Discrete Mathematics in Communications and Computation
Mathématiques discrètes en communications et en informatique
(Org: **Megan Dewar** (The Tutte Institute for Mathematics in Computing), **Daniel Panario** (Carleton University) and/et **David Thomson** (Carleton University))

TIM ALDERSON, University of New Brunswick Saint John
Maximum and Full Weight Spectrum Codes

In the recent work [3], a combinatorial problem concerning linear codes over a finite field $\mathbb{F}_q$ was introduced. In that work the authors studied the weight set of an $[n,k]_q$ linear code, that is the set of non-zero distinct Hamming weights, showing that its cardinality is upper bounded by $\frac{q^k-1}{q-1}$. Codes meeting this bound are said to be *maximum weight spectrum* (MWS) codes. Shi *et. al.* showed that MWS codes exist in the case $q=2$, and in the case $k=2$. They conjectured that MWS codes exist for every prime power q and every positive integer k. In this talk I discuss bounds on the length of MWS codes, and in the process, prove the conjecture. I also discuss a related question regarding full weight spectrum (FWS) codes, which are those codes having codewords of each weight less than or equal to n. Results discussed may be found in [1,2].

[1] TA, A note on full weight spectrum codes, *Transactions on Combinatorics*, (to appear).

[2] TA, and Alessandro Neri, Maximum weight spectrum codes,*Advances in Mathematics of Communications*, (to appear).

[3] Minjia Shi, Hongwei Zhu, Patrick Solé, and Gérard D. Cohen, How many weights can a linear code have?, *Designs, Codes and Cryptography*, May 2018.

MEGAN DEWAR, Tutte Institute for Mathematics and Computing
Connectivity in hypergraphs

The connectivity of a connected, nontrivial graph G, $\kappa(G)$, is the least number of vertices whose deletion from G results in a graph that is not connected. Deleting a vertex v means removing v from $V(G)$ and either removing v from each edge that contains it, or removing from $E(G)$ each edge that contains v. For graphs there is no practical difference between the two approaches, but for hypergraphs these two options can yield very different results. In this talk we'll explore these two definitions of hypergraph connectivity, known as weak and strong vertex deletion, respectively. We'll use a good number of examples to illustrate the concepts. Along the way we'll prove that the strong vertex connectivity (κ_s) of a hypergraph is always less than or equal to the weak vertex connectivity (κ_w) and we'll discuss the tractability of determining κ_w and κ_s. Finally, we'll extend a theorem of Whitney from graphs to hypergraphs – introducing the concepts of weak and strong edge deletion – furthering our understanding of the relationship between these various notions of hypergraph connectivity.

THAIS IDALINO, University of Ottawa
Efficient Unbounded Fault-Tolerant Aggregate Signatures Using Nested Cover-Free Families

Several applications deal with a large amount of data and digital signatures, such as outsourced databases, secure logging, sensor networks, etc. These applications require a way of saving on storage and communication, as well as a fast mechanism for verifying the signatures. We can solve these problems by using aggregate signature schemes, which combine all signatures into one. However, if at least one of the signatures is invalid, the entire aggregate is invalidated.

A fault-tolerant aggregate signature scheme is important for scenarios where we still want to identify the valid signatures and have the benefits of aggregation. This can be done by using d-cover-free families (d-CFFs) [1]. Given a bound d on the number of invalid signatures, the scheme can determine which signatures are invalid and guarantees a moderate increase on the size of the aggregate signature when there is an upper bound on the number n of signatures to be aggregated. However, for the case of unbounded n the constructions provided had a constant compression ratio, i.e. the signature size grew linearly with n. We propose a solution to the unbounded scheme with increasing compression ratio for every d, by proposing what we call a *nested family* of d-CFFs [2]. In particular, for $d=1$ the compression ratio meets the information theoretical bound.

[1] Hartung, G., Kaidel, B., Koch, A., Koch, J., Rupp, A.: "Fault-tolerant aggregate signatures". In: PKC 2016.

[2] Idalino T. B., Moura L. "Efficient Unbounded Fault-Tolerant Aggregate Signatures Using Nested Cover-Free Families". IWOCA 2018.

JONATHAN JEDWAB, Simon Fraser University

A recursive construction of linking systems of difference sets

Group difference sets are symmetric designs having a regular automorphism group. Difference sets in abelian groups correspond to multi-dimensional arrays over the alphabet $\{1, -1\}$ having all out-of-phase periodic autocorrelations zero, and these arrays have a wide range of applications in digital communications including synchronization, coded aperture imaging, and optical image alignment.

In 2014, Davis, Martin and Polhill introduced the concept of a linking system of difference sets, which is a collection of related difference sets having advantageous mutual properties. Such systems provide examples of systems of linked symmetric designs, as studied by Cameron and Seidel in 1973. The central problems are to determine which groups contain a linking system of difference sets, and how large such a system can be. Examples have been previously found using Galois rings, partial difference sets, a product construction, and group difference matrices.

I shall describe a new recursive construction of linking systems of difference sets in 2-groups. This is joint work with Shuxing Li and Samuel Simon.

PETR LISONEK, Simon Fraser University

Maximally non-associative quasigroups

A quasigroup $(Q, \cdot)$ is an algebraic structure whose multiplication table is a Latin square. We say that $(x, y, z) \in Q^3$ is an associative triple if $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Quasigroups with few associative triples were proposed for various applications in cryptography. Let $a(Q)$ denote the number of associative triples in Q. It is easy to show that $a(Q) \geq |Q|$. In 2012 Grošek and Horák conjectured that $a(Q) = |Q|$ never occurs. Let us call Q maximally non-associative if $a(Q) = |Q|$. The first example of a maximally non-associative quasigroup (of order 9) was found by Drápal and Valent (J. Combin. Des. 2018). In this work we use nearfields and their associated sharply two-transitive groups to construct maximally non-associative quasigroups. We conjecture that any nearfield that is not a field produces examples. We report results of an extensive and successful computer search. When q is an odd prime power, we show that a non-constructive existence result for maximally non-associative quasigroups of order q^2 can be obtained if certain character sums can be suitably bounded. This is joint work with Aleš Drápal (Charles University, Prague).

LUCIA MOURA, University of Ottawa

Covering Arrays and Combinatorial Testing

In the past decades, several combinatorial arrays useful in testing applications have been investigated. For example, cover-free families are used in group testing, while covering arrays and locating arrays are used in hardware and software testing. These objects have close ties to extremal set systems and error correcting codes, which have played an important role in combinatorial array construction. In this talk, we discuss common properties of various types of combinatorial arrays, as well as construction techniques and applications in computer science.

UPCOMING OPPORTUNITIES,

Upcoming Opportunities in Discrete Mathematics

At the conclusion of our scientific session, we will open the floor for announcements of "Upcoming Opportunities". Speakers (and other interested participants) will be free to announce positions, funding opportunities, solicit post-docs, students and collaborators.

AIDAN ROY, D-Wave Systems, Inc.
Mixed-integer linear programs and graph minors for quantum annealing

Quantum annealing (QA) is a type of computation which exploits quantum mechanical effects to solve discrete optimization problems, potentially faster than any classical algorithm. D-Wave Systems has developed a QA processor that optimizes over a restricted problem class, namely quadratic pseudo-boolean optimization problems, which allows scaling to many more qubits than is currently possible with gate-model quantum computers. However, the ability to solve real-world problems is still limited by issues of noise, connectivity, and size.

In this talk, I will present some interesting problems in discrete mathematics that arise from attempting to circumvent those limitations. First, I'll describe how noise and finite temperature in QA lead to mixed-integer linear programs for finding QUBOs, and I'll present new solution methods using SMT solvers. Second, I'll explain how sparse processor connectivity leads to a search for graph minors, and I'll describe a heuristic algorithm for finding them.

DAVID THOMSON, Carleton University
Low complexity normal bases over $\mathbb{F}_2$

This talk deals with basis representations of finite fields $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for computational purposes. We focus on *normal bases* that arise from the Galois orbit of a single field element. Explicitly, a normal basis is given by $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$ for some $\alpha \in \mathbb{F}_{2^n}$. Normal bases are required when exponentiation, and in particular squaring, is a critical operation within an application. Examples where normal basis representation is prescribed include small characteristic Diffie-Hellman, elliptic curve computations and decoding random linear network codes.

Generic field multiplication can be expensive under normal basis representation. A measure of the cost of multiplication is the complexity (or density) of the multiplication tables of the basis. We will discuss an efficient algorithm to exhaustive search $\mathbb{F}_{2^n}$ for $n \leq 46$ (and counting...) for the minimum complexity normal basis.