Workshop on interactions between number theory and wireless communication: York2016

4 – 8 July 2016

Abstracts of talks

Faustin Adiceam (University of York)

Quadratic forms, lattice points and interference alignment

We will be concerned with the estimate of the probability that a positive definite quadratic form admits a minimum over non zero lattice points less than a given constant. This will first require the definition of a suitable class of probability measures. The latter will be defined from either the spectral or the Cholesky decomposition of a positive definite matrix. This theory is developed here with a view towards interference alignment. More precisely, we will use it to study the performance of some recently introduced channel architectures. A concise introduction to the theory of Signal Processing fitted to our purpose will be provided for the non-specialists. This is joint work with Evgeniy Zorin.

Alister Burr (University of York)

Multilevel Lattice Network Codes

We describe a multilevel framework for the design of lattices over a PID (and especially over the Eisenstein integers). We first motivate the use of a multilevel framework with reference to multilevel coded modulation, showing how it can increase flexibility and reduce complexity compared to Construction A based on a field homomorphism. We then introduce the framework we term the elementary divisor construction, and show how it can be used both to encode and decode lattice codes in the context of physical layer network coding. This is joint work with Yi Wang.

Uri Erez (Tel Aviv University, Israel)

Precoded integer-forcing equalization: a matrix “double-sided” diophantine approximation problem

Integer forcing is an equalization scheme for the multiple-input multiple-output (MIMO) communication channel that has been demonstrated to allow operating close to capacity for most MIMO channels, under several different notions of most. Specifically, it has been shown that for almost all real-valued $M \times N$ MIMO channels (w.r.t. Lebesgue measure), IF equalization achieves the optimal number of degrees-of-freedom (DoF). This stands in strong contrast to standard linear equalizers, such as the zero-forcing equalizer, or the MMSE equalizer, that fail to achieve the optimal number of DoF when $N < M$ (in fact, when $N < M$, they achieve zero DoF).

We show that integer-forcing is good for "most" channels also in a statistical sense, where now by "most" we mean that up to a small outage probability, close-to-capacity transmission rates are guaranteed for non-asymptotic values of signal-to-noise ratios, and where the probability is taken w.r.t. random unitary precoding. We further provide numerical evidence suggesting that for any MIMO channel, there exists a unitary precoding matrix for which integer-forcing is guaranteed to achieve a large fraction of capacity. Proving this statement and finding (or lower bounding) the latter guaranteed fraction is posed as an open problem.

Antonio Campello (Tlcom ParisTech, France)
Random Ensembles of Lattices with Multiplicative Structure

Lattice codes constitute a very suitable framework for constructing structured codes for a number of communication systems, from Gaussian channels to wireless networks. For several applications, such as the transmission of information over fading or multiple antennas, high coding performance is achieved by enriching the lattices with some algebraic (multiplicative) structure, which is often inherited by the properties of Number Fields. To this purpose, some recent works present different constructions that attach a linear code to an algebraic lattice. In this talk, we revisit these lattice constructions in a general setting, and then introduce a general method for establishing the goodness of random ensembles of such lattices. In particular, we describe a generalized version of a classic theorem in the Geometry of Numbers, the Minkowski-Hlawka theorem, for algebraic lattices. We then use this theorem to construct algebraic lattice codes that, leveraging from their underlying multiplicative structure, universally achieve the capacity of block-fading, ergodic fading and MIMO channels. This talk is based on joint work with Cong Ling and Jean-Claude Belfiore.

Chen Feng (University of British Columbia, Canada)
Wireless Network Coding over Finite Rings

Though network coding is traditionally performed over finite fields, recent work on wireless network coding suggests that the use of finite rings leads to better performance. This motivates a systematic study of wireless network coding over finite rings. As a starting point, the problem of communication over a finite-ring matrix channel $Y = AX + Z$ is considered; capacity results and capacity-achieving coding schemes are provided, extending the work of Silva, Kschischang and Koetter (2010), who handled the case of finite fields. A key step in this extension is a finite-ring version of Gaussian-Jordan elimination. Joint work with Roberto W. Nobrega and Frank R. Kschischang.

Camilla Hollanti (Aalto University, Finland)

Number-theoretic fast-decodable space-time codes for multiuser communications

We present the first general constructions of fast-decodable spacetime block codes for the Non-orthogonal Amplify and Forward (NAF) Multiple-Input Multiple-Output (MIMO) relay channel under the half-duplex constraint. In this scenario, the source and the intermediate relays used for data amplification are allowed to employ multiple antennas for data transmission and reception. The worst-case decoding complexity of the codes obtained by using number-theoretic methods is reduced by up to 75%. In addition to being fast-decodable, the proposed codes achieve full diversity and have non-vanishing determinants, which has been shown to be useful for achieving the optimal Diversity-Multiplexing Tradeoff (DMT) of the NAF channel. The talk is based on [A. Barreal, C. Hollanti, N. Markin, ”Fast-Decodable SpaceTime Codes for the N-Relay and Multiple-Access MIMO Channel”, IEEE Trans. Wireless Communications, 2016].

Yu-Chih (Jerry) Huang (National Taipei University, Taiwan)

Construction π_A Lattices: A Review and Recent Results

Construction π_A is a novel lattice construction recently proposed by Huang and Narayanan. The goodness for channel coding under multistage decoding and the goodness for MSE quantization of lattices thus constructed have been proved. These results have then been leveraged to construct capacity-achieving nested lattice codes for the AWGN channel under multistage decoding and to enable multistage compute-and-forward. In this talk, we will first review this lattice construction and its applications to the aforementioned two problems. We will then investigate further properties of Construction π_A lattices. We will show that the structure of such lattices makes them naturally suitted to the broadcast channel with message side information where each receiver demands all the messages and has an arbitrary subset of the messages as side information. Last, we will use these lattices to construct lattice index codes that achieve the capacity region of the broadcast channel with message side information.

Cong Ling (Imperial College London)

Secure Wireless Communications Using Algebraic Number Theory

Information theoretic security promises secure communications without using keys. This talk is concerned with secrecy coding over fading/MIMO wiretap channels. The construction of information theoretically secure codes over such channels remains an open problem, despite some works on fading wiretap codes from the error probability perspective. We show how a combination of algebraic number theory and information theory can be used to build secure lattices codes over fading/MIMO channels, towards achieving secrecy capacity.

Laura Luzzi (ENSEA, France)

DMT classification of MIMO codes and ergodic theory of Lie groups

In this work we provide new bounds for the diversity-multiplexing gain trade-off of space-time codes based on division algebras. We consider the union bound for the pairwise error probabilities, and show that its behavior at high SNR is essentially determined by the structure of the group of units of the division algebra. The corresponding sum over units can be estimated using tools from ergodic theory. In particular, the new bounds for codes derived from Q-central division algebras suggest that these codes can be divided into two classes based on their Hasse invariants at the infinite places. (This talk is based on a joint work with Roope Vehkalahti and Alexander Gorodnik).

Bobak Nazer (Boston University, US)

Towards an Algebraic Network Information Theory

Network information theory explores the fundamental limits of reliable communication and compression across a network. The classical approach to this theory uses random i.i.d. codebook constructions to obtain rate regions, which can in turn be evaluated and optimized to obtain performance limits. For example, Gaussian specializations of the multiple-access and broadcast rate regions have shaped the design of modern cellular networks.

Recent efforts have demonstrated that, in certain topologies, it is possible to outperform random i.i.d. codebooks by employing codebooks with algebraic structure. This algebraic structure may emerge either from the fact that the receivers only want a function of the transmitted messages (e.g., physical-layer network coding) or from the structure of the channel itself (e.g., interference alignment). Although there are now many examples highlighting the potential gains of codebooks with algebraic structure, it remains unclear if these examples can be captured as part of an accessible framework, i.e., an algebraic network information theory. In this talk, I will discuss, through a series of examples, recent progress towards such a theory and its implications for distributed source and channel coding.

Or Ordentlich (Massachusetts Institute of Technology, US)

Integer-Forcing Source Coding

Integer-Forcing (IF) is a framework, based on compute-and-forward, for decoding multiple integer linear combinations from the output of a Gaussian multiple-input multiple-output channel. This work develops the source coding dual of the IF approach to arrive at a new low-complexity scheme, IF source coding, for distributed lossy compression of correlated Gaussian sources under a minimum mean squared error distortion measure. All encoders use the same nested lattice codebook. Each encoder quantizes its observation using the fine lattice as a quantizer and reduces the result modulo the coarse lattice, which plays the role of binning. Rather than directly recovering the individual quantized signals, the decoder first recovers a full-rank set of judiciously chosen integer linear combinations of the quantized signals, and then inverts it. In general, the linear combinations have smaller average powers than the original signals. This allows to increase the density of the coarse lattice, which in turn translates to lower compression rates. We also propose and analyze a one-shot version of IF source coding, that is simple enough to potentially lead to a new design principle for analog-to-digital converters that can exploit spatial correlations between the sampled signals.

Roope Vehkalahti (University of Turku, Finland)

Fading channel analogues of the Hermite invariant

Classical information theory of the additive white Gaussian noise (AWGN) channel naturally suggests several coding theoretic problems that can be formulated on lattice theoretic language. For example, performance of a lattice code can be roughly estimated by it's Hermite invariant. By building sequence of lattice codes having linearly growing Hermite invariants we can also approach AWGN capacity. In this talk we will describe how it is possible to build an analogous theory of lattice codes for fading channels. In this theory classical Hermite invariant will get replaced by the concept of reduced Hermite invariant, which depends on the fading process. Building then families of lattices where the reduced Hermite invariants grow linearly will again lead to codes approaching the capacity of the targeted fading channel. We will further prove that in many cases reduced Hermite invariant can be realized as a minima of a certain homogeneous form. The talk is based on a joint work with Laura Luzzi.

Yihong Wu (Yale University, US)

Additive combinatorics and applications in interference channels

Additive combinatorics deals with the structures of sumsets and difference sets in groups. Many sumset inequalities involving set cardinalities have exact counterparts in information theory in the form of inequalities relating Shannon entropy of sums and difference of independent group-valued random variables. In the first part of the talk I will discuss how the high-SNR approximation of the capacity region of Gaussian interference channels, namely, the degrees of freedom region, can expressed in terms of ratios of Shannon entropy of linear combinations of independent random variables, which is directly related to sharp constants in additive combinatorial linear entropy inequalities. This will be the topic of the second part, where I will discuss some partial results and related observations.