Mathematics of Digital Communications
Les mathématiques de la communication digitale

(Org: **Jonathan Jedwab**, **Shuxing Li** and/et **Petr Lisonek** (Simon Fraser))

SIMEON BALL, Universitat Politecnica Catalunya
Hermitian self-orthogonal codes

Let C be a $[n,k]_{q^2}$ linear code,.

C is linearly equivalent to a Hermitian self-orthogonal code if and only if there are non-zero $\lambda_i \in \mathbb{F}_q$ such that

$$\sum_{i=1}^{n} \lambda_i u_i v_i^q = 0,$$

for all $u, v \in C$.

For any linear code C over $\mathbb{F}_{q^2}$ of length n, Rains defined the *puncture code* $P(C)$ to be

$$P(C) = \{\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{F}_q^n \mid \sum_{i=1}^{n} \lambda_i u_i v_i^q = 0, \text{ for all } u, v \in C\}.$$

C has a truncation of length $r \leqslant n$ which is linearly equivalent to a Hermitian self-orthogonal code if and only if there is an element of $P(C)$ of weight r.

Rains was motivated to look for Hermitian self-orthogonal codes, since there is a simple way to construct a $[\![n, n-2k]\!]_q$ quantum code, given a Hermitian self-orthogonal code.

In this talk, I will detail an effective way to calculate the puncture code. I will outline how to prove various results about when a linear code has a truncation which is linearly equivalent to a Hermitian self-orthogonal linear code and how to extend it to one that does in the case that it has no such truncation. In the case that the code is a Reed-Solomon code, it turns out that the existence of such a truncation of length r is equivalent to the existence of a polynomial $g(X) \in \mathbb{F}_{q^2}[X]$ of degree at most $(q-k)q-1$ with the property that $g(X) + g(X)^q$ has $q^2 - r$ distinct zeros in $\mathbb{F}_{q^2}$.

NINA BINDEL, University of Waterloo and IQC
Post-quantum cryptography: faster, smaller, harder?

Large quantum computers will be able to break essentially all of our asymmetric cryptography used today, as Shor's quantum algorithm solves the discrete logarithm and prime factorization problem in polynomial time. To maintain security also in the future, researchers, industry and standardization bodies are busily constructing cryptographic algorithms whose security is based on problems that cannot be efficiently solved by known classical or quantum algorithms. Many of these "post-quantum" cryptographic algorithms are constructed over lattices with security based on the hardness of finding closest or shortest vectors in a lattice. For efficiency reasons, these hardness assumptions are tweaked, optimized, and tailored to the cryptographic algorithms and applications. In this talk we will give an overview into the topic of post-quantum cryptography and different variants of hardness assumptions in modern lattice-based cryptography. Furthermore, we will discuss known differences in the concrete hardness of these assumptions and open gaps.

LILYA BUDAGHYAN, University of Bergen
On isotopisms of commutative semifields

Commutative semifields are objects defined by the same axioms as a field but without requiring associativity of multiplication. Commutative semifields define optimal objects in projective geometry and cryptographic Boolean functions. Construction of infinite classes of commutative semifields of odd order has been a hard task and only a handful of these constructions is known. However, a natural construction method might be hidden in the very notion of isotopism, the equivalence relation used for classification of semifields.

CLAUDE CARLET, University of Paris 8 and University of Bergen
Revisiting some results on Almost Perfect Nonlinear functions

We push a little further the study of two recent characterizations of almost perfect nonlinear (APN) functions. We state open problems about them, and we revisit in their perspective a well-known result from Dobbertin on APN exponents. This leads us to a new result about APN power functions and more general APN polynomials with coefficients in a subfield $\mathbb{F}_{2^k}$, which eases the research of such functions. It also allows to construct automatically many differentially uniform functions from them (this avoids calculations for proving their differential uniformity as done in a recent paper, which are tedious and specific to each APN function). Finally we introduce a new representation of the Kasami APN functions in odd dimension and deduce the exact values (with their sign) of two thirds of their Walsh transform values (this latter work is in common with L. Budaghyan, M. Calderini, D. Davidova and N. Kaleyski).

TUVI ETZION, Technion, Israel Institute of Technology
Diameter Perfect Codes

Diameter perfect codes form a natural generalization for perfect codes. They are based on the code-anticode bound which generalizes the sphere-packing bound. The code-anticode bound was proved by Delsarte for distance-regular graphs and it holds for some other metrics too. In this talk we present a short introduction on the known results. We concentrate on new results for non-binary diameter perfect constant-weight codes and present a list of open problems.

GUANG GONG, University of Waterloo
M-sequences and complete complementary codes

How do m-sequences meet complete complementary codes? Maximal length shift register sequences (m-sequences) found their first applications in signal detection in Explorer, the first satellite launched by US in 1958. Currently, it has found applications in almost every corner of engineering and computer science. The autocorrelation of m-sequences resembles that of white Gaussian noise, so it is also populated as pseudo noise, where the autocorrelation is computed in a circular way (i.e., periodic correlation). The concept of Golay sequence pair was first introduced by Golay in 1961 for the application of static multislit spectrometry (1951), and it was extended to complementary sequence set (CSS) and complete complementary codes since then. However, those autocorrelation functions are computed in a linear way (i.e., aperiodic correlation). The research in those two areas are parallelly advanced without any crossing point in about seven decades. In this talk, I will present a bridge which links the concepts of m-sequences, more generally, 2-level autocorrelation sequences and CSS/CCC through Hadamard matrices Hadamard matrices and permutations. I will show how to construct CSS/CCC starting with a single m-sequence or any 2-level autocorrelation sequence.

TOR HELLESETH, University of Bergen, Norway
Correlation of m-sequences and their applications

Abstract: The correlation between two binary sequences is the number of agreements minus the number of disagreements over a full period. In modern communication systems one needs families of sequences with good correlation properties. Many sequence families used in practical communication systems depend heavily on properties of m-sequences (maximum-length sequences) and their correlation properties.

In this talk we give a brief overview of the cross-correlation between m-sequences and some applications. Furthermore, we show how some problems on m-sequences are related to problems in other areas of mathematics such as difference sets, strongly regular graphs, almost perfect nonlinear functions, solutions of equations over finite fields.

THAÍS IDALINO, Universidade Federal de Santa Catarina
Modification-Tolerant Signature Schemes

Classical digital signature schemes are used to guarantee that a document was created by the sender (authenticity) and has not been modified along the way (integrity). However, the signature verification algorithm has a boolean output: a successful outcome is achieved if and only if both the signature is valid and the document has not been modified.

In this work, we consider more general digital signature schemes which we call modification-tolerant signature schemes, which go beyond the ability of detecting modifications, and have the ability of locating modifications or locating and correcting modifications. They can be used in applications where either the data can be modified (collaborative work), or the data must be modified (redactable and content extraction signatures) or we need to know which parts of the data have been modified (data forensics).

We discuss two types of modification-tolerant signature schemes: a general one that allows the location of modified blocks of the data, and a scheme with correction capability, that allows the correction of the modified blocks, recovering the original message. We give three instantiations of the scheme for the purpose of location, correction, and redaction. The schemes are proposed using techniques from combinatorial group testing.

This talk is based on joint work with Lucia Moura and Carlisle Adams.

GOHAR KYUREGHYAN, University of Rostock
New and old insights on APN maps

An APN map $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined by the property that for every non-zero $a \in \mathbb{F}_{2^n}$ the set $D_a = \{f(x+a) + f(x) \mid x \in \mathbb{F}_{2^n}\}$ contains exactly 2^{n-1} elements. The APN maps provide optimal resistance against differential attacks in cryptological applications, and they yield constructions for special codes. In this talk we show that to check the APN property for a generic map it is enough to consider the sets D_a for elements a from a hyperplane. We present some results on the image sets of APN maps, which indicate that a better understanding of the image sets of APN maps will allow progressing on some of main challenges in the research area.

The talk is based on joint works with Pascale Charpin and Lukas Kölsch, Björn Kriepke.

DANIEL PANARIO, Carleton University
Towards constant-time probabilistic root finding for code-based cryptography

In code-based cryptography, deterministic algorithms are used in the root-finding step of the decryption process. However, probabilistic algorithms are, in general, more time efficient than deterministic ones for large fields. These algorithms can be useful for long-term security where larger parameters are relevant. Still, current probabilistic root-finding algorithms suffer from time variations making them susceptible to timing side-channel attacks. To prevent these attacks, we propose a countermeasure to a probabilistic root-finding algorithm so that its execution time does not depend on the degree of the input polynomial but on the cryptosystem parameters. We compare the performance of our proposed algorithm to other root-finding algorithms already used in code-based cryptography. In general, our method is faster than the straightforward algorithm in Classic McEliece. The results also show the range of degrees in larger finite fields where our proposed algorithm is faster than the Additive Fast Fourier Transform algorithm also used in code-based cryptosystems.

Joint work with Dunia Marchiori, Ricardo Custodio and Lucia Moura.

MOSHE SCHWARTZ, Ben-Gurion University of the Negev
The Generalized Covering Radii of Linear Codes

Motivated by an application to database linear querying, such as private information-retrieval protocols, we suggest a fundamental property of linear codes – the generalized covering radius. The generalized covering-radius hierarchy of a linear code characterizes the trade-off between storage amount, latency, and access complexity, in such database systems. Several equivalent definitions are provided, showing this as a combinatorial, geometric, and algebraic notion. We derive bounds on the code parameters in relation with the generalized covering radii, study the effect of simple code operations, and describe a connection with generalized Hamming weights.

EMINA SOLJANIN, Rutgers University
Multiple Concurrent (Local) Data Access with Codes

Distributed storage systems strive to maximize the number of concurrent data access requests they can support with fixed resources. Replicating data objects according to their relative popularity and access volume helps achieve this goal. However, these quantities are often unpredictable. In emerging applications such as edge computing, even the expected numbers of users and their data interests extensively fluctuate, and data storage schemes should support such dynamics. Erasure-coding has emerged as an efficient and robust form of redundant storage. In erasure-coded models, data objects are elements of a finite field. Each node in the system stores one or more linear combinations of data objects. This talk asks 1) which data access rates an erasure-coded system can support and 2) which codes can support a specified region of access rates. We will address these questions by formulating them as some known and some new combinatorial optimization problems on graphs. We will explain connections with batch codes. This talk will also describe how, instead of a combinatorial, one can adopt a geometric approach to the problem.

DOUG STINSON, University of Waterloo
Generalizations of All-or-Nothing Transforms

All-or-nothing transforms (AONTs) were originally defined by Rivest as bijections from s input blocks to s output blocks such that no information can be obtained about any input block in the absence of any output block. Numerous generalizations and extensions of all-or-nothing transforms have been discussed in recent years, many of which are motivated by diverse applications in cryptography, information security, secure distributed storage, etc. In particular, t-AONTs, in which no information can be obtained about any t input blocks in the absence of any t output blocks, have received considerable study.

Three recent generalizations of AONTs are motivated by applications due to Pham et al. and Oliveira et al. We term these generalizations rectangular, range, and restricted AONTs. Briefly, in a rectangular AONT, the number of outputs is greater than the number of inputs. A range AONT satisfies the t-AONT property for a range of consecutive values of t. Finally, in a restricted AONT, the unknown outputs are assumed to occur within a specified set of "secure" output blocks. We study existence and non-existence and provide examples and constructions for these generalizations. We also demonstrate interesting connections with combinatorial structures such as orthogonal arrays, split orthogonal arrays, MDS codes and difference matrices.

This talk is based on joint work with Navid Nasr Esfahani.

ANTONIA WACHTER-ZEH, Technical University of Munich (TUM)
Function-Correcting Codes

Motivated by applications in machine learning and archival data storage, we introduce function-correcting codes, a new class of codes designed to protect a function evaluation of the data against errors. We show that function-correcting codes are equivalent to irregular-distance codes, i.e., codes that obey some given distance requirement between each pair of codewords. Using these connections, we study irregular-distance codes and derive general upper and lower bounds on their optimal redundancy. Since these bounds heavily depend on the specific function, we provide simplified, suboptimal bounds that are easier to evaluate. We further employ our general results to specific functions of interest and compare our results to standard error-correcting codes which protect the whole data.

ALFRED WASSERMANN, University of Bayreuth
Linear Codes from q-analogues in Design Theory

Rudolph (1967) introduced majority logic decoding for linear codes from combinatorial designs: If the point-block incidence matrix of a combinatorial t-design (with $t \geq 2$) is taken as a parity check matrix of a linear code, majority logic decoding can be used for this code.

However, such a linear code is only interesting if the p-rank of the point-block incidence matrix is small enough. Hamada (1973) determined the p-rank for the incidence matrices of so-called classical or geometric designs. It is a long-standing conjecture that the incidence matrices from this class of designs are of minimal p-rank.

Dela Cruz, Wassermann (2021) showed that linear codes from subspace designs (q-analogues of combinatorial designs) have the same decoding properties as the linear codes from their corresponding geometric designs, but for many parameters the majority logic decoder needs exponentially less parity check equations.

In this talk, we will show that Hamada's formula can also be applied to q-analogues of group divisible designs and lifted MRD codes (q-analogues of transversal designs), which may make these classes of codes interesting.

Today, majority logic decodable codes are still interesting for devices with low computational power and because of the relation to linear locally repairable codes and private information retrieval (PIR) codes.

YUE ZHOU, National University of Defense Technology

Perfect and almost perfect linear Lee codes

Given a positive integer r, an abelian group G and a subset $T = \{a_1, a_2, \cdots, a_n\} \subseteq G \setminus \{e\}$, if all elements in the multiset

$$\Psi := \left\{ * \, a_1^{\pm j_1} \cdots a_n^{\pm j_n} : 0 \leq \sum_{k=1}^{n} j_k \leq r, j_k \in \mathbb{Z}_{\geq 0} \, * \right\}$$

are distinct, and $G = \Psi$, then we call the Cayley graph $\Gamma(G, S)$ an *Abelian-Cayley-Moore graph*, where $S := T \cup T^{(-1)}$. Under this condition, the size of G (i.e. $|\Psi|$) is $\sum_{i=0}^{\min\{n,r\}} 2^i \binom{n}{i}\binom{r}{i}$.

It is a bit surprising that the existence of an Abelian-Cayley Moore graph is equivalent to a perfect linear Lee code of radius r in $\mathbb{Z}^n$, that is a lattice tiling of $\mathbb{Z}^n$ by the translations of an ℓ_1-metric sphere of radius r. More than 50 years ago, Golomb and Welch conjectured that there is no perfect Lee code C for $r \geq 2$ and $n \geq 3$. Recently, Leung and the speaker proved that if C is linear, then Golomb-Welch conjecture is true for $r = 2$ and $n \geq 3$.

In this talk, we consider the classification of linear Lee codes of the second best possibility, that is the density of the lattice packing of $\mathbb{Z}^n$ by Lee spheres $S(n, r)$ equals $\frac{|S(n,r)|}{|S(n,r)|+1}$. By checking the corresponding abelian Cayley graphs, an almost perfect linear Lee code is equivalent to the case with $G = \Psi \cup \{f\}$ where f is the unique element of order 2 in G.