Coding theory and cryptography

A conference in the honor of Joachim Rosenthal's 60th birthday

July 11 - 15, 2022 | **University of Zurich**

Program

Monday, July 11, 2022

08:45 - 10:25	Opening Quantum Convolutional Codes, *Markus Grassl (University of Gdansk, Poland)* Erasure decoding of convolutional codes with the help of linear systems, *Julia Lieb (University of Zurich, Switzerland)* Construction of an Optimal Convolutional Code of Rate 1/2, *Zita Abreu (University of Aveiro, Portugal)*
10:25 - 10:55	Coffee Break
10:55 - 12:35	Computing a Minimal Input-State-Output Representation of Convolutional Codes, *Verónica Requena (University of Alicante, Spain)* State space Realizations of periodic convolutional codes, *Maria Raquel Rocha Pinto (University of Aveiro, Portugal)* MRD convolutional codes, *Filipa Santana (University of Aveiro, Portugal)* Generalized weights of convolutional codes, *Flavio Salizzoni (University of Neuchatel, Switzerland)*
12:35 - 14:00	Lunch
14:00 - 15:40	A notion of bent sequences based on Hadamard matrices, *Patrick Solé (Institut de Mathématiques de Marseille, France)* On image sets and the univariate representation of APN maps, *Gohar Kyureghyan (University of Rostock, Germany)* On the relationship between irreducible cyclic codes, finite projective planes and non-weakly regular bent functions, *Rumi Melih Pelen (Erzurum Technical University, Turkey)* Resolution of an equation over finite fields and its impacts, *Sihem Mesnager (University of Paris VIII, France)*
15:40 - 16:10	Coffee Break

Evening	Zoo visit and Welcome Apéro (17:00 onwards)

Tuesday, July 12, 2022

08:45 - 10:25	Non-Special Divisors of Small Degrees and LCD Codes from Hermitian curves, *Eduardo Camps-Moreno (Instituto Politécnico Nacional, Mexico)* k-Galois Hull of Constacyclic Codes, *Habibul Islam (University of St. Gallen, Switzerland)* A Monoid structure on the set of all binary operations over a fixed set , *Sergio López-Permouth (Ohio University, United States of America)* New advances in permutation decoding of first-order Reed-Muller codes, *José Joaquín Bernal (Universidad de Murcia, Spain)*
10:25 - 10:55	Coffee Break
10:55 - 12:35	Rank Metric Codes, Subcodes and Different Notions of Duality, *Ferruh Özbudak (Middle East Technical University, Turkey)* Universal Decoding of Interleaved Linearized Reed–SolomonCodes in the Sum-Rank Metric, *Hannes Bartz (German Aerospace Center, Germany)* The Density of Extremal Codes with Sublinearity, *Nadja Willenborg (University of St. Gallen, Switzerland)* Speeding up Error-Erasure Decoding of Linearized Reed–Solomon Codes in the Sum-Rank Metric, *Felicitas Hörmann (German Aerospace Center, Germany)*
12:35 - 14:00	Lunch
14:00 - 15:40	Pseudorandom sequences from hyperelliptic curves, *Vishnupriya Anupindi (RICAM (Johann Radon Institute for Computational and Applied Mathematics), Austria)* Computing Riemann-Roch spaces for algebraic geometry codes, *Elena Berardini (Eindhoven University of Technology, The Netherlands)* Computing the endomorphism ring of a supersingular elliptic curve, *Annamaria Iezzi (Università degli Studi di Napoli Federico II, Italy)* Quantum codes from generalized AG codes, *José Ignacio Iglesias Curto (University of Salamanca, Spain)*
15:40 - 16:10	Coffee Break
16:10 - 17:25	Coproducts in Categories of q-Matroids, *Heide Gluesing-Luerssen (University of Kentucky, United States of America)* Lifting codes and deriving matroids, *Ragnar Freij-Hollanti (Aalto University, Finland)* The Characteristic Polynomial of q-Matroids, *Benjamin Jany (University of Kentucky, United States of America)*

Evening	Online Greetings Session (18:00 onwards)

Thursday, July 14, 2022

08:45 - 10:25	Developing Innovative Frameworks for Efficient Code-based Signatures, *Edoardo Persichetti (Florida Atlantic University, United States of America)* Non Commutative Goppa Codes and their Use in Code-based Cryptography, *Francisco Javier Lobillo (Universidad de Granada, Spain)* The Marginal Distribution of the Lee Channel and its Applications, *Jessica Bariffi (German Aerospace Center, Germany and University of Zurich, Switzerland)* Smaller Keys for the McEliece Cryptosystem: A convolutional variant with GRS codes, *Paulo Almeida (University of Aveiro, Portugal)*
10:25 - 10:55	Coffee Break
10:55 - 12:35	CSS-T Codes from Reed-Muller Codes For Quantum Fault-Tolerance, *Felice Manganiello (Clemson University, United States of America)* Purity of Free Resolutions of Affine and Projective Reed-Muller Codes, *Rati Ludhani (Indian Institute of Technology Bombay, India)* Free Resolutions and Generalized Hamming Weights of binary linear codes, *Edgar Martínez-Moro (University of Valladolid, Castilla, Spain)* Modeling Sliding Window Decoder Error Propagation Effects for Spatially Coupled LDPC Codes, *Daniel Costello (University of Notre Dame, United States of America)*
12:35 - 14:00	Lunch
14:00 - 15:40	Sequential Locally Recoverable Codes for Multiple Erasures from Finite Geometry, *Marc Newman (University of St. Gallen, Switzerland)* Update and Repair Efficient Storage Codes with Availability via Finite Projective Planes, *Junming Ke (University of Tartu, Estonia)* Batch Code Properties of the Simplex Code, *Ago-Erik Reit (University of Tartu, Estonia)* Function computation on reconciled data, *Vitaly Skachek (University of Tartu, Estonia)*
15:40 - 16:10	Coffee Break
16:10 - 17:25	NP-Complete Problems in Graph Groups and connection to Post-quantum Cryptography, *Delaram Kahrobaei (The City University of New York, United States of America)* Semidirect product key exchange: the state of play, *Christopher Battarbee (The City University of New York, United States of America)* Higher dimensional platforms for Tillich-Zéemor hash functions, *Corentin Le Coz (Technion, Israel)*

Evening	Social Dinner (19:00 onwards)

Friday, July 15, 2022

08:45 - 10:25	Error Correcting Codes in a Frobenius Algebra Ambient, *Erik Hieta-aho (Aalto University, Finland)* Multi-twisted additive codes over finite fields , *Sandeep Sharma (Indraprastha Institute of Information Technology Delhi, India)* Enumeration formulae for self-orthogonal, self-dual and LCD codes over finite commutative chain rings , *Monika Yadav (Indraprastha Institute of Information Technology Delhi, India)* MacWilliams extending conditions and quasi-Frobenius rings , *Ashish Srivastava (Saint Louis University, United States of America)*
10:25 - 10:55	Coffee Break
10:55 - 12:35	Open Problems on Subspace Codes and Designs , *Tuvi Etzion (Technion, Israel)* New 2-designs in polar spaces , *Alfred Wassermann (University of Bayreuth, Germany)* Sphere Packing Lower Bounds: New Developments, *Vlad Serban (EPFL, Switzerland)* Explicit constructions of asymptotically good minimal linear codes from graphs, *Alessandro Neri (Max Planck Institute for Mathematics in the Sciences, Germany)*
12:35 - 14:00	Lunch
14:00 - 15:40	Linear Codes associated to Flag Varieties over Finite Fields, *Sudhir R. Ghorpade (Indian Institute of Technology Bombay, India)* Cyclic orbit flag codes, *Miguel-Ángel Navarro-Pérez (Centro Universitario EDEM Escuela de Empresarios, Spain)* Higher Grassmann Codes, *Mahir Bilen Can (Tulane University, United States of America)* Minimum Weight Codewords of Schubert Codes, *Avijit Panja (Indian Institute of Technology Bombay, India)*
15:40 - 16:10	Coffee Break
16:10 - 17:25	SPANSE: combining sparsity with density for efficient one-time code-based digital signatures, *Marco Baldi (Università Politecnica delle Marche, Italy)* Algebraic Connections Between Absorbing Sets and Cosets, *Emily McMillon (University of Nebraska-Lincoln, United States of America)* Network Decoding Against Restricted Adversaries , *Altan Kılıç (Eindhoven University of Technology, The Netherlands)*