# Sequences and Codes
# IRMACS, Simon Fraser University
# 17-21 July 2006
# Conference Programme

We are very pleased to welcome you to the inter-disciplinary conference on Sequences and Codes. Our aim is to encourage interaction between mathematicians and engineers in these areas, both during the technical sessions and informally during the week.

We are grateful to the IRMACS Centre for hosting the conference, and to all our sponsors for their generous financial support of early career participants:

Pacific Institute for the Mathematical Sciences (PIMS)
Mathematics of Information Technology and Complex Systems (MITACS)
National Science Foundation (NSF)
Simon Fraser University (SFU)
Pacific Rim Mathematical Association (PRIMA).

We hope you find the conference enjoyable and stimulating.

Nigel Boston
Robert Calderbank
Jonathan Jedwab

# Conference Schedule

All sessions take place in the IRMACS Theatre unless otherwise noted

## Monday 17 July

8.30–9.00 Collection of conference materials and IRMACS access cards
9.00–9.15 Brian Corrie, IRMACS: Demonstration of IRMACS audio-visual facilities
9.15–9.30 Opening and welcome

- Mario Pinto, SFU VP Research
- Alejandro Adem, PIMS
- Arvind Gupta, MITACS
- Pam Borghardt, IRMACS

9.30–10.20 Bernhard Schmidt, "*Codes and Weil numbers*"

Coffee Break

10.50–11.20 Ken Smith, "*Rational idempotents and cyclic difference sets*"
11.30–12.00 Frederique Oggier, "*Algebraic Cayley differential space-time codes*"

Lunch Break

2.00–2.30 Kayo Yoshida, "*The peak sidelobe level of families of binary sequences*"
2.40–3.10 Anna Gilbert, "*List decoding of noisy Reed-Muller-like codes*"

Coffee Break

3.40–4.10 Felipe Voloch, "*Algebraic Geometric codes on surfaces*"
4.20–4.50 Mohamed Oussama Damen, "*Algebraic constructions outperforming the Alamouti scheme*"

5.00–10.00 Pub night, **SFU Pub**

## Tuesday 18 July

9.30–10.20 Jean-Claude Belfiore, "*Space-time block codes from cyclic division algebras: codes, encoders and decoders*"

Coffee Break

10.50–11.20 Frank Fiedler, "*Turyn's product construction revisited*"
11.30–12.00 Ghaya Rekaya-Ben Othman, "*A very efficient algebraic lattice reduction for algebraic STB codes*"

Lunch Break

2.00–2.50 Robert Calderbank, "*Heisenberg-Weyl groups and their application to sequence design*". PIMS Distinguished Lecture, **Images Theatre**.

3.00–3.50 Ingrid Daubechies, "*Introduction to wavelets*". PIMS Distinguished Lecture, **Images Theatre**.

Coffee, IRMACS Atrium

4.30–5.45 Question & Answer session with Robert Calderbank and Ingrid Daubechies (undergraduate and graduate students only), IRMACS Theatre

6.00 Reception, IRMACS Atrium

8.00 Outdoor chamber music concert (Mozart & Rossini), **Reflecting Pond**.

## Wednesday 19 July

9.30–10.20 Ralf Koetter, "*Coding, polytopes and low complexity algorithms*"

Coffee Break

10.50–11.40 Robert Calderbank, "*Heisenberg-Weyl groups and their application to sequence design II*"

12.00 First coach leaves **SFU Bus Loop** for excursion to Stanley Park
2.00 Second coach leaves **SFU Bus Loop** for excursion to Stanley Park
6.30 First coach returns to SFU from Stanley Park
9.30 Second coach returns to SFU from Stanley Park

## Thursday 20 July

9.30–10.20 Stephen Howard, "*Golay sequences – a tale of two Heisenberg groups"*

Coffee Break

10.50–11.20 Sinan Gunturk, "*On iterated running sums of* $\pm 1$ *sequences*"
11.30–12.00 James Davis, "*A proof of the Barker array conjecture*"

Lunch Break

2.00–2.30 Yi Hong, "*High rate space-time trellis coded modulation*"
2.40–3.10 David Grant, "*Aspects of space-time codes over finite fields*"

Coffee Break

3.45–5.15 Panel Discussion: "*Future directions in sequences and codes*"

- Arvind Gupta: "Future models of research in the mathematical sciences"
- James Davis: "Future research directions in sequences"
- Ralf Koetter: "Future research directions in codes"

7.30 Conference Banquet, **Diamond Alumni Centre**

## Friday 21 July

9.30–10.20 Judy Walker, "*Pseudocodewords of LDPC codes*"

Coffee Break

10.50–11.20 Stephen Choi, "*The limiting distribution of merit factors*"
11.30–12.00 Ozgur Yilmaz, "*Alternate duals for sigma-delta quantization of frame expansions*"

12.00 Closing

# Abstracts, in order of presentation

## Monday 17 July

**Bernhard Schmidt**, Nanyang Technological University
"*Large Codes and Weil numbers*"

For a positive integer *m*, an *m*-Weil number is an algebraic integer with squared absolute value *m* under every imbedding of $\mathbf{Q}(\alpha)$ into the complex numbers. Weil numbers are useful in certain areas of Design and Coding Theory. For example, recent progress on the Barker Sequence and Circulant Hadamard Matrix Conjectures solely relies on properties of Weil numbers. Another application of Weil numbers, a constructive method for the classification of difference sets, was developed by Baumert already in the 1960s/70s. In joint work with McEliece, Baumert extended this method and was able to compute the weight distribution of a large class of binary cyclic irreducible codes. As an input, Baumert's method needs all relevant *m*-Weil numbers in certain cyclotomic fields for certain *m*. However, using current software, Weil numbers $\alpha$ usually can only be computed if the degree of $\mathbf{Q}(\alpha\zeta)/\mathbf{Q}$ is very small for some root of unity $\zeta$.

We propose an algorithm based on lattice basis reduction techniques which allows to compute Weil numbers for considerably larger degrees. As an application, we compute the weight distribution of some classes of binary irreducible cyclic codes, extending previous work of Baumert, Rumsey, McEliece, MacWilliams, Seery, Segal and Ward.

(Joint work with Dang Khoa Nguyen, Nanyang Technological University)

**Ken Smith**, Central Michigan University
"*Rational idempotents and cyclic difference sets*"

An element *D* of the integral group ring $\mathbf{Z}[G]$ may be written as a $\mathbf{Z}[G]$-linear combination of rational idempotents of the group ring *G*. In certain cases, this viewpoint provides strong restrictions on the construction of the element *D*.

We describe applications of rational idempotents to difference sets in abelian groups, focusing on Hadamard difference sets where the group *G* has a large cyclic subgroup.

(Joint work with Jim Davis, University of Richmond)

**Frederique Oggier**, Calfornia Institute of Technology
"*Algebraic Cayley differential space-time codes*"

We consider the problem of designing Space-Time Codes for the non-coherent MIMO channel, that is, when the receiver has no knowledge of the channel. In such scenario, a scheme called differential modulation has been shown to allow decoding at the receiver. This scheme requires the design of unitary matrices, and the computation of an upper bound on the pairwise probability of error shows that in order to get good performance, the unitary matrices have to be fully-diverse, namely the determinant of the difference of any two matrices has to be non-zero. Based on the Cayley transform that maps an Hermitian matrix to a unitary matrix, Cayley codes have been proposed as an approach to that problem. However, previous work on Cayley codes focussed on the mutual information between the input and output matrix, arguing that at high rate, the huge number of signals makes the computation of the diversity intractable and lessens its usefulness as a performance criterion. Recently, division algebras have been introduced as a tool for Space-Time Coding, since by definition, these algebras yield families of matrices that are fully-diverse.

In this work, we explain how to design Cayley codes from division algebras, and show that this approach yields Cayley codes whose performance compares with the optimized existing Cayley codes and other unitary codes obtained from Lie algebras.

**Kayo Yoshida**, Simon Fraser University
"*The peak sidelobe level of families of binary sequences*"

A numerical investigation is presented for the peak sidelobe level (PSL) of Legendre sequences and maximal length shift register sequences (*m*-sequences). The PSL gives an alternative to the merit factor for measuring the collective smallness of the aperiodic autocorrelations of a binary sequence. The growth of the PSL of these infinite families of binary sequences is tested against the desired growth rate $o(\sqrt{n \ln n})$ for sequence length $n$. The claim that the PSL of *m*-sequences grows like $O(\sqrt{n})$, which appears frequently in the radar literature, is concluded to be unproven and not currently supported by data.

(Joint work with Jonathan Jedwab, Simon Fraser University)

**Anna Gilbert**, University of Michigan
"*List decoding of noisy Reed-Muller-like codes*"

Coding theory has played a central role in the development of computer science. One critical point of interaction is decoding error-correcting codes. First- and second-order Reed-Muller (RM(1) and RM(2), respectively) codes are two fundamental error-correcting codes which arise in communication as well as in probabilistically checkable proofs and learning. In this paper, we take the first steps toward extending the decoding tools of RM(1) into the realm of quadratic binary and, equivalently, $Z_4$ codes. We show how to recover a substantial subcode of RM(2), a Kerdock code, in the presence of significant noise. The Kerdock codes are a well-studied family of codes for coding theory, radar signaling, and spread spectrum communication. Our result is a list-decoding result for Kerdock codes which is roughly analogous to that of RM(1). In addition, we present a new algorithmic characterization of Kerdock codes that we hope will be more useful to the algorithmic (and coding theory) community than the classic descriptions.

**Felipe Voloch**, University of Texas at Austin
"*Algebraic Geometric codes on surfaces*"

This talk presents some results obtained by my student M. Zarzar and myself on Algebraic Geometric codes on surfaces. In particular, I will discuss the minimal distance of these codes and decoding algorithms. To obtain bounds for the minimal distance we needed to understand how zero sets of functions on surfaces decompose in irreducible components and this led to some geometric results. We discuss a decoding algorithm which uses the LDPC structure of these codes and extends some work of Luby and Mitzenmacher on decoding LDPC codes over large alphabets.

**Mohamed Oussama Damen**, University of Waterloo
"*Algebraic constructions outperforming the Alamouti scheme*"

The Alamouti scheme achieves the maximum diversity over $M$=2 transmit antennas and $T$=2 symbol periods, and has a simple linear processing maximum likelihood decoder without data rate reduction when the number of receive antennas $N$=1. It has many interesting algebraic properties and has been studied extensively in the last 7 years and is adopted in the standard of the third generation mobile radio system (UMTS and CDMA2000) as well as broadband wireless networks WiMax (IEEE802.16e). In this talk, a thorough comparison is done between $2 \times 2$ space-time block codes outperforming the Alamouti scheme when the number of receive antennas is greater than 1. The codes with the best tradeoff between performances, complexities, and peak power constraints are identified.

## Tuesday 18 July

**Jean-Claude Belfiore**, Ecole Nationale Superieure des Telecommunications
"*Space-time block codes from cyclic division algebras: codes, encoders and decoders*"

Division algebra is the appropriate structure to construct space-time block codes. The Alamouti code relies on the Hamilton quaternions which is the most famous division algebra. We know that this code is optimal (in the sense of some criteria that will be exposed) when the number of transmit antennas is equal to 2 and the number of receive antennas is equal to one. By considering other division algebras we will show the construction of the Golden code, which is optimal for 2 transmit antennas and 2 or more receive antennas, and the perfect space-time block codes when the number of transmit antennas is larger than 2. We have the codes. Finally, some preliminary results will be given on the structure of encoders and decoders using such codes by taking the Golden Code as an example.

**Frank Fiedler**, Allegheny College
"*Turyn's product construction revisited*"

We provide a minimal framework of constructions to generate the known Golay complementary sequences of length $2^m$ with entries in $\mathbf{Z}_{2^h}$ from pairs of Golay sequences. This framework involves several generalizations of Turyn's 1974 product construction and symmetry operations. Recursive use of these constructions yield all standard Golay pairs as listed by Davis and Jedwab in 1999, as well as new examples listed by Li and Chu in 2005, and sequences arising from these new examples.

(Joint work with Jonathan Jedwab, Simon Fraser University and Matthew Parker, University of Bergen)

**Ghaya Rekaya-Ben Othman**, Ecole Nationale Superieure des Telecommunications
"*A very efficient algebraic lattice reduction for algebraic STB codes*"

Full rate, full diversity Space-Time codes that achieve the Diversity-Multiplexing Gain tradeoff are constructed from cyclic division algebras, like the Golden code and Perfect codes. For a number of antennas larger than 3, the decoding complexity of such codes makes difficult their practical use.

Our idea is to find a lattice reduction adapted to code algebraic construction, which provides a quasi-orthogonal lattice base, and then reduce the decoding complexity. We propose a new algebraic lattice reduction based on the search of cyclic algebra units. Simulation results show that algebraic reduction followed by a ZD-DFE gives quasi-ML performances and preserve the diversity gain of the code.

(Joint work with Jean-Claude Belfiore, ENST)

**Robert Calderbank**, Princeton University
"*Heisenberg-Weyl groups and their application to sequence design I*"
PIMS Distinguished Lecture

We will describe how Heisenberg-Weyl groups appear in the construction of phase coded radar waveforms, in the design of spreading sequences in wireless communications, and in the theory of classical and quantum error-correcting codes. Interesting examples include the first and second order Reed-Muller codes, the binary and quaternary Kerdock codes, and the Welti and other Golay complementary sequences. These talks will focus on sequences contained in orthonormal bases fixed by maximal abelian subgroups of the Heisenberg-Weyl group. We will describe how the correlation properties of sequences in these orthonormal bases are determined by the symmetry group of the basis in the Heisenberg-Weyl group.

**Ingrid Daubechies**, Princeton University
"*Introduction to Wavelets*"
PIMS Distinguished Lecture

Wavelets are a new approach used in the analysis of sounds and images, as well as in many other applications. The wavelet transform provides a mathematical analog to a music score: just as the score tells a musician which notes to play when, the wavelet analysis of a sound takes things apart into elementary units with a well defined frequency (which note?) and at a well defined time (when?). For images wavelets allow you to first describe the coarse features with a broad brush, and then later to fill in details, similar to zooming in with a camera. For this reason, the wavelet transform is sometimes called a "mathematical microscope".

Wavelets are used by many scientists and engineers for a wide range of applications. In particular, they have been incorporated in the JPEG2000 image compression standard.

The talk will start by explaining the basic principles of wavelets, which are very simple. Then they will be illustrated with some examples, including pictures of the wavelet scheme used by the FBI. Throughout the talk we will see how wavelets emerged as a synthesis of ideas from many different directions.

## Wednesday 19 July

**Ralf Koetter**, University of Illinois
"*Coding, polytopes and low complexity algorithms*"

Low complexity coding algorithms, in particular message passing algorithms have drastically changed the landscape for high performance codes in practice. While the underpinnings of these algorithms were not well understood for the last few years, by now strong connection to various combinatorial optimization approaches can be made. A central role here plays the formulation of the decoding problem as a linear program (LP). While it is clear that one can use any general-purpose LP solver to solve the LP that appears in the decoding problem, we argue that the LP at hand is equipped with a lot of structure that one should take advantage of.

Towards this goal, we study the dual LP and show how message passing algorithms can actually be used as LP solvers. This shows that LP solvers with complexity similar to the min-sum algorithm and the sum-product algorithm are feasible.

(Joint work with Pascal Vontobel, Massachusetts Institute of Technology)

**Robert Calderbank**, Princeton University
"*Heisenberg-Weyl groups and their application to sequence design II*"

We will describe how Heisenberg-Weyl groups appear in the construction of phase coded radar waveforms, in the design of spreading sequences in wireless communications, and in the theory of classical and quantum error-correcting codes. Interesting examples include the first and second order Reed-Muller codes, the binary and quaternary Kerdock codes, and the Welti and other Golay complementary sequences. These talks will focus on sequences contained in orthonormal bases fixed by maximal abelian subgroups of the Heisenberg-Weyl group. We will describe how the correlation properties of sequences in these orthonormal bases are determined by the symmetry group of the basis in the Heisenberg-Weyl group.

## Thursday 20 July

**Stephen Howard**, Defence Science and Technology Organisation, Australia

*"Golay sequences – a tale of two Heisenberg groups"*

For some time it has been known that the continuous Heisenberg-Weyl group provides a theoretical basis for radar detection. However, it has recently become apparent that the finite multidimensional Heisenberg-Weyl groups also have a role to play. In this talk we will describe the theory of the Heisenberg-Weyl groups in relation to the development of waveform libraries for adaptive radar. These groups form the basis for the representation of the radar environment in terms of operators on the space of waveforms, as well as a unified basis for the construction of useful waveform/sequence libraries for radar.

We will emphasize the Golay complementary or Welti waveforms/sequences and show that their existence and properties can be understood in terms of the relationship between two different finite Heisenberg-Weyl groups. The first of these groups is more familiar in coding theory for communications, where it is used to study of the Kerdock codes and quantum error correcting codes, while the other appears in a discrete model of radar.

**Sinan Gunturk**, Courant Institute of Mathematical Sciences

"*On iterated running sums of* $\pm 1$ *sequences*"

In this talk we provide tight asymptotical bounds on the minimal growth rate of the sup-norm of iterated running sums of infinite $\pm 1$ sequences. Let $S$ denote the summation operator defined by $(Sw)_n = w_0 + w_1 + \ldots + w_n$. The celebrated Thue-Morse sequence $\tau$ has the property that $S^k\tau$ is a bounded sequence for all $k \geq 0$ and $\left\|S^k\tau\right\|_\infty \sim c^{k^2}$ for some $c > 0$.

We show that there are two positive constants $A$ and $B$ such that for all positive integers $k$

$$(Ak)^k \leq \inf_{q\in\{-1,1\}^N} \left\|S^k q\right\|_\infty \leq (Bk)^k.$$

A slightly weaker upper bound can still be achieved even if we require that $q$ be independent of $k$; hence the Thue-Morse sequence is asymptotically suboptimal for this problem.

(Joint work with Sergei Konyagin, Moscow State University)

**James Davis**, University of Richmond
"*A proof of the Barker array conjecture*"

Using only elementary methods, we prove Alquaddoomi and Scholtz's conjecture of 1989, that no $s \times t$ Barker array having $s, t > 1$ exists except when $s = t = 2$.

(Joint work with Jonathan Jedwab, Simon Fraser University and Ken Smith, Central Michigan University)

**Yi Hong**, University of South Australia
"*High rate space-time trellis coded modulation*"

In this paper, we present a concatenated scheme for a $2 \times 2$ multiple-input multiple-output (MIMO) system over slow fading channels. The inner code is the Golden code and the outer code is a trellis code. Lattice set partitioning is designed specifically to increase the minimum determinant of the Golden codewords, which will label the branches of the outer trellis code. The Viterbi algorithm is applied in the trellis decoding, where each branch metric is computed using a lattice decoder. The performance of the proposed concatenated scheme is evaluated by simulation. It is shown that the proposed scheme achieves performance gains over the uncoded Golden code.

**David Grant**, University of Colorado at Boulder
"*Aspects of space-time codes over finite fields*"

Dayal and Varanasi recently specified design criteria (including diversity orders) for space-times codes taking into account spatial correlation at both the transmit and receive antennas and temporal correlation. Recently the speakers showed that every "algebraic" space-time code can be arbitrarily-well approximated by an "equivalent" one over a finite field.

In this talk we will show that among all these space-time codes designed for general spatial-temporal correlated channels, the only ones whose finite field analogues have a duality theory are the ones whose diversity orders are the column distance and the rank distance. Gabidulin related column distance codes over finite fields to Hamming distance codes over extension fields. The duality theory for rank codes over finite fields (also called *q*-codes) was developed by Delsarte. Recently the speakers derived a rank enumerator for a rank code over a finite field that has a functional equation relating it to the rank enumerator of its dual. We will explain how this leads to an analogue of Gleason's Theorem for self-dual rank codes over finite fields.

(Joint work with Mahesh Varanasi, University of Colorado at Boulder)

## Friday 21 July

**Judy Walker**, University of Nebraska
"*Characterizations of pseudocodewords of LDPC codes*"

The greatest strength of low density parity check (LDPC) codes is the existence of an extremely efficient iterative decoding algorithm for them. This algorithm's low complexity results from the fact that it operates locally on the bipartite graph $T$ associated to the code. But the local nature of the algorithm also leads to a weakness of LDPC codes: codewords in codes corresponding to finite covers of $T$ lead to pseudocodewords, which interfere with decoding. We will discuss two characterizations of these pseudocodewords, one in terms of a geometric object called the fundamental cone, and the other in terms of a multivariable zeta function associated to $T$.

(Joint work with Ralf Koetter, University of Illinois, Winnie Li, Pennsylvania State University and Pascal Vontobel, Massachusetts Institute of Technology)

**Stephen Choi**, Simon Fraser University
"*The limiting distribution of merit factors*"

The distribution of the merit factors of finite binary sequences of length $N$ will be studied and we will prove that the limiting distribution is the one-point Dirac distribution as $N$ to infinity.

**Ozgur Yilmaz**, University of British Columbia
"*Alternate duals for sigma-delta quantization of frame expansions*"

A basic problem in signal processing, when analyzing a given signal of interest, is to obtain a digital representation that is suitable for storage, transmission, and recovery. A reasonable approach is to first decompose the signal as a sum of appropriate harmonics, where each harmonic has a real (or complex) coefficient. Next, one "quantizes" the coefficients, i.e., one replaces each coefficient by an element of a given finite set (e.g. $\{-1,1\}$). The problem of how to quantize a given expansion is non-trivial when the expansion is redundant.

In this talk, we shall consider redundant frame expansions, and show that sigma-delta modulators provide efficient quantization algorithms in the case of finite frame expansions in Euclidean space. In particular, we shall construct alternate dual frame sequences which ensure that a $k$th-order sigma-delta quantizer produces approximations where the approximation error is of order $A^{-k}$ if the original frame is a tight frame with frame bound $A$. We then use this construction to prove that the vector quantizer associated with the sigma-delta family has exponential precision with respect to bit-rate.