Error Control Codes, Information Theory and Applied Cryptography
Codes de contrôle d'erreurs, théorie de l'information et cryptographie appliquée

(Org: **Aiden Bruen** (Calgary) and/et **David Wehlau** (Queens; RMC))

TIM ALDERSON, University of New Brunswick Saint John, 100 Tucker Park Rd., PO Box 5050, Saint John, New Brunswick, E2L 4L5

Maximal Projective Codes

For $n \geq k$, an $(n, k, d)_q$*-code* C is a collection of q^k n-tuples (or *codewords*) over an alphabet $\mathcal{A}$ of size q such that the minimum (Hamming) distance between any two codewords of C is d. For such a code, the Singleton bound ($|C| \leq |\mathcal{A}|^{n-d+1}$) gives $d \leq n - k + 1$. The *Singleton defect of* C, $S(C)$, is defined by $S(C) = n - k + 1 - d$. A code C' obtained by deleting some fixed coordinate from each codeword of C is called a *punctured code* of C. In the case that $S(C') = S(C)$, C is said to be an *extension* of C', equivalently, C' is said to be *extendable* to the code C. A code is *maximal* if it admits no extensions.

In the special case that $\mathcal{A} = GF(q)$ and C is a vector space of dimension k, C is a *linear* $(n, k, d)_q$-code. C then has an associated generator matrix G whose columns can be considered as a projective multiset $\mathcal{G}$ of n points in $PG(k-1, q)$ at most $n-d$ per hyperplane-called a *projective system* associated with C. If the points in $\mathcal{G}$ are distinct (so that essentially there are no repeated coordinates), C is a *projective code*. Hence, complete (n, r)-arcs in $PG(k-1, q)$ and projective $(n, k, n-r)_q$-codes that admit no projective extensions are equivalent objects. This begs the question: *Is a projective code corresponding to a complete arc necessarily maximal?* We show that projective codes of reasonable length admit only projective extensions. Many examples of large complete arcs exist; our results show that in many cases the corresponding codes are maximal. The methods used are based on the Bruen–Silverman model of linear codes utilizing coprimitive sets as well as the theory of Rédei blocking sets.

Joint work with A. A. Bruen.

ELWYN BERLEKAMP, University of California at Berkeley

History of Long Block Codes

In the first two decades following Shannon's classic 1948 paper, there were numerous studies aimed at determining the theoretical limitations on the performance of long block codes over a variety of channels, with and without such embellishments as list decoding or noiseless feedback. Concurrently, techniques to construct specific classes of block codes were introduced by Hamming, Elias, Reed–Muller, Bose–Chaudhuri–Hocquenhem, Reed–Solomon, and Gallager. Decoding algorithms, implementations, and applications came later.

This two-part talk will review some of the salient parts of this history, and identify a few of the problems which are still not completely solved.

RICHARD BLAHUT, University of Illinois

Source Coding in Information Theory

We survey some old results and discuss some new research in the general area of source coding in classical information theory.

KELDON DRUDGE, Prism Valuations, Toronto

Existence and non-existence results for "Extremal" line sets in $\mathrm{PG}(3, q)$

For a set of lines of $\mathrm{PG}(3,q)$ of a fixed cardinality, what are the maximum and minimum number of intersections between pairs of lines of the set? The question was posed (and answered) by J. Eisfeld in 1998. Both his upper and lower bounds are tight, but the sets meeting them have not been fully classified. In this talk we review the known results in the area and add a new example.

PETER DUKES, University of Victoria
Directed complete bipartite graph decompositions and three-state sensor networks

We examine edge-decompositions of the complete λ-fold directed graph $\vec{K}_n$ into complete bipartite directed subgraphs $\vec{K}_{a,b}$ as a model for communication in sensor or mobile ad hoc networks. In such a network, each node can be in one of three states: asleep (powered down), listening, or transmitting. Communication is effective only when the sender is transmitting, the destination is listening, and no other node in proximity to the receiver is also transmitting. We associate the vertices of $\vec{K}_n$ with nodes of the network, and blocks of the graph decomposition with time slots for communication.

A block with out-vertices A and in-vertices B corresponds to a slot in which the nodes in A are transmitting, those in B are receiving, and all others are asleep. Thus, such a decomposition of $\lambda\vec{K}_n$ guarantees every ordered pair of nodes in the associated network can communicate in λ time slots. However, it is also desirable to minimize interference by a third node. This talk will mention various constructions for these graph decompositions, with particular emphasis on properties minimizing interference.

VINCENT GAUDET, University of Alberta, Edmonton, AB T6G 2V4
Energy Efficient Decoding Using Analog VLSI Techniques

Low-density parity-check (LDPC) codes have become one of the preferred methods for forward error control in digital communications systems. These codes approach the Shannon capacity limit, and as such address the issue of transmit power. However, the use of such coding techniques also incurs a computational energy cost at the receiver that is not traditionally accounted for in the code design process. LDPC decoding is typically conducted using a message-passing algorithm that runs over a graphical representation of the code. Typical graphs may have tens of thousands of connections, each requiring several multi-bit messages to be passed during a decoding cycle, and perhaps requiring aggregate signaling rates on the order of Terabits per second! Since dynamic power consumption in a VLSI chip is related to the signaling rate, this represents a considerable challenge. In this talk I will present message-passing VLSI architectures that are guided by these computational energy constraints.

Analog decoders are message passing decoders that process LLR messages in continuous-time and using continuous-valued voltages and currents to represent likelihood messages. Only the outputs of decoders are binary, and as such analog decoders do not require high-speed analog-to-digital converters as a front end. Such decoders, often based on the Gilbert multiplier using sub-threshold mode CMOS transistors, have been shown in physical measurements to be computationally efficient. This talk will provide an introduction to the circuits used in such analog decoders, as well as the design challenges and limitations of the technology.

MARTIN HASSNER, Hitachi Global Storage Technology Research
Self-Replicating Trellis Graphs

Trellis Codes are described by Lie Algebra Root Lattices where the encoder redundancy is due to the choice of a Sublattice. In this talk we discuss Root Sublattice Coupling Algebras whose character multiplication has the property of "Self-Replication".

OLOF HEDEN, Department of Mathematics, KTH, S-100 44 Stockholm, Sweden
A tree of perfect codes

There are now more than 20, or perhaps 30, different constructions of perfect codes. The classification and enumeration of all perfect codes of length n is still an open problem, even for such small lengths as $n = 15$.

By considering tiles of Z_2^k, one may to any perfect 1-error correcting binary code C of length n recursively associate a tree. The root of the tree will be the perfect code C and all vertices will be perfect codes of shorter length than n. The leaves will be either linear perfect codes or full rank perfect codes. (A perfect code of length n has full rank if the dimension of the linear span of the words of the code will be equal to n.) This will show that full rank perfect codes act like prime elements and that the classification of full rank perfect codes is the key to the classification of all perfect 1-error correcting binary codes.

References

[1] O. Heden, *The partial order of perfect codes associated to a perfect code.* Advances in Mathematics of Communications, to appear.

PETER LISONEK, Simon Fraser University, Burnaby, BC

Steganography with linear codes

Steganography is the science of information hiding. The sender embeds a secret message into a cover object (e.g., a multimedia file) by slightly distorting it in a way that enables the intended recipient to retrieve the hidden message; at the same time the very existence of the hidden message should be impossible to detect by any third party.

The main goal of steganography is to manage the trade-off between the amount of communicated information and the amount of introduced distortion. We will show how linear codes can be used for this purpose. We will survey the recent results and list some open problems.

JIM McQUILLAN, Western Illinois University, Department of Computer Science, 447 Stipes Hall, Macomb, IL 61455, USA

Codes and Hyperovals

We investigate connections between codes and hyperovals. In $PG(2,4)$, for example, we can exploit the even intersection equivalence relation amongst the hyperovals to help us construct a self-dual code.

MICHELE MOSCA, Institute for Quantum Computing (UW) and Perimeter Institute

Self-testing Quantum Apparatus

In order to execute any quantum cryptographic protocol in practice, one must somehow trust that their quantum apparatus is faithfully executing the protocol.

Quantum self-testing defines a framework for testing quantum apparatus. I will show how a quantum circuit together with measurement apparatuses and EPR sources can be fully verified without any reference to some other trusted set of quantum devices (joint work with Magniez, Mayers and Ollivier). Our main assumption is that the physical system we are working with consists of several identifiable sub-systems, on which we can apply some given gates locally. We design a test for any quantum circuit whose complexity is linear in the number of gates and qubits, and polynomial in the required precision.

This self-testing procedure applies to protocols that only require states and operations with real-valued coefficients. The reason for this restriction was an intuition that computations with complex amplitudes can be simulated using only real amplitudes, and the simulation would not be unitarily equivalent to the desired complex amplitude computation. Recent work (with Matthew McKague) gives a simulation of general quantum circuits using states and unitaries with real coefficients only.

AIDAN ROY, University of Calgary

Highly nonlinear functions in terms of codes, graphs, and designs

As well as having a number of applications in cryptography, some highly nonlinear functions over finite fields can be used to produce interesting graphs and error-correcting codes. In this talk we show that crooked functions can be characterized by both the distance of a Preparata-like code and the distance-regularity of a crooked graph. We then introduce another application for nonlinear functions, namely spherical designs, and show that differentially 1-uniform functions over abelian groups can be characterized by weighted complex 2-designs.

CHRISTIAN SCHLEGEL, University of Alberta, Edmonton, AB T6G 2V4, Canada

Generalized Modulation and Iterative Demodulation

Modulation is the process of mapping discrete signals onto basis waveforms suitable for transmission. These basis waveforms are typically engineered to be orthogonal. However, in many modern high-density communications channels, orthogonality of these basis waveforms cannot be guaranteed and is often lost. In this talk we consider modulation where the signal waveforms are correlated.

While it is well-known that for low spectral efficiencies linear separation via minimum mean-square error (MMSE) filtering provides close to optimal performance, linear approaches fail as higher spectral utilization is desired. The alternatives of approximations to maximum-likelihood decoders, such as sphere decoding quickly become practically infeasible due to complexity constraints. We propose an alternate method where the redundancy required to achieve reliability is achieved by increasing the number of signal functions used. It is shown that for the case of uniformly random signal functions, the capacity of the increased set of signal waveforms is nondecreasing and achieves the capacity of the Gaussian multiple access channel as it upper limit, when the number of waveforms becomes large. Furthermore, a simple iterative demodulator allows achievable spectral efficiencies beyond those achieved by linear processing, and it is proven that the capacity of the channel can be achieved to within less than 1 bit as the number of signal functions becomes large.

CLAUDE TARDIF, Royal Military College of Canada, PO Box 17000, Station "Forces" Kingston, Ontario K7K 7B4, Canada

A dualistic approach to graph colouring

It is possible to give an upper bound for the chromatic number or fractional chromatic number of a graph by finding a suitable orientation of its edges avoiding homomorphisms from certain prescribed paths. The classical example is given by the classical "Gallai–Roy" theorem, which states that any graph that admits an orientation with no homomorphic image of the directed path with n edges can be coloured with n colours. Apart from the directed path with n edges, there are other paths that lead to similar and independent (perhaps non-constructive) certifications of n-colourability.

In this talk I will present some developments in this direction obtained jointly with Jaroslav Nesetril.

DMITRY TRUKACHEV, University of Alberta, Edmonton, Alberta, Canada

Analyzing Capacity of Ad-hoc Wireless Networks

Ad-hoc wireless networking is envisioned to be the next revolution in data communications with a number of applications ranging from people-to-people to device-to-device communication. Habitat monitoring and object tracking with sensors, distributed database synchronization, and communication in disaster recovery are a few examples. Such systems consist of node-pairs communicating without a fixed infrastructure. Data packets are usually delivered from source to destination via multiple hops through other nodes helping to relay the information. Despite huge interest in ad-hoc wireless networks little is known about the capability of these networks to carry information. Therefore, it is important to understand theoretical throughput and capacity limits and possible network operation strategies which can achieve these predicted limits.

In my lecture I will talk about network models, summarize early results on ad-hoc network capacity, describe common upper bounding techniques, and derivation of the achievability methods. In addition I will talk about the improvement of the scaling laws which can be obtained using multiple user detection techniques. Finally I will discuss the impact if traffic localization on the network capacity scaling laws.