Chapter One

Introduction

The purpose of this book is three-fold: to report the current status of existence and construction problems for Hadamard matrices and their generalisations; to give an accessible account of the new unifying approach to these problems using group cohomology; and to support an understanding of how these ideas are applied in digital communications. I have tried to present results and open problems with sufficient rigour, and direction to the literature, to enable readers to begin their own research, but with enough perspective for them to gain an overview without needing in-depth knowledge of the algebraic background.

The book has two Parts. In Part 1, consisting of four Chapters, our present understanding of Hadamard matrices, generalised Hadamard matrices and higher dimensional Hadamard matrices is summarised. One Chapter is devoted to introduction and explanation of the main applications of Hadamard matrices in digital signal and data sequence processing, principally for spectral analysis and signal error protection, separation or encryption.

Generalised Hadamard matrices and higher dimensional Hadamard matrices are each natural enlargements of the class of Hadamard matrices, in the direction of entries not restricted to $\{\pm 1\}$ and not restricted to 2-dimensional (2-D) arrays, respectively. Part 1 contains the basic definitions and properties of these three types of Hadamard matrices and, for each of them, a status report on recent results using classical techniques. The two ideas from which Warwick de Launey and I developed the group extensions approach to Hadamard matrices: group development of Hadamard matrices and construction of higher dimensional Hadamard matrices from relative difference sets are highlighted.

Part 2, also consisting of four Chapters, develops in detail the unifying group extensions approach to existence and construction of the three types of Hadamard matrices covered in Part 1. Some necessary algebraic background is included. This Part covers the major theoretical advances made over the past 15 years, culminating in the Five-fold Constellation, which identifies cocyclic generalised Hadamard matrices with particular 'stars' in four other areas of mathematics and engineering: group cohomology (factor pairs), incidence structures (divisible designs), combinatorics (relative difference sets) and signal correlation (perfect arrays). The work in this Part has not been collected before, or is accessible only in journal articles. Some is not yet published.

The latter half of Part 2 introduces less mature, but very exciting, theoretical results on the atomic structure of cohomology classes. These *shift orbits* have remained invisible for nearly a century, but carry the statistical information about distributions of the entries of cocyclic matrices that determines whether or not

they will produce Hadamard matrices, high-distance error-correcting codes and low-correlation sequences. Finally, the first applications of the theory of cocyclic Hadamard matrices to multiphase signal and data sequence processing are presented. We construct novel and optimal families of such cocyclic generalised Hadamard matrices and their corresponding Generalised Hadamard Transforms, codes and sequences.

Half the open research problems arise in this last quarter of the book.

A summary of each Chapter follows.

Chapter 2 covers basic definitions and properties of Hadamard matrices, in abbreviated form. There are many excellent texts [288, 1, 123, 315], reviews [68, 69] and databases [212, 287, 297], describing Hadamard matrices and their numerous constructions in more detail; the intention here is to provide a succinct summary and update of research over the past decade or so. Direct constructions of Hadamard matrices by Sylvester, Paley and Williamson and from Hadamard designs are described and illustrated.

More modern techniques of constructing Hadamard matrices, by patterning entries according to the multiplication table of a group, are treated next. This is our first link to cocycles and cocyclic Hadamard matrices. In the final section of Chapter 2, advances towards direct confirmation of the celebrated Hadamard Conjecture, and improved asymptotic support for it, are outlined, as is progress on the circulant Hadamard conjecture.

The purely intellectual excitement and challenge of finding new Hadamard matrices and homing in on confirmation of the Hadamard Conjecture is heightened by the knowledge that they are marvellously useful. *Chapter 3* is devoted to two of their three principal applications: Hadamard transform spectroscopy and object recognition, and coding of digital signals. Applications in design of experiments are not included. Most emphasis is placed on coding of digital signals or data sequences for error correction, separation, correlation or encryption.

Each application area is introduced briefly to explain how the Hadamard matrix is applied, but in enough detail, and in the language of the application, to explain current trends. My aim is to bridge the two worlds: to translate the physical application into terms a pure mathematician will appreciate and the theoretical structure into terms an applied mathematician, computer scientist or communications engineer can adapt and use.

Chapter 4 moves us from Hadamard matrices to generalisations where matrix entries are not restricted to $\{\pm 1\}$. More than one direction for enlargement of the class of Hadamard matrices has flourished, but generalisations to maximal determinant matrices, weighing matrices, orthogonal designs and nonsquare matrices will not be covered. The two main formulations we treat are *complex Hadamard matrices* (invertible, with entries on the complex unit circle) — especially those with entries which are roots of unity, called *Butson matrices* here — and *generalised Hadamard matrices* (with entries from a finite group N, for which the inner quotient of any distinct pair of rows in the integral group ring $\mathbb{Z}N$ equals $\lambda\,(\sum_{u\in N} u)$, for some fixed integer λ). To complicate matters, in the literature the term complex Hadamard matrix often refers only to a Butson matrix with entries in $\{\pm 1, \pm\sqrt{-1}\}$, of which those with uniformly distributed rows are also called *quaternary* gener-

alised Hadamard matrices. Although complex Hadamard matrices will be revisited on occasion, the principal subject of this book is generalised Hadamard matrices. Jungnickel's seminal 1982 result, relating generalised Hadamard matrices, class regular divisible designs and relative difference sets, underscores the richness of the interconnections between these areas and the group extensions approach described in the second part.

This Chapter follows the structure of Chapter 2, for each of Butson, complex Hadamard and generalised Hadamard matrices in turn, illustrated with numerous examples. One section covers their applications to multiphase signals and sequences. The final section is new work, unifying the two formulations in the invertible *Generalised Butson Hadamard* matrices, which include all complex Hadamard matrices and all invertible generalised Hadamard matrices, and their *Generalised Hadamard Transforms*.

Chapter 5 enlarges the class of Hadamard matrices from 2-D to n-dimensional arrays with entries from $\{\pm 1\}$. It deals with *n-dimensional proper Hadamard matrices*, introduced by Shlichta in 1971, which have the property that all 2-D subarrays obtained by fixing any $n-2$ coordinates are Hadamard matrices.

Despite a strong presumption of their utility — based on that of Hadamard matrices — and their formative role in development of the group extensions approach to Hadamard matrices, remarkably little is known about higher dimensional proper Hadamard matrices. The first monograph on the subject is Yang [334]. A summary of construction techniques, relationships between these techniques, equivalence classes and applications to Boolean functions useful for cryptography and to error-correcting array codes is presented.

Higher dimensional proper Hadamard matrices were central to the discovery of cocyclic Hadamard matrices by Warwick de Launey and myself. His effort to characterise those Hadamard matrices which would generate higher dimensional proper Hadamard matrices led him to isolate functions which must satisfy specific relations between their values and which I subsequently identified as cocycles.

A 2-dimensional *cocycle* between finite groups G and N, with trivial action, is a function $\psi : G \times G \to N$ satisfying the equation

$$\psi(g,h)\psi(gh,k) = \psi(h,k)\psi(g,hk), \ \ \forall\, g,h,k \in G.$$

We then rederived this equation by asking when an abstract combinatorial design could be functionally generated from a single row. This *cocyclic development* of matrices includes group development of matrices, which was described in Chapter 2. The *cocyclic matrix* developed from $\psi : G \times G \to N$ is

$$[\psi(g,h)]_{g,h\in G}.$$

A cocycle whose matrix is Hadamard is called *orthogonal*.

The first Chapter of Part 2, *Chapter 6*, concerns cocycles, which arise naturally in many areas: surface topology, algebra and quantum mechanics, for instance. The usual unit studied in group cohomology is a cohomology (equivalence) class of cocycles, not the individual cocycles comprising it, so the examples, properties and constructions collected here do not appear in cohomology texts and are listed for the first time.

Some time is spent on the practicalities of computing cocycles. One of the advantages of the group extensions approach to Hadamard matrices is that the internal structure of a cocyclic matrix promises efficiency in computer searches for generalised Hadamard matrices, cutting down the search space over exhaustion dramatically. But first we need to find and list the cocycles. Three algorithms are presented: one, the Flannery-O'Brien algorithm, was developed to exploit the ideas presented in this book and is distributed as a module in the computer algebra package MAGMA.

The Chapter continues by showing that most of the direct constructions of Hadamard matrices listed in Chapter 2 are cocyclic, for some group G and $N = \{\pm 1\}$. To date, cocyclic construction is the most successful general method known, both theoretical and computational, for finding Hadamard matrices. In particular, the most productive single construction of Hadamard matrices, due to Ito, is cocyclic over the dihedral groups. The Cocyclic Hadamard Conjecture follows: that for each odd t there is a group G of order $4t$ such that a G-cocyclic Hadamard matrix exists. The Chapter concludes with a status report on 12 research questions posed by the author in earlier papers on cocyclic Hadamard matrices.

Cocycles are special cases of *factor pairs* of functions. *Chapter 7* contains the full description of the theory of orthogonal factor pairs and the generalised Hadamard matrices they determine. The theory has been complete for only a few years. Sufficient background information on group extensions, factor pairs and cohomology of finite groups is included to make the book self-contained.

The limiting class of generalised Hadamard matrices obtained using the group extensions approach is the class of *coupled cocyclic* generalised Hadamard matrices. We can do no better than this. Whilst not every generalised Hadamard matrix is a coupled cocyclic matrix, I know of only one counterexample, a matrix of order 6 with entries from the group $\mathbb{Z}_3$ of integers modulo 3. I know of no Hadamard matrix which is not cocyclic — but the sheer number of inequivalent Hadamard matrices even for small orders makes it unlikely all will be cocyclic.

The Chapter's central purpose is to convey the pervasive influence of cocyclic generalised Hadamard matrices, by locating them (in four different guises) within combinatorics, group cohomology, incidence structures and digital sequence design. This is done by proving mutual equivalences — the *Five-fold Constellation* — between coupled cocyclic generalised Hadamard matrices, semiregular relative difference sets, orthogonal factor pairs, semiregular class regular divisible designs with regular action and well-correlated arrays. These equivalences have been established in increasing generality over the past decade by de Launey, Flannery, Perera, Hughes and the author, with the fullest expression due to Galati. The general form of the fifth equivalence — with well-correlated arrays — is given here for the first time. Such universality helps to explain the tremendous variety of uses to which we can put these matrices.

Chapter 8 deals with the way in which different definitions of equivalence class interrelate within the Five-fold Constellation. There are preexisting concepts of equivalence for generalised Hadamard matrices, for transversals of subgroups in groups, and for factor pairs and group extensions arising naturally from theoretical considerations in each area, and they do not coincide. The equivalence relation for

transversals is revealed to be the strongest relation. It becomes a very productive and novel way of investigating each of the 'stars' of the Constellation.

When equivalence of transversals is transcribed to an action on factor pairs, it forms orbits termed *bundles*. These bundles are copied around the Five-fold Constellation. For splitting factor pairs, bundles define equivalence classes of functions $G \to N$, which form the basis of a new theory of nonlinearity. For semiregular relative difference sets, the resulting taxonomy allows us to establish a classification program for their equivalence classes and begin to populate it. This problem is at the heart of research in relative difference sets.

Two components of bundle action can be isolated, one an action by automorphism groups of G and N and the other a differential G-action called *shift action* which arises from translation and renormalisation of transversals. Thus a bundle is an automorphism orbit of shift orbits, and vice versa. These components, though not wholly independent, can be extracted and investigated in more general situations.

Shift action is a remarkably universal action and should be identifiable in more contexts than in fact appears to be the case. Shift action operates wholly within the natural equivalence classes of factor pairs, partitioning each one into shift orbits — its atomic structure. So, it is invisible from the point of view of cohomology theory, but it is critical to our study. Shift orbits (and the bundles they generate) carry the statistical information about distributions of the entries of cocyclic matrices that determines whether or not they will produce Hadamard matrices, high-distance error-correcting codes and low-correlation sequences.

Some external sightings of shift action in disguise have been made: in differential cryptanalysis and in the Loewy series for p-groups. LeBel's thesis [217] identifies shift action within the trivial cohomology class with a natural action in a quotient algebra of the standard module of a group ring.

In the final, and longest, Chapter, we begin to reap the rewards of all the preceding hard work. *Chapter 9* contains a multitude of new constructions and applications of cocyclic complex and generalised Hadamard matrices, and a tantalising set of new problems, too.

Initially we look at several recent applications of cocycles, not necessarily orthogonal, to computation in Galois rings, to elliptic curve cryptography and to the developing field of *cocyclic codes* over nonbinary alphabets.

Then splitting orthogonal factor pairs are applied to establish a general theory of nonlinear functions suitable for use as cryptographic primitives. These include planar, bent and maximally nonlinear functions, and surprising and beautiful connections with finite presemifields and projective planes are uncovered.

In turn, these help identify large classes of new cocyclic generalised Hadamard matrices. We are next led to the discovery of families of optimal codes, such as the q-ary codes meeting the Plotkin bound found by Udaya and myself and the extremal self-dual binary codes found by Rao.

Finally, differential uniformity, an important measure of the resistance of a block encryption cipher to differential attack, is extended to array encryption ciphers, and a class of orthogonal cocycles proposed as array S-box functions.

I hope the reader will find this field as rich and exciting as I do. Good luck and good hunting!