

Yves Aubry

University of Toulon, IMATH and I2M, France

(Joint work with Fabien Herbaut — University of Nice, IMATH, ESPE Nice-Toulon)

Abstract

For any polynomial f of $\mathbb{F}_q[x]$ $(q = 2^n)$ we introduce the following characteristic of the distribution of its second order derivative, which extends the differential uniformity notion and which is related to differential cryptanalysis:

$$\delta^2(f) := \max_{\alpha\in\mathbb{F}_q^*,\alpha'\in\mathbb{F}_q^*,\beta\in\mathbb{F}_q,\alpha\neq\alpha'} \sharp\{x \in \mathbb{F}_q \mid D^2_{\alpha,\alpha'}f(x) = \beta\}$$

where $D^2_{\alpha,\alpha'}f(x) := D_{\alpha'}(D_\alpha f(x)) = f(x) + f(x+\alpha) + f(x+\alpha') + f(x+\alpha+\alpha')$ is the second order derivative. We prove the following density theorem relative to this quantity, which is an analogue of a theorem proved by Voloch for the differential uniformity:

Theorem 1. *For a given integer $m \geq 7$ such that $m \equiv 0 \pmod 8$ (respectively $m \equiv 1, 2, 7 \pmod 8$), and with $\delta_0 = m-4$ (respectively $\delta_0 = m-5, m-6, m-3$) we have*

$$\lim_{n\to\infty} \frac{\sharp\{f \in \mathbb{F}_{2^n}[x] \mid \deg(f) = m,\ \delta^2(f) = \delta_0\}}{\sharp\{f \in \mathbb{F}_{2^n}[x] \mid \deg(f) = m\}} = 1.$$

Sketch of the proof. We introduce a polynomial $L_{\alpha,\alpha'}(f)$ such that: $D^2_{\alpha,\alpha'}f(x) = L_{\alpha,\alpha'}(f)\big(x(x+\alpha)(x+\alpha')(x+\alpha+\alpha')\big)$. We give a lower bound for the number of polynomials f such that $L_{\alpha,\alpha'}(f)$ is Morse for which we know the geometric and arithmetic monodromy groups.

Then we give a condition of regularity, that is a condition for $\mathbb{F}_q$ to be algebraically closed in the Galois closure of the polynomial $D^2_{\alpha,\alpha'}f(x)$, and the Chebotarev's density theorem enables us to prove that for q sufficiently large the polynomial $D^2_{\alpha,\alpha'}f(x) + \beta$ totally splits in $\mathbb{F}_q[x]$.

Finally we show that we can choose a finite set of couples (α_i, α_i') such that most polynomials $f \in \mathbb{F}_q[x]$ of degree m satisfy the above regularity condition.

Keywords: Differential uniformity, Galois closure of a map, monodromy groups, Morse polynomial, Chebotarev density theorem.

Arcs and the $\sqrt{q}$ conjecture

Simeon Ball

Universitat Politècnica Catalunya, Barcelona

(Joint work with Michel Lavrauw — Sabancı University, Istanbul)

Abstract

Let $\mathrm{PG}_2(\mathbb{F}_q)$ denote the projective plane over $\mathbb{F}_q$. An *arc* (or planar arc) of $\mathrm{PG}_2(\mathbb{F}_q)$ is a set of points in which any 3 points span the whole plane. An arc is *complete* if it cannot be extended to a larger arc.

In 1967 Beniamino Segre proved that the set of tangents to a planar arc of size $q+2-t$, when viewed as a set of points in the dual plane, is contained in an algebraic curve of small degree d. Specifically, if q is even then $d=t$ and if q is odd then $d=2t$. By combining this result with the Hasse-Weil theorem he proved the following conjecture for q even.

Conjecture 1. *If $q>13$ and $2\leqslant t\leqslant\sqrt{q}$ then a planar arc of size $q+2-t$ can be extended to a larger arc.*

If true in general, the bound in the conjecture is tight. There are examples of complete arcs of size $q+1-\sqrt{q}$ in $\mathrm{PG}_2(\mathbb{F}_q)$ when q is square, first discovered by Kestenband in 1981.

The conjecture was proven by Voloch in the early 1990's for q odd and not a square. If q is odd and a square, the conjecture was verified for $t<\frac{1}{2}\sqrt{q}+c$ by Hirschfeld and Korchmáros in the late 1990's.

In this talk I will outline a proof of the following theorem. Here p denotes the characteristic of $\mathbb{F}_q$.

Theorem 2. *If q is odd and $(t+p^{\lfloor\log_p t\rfloor})^2<q+2-t$ then a complete planar arc of size $q+2-t$ is a conic.*

This has the following corollary.

Theorem 3. *If $q>13$ and $2\leqslant t\leqslant\sqrt{q}-\sqrt{q}/p-1$ then a planar arc of size $q+2-t$ can be extended to a larger arc.*

Keywords: arcs, finite projective plane

AG codes from the GK and the GGS curves

Daniele Bartoli

University of Perugia

(Joint work with M. Montanucci — University of Basilicata, G. Zini — University of Firenze)

Abstract

Giulietti-Korchmáros curve and Garcia-Güneri-Stichtenoth curve are well known families of maximal curves, that is curves attaining the maximum possible number of rational points with respect to their genus. In this talk we provide Algebraic-Geometric (AG) codes associated with these two families of curves.

In particular, we investigate multi-point AG codes associated with the GK maximal curve, starting from a divisor which is invariant under a large automorphism group of the curve, constructing families of codes with large automorphism groups.

Also, we determine the Weierstrass semigroup at all $\mathbb{F}_{q^2}$-rational points of the GGS curve and we compute the Feng-Rao designed minimum distance for infinite families of codes associated with GGS curve, as well as the automorphism group. As a result, some linear codes with better relative parameters with respect to one-point Hermitian codes are discovered. Finally, we provide some classes of quantum and convolutional codes relying on the constructed AG codes.

Keywords: Algebraic-Geometric codes, GK curve, GGS curve

Additive quaternary codes

Jürgen Bierbrauer

Michigan Technological University

(Joint work with Stefano Marcugini and Fernanda Pambianco - Perugia)

Abstract

The notion of an additive quaternary code generalizes the notion of a linear quaternary code: linearity is over $GF(2)$, the alphabet is the Klein group $Z_2 \times Z_2$. The geometric description is in terms of families of lines (codelines) in binary projective spaces. The distance is d if at most $n - d$ codelines are on each hyperplane. The dual distance is $t + 1$ if any t of the codelines are in general position. The binary quantum stabilizer codes form a special case.
As an example, an additive $[7, 3.5, 4]_4$-code is equivalent to a family of 7 lines in $PG(6, 2)$ such that at most $7 - 4 = 3$ codelines are on a hyperplane. It has $4^{3.5} = 2^7 = 128$ codewords. If it is self-dual then any three codelines generate a hyperplane.
We determine the optimal parameters for length $n \leq 13$, we show that $[17, 4, 12]_4$-codes and $[17, 13, 4]_4$-codes are uniquely determined (the code generated by an elliptic quadric in $PG(3, 4)$ and its dual), show the non-existence of $[18, 14, 4]_4$-codes and we construct $[18, 13.5, 4]_4$-codes.

Keywords: linear codes, additive codes, quaternary codes, quantum stabilizer codes,projective space, hyperplane, distance, dual code.

The cage problem and finite geometry

Anurag Bishnoi

Ghent University

(Joint work with John Bamberg and Gordon Royle)

Abstract

The cage problem asks for the smallest number $c(k,g)$ of vertices in a k-regular graph of girth g. The (k,g) graphs which have $c(k,g)$ vertices are known as cages. Cages are known to exist for all integers $k \geq 2$ and $g \geq 3$, but an explicit construction is known only for some small values of k, g and three infinite families where $g \in \{6,8,12\}$ and $k-1$ is a prime power. These infinite families come from the incidence graphs of generalized polygons. When $k-1$ is not a prime power and $g \in \{6,8,12\}$ we can construct small (k,g) graphs by picking a prime power $q \geq k$ and then looking at the smallest induced k-regular subgraphs of the incidence graph of a generalized $g/2$-gon of order q. This approach has been used to obtain some of the best known upper bounds on $c(k,g)$ for these values of g.

In this talk I will first present a general lower bound on the number of vertices in an induced k-regular subgraph of the incidence graph of a generalized polygon. This bound shows that the known construction of $(k,6)$ graphs using Baer subplanes of the projective plane $\mathrm{PG}(2,q)$, with q an even power of prime, is the best possible. For generalized quadrangles, our bound improves the known lower bound for the size of an induced $(q,8)$-regular subgraphs of generalized quadrangles of order q and shows that the known constructions are asymptotically sharp.

I will then discuss a new construction of induced q-regular subgraphs of the generalized quadrangle $W(3,q)$, which is the point-line geometry obtained by taking the totally isotropic points and lines with respect to a symplectic form in $\mathrm{PG}(3,q)$. Our construction proves that $c(q,8) \leq 2(q^3 - q\sqrt{q} - q)$ for every $q = p^{2h} \geq 9$, where p is a prime and h is an integer, which improves the current best bound of $2(q^3 - 3q - 2)$ for q even and $2(q^3 - 2q)$ for q odd.

Keywords: cage, projective plane, generalized polygon, expander mixing lemma

Rank metric codes and Zeta functions: bounds, functional equations and conjectures

Iván Blanco-Chacón

University College Dublin

Abstract

In a series of works, I. Duursma introduced the zeta function of a linear code. Such zeta function mimics, at least formally, the main properties of the Weil zeta function for a smooth projective curve defined over a finite field. Zeta functions of linear codes contain the same information as the Hammingweight enumerator, but presented in a particular way which makes possible to derive interesting estimates for the minimal distance, in terms of the reciprocal roots of the zeta function, which are the code-analogue of the Hasse bound for smooth projective curves. As in the smooth curve setting, a RiemannHypothesis analogue holds for certain families of codes (e.g. for self-dual, divisible random codes), but it is not clear at the moment which is the most general condition to grant that the Riemann hypothesis holds for a family of codes. Codes satisfying a Riemann hypothesis attain sharp asymptotic estimates for the relative rate, along the lines of Gilbert-Varshamov's ones. In my talk, I will recall the above ideas and results and I will present part of a joint recent paper with E. Byrne, I. Duursma and J. Sheekey, where we have introduced the notion of zeta function of a rank-metric code. Most of the properties of the zeta function for Hamming-metric codes still hold in our case. However, the proofs involve some technicalities, which will be discussed in other talk. In particular, I will show that our zeta function is a generating function for the family of rank metric weight enumerators, and satisfies a functional equation, as in the Hamming setting. Moreover, I will also also relate the minimal rank-distance with the sum of reciprocal roots of the zeta-function

Keywords: rank-metric codes, zeta-functions

Minimal weight codewords of some codes from the GK curve

Matteo Bonini

University of Trento

(Joint work with Daniele Bartoli — University of Perugia)

Abstract

Giulietti and Korchmáros introduced a maximal curve over $\mathbb{F}_{q^6}$ which is not a subcover of the corresponding Hermitian curve for $q \neq 2$. We study the maximum number of collinear points on such a curve and we give a geometrical characterization of the smallest-weight codewords, obtaining the exact minimum distance for a class of Algebraic-Geometric codes from the GK curve.

Also, we compute the number of minimal weight codewords for such codes, using techniques similar to the ones used by Marcolla, Pellegrini, and Sala for first-phase Hermitian codes.

Keywords: GK curve, Algebraic-Geometric codes, Hamming weight

Symmetries of weight enumerators

Martino Borello

University of Paris 8 - LAGA

(Joint work with Olivier Mila — University of Bern)

Abstract

Gleason's 1970 theorem about the weight enumerators of self-dual codes is one of the most remarkable theorem in coding theory in its connection with invariant theory. Weight enumerators of self-dual doubly-even codes are invariant under the action of a group of order 192, generated by the symmetry coming from MacWilliams' identities and by the symmetry coming from the divisibility condition. This simple observation led Gleason to prove, by classical invariant theory arguments, that the weight enumerator of a self-dual doubly-even code belongs to the polynomial ring generated by the weight enumerators of the extended Hamming code of length 8 and of the extended Golay code of length 24. The importance of Gleason's theorem is surely due to its fecundity and to the numerous new research problems it has generated.

Plenty of generalizations of Gleason's theorem to other family of self-dual codes have been proved. All of them make use of MacWilliams' identities and their generalizations, which give a symmetry of the weight enumerator only if the code is self-dual or eventually formally self-dual. To our knowledge, no one has investigated general cases for which MacWilliams' identities do not give a symmetry. However, many interesting families of codes (e.g. Reed-Muller codes) do not have this property and yet it would be useful to have a similar result about their weight enumerators. In the talk we will present our first steps in this direction. Using the well-known classification of finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ and other algebraic tools, we show general results on the group of symmetry, we present a new algorithm to find it and we investigate the case of Reed-Muller codes.

Keywords: Linear codes, weight enumerators, invariant theory

Entropy Extraction via Decimation

Marco Bucci

Infineon Technologies AG

(Joint work with Rainer Göttfert)

Abstract

Consider der following postprocessing algorithm in a random bit generator. The sequence $X = (x_j)_{j=0}^{\infty}$ of digitized noise signals (produced by some physical noise source) is fed, bit by bit, into a linear feedback shift register (LFSR) of length n and with characteristic polynomial $f(x)$. At the same time, and at the same rate, the LFSR outputs a binary sequence $Y = (y_j)_{j=0}^{\infty}$. For each bit x_j fed into the LFSR one state bit y_j is extracted from the LFSR. The sequence Y is then decimated according to some decimation factor $k > 1$. The decimated sequence $R = (r_j)_{j=0}^{\infty} = (y_{jk})_{j=0}^{\infty}$ is used as the final random bit sequence.

Due to the decimation and a memory effect arising from the LFSR scrambling, longer segments of the input sequence X are compressed into shorter segments of the output sequence R. The sequence R is produced at a lower rate than X which results in a higher per-bit entropy of the sequence R. The greater the length n of the LFSR and the greater the decimation factor k, the higher the average per-bit entropy of the sequence R. Fix the parameters n and k. Assume that the input sequence X is i.i.d., and that k is a power of 2. What is the best choice for the characteristic polynomial $f(x)$? For which LFSRs is the amount of entropy in R, extracted from X, maximum?

To investigate this problem, the linear operator

$$D_k \circ f^{k-1}(E)$$

is useful. Here, D_k denotes the decimation operator defined by $D_k(u_j)_{j=0}^{\infty} = (u_{jk})_{j=0}^{\infty}$, and E the shift operator defined by $E(u_j)_{j=0}^{\infty} = (u_{j+1})_{j=0}^{\infty}$. Both operators are defined on the $\mathbb{F}_2-$vector space V of all binary sequences. The linear operator is used to set-up a binary matrix which defines a linear code. The best choice for $f(x)$ corresponds to a linear code with the greatest possible minimum distance.

Keywords: LFSR, decimation, entropy extraction

Combinatorial designs over finite fields

Marco Buratti

University of Perugia

(Joint work with Anamari Nakic — University of Zagreb)

Abstract

A t-design of order v and index λ over the finite field $\mathbb{F}_q$ is a collection $\mathcal{S}$ of subspaces of the vector space $\mathbb{F}_q^v$ with the property that any t-dimensional subspace of $\mathbb{F}_q^v$ is contained in exactly λ members of $\mathcal{S}$.

Generalizing some old results by Thomas, we present a few new theoretical results on the existence of 2-designs over $\mathbb{F}_2$.

We note that a 2-design of order v and index λ over $\mathbb{F}_q$ can be viewed as a decomposition of the λ-fold of the complete graph on the points of the projective space $\mathrm{PG}(v-1,q)$ (briefly $[\lambda K_v]_q$) into cliques whose sets of vertices are subspaces of $\mathrm{PG}(v-1,q)$. In our opinion this observation naturally leads to the new notion of a graph decomposition over $\mathbb{F}_q$ as a decomposition of $[\lambda K_v]_q$ into graphs (not necessarily cliques) each of which has vertex-set coinciding with a subspace of $\mathrm{PG}(v-1,q)$. We present some concrete constructions and some variants of this concept.

Keywords: design over a finite field; graph decomposition.

Puncturing, Shortening and the Rank Metric Zeta Function

Eimear Byrne

University College Dublin

(Joint work with Ivan Blanco-Chacón (UCD), Iwan Duursma (UIUC), John Sheekey (UCD))

Abstract

Puncturing and shortening are fundamental coding theoretic operations in classical coding theory. They play an important role in questions of code optimality and code constructions. They also arise in discussions on the zeta function of a classical code for the Hamming metric (c.f. Duursma 2001). In this talk we describe properties of shortened and punctured codes for matrix codes, with respect to the rank metric. We use the notion of a rank metric shortened subcode to define the rank metric zeta function of a code as a generating function of its q-binomial moments. We define the zeta polynomial $P(T)$ of a rank metric code C in terms of its zeta function and show that it expresses the weight enumerator polynomial $W(x,y)$ of C as a linear combination of maximum rank distance weight enumerators. We show that the coefficient of T^{n-d} in the expression

$$\frac{P(T)\phi_n(T)}{(1-T)(1-q^mT)}$$

is given by $(q^m-1)^{-1}(W(x,y)-x^n)$, where $\phi_n(T)$ is determined via a recurrence relation on MRD weight enumerators.

We introduce algebraic operations on weight enumerators corresponding to puncturing and shortening and show that these may be realised in the form of q-derivatives. We show that, as in the Hamming metric case, the normalized weight enumerator of a rank-metric code is invariant under shortening and puncturing. We show further that puncturing of a normalized weight enumerator can be expressed in terms of q-commuting operators. We outline the differences between the Hamming and rank metric theories on this topic, and mention some open problems.

Keywords: rank metric codes, zeta functions, rank metric weight enumerators, MRD codes, puncturing, shortening, q-derivatives

On transparent embeddings of point-line geometries

Ilaria Cardinali

University of Siena

(Joint work with Luca Giuzzi and Antonio Pasini)

Abstract

We introduce the class of transparent embeddings for a point-line geometry $\Gamma = (\mathcal{P}, \mathcal{L})$ as the class of full projective embeddings ε of Γ such that the preimage of any projective line fully contained in $\varepsilon(\mathcal{P})$ is a line of Γ.

We will then focus on the transparency of Plücker embeddings of projective and polar grassmannians and spin embeddings of half-spin geometries and dual polar spaces of orthogonal type. As an application of our results on transparency, we will derive several Chow-like theorems for polar grassmannians and half-spin geometries.

Keywords: Plücker Embeddings, Spin Embeddings, Polar grassmannians, Automorphisms

References

[1] I. Cardinali, L. Giuzzi, A. Pasini. On transparent embeddings of point-line geometries. *Preprint* ArXiv:1611.07877.

Generalised Round Functions for Block Ciphers

Roberto Civino

University of Trento

(Joint work with R. Aragona, M. Calderini, M. Sala, and I. Zappatore)

Abstract

Round functions used as building blocks for iterated block ciphers, both in the case of Substitution-Permutation Networks (SPN) and Feistel networks, are obtained as the composition of different layers which provides confusion and diffusion, and key additions. The bijectivity of any encryption function, crucial in order to make the decryption possible, is guaranteed by the use of invertible layers. Moreover, decryption is efficient since each inverse function can be easily computed considering the inverse of each layer. In this talk a new family of ciphers, called *wave ciphers*, is introduced. Wave round functions are bijective functions obtained as the composition of *non invertible* layers, where the confusion layer enlarges the message which returns in the end to its original size after the diffusion layer is applied. Relaxing the requirement that all the layers are invertible allows considering functions which are optimal with regard to non-linearity. Since decryption cannot be realised considering the inverse of each layer involved, as it usually occurs in the case of SPN's, one way to guarantee efficient decryption is to use wave round functions in Feistel networks, where computing inverse functions is not required in order to decrypt. A first example of wave cipher is shown. The latter is a 16-bit Feistel network whose bijective round functions are the composition of an injective non-linear bricklayer transformation from 16 to 20 bit and a surjective linear function from 20 to 16 bits, whereas key addition is the classical bitwise XOR with the round key. With regard to security, immunity from some group theoretical attacks is investigated. In particular it is shown how to avoid that the group generated by the round functions of the cipher acts imprimitively on the message space, which would represent a serious flaw for the cipher.

Keywords: cryptography, block ciphers design, cryptanalysis, primitive groups

Blocking sets of Hall planes and value sets of polynomials over finite fields

Jan De Beule

Vrije Universiteit Brussel

(Joint work with:
Tamás Héger, Tamás Szőnyi — Eötvös Loránd University, Budapest
and Geertrui Van de Voorde, University of Canterbury, Christchurch)

Abstract

Let $f \in \mathbb{F}_q[x]$ be a polynomial over the finite field of order q. Then $V(f) := \{f(x) | x \in \mathbb{F}_q\}$ is called the value set of f. Cusick and Rosendahl studied value sets of polynomials in $\mathbb{F}_{q^h}[x]$, $h \geq 2$, of the form

$$f_a(x) = x^a(x+1)^{q-1}\,.$$

We discuss the connection between their result and an additional result on the value set of a particular polynomial $f_q(x)$, and the construction of a blocking set of the Hall plane of order q^2.

Let Π_q be a projective plane of order q. A *blocking set* is a set of points meeting every line of Π_q. We assume that a blocking set does not contain a line, otherwise it is called trivial. Gordon Royle posed the question whether for non Desarguesian planes the so-called 1 mod p result stays valid. In this talk we will discuss a construction of a blocking set of the Hall plane of order q^2, that does not satisfy the 1 mod p property. This leads to an example of a blocking set of a non-Desarguesian affine plane of order q^2 of size considerably smaller than $2q^2 - 1$. Furthermore, we discuss the connection of this blocking set with value sets of certain polynomials.

Keywords: blocking set, Hall plane, value set

New families of KM-arcs

Maarten De Boeck

UGent (Ghent University)

(Joint work with Geertrui Van de Voorde — University of Canterbury, Christchurch)

Abstract

A *KM-arc of type* t in $\mathrm{PG}(2,q)$ is a set of $q+t$ points in the Desarguesian projective plane $\mathrm{PG}(2,q)$ such that any line meets it in 0, 2 or t points, with $2 \leq t < q$. These sets are named after Korchmáros and Mazzocca who introduced and investigated these point sets in [4]. If a KM-arc of type t in $\mathrm{PG}(2,q)$ exists, then q is even and t is a divisor of q. Further theoretical results were obtained in [3].

In [4] Korchmáros and Mazzocca constructed KM-arcs of type 2^i in $\mathrm{PG}(2,2^h)$ for all $i>0$ such that $h-i$ is a divisor of h. In [3] Gács and Weiner gave a geometrical description of the KM-arcs described in [4] and constructed a family of KM-arcs of type 2^i in $\mathrm{PG}(2,2^h)$ for all i such that $h-i+1$ a divisor of h. A large family of KM-arcs of type $q/4$ in $\mathrm{PG}(2,q)$ was constructed in [2].

In this talk, based on [2], we introduce families of KM-arcs of type $q/8$ and $q/16$ in $\mathrm{PG}(2,q)$, solving the existence problem for some parameter values. We also discuss the group of elations stabilising these KM-arcs.

Keywords: KM-arcs, elations

References

[1] M. De Boeck and G. Van de Voorde. A linear set view on KM-arcs. *J. Algebraic Combin.*, 44(1):131–164, 2016.

[2] M. De Boeck and G. Van de Voorde. Elation KM-arcs. *Preprint*, 2017.

[3] A. Gács and Zs. Weiner. On $(q+t)$-arcs of type $(0,2,t)$. *Des. Codes Cryptogr.*, **29 (1-3)** (2003), 131–139.

[4] G. Korchmáros and F. Mazzocca. On $(q+t)$-arcs of type $(0,2,t)$ in a desarguesian plane of order q. *Math. Proc. Cambridge Philos. Soc.*, **108 (3)** (1990), 445–459.

Constructions of Partial Geometric Difference Sets

Jim Davis

University of Richmond

(Joint work with Joint Author Oktay Olmez — University of Ankara)

Abstract

Partial Geometric Difference Sets (PGDSs) were recently defined. They are used to construct Partial Geometric Designs. We use the framework of Extended Building Sets to find infinite families of PGDSs in abelian groups. Included in our new families of PGDSs are generalizations of the Hadamard, McFarland, Spence, Davis-Jedwab, and Chen difference sets.

Keywords: Difference Sets, Partial Geometric Difference Sets

On a generalisation of Dillon's APN permutation

Sébastien Duval

Sorbonne Universités/UPMC Univ. Paris 06/Inria, France

(Joint work with A. Canteaut — Inria, France and L. Perrin — SnT, Univ. Luxembourg)

Abstract

Nonlinear functions, also called S-Boxes, are building blocks for symmetric cryptography primitives. The robustness of S-Boxes is measured using properties of Boolean functions, such as differential uniformity and non-linearity.

In particular, the lower the differential uniformity, the better the resistance to differential attacks. Functions which reach the best differential uniformity, which is 2, are called Almost Perfect Nonlinear (APN). In 2009, Dillon et al. exhibited an APN permutation on six variables. This is however the only known APN permutation on an even number of variables. In 2016, Perrin et al. introduced the butterfly structure on $(4k+2)$ variables, which defines a family of permutations with differential uniformity of at most 4, and includes the Dillon APN permutation when $k=1$ (i.e. for 6 variables). It remained to find their non-linearity and whether APN butterflies exist on more than 6 variables.

In this work, we generalise butterflies by looking at involutions H_R on $(4k+2)$ variables defined by $\mathsf{H}_R(x,y) = \left(R_{R_y^{-1}(x)}(y), R_y^{-1}(x)\right)$ with $R : \mathbb{F}_2^{4k+2} \to \mathbb{F}_2^{2k+1}$ such that $x \mapsto R_y(x) = R(x,y)$ is a permutation. When the algebraic degree of R (i.e. the maximal degree of the algebraic normal forms of its coordinates) is at most 3, this family includes the Dillon permutation and all permutations defined by Perrin et al. Moreover, we can use properties of degree 3 Boolean functions to study the properties of our construction and solve the two open problems from Perrin et al.

We prove that all generalised butterflies have the best known non-linearity. Sadly, we also prove that the Dillon permutation is, up to affine equivalence, the only APN permutation in this family: other functions have differential uniformity 4. Anyhow, these new permutations still reach an excellent robustness and have an easy structure which allows for a lightweight implementation.

Keywords: Boolean function, Sbox, APN, differential uniformity, nonlinearity

On the height of the formal group of a smooth projective hypersurface

Stiofáin Fordham

University College Dublin

Abstract

Given a smooth projective hypersurface over a finite field, we can associate to the defining polynomial a descending chain of ideals after Àlvarez-Montaner–Blickle–Lyubeznik. Then a result of Boix–de Stefani–Vanzo related the point at which the chain stabilises to the height of the associated formal group in the case of an elliptic curve. I will explain how to re-interpret their result using Frobenius-splitting methods, and work in progress in extending their result to the Calabi-Yau case.

Keywords: Algebraic geometry, formal groups, Frobenius splitting

A birational embedding of an algebraic curve into a projective plane with two Galois points

Satoru Fukasawa

Yamagata University

Abstract

A criterion for the existence of a birational embedding of an algebraic curve into a projective plane with two Galois points is presented. As an application, several new examples of plane curves with two inner Galois points are described. Finite fields are used to construct such examples of curves.

Let C be a (reduced, irreducible) smooth projective curve over an algebraically closed field. We consider a rational map φ from C to $\mathbb{P}^2$, which is birational onto its image. For a point $P \in \mathbb{P}^2$, if the function field extension induced by the projection from P is Galois, then P is called a Galois point for $\varphi(C)$. This notion was introduced by Yoshihara in 1996. Furthermore, if a Galois point P is a smooth point of $\varphi(C)$, then P is said to be inner. The associated Galois group at P is denoted by G_P. There are not so many examples of plane curves with two inner Galois points. In this talk, the following criterion is presented.

Theorem 1. *Let C be a smooth projective curve and let G_1 and G_2 be different finite subgroups of the automorphism group* $\mathrm{Aut}(C)$. *Then, there exist a morphism $\varphi : C \to \mathbb{P}^2$ and different inner Galois points $\varphi(P_1)$ and $\varphi(P_2) \in \varphi(C)$ such that φ is birational onto its image and $G_{\varphi(P_i)} = G_i$ for $i = 1, 2$, if and only if the following conditions are satisfied.*

(a) $C/G_1 \cong \mathbb{P}^1$ *and* $C/G_2 \cong \mathbb{P}^1$. *(b)* $G_1 \cap G_2 = \{1\}$.

(c) There exist two different points P_1 and $P_2 \in C$ such that

$$P_1 + \sum_{\sigma \in G_1} \sigma(P_2) = P_2 + \sum_{\tau \in G_2} \tau(P_1)$$

as divisors.

Keywords: Galois point, plane curve, algebraic curve, Galois group

Hermitian Line Polar Grassmann Codes

Luca Giuzzi

University of Brescia

(Joint work with Ilaria Cardinali — University of Siena)

Abstract

In a recent series of papers we have studied the linear codes arising from the Grassmann embedding of line polar Grassmannians [1]. The minimum distance in the orthogonal case has been determined in [3] for q odd and [4] for q even, while the symplectic case has been dealt with in [2]. In [5], efficient algorithms for encoding, error correction and decoding for those cases have been introduced. In this talk we shall introduce line polar Grassmann codes arising from Hermitian polar spaces, determine their minimum distances and monomial automorphism groups and discuss the corresponding encoding algorithms.

Keywords: Hermitian Varieties, Polar Grassmann Codes, Projective Systems, Enumerative Coding.

References

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

[2] I. Cardinali and L. Giuzzi. Minimum distance of symplectic Grassmann codes. *Linear Algebra Appl.*, 488:124–134, 2016.

[3] I. Cardinali, L. Giuzzi, K. V. Kaipa, and A. Pasini. Line polar Grassmann codes of orthogonal type. *J. Pure Appl. Algebra*, 220(5):1924–1934, 2016.

[4] I. Cardinali, L. Giuzzi, Minimum distance of Line Orthogonal Grassmann codes in even characteristic. *preprint*, arXiv:1605.09333.

[5] I. Cardinali, L. Giuzzi, Enumerative coding for line polar Grassmannians with applications to codes. *Finite Fields Appl.*, 46:107–138, 2017.

[6] I. Cardinali, L. GIuzzi, Hermitian line polar Grassmann codes and their encoding. *in preparation*.

On the expansion complexity and i-expansion complexity

Domingo Gomez-Perez

Universidad de Cantabria

Abstract

In 2012, Diem introduced a new figure of merit for cryptographic sequences called expansion complexity. Since then, several articles have studied properties of expansion complexity and values for sequences, however little is known about the average value of a sequence of fixed length L. In this talk, we study the average value of the expansion complexity when L is much smaller than the characteristic.

A related complexity measure is the I-expansion complexity. We give a relationship between both measures and give an approximation to its average value when the length of the sequence is fixed.

Keywords: Sequences, Expansion complexity, I-expansion complexity

On the Enumeration of Irreducible Polynomials over GF(q) with Prescribed Coefficients

Robert Granger

École polytechnique fédérale de Lausanne, Switzerland

Abstract

In this talk we will present an algorithm which for any prime power $q = p^r$, any positive integer $l < p$ and any $n \geq l$ coprime to p, outputs exact expressions for the number of elements of $\mathbb{F}_{q^n}$ for which any subset of the first l traces are prescribed. To do so, for each such problem the algorithm computes an associated affine algebraic set $U_{\mathbf{r},\overline{n}}$ defined over $\mathbb{F}_q$ whose coefficients are functions of the prescribed values, $\mathbf{r} = (r_0, \ldots, r_{s-1}) \in (\mathbb{F}_q)^s$ for some $s \geq 1$, and $\overline{n} \in \{1, \ldots, p-1\}$. Then for each $\overline{n}$ the exact counts, which apply for all $n \equiv \overline{n} \pmod{p}$ with $n \geq l$, arise by taking the average over all specialisations of $\mathbf{r}$ of the number of $\mathbb{F}_{q^n}$-rational points on $U_{\mathbf{r},\overline{n}}$. Thanks to Dwork's theorem on the rationality of the zeta function of affine algebraic sets, we deduce that each of these counts is expressible as a $\mathbb{Q}$-linear combination of n-th powers of a finite set of algebraic integers. By an existing application of the multinomial theorem and a generalised Möbius inversion-type argument one can deduce from these formulae the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n for which the coefficients of any subset of $x^{n-1}, \ldots, x^{n-l}$ are prescribed. As well as applying the algorithm to compute examples of these algebraic sets for $q = 5$ and $l = 4$, we used an analogous algorithm to compute examples for $q = 2$ and $l \leq 7$, and for $q = 3$ and $l = 3$. All such examples were found to be absolutely irreducible curves. For $q = 2$ we computed the relevant zeta functions for $l = 4$ and $l = 5$, obtaining explicit formulae for these open problems for n odd, as well as for subsets of these problems for all n, while for $q = 3$ we obtained explicit formulae for $l = 3$ and $n \not\equiv 0 \pmod{3}$. We will also discuss some of the computational challenges and theoretical questions arising from this approach in the general case, and propose some natural conjectures and open problems.

L^α norms of polynomials derived from characters of finite fields

Christian Günther

Paderborn University

(Joint work with Kai-Uwe Schmidt — Paderborn University)

Abstract

A Littlewood polynomial is a polynomial in $\mathbb{C}[z]$ having all of its coefficients in $\{-1, 1\}$. There are various old unsolved problems, mostly due to Littlewood and Erdős, that ask for Littlewood polynomials that provide a good approximation to a function that is constant on the complex unit circle, and in particular have small L^α norm on the complex unit circle. Such problems are closely related to questions about the minimisation of the mean-squared aperiodic autocorrelations of binary sequences. Indeed, the L^4 norm of a Littlewood polynomial equals the sum of squared aperiodic autocorrelations of the binary sequence obtained from the coefficients of the polynomial.

We consider polynomials whose coefficients are obtained from additive and multiplicative characters of finite fields, and give explicit and recursive formulas for the limit of the ratio of L^α and L^2 norm of these polynomials when α is an even positive integer and the degree tends to infinity. To our knowledge, these are the first results that give these limiting values for specific sequences of nontrivial Littlewood polynomials and infinitely many α. These results vastly generalise earlier results on the L^4 norm of these polynomials.

Keywords: Littlewood polynomials, L^α norms, characters

Structure of Group Invariant Weighing Matrices of Small Weight

Ka Hin Leung

National University of Singapore

(Joint work with Bernhard Schmidt — Nanyang Technological University)

Abstract

It is well known that for an abelian group G, the existence of G-invariant weighing matrix of weight n is equivalent to the existence of $X \in \mathbb{Z}[G]$ with coefficients $0, \pm 1$ only such that $XX^{(-1)} = n$; and n is called the **weight** of the matrix.

Many group invariant weighing matrices can be constructed as follows. Let H be a subgroup of a finite abelian group G and let $g_1, \ldots, g_K \in G$ be representatives of distinct cosets of H in G. Suppose that $X_1, \ldots, X_K \in \mathbb{Z}[H]$ have coefficients $0, \pm 1$ only and that $\sum_{i=1}^{K} X_i X_i^{(-1)} = n$ and $X_i X_j = 0$ whenever $i \neq j$. It can then be shown that

$$X = \sum_{i=1}^{K} X_i g_i \tag{1}$$

is a G-invariant weighing matrix of weight n.

The main objective of our work is to show that group invariant weighing matrices *necessarily* have the form in Equation (1) if their weight is small compared to order of the underlying group. Moreover, we show that the order of the group H which contains the "building blocks" X_i is bounded by a constant only depending on n. Our main result is the following:

Theorem Let n be a positive integer. Every weighing matrix of weight n invariant under an abelian group G is generated from a subgroup H of G with $|H| \leq 2^{n-1}$.

Keywords: Weighing matrices

A Complete Classification of Partial-MDS (Maximally Recoverable) Codes Correcting one Additional Erasure

Anna-Lena Horlemann-Trautmann

University of St. Gallen

(Joint work with Alessandro Neri — University of Zürich)

Abstract

Partial-MDS (PMDS) codes are a family of locally repairable codes, mainly used for distributed storage. They are defined to be able to correct any pattern of s additional erasures, after a given number of erasures per locality group have occurred. This makes them also *maximally recoverable (MR) codes*, another class of locally repairable codes.

It is known that MR codes in general, and PMDS codes in particular, exist for any set of parameters, if the field size is large enough.[1] Moreover, some explicit constructions of PMDS codes are known, mostly with a strong restriction on the number of erasures that can be corrected per locality group.

In this talk we give a general construction of PMDS codes that can correct any number of erasures per locality group, with the restriction $s = 1$, i.e., only one additional erasure can be corrected. Furthermore, we show that all PMDS codes for the given parameters are of this form, i.e., we give a classification of these codes. This implies a necessary and sufficient condition on the underlying field size for the existence of these codes (assuming that the MDS conjecture is true). This bound on the field size is in general much smaller than the previously known ones.

Keywords: partial-MDS codes, maximally recoverable codes, locally repairable codes, distributed storage

[1] M. Chen, C. Huang, and J. Li. *On the maximally recoverable property for multi-protection group codes*. In 2007 IEEE International Symposium on Information Theory, pages 486–490, June 2007.

Costas cubes

Jonathan Jedwab

Simon Fraser University

(Joint work with Lily Yen — Capilano University)

Abstract

A Costas array is a permutation array for which the vectors joining pairs of 1s are all distinct. We propose a new three-dimensional combinatorial object related to Costas arrays: an order n Costas cube is an array $(d_{i,j,k})$ of size $n \times n \times n$ over $\mathbb{Z}_2$ for which each of the three projections of the array onto two dimensions, namely $(\sum_i d_{i,j,k})$ and $(\sum_j d_{i,j,k})$ and $(\sum_k d_{i,j,k})$, is an order n Costas array.

We determine all Costas cubes of order at most 29, showing that Costas cubes exist for all these orders except 18 and 19 and that a significant proportion of the Costas arrays of certain orders occur as projections of Costas cubes. We then present constructions for two infinite families of Costas cubes.

Keywords: Costas array, three-dimensional, projection

A q-analogue of perfect matroid designs

Relinde Jurrius

University of Neuchâtel, Switzerland

Abstract

Perfect matroid designs (PMD) are matroids where flats of equal rank have equal cardinality. An important class of PMDs are Steiner systems. In the 1970's – 1980's, matroid theory and PMDs helped achieving results about the existence of Steiner systems and designs [1].

Nowadays, the q-analogues of designs and Steiner systems attract much attention. The existence and construction of non-trivial q-Steiner systems seems (at the moment) to be not so easy. Since recently the q-analogue of a matroid was (re-)defined [2], it is natural to ask if the q-analogue of PMD's might help in studying the q-analogues of Steiner systems. In this talk, we set the first steps in this direction and discuss possible further research in this direction.

References

[1] M. Deza, Perfect Matroid Designs, in *Matroid Applications* ed. N. White, pp.54–72, Encyc. Math. Appl. **40**, Cambridge University Press, 1992.

[2] R. Jurrius and R. Pellikaan, *Defining the q-analogue of a matroid*, `arXiv:1610.09250`, submitted.

On a conjecture of Morgan and Mullen

Giorgos Kapetanakis

Sabanci University

(Joint work with Theodoulos Garefalakis — University of Crete)

Abstract

Let $\mathbb{F}_q$ be the finite field of cardinality q and $\mathbb{F}_{q^n}$ its extension of degree n, where q is a prime power and n is a positive integer. A generator of the multiplicative group $\mathbb{F}_{q^n}^*$ is called *primitive*. An $\mathbb{F}_q$*-normal basis* of $\mathbb{F}_{q^n}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ of the form $\{x, x^q, \ldots, x^{q^{n-1}}\}$ and the element $x \in \mathbb{F}_{q^n}$ is called *normal over* $\mathbb{F}_q$. An element of $\mathbb{F}_{q^n}$ that is simultaneously normal over $\mathbb{F}_{q^l}$ for all $l \mid n$ is called *completely normal over* $\mathbb{F}_q$.

It is well-known that primitive and normal elements exist for every q and n. The existence of elements that are simultaneously primitive and normal is also well-known for every q and n. Further, it is also known that for all q and n there exist completely normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Morgan and Mullen [*Util. Math.*, 49:21–43, 1996], took the next step and conjectured that for any q and n, there exists a primitive completely normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

This conjecture is yet to be established for arbitrary q and n, but instead there are have partial results, covering special types of extensions. Recently, Hachenberger [*Des. Codes Cryptogr.*, 80(3):577–586, 2016] using elementary methods, proved the validity of the Morgan-Mullen conjecture for $q \geq n^3$ and $n \geq 37$.

In this work, we use character sum techniques and prove the validity of the Morgan-Mullen conjecture for all q and n, provided that $q > n$. In the talk, the previous results will briefly be presented, our proof will be outlined and possible improvements will be discussed.

Keywords: Morgan-Mullen conjecture, character sums, primitive elements, normal bases, completely normal bases

Number of points of a nonsingular hypersurface in an odd-dimensional projective space

Seon Jeong Kim

Gyeongsang National University, Korea

(Joint work with Masaaki Homma — Kanagawa University, Japan)

Abstract

We consider the numbers of $\mathbb{F}_q$-points of nonsingular hypersurfaces of a fixed degree in an odd-dimensional projective space, and find an upper bound for them. Also we give the complete list of nonsingular hypersurfaces each of which realizes the upper bound. This is a natural generalization of our previous study of surfaces in projective 3-space.

We prove the following theorem.

Theorem. Let n be an odd integer at least 3. Let X be a nonsingular hypersurface of degree $d \geq 2$ in $\mathbb{P}^n$ defined over $\mathbb{F}_q$, and $N(X)$ the number of $\mathbb{F}_q$-points of X. Then

$$N_q(X) \leq \theta_q\left(\frac{n-1}{2}\right) \cdot \left((d-1)q^{\frac{n-1}{2}} + 1\right),$$

where $\theta_q(m)$ denotes the number of $\mathbb{F}_q$-points of $\mathbb{P}^m$, and equality holds if and only if one of the following three cases occurs.

(i) $d = 2$ and X is a nonsingular hyperbolic quadric hypersurface, that is, X is projectively equivalent over $\mathbb{F}_q$ to the hypersurface $\sum_{i=0}^{\frac{n-1}{2}} X_{2i}X_{2i+1} = 0$.

(ii) $d = \sqrt{q}+1$ where q is square, and X is a nonsingular Hermitian hypersurface, that is, X is projectively equivalent over $\mathbb{F}_q$ to the hypersurface $\sum_{i=0}^{\frac{n-1}{2}} (X_{2i}^{\sqrt{q}}X_{2i+1} + X_{2i}X_{2i+1}^{\sqrt{q}}) = 0$.

(iii) $d = q + 1$ and X is a nonsingular $\mathbb{P}^n$-filling hypersurface over $\mathbb{F}_q$, that is, X is projectively equivalent over $\mathbb{F}_q$ to the hypersurface $\sum_{i=0}^{\frac{n-1}{2}} (X_{2i}^{q}X_{2i+1} - X_{2i}X_{2i+1}^{q}) = 0$.

Keywords: Finite field, Hypersurface, Hermitian variety

On Permutation Polynomial Representatives, their Matrices and their Inverses

Megha Kolhekar

Department of Electrical Engineering, IIT Bombay, India

(Joint work with Harish K. Pillai, Department of Electrical Engineering, IIT Bombay, India)

Abstract

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power, and let $\mathbb{F}_q[x]$ be the ring of polynomials in a single indeterminate x over $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial of $\mathbb{F}_q$ if it induces a one-to-one map from $\mathbb{F}_q$ to itself. Permutation Polynomials (PP) over finite fields are interesting objects of study due to their applications in coding theory, combinatorics and cryptography.

Let $\alpha \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_q^*$, where $\mathbb{F}_q^*$ is the group of non-zero elements in $\mathbb{F}_q$. We say that a PP f is equivalent to another PP g if there exist some α and β such that $f = \beta g + \alpha$. With suitable choices of α and β, every PP is equivalent to a monic PP which maps 0 of the field to 0. This "special" representative of the equivalence class is named as the *Permutation Polynomial Representative (PPR)*. We characterize the PPRs through their $(q-1)^{th}$ powers. It is well known that permutation polynomials form a group under the operation of composition. This operation inherently associates a matrix of size $(q-2) \times (q-2)$ with a PPR, which we term as the *PPR Matrix*. We study this matrix and discuss some results on the necessary and sufficient condition for a $(q-2) \times (q-2)$ matrix over $\mathbb{F}_q$ to be a PPR Matrix; constructing compositiona l inverses; as well as the number of permutation polynomials that this matrix divulges.

Keywords: permutation polynomials, polynomial matices, compositional inverses

Curves with large automorphism groups in positive characteristic

Gábor Korchmáros

University of Basilicata (Italy)

(Joint work with M. Giulietti, M. Montanucci and P. Speziali)

Abstract

Let $\mathcal{X}$ be a (projective, geometrically irreducible, non-singular) algebraic curve defined over an algebraically closed field $\mathbb{K}$ of characteristic $p > 0$. We mainly focus on the case where $\mathbb{K}$ is the algebraic closure of a finite field. Let $\mathbb{K}(\mathcal{X})$ be the field of rational functions (the function field of transcendency degree one over $\mathbb{K}$) of $\mathcal{X}$. The $\mathbb{K}$–automorphism group $\mathrm{Aut}(\mathcal{X})$ of $\mathcal{X}$ is defined to be the automorphism group $\mathrm{Aut}(\mathbb{K}(\mathcal{X}))$ consisting of those automorphisms of $\mathbb{K}(\mathcal{X})$ which fix each element of $\mathbb{K}$. $\mathrm{Aut}(\mathcal{X})$ has a faithful action on the set of points of $\mathcal{X}$.

By a classical result, $\mathrm{Aut}(\mathcal{X})$ is finite if the genus g of $\mathcal{X}$ is at least two.

This result raised a general problem for groups and curves: Determine the finite groups that can be realized as the $\mathbb{K}$-automorphism group of some curve with a given invariant. The most important such invariant is the genus g of the curve, and there is a long history of results on the interaction between the automorphism group of a curve and its genus.

In positive characteristic, another important invariant is the p-rank of the curve (also called the Hasse-Witt invariant), which is the integer γ so that the Jacobian of $\mathcal{X}$ has p^γ points of order p. It is known that $0 \le \gamma \le \mathrm{g}$.

In this survey we focus on the following issues:

(i) Upper bounds on the size of G depending on g.

(ii) The possibilities for G when the p-rank is 0.

(iii) Upper bounds on the size of the p-subgroups of G depending on the p-rank.

(iv) Large automorphism group implies zero p-rank.

Keywords: Algebraic curves, automorphisms, positive characteristic

Bivariate polynomial mappings associated with simple complex Lie algebras

Ömer Küçüksakallı

Middle East Technical University, Turkey

Abstract

A polynomial is called exceptional if it induces a permutation over infinitely many residue fields. It is well known that a polynomial is exceptional if and only if it is a composition of linear polynomials, monomials and Chebyshev polynomials. Lidl and Wells have generalized Chebyshev polynomials to several variables and shown that certain such maps induce permutations over infinitely many finite fields. One can show that their multivariate polynomials correspond to a family of maps associated with Lie algebras A_n. In this talk, we will focus on the bivariate polynomial maps associated with the rank-2 simple complex Lie algebras B_2 and G_2. We will give criteria when these bivariate maps induce a permutation over a finite field. Using these criteria, we will disprove a conjecture of Lidl and Wells.

Keywords: exceptional polynomial, Chebyshev polynomial

Upper bounds for partial spreads from divisible codes

Sascha Kurz

University of Bayreuth

(Joint work with D. Heinlein, M. Kiermaier, A. Wassermann and T. Honold)

Abstract

A partial t-spread in $GF(q)^n$ is a collection of t-dimensional subspaces with trivial intersection such that each non-zero vector is covered at most once. How many t-dimensional subspaces can be packed into $GF(q)^n$, i.e., what is the maximum cardinality of a partial t-spread? An upper bound, given by Drake and Freeman [1], survived almost forty years without any improvement. At the end of 2015, the upper bounds started to crumble [2]. Here, the theoretical foundation is provided by the fact that the uncovered points, called holes in this context, form a projective q^{t-1}-divisible linear block code. This allows to apply the linear programming method, i.e., to utilize the so-called MacWilliams identities and the positivity of the coefficients of the weight enumerator of the corresponding dual code. In this talk we will exhibit how this well known approach from coding theory can used to obtain analytical bounds on the maximum size of partial t-spreads that form the present state-of-the-art.

Keywords: Finite geometry, projective geometry, partial spreads, constant dimension subspace codes, divisible codes

References

[1] D.A. Drake and J.W. Freeman, *Partial t-spreads and group constructible (s, r, μ)-nets*, J. Geom. **13**, 2, pp. 210–216 (1979).

[2] S. Kurz, *Packing vector spaces into vector spaces*, Australas. J. Combin. **68**, 1, pp. 122-130 (2017).

SR-construction of linear codes and application to the simplex codes

Mariusz Kwiatkowski

University of Warmia and Mazury

Abstract

I will present a SR-construction of linear codes. The idea for this construction came from the study of the graph of non-degenerate linear codes, and the codes at maximal distance in this graph. For two arbitrary $[n_1, k_1]_q, [n_2, k_2]_q$ codes the SR-construction gives a $[n_1 n_2, k']_q$ code where k' is one smaller or equal to $k_1 + k_2$. So the SR-construction is a binary operation on linear codes over a given finite field. I will discuss properties of this construction and apply it to the simplex codes (codes dual to the binary Hamming codes). In this case the parameters of the resulting codes meet the Griesmer bound.

Keywords: Linear codes, Griesmer bound,

On permutation polynomials of shape $X^k + \gamma \operatorname{Tr}_{q^n/q}(X^d)$

Gohar Kyureghyan

University of Rostock, Germany

Abstract

In this talk we survey recent progress on the characterization and the classification of permutation polynomials on $\mathbb{F}_{q^n}$ of shape $X^k + \gamma Tr_{q^n/q}(X^d)$. Presented results are joint work with Daniel Gerike (Otto-von-Guericke University Magdeburg) and Michael Zieve (University of Michigan).

Keywords: Permutation polynomials, permutation trinomials, trace, switching

On Homogeneous Arcs and Linear Codes over Finite Chain Rings

Ivan Landjev

New Bulgarian University

Abstract

Let R be a finite chain ring with $|R| = q^2$, $R/\mathrm{rad}R \cong \mathbb{F}_q$. A multiarc in the projective Hjelmslev geometry $\Pi_n = \mathrm{PHG}({}_RR^n)$ is a mapping $\mathcal{K} : \mathcal{P} \to \mathbb{N}_0$, where $\mathcal{P}$ is the pointset of Π_n. For every subspace S in Π_n, we set

$$\omega(S) := \mathcal{K}(S) - \frac{1}{q-1}\mathcal{K}([S] - S).$$

Here $[S]$ is the set of all points that are neighbours to a point in S. The multiset $\mathcal{K}$ is called a homogeneous (N, W)-arc if (1) $\mathcal{K}(\mathcal{P}) = N$, (2) $\omega(H) \leq W$ for every hyperplane H, and (3) $\omega(H_0) = W$ for some hyperplane H_0. A code over $\mathbb{F}_q$ (not necessarily linear) is called linearly representable if it can be obtained as the q-ary image of an R-linear code under the Reed-Solomon map: $\psi_{\mathrm{RS}}\colon r = r_0 + r_1\theta \to (r_0, r_1)\begin{pmatrix} 0 & 1 & \zeta & \dots & \zeta^{q-2} \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix}$. Here θ is a generator of $\mathrm{rad}R$, ζ is a primitive element of $\mathbb{F}_q$ and r_i are chosen from a fixed set $\Gamma \cong \mathbb{F}_q$ of q elements from R no two of which are congruent modulo $\mathrm{rad}R$. The importance of the homogeneous arcs is due to the following fact.

Theorem 1. A linearly representable q-ary code with parameters $(Nq, q^{2k}, (q-1)(N-W))$ exists if and only if there exists a homogeneous (N, W)-arc in Π_k, whose support generates the whole geometry Π_k.

In 1984 Bonisoli proved that a linear code in which all non-zero words have the same weight is concatenation of simplex codes. Geometrically, arcs for which all hyperplanes have the same multiplicity are the sum of several copies of the whole space. The next result is an analogue of Bonisoli's theorem.

Theorem 2. Let $\mathcal{K}$ be a homogeneous (N, W)-arc in Π_k. Then $\omega(H) = 0$ for every hyperplane H and $\mathcal{K}$ is a sum of neighbour classes of points.

Keywords: homogeneous arcs, constant weight codes, projective Hjelmslev spaces

On a family of APN quadrinomials

Petr Lisoněk

Simon Fraser University

(Joint work with Faruk Göloğlu and Dáša Krasnayová — Charles University)

Abstract

Let $q = 2^m$. For $b, c, d \in \mathbb{F}_q$ we study functions $F : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ defined by

$$F(x) = x^3 + bx^{3q} + cx^{2q+1} + dx^{q+2}.$$

These functions obey the subspace property characterized by $F(\lambda z) = \lambda^3 F(z)$ for all $\lambda \in \mathbb{F}_q$. They generalize the Kim function defined on $\mathbb{F}_{2^6}$ which Browning, Dillon, McQuistan and Wolfe used to construct an APN (almost perfect nonlinear) permutation of $\mathbb{F}_{2^6}$. We study the conditions on b, c, d under which F is APN. Using Trace-0/Trace-1 decomposition of elements of $\mathbb{F}_{q^2}$ we prove that F is APN if and only if $\mathrm{tr}_1^m(R(T)) = 0$ for all $T \in \mathbb{F}_q$ such that $\mathrm{tr}_1^m(T) = 1$ (with several exceptions allowed), where R is a certain rational function over $\mathbb{F}_q$, and with some additional conditions imposed. We deduce from the form of R that there are one or two large families of APN functions F, depending on the parity of m. Each of the two APN families is characterized by an algebraic condition on b, c, d. We show that APN functions in the first family exist for all m and they are linearly equivalent to the Gold function $f(x) = x^3$, while the APN functions in the second family exist only for even m and they are linearly equivalent to the Gold function $f(x) = x^{2^{m-1}+1}$. By counting points on a certain algebraic curve over $\mathbb{F}_q$ we prove that if F is APN and $m > 3$, then F belongs to one of the two families introduced above. For $m \leq 3$ we show that the only other case when F is APN occurs when $m = 3$ and F is CCZ equivalent to the Kim function.

Keywords: APN function, APN permutation, subspace property

Pre-sympletic semifields

Giovanni Longobardi

University of Naples "Federico II"

(Joint work with Guglielmo Lunardon)

Abstract

Using the known sympletic semifields of order q^3, q a prime power, and exploiting a projection argument in $PG(2, q^3)$, we will construct a family of semifields called $pre\text{-}sympletic\ semifields$ which have rank three on their left nucleus.
In even characteristic we will exhibit a new semifield with center $\mathbb{F}_2$, which belongs to the relevant family.

Keywords: Semifields, spreads, translation planes, linear sets.

Collision-free bounds for the BSV hash

Ariane Masuda

New York City College of Technology, CUNY

(Joint work with Sandie Han, Satyanand Singh and Johann Thiel)

Abstract

Let $L_u = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$ and $R_v = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}$ be matrices in $SL_2(\mathbb{Z})$ with $u, v \geq 1$. In 1991, Zémor developed a hash function over finite fields based on L_1 and R_1. Recently, Bromberg, Shpilrain, and Vdovina proposed a hash function based on L_u and R_v when $u = v \in \{2, 3\}$. For these values of u and v, they analyzed the girth of the Cayley graph of the monoid generated by L_u and R_v. As a consequence, they obtained lower bounds on the length of collisions for the corresponding hash functions. By using ideas from our previous work on (u,v)-Calkin-Wilf trees generated by L_u and R_v, we extend their results for any $u, v \geq 1$.

Keywords: hash function, collision, Calkin-Wilf tree

Improved decoding of Quick Response (QR) codes

Todd Mateer

Department of Defense

Abstract

Quick response (QR) codes have recently become a popular method to communicate information to smartphones equipped with cameras. This paper introduces a new technique which can allow for the correction of many additional mistakes in received QR codes. By improving smartphones to use the decoding algorithms described in this paper, advertisers can exploit this additional decoding capability to integrate elaborate company logos into QR codes.

Keywords: QR codes, Reed-Solomon codes

The (weak) cylinder conjecture and its reduction to a weight function in AG$(2, p)$

Sam Mattheus

Vrije Universiteit Brussel, Belgium

(Joint work with J. De Beule — VUB, J. Demeyer — UGent, P. Sziklai — ELTE Budapest)

Abstract

The (strong) cylinder conjecture states that a set S of p^2 points in AG$(3, p)$ such that every plane contains $0 \pmod p$ of S must be a cylinder (which consists of p parallel lines). Many researchers have tried to attack this problem, and its weaker version, without success. We reduce the problem to a question concerning a function $w(X, Y) : \mathrm{AG}(2, p) \to \mathbb{F}_p$ satisfying 4 properties. We will discuss this reduction and its relation to the original problem. In particular, showing that there exists no such function $w(X, Y)$ implies the (weak) cylinder conjecture. Using this fact, we have shown, assisted by a computer, that the weak cylinder conjecture is true for all primes at most 13.

Keywords: weight function, affine plane, cylinder conjecture

Bent function generalizations and their transforms

Wilfried Meidl

RICAM, Linz, Austria

(Joint work with S. Hodzic, E. Pasalic, FAMNIT, Koper; N. Anbar, RICAM)

Abstract

For two (abelian) groups G, N, a bent function $f : G \to N$ is a function for which the character sum $\sum_{x\in G} \chi(x, f(x))$ has absolute value $\sqrt{G}$ for all characters χ of $G \times N$ which are non-principal on $\{0\} \times N$, and 0 otherwise (except for $\chi = \chi_0$). The graph $\{(x, f(x)) : x \in G\}$ of f is then a relative difference set in $G \times N$. The classical examples are functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, for which the *Walsh transform* $\mathcal{W}_f(u) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}(ux)}$ has absolute value $2^{n/2}$ for all $u \in \mathbb{F}_{2^n}$. Alternatively, $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is bent iff $f(x + a) + f(x)$ is balanced for every nonzero $a \in \mathbb{F}_{2^n}$. Many classes of bent functions f are known from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, and more general from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$, $m|n$, f is then a vector space of dimension m of Boolean (p-ary) bent functions.

Functions f from $\mathbb{F}_{2^n}$ to the cyclic group $\mathbb{Z}_{2^k}$ are bent if $\mathcal{H}_f(\alpha, u) = \sum_{x\in\mathbb{F}_{2^n}} \zeta_{2^k}^{\alpha f(x)}(-1)^{\mathrm{Tr}(ux)}$, $\zeta_{2^k} = e^{2\pi i/2^k}$, has absolute value $2^{n/2}$ for all nonzero $\alpha \in \mathbb{Z}_{2^k}$ and $u \in \mathbb{F}_{2^n}$. Such bent functions seem rare, the standard examples are obtained from spreads of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. Motivated by applications in CDMA systems (for $k = 2$), functions satisfying $|\mathcal{H}_f(1, u)| = 2^{n/2}$ for all $u \in \mathbb{F}_{2^n}$ have been defined as gbent functions. Though such functions in general do not yield relative difference, they are interesting as they correspond to affine spaces of Boolean bent or semibent functions. In joint work with Hodzic and Pasalic we completely characterize those affine spaces which are the gbent functions. This is a crucial step towards a possible classification of gbent functions.

A generalization of a different type is obtained if one requires that $f(a + x) + f(x) + \mathrm{Tr}(cax)$ is balanced for a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. For $c = 0$ such a function is bent, for $c = 1$ it is called a univariate negabent function. In joint work with Anbar we describe these functions with character sums over certain groups, which then directly connects them with relative difference in those groups. One motivation comes from connections to modified planar functions.

Keywords: Bent function, Walsh transform, gbent function, negabent function

On the pseudorandomness of automatic sequences

László Mérai

RICAM (Austrian Academy of Sciences)

(Joint work with Arne Winterhof — RICAM (Austrian Academy of Sciences))

Abstract

A k-automatic sequence (s_n) over an alphabet $\mathcal{A}$ is the output sequence of a finite automaton, where the input is the k-ary digital expansion of n. Classical examples for 2-automatic sequences are the Thue-Morse and the Rudin-Shapiro sequences.

For a prime $k = p$, p-automatic sequences (s_n) over the finite field $\mathcal{A} = \mathbb{F}_p$ of p elements can be characterized by a result of Christol: a sequence is p-automatic if and only if its generating function is algebraic over $\mathbb{F}_p[x]$.

We give lower and upper bounds on the Nth linear complexity of p-automatic sequences in terms of the characteristic equation of the generating function of the sequence. Consequently, we show that any p-automatic sequence over $\mathbb{F}_p$ which is not ultimately periodic has Nth linear complexity of (best possible) order of magnitude N.

We also study the correlation measure of k-automatic binary sequences. We give lower bound on the Nth correlation measure of order 2 of k-automatic sequences in terms of the generating automaton. Specially, we obtain that any binary k-automatic sequence has Nth correlation measure of order 2 of (worst possible) order of magnitude N.

Thus these sequences are the first examples which have good linear complexity but bad correlation measure simultaneously.

Keywords: sequences, pseudorandom, automatic sequences, linear complexity, correlation measure

On the nonlinearity of Boolean functions with restricted input

Sihem Mesnager

Université de Paris VIII

Abstract

At Eurocrypt 2016, Meaux et *al.* proposed a new stream cipher construction FLIP intended in Fully Homomorphic Encryption. The main feature of that new stream cipher is that the Hamming weight of the stream register is invariant. The classical cryptographic features as balancedness, nonlinearity and algebraic immunity have therefore to be revisited. Indeed, they are designed to Boolean functions on the vectorspaces $\mathbb{F}_2^n$ and not to Boolean functions whose inputs are restricted to subsets E of $\mathbb{F}_2^n$. Very recently, Carlet et *al* introduce the notion of nonlinearity over a subset E of $\mathbb{F}_2^n$: $NL_E(f) = \frac{\#E}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\left|\sum_{x\in E}(-1)^{f(x)+a\cdot x}\right|$ (here $\#$ denotes the cardinality of E). They established an upper bound involving the derivatives of the Boolean function : $NL_E(f) \leq \frac{\#E}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\sqrt{\#E + |\sum_{x,x+a\in E}(-1)^{D_af(x)}|}$. We have pushed further the analysis initiated by Carlet et *al* and establish a better, but more complex, upper bound :

Theorem 1.

$$NL_E(f) \leq \frac{\#E}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\sqrt{\#E + |\sum_{x,x+a\in E}(-1)^{D_af(x)}| + R(f,E,a)},$$

where $R(f,E,a) \geq 0$ *for every* $a \in \mathbb{F}_2^n$.

Due to the page limitation, we cannot give the exact expression of $R(f,E,a)$. However we indicate that its expression involves sums of the form $\sum_{x,x+u\in E}(-1)^{D_uf(x)}$. The core of our approach is that we link the question of estimating $NL_E(f)$ with sums of power of Walsh transform of f.

Secondly, the motivation of NL_E being purposed to analyze the security of FLIP, we specialize our study to the case where all the elements of E have the same weight.

Keywords: Homomorphic Fully Encryption, Boolean functions, Nonlinearity, Walsh transforms

Regular patterns of Irreducible Polynomials

Giacomo Micheli

University of Oxford

Abstract

In this talk we first survey the recent developments in the context of dynamically irreducible polynomials [1, 2]. This is a joint work with D. R. Heath-Brown (University of Oxford). Once this is done, we explain a new connection between the theory of irreducible polynomials over finite fields and the theory of finite automata [3]. This is a joint work with A. Ferraguti (University of Cambridge) and R. Schnyder (University of Zurich). In particular, we set up an infrastructure which allows the use of machinery from automata theory to address irreducibility questions for a special class of polynomials which has been widely studied in the literature (i.e. decomposable polynomials). Interestingly enough, such bridge can be constructed by means of elementary tools. In turn, it seems that this idea allows synergic combination of tools from the theory of finite fields and from the theory of regular languages. As an example, we are able to show non-trivial rational patterns in certain infinite subsets of primes of $\mathbb{F}_q[x]$, where $\mathbb{F}_q$ is a finite field (see [3, Theorem 3.10]). The theory seems also to lift quite naturally to the context of local fields. New questions arise from this framework.

Keywords: Finite Fields, Automata, Irreducible Polynomials, Semigroups, Graphs.

References

[1] A. Ferraguti, G. Micheli and R. Schnyder, On sets of irreducible polynomials closed by composition, *Lecture Notes in Computer Science*, 10064 pp. 77–83 (2017).

[2] D.R. Heath-Brown, G. Micheli, Irreducible polynomials over finite fields produced by composition of quadratics, arXiv preprint arXiv:1701.05031 (2017).

[3] A. Ferraguti, G. Micheli, R. Schnyder Irreducible compositions of degree two polynomials over finite fields have regular structure, arXiv preprint arXiv:1701.06040 (2017).

$\mathbb{F}_{p^2}$-maximal curves with many automorphisms are Galois-covered by the Hermitian curve

Maria Montanucci

Universitá degli studi della Basilicata

(Joint work with Daniele Bartoli and Fernando Torres)

Abstract

The Hermitian curve $\mathcal{H}_q : y^q+y = x^{q+1}$, for a prime power q, is the best known example of $\mathbb{F}_{q^2}$-maximal curves; i.e curves whose number $N(\mathcal{H}_q)$ of $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound $N(\mathcal{H}_q) = q^2 + 1 + 2g(\mathcal{H}_q)q$. Each curve $\mathcal{Y}$ which is covered by an $\mathbb{F}_{q^2}$-maximal curve is also $\mathbb{F}_{q^2}$-maximal. It is an open problem to decide whether any $\mathbb{F}_{p^2}$-maximal curve is $\mathbb{F}_{p^2}$-covered by the Hermitian curve $\mathcal{H}_p$ or not. We give an affirmative answer for $\mathbb{F}_{p^2}$-maximal curves $\mathcal{X}$ having a large automorphism group, showing that if $|Aut(\mathcal{X})| > 84(g(\mathcal{X}) - 1)$ then $\mathcal{X}$ is Galois covered by $\mathcal{H}_p$. Moreover, we show that this result does not extend to curves whose full automorphism group satisfies $|Aut(\mathcal{X})| \leq 84(g(\mathcal{X}) - 1)$, as we construct an $\mathbb{F}_{71^2}$-maximal curve $\mathcal{F}$ of genus 7, having a Hurwitz automorphism group of order 504 which is not Galois covered by $\mathcal{H}_{71}$. The curve $\mathcal{F}$ is the positive characteristic analog of the so called Fricke-MacBeath curve in zero characteristic, and it is the first known example of $\mathbb{F}_{p^2}$-maximal curve which is not Galois-covered by the Hermitian curve $\mathcal{H}_p$.

Keywords: Maximal curves, Hermitian curve, Fricke-MacBeath curve

P-Chain Codes

Beatriz Motta

Universidade Federal de Juiz de Fora

(Joint work with P. Esperidião and A. Moura - Universidade Federal de Viçosa)

Abstract

Let P be a partially ordered set (poset) on the set $[n] = \{1, 2, ..., n\}$, the set of ordered coordinate positions of $\mathbb{F}_q^n$. It is known that P gives rise to a $P-$distance between two vectors $u, v \in \mathbb{F}_q^n$, namely $d_P(u, v) = |supp\,\langle v - u\rangle\,|$.

A $P-$linear code C is a vector subspace of the $P-$space $(\mathbb{F}_q^n, d_P)$ which we refer to as an $[n, k]_q\, P-$code if $\dim C = k$. We define the $P-$ weight of a subspace $D \subseteq \mathbb{F}_q^n$ as $w_P(D) := |\,\langle suppD\rangle_P\,|$ and the $r-$th minimal generalized $P-$weight of an $[n, k]_q\, P-$ code C as

$$d_r^P(C) = \min\{w_P(D) | D \subseteq C,\ \dim D = r\}.$$

An $[n, k]_q\, P-$code C is said to be a $P-$ chain code if there is a sequence of linear subspaces $\{0\} = D_0 \subseteq D_1 \subseteq D_2 \subseteq \cdots \subseteq D_k = C$ such that $w_P(D_r) = d_r^P(C)$ and $\dim D_r = r$ for every $r \in \{1, 2, ..., k\}$. In this work we present some sufficient conditions for the existence of a $P-$chain code improving the previous work by A. Moura and M. Firer, Duality for Poset Codes.

Keywords: Posets, P-Codes, P-Chain

Counting Extended Irreducible Binary Goppa Codes of Degree $2p$ and Length $2^n + 1$

Augustine Musukwa

University of Trento

(Joint work with John A. Ryan — Mzuzu University)

Abstract

Let n and p be odd primes such that $p \neq n$. An upper bound on the number of inequivalent extended irreducible binary Goppa codes of degree $2p$ and length $2^n + 1$ is produced. Examples are included to illustrate our results.

Keywords: Goppa codes, Extended codes, Irreducible Goppa codes, Equivalent codes

Construction of binary quantum codes on closed orientable surfaces

Avaz Naghipour
Department of Computer Engineering, University College of Nabi Akram

Abstract

In this paper we construct classes of new binary quantum error-correcting codes on closed orientable surfaces. These codes are derived from self-dual orientable embeddings of complete bipartite graphs and complete multipartite graphs on the corresponding closed orientable surfaces. We also show a table comparing the rate of these quantum codes when fixing the minimum distance to 3 and 4.

Keywords: quantum codes; self-dual; orientable surfaces; embeddings; bipartite graphs; multipartite graphs

On the computer algebra implementation of Hermitian codes

Gábor P. Nagy
Budapest University of Technology and University of Szeged
(Hungary)

Abstract

Let $\mathcal{X}$ be an irreducible algebraic curve over the finite field $\mathbb{F}_q$, G an $\mathbb{F}_q$-rational divisor of $\mathcal{X}$ and $P_1, \ldots, P_n$ smooth points of $\mathcal{X}$ defined over $\mathbb{F}_q$. Then one can construct the functional code $C_{\mathcal{L}}(D, G)$ and the differential code $C_{\Omega}(D, G)$, where $D = P_1 + \cdots + P_n$. Special cases are the generalized Reed-Solomon codes, the BCH codes and the Goppa codes over curves of genus 0. Algebraic geometry codes have good parameters and decoding algorithms exists with polynomial complexity with respect to their length and dimension.

Our aim is to implement the codes over Hermitian curves in the computer algebra system GAP4. In this talk, I will survey the available tools and their limitations. I also would like to present the main steps of the implementation:

(1) Hermitian function fields over $\overline{\mathbb{F}}_{q^2}$ with elements as bivariate polynomials and their reduction modulo $X^{q+1} - Y^q - Y$.

(2) Places, divisors and their arithmetics.

(3) Action of the Frobenius automorphism $x \to x^{q^2}$ on functions, places and divisors. Rationality.

(4) Computation of Riemann-Roch spaces and the corresponding functional codes.

(5) Implementing the decoding algorithms.

Keywords: Hermitian codes, computer algebra, decoding

On linear Generalized Twisted Gabidulin codes and the existence of new MRD codes

Alessandro Neri

University of Zürich

(Joint work with Stefano De Salvo — University of Pisa)

Abstract

Codes in the rank metric have been introduced by Gabidulin and Delsarte, and recently have gained a lot of interest due to their application in network coding. An mportant class of rank metric codes is the one of Maximum Rank Distance (MRD) codes, that are the equivalent of Maximum Distance Separable codes in the rank metric. The first important construction of MRD codes is given by Kshevetskiy and Gabiudlin. These codes are called Generalized Gabidulin codes.

Despite it has been shown that almost every linear code is MRD, for many years only few different new constructions of MRD codes have been discussed. In 2016 Twisted Gabidulin codes have been introduced by Sheekey, and then generalized by Lunardon et al. These codes are constructed as a slight modification of Gabidulin codes, by introducing a parameter η whose norm is not equal to $(-1)^{km}$, where k is the dimension of the code and m is the degree of the extension field.

Let q be a prime power, and m be a positive integer. In our work we focus only on $\mathbb{F}_{q^m}$-linear codes. In this framework a Generalized Twisted Gabidulin code of dimension k has the property that is contained in a Generalized Gabidulin code of dimension $k+1$ and contains a Generalized Gabidulin code of dimension $k-1$. However, we show that this property is not characterizing, i.e. there exist other MRD codes with the same property. In particular, we prove that the condition on the norm of η to be different from $(-1)^{km}$ is not necessary for almost every m. In order to do that, we transform the problem in a multilinear algebra problem over finite fields involving Plücker embedding and we also give an easy proof of the fact that $\mathbb{F}_{q^m}$-linear Generalized Twisted Gabidulin codes are MRD.

Keywords: rank-metric codes, twisted Gabidulin codes, algebraic coding theory

The Lefschetz properties of monomial algebras over finite fields

Lisa Nicklasson

Stockholm University

(Joint work with Samuel Lundqvist — Stockholm University)

Abstract

A graded algebra is said to have the weak Lefschetz property if there is a linear form such that multiplication by this form has maximal rank in every degree. The algebra has the strong Lefschetz property if all powers of this linear form also induces multiplication maps of maximal rank. We will consider monomial complete intersection algebras, i. e. algebras of the type $k[x_1, \dots, x_n]/(x_1^{d_1}, \dots, x_n^{d_n})$, where k is a field. There have been several papers on the presence of the Lefschetz properties of these algebras over the last few years, both considering $k = \mathbb{C}$ and k of positive characteristic. Remarkable is that all results on positive characteristic have been under the assumption that the residue field is infinite. In this talk we will see some recent results, and most important, we will see that all the results on positive characteristic also hold over finite fields.

Keywords: Lefschetz properties, graded algebras

Binary three-weight linear codes from partial geometric difference sets

Oktay Ölmez

Ankara University

Abstract

Links between linear codes, non-linear functions from cryptography, graphs and combinatorial designs have attracted the attention of many researchers over the last 50 years. Difference set method is a powerful tool to construct designs and explore the links between designs and many other combinatorial objects.

In this talk, we will introduce a generalization of $(v, k, \lambda)-$difference sets known as partial geometric difference sets. In particular, we will show that existence of a family of partial geometric difference sets is equivalent to existence of a certain family of three-weight linear codes. We also provide a link between binary plateaued functions, three-weight linear codes and partial geometric difference sets.

Keywords: partial geometric designs, partial geometric difference sets, plateaued functions, three-weight linear codes

Self-duality of generalized twisted Gabidulin codes

Ferruh Özbudak

Middle East Technical University, Ankara, Turkey

(Joint work with Kamil Otal and Wolfgang Willems)

Abstract

Self-duality of Gabidulin codes were investigated in [1]. The authors provided an if and only if condition for a Gabidulin code to be equivalent to a self-dual maximum rank distance (MRD) code. In this paper, we study the same problem for generalized twisted Gabidulin codes (a larger family of linear MRD codes including Gabidulin codes). We observe that the condition stated in [1] also holds for generalized Gabidulin codes (an intermediate family between Gabidulin codes and generalized twisted Gabidulin codes). However, outside of the family of generalized Gabidulin codes there are no generalized twisted Gabidulin codes which are equivalent to self-dual MRD codes. Our tools are similar to those in [1], but we also use linearized polynomials, which allows us to construct some additional tools and direct proofs.

Keywords: Rank metric codes, self-dual maximum rank distance (MRD) codes, generalized twisted Gabidulin codes, linearized polynomials.

References

[1] G. Nebe and W. Willems, On self-dual MRD codes, Advances Math.Comm. 10 (2016), 633-642.

Some Recent Results on LCD Codes

Buket Özkaya

Sabanci University, İstanbul

Abstract

Linear complementary dual (LCD) codes are linear codes that intersect with their dual trivially. Several constructions of LCD codes using orthogonal matrices, self-dual codes, combinatorial designs and Gray map from codes over the rings were given in [3], along with a linear programming bound on the largest size of an LCD code of given length and minimum distance.

In [4], the class of quasi-cyclic LCD codes was shown to be "good", by using their concatenated structure and a characterization of Hermitian LCD codes. Explicit constructions from codes over larger alphabets were also given.

Recently, some classes of one-generator quasi-twisted codes, namely LCD multinegacirculant codes, are shown to be not only good, but better than the Varshamov-Gilbert bound. Their concatenated structure yields exact enumeration results for index 2 and index 3, whereas for a general index t and co-index power of 2, a special enumeration is given which is needed for the asymptotic analysis by means of Dickson polynomials. In [2], analogous techniques were used to characterize and enumerate self-dual double negacirculant codes, which also have infinite families with relative distance satisfying a modified Varshamov-Gilbert bound.

References

[1] A. Alahmadi, C. Güneri, B. Özkaya, H. Shoaib and P. Solé, "On linear complementary-dual multinegacirculant codes", *submitted*.

[2] A. Alahmadi, C. Güneri, B. Özkaya, H. Shoaib and P. Solé, "On self-dual double negacirculant codes", *Disc. Appl. Math.*, vol. 222, 205-212, 2017.

[3] S.T. Dougherty, J.-L. Kim, B. Özkaya, L. Sok and P. Solé, "The combinatorics of LCD codes: Linear programming bound and orthogonal matrices", *Int. J. Inf. and Cod. Theory*, vol. 4, no. 2/3, 116-128, 2017.

[4] C. Güneri, B. Özkaya and P. Solé, "Quasi-cyclic complementary dual codes", *Finite Fields Appl.*, vol. 42, 67-80, 2016.

The Graph Structure of Chebyshev Polynomials over Finite Fields

Daniel Panario

Carleton University

(Joint work with C. Qureshi, Carleton University)

Abstract

The iteration of polynomials and rational functions over finite fields have become an active research topic. These dynamical systems have found applications in diverse areas, including cryptography, biology and physics. In cryptography, iterations of functions over finite fields were popularized by the Pollard rho algorithm for integer factorization; its variant for computing discrete logarithms is considered the most efficient method against elliptic curve cryptography based on the discrete logarithm problem.

When we iterate functions over finite structures, there is an underlying natural functional graph. For a function f over a finite field $\mathbb{F}_q$, this graph has q nodes and a directed edge from vertex a to vertex b if and only if $f(a) = b$. It is well known, combinatorially, that functional graphs are sets of connected components, components are directed cycles of nodes, and each of these nodes is the root of a directed tree from leaves to its root.

Some functions over finite fields when iterated present strong symmetry properties. These symmetries allow mathematical proofs for some dynamical properties such as period and preperiod of a generic element, (average) "rho length", number of connected components, cycle lengths, etc. We are interested on these kinds of properties for Chebyshev polynomials over finite fields. Previous results for iterations of Chebyshev polynomials over finite fields have been given by Gassert (2014).

We describe the functional graph of Chebyshev polynomials of any degree over a finite field of odd characteristic. Then, we use our structural results to obtain estimates for the average rho length, average number of connected components and the expected value for the period and preperiod of iterating Chebyshev polynomials.

Keywords: Chebyshev polynomials, iteration of functions, period.

Isometric embeddings of Johnson graphs in Grassmann graphs and generalized arcs

Mark Pankov

University of Warmia and Mazury

Abstract

A k-arc in the n-dimensional projective space $\mathrm{PG}(n,q)$ is a set of k points such that $k \geq n+1$ and any $n+1$ points from this subset span the projective space. We define an *m-independent k-arc in* $\mathrm{PG}(n,q)$ with $m \leq n+1$ as a set of k points such that $k \geq m$ any m points from this subset span an $(m-1)$-dimensional subspace. Using such generalized arcs we classify isometric embeddings of Johnson graphs in Grassmann graphs.

Keywords: generalized arc, Johnson graph, Grassmann graph

Ovoids of $\mathcal{H}(3, q^2)$, q odd, admitting a group of order $\frac{(q+1)^3}{2}$

Francesco Pavese

Politecnico di Bari

Abstract

Let $\mathcal{H}(3, q^2)$ be the incidence structure of all points and lines (generators) of a non–degenerate Hermitian surface of $\mathrm{PG}(3, q^2)$. $\mathcal{H}(3, q^2)$ is a generalized quadrangle of order (q^2, q), with linear automorphism group $\mathrm{PGU}(4, q^2)$. An *ovoid* of a generalized quadrangle $\mathcal{Q}$ is a set of points of $\mathcal{Q}$ meeting every line of $\mathcal{Q}$ in exactly one point. Ovoids of generalized quadrangles and finite classical polar spaces have been intensively investigated by many authors, especially in the last three decades.

In this talk I will present a new ovoid $\mathcal{O}$ of the Hermitian surface $\mathcal{H}(3, q^2)$, $q > 3$ odd. In particular, $\mathcal{O}$ is left invariant by a group of order $\frac{(q+1)^3}{2}$, it cannot be obtained from a Hermitian curve by means of multiple derivation and it is not locally Hermitian.

Keywords: Hermitian surface, ovoid.

Symplectic semifield spreads of PG$(5, q)$, q even

Valentina Pepe

Sapienza University of Rome

Abstract

It is well known that a symplectic semifield spread of PG$(3, q)$ must be a Desarguesian spread, provided q is not "small". We prove an analogous result for the 5-dimensional space.

Let $q > 2 \cdot 3^{4t}$ be even. We prove that the only symplectic semifield spread of PG$(5, q^t)$, whose associate semifield has center containing $\mathbb{F}_q$, is the Desarguesian spread. We do that by proving that the only possible $\mathbb{F}_q$-linear set of rank $3t$ in PG$(5, q^t)$ disjoint from the secant variety of the Veronese surface is a plane of PG$(5, q^t)$.

Keywords: Semifield spread, linear set

New Constructions of Permutation Polynomials with the Form of $xh\left(x^{q-1}\right)$ over $\mathbb{F}_{q^2}$

Longjiang Qu

National University of Defence Technology

(Joint work with Kangquan Li and Chao Li)

Abstract

Permutation polynomials over finite fields constitute an active research area for their wide applications in cryptography, coding theory, communication theory, etc. For example, Dobbertin proved that the power function x^{2^m+3} on $\mathbb{F}_{2^{2m+1}}$ is an APN function and the key of his proof was the discovery of a class of permutation trinomials. Recently, some authors constructed permutation trinomials with the form of $x^r h\left(x^{q-1}\right)$ over $\mathbb{F}_{q^2}$, where $q=2^k$, $h(x)=1+x^s+x^t$ and $r,s,t,k>0$ are integers. The main methods they used were similar, which transformed the problem of proving permutation polynomials over $\mathbb{F}_{q^2}$ into that of showing permutations over μ_{q+1}, where $\mu_{q+1}:=\{x\in\mathbb{F}_{q^2}: x^{q+1}=1\}$. If $\gcd\left(r,q^2-1\right)=1$, we may assume that $r=1$. Motivated by these results, we consider the permutation polynomials with the form of $xh\left(x^{q-1}\right)$ over $\mathbb{F}_{q^2}$, where $h(x)\in\mathbb{F}_q[x]$ and $q=2^k$. Let $T:=\{b\in\mathbb{F}_q:\mathrm{Tr}(b)=1\}$, where $\mathrm{Tr}(\cdot)$ is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_2$. Let $h(x)\in\mathbb{F}_q[x]$ and $h(x)\neq 0$ for any $x\in\mu_{q+1}$. We find a direct relationship between $f(x)=xh\left(x^{q-1}\right)$ permuting $\mathbb{F}_{q^2}$ and $L(b)=b+l(b)+l(b)^2$ permuting T, where $l(b)$ is a rational function over T, and $l(b)$ and $h(x)$ can be determined from each other by an algorithm. Hence our method transforms the problem of proving permutation polynomials over $\mathbb{F}_{q^2}$ into that of showing permutations over T, which is distinguish from most known results which were investigated over μ_{q+1}. With this new method, more new permutation polynomials with the form of $xh\left(x^{q-1}\right)$ over $\mathbb{F}_{q^2}$ are constructed from some $l(b)$ over T with special forms, such as monomials, linearized polynomials and so on. Several known permutation trinomials are also reconstructed. It seems that some newly constructed permutation polynomials cannot be proved by previous methods easily.

Keywords: Permutation Polynomials, Rational Function, Finite Fields

On constacyclic codes over a class of finite local non-chain Frobenius rings

Horacio Tapia-Recillas

Universidad Autónoma Metropolitana-I, México City

(Joint work with C. Castillo-Guillén and C. Rentería-Márquez, México City)

Abstract

The study of linear codes over finite rings, following the work of R. Hammons et al., has generated results in several directions including the description of structural properties of codes over several families of finite rings, particularly finite fields and finite chain rings. Finite Frobenius rings represent an interesting family of rings in Coding theory due to the fact that MacWilliams identities on the weight enumerator polynomial of a linear code are satisfied (Wood). Finite chain rings are a subfamily of the family of finite Frobenius local rings. Recently a finite local non-chain Frobenius ring with 2^4 elements and results on codes over this ring were considered (Martínez-Moro, Szabo).

The purpose of this talk is two-fold. First, the family of finite local non-chain Frobenius rings of length 4 (hence of nilpotency index 3) is determined and, as a by-product, all finite local Frobenius non-chain rings with p^4 elements, (p a prime) are given. Second, the number and structure of γ-constacyclic codes over finite local Frobenius non-chain rings with nilpotency index 3, of length relatively prime to the characteristic of the residue field of the ring, is determined.

Keywords: Chain rings, Frobenius rings, constacyclic codes.

On the factorization of polynomials of the form $f(x^n)$ over finite fields

Lucas Reis

Universidade Federal de Minas Gerais

(Joint work with F.E. Brochero Martinez — Universidade Federal de Minas Gerais)

Abstract

Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and exponent e and n be a positive integer such that $\nu_p(q-1) \geq \nu_p(e) + \nu_p(n)$ for all prime divisors p of n. In this talk we show a fast algorithm to determine the irreducible factors of $f(x^n)$. As an application of our main result, we explore the factorization of some classes of cyclotomic polynomials.

Keywords: Factorization of Polynomials, Cyclotomic Polynomials

On Arcs with High Divisibility Related to Linear Codes

Assia Rousseva

Sofia University

(Joint work with Ivan Landjev, New Bulgarian University)

Abstract

An arc $\mathcal{F}$ in $\mathrm{PG}(r,q)$ is called a $(t \mod q)$-arc if the multiplicity of each line is congruent to t modulo q. The sum of a $(t_1 \mod q)$- and a $(t_2 \mod q)$-arc is a $(t \mod q)$-arc with $t = t_1 + t_2 \mod q$. Hence the sum of t hyperplanes is a $(t \mod q)$-arc. The so-called lifting construction produces a broad class of such arcs in the projective geometries of arbitrary dimension. The $(t \mod q)$-arcs associated with t-quasidivisible codes have the additional property that the multiplicity of each point is at most t.

In this talk we consider $(t \mod q)$-arcs in geometries over prime fields $\mathbb{F}_p$, p a prime. We prove that every $(0 \mod p)$-arc in $\mathrm{PG}(r,p)$ is the sum of the complements of hyperplanes. Hence every $(0 \mod p)$-arc is the sum of lifted $(0 \mod p)$-arcs. Furthermore, we prove using a result of Blokhuis that every plane $(0 \mod p)$-arc is the sum of at most p lifted arcs.

We discuss applications of these results to the existence problem for linear codes with parameters $[104, 4, 82]_5$ and $[204, 4, 162]_5$.

Acknowledgments. This research has been supported by the Science Research Fund of Sofia University.

Keywords: $(t \mod q)$-arcs, lifted arcs, optimal linear codes, extendable codes

Concatenated Structure and a Minimum Distance Bound for Generalized Quasi-Cyclic Codes

Elif Saçıkara

Sabanci University

(Joint work with Güneri - Özbudak - Özkaya - Sepasdar - Solé)

Abstract

Generalized quasi-cyclic (GQC) codes are mixed alphabet codes over a family of ring alphabets. Namely, if $R_j := {}^{F_q[x]}/_{\langle x^{m_j}-1\rangle}$ for each $j = 0, \ldots, \ell-1$ and positive integers $m_0, \ldots, m_{\ell-1}$, an $F_q[x]$-submodule of $R' := R_0 \times \cdots \times R_{\ell-1}$ is called a GQC code. Compared to the special case of quasi-cyclic (QC) codes, allowing integers m_j to be different gives freedom on the length of the code. We present a concatenated structure for GQC codes, which is more complicated to express than the QC case. Compatibility of the concatenated decomposition and the Chinese Remainder Theorem decomposition is also shown, which extends the analogous result of Güneri-Özbudak for QC codes. Concatenated structure also leads to a general minimum distance bound, extending the analogous bound for QC codes due to Jensen.

(This work is supported by TÜBİTAK, project number 114F432.)

Keywords: quasi-cyclic codes, concatenated codes, generalized concatenated codes, generalized quasi-cyclic codes

On the number of inequivalent MRD codes

Kai-Uwe Schmidt

Paderborn University, Germany

(Joint work with Yue Zhou — National University of Defense Technology, China)

Abstract

Maximum rank-distance (MRD) codes are extremal codes in the space of $m \times n$ matrices over a finite field, equipped with the rank metric. Up to generalizations, the classical examples of such codes were constructed in the 1970s by Delsarte and are popular today under the name Gabidulin codes. Motivated by several recent approaches to construct MRD codes that are inequivalent to Gabidulin codes, we study the equivalence issue for Gabidulin codes themselves. This shows in particular that the family of Gabidulin codes already contains a huge subset of MRD codes that are pairwise inequivalent, provided that $2 \leq m \leq n - 2$.

Existence of normal elements with prescribed trace vectors over finite fields

P.L. Sharma

Department of Mathematics and Statistics, Himachal Pradesh University, Shimla (India)

Abstract

Normal bases over finite fields have been widely used in many applications of coding theory and cryptography. The normal bases are also important for Frobenius mapping and efficient for the implementation of the arithmetic of finite fields. Also, the self dual normal bases are of much importance for Frobenius mapping as well as for trace calculations. Let α be a normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and $u = \{u_0, u_1, ..., u_{n-1}\}$ be a vector of $\mathbb{F}_{2^n}$. The vector u is symmetric if $u_i = u_{n-i}$ for all $1 \leq i \leq n-1$. We show that there exists a normal element α corresponding to a prescribed vector u such that $u_i = Tr_{2^n|2}(\alpha^{2^{2i}-2^i+1})$ for $0 \leq i \leq n-1$, where n is positive integer if and only if vector u is symmetric and either $\left(\sum_{0\leq i\leq n-1} u_i x^i,\ x^n - 1\right) = 1$ for even n or $u_0 = 1, \sum u_i = 1$, for odd n.

Keywords: Normal basis, Trace function, Hamming weight, Symmetric vector, Frobenius mapping

An algebraic construction for new MRD codes and new semifields

John Sheekey

University College Dublin

Abstract

Rank-metric codes are codes consisting of matrices over a field, with the distance between two codewords being the rank of their difference. Maximum Rank Distance (MRD) codes are the rank-metric analogues of MDS codes.

There has been a strong interest in these codes recently, in part due to their applications in Random Linear Network Coding. Further interest comes from the special case of maximum minimum distance, for which linear MRD codes correspond to algebraic structures known as semifields. These have important connections to many topics in finite geometry.

In this talk we review the known constructions, and present a new algebraic construction which leads to new MRD codes for all parameters, including new semifields, and connects some previously known families into one common construction.

Keywords: rank metric, MRD, semifield

Puncturing maximum rank distance codes

Alessandro Siciliano

Università degli Studi della Basilicata, Italy

(Joint work with Bence Csajbók — Eötvös Loránd University)

Abstract

Let $M_{m,n}(\mathbb{F}_q)$, $m \leq n$, be the rank metric space of all the $m \times n$ matrices with entries in the finite field $\mathbb{F}_q$ with q elements, $q = p^h$, p a prime. An $(m, n, q; s)$-*rank distance code* is any subset $\mathcal{X}$ of $M_{m,n}(\mathbb{F}_q)$ such that the the rank of the difference of two of its distinct elements is at least s.

It is known that the size of an $(m, n, q; s)$-rank distance code $\mathcal{X}$ is bounded by $q^{n(m-s+1)}$. When this bound is achieved, $\mathcal{X}$ is called an $(m, n, q; s)$-*maximum rank distance code*, or $(m, n, q; s)$-*MRD code*, for short.

For many years the only known MRD codes were the so-called *Generalized Gabidulin codes*. Recently, these have been extended to new infinite families: the *Generalized Twisted Gabidulin codes*.

Given a rank metric code $\mathcal{X}$ in $M_{n,n}(\mathbb{F}_q)$, one can obtain a rank distance code in $M_{m,n}(\mathbb{F}_q)$, by *puncturing* the code $\mathcal{X}$ with a suitable $m \times n$ matrix A.

In this talk the most relevant properties of the punctured MRD codes will be reported. Particular attention will be paid to the punctured Generalized Twisted Gabidulin codes.

While a very recent preprint of Trombetti and Zhou deals with the same problem by using q-linearized polynomials, our arguments will be carried out in the framework of bilinear forms represented by q^k-circulant matrices acting on cyclic models of finite vector spaces over $\mathbb{F}_q$.

Keywords: Maximum rank distance code, punctured code, bilinear form

Inherited unitals in Moulton planes of odd order

Angelo Sonnino

Università degli Studi della Basilicata

(Joint work with Gábor Korchmáros and Tamás Szőnyi)

Abstract

We prove that every Moulton plane of odd order—by duality every generalised André plane—contains a unital. We conjecture that such unitals are non-classical, that is, they are not isomorphic, as designs, to the Hermitian unital. We prove our conjecture for Moulton planes which differ from $\mathrm{PG}(2, q^2)$ by a relatively small number of point-line incidences. Up to duality, our results extend previous analogous results—due to Barwick and Grüning—concerning inherited unitals in Hall planes.

Keywords: unital, design, projective plane, affine plane.

Automorphisms of even genus ordinary curves

Pietro Speziali

University of Basilicata

(Joint work with Maria Montanucci — University of Basilicata)

Abstract

Let $\mathcal{X}$ be a (algebraic, projective, absolutely irreducible) curve defined over an algebraically closed field K of characteristic $p > 0$. Let g be its genus, γ its Hasse-Witt invariant and G its automorphism group. As in positive characteristic a number of exceptions to the classical Hurwitz bound $|G| \leq 84(g-1)$ arise, it is of great interest to find *good* bounds for $|G|$ in terms of g and γ. Henn proved that $|G| \leq 8g^3$ unless $\mathcal{X}$ belongs to one of four exceptional isomorphism classes. Remarkably, for all of this exceptional curves we have $\gamma = 0$. However, a general curve is *ordinary*, that is, $g = \gamma$. For ordinary curves, Nakajima [4] proved $|G| \leq 84(g-1)g$. Recently, Korchmáros and Montanucci [3] proved that for a *solvable* automorphism group G of $\mathcal{X}$ an even better bound $|G| \leq cg^{3/2}$ can be achieved. In this talk, we deal with the size of automorphism groups of ordinary curves of even genus. The latter hypothesis imposes strong conditions on the structure of G [2]. We prove that, for the even genus case, a bound $|G| \leq cg^{7/4}$ holds, except $p = 3, g = 26, G = M_{11}$ with M_{11} the Mathieu group of degree 11. We also address the problem of the existence and unicity of such counterexamples.

Keywords: Algebraic curve, automorphism group, Hasse-Witt invariant

References

[1] M. Giulietti, G. Korchmáros, Algebraic curves with many automorphisms, arXiv:1702.08812.

[2] G. Korchmáros, M. Montanucci, Ordinary algebraic curves with many automorphisms in positive characteristic, arXiv:1610.05252 .

[3] S. Nakajima, p-ranks and automorphism groups of algebraic curves, *Trans. Amer. Math. Soc.* **303** (1987), 595-607.

On the geometrical sunflower bound

Leo Storme

Ghent University

(Joint work with Lisa Hernandez Lucas, Ivan Landjev and Peter Vandendriessche)

Abstract

A *t-intersecting constant dimension code* is a set of k-dimensional subspaces of a vector space $V(N, q)$ of dimension N over the finite field $\mathbb{F}_q$ of order q, pairwise intersecting in a t-dimensional space.

The classical example of a t-intersecting constant dimension code is a *sunflower*, i.e., a set of subspaces pairwise intersecting in the same t-dimensional space.

A known theorem on these t-intersecting constant dimension codes states that, from a certain size on, these codes always are equal to sunflowers. The lower bound for this size is called the *sunflower bound*.

Recently, Barrolleta, Suárez-Canedo, Storme and Vandendriessche proved a geometrical sunflower bound. They managed to prove for a $(k-t)$-intersecting constant dimension code $C = \{\pi_1, \ldots, \pi_n\}$ of k-dimensional codewords, if $\dim\langle \pi_1, \ldots, \pi_n \rangle \geq k + (t-1)(n-1) + 2$, then C is a sunflower.

This lower bound is sharp. When $\dim\langle \pi_1, \ldots, \pi_n \rangle \geq k + (t-1)(n-1) + 1$, then C is a sunflower or is one of two other types of subspace codes.

Recently, Lisa Hernandez Lucas, Ivan Landjev, Peter Vandendriessche and I have been studying the case in which $\dim\langle \pi_1, \ldots, \pi_n \rangle \geq k + (t-1)(n-1) + 1 - \epsilon, \epsilon > 0$ small. We have proven that still a large part of the code can be described exactly, showing that there are some patterns in the $(k-t)$-intersecting constant dimension codes, generating a large dimension.

Keywords: Subspace codes, constant dimension codes

A Note on Complete Mappings over $\mathbb{F}_{2^n}$

Valentin Suder

University of Versailles Saint-Quentin (France)

(Joint work with Guang Gong and Krystal Guo — University of Waterloo (Canada))

Abstract

Over a finite field $\mathbb{F}_{2^n}$, a mapping $x \mapsto f(x)$ is said to be a *complete mapping* if it is bijective and the mapping $x \mapsto f(x)+x$ is also bijective. Note that over finite fields in characteristic 2, the notion of complete mapping coincide with the notion of *orthomorphism*, where the requirement is that both mappings $x \mapsto f(x)$ and $x \mapsto f(x) - x$ are bijective.

Complete mappings never stopped to attract a lot of attention from researchers as they form a very special kind of permutations. In addition to be a combinatorial curiosity, they have been proven useful in cryptography, coding theory and for the construction of bent functions among other applications. However, very little is known about the subset of permutations that are complete mappings, how many of them exist and what are the possible cycle structures. Moreover, not so many classes of complete mappings are known, and most of them are, in univariate polynomial form, monomials, binomials and linearized.

In this work, we first aim at generalizing some existing properties, and thus expanding the number of known complete mappings. More specifically, we give two equivalence of complete mappings. The first one comes from the action of the Dihedral group of order 6 over the set of all complete mappings. The second one is a generalization of the fact that the inverse (for the composition) of a complete mapping is again a complete mapping.

Finally, we give some sufficient conditions for cyclotomic mappings to be complete.

Keywords: Complete mappings, orthomorphisms, cyclotomic mappings, permutation polynomials

Digits in finite fields

Cathy Swaenepoel

Aix-Marseille Université

Abstract

The study of the connection between the arithmetic properties of an integer and the properties of its digits in a given basis produces a lot of interesting questions and a lot of papers have been devoted to this topic. In the context of finite fields, the algebraic structure permits to formulate and study new problems of interest which might be out of reach in $\mathbb{N}$. Dartyge and Sárközy [2] initiated the study of the concept of digits in $\mathbb{F}_q$, establishing estimates for the number of squares whose sum of digits is fixed. They also obtained results for polynomial values, resp. polynomial values with primitive element arguments whose sum of digits is fixed. Further results can be found in [3].

We will study new questions in this spirit: 1) give (more precise) estimates for the number of elements of $\mathbb{F}_q$ that belong to a special sequence and whose sum of digits is fixed; 2) given subsets $\mathcal{C}$ and $\mathcal{D}$ of $\mathbb{F}_q$, find conditions on $|\mathcal{C}|$ and $|\mathcal{D}|$ to ensure that there exists $(c, d) \in \mathcal{C} \times \mathcal{D}$ such that the sum of digits of cd belongs to a predefined subset of $\mathbb{F}_p$; 3) given a special sequence $\mathcal{Q}$ in $\mathbb{F}_q$, estimate the number of elements of $\mathcal{Q}$ with preassigned digits. For this last problem, we show that we can preassign a positive proportion of digits, in the spirit of a recent result of Bourgain [1] who studied the number of prime numbers with a positive proportion of preassigned digits.

Keywords: finite fields, sum of digits function, preassigned digits, products of subsets, squares, primitive elements.

References

[1] J. Bourgain, *Prescribing the binary digits of primes, II*, Israel J. Math., 206 (2015), pp. 165–182.

[2] C. Dartyge and A. Sárközy, *The sum of digits function in finite fields*, Proc. Amer. Math. Soc., 141 (2013), pp. 4119–4124.

[3] R. Dietmann, C. Elsholtz, and I. E. Shparlinski, *Prescribing the binary digits of squarefree numbers and quadratic residues*, arXiv:1601.04754v1, (2016).

Dual hyperovals from three or more binary presemifields

Hiroaki Taniguchi

National Institute of Technology, Kagawa College

Abstract

The concept of higher dimensional dual hyperovals are introdeced in [1]. In [2], we construct higher dimensional bilinear dual hyperovals from binary commutative presemifield. In this talk, we consider a generalization of this construction. We use binary commutative presemifields S_i for $i = 1, \ldots, n$ (the sizes of them may be different) and presemifields S_{ij} for $1 \leq i < j \leq n$ which may not be commutative, and the bilinear mappings $B_i : V_i \oplus V_i \to S_i$ as in [2], where V_i is a $GF(2)$-vector space $V_i = S_i \oplus \langle e_0 \rangle$. ($\langle e_0 \rangle$ is the $GF(2)$-vector space generated by a fixed element e_0.) Then we glue the bilinear mappings B_i and B_j using the presemifields S_{ij} for $1 \leq i < j \leq n$, thus we have a bilinear mapping $B : V \oplus V \to W = (S_1 \oplus \ldots \oplus S_n) \oplus (S_{12} \oplus \ldots \oplus S_{n-1,n})$, where $V = S_1 \oplus S_2 \oplus \cdots \oplus S_n \oplus \langle e_0 \rangle$. Using this bilinear mapping, we have a bilinear dual hyperoval. We also study on the isomorphism problems on these dual hyperovals under some conditions.

Keywords: dimensional dual hyperoval, presemifield

References

[1] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, Contribution to Algebra and Geometry, **40** (1999), 503–532.

[2] Bilinear dual hyperovals from binary commutative presemifields, Finite Fields and their Applications **42** (2016), 93–101.

Towards primitive k-normality

David Thomson

Carleton University

(Joint work with Lucas Reis, Universidade Federal de Minas Gerais)

Abstract

A generalization of normal bases over finite fields, k-normal elements, are generators of Frobenius-stable subspaces of co-dimension k in finite fields. The study of k-normal elements has picked up recently; for example, see [1, 2, 4]. Existence of elements that are simultaneously primitive (generators of the multiplicative group of the finite field) and 1-normal (generators of a hyperplane) were given in [3] for finite fields of odd characteristics not dividing the degree of the extension. In this talk, we will discuss how to remove both obstructions: namely, to show existence of primitive, 1-normal elements over all characteristics and when the characteristic divides the extension degree.

Keywords: Normal bases, k-normal elements, Frobenius modules

References

[1] M. Alizadeh, Some notes on the k-normal elements and k-normal polynomials over finite fields. *Journal of Algebra and Its Applications* **16** (2017), 1750006 (11 pages).

[2] M. Alizadeh and S. Mehrabi, Recursive constructions of k-normal polynomials over finite fields, arXiv Preprint arXiv:1610.05684 (2016).

[3] S. Huczynska, G. L. Mullen, D. Panario and D. Thomson, Existence and properties of k-normal elements over finite fields, *Finite Fields and Their Applications*, **24** (2013), 170–183.

[4] L. Reis, Existence results on k-normal elements over finite fields, arXiv Preprint arXiv:1612.05931 (2016).

On some iterative constructions of irreducible polynomials over finite fields

Simone Ugolini

University of Trento (Italy)

Abstract

In this talk I will briefly review some well-known iterative constructions of irreducible polynomials over finite fields, which go back to Cohen, Meyn et al.

Then I will present an iterative construction, which makes use of transforms involving some rational maps. Such maps appear in the definition of certain endomorphisms of elliptic curves. More specifically, I will show how to produce an infinite sequence $\{f_i\}_i$ of irreducible polynomials, starting from an irreducible polynomial f_0, in such a way that, for any sufficiently large index i, all the polynomials in the sequence can be inexpensively generated just setting $f_{i+1} := f_i^r$, where r is one of the transforms mentioned above.

Keywords: Irreducible polynomials, iterative constructions

General Properties of Costas Permutations and Graphs from Hops and Alternating Runs

Jordy Vanpoucke

Vrije Universiteit Brussel

(Joint work with Philippe Cara — Vrije Universiteit Brussel)

Abstract

We present several concepts that can be used to determine whether a permutation or graph can be Costas or not. First of all we introduce the concept of *hops*, which is used to define a Costas permutation and plays an important role in several proofs. Another important concept that is introduced, is that of *alternating runs*, which gives us a deeper understanding in the structure of Costas permutations. By using the concept of hops we prove that a permutation of degree n corresponding to a path graph can not be Costas if $n > 5$ and by combining hops and alternating runs we prove a general bound on the number of alternating runs of a Costas permutation of degree n, giving us general values for which Costas permutations cannot exist. Finally we give some lower and upper bounds for decreasing subsequences appearing in Costas permutations, which is equivalent with bounds on complete subgraphs in Costas graphs.

Keywords: Costas arrays, permutations, subsequences, alternating runs, permutation graphs, bounds

Lattice basis reduction algorithm over the ring of linearized polynomials with composition and its applications in cryptography and coding theory

Li-Ping Wang

Institute of Information Engineering, Chinese Academy of Sciences

Abstract

In this paper we propose a lattice basis reduction algorithm over the ring of linearized polynomials with composition similar to the algorithm over the ring of polynomials. Using this algorithm, we give a multisequece linearized shift-register synthesis algorithm and a decoding algorithm for interleaved Gabidulin codes as applications in cryptography and coding theory.

Keywords: Lattice basis reduction algorithm, Gabidulin codes, linear feedback shift-register synthesis, linearized polynomials

Weight Two Masking in the McEliece System

Violetta Weger

University of Zurich

(Joint work with Joachim Rosenthal — University of Zurich)

Abstract

The National Institute of Standards and Technology (NIST) encouraged a year ago research in public key cryptosystems which would resist the computing capability of a quantum computer. One of the most promising candidates for post-quantum cryptography are code-based cryptosystems. The idea goes back to a proposal [1] by McEliece who proposed the use of classical Goppa codes, disguised by a monomial transformation. The main drawback of the original proposal was the large key size. For this reason many researchers proposed alternative systems having smaller key size. In this talk we present a variant [2] of the McEliece system, proposed by Bolkema *et al.* using Generalized Reed Solomon (GRS) codes and a matrix with constant row weight two as scrambling transformation. This variant is a special case of the BBCRS scheme [3], proposed by Baldi *et al.* Couvreur *et al.* provided a distinguisher attack [4], in case that the square code has not maximal dimension. In this talk we provide evidence that the weight two masking leads to maximal dimension of the square code avoiding in this way the distinguisher attack.

Keywords: McEliece, Coding Theory, Cryptography

[1] Robert J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 44:114-116, January 1978.

[2] Jessalyn Bolkema, Heide Gluesing-Luerssen, Christine A. Kelley, Kristin E. Lauter, Beth Malmskog, and Joachim Rosenthal. Variations of the McEliece Cryptosystem. *CoRR*, abs/1612.05085, 2016.

[3] Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Rosenthal, and Davide Schipani. Enhanced Public Key Security for the McEliece Cryptosystem. *Journal of Cryptology*,29(1):1-27, 2016.

[4] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tilich. Distinguisher-Based Attacks on Public-Key Cryptosystems Using Reed-Solomon Codes. *Designs, Codes and Cryptography*, 73(2):641-666, 2014.

Carlitz rank and index of permutation polynomials

Arne Guenther Winterhof

Austrian Academy of Sciences

(Joint work with L. Işık)

Abstract

Carlitz rank and index are two important measures for the complexity of a permutation polynomial $f(x)$ over the finite field $\mathbb{F}_q$. In particular, for cryptographic applications we need both, a high Carlitz rank and a high index. In this article we study the relationship between Carlitz rank $Crk(f)$ and index $Ind(f)$. More precisely, if the permutation polynomial is neither close to a polynomial of the form ax nor a rational function of the form ax^{-1}, then we show that $Crk(f) > q - \max\{3Ind(f), (3q)^{1/2}\}$. Moreover we show that the permutation polynomial which represents the discrete logarithm guarantees both a large index and a large Carlitz rank.

Keywords: Carlitz rank, character sums, cryptography, finite fields, index, invertibility, linearity, permutation polynomials, cyclotomic mappings, discrete logarithm.

Cyclic codes of composite length and the minimum distance

Maosheng Xiong

Hong Kong University of Science and Technology

Abstract

In an interesting paper Professor Cunsheng Ding provided three constructions of cyclic codes of length being a product of two primes. Numerical data shows that many codes from these constructions are best cyclic codes of the same length and dimension over the same finite field. However, not much is known about these codes. In this paper we explain some of the mysteries of the numerical data by developing a general method on cyclic codes of composite length and on estimating the minimal distance. Inspired by the new method, we also provide a general construction of cyclic codes of composite length. Numerical data shows that it produces many best cyclic codes as well. Finally, we point out how these cyclic codes can be used to construct convolutional codes with large free distance.

Keywords: Quadratic residue code, cyclic code of composite length, minimum distance, convolutional code.

Counting Points on Curves and Irreducible Polynomials over Finie Fields

Emrah Sercan Yilmaz

University College Dublin

(Joint work with Gary McGuire — University College Dublin)

Abstract

For any integer $n \geq 2$ and prime power q we present formulae for the number of irreducible polynomials of degree n over the finite field $\mathbb{F}_q$ where the coefficients of x^{n-1} and x^{n-2} are fixed. Our proofs involve counting the number of points on certain algebraic curves over finite fields.

Keywords: Supersingular curves, irreducible polynomials, prescribed coefficients.

Generalized Artin-Mumford curves and their automorphisms

Giovanni Zini

University of Florence

(Joint work with M. Giulietti, M. Montanucci, and L. Quoos)

Abstract

Over a finite field $\mathbb{F}_q$ of odd characteristic p, we define the generalized Artin-Mumford curve $\mathcal{X}_{(L_1,L_2)}$ with affine equation $L_1(x) \cdot L_2(y) = 1$. Here, $L_1, L_2 \in \mathbb{F}_q[x]$ are any two separable $\bar{q}$-linearized polynomials of degree q, where q is a power of $\bar{q}$.

We determine the full automorphism group G of $\mathcal{X}_{(L_1,L_2)}$ over the algebraic closure $\overline{\mathbb{F}}_q$. Using tools from algebraic geometry and finite groups theory, we also characterize the generalized Artin-Mumford curves in terms of their genus and their automorphism group; that is, any curve over $\mathbb{F}_q$ having genus $(q-1)^2$ and an automorphism group isomorphic to a certain subgroup of G is birationally equivalent to some $\mathcal{X}_{(L_1,L_2)}$.

This extends results by Arakelian-Korchmáros [1] and van der Geer-van der Vlugt [3] on the Artin-Mumford curve, i.e. when $L_1(x) = L_2(x) = x^p - x$.

Keywords: algebraic curves; automorphism groups.

References

[1] N. Arakelian and G. Korchmáros, A characterization of the Artin-Mumford curve, *J. Number Theory* **154** (2015), 278–291.

[2] M. Montanucci and G. Zini, Generalized Artin-Mumford curves over finite fields, *J. Algebra*, to appear.

[3] G. van der Geer and M. van der Vlugt, Kloosterman sums and the p-torsion of certain Jacobians, *Math. Ann.* **290** (1991), 549–563.

List of Talks

List of talks

web: http://www.dma.unina.it/Fq13/

email: fq13@unina.it