www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 4 No. 4 (2015), pp. 1-23.

www.ui.ac.ir

GROUP RINGS FOR COMMUNICATIONS

TED HURLEY

Communicated by Victor Bovdi

Abstract. This is a survey of some recent applications of abstract algebra, and in particular group rings, to the communications' areas.

1. **Abstract algebra**

Abstract algebraic structures are fundamental building blocks for designs within the communications' areas. Structures used include fields, rings, groups, group rings, orthonormal bases, idempotents structures and their associated matrices and representations. Here we are particularly interested in such designs and methods in which group ring structures and related areas are involved; in recent times these have been shown to be eminently useful.

An engineer may design a structure without realising the significance of the general abstract structure within which the structure resides. Better designs/systems may be realised using abstract algebra structures, and required systems which have resisted design by ad-hoc methods can be constructed by abstract algebra methods.

We, the mathematicians, are more interested in *theorems* on the *whole* algebraic structures rather than the *elements* of the structures or the properties of the elements themselves. Engineers require *machines* (= elements) that work in order to perform a specific task. Mathematicians can design the 'machine' or system which they know from theory will work. For an engineer or computer scientist the mathematics becomes crucial; but *practical implementation* of the mathematics is required by them. Mathematicians often have a blind spot for applications and fail to recognise the applications of their work.

MSC(2010): Primary: 15B99; Secondary: 94A12.

Keywords: Communications, Group Rings.

Received: 3 May 2014, Accepted: 18 May 2014.

The *element* is the *machine* designed from the mathematical concept produced to perform a particular practical task. For example the extended Golay code, which is used widely in communications, is a particular *element* of an abstract algebraic structure [38]; engineers study this element for its use. An encryption system for say RSA with *specific key* $\{$*public key* $= (n, e)$, *private key* $= d\}$ is the element = machine which is constructed.

A code or filterbank which behaves in a certain way may be required; the mathematician supplies the algebra that he/she knows from theory will produce the code or filterbank to the required specifications. A particular case is a requirement for codes for devices with *low storage and low power*, as for example for *implanted medical devices*. A code stored by an algebraic formula which generates the code is the solution. The matrix size could be of large order but an algebraic expression to produce the code may require storing only a small number of elements, see for example [30]. This produces a code not only stored by an algebraic formula but also what is called a *Low density parity check* (LDPC) code and these types are 'known' to perform well in practice. Convolutional codes, see [4] for basic information on such, in general are designed by computer search but now for large size requirements such searches are impractical and algebraic methods are needed, [40, 41, 42].

1.1. **Areas of application.** Here are communications' areas where abstract algebra methods have played major roles:

(1) Cryptography.
(2) Coding Theory.
(3) Signal processing (filterbanks, wavelets).
(4) Multiple antenna code design. The design problem for unitary space time constellations: This has applications such as for *mobile phone* communications.
(5) Compressed sensing.
(6) Search engines, internet nodes.
(7) Threshold functions/logic.
(8) Software engineering.
(9) ...

1.2. **Background discussion.** These are huge areas of research nowadays with massive numbers of engineers, scientists and mathematicians working therein. Unique approaches are now required in order to make real headway; it is our claim that novel approaches require *abstract algebraic techniques* much more so now than ever before.

Nowadays 'Intellectual Property' (IP) is a buzz word and almost all Universities have big and expanding 'Technology Transfer'-type units whose sole business is to interact with industry and acquire IP. In addition quantity policies of 'increase by x% the number of patents, increase IP, increase citations, increase impact factors' are prevalent and are being used as an important measurement for appointment and promotion. Why has 'peer-review' taken such a back stage? What has happened to 'quality' as a measurement?

New designs are often considered as 'inventions' in the industry and may be patented so as acquire IP with the idea of obtaining market advantage or simply just in order to prevent someone else from obtaining an advantage.

To what extent have mathematicians been involved in these activities? Should mathematicians be (more) involved in these activities? Mathematics itself cannot be patented so patents which are essentially mathematics are presented as 'machines' for performing particular tasks. Patent laws differ in countries or group of countries. The laws have also changed recently so that now the *date of filing* and who files at that time is what counts. Thus someone could 'invent' something, publish it and then someone else could file a patent based on the 'invention' and get priority. What often happens is that the mathematician makes a breakthrough (knowing or unknowingly) which is then patented by someone else. It is clear also that (potential) IP is also now very often a requirement for obtaining funding and Government agencies insist on industry involvement or potential industrial involvement before they will even consider an application.

The PageRank patent from which Google developed is an interesting case. 'Method for node ranking in a linked database' was filed in 1998; the invention is assigned to Stanford University and the inventor is listed as Lawrence Page who with Sergey Brin founded Google at around the same time. Being mathematicians, Page and Brin termed the company 'Google' as a twist or pun on the mathematical term 'Googol' which specifically denotes 10^{100}. 'Google' turned out to be a wise and fortuitous term indeed. 'Googleplex' is the corporate headquarters of Google; in mathematics a googolplex is $10^{googol} = 10^{10^{100}}$. The term 'Google' has now entered languages as an action/verb word – *google it!*.

1.2.1. **'Engineering' mathematics.** Engineering and Computer Science courses have now *less* Mathematics courses than ever and *little if any* more advanced algebra courses. Thus many engineers are unable to get to the cutting edge in communications' areas which now require abstract algebraic techniques; these are very often capable people and well able to cope with the ideas, given the right background. Mathematicians often do not realise the applications of their areas – or indeed do not want and/or are unwilling to get involved or associate with the practitioners.

A practising software engineer, Dick Hamlet, with many books and articles in the area to his credit, recently published an interesting paper [18] which discusses the often tempestuous relationships between engineers and mathematicians (and scientists). Here is just one quotation: "For an engineer, the mathematics of a science becomes an indispensable tool. The devices that an engineer designs must conform to physical reality or they won't work, and mathematics is the method by which details of the design are worked to properly serve reality. In some cases, special mathematics makes the engineers job easier. The best example comes from electrical engineering, where the Fourier and Laplace transforms are used to convert differential equations into algebra. Where a physicist understands an electronic circuit as a set of simultaneous differential equations, an electrical engineer can describe the circuit with high school mathematics."

1.3. **Basic references.** Basic backgrounds for different areas may be obtained in the following books: for algebra see [39], [9], for coding theory see [4], for cryptography consult [34], for signal processing use [46] or [50]. In recent times three related rather nice survey type articles appeared in the Notices of the AMS [43], [35], [36]; all are well worth investigating for further background information and inspiration. The book [5] presents related aspects of algebra in communications.

Coding theory is used for the *safe* transmission of data and cryptography is used for the *secret* transmission of data. Group rings and their applications to cryptography and some related areas are dealt with in another article in this proceedings, [8], and a scheme related to group rings is presented in section 8.

In coding theory larger systems are now required, such as for convolutional codes, and search and ad-hoc methods are beyond the range of computer calculation and construction; algebraic approaches and constructions are required.

There are nice theorems involved; the mathematicians who have an aversion to applications should also be happy! Group ring methods turn out very useful for various constructions and many existing and often used structures, such as cyclic codes, are special cases of constructions with group rings and related structures.

1.4. **Topics by section.** The rest of the paper treats the topics listed in Section 1.1 from the point of view of abstract algebra and in particular in relation to group rings and their associated structures. The basics of the algebraic structures are drawn up and then references to the literature for further details are given as required. Each section may essentially be read independently of the others.

- Section 2 considers aspects of Coding Theory and section 6 develops methods for constructing and analysing mds (maximum distance separable) codes with group rings.
- Section 3 develops the interplay between Fourier matrices and circulant matrices; circulant matrices are group ring matrices of the cyclic group and are diagonalised by the Fourier matrix.
- Section 4 considers aspects of orthogonal sets of idempotents as building blocks for paraunitary matrices; in the research areas of filterbanks and wavelets the concept of a paraunitary matrix has a fundamental relationship.
- In Section 5 applications to multiple antenna design using complete orthogonal sets of idempotents are developed.
- Section 7 discusses the surprising relationships of the algebra to *compressed sensing*, an area which has applications in such areas as MRI, astronomy and others.
- In section 8 cryptographic systems from group rings are constructed.
- Search engines and threshold logic are briefly discussed in Section 9.

2. Coding theory

In a nutshell linear Coding Theory may be construed as:

$$GH^{\mathrm{T}} = 0$$

where G is an $r \times n$ matrix of rank r and H^{T} is an $n \times (n-r)$ matrix of rank$(n-r)$. This gives an (n, r) code of length n and dimension r with generator matrix G and check matrix H.

This set-up should remind one of *zero-divisors*.

The distance d of such a code is a function of the maximum number of linearly independent columns of H; see [4]. We would like d to be as large as possible. Knowing d we then write (n, r, d) for the type of code.

2.1. **Use units to construct codes as well as zero-divisors.** A non-zero element of a group ring over a field is either a zero-divisor or a unit when the group is finite. An element in a group ring can be mapped uniquely to an element in the corresponding matrix ring and this gives an interplay between properties and constructions in the group ring and the matrix ring, [23], which is particularly useful in coding theory.

It is common to consider codes formed from zero-divisors and ideals in group rings; for example cyclic codes are determined from *zero divisors in the cyclic group ring* and are ideals in the cyclic group ring. But indeed codes of many types and forms may also be constructed from units.

See [20, 21] for further details on the following. Suppose $UV = I$ in $R_{n\times n}$ where R is a ring with identity, $R_{n\times n}$ is the ring of $n \times n$ matrices with coefficients from R and I is the identity $n \times n$ matrix.

Divide $U = \begin{pmatrix} A \\ B \end{pmatrix}$ into block matrices where A is $r \times n$ and B is $(n-r) \times n$. Similarly, let $V = \begin{pmatrix} C & D \end{pmatrix}$ where C is $n \times r$ and D is $n \times (n-r)$.

Now $UV = \begin{pmatrix} AC & AD \\ BC & BD \end{pmatrix} = I$ and so $AD = 0$. It follows A is a generator matrix for a code and D^{T} is a check matrix for this code!

U, V could be the matrices of group ring elements or in general are elements of a matrix ring with coefficients from a ring.

This can be generalised as follows: Choose *any* rows of U as constituting a generator matrix G; delete the corresponding columns of V to form the matrix H^{T} and then H is the check matrix of the code.

This method has been exploited in a number of ways to construct various types of error-correcting codes and to deduce properties of such code from the method of construction.

What is your favourite unit? Construct codes from it using this method of unit derived codes. How many codes of the form $(101, 50)$ could one get when U, V have size (101×101)? *Unitary* or *paraunitary* matrices are particularly nice and may be used to form self-dual or dual-containing codes, [25].

This unit-derived method for codes can be formed from units in *any* system. For example if one has $U(z)V(z) = I$ in a polynomial ring then from this *convolutional codes* may be formed. Correspondingly

units of group rings of group rings over infinite cyclic groups may be used to construct convolutional codes, [22, 24, 40, 41, 42].

Using units in group ring with $uv = 1$ where the *support* of v is small may be used to form *Low Density Parity Check (LDPC)* codes, [22, 30]. (Support = number of non-zero coefficients in the expression as a group ring element.)

Properties of the codes may be deduced from properties of the group rings. See Section 6 for further coding theory based on properties of group rings and related structures.

3. **The ubiquitous Fourier matrix; circulants**

The entries of the Fourier matrix are powers of primitive n^{th} roots of unity. In general the $n \times n$ Fourier matrix F_n is the matrix whose (i, j) entry is ω^{ij} for $0 \leq i, j \leq (n-1)$ where ω is a primitive n^{th} root of unity. Suppose the field K has a primitive n^{th} root of 1 and in this case n has an inverse in K. The Fourier $n \times n$ matrix F_n over K is defined as follows:

$$F_n = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{(n-1)} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \dots & \alpha^{(n-1)(n-1)} \end{pmatrix}.$$

The inverse of F_n is

$$F_n^* = \frac{1}{n} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha^{-1} & \alpha^{-2} & \dots & \alpha^{-(n-1)} \\ 1 & \alpha^{-2} & \alpha^{-4} & \dots & \alpha^{-2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{-(n-1)} & \alpha^{-2(n-1)} & \dots & \alpha^{-(n-1)(n-1)} \end{pmatrix}.$$

(α^{-1} is a primitive n^{th} root of 1 also and the matrix nF_n^* may also be considered a Fourier matrix over K.)

When $\frac{1}{\sqrt{n}}$ exists in K then F_n may be replaced by $\frac{1}{\sqrt{n}}F_n$ to obtain a unitary matrix. The Fourier matrix has numerous applications in communications. The applications work essentially because the Fourier matrix diagonalises any *circulant* matrix; the diagonalising matrix (the Fourier matrix) is *independent* of the entries of the circulant.

The input to the Discrete or finite Fourier Transform (DFT) is a finite sequence of numbers and this makes the DFT ideal for processing information stored in computers. The DFT is used widely in *signal processing and related fields* so as to analyse frequencies in a sampled signal, to *solve partial differential equations*, and is used to perform other operations such as *convolutions or multiplying large integers* and in *data compression*. The DFT can be performed efficiently using a fast Fourier transform (FFT) algorithm.

3.1. **Cyclic group ring, circulant matrix.**

But note that the ring of circulant $n \times n$ matrices over R is isomorphic to the group ring RC_n of the cyclic group C_n over R. *Convolution* of vectors used extensively in the communications' areas, is the same as the *multiplication* of group ring elements in the cyclic group ring.

An excellent survey article 'On Circulant Matrices' by Kra and Simanca appeared in Notices of the AMS, March 2012 [35]. It commences: 'Some mathematical topics – circulant matrices, in particular – are pure gems that cry out to be admired and studied with different techniques or perspectives

in mind.' A number of monographs on Circulant Matrices have appeared over the years, beginning, perhaps, with Philip Davis' monograph in 1979; this was reproduced and expanded in AMS monograph 1994 [10]. Seemingly circulant matrices first appeared, as examples, in a 1846 paper by Catalan.

Other types of matrices are determined by their first row or column and these include *group ring matrices* [23] and see section 3.2 below. Circulant matrices are special cases of group ring matrices. Group ring matrices obtained from (finitely generated) abelian groups correspond to *multidimensional Fourier Transforms*.

3.2. **Group ring matrices.** Suppose now G is a group of order n. An RG-matrix is a matrix corresponding to a group ring element in the isomorphism from the group ring into the ring of $R_{n\times n}$ matrices, see for example [23]. Specifically suppose $w = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$. The RG-matrix of w denoted by $M(RG, w)$ is defined as follows:

$$\begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \dots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \dots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \dots & \alpha_{g_n^{-1}g_n} \end{pmatrix}$$

The matrix is in $R_{n\times n}$ and depends on the listing of the elements. Changing the listing changes the matrix; if A, B are RG-matrices for the element $w \in RG$ relative to different listings then B may be obtained from A by a sequence of [interchanging two rows and then interchanging the corresponding two columns].

Given the entries of the first row of an RG-matrix, and a listing, the entries of the other rows are determined from the multiplication of the elements of G and each row and each column is a permutation of the first row.

Theorem 3.1. *Given a listing of the elements of a group G of order n there is a bijective ring homomorphism between RG and the $n \times n$ RG-matrices. This bijective ring homomorphism is given by $\sigma : w \mapsto M(RG, w)$.*

An RG-matrix for a cyclic group G is a circulant matrix; an RG-matrix when G is a dihedral group is one of the form $\left(\begin{smallmatrix} A & B \\ B & A \end{smallmatrix}\right)$ (in the natural listing of the elements of G), where A is circulant and B is reverse circulant.

The Fourier matrix is very closely related to the representation theory of the cyclic group. Its rows are obtained from the *idempotents*.

A circulant matrix is diagonalisable by the Fourier matrix (of the correct size) *independent of the entries of the circulant*. Of course the circulant is determined by the entries of its first row or first column. Can the Fourier diagonalisation of a circulant matrix be generalised?

Theorem 3.2. *Let A be a $\mathbb{C}G$-matrix. Then there exists a unitary matrix P such that $P^*AP = T$ where T is a block diagonal matrix with blocks of size $r_i \times r_i$, for $i = 1, 2, \dots, k$, along the diagonal and r_i are the sizes of the conjugacy classes of G.*

This is closely related to representation theory and characters. When $G = C_n$, the cyclic group of order n, the matrix P of Theorem 3.2 is the Fourier matrix and T is a diagonal matrix.

For any $w \in RG$ the corresponding capital letter W is used to denote the image of w in the isomorphism of Theorem 3.2.

3.2.1. **Examples with symmetric, dihedral groups.** For details on character theory and representations see [39] or [9]. Let D_{2n} denote the dihedral group of order $2n$. As every element in D_{2n} is conjugate to its inverse, the complex characters of D_{2n} are real. The characters of D_{2n} are contained in an extension of $\mathbb{Q}$ of degree $\phi(n)/2$ and this is $\mathbb{Q}$ only for $2n \leq 6$.

Let S_n denote the symmetric group of order n. Representations and orthogonal idempotents of the symmetric group are known; see for example [9]. The characters of S_n are rational.

The dihedral group D_{2n} is generated by elements a and b with presentation:

$\langle a, b \mid a^n = 1,\ b^2 = 1,\ bab = a^{-1} \rangle$.

It has order $2n$, with elements $\{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$.

By Theorem 3.2 given A, a group ring matrix in $\mathbb{C}D_{2n}$, there is a real unitary matrix P (independent of the entries of A) such that:

$P^{\mathrm{T}}AP = \mathrm{diag}(d_1, d_2, T_1, T_2, \ldots, T_k)$ when n is odd,

$P^{\mathrm{T}}AP = \mathrm{diag}(d_1, d_2, d_3, d_4, T_1, T_2, \ldots, T_k)$ when n is even

where d_j are scalars and T_i are 4×4 matrices.

In this case note that P is real orthogonal so that $P^* = P^{\mathrm{T}}$.

In particular consider $D_6 = S_3$. The conjugacy classes are $\{1\}, \{a, a^2\}, \{b, ab, ab^2\}$. The idempotents are then $e_0 = 1/6(1 + a + a^2 + b + ba + ba^2), e_1 = 1/6(1 + a + a^2 - b - ba - ba^2), e_3 = 1/3(2 - a - a^2)$.

From these an orthonormal basis for $\mathbb{C}_{6\times 6}$ may be constructed:

$v_1 = \sqrt{\frac{1}{6}}(1,1,1,1,1,1), v_2 = \sqrt{\frac{1}{6}}(1,1,1,-1,-1,-1)^{\mathrm{T}}, v_3 = \sqrt{\frac{1}{6}}(2,-1,-1,0,0,0)^{\mathrm{T}},$

$v_4 = \sqrt{\frac{1}{2}}(0,1,-1,0,0,0)^{\mathrm{T}}, v_5 = \sqrt{\frac{1}{6}}(0,0,0,2,-1,-1)^{\mathrm{T}}, v_6 = \sqrt{\frac{1}{2}}(0,0,0,0,1,-1)^{\mathrm{T}}.$

Construct the orthogonal matrix $P = (v_1, v_2, v_3, v_4, v_5, v_6)$. Then for any $\mathbb{C}D_6$-matrix A it follows that $P^{\mathrm{T}}AP = \mathrm{diag}(a, b, D)$ where D is a 4×4 matrix.

Consider D_{10}.

This has conjugacy classes $\{1\}, \{b, ba, ba^2, ba^3, ba^4\}, \{a, a^4\}, \{a^2, a^3\}$ and character table:

$$\left(\begin{array}{cccc} 1 & b & a & a^2 \\ 1 & 5 & 2 & 2 \\ \hline 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 2 & 0 & 2\cos(2\pi/5) & 2\cos(4\pi/5) \\ 2 & 0 & 2\cos(4\pi/5) & 2\cos(8\pi/5) \end{array}\right).$$

This gives the following idempotents: $e_0 = 1 + a + a^2 + a^3 + a^4 + b + ba + ba^2 + ba^3 + ba^4, e_1 = 1 + a^2 + a^3 + a^4 - b - ba - ba^2 - ba^3 - ba^4, e_2 = 2(1 + \cos(2\pi/5)a + \cos(4\pi/5)a^2 + \cos(4\pi/5)a^3 + 2\cos(2\pi/5)a^4), e_3 = 2(1 + \cos(4\pi/5)a + \cos(8\pi/5)a^2 + \cos(8\pi/5)a^3 + \cos(4\pi/5)a^4$.

Each of $\{E_0, E_1\}$ has rank 1 and each of $\{E_2, E_3\}$ has rank 4. One normalised column from each of $\{E_0, E_1\}$ and four orthonormal (independent) columns from each of $\{E_2, E_3\}$ are easy to obtain and the matrix formed from these performs the task of P in Theorem 3.2 for any $\mathbb{C}D_{10}$-matrix.

Generalisation to D_{2n} are possible using its character tables which are known.

4. **Filters: Idempotent systems for paraunitary matrices**

Complete orthogonal sets of idempotents turn out useful for constructions in the communications' areas; constructions already in use are often seen to be special cases of constructions with orthogonal sets of idempotents.

Let R be a ring with identity $1_R = 1$. A *complete family of orthogonal idempotents* is a set $\{e_1, e_2, \ldots, e_k\}$ in R such that
(i) $e_i \neq 0$ and $e_i^2 = e_i$, $1 \leq i \leq k$;
(ii) If $i \neq j$ then $e_i e_j = 0$;
(iii) $1 = e_1 + e_2 + \ldots + e_k$.

The idempotent e_i is said to be *primitive* if it cannot be written as $e_i = e_i^{'} + e_i^{''}$ where $e_i^{'}, e_i^{''}$ are idempotents such that $e_i^{'}, e_i^{''} \neq 0$ and $e_i^{'} e_i^{''} = 0$. A set of idempotents is said to be *primitive* if each idempotent in the set is primitive.

A mapping $^* : R \to R$ in which $r \mapsto r^*, (r \in R)$ is said to be an *involution* on R if and only if (i) $r^{**} = r$, $\forall r \in R$, (ii) $(a+b)^* = a^* + b^*$, $\forall a, b \in R$, and (iii) $(ab)^* = b^* a^*$, $\forall a, b \in R$.

Of particular interest is the case where * denotes complex conjugate transpose in the case of matrices over $\mathbb{C}$ and denotes transpose for matrices over other fields.

An element $r \in R$ is said to be *symmetric* (relative to *) if $r^* = r$ and a set of elements is said to be symmetric if each element in the set is symmetric.

Complete orthogonal sets of idempotents arise naturally with group rings; indeed in these cases the idempotents are *symmetric*. For example a set of primitive orthogonal idempotents of $C_2 \times C_2$ consists of $f_1 = \frac{1}{4}(1+a+b+ab), f_2 = \frac{1}{4}(1-a+b-ab), f_3 = \frac{1}{4}(1-a-b+ab), f_4 = \frac{1}{4}(1+a-b-ab)$. These then give corresponding matrix complete orthogonal set of idempotents of the form $\left(\begin{smallmatrix} A & B \\ B & A \end{smallmatrix}\right)$ where A, B are 2×2 matrices, [23], as for example $F_3 = \frac{1}{4}\begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$ which corresponds with f_3.

Complete orthogonal sets of idempotents may also be constructed from orthonormal bases and similar structures. For example $\{v_1 = 1/3(2,1,2), v_2 = 1/3(1,2,-2), v_3 = 1/3(-2,2,1)\}$ is an orthonormal basis for $\mathbb{Q}_3$. Then define $P_1 = {v_1}^{\mathrm{T}} v_1 = \frac{1}{9}\begin{pmatrix} 4 & 2 & 4 \\ 2 & 1 & 2 \\ 4 & 2 & 4 \end{pmatrix}, P_2 = {v_2}^{\mathrm{T}} v_2 = \frac{1}{9}\begin{pmatrix} 1 & 2 & -2 \\ 2 & 4 & -4 \\ -2 & -4 & 4 \end{pmatrix}, P_3 = {v_3}^{\mathrm{T}} v_3 = \frac{1}{9}\begin{pmatrix} 4 & -4 & -2 \\ -4 & 4 & 2 \\ -2 & 2 & 1 \end{pmatrix}$. Now $\{P_1, P_2, P_3\}$ is a complete symmetric orthogonal set of idempotents; each P_i has rank 1. $\{(P_1 + P_2), P_3\}$ is also a complete symmetric set of orthogonal idempotents where $(P_1 + P_2)$ has rank 2. Another set in $\mathbb{C}_{2\times 2}$ is: $\{\frac{1}{2}\left(\begin{smallmatrix} 1 & -i \\ i & 1 \end{smallmatrix}\right), \frac{1}{2}\left(\begin{smallmatrix} 1 & i \\ -i & 1 \end{smallmatrix}\right)\}$.

4.1. **Rank of sum of idempotents.**

Wouldn't it be nice if $(a+b)^2 = a^2 + b^2$?! Sometimes it is and structures over fields of characteristic 2 are extremely useful and nice. Wouldn't it be nice if $\mathrm{rank}(A+B) = \mathrm{rank}\, A + \mathrm{rank}\, B$? Sometimes it is and cases where it's true turn out to produce useful constructions. A corollary of the following shows that such a rank result holds for orthogonal idempotents; a proof may be found in [2].

Theorem 4.1. *Let I be an idempotent matrix. Then* $\mathrm{rank}\, I = tr(I)$*, the trace of I.*

Corollary 4.2. *Suppose A, B are orthogonal idempotents. Then* $\mathrm{rank}(A+B) = \mathrm{rank}\, A + \mathrm{rank}\, B$.

The rank of a sum of elements within an orthogonal set of idempotents is then immediate. Let $\{E_1, E_2, \ldots, E_k\}$ be a complete symmetric orthogonal set of idempotents in $F_{n\times n}$ and $\operatorname{rank} E_i = r_i$. In particular $\sum_{i=1}^{k} r_i = n$. Let $G = (E_1 + E_2 + \ldots + E_s)$ with $s < k$ and $H = E_{s+1} + \ldots + E_k$. Then Theorem 4.1 allows us to deduce:

Corollary 4.3. $\operatorname{rank} G = (r_1 + r_2 + \ldots + r_s) = r,\ \operatorname{rank} H = (r_{s+1} + r_{s+2} + \ldots + r_k) = (n - \operatorname{rank} G) = (n - r)$.

In addition it is noted that $GH = 0$.

4.2. **Paraunitary matrices.** A unitary matrix is a matrix U satisfying $UU^* = 1$. Here U^* means complex conjugate transposed for $\mathbb{C}$, the complex numbers, and $U^* = U^{\mathrm{T}}$ for other fields. Over $\mathbb{R}$ a unitary matrix is usually referred to as an orthogonal matrix. The nicest such examples are perhaps the normalised Fourier matrices.

A one-dimensional (1D) *paraunitary matrix* is a polynomial matrix $U(z)$ in the variable z such that $U(z)U^*(z^{-1}) = 1$. A k-dimensional (kD) paraunitary matrix is a polynomial matrix $U(\mathbf{z})$ in the (commuting) variables $\mathbf{z} = (z_1, z_2, \ldots, z_k)$ such that $U(\mathbf{z})U^*(\mathbf{z}^{-1}) = 1$ where $\mathbf{z}^{-1} = (z_1^{-1}, z_2^{-1}, \ldots, z_k^{-1})$.

Paraunitary matrices are important in signal processing; more specifically: '..in the research area of multirate filterbanks, wavelets and multiwavelets, the concept of a paraunitary matrix plays a fundamental role'. Essentially each filterbank determines a paraunitary matrix and each paraunitary matrix determines a filterbank. Strang + Nguyen's book on 'Wavelets and filterbanks' [46] gives the necessary background. The polyphase matrix is paraunitary if and only if the wavelet is orthonormal – see for example [45]. The current standard for image compression, JPEG2000, is wavelet based.

A product of paraunitary matrices is a paraunitary matrix. Engineering Problem: How are such matrices constructed? In other words, what are the building blocks for paraunitary matrices? Answer: The building blocks for such 1D paraunitary matrices are *orthogonal sets of idempotents.*

Lemma 4.4. *Suppose* $\{E_1, E_2, \ldots, E_k\}$ *is a complete orthogonal set of idempotents. Define* $U(z) = \sum_{i=0}^{k} \alpha_i E_i z^{t_i}$ *with* $t_i \geq 0$ *and* $|\alpha_i| = 1$. *Then* $U(z)U^*(z^{-1}) = 1$.

In $\mathbb{C}$ that $|\alpha| = 1$ means the modulus of α is 1 and for other fields it is taken that $|\alpha_i| = 1$ means $\alpha_i = \pm 1$.

To construct paraunitary matrices by this method, it is only necessary to find complete symmetric sets of orthogonal idempotents. Then take a sum of these with coefficients of modulus 1. The great factorisation theorem due to Belevitch and Vaidyanathan, see [50] for details, may be interpreted as follows:

Theorem 4.5. *1D paraunitary matrices are all produced in this manner.*

Thus any paraunitary 1D matrix is a product of paraunitary matrices each of which is a sum with coefficients of modulus 1 of a complete symmetric orthogonal set of idempotents. The interpretation of the factorisation theorem in this form may be found in [26].

4.3. **Multidimensional.** General methods for the construction of multidimensional paraunitary matrices are hard to come by due to the absence of theorems like 4.5. What is required though here are *non-separable* multidimensional such matrices. A paraunitary matrix is non-separable essentially means that it cannot be broken down as a (non-trivial) product of one dimensional paraunitary matrices nor as a tensor product of such. An abstract algebra method for constructing non-separable multidimensional paraunitary matrices is as follows.

4.3.1. **Non-separable constructions.**

A general construction: The main reference here is [26].

Proposition 4.6. *Let A, B be paraunitary matrices of the same size over a field in which 2 has a square root. Then $W = \frac{1}{\sqrt{2}}\begin{pmatrix} A & B \\ A & -B \end{pmatrix}$ and $Q = \frac{1}{\sqrt{2}}\begin{pmatrix} A & A \\ B & -B \end{pmatrix}$ is a paraunitary matrix in the union of the variables in $\{A, B\}$.*

Proof. Suppose A, B are $n \times n$ matrices. Then

$$\begin{aligned} WW^* &= \frac{1}{2}\left(\begin{smallmatrix} A & B \\ A & -B \end{smallmatrix}\right)\left(\begin{smallmatrix} A^* & A^* \\ B^* & -B^* \end{smallmatrix}\right) \\ &= \frac{1}{2}\left(\begin{smallmatrix} AA^*+BB^* & AA^*-BB^* \\ AA^*-BB^* & AA^*+BB^* \end{smallmatrix}\right) \\ &= \frac{1}{2}\left(\begin{smallmatrix} I_n+I_n & I_n-I_n \\ I_n-I_n & I_n+I_n \end{smallmatrix}\right) = I_{2n} \end{aligned}$$

Similarly it may be shown that Q is a paraunitary matrix; this also follows from the fact that Q is the transpose of $\frac{1}{\sqrt{2}}\begin{pmatrix} A^{\mathrm{T}} & B^{\mathrm{T}} \\ A^{\mathrm{T}} & -B^{\mathrm{T}} \end{pmatrix}$ and $A^{\mathrm{T}}, B^{\mathrm{T}}$ are paraunitary. □

The variables in A need not be the same as the variables in B. Proposition 4.6 enables the construction of non-separable multidimensional paraunitary matrices. Paraunitary matrices constructed by this or other methods may be used as input to Proposition 4.6 to construct further multidimensional non-separable paraunitary matrices.

The methods are fairly general and it is easy to produce examples for input using various complete orthogonal sets of idempotents. The result holds in general over any field which contains the square root of 2.

If $A = B$ then W in Proposition 4.6 is the tensor product $A \otimes J$ where $J = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. If A and B are formed using the *same* complete symmetric orthogonal set of idempotents as in section 4.2 then W can be shown to be separable.

If $W = \begin{pmatrix} X & Y \\ Z & T \end{pmatrix}$ where X, Y, Z, T are matrices of the same size then $\{X, Y, Z, T\}$ are referred to as the *blocks* of W and $\begin{pmatrix} X & Y \end{pmatrix}$ and $\begin{pmatrix} Z & T \end{pmatrix}$ are the *row blocks* of W. Similarly *column blocks* of W are defined.

Suppose A, B are matrices of the same size. Then a *tangle* of $\{A, B\}$ is one of

(1) $W = \frac{1}{\sqrt{2}} \begin{pmatrix} A & B \\ A & -B \end{pmatrix}$.

(2) A matrix obtained from 1. by interchanging rows of blocks and/or columns of blocks.

(3) The transpose of any matrix obtained in 1. or 2.

A tangle of $\{A, B\}$ is not the same as, and is not necessarily equivalent to, a tangle of $\{B, A\}$. Note that interchanging any rows and/or columns of a paraunitary matrix results in an (equivalent) paraunitary matrix. Thus in particular interchanging rows and/or columns of blocks also results in equivalent paraunitary matrices; hence item 2. gives equivalent paraunitary matrices to item 1. The negative of a paraunitary matrix is a paraunitary matrix as is the * of a paraunitary matrix.

For example
$\frac{1}{\sqrt{2}} \left(\begin{smallmatrix} A & B \\ A & -B \end{smallmatrix}\right), \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} A & -B \\ A & B \end{smallmatrix}\right), \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} A & A \\ B & -B \end{smallmatrix}\right)$ are tangles of $\{A, B\}$
and
$\frac{1}{\sqrt{2}} \left(\begin{smallmatrix} B & A \\ B & -A \end{smallmatrix}\right), \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} B & -A \\ B & A \end{smallmatrix}\right), \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} B & B \\ A & -A \end{smallmatrix}\right)$ are tangles of $\{B, A\}$.

Proposition 4.6 may be generalised as follows.

Proposition 4.7. *Let A, B be paraunitary matrices of the same size but not necessarily with the same variables. Then a tangle of $\{A, B\}$ or $\{B, A\}$ is a paraunitary matrix.*

4.3.2. **Examples.**

(1) (a) Construct $A = (x)$ and $B = (y)$.
(b) Construct $W = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} A & B \\ A & -B \end{smallmatrix}\right) = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} x & y \\ x & -y \end{smallmatrix}\right)$. Then W is a paraunitary matrix.
(c) Similarly construct $Q = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} z & t \\ z & -t \end{smallmatrix}\right)$.
(d) Form a tangle of W and Q to produce for example the paraunitary matrix $T = \frac{1}{2} \begin{pmatrix} x & y & z & t \\ x & -y & z & -t \\ x & y & -z & -t \\ x & -y & -z & y \end{pmatrix}$.
(e) The process can be continued: Matrices produced from (d), with different variables, can be input to form further paraunitary matrices.

(2) (a) Construct the following complete symmetric sets of idempotents in 3×3 matrices over $\mathbb{F}_7$:
$\{P_0 = \left(\begin{smallmatrix} 2 & 1 & 2 \\ 1 & 4 & 1 \\ 2 & 1 & 2 \end{smallmatrix}\right), P_1 = \left(\begin{smallmatrix} 4 & 1 & 6 \\ 1 & 2 & 5 \\ 6 & 5 & 2 \end{smallmatrix}\right), P_2 \left(\begin{smallmatrix} 2 & 5 & 6 \\ 5 & 2 & 1 \\ 6 & 1 & 4 \end{smallmatrix}\right)\}$, $\{Q_0 = \left(\begin{smallmatrix} 6 & 5 & 6 \\ 5 & 3 & 5 \\ 6 & 5 & 6 \end{smallmatrix}\right), Q_1 = \left(\begin{smallmatrix} 5 & 2 & 5 \\ 2 & 5 & 2 \\ 5 & 2 & 5 \end{smallmatrix}\right), Q_2 = \left(\begin{smallmatrix} 4 & 0 & 3 \\ 0 & 0 & 0 \\ 3 & 0 & 4 \end{smallmatrix}\right)\}$.
(b) Form $A = xP_0 + yP_1 + zP_2, B = tQ_0 + rQ_1 + sQ_2$.
(c) Tangle A, B to form for example the following paraunitary matrix over $\mathbb{F}_7$: $\frac{1}{\sqrt{2}} \left(\begin{smallmatrix} A & A \\ -B & B \end{smallmatrix}\right) = 5 \left(\begin{smallmatrix} A & A \\ -B & B \end{smallmatrix}\right)$.

(3) (a) Construct, in $\mathbb{C}_{2\times 2}$, the following complete symmetric (different) sets of orthogonal idempotents $\{E_0, E_1\}$ and $\{Q_0, Q_1\}$ where:
$E_0 = \frac{1}{2} \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right), E_1 = \frac{1}{2} \left(\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix}\right)$. $\quad Q_0 = \frac{1}{5} \left(\begin{smallmatrix} 4 & 2 \\ 2 & 1 \end{smallmatrix}\right), Q_1 = \frac{1}{5} \left(\begin{smallmatrix} 1 & -2 \\ -2 & 4 \end{smallmatrix}\right)$.
(b) Construct $A = xE_0 + yE_1, B = zQ_0 + tQ_1$.
(c) Construct $W = \frac{1}{\sqrt{2}} \begin{pmatrix} A & B \\ A & -B \end{pmatrix}$. Then W is a paraunitary matrix of size 4×4 with variables $\{x, y, z, t\}$.

(4) The following is a paraunitary matrix:

$$\frac{1}{2\sqrt{2}}\begin{pmatrix} x & x & y & -y & u & -iu & v & iv \\ x & x & -y & y & iu & u & -iv & v \\ r & -r & p & p & z & iz & t & -it \\ -r & r & p & p & -iz & z & it & t \\ x & x & y & -y & -u & iu & -v & -iv \\ x & x & -y & y & -iu & -u & iv & -v \\ r & -r & p & p & -z & -iz & -v & iv \\ -r & r & p & p & iz & -z & -iz & z \end{pmatrix}.$$

(5) By giving values of modulus 1 to the variables, complex Hadamard matrices are obtained. For example letting all the variables have the value +1 gives the following complex Hadamard matrix:

$$\begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -i & 1 & i \\ 1 & 1 & -1 & 1 & i & 1 & -i & 1 \\ 1 & -1 & 1 & 1 & 1 & i & 1 & -i \\ -1 & 1 & 1 & 1 & -i & 1 & i & 1 \\ 1 & 1 & 1 & -1 & -1 & i & -1 & -i \\ 1 & 1 & -1 & 1 & -i & -1 & i & -1 \\ 1 & -1 & 1 & 1 & -1 & -i & -1 & i \\ -1 & 1 & 1 & 1 & i & -1 & -i & 1 \end{pmatrix}.$$

A complex Hadamard matrix is a matrix H of size $n \times n$ with entries of modulus 1 and satisfying $HH^* = nI_n$. Complex Hadamard matrices arise in the study of operator algebras and the theory of quantum computation.

By giving values which are k^{th} of unity to the variables, with k divisible by 4, in the above example 4, special types of complex Hadamard matrices which are called *Butson-type* are obtained. A Butson type Hadamard $H(q, n)$ matrix is a complex Hadamard matrix of size $n \times n$ all of whose entries are q^{th} roots of unity.

Question. Algorithms using the above constructions may then be set up with which to form non-separable multidimensional paraunitary matrices. These will certainly give required matrices but a question remains of whether these algorithms give all such matrices.

5. **Multiple antenna design**

An excellent survey article by B.A. Sethuraman on multiple antenna design appeared in Notices of the AMS [43]. References in this paper gives further background and theory. The applications occur in communications involving multiple transmitting and multiple receiving antennas known as MIMO which stands for multiple-input-multiple-output. Particular applications are to mobile phone communications.

The design problem for what are called *unitary space time constellations* is nicely set out in [44] and in [12]: 'Let M be the number of transmitter antennas and R the desired transmission rate. Construct a set $\mathcal{V}$ of $L = 2^{RM}$ unitary $M \times M$ matrices such that for any two distinct elements A, B in $\mathcal{V}$, the quantity $|\det(A - B)|$ is as large as possible. Any set $\mathcal{V}$ such that $|\det(A - B)| > 0$ for all distinct A, B is said to have *full diversity.*'

The number of transmitter antennas is the size M of the matrices. The set $\mathcal{V}$ is known as a *constellation.* In [44] also it is explained that the *quality* of the constellation is measured by

$$\zeta_{\mathcal{V}} = \frac{1}{2} \min_{V_l, V_m \in \mathcal{V}, V_l \neq V_m} |\det(V_l - V_m)|^{\frac{1}{M}}$$

The paper [43] suggests using Division Algebras for such design. Sticking with our themes we present general methods for constructing such constellations of unitary matrices from complete orthogonal sets

of idempotents and tangles of matrices. This enables the construction of constellations as required and the quality may then be algebraically determined. Examples are given showing that good quality constellations can be obtained by this approach.

5.1. **Unitary.** Why are complete orthogonal sets of idempotents a good way for looking at constellations of unitary matrices? Unitary matrices over $\mathbb{C}$ are built from complete symmetric orthogonal sets of matrices as follows:

Proposition 5.1. *U is a unitary $n\times n$ matrix over $\mathbb{C}$ if and only if $U=\alpha_1v_1^*v_1+\alpha_2v_2^*v_1+\ldots+\alpha_nv_n^*v_n$ where $\{v_1^*v_1,v_2^*v_2,\ldots,v_n^*v_n\}$ is a complete symmetric orthogonal set of idempotents in $\mathbb{C}_{n\times n}$ and $\alpha_i\in\mathbb{C}$, $|\alpha_i|=1$, $\forall i$. Further the α_i are the eigenvalues of U.*

Proof. Suppose $U=\alpha_1v_1^*v_1+\alpha_2v_2^*v_1+\ldots+\alpha_nv_n^*v_n$ where $\{v_1^*v_1,v_2^*v_2,\ldots,v_n^*v_n\}$ a complete orthogonal set of idempotents and $|\alpha_i|=1$. It is easy to check that $UU^*=1$. Then $Uv_i^*=\alpha_iv_i^*$ and so the α_i are the eigenvalues of U.

Suppose then U is a unitary matrix. It is known (as in particular U is a normal matrix) that there exists a unitary matrix P such that $U=P^*DP$ where D is diagonal. The entries of D must have modulus 1. Then P has the form $P=\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}$ where $\{v_1,v_2,\ldots,v_n\}$ is an orthonormal basis (of row vectors) for $\mathbb{C}_n$ and $D=\mathrm{diag}(\alpha_1,\alpha_2,\ldots,\alpha_n)$ with $|\alpha_i|=1$ and the α_i are the eigenvalues of U. Then

$$\begin{aligned}U=P^*DP&\\&=(v_1^*,v_2^*,\ldots,v_n^*)\begin{pmatrix}\alpha_1&0&\ldots&0\\0&\alpha_2&\ldots&0\\\vdots&\vdots&\vdots&\vdots\\0&0&\ldots&\alpha_n\end{pmatrix}\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}\\&=(\alpha_1v_1^*,\alpha_2v_2^*,\ldots,\alpha_nv_n^*)\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}\\&=\alpha_1v_1^*v_1+\alpha_2v_2^*v_2+\ldots+\alpha_nv_n^*v_n.\end{aligned}$$

□

Thus unitary matrices are generated by complete symmetric orthogonal sets of idempotents formed from the diagonalising unitary matrix. Notice that the α_i are the eigenvalues of U.

Construction methods for complete symmetric orthogonal systems of idempotents are known; see for example [26]. The methods use essentially (a) orthogonal projections; (b) group rings. These are reviewed briefly here for completeness.

5.1.1. **Example.** For example consider the real orthogonal/unitary matrix $U=\left(\begin{smallmatrix}\cos\theta&\sin\theta\\-\sin\theta&\cos\theta\end{smallmatrix}\right)$. This has eigenvalues $e^{i\theta},e^{-i\theta}$ and $P=\frac{1}{\sqrt{2}}\left(\begin{smallmatrix}-1&-i\\i&1\end{smallmatrix}\right)$ is a diagonalising unitary matrix. Take the rows $v_1=\frac{1}{\sqrt{2}}(-1,-i)$, $v_2=\frac{1}{\sqrt{2}}(i,1)$ of P and consider the complete orthogonal symmetric set of idempotents $\{P_1=v_1^*v_1=\frac{1}{2}\left(\begin{smallmatrix}1&-i\\i&1\end{smallmatrix}\right),P_2=v_2^*v_2=\frac{1}{2}\left(\begin{smallmatrix}1&i\\-i&1\end{smallmatrix}\right)\}$.

Then applying Proposition 5.1 gives $U=e^{i\theta}P_1+e^{-i\theta}P_2=\frac{1}{2}e^{i\theta}\left(\begin{smallmatrix}1&-i\\i&1\end{smallmatrix}\right)+\frac{1}{2}e^{-i\theta}\left(\begin{smallmatrix}1&i\\-i&1\end{smallmatrix}\right)$, which may be checked independently.

Now $\{v_1 = \frac{1}{3}(2,1,2), v_2 = \frac{1}{3}(1,2,-2), v_3 = \frac{1}{3}(2,-2,-1)\}$ is an orthonormal basis for $\mathbb{R}^3$. The projection matrices are respectively $P_1 = {v_1}^{\mathrm{T}}v_1 = \frac{1}{9}\begin{pmatrix} 4 & 2 & 4 \\ 2 & 1 & 2 \\ 4 & 2 & 4 \end{pmatrix}, P_2 = {v_2}^{\mathrm{T}}v_2 = \frac{1}{9}\begin{pmatrix} 1 & 2 & -2 \\ 2 & 4 & -4 \\ -2 & -4 & 4 \end{pmatrix}, P_3 = {v_3}^{\mathrm{T}}v_3 = \frac{1}{9}\begin{pmatrix} 4 & -4 & -2 \\ -4 & 4 & 2 \\ -2 & 2 & 1 \end{pmatrix}$.

Then $\{P_1, P_2, P_3\}$ is a complete symmetric orthogonal set of idempotents and each P_i has rank 1. Let $\hat{P}_2 = P_2 + P_3$ and then $\{P_1, \hat{P}_2\}$ is a complete symmetric orthogonal set of idempotents also with $\mathrm{rank}(\hat{P}_2) = 2$.

5.1.2. **Idempotents from unitary matrices.** Let U be a unitary $n \times n$ matrix. The rows $\{v_1, v_2, \ldots, v_n\}$ of U satisfy $v_i v_i^* = 1$, $v_i v_j^* = 0$, $i \neq j$.

Define $P_i = v_i^* v_i$ for $i = 1, 2, \ldots, n$. Then each P_i is an $n \times n$ matrix of rank 1 and $\{P_1, P_2, \ldots, P_n\}$ is a complete symmetric orthogonal set of idempotents.

Group rings are a rich source of complete sets of orthogonal idempotents and this enriches the families of structured unitary matrices available for applications and properties. See [26] for the construction of unitary matrices using group rings. Orthogonal sets of idempotents in group rings brings comes into the realm of *character theory* in group rings. The orthogonal idempotents are obtained from the conjugacy classes and character tables of the group ring, see e.g. [39, 9] for details. The families depend on the field used; for unitary matrices the required field is usually $\mathbb{C}$. Such sets over the rationals are also easily obtainable by these methods. There are many papers in the literature on the construction of character tables of groups.

The following result is useful for determining the quality of constellations constructed by the methods of idempotents. The proof may be found in [26].

Theorem 5.2. *Suppose $\{E_1, E_2, \ldots, E_k\}$ is a complete symmetric orthogonal set of idempotents in $F_{n\times n}$. Let $A = a_1E_1 + a_2E_2 + \ldots + a_kE_k$. Then the determinant of A is $|A| = a_1^{\mathrm{rank}\, E_1} a_2^{\mathrm{rank}\, E_2} \ldots a_k^{\mathrm{rank}\, E_k}$.*

Tangle of matrices as introduced in section 4.3.1 may also be used to design constellations. The determinants of differences of tangles may be determined as follows:

Proposition 5.3. *Let $W = \frac{1}{\sqrt{2}}\begin{pmatrix} A & B \\ A & -B \end{pmatrix}$. Then $\det(W) = \det(A)\det(B)$.*

Constellations may then be constructed from idempotents and tangles of matrices and Theorem 5.2 and Proposition 5.3 may then be used to work out their qualities algebraically.

6. **Further Coding theory**

A maximum distance separable code is a code of the form $(n, r, n - r + 1)$ where n is the length, r is the dimension and $d = n - r + 1$ is the distance of the code [4]. These types of codes are used in applications such as satellite communications, high definition TV, compact disc players, DVDs, disk drives, bar codes and elsewhere. Here we consider maximum distance separable codes which are related to the idempotent systems of the cyclic group ring.

6.1. **A nice theorem.** The Fourier matrix has some very nice properties as already noted. Here's another due to

Theorem 6.1. *(Chebotarëv) Let F_p denote the Fourier $p \times p$ matrix where p is a prime. Then the determinant of* any *submatrix of F_p is non-zero.*

A proof of this Chebotarëv theorem may be found in [13] and proofs also appear in the expository paper of P. Stevenhagen and H. W. Lenstra [47]; paper [14] contains a relatively short proof. There are several other proofs in the literature some of which are referred to in [47]. A proof of the Theorem is also contained in [17] and this paper contains many nice related results, and results related to fields in general including if and only if theorems for cases other than $\mathbb{C}$. Paper [48] contains a proof of Chebotarëv's theorem and refers to it as 'an uncertainty principle'.

6.2. **MDS Codes.** In general say a matrix has the Chebotarëv property if the determinant of any submatrix is non-zero. Thus the Fourier $p \times p$ matrix over $\mathbb{C}$ has the Chebotarëv property.

Suppose then A is an $n \times n$ matrix over a field K which has this Chebotarëv property. Then by the method of unit-derived codes as in [23] any r rows of A may be used to form and (n, r) code and the other corresponding $(n - r)$ columns of A give a check matrix H. On account of the Chebotarëv property the distance of this code is then $(n - r + 1)$ which is best possible as any $(n - r) \times (n - r)$ submatrix of B has non-zero determinant, see [4], Theorem 3.2.2.

6.3. **Finite field.** The Fourier matrix F_p can be defined over a finite field provided the field has a primitive p^{th} root of unity; in this case the characteristic of the field does not divide p. Suppose all that is done.

It's not true in general that the determinants of submatrices of the $p \times p$ Fourier matrix over a finite field (when p is prime) are non-zero. However as pointed out by Isaacs et al. (2005) there are very few fields for which this does not hold. (They give necessary and sufficient conditions.) Maximum distance separable codes, and 'lots' of them, can then be constructed using $p \times p$ matrices for which the Chebotarëv property holds. The constructions also lead to efficient decoding methods. See [28] for details and examples.

6.3.1. **Examples.** The Fourier F_5 over $GF(11)$ has the Chebotarëv property. From this mds codes many be constructed. Here 2 is a primitive root and so $2^2 = 4$ has order 5. Thus then

$$F_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 4^2 & 4^3 & 4^4 \\ 1 & 4^2 & 4^4 & 4 & 4^3 \\ 1 & 4^3 & 4 & 4^4 & 4^2 \\ 1 & 4^4 & 4^3 & 4^2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 5 & 9 & 3 \\ 1 & 5 & 3 & 4 & 9 \\ 1 & 9 & 4 & 3 & 5 \\ 1 & 3 & 9 & 5 & 4 \end{pmatrix}$$

is a Fourier matrix over $GF(11)$ which has the Chebotarëv property. This gives for example $\binom{5}{3} = 10$ mds codes $(5, 3, 3)$ over $\mathbf{Z}_{11}$ which are 1-error correcting.

The Fourier matrix F_{11} exists over $GF(23)$ and satisfies the Chebotarëv condition. In $GF(23)$ a primitive element is 5 and so $5^2 = 2$ is an element of order 11 from which the Fourier matrix F_{11} over $GF(23)$ can be constructed. This gives

$$F_{11} = \begin{pmatrix} 1 & 1 & 1 & ... & 1 \\ 1 & 2 & 2^2 & ... & 2^{10} \\ 1 & 2^2 & 2^4 & ... & 2^{20} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 2^{10} & 2^{20} & ... & 2^{100} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & ... & 1 \\ 1 & 2 & 4 & ... & 12 \\ 1 & 4 & 14 & ... & 6 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 12 & 6 & ... & 2 \end{pmatrix}.$$

From this mds codes over $GF(23)$ may be constructed.

Let ω be a primitive 7^{th} root of 1 in K. Consider $F_7 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 \\ 1 & \omega^3 & \omega^6 & \omega^2 & \omega^5 & \omega & \omega^4 \\ 1 & \omega^4 & \omega & \omega^5 & \omega^2 & \omega^6 & \omega^3 \\ 1 & \omega^5 & \omega^3 & \omega & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}$.

Let $\mathcal{C}_4$ be the code generated by the following matrix: $A = \begin{pmatrix} 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 \\ 1 & \omega^5 & \omega^3 & \omega & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}$.

A has rank 4. A check matrix for $\mathcal{C}_4$ is $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^4 & \omega & \omega^5 & \omega^2 & \omega^6 & \omega^3 \\ 1 & \omega^3 & \omega^6 & \omega^2 & \omega^5 & \omega & \omega^4 \end{pmatrix}$. This has rank 3.

The code $\mathcal{C}_4$ is a $(7, 4, 4)$ code. Indeed $\binom{7}{4} = 35$ different such codes may be derived from this F_7.

Suppose then we have for example a Fourier matrix say F_{89} over a field and it has this Chebotarëv property. Then any choice of 45 of the rows of F_{89} to form a generator matrix for a $(89, 45)$ code. The other 51 will form the check matrix. Because of the Chebotarëv property, the code has maximum distance possible and so is an $(89, 45, 45)$ code. Each choice gives a different code and 89 choose 45 has the order of 5×10^{25}.

Codes may also be obtained from complete orthogonal sets of idempotents and these also can have nice properties.

Problem. Given a prime p, find the finite fields, and then the smallest finite field, for which the Fourier $p \times p$ matrix exists over this field and satisfies the Chebotarëv condition. Construct maximum distance separable codes from this matrix.

7. **Compressed sensing**

Compressed sensing is a signal processing technique for efficiently acquiring and reconstructing a signal, by finding solutions to underdetermined linear systems. This takes advantage of the signal's sparseness or compressibility in some domain, allowing the entire signal to be determined from relatively few measurements. Applications include MRI (scanning), astronomy, space coding, sensor networks, etc. . See Terence Tao's blog [49] which discusses compressed sensing in a non-technical way by relating it to applications for a *single pixel camera.*

Real world signals, such as sound video, images, can be viewed as as an n-dimensional vector of real numbers where n is large, $n \approx 10^6$. To acquire this signal, inner products of $\underline{x}$ with rows of a measurement matrix A are acquired; $\underline{u} = A\underline{x}$ is measured. The matrix A could be some sort of Fourier matrix.

This leads to the classical problem in underdetermined linear equations as to how many measurements need to be taken in order to recover the original signal $\underline{x}$ either exactly or approximately. This is asking: When can the equation $A\underline{x} = \underline{u}$ be solved?

Of course in general it cannot always be solved. When the $\underline{x}$ is known to have at most s non-zero coefficients, where s is small compared to n, is of particular interest; this is referred to as *compressed sensing* or compressed sampling. The term s-sparse is used in this situation. Intuitively if the signal

is s-sparse then the signal should have just s degrees of freedom and should only need a small number of measurements in order to reconstruct u.

Proposition 7.1. *Suppose that any $2s$ columns of the $m \times n$ matrix A are linearly independent. Then any s-sparse signal can be reconstructed uniquely from $A\underline{x}$.*

The proof is fairly easy:

Proof. Suppose not; then there are two s-sparse signals $\underline{x}_1$ and $\underline{x}_2$ with $A\underline{x}_1 = A\underline{x}_2$ which implies $A(\underline{x}_1 - \underline{x}_2) = 0$. But $\underline{x}_1 - \underline{x}_2$ is $2s$ sparse so there is a linear dependence between $2s$ columns of A; hence $\underline{x}_1 = \underline{x}_2$ □

The above proof of Proposition 7.1 shows how to reconstruct an s-sparse signal from the measurements $\underline{u} = A\underline{x}$: x is the unique sparsest solution to $A\underline{x} = \underline{u}$. A major breakthrough came about with [7] and related papers which showed that l_1-minimisation works extremely well in theory and practice; over 200 papers followed on from this within 6 years.

The condition that any $2s$ columns of A be independent reminds one of Chebotarëv's Theorem 6.1; this may then be a theoretical basis for practical implementation. As already noted this theorem has been proved and reproved a number of times [47, 14, 13, 48] and is sometimes referred to as an *uncertainty principle*. Chebotarëv's theorem concerns the Fourier matrix.

Compressed sensing starts by taking a combination of samples or measurements in a basis different from the basis in which the signal is known to be sparse. Theoretical results showed that the number of these measurments can be relatively small and still contain all the useful information. Results of E. Candés, J. Romberg, T. Tao and D. Donoho are fundamental in this area. Particularly worth noting from our point of view is the use of Chebotarev's result Theorem 6.1 and the fundamental paper [7] of Candés, Romberg and Tao.

Let now n be an integer and $f : \mathbb{Z}_n \to \mathbb{C}$. Then $supp(f)$ is the number of non-zero coefficients of f and $\hat{f}$ denotes the Fourier transform of f. An informal way of thinking of the uncertainty principle is that if a function is non-zero but sparse then its Fourier transform should be non-sparse. This can be formally stated as follows:

Theorem 7.2. *For a non-zero function f, $|supp(f)| \times |supp(\hat{f})| \geq n$.*

A corollary of Chebatorëv's Theorem 6.1 is the following uncertainty principle for cyclic groups of prime order:

Corollary 7.3. *When n is prime and f is not identically zero then $|supp(f)| + |supp(\hat{f}))| \geq n + 1$.*

The paper [17] involving in general groups, rings and modules is the natural mathematical extension of these results.

8. **Cryptographic schemes**

Cryptography is a widely used tool in communications, computer networks and computer security generally. Modern cryptographic techniques can only keep their keys secret provided certain mathematical problems, such as integer factorization or discrete logarithms, are intractable and hence there are deep connections with abstract algebra techniques. Volumes of research continues to appear on symmetric cryptography and asymmetric (public key) cryptography. The best known public key cryptosystems include RSA and elliptic curve cryptography (ECC). Diffie-Hellman key exchange [11] and variations are used frequently for exchanging (symmetric) keys over an insecure network. A basic reference is [34] or [33] and much information is also available on the internet.

System designers must consider probable future developments when working with their designs. It appears that the *one-time-pad* [33, 3] remains the only theoretical unbreakable cryptographic system. (The word *appears* can often be used within cryptography.) The papers [32] and [28] use group rings and matrices over group rings for designing cryptographic systems. These are related to representation theory and systems of idempotents. The paper [8] in this proceedings deals with cryptographic systems with group rings and related results.

Here we (briefly) present a system related to group rings, see [29] for details. Keys are constructed at both ends for each communication and are randomly chosen within group ring structures and *need only be used once*.

8.1. **A basic system with group rings.** It is required to communicate secretly data $\underline{x}$ from A to B. Data is represented in vector form and matrices are denoted by capital letters. For details on *group ring matrices* see for example [23]; the set-up and main properties of these are given in section 3.2. These are also referred to as *RG-matrices* when the group ring in question is specified and are obtained from the embeddings of a group rings into rings of matrices; they include such matrices as circulant matrices, circulant of circulant matrices and similar such.

An RG-matrix, which is of size $|G|\times|G|$, is determined by its first row and is a matrix corresponding to a group ring element, relative to a listing of the elements of G. Two RG-matrices obtained from the same group ring RG (relative to the same listing) are said to be of the same *type*. The RG-matrices commute if and only if G is commutative. Methods to randomly choose singular and non-singular matrices with certain properties from a huge pool of such matrices are given in [29].

Let $\underline{x}$ be a row vector with entries from R. Then the *completion* of $\underline{x}$ in RG (relevant to a particular listing) is the RG-matrix with first row $\underline{x}$. The *rank of a vector*, relative to its completion in a specified group ring, is defined as the rank of its completion; this gives meaning to *kernel of a vector* relative to its group ring completion.

The completion of the vector $\underline{x}$ is denoted by the corresponding capital letter X (without underlining). For $a \in RG$ its image in $R_{n\times n}$ under the embedding of RG into $R_{n\times n}$ is denoted by the corresponding capital letter A. When $\underline{x}$ is a vector, to be considered as an element of RG, then also use X (without underlining) to denote its image under this embedding.

The following Lemma is immediate.

Lemma 8.1. *Suppose P, Q are RG-matrices with the same first row. Then $P = Q$.*

Thus if $\underline{x}$ is a vector in R^n and A is an RG-matrix of size $n \times n$ then from Lemma 8.1 the completion of $\underline{x}A$ in RG is XA where X is the completion of $\underline{x}$ in RG.

Let $\underline{x}$ be the data to be transmitted secretly from A(lice) to B(ob). The data $\underline{x}$ is arranged so that X is singular with large kernel where X is the completion of $\underline{x}$ in same type of RG-matrix as A (the matrix chosen by A below in 1.); details on how this can be arranged are given in [29]. When X is singular with large kernel then also CX, XC are singular with large kernel for any matrix C.

8.1.1. **General set-up.**

(1) A chooses A, a non-singular group ring matrix, and transmits $\underline{x}A$.
(2) B chooses B non-singular and transmits BXA.
(3) A transmits BX.
(4) B works out $B^{-1}BX = X$.

This method B need not in general be a group ring matrix and even if so it need not be of the same type as A. If B is of the same type as A and X then only the first row of the matrices in 2. and 3. need be transmitted. In 4. only the first row of $B^{-1}BX$ need be calculated as the first row of X give $\underline{x}$. The inverses of A, B should be easily obtainable; pools of matrices from which such matrices may be drawn can also be drawn up. When using matrices with certain structures such as RG-matrices the matrix multiplications and vector-matrix multiplications may be performed by convolutional methods.

The matrices A, B here are as large as the vector of data $\underline{x}$ and chosen randomly. The data may also be broken up and multiple vector design schemes implemented as shown in [29]. Simplified schemes with commuting matrices may also be derived; these do not necessarily need RG-matrices – see [29] for details.

When some matrices commute the data $\underline{x}$ may also be 'protected' at each end. Generalisations on this method where the data being transmitted is broken into blocks and each block is kept secret by a possibly different matrix can also be similarly constructed. The matrices can be large and encryption and decryption can be done in $O(n \log n)$ time.

8.2. **Key exchange.** The basic methods may be used for key exchange. Let $\underline{x}, \underline{y}$ be vectors so that X, Y are singular but $X + Y$ or some combination of X, Y is non-singular.

(1) A transmits $\underline{x}A$.
(2) B replies with BXA.
(3) A replies with BX.
(4) B now knows X. A can now repeat the process to get Y secretly to B. Or else:
    (a) B can choose Y so that $X + Y$ or a combination of X, Y is non-singular.
    (b) B transmits B_1Y.
    (c) A replies B_1YA.
    (d) B replies YA.
(5) Both A and B now have X, Y from which to form the encoding matrix.

X, Y may be taken so that $X^2 = 0 = Y^2$ or small powers of X, Y are zero. This ensures that $\operatorname{rank} X, \operatorname{rank} Y$ are small so that $\operatorname{rank} XA, \operatorname{rank} BY$ are also small.

9. **Search engines, internet, threshold logic**

Two areas mentioned in section 1.1, search engines and threshold logic, are very interesting topics which involve abstract algebra but fall outside our theme (at present!). These are given just brief descriptions below; details may be obtained from a good search engine!

9.1. **Search engine.** The most famous search engine is of course Google which is used millions of times each day. Courses at advanced undergraduate and graduate levels on the *Google Matrix* have now been introduced at various institutes of higher learning.

The *Google Matrix* is a matrix describing the connections and pointers between sites on the web - the entry in the (i, j) position is determined by calculating a finite sum of reciprocals determined by the number of such connections weighted in a certain way. It is an extremely large (its order is 10^s of billions and growing all the time) fairly sparse stochastic matrix A.

If you use google to find a hotel in a particular city the machine finds all hotel websites in that city and suggests them to you in a particular order. This ordering is determined as follows - each coordinate corresponds to a website and A, the Google matrix, has a *row eigenvector* v corresponding to the eigenvalue 1. The fundamental idea put forward is that the importance of a page is judged by the number of pages which link to it as well as their importance. Standard mathematical tools are used to make the 'engine' work. A simple, clever idea using relatively standard mathematical ideas as linear algebra and probability theory has led to a immense breakthrough in the efficiency of search engines, and to the start of a commercial giant.

9.2. **Threshold logic.** Interest in threshold functions and logic comes from computer science, pattern recognition and neural networks. An algebraic approach to Boolean threshold functions using methods of group rings [1] has only recently attracted attention. The Boolean case in [1] uses group ring structures over fields of characteristic 2. It's clear that further advancement can be made using fields of other characteristic and this is and will be a fruitful area for research.

10. **Finally**

We have attempted here to demonstrate how certain abstract mathematical concepts are now more than ever so important and fundamental within the communications' areas.

It took over 200 years for *Field Theory* to become 'useful' and this theory is now so important in many areas and applications. The 'turnover' time can be much shorter. Which areas are now 'useful' and which areas will become 'useful'?

An attempt to list important areas of modern 'pure' mathematics would include many topics of great practical importance and any 'applied' mathematician is naturally led to study abstract mathematical concepts and problems. Any division between 'Pure Mathematics' and 'Applied Mathematics' is a rather false one; the word 'Mathematics' covers all areas which are mathematical in nature and content.

References

[1] N. N. Azenber, A. A. Bovdi, E. I. Gergo and F. E. Geche, Algebraic aspects of threshold logic, (Russian), *Cybernetics*, no. 2 (1980) 26-30.

[2] O. M. Baksalary, D. S. Bernstein and G. Trenkler, On the equality between rank and trace of an idempotent matrix, *Appl. Math. Comput.*, **217** (2010) 4076-4080.

[3] S. Bellovin and F. Miller, Inventor of One-Time pad, *Cryptologia*, **35** no. 3 (2011) 203-222.

[4] R. E. Blahut, *Algebraic Codes for data transmission*, Cambridge University Press, 2003.

[5] N. Boston, *Applications of Algebra to Communications*, Control and Signal Processing, Springer, 2012.

[6] S. Buckley, Why do research in pure mathematics?, *Irish Math. Soc. Bulletin*, no. 72 2013 39-44.

[7] E. Candés, J. Romberg and T. Tao, Robust Uncertainty Principles: Exact Signal Reconstruction From Highly Incomplete Frequency Information, *IEEE Trans. Inform. Theory*, **52** no. 2 (2006) 489–509.

[8] C. Carlet and Y. Tan, On Group Rings and some of their applications to combinatorics and symmetric Cryptography, these proceedings.

[9] C. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, *Amer. Math. Soc.*, 1962.

[10] P. Davis, *Circulant matrices*, AMS Chelsea Publishing, 1994.

[11] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. Information Theory*, **22** no. 6 (1976) 644–654.

[12] B. Hochwald and W. Sweldens, Differential unitary space time modulation, *IEEE Trans. Comm.*, **48**(2000) 2041-2052.

[13] R. J. Evans and I. M. Isaacs, Generalized Vandermonde determinants and roots of unity of prime order, *Proc. Amer. Math. Soc.*, **58**(1976) 51-54.

[14] P. E. Frenkel, Simple proof of Chebotarëv's theorem on roots of unity, http://arxiv.org/abs/0312398.

[15] GAP – Groups, Algorithms and Programming, www.gap-system.org

[16] R. G. Gallager, Low Density Parity Check Codes, *IRE Trans.*, **8** (1962) 21-28.

[17] D. Goldstein, R. M. Guralnick and I. M. Isaacs, Inequalities for finite group permutation modules, *Trans. Amer. Math. Soc.*, **357** no. 10 (2005) 4017–4042.

[18] D. Hamlet, Science, Mathematics, Computer Science, Software Engineering, *The Computer Journal*, **55** no. 1 (2012) 99-110, (doi:10.1093/comjnl/bxr090).

[19] W. C. Huffman, V. S. Pless and R. A. Brualdi, *Handbook of Coding Theory*, **1,2**, North-Holland, Amsterdam, 1998.

[20] P. Hurley and T. Hurley, Codes from zero-divisors and units in group rings, *Int. J. Inf. Coding Theory*, **1** no. 1 (2009) 57–87.

[21] P. Hurley and T. Hurley, Block codes from matrix and group rings, Chapter 5, in *Selected Topics in Information and Coding Theory*, eds. I. Woungang, S. Misra, S.C. Misma, World Scientific, 2010 159-194.

[22] P. Hurley and T. Hurley, LDPC and convolutional codes codes from matrix and group rings, Chapter 6, in *Selected Topics in Information and Coding Theory*, eds. I. Woungang, S. Misra, S. C. Misma, World Scientific, 2010 195-238.

[23] T. Hurley, Group rings and rings of matrices, *Int. J. Pure Appl. Math.*, **31** no. 3 (2006) 319–335.

[24] T. Hurley, Convolutional codes from units in matrix and group rings, *Int. J. Pure Appl. Math.*, **50** no. 3 (2009) 431–463.

[25] T. Hurley, Self-dual and dual-containing codes using group rings, http://arxiv.org/abs/0711.3983.

[26] B. Hurley and Ted Hurley, Paraunitary matrices and group rings, *Int. J. Group Theory*, **3** no. 1 (2014) 31–56, http://arxiv.org/abs/1205.0703.

[27] B. Hurley and T. Hurley, Group ring cryptography, *Int. J. Pure Appl. Math.*, **69** no. 1 (2011) 67–86.

[28] B. Hurley and T. Hurley, Systems of MDS codes from units and idempotents, http://arxiv.org/abs/1301.5596, 2013.

[29] T. Hurley, Cryptography, key exchange, public key, http://arxiv.org/abs/1305.4063.

[30] T. Hurley, P. McEvoy and J. Wenus, Algebraic constructions of LDPC codes with no short cycles, *Int. J. Inf. Coding Theory*, **1** no. 3 (2010) 285–297.

[31] R. Johannesson and K. Zigangirov, *Fundamentals of Convolutional Coding*, IEEE Press, New York, 1999.

[32] D. Kahrobaei, Ch. Koupparis and V. Shpilrain, Public Key Exchange Using Matrices Over Group Rings, *Groups Complex. Cryptol*, **5** no. 1 (2013) 97–115.

[33] J. Katz and Y. Lindell, *Introduction to modern cryptography*, Chapman and Hall, Boca Raton, 2008.

[34] N. Koblitz, *A Course in Number Theory and Cryptography*, **114**, Springer-Verlag, New York, 1994.

[35] I. Kra and S. Simanca, On circulant matrices, Notices Amer. Math. Soc., **59** no. 3 (2012) 368–377.

[36] D. Labate, G. Weiss and E. Wilson, Wavelets, *Notices Amer. Math. Soc.*, **60** no. 1 (2013) 66-76.

[37] D. J. C. MacKay, *Information theory, Inference and Learning Algorithms*, Cambridge University Press, New York, 2003.

[38] I. McLoughlin and T. Hurley, A Group Ring Construction of the Extended Binary Golay Code, *IEEE Trans. Inform. Theory*, **54** no. 9 (2008) 4381-4383.

[39] C. Milies and S. Sehgal, *An introduction to Group Rings*, Klumer, 2002.

[40] J. O'Shaughnessy, *Convolutional codes from group rings*, Thesis, National University of Ireland Galway, 2011.

[41] J. O'Shaughnessy, Convolutional codes from group rings, to appear *IJICoT (Int. J. Inf. Coding Theory)*.

[42] J. O'Shaughnessy, 'Quick look in' convolutional codes from group rings, preprint.

[43] B. A. Sethuraman, Division Algebras and Wireless Communication, *Notices Amer. Math. Soc.*, **57** no. 11 (2010) 1432-1439.

[44] A. Shokrollahi, B. Hassibi, B. M. Hochwald and W. Sweldens, Representation theory for high-rate multiple-antenna code design, *IEEE Trans. Inform. Theory*, **47** no. 6 (2001) 2335-2367.

[45] A. Soman and P. Vaidyanathan, On orthonormal wavelets and paraunitary filterbanks, *IEEE Trans. on Signal Processing*, **41** no. 3 (1993) 1170-1183.

[46] G. Strang and T. Nguyen, *Wavelet and Filter Banks*, Wellesley-Cambridge Press, 1997.

[47] P. Stevenhagen and H. W. Lenstra Jr., Chebotarëv and his density theorem, *Math. Intell.*, **18** (1996) 26-37.

[48] T. Tao, An uncertainty principle for cyclic groups of prime order, *Math. Res. Lett.*, **12** no. 1 (2005) 121-127.

[49] T. T. blog, http://terrytao.wordpress.com/2007/04/13/compressed-sensing-and-single-pixel-cameras/

[50] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*, Prentice-Hall, 1993.

Ted Hurley

Department of Mathematics, National University of Ireland Galway, Galway, Ireland

Email: ted.hurley@nuigalway,ie