BINARY FRAMES, CODES AND EUCLIDEAN EMBEDDINGS

A Dissertation Presented to
the Faculty of the Department of Mathematics
University of Houston

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

By
Robert Paul Mendez
December 2018

BINARY FRAMES, CODES AND EUCLIDEAN EMBEDDINGS

Robert Paul Mendez

APPROVED:

Dr. Bernhard G. Bodmann, Committee Chair
Department of Mathematics

Dr. Mehrdad Kalantar
Department of Mathematics, University of Houston

Dr. Demetrio Labate
Department of Mathematics, University of Houston

Dr. Rachel A. Ward
Department of Mathematics,
University of Texas at Austin

Dean, College of Natural Sciences and Mathematics

Acknowledgements

To thank a village...

Financial support

The research represented herein was partially supported by the National Science Foundation through NSF grants DMS-1412524 and DMS-1715735. I believe that government support of the sciences is crucial to growth as a society. My ability to perform research at the University of Houston was additionally financially supported by the university's Graduate Tuition Fellowship and my work for the Houston Journal of Mathematics. I am particularly grateful for to the managing editor at the time of my hiring to the Journal, Klaus Kaiser. His guidance, encouragement, mentorship and historical storytelling(!) in that office have been invaluable. Finally, I am grateful for a number of scholarships from the University of Houston Alumni Association.

Addtional support: primary investors

Six and a half years ago, R. Jon Mendez[1] gave me an audiobook copy of [32], James Gleick's *The Information: A History, a Theory, a Flood*. Upon my return to graduate school a few years later, it was my fascination with this work that led me to take Bernhard Bodmann's *Information Theory* course.

I do not care to imagine how different the last few years might have been had my timing been a little different—in one of only two uses of the second-person specific singular form within these pages, I say, *thank you, Bernhard, for everything*. It would be hyperbole to say I could not have done it without him, but it is with statistically significant anecdotal evidence that I declare that Dr. Bodmann is among the greatest advisors a student researcher could hope for. I am grateful for his patience, his levels of mentorship, and his attentiveness to the types and range of details that encumber[2] the life academic, as well as his willingness to balance guidance and freedom.

There are three people who have invested so much in my current endeavor—the effort and growth which precede certification as a researcher—that it is hard to believe that I am the only one to be honored in my pending graduation. Having just thanked my advisor, I move now to thank my first mentor in this arena, Dr. Gordon Johnson. I will forever cherish our years of mathematical and philosophical conversation, and I know additionally that the educator I am today is tremendously influenced by the methods and spirit he brings to every learning environment.

Another adoring fan of Dr. Johnson is the remaining critical investor in my goals: my bride of 22 years, Trudi Lynn Mendez. I was inspired during a classical music concert in February 2014—utterly indwelt with a *need*—to return to university for mathematics research. She did not hesitate in her response, and I started in the fall. This has been a tremendous

[1] a dear *tío*

[2] Or, as he would encourage me to say, "enrich".

undertaking, and we both knew when it started that this season would violate all standards of "work/life balance". She has never faltered in her support, despite many, many, *many* late nights at school and dropped balls at home. I do not know how I could adore her more, and it is ridiculous to imagine that I can completely express my thankfulness to her here. I am glad that I can now fulfill my promise to her that this was, in fact, a season.

Additional support: the village

I did not complete my graduate school efforts in one run; in 2007 I accepted some important advice from Jeff Morgan, who pointed out that I was not demonstrating the passion he had seen evidenced in my philanthropic work and previous educational efforts. His kind directness put me in a position to reevaluate my goals, and I similarly strive to balance truth and kindness in my own opportunities to guide people. A year later, Krešimir Josić reached out to me to encourage me to reconsider my position on education; at the time, it was not a viable option for me, but he planted a seed. Mark Tomforde invited me to sit down and evaluate my course selections and research goals soon after I came back to grad school, resulting in some important shifts in my schedule and mindset. These may sound like casual anecdotes, but they reflect formative and critical junctures in my path, and I am thankful.

In those first semesters starting fall 2014, I spent a great deal of time in Vaughn Climenhaga's office, where I always could count on clear and enthusiastic mathematics conversation and guidance on the nuances of academia. As supportive as he was in that time, I can only imagine how many students he has helped since then.

A group of my peers have been family, and we have learned together and taught one another and encouraged one another. I must express thanks and cheers to my brothers Richard Walden, Kazem Safari, Adrian Radillo, Nickos Karantzas, and Mo Haque, and to my sisters, Duong Nguyen, Jennifer May, Daewa Kim, Sarah Chehade, Kayla Bicol, and Prajakta Bedekar. My *academic* brother and officemate, Dylan Domel-White, receives special mention for the scores and scores of hours we have spent on so many different mathematical adventures.

Finally, to Tío Jon: Thank you for your encouragement and fraternity, and for the incidental and critical role your thoughtfulness played in my journey.

BINARY FRAMES, CODES AND EUCLIDEAN EMBEDDINGS

An Abstract of a Dissertation
Presented to
the Faculty of the Department of Mathematics
University of Houston

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

By
Robert Paul Mendez
December 2018

Abstract

This dissertation has two parts. The first part is concerned with using Euclidean embeddings and random hyperplane tessellations to construct binary block codes. The construction proceeds in two stages. First, an auxiliary ternary code is chosen which consists of vectors in the union of coordinate subspaces. The subspaces are selected so that any two vectors of different support have a sufficiently large distance. In addition, any two ternary vectors from the auxiliary codebook with common support are at a guaranteed minimum distance. In the second stage, the auxiliary ternary code is converted to a binary code by an additional random hyperplane tessellation.

The second part of this dissertation is dedicated to Binary Parseval frames, which share many structural properties with real and complex ones. On the other hand, there are subtle differences, for example that the Gramian of a binary Parseval frame is characterized as a symmetric idempotent whose range contains at least one odd vector. Here, we study binary Parseval frames obtained from the orbit of a vector under a group representation, in short, binary Parseval group frames. In this case, the Gramian of the frame is in the algebra generated by the right regular representation. We identify equivalence classes of such Parseval frames with binary functions on the group that satisfy a convolution identity. This allows us to find structural constraints for such frames. We use these constraints to catalogue equivalence classes of binary Parseval frames obtained from group representations. As an application, we study the performance of binary Parseval frames generated with abelian groups for purposes of error correction. We show that if p is an odd prime, then the group $\mathbb{Z}_p^q$ is always preferable to $\mathbb{Z}_{p^q}$ when searching for best performing codes associated with binary Parseval group frames.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

> *The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have* meaning... [71]
>
> —Claude E. Shannon, *A Mathematical Theory of Communication*

Introducing some of the notions in this dissertation involves an effort to overcome ambiguities that can arise from the use of commonly understood words like "communication", "message" and "transmit" as formally defined concepts. Implicit in Shannon's statement is that a message is to be *communicated*. Hereafter, a message is a *discrete* message: a finite sequence drawn from a discrete set of symbols. To *transmit* is to commit the action which physically permits the reproduction of a selected message; the existence of this dissertation, for example, is evidence of *transmission*. Upon transmission, a message becomes a *signal* carried by some medium, denoted as the *channel*.

This physical nature constrains communication by virtue of the existence of *noise* in a channel, which degrades the channel's *capacity*. In this context, the function of a code is to provide a vehicle designed to ensure that a discrete message can be reproduced after transmission through a *noisy* channel. Given an error-tolerance parameter and a channel capacity, Shannon's famed noisy-channel coding theorem[1] provides for the existence of such a code. *Producing* such a code is another matter, as well as a motivating factor for the study of *block* codes [30].

Specific to this dissertation, a *binary code* may be taken to be a collection of vectors $\{a, b\}^n \subseteq V$, for some vector space V (see Definition 2.1.1). A *constant weight* binary code is a binary code $\{0, 1\}^n \subseteq V$ having the property that each vector has the same ℓ_1 norm. A *binary block code* is an injective map from a message set $\{a, b\}^n$ in a vector space V to a presumably

[1] Formally, it is Theorem 11 in [71], under the section heading "The Fundamental Theorem for a Discrete Channel with Noise".

larger set of binary vectors $\{c, d\}^m \subset W$. How these fit Shannon's communications model is made explicit in the next chapter.

The main results in this dissertation advance the theory of binary codes, doing so from analytic, algebraic, and frame-theoretic perspectives. In each of the main results, constant weight binary codes or cyclic codes play a central role; there is much literature on such codes [23, 26, 27, 29, 35, 36, 47, 48, 60, 65, 72].

The remainder of this dissertation is organized as follows:

Inspired by and standing on the shoulders of research in compressed sensing and one-bit compressed sensing, the first chapters address methods of producing random binary codes.

Chapter 2 focuses on providing the terminology, concepts and notation that will be used throughout. This begins with an introduction to binary codes, taking them first to be structureless sequences of symbols. The discussion of associated measures of quality is motivated by narrative evolving from classic Shannon communications model. Binary codes are almost immediately considered as embedded in a vector space, and elements are treated as vectors from then on. The discussion on robustness leads to the declaration that errors herein are taken to be bit flips (Remark 2.1.8. Section 2.2 introduces the primary tool for producing random codes in this dissertation, the *(standard) random hyperplane tessellation*, which is the composition of the componentwise sign map with a Gaussian random matrix (see Definition 2.2.1). This is a commonly used tool of the one-bit compressed sensing community. In preparation for Chapter 3, random hyperplane tessellations (Φ) are studied. Properties of the distribution of points under Φ are addressed, in particular the expected Hamming separation of points as normalized geodesic distance in the domain. Block codes are introduced via a restricted communications model in Section 2.3. Chapter 1 closes with two examples of random binary codes and a discussion of the intuition as to why $\Phi(\{\pm 1\}^n)$ provides a trivial code rate, asymptotically.

Chapter 3 is dedicated to describing and demonstrating the first main result in this dissertation: a channel coding of $\{\pm 1\}^n$ into $\{\pm 1, 0\}^M$ which, under random hyperplane tessellation, achieves our asymptotic robustness and information rate goals. This adaptation of techniques developed by Plan and Vershynin for sparse recovery (e.g., [61]) to the design of binary block codes admits the use of linear programming for error correction purposes. The main innovation in the embedding is the use of a random constant weight binary code as the support vectors for an intermediate embedding.

The chapter's main result, Theorem 3.1.1, provides parameters for and claims the validity of a proposed random embedding Ψ, which is to map the Hamming cube $Q_n := \{\pm 1\}$ into Q_M by a two-stage process. The chapter begins with a description of the embedding Ψ, followed by the statement of the theorem, with the bulk of the chapter devoted to proving the result. The proof is laid out much along the lines of the construction of Ψ.

Stage 1 of the embedding occurs in three parts, each of which introduces a $1 - e^{O(n)}$ factor to the overall probability of success; the result of the stage is a ternary code in which 2^l copies

of $\Phi(Q_{n-l})$ are embedded by inclusion into $\mathbb{R}^M$, where Φ is a random hyperplane tessellation. Section 3.2 is devoted to the subordinate proofs, culminating with an explicit description of the section's construction in Section 3.2.4. Stage 2 is validated in Section 3.3, followed immediately by the proof of Theorem 3.1.1.

The work in Chapter 3 appeared in a very similar form as sections of "Binary block codes from Euclidean embeddings and random hyperplane tessellations", published in Proceedings of SPIE 10394, Wavelets and Sparsity XVII [6] and co-authored with Bernhard G. Bodmann.

In Chapter 4, we explore another important tool in code theory, (finite) group frames; this is a continuation of the efforts in [2], [4] and [5] in developing the theory of binary frames. Group frames are spanning families of vectors produced by the orbit of a single vector under the action of a group representation; the vectors of a *Parseval* group frame induce a *linear* code with a built-in decoder and, often, desirable robustness owed to a trait called *equiangularity*. There is already a substantial amount of literature on real and complex group frames [21, 40, 74, 75, 76, 77]; the focus of the present work is on *binary* Parseval group frames. Here, "binary" refers to the underlying field for the ambient vector space, the Galois field of two elements. The Gramians of Parseval frames satisfy conditions that make them suitable class representatives for each of the frame equivalence relations we use, and so we place special emphasis on the structure of the Gramians associated with binary Parseval group frames.

Chapter 4 provides relevant definitions of binary group frames and illustrating examples throughout. In the theory of real and complex frames, every group representation that generates a Parseval group frame is unitary; Section 4.2 concludes with the corresponding binary result and provides an explicit formulation of such representations in terms of the frame vectors and the group algebra. This development of binary Parseval group frame theory continues to parallel that of group frames over $\mathbb{R}$ and $\mathbb{C}$, and leads to the next main result in this dissertation: a characterization of binary Parseval group frames with respect to their Gramians, which coincide with the the *candidates* for such Gramians in the group algebra. That is, the Gram of a binary Parseval group frame is a (binary) linear combination of elements of the group's right regular representation, and every matrix in the group algebra that satisfies the conditions for a binary Parseval frame is the Gram matrix of a binary Parseval *group* frame induced by the original group.

We extend this result by further characterizing such Gramians in terms of binary functions over the group, so that binary Parseval group frames (and hence, their induced codes) may be enumerated by examining binary coefficient sequences over the group algebra. In the case that the underlying group is abelian and of odd order, we prove a simple algorithm for enumerating the associated group frames constructively.

The results on the structure of binary Parseval frames have significance for the design of error-correcting codes [3, 55]. Real and complex frames as codes have been given much attention [7, 34, 42, 49, 56, 57, 66, 67]. In an earlier paper ([4]), Bodmann et al. developed results in binary code design from a graph-theoretical perspective; Our work here applies

methods from frame theory to continue that effort. We introduce the notion of *automorphic switching equivalence* among binary group frames, a refinement of switching equivalence which preserves partitions on (induced) binary codes. This leads to a recognition that in the search for codes via group action, the choice of group can have significant impact on the coding performance of the resulting frame: Under this partitioning, we demonstrate that the classes of binary Parseval group frames induced by $\mathbb{Z}_{p^q}$ are subsumed by the classes induced by $\mathbb{Z}_p^q$. Thus, when searching for best performers, the group $\mathbb{Z}_p^q$ is a better choice.

We investigate group representations of $\mathbb{Z}_p^q$ and $\mathbb{Z}_{p^q}$ for small values of p and q and explicitly determine the best performance for $p = q = 3$ and $p = 5$, $q = 3$.

The work in Chapter 4 appeared in a very similar form as "Binary Parseval frames from group orbits" in Linear Algebra and its Applications, published November 2018 [59] with co-authors Bernhard G. Bodmann, Zachery J. Baker, Micah G. Bullock and Jacob E. McLaney.

1.1 A last initial note.

Out of respect for the reader and gratitude for their time, an effort has been made to enhance readability of this manuscript and the accessibility of its contents. The global layout and internal formatting are designed to permit the seeker of particular information to easily track down any definitions or details required to understand a given passage or result.

Regarding definitions, the reader may note a balance between formal definitions and those incorporated within the flow of the narrative. Of course, there are many instances of the use of a formal definition environment throughout this manuscript; the visual segmentation from the main text and the precise explication of a formal definition provide rigor and clarity while emphasizing the significance of the entry. On the other hand, there are times when slightly relaxed approach accomplishes the desired communication in a more compact, yet natural form. Awareness of the following list of intended outcomes may facilitate the reader's extraction of information from these pages:

- While there is occasional use of italics for for simple emphasis, such emphasis is generally indicative of the first use of a key word or phrase.
- Key words and phrases which appear outside their defining subsection appear in the index.
- Key words and phrases may be defined formally, in-line, or contextually; this distinction is reflected in the typeface of page numbers in the index, as illustrated in Table 1.1.

Table 1.1: Descriptive sample entries from the index.

First appearance in text	Index entry
"This type of error is known as a *bit flip*."	bit flip, 12
"**Definition 2.2.2** (Hamming ball). ..."	Hamming ball (B_H), **10**
"The signal may be subject to *noise* while in the channel, and thus be modified."	noise, *12*
"The code rate is sometimes called the *information rate*."	information rate, 8, *see also* code rate (syn.)

Formal definitions are given bold page numbers, while "in-line" definitions have normal page numbers. Italic page numbers indicate expressions defined contextually, and declarations of synonymity are treated as in-line definitions with a reference to the originally defined word.

Chapter 2

Preliminaries

2.1 Binary codes: a primer

Binary codes, central to every aspect of this dissertation, are collections of finite binary sequences, called *code words*; a binary sequence of length m, in turn, is simply an ordered m-tuple of two symbols. The symbols need not inherently offer any information beyond their distinguishability. More explicitly,

Definition 2.1.1. Given $m \in \mathbb{N}$ and distinct symbols a and b, the set of $\{a, b\}$-binary sequences of length m is the collection of functions $x : \{1, 2, \ldots, m\} \to \{a, b\}$. An $\{a, b\}$-binary m-code is a collection of $\{a, b\}$-binary sequences of length m.

Equivalently, we will consider the $\{a, b\}$-binary sequences of length m to be the elements of $\{a, b\}^m$, which we may refer to as the *code space*. In light of this equivalence, we may refer to the terms of a binary sequence as its *entries*, and we may alternately call them *bits*[71][1]. Additionally, let us consider the prefixes $\{a, b\}$- and m- as prescriptive modifiers in the expressions "$\{a, b\}$-binary sequence" and "$\{a, b\}$-binary m-code", so that phrases such as "binary m-code" are read as natural generalizations.

2.1.1 Quantifying code qualities

In classic metonymous fashion, we also use "bit" as a unit of measurement: the 2^m binary sequences in the set $\{a, b\}^m$ provide m *bits of information*, to be defined momentarily. Additionally, we use a unitless ratio of bits-of-information to bits-of-information to define the quality of a binary code known as its *rate*.

[1] "Bit" is a portmanteau of "binary digit", attributed to John W. Tukey in [71].

Definition 2.1.2 (bit of information, rate of a code)**.** Given a set C of order $|C| = N$ and setting $k = \log_2(N)$, we say that C represents k *bits of information*. If C is a binary m-code, the *code rate* of C is defined as $\log_2(N)/m$.

The code rate is sometimes called the *information rate* (see, e.g., [44]). Since there are 2^m candidates for code words, the code rate is the ratio of encoded bits of information to available bits of information in a binary m-code. The conversation regarding the quantification of code qualities is not complete without addressing the notion of distance between code words, which is satisfied by a natural metric on a code space. The *Hamming distance*[2] between two finite sequences of the same length is the number of entries in which they disagree.

Definition 2.1.3 (Hamming distance, $\mathrm{d_H}$, $\mathrm{B_H}$)**.** The *Hamming distance* between two arbitrary sequences $x = (x_i)_{i=1}^m$ and $y = (y_i)_{i=1}^m$ is defined to be

$$\mathrm{d_H}(x, y) := \left|\{i : x_i \neq y_i\}\right|.$$

Definition 2.1.4 (Hamming ball, $\mathrm{B_H}$)**.** For $x \in \{a, b\}^m$ and $k \in \mathbb{N}$, the *Hamming ball* of radius k centered on x is the set

$$\mathrm{B_H}(x, k) := \{y \in \{a, b\}^m \mid \mathrm{d_H}(x, y) \leq k\}.$$

To see that $\mathrm{d_H}$ satisfies the triangle inequality, note that the Hamming distance between two sequences can be interpreted as the number of entries in one sequence that must be changed in order to obtain the other sequence. Then, for sequences x, y and z we can interpret $\mathrm{d_H}(x, y) + \mathrm{d_H}(y, z)$ as the number of entry-changes to turn x into y plus the number of entry-changes to turn y into z—a sum which cannot be less than $\mathrm{d_H}(x, z)$, which counts the needed changes to get from x to z.

Now, given a binary m-code, the set of Hamming distances between distinct pairs is a subset of $\{1, 2, \ldots, m\}$. As a finite ordered set, it contains its minimum value, which we refer to as the code's *minimum Hamming distance*. More generally,

Definition 2.1.5 (minimum $\mathrm{d}_\#$-distance, $\mathrm{mindist}_\#(X)$)**.** Given a metric $\mathrm{d}_\#$ defined on a set $\mathcal{X}$, the *minimum* $\mathrm{d}_\#$*-distance* of a finite set $X \subseteq \mathcal{X}$ is given by

$$\mathrm{mindist}_\#(X) := \min_{\substack{\mathbf{x},\mathbf{y} \in X \\ \mathbf{x} \neq \mathbf{y}}} \left\{\mathrm{d}_\#(\mathbf{x}, \mathbf{y})\right\}.$$

Remark 2.1.6. For a binary code C, the literature applies a variety of names to $\mathrm{mindist_H}(C)$, including *minimum code distance*, *minimum distance* (see, e.g., [44],[53]), and simply *distance* (see, e.g.,[44],[73]).

[2]Named for Richard W. Hamming, whose first published use of it as $D(x, y)$ appears to be [38].

2.1.2 Binary sequences as binary vectors

We can effectively embed a binary sequence space into a vector space by our choice of symbols, thus imposing structure on the sequences. For example, the $\{0,1\}$-binary sequences of length m may be seen as vectors in $\mathbb{R}^m$ by the natural embedding. A first consequence of such an embedding is the induced ability to meaningfully compare sequence terms to *zero*.

Definition 2.1.7 (Hamming weight, $\|\cdot\|_0$, k-sparse, support of a vector)**.** Given a vector space V and vector $\mathbf{x} \in V$, the *support* of $\mathbf{x}$ is given by $\operatorname{supp}(\mathbf{x}) := \{i : x_i \neq 0\}$. The *Hamming weight*[3] of $\mathbf{x}$ is the number of nonzero entries in $\mathbf{x}$, and is denoted

$$\|\mathbf{x}\|_0 := \big|\{i : x_i \neq 0\}\big| = \big|\operatorname{supp}(\mathbf{x})\big|\,.$$

A vector $\mathbf{x}$ is is called *k-sparse* if $\|\mathbf{x}\|_0 \leq k$.

Note that the Hamming distance on any vector space V can be expressed in terms of the support size of a difference vector—that is, $\mathrm{d_H}(\mathbf{x},\mathbf{y}) = \|\mathbf{x}-\mathbf{y}\|_0$ for $\mathbf{x},\mathbf{y} \in V$.

Throughout this manuscript, we will consider binary sequences as binary *vectors* (set in bold typeface, e.g., $\mathbf{x} \in \mathbb{R}^m$), usually assuming the natural embeddings without remark. To that end, the following list describes particular embeddings of binary code spaces into vector spaces that will play a major role in the chapters to come:

Embedding 1: $Q_n := \{-1,1\}^n$ in $\mathbb{R}^n$, the *Hamming cube*. We may view elements of the set of $\{-1,+1\}$-binary sequences of length n as vectors in $\mathbb{R}^n$ whose entries are either 1 or -1.

This choice of symbols is natural in the 1-bit compressed sensing setting, where binary sequences are commonly induced by a quantization that records only whether a measurement is positive or negative. "Random hyperplane tessellations", introduced in Section 2.2 and used extensively throughout this manuscript, model this regime. The points in $Q_n := \{-1,1\}^n \subset \mathbb{R}^n$ coincide with the vertices of an n-dimensional hypercube centered at the origin.

Embedding 2: $\Sigma^n := \{0,1\}^n$ in $\mathbb{R}^n$, the *Boolean cube*. Identifying the symbols 0 and 1 with their real counterparts produces the vertices of another cube in $\mathbb{R}^n$. When support size matters, we may use the notation $\Sigma^n_s \subset \Sigma^n$ to indicate the subset of exactly s-sparse vectors. One computational nicety of this embedding is that the inner product of two vectors in Σ^n provides the number of entries in which both vectors are nonzero. Note that we can shift and scale Σ^n onto Q_n via the invertible map $\mathbf{x} \to 2\mathbf{x} - 1$.

[3]The norm-like notation for the counting of non-zero coefficients is widely used, and very frequently accompanied by the gentle reminder/caveat that $\|\cdot\|_0$ is not a norm. This is most likely—at least in part—because it isn't.

Embedding 3: $\mathbb{Z}_2^n \equiv \mathrm{GF}(2)^n = \{0,1\}^n$**.** Alternatively, when we consider 0 and 1 as the elements of $\mathbb{Z}_2 \equiv \mathrm{GF}(2)$, the finite field of two elements, the set $\{0,1\}^n$ itself is a vector space. In Chapter 4 we shall see the induced structure underlying the search for binary block codes from group orbits.

2.1.3 Binary codes in the context of communications

In his 1948 treatise *A Mathematical Theory of Communication*, Claude Shannon introduces the notion of a "communication system" with the description "Schematic diagram of a general communication system" captioning the diagram reproduced here as Fig. 2.1. In this classic

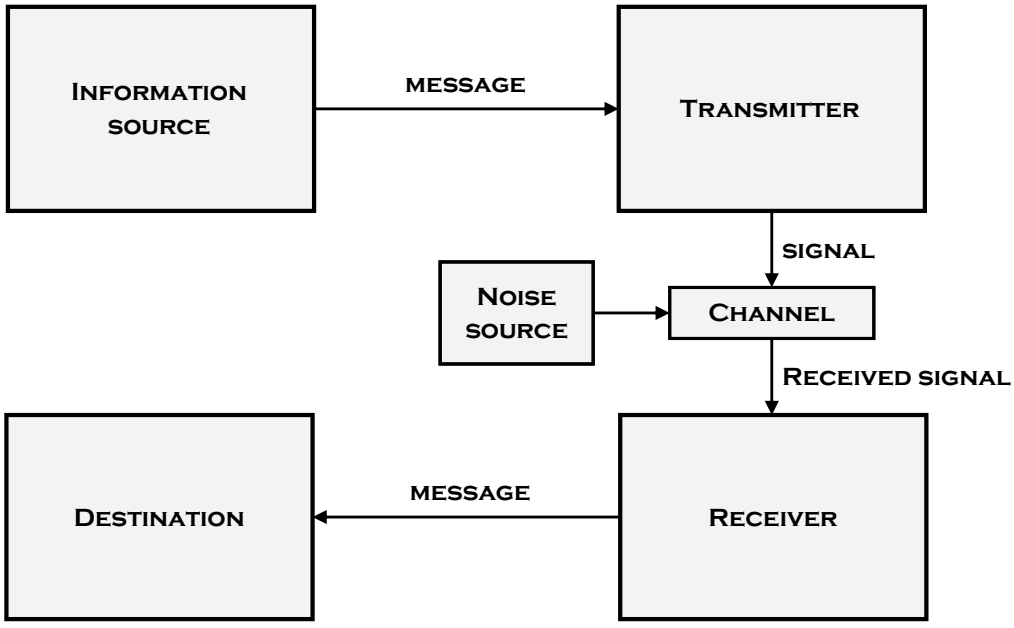

Figure 2.1: The Shannon communications model [71].

communications model, an *information source* produces a *message* that is necessarily selected from a collection of possible messages.[4] A *transmitter* converts the message into a *signal* to allow transmission via some medium—called the *channel*—to a *receiver*. The receiver, in turn, converts the *received signal* back into the original message for consumption by the *destination*. In a simple example, we may imagine a message in the form of a string of alphanumeric characters being converted by a computer into a sequence of 1's and 0's for

[4]For clarity, it may be important to note that the model does not account for a sense of *meaning* in a message—what matters is how well we can expect the *destination* to receive the intended message. By way of example, a person sending a text message to a friend may produce a string of characters on a device with the idea that the string will be perfectly replicated on the screen of another device. Whether the string of characters is what the texter *meant* to say does not factor into the model, nor does whether or not the friend interprets the message as intended.

digital transmission over a *binary channel* to another machine, which then *decodes* the binary sequence to produce the original string of characters on a screen for viewing.

Now, a channel may be subject to *noise*, which by definition has the potential to cause the received signal to be different than the (sent) signal. If we modify the preceding example to include a *noisy* binary channel, it is natural to wonder how the noise will affect the decoder's ability to produce the intended alphanumeric message from a perturbed binary signal. To be able to address this, it is necessary to know something about the distribution of errors among and within transmissions. Given a noisy binary channel, we shall assume an upper bound on the fraction of corrupted entries.

2.1.4 Robustness of a code against errors in transmission

In much the way that a few typos may not prevent perfect understanding of a typed message, a code may have the property that, for each of its code words, any small collection of errors is not enough to make it "unreadable." Given a binary code and a noise constraint in the form of an upper bound on the fraction of corrupted entries, we would like to know if every transmitted code word is guaranteed to result in a received signal that is uniquely associated with the intended code word. In this paradigm, noise is considered *adversarial*, as opposed to *random*; we are not asking for the *odds* that a certain fraction of errors results in a *decoding error*, we are asking if a certain fraction of errors *can* result in decoding error. We phrase our question more succinctly: is a given binary m-code *robust* against $\rho \cdot m$ errors induced by a particular channel?

To address the challenge, first note that having an error in an entry means, necessarily, one of two things: neither binary symbol appears in the entry (an *erasure error*), or the incorrect symbol appears in the entry (a *symbol error*). These may be called "erasures" and "errors" (see, e.g., [79]), but this may introduce ambiguity here. We shall instead use the terms *erasure* and *bit flip*, reserving *error* as the more general term to describe either.

Furthermore, we shall operate under the assumption that a given channel induces only one type of error and assume no special structure in the distribution of errors. Let us now examine how these conditions affect recoverability.

2.1.4.1 Errors and recoverability: a toy example

Take C to be a binary m-code containing exactly two elements, $\mathbf{x}$ and $\mathbf{y}$, with $k := \mathrm{d_H}(\mathbf{x}, \mathbf{y})$. We consider transmission over a noisy channel.

In an erasure channel: First, suppose we expect a number of erasures between 0 and $k-1$. We know, then, that least one of the distinguishing entries between $\mathbf{x}$ and $\mathbf{y}$ will survive transmission, and this is sufficient to indicate which vector was sent. On the other hand,

if there is a chance that k or more erasures can occur, then there is a chance that the k entries that distinguish $\mathbf{x}$ from $\mathbf{y}$ get erased. It follows that in such a case, C does not guarantee accurate recovery over this channel.

In a bit flip channel: Next, suppose that the channel admits no erasures, but instead offers an upper bound j on the possible quantity of bit flips. In this case, transmitting $\mathbf{x}$ or $\mathbf{y}$ over the channel yields a vector in our code space that is in the Hamming ball of radius j centered the signal. It follows that we can guarantee recovery if and only if $\mathrm{B_H}(\mathbf{x}, j)$ and $\mathrm{B_H}(\mathbf{y}, j)$ do not intersect—that is, if and only if $j < k/2$. Note that this implies that no binary m-code is robust against $\lceil n/2 \rceil$ bit flips.

We see, then, that whether a noisy channel induces erasures or bit flips, the question of guaranteed accurate recovery for a given binary m-code reduces to a question of the code's minimum Hamming distance.

Remark 2.1.8 (Justification for considering only bit-flipping channels)**.** It is evident that in comparing the robustness of two binary m-codes, we need not consider the type of error induced by a channel: If they have the same minimum Hamming distance, they are equally robust in either type of channel; if one has has a smaller minimum Hamming distance than the other, it cannot be more robust than the other. In light of this, we need only consider the minimum Hamming distance of a code when considering its robustness. Without qualitative loss, then, we shall restrict our attention to noisy channels that induce bit flips.

Remark 2.1.9 (Normalized robustness)**.** Additionally, the knowledge that a code is robust against, say, 100 bit flips, may not be particularly informative—how does that number compare to the length of a code word? It makes sense, then, that we consider a normalized robustness when comparing binary codes, instead noting the *fraction* of bit-flipped entries a code can withstand. Let $0 < \rho < 1$. Noting that a binary m-code C is robust against $\lfloor \rho m \rfloor$ bit flips if and only if $\lfloor \rho m \rfloor < \mathrm{mindist_H}(C)/2$, dividing each side of the inequality by m leads to the following definition:

Definition 2.1.10. Given noise parameter $\rho \in (0, 1/2)$ and binary m-code C, the statement that C is *robust against noise ratio* ρ means that

$$\frac{1}{2m}\mathrm{mindist_H}(C) \equiv \frac{1}{2}\mathrm{mindist_h}(C) > \frac{\lfloor \rho m \rfloor}{m}.$$

Note that the definition is satisfied if $\mathrm{mindist_h}(C)/2 > \rho$, since $\rho \geq \lfloor \rho m \rfloor / m$.

2.1.5 Code rate versus robustness

Before closing out this introduction to binary codes, it is worth noting that code rate and robustness are, more or less, competing desirable attributes. To see this, consider binary m-codes C_1 and C_2 such that $C_1 \subset C_2$. C_2 has more code words than C_1 and lives in the same

space, so it has a higher code rate. On the other hand, the containment also implies that $\mathrm{mindist}_{\mathrm{H}}(C_2) \leq \mathrm{mindist}_{\mathrm{H}}(C_1)$, which means C_1 is at least as robust as C_2, if not moreso.

2.2 Random hyperplane tessellations

The embedding described in Section 2.1.2 that identifies a binary sequence as an element of a vector space presupposes the existence of a binary sequence. We now address a source of such sequences that shall be instrumental in the construction of codes in Chapter 3: maps knowns as *hyperplane tessellations* (see, e.g., [63, 62]) obtained from random linear functionals. Casually speaking, a hyperplane tessellation is a partitioning of a vector space into convex sets whose collective boundaries take the form of a collection of hyperplanes.

Definition 2.2.1 (hyperplane tessellation, sign)**.** A *standard random hyperplane tessellation* is a map $\Phi : \mathbb{R}^n \to Q_m := \{-1, 1\}^m$ defined by $\mathbf{x} \mapsto \mathrm{sign}(A\mathbf{x})$, where $A \in \mathbb{R}^{m\times n}$ is a fixed random matrix with independent standard normal entries and $\mathbf{q} = \mathrm{sign}(A\mathbf{x}) \in Q_m$ is defined entrywise by $q_i = 1$ if $(A\mathbf{x})_i \geq 0$ and -1 otherwise.

The assignment $\mathrm{sign} : 0 \mapsto 1$ (instead of $0 \mapsto 0$) is a convention adopted here to ensure that the images of our finite subsets of $\mathbb{R}^n$ are indeed binary. This is largely a formality, since for a given $\mathbf{x} \in \mathbb{R}^n$, it is with probability zero that $(\Phi(x))_i = 0$ for some i.

As linear functionals, the row vectors of the matrix A in this definition induce hyperplanes which divide $\mathbb{R}^n$ into half spaces; specifically, letting $\mathbf{a}_i^\top$ denote the i-th row vector of A, the linear functional $\langle \mathbf{a}_i, \cdot \rangle$ is zero on the hyperplane normal to $\mathbf{a}_i$, positive on one side of that plane and negative on the other. The natural notion of this hyperplane separating a pair of a pair of vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ is encoded in sign of the product $\langle \mathbf{a}_i, \mathbf{x} \rangle \cdot \langle \mathbf{a}_i, \mathbf{y} \rangle$. We shall say that $\mathbf{a}_i$ *separates* a pair of vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ if $\mathrm{sign}\big(\langle \mathbf{a}_i, \mathbf{x} \rangle\big) \cdot \mathrm{sign}\big(\langle \mathbf{a}_i, \mathbf{y} \rangle\big) < 0$, which corresponds to $\big(\Phi(\mathbf{x})\big)_i \neq \big(\Phi(\mathbf{y})\big)_i$. It follows that the number of A-induced hyperplanes that separate $\mathbf{x}$ and $\mathbf{y}$ coincides with $\mathrm{d}_{\mathrm{H}}\big(\Phi(\mathbf{x}), \Phi(\mathbf{y})\big)$.

It should be clear, then, that given a point $\mathbf{x} \in \mathbb{R}^n$ and a standard random hyperplane tessellation Φ acting on $\mathbb{R}^n$, $\Phi(\mathbf{x}) = \Phi(c\mathbf{x})$ for all $c > 0$. By the same token, whether an A-induced hyperplane separates a pair $\mathbf{x}$ and $\mathbf{y}$ is independent of the magnitudes of $\mathbf{x}$, $\mathbf{y}$, and the hyperplane-inducing vector $\mathbf{a}_i$. It follows that recovery of a vector $\mathbf{x}$ from $\Phi(\mathbf{x})$ means recovering the direction of $\mathbf{x}$ without regard for magnitude.[5] As a consequence, we may describe signals as elements of Q_n or as elements of $\frac{1}{\sqrt{n}}Q_n \subset \mathbb{S}^{n-1}$, as convenience dictates.

[5] In fact, magnitude *can* be reasonably extracted from one-bit measurements. Reference [50] demonstrates two distinct reconstruction methods, each relying on replacing A with an augmented matrix $[A|b]$ (with $b = \mathbf{1}_m$ or random $b \sim \mathcal{N}\big(0, \tau^2 I_m\big)$) and declaring $x_{n+1} = 1$ for each received $\mathbf{x}$.

2.2.1 Random hyperplane tessellations, sparsity and compressed sensing

An important feature of random hyperplane tessellations is that they can have practical inverses, even though the maps are clearly not injective—the "secret" lies in the restriction of the preimage of Φ. One natural way to define a restricted set of signals is by requiring *sparsity*; a vector is *s-sparse* if no more than s of its entries are nonzero. To address how such a restriction is natural, let us consider the matrix A with normalized columns (in expectation).

2.2.1.1 Properties of the random matrix $A' := \frac{1}{\sqrt{m}}A$

Let A' be an $m \times n$ random matrix with independent Gaussian entries, each with mean 0 and variance $\frac{1}{m}$, so that A' is just a scaled copy of the matrix underlying Φ. In a landmark paper ([15]), Candès and Tao showed that with high probability, the columns of A' form a "restrictedly almost orthonormal system"—that is, a collection of vectors such that any small subcollection is an almost orthonormal system. To quantify "almost":

Definition 2.2.2 (Restricted isometry constants δ_s)**.** Given $m \times n$ matrix A and natural number $s \leq n$, the *restricted isometry constant* $\delta_s := \delta_s(A)$ is the least positive value satifying

$$(1 - \delta_s)\|\mathbf{x}\|_2^2 \leq \left\|A'\mathbf{x}\right\|_2^2 \leq (1 + \delta_s)\|\mathbf{x}\|_2^2 \tag{2.1}$$

for all s-sparse $\mathbf{x} \in \mathbb{R}^n$. In describing the matrix, we say that A satisfies the *restricted isometry property* (RIP) of order s with restricted isometry constant δ_s [28].

With high probability, a random $m \times n$ matrix A with independent Gaussian entries $a_{ij} \sim \mathcal{N}\big(0, \frac{1}{m}\big)$ satisfies the restricted isometry principle for meaningful constants. Now, a short, fat matrix A—even without the sign operation following it—is not invertible. But as a consequence of the restricted isometry property, each s-sparse $\mathbf{x} \in \mathbb{R}^n$ has the property that it is sparsest vector in $\{\mathbf{x}' : A\mathbf{x}' = A\mathbf{x}\}$ [15, 10], as well as, often enough, the smallest in ℓ_1 measure [16, 10, 12, 14, 25, 69]. In this sense, the random matrix A *induces* a restricted preimage, the collection of "sparse enough" vectors. Here, the question of "sufficient sparsity" is perhaps more naturally framed as in terms of the number of measurements needed to ensure accurate recovery of any s-sparse signal in $\mathbb{R}^n$; Rudelson and Vershynin [69] demonstrated that with overwhelming probability, given s, n, and $m = O(s\ln(\frac{n}{s}))$, a random $m \times n$ matrix A allows for perfect reconstruction of any s-sparse signal $\mathbf{x}$ in $\mathbb{R}^n$ from $A\mathbf{x}$ by the linear program sometimes refered to as *Basis Pursuit* [20],

$$\mathbf{x} = \arg\min\|A\hat{\mathbf{x}}\|_1 \quad \text{subject to } A\hat{\mathbf{x}} = A\mathbf{x}.$$

The scale hidden in the big-O notation is surprisingly non-immense: $m > 12s\ln(\frac{n}{2s})$ is sufficient engage an exponentially decaying rate of failure, with the probability that A uniformly satisfies the perfect reconstruction property bounded below by $1 - \frac{7}{2}\exp(-\frac{1}{18}[\sqrt{m} - \sqrt{12s\ln(\frac{n}{2s})}]^2)$ [69].

The field of *compressed sensing*[6] is directly interested in this quality of recovering, exactly or approximately, signals in such underdetermined settings (e.g., [8],[13],[24], [28]). *One bit* compressed sensing involves the recovery of sparse (or "essentially sparse", e.g., [62]) vectors from *binary* measurements, as in the case of standard random hyperplane tessellations. Here, the apparent undersampling includes the heavy quantization, but we may achieve similar results with $m \sim s\ln^2(n/s)$ in the noiseless case ([62]), $m \sim s\ln(2n/s)$ if subject to bit flips ([61])

Efforts in (one bit) compressed sensing (e.g., [11],[68],[78]), often rely on ℓ_1 minimization to recover sparse messages from their tessellated images, and these techniques are considered quite feasible. References [61] and [64] demonstrate similar feasible recovery with a generalized random hyperplane tessellation model, in which a nonlinear function f acts on the embedded coefficients before taking the sign, as in $(\widetilde{\Phi}(\mathbf{x}))_i = \operatorname{sign}\big(f(\langle \mathbf{a}_i, \mathbf{x}\rangle)\big)$.

A note: in the scenarios described above, the list of possible messages is restricted according to sparsity. Although the set Q_n is composed of non-sparse vectors,[7] there is a sense of "geometric sparsity" to the set which inspired the research for much of the following chapters; as noted in References [9] and [19], the property of sparsity may take a different form.

2.2.2 Predicting tessellation-induced separation of vectors

We have noted that the Hamming distance is a natural metric on binary sequences and vectors. In the context of random hyperplane tessellations, it is additionally useful to consider a metric which in some way measures the angular separation between vectors.

Definition 2.2.3 (normalized geodesic distance, $\mathrm{d_g}$)**.** Given $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, the *normalized geodesic distance* between $\mathbf{x}$ and $\mathbf{y}$ is given by

$$\mathrm{d_g}(\mathbf{x}, \mathbf{y}) := \frac{1}{\pi}\cos^{-1}\left(\frac{\langle \mathbf{x}, \mathbf{y}\rangle}{\|\mathbf{x}\|_2\|\mathbf{y}\|_2}\right).$$

Remark 2.2.4. In a sense, $\mathrm{d_g}$ is doubly normalized. Re-expressing the argument $\langle \mathbf{x}, \mathbf{y}\rangle / \|\mathbf{x}\|_2\|\mathbf{y}\|_2$ as $\left\langle \mathbf{x}/\|\mathbf{x}\|_2, \mathbf{y}/\|\mathbf{y}\|_2 \right\rangle$ illuminates vector normalization as the projection of $\mathbf{x}$ and $\mathbf{y}$ onto the Euclidean unit sphere; that sphere is the manifold implied by the adjective "geodesic". On that sphere, geodesic distance between points $\tilde{\mathbf{x}}$ and $\tilde{\mathbf{y}}$ coincides with the measure of angle between the vectors—that is, $\cos^{-1}\big(\langle \tilde{\mathbf{x}}, \tilde{\mathbf{y}}\rangle\big) \in [0, \pi]$. The normalizing factor $1/\pi$ thus converts the angular measure into a ratio in the unit interval.

Remark 2.2.5 (Normalized vs. non-normalized metrics)**.** Given $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, we have $\mathrm{d_H}(\mathbf{x}, \mathbf{y}) \in \{0, 1, \ldots, n\}$ and $\mathrm{d_g}(\mathbf{x}, \mathbf{y}) \in [0, 1]$. How we apply these metrics informs this choice of

[6] Also called *compressive sensing* ([46]) and *compressive sampling* ([13],[17])

[7] In fact, the set is as far from the entrywise sparse sets as possible, forming the vertices of the dual of the ℓ_1 ball.

normalizing one and not the other: the Hamming distance counts a finite set, whereas the normalized geodesic distance gives the angular separation of two vectors as a ratio. As a consequence of this choice, we shall see a normalizing factor in any expression containing both distances. If it were to become useful to use normalized Hamming distance, say, during a discussion of code rates or error rates, the notation $\mathrm{d_h}$ would be consistent with convention already established: indeed, the use of the lower case g for the smaller-valued distance and upper case H for the larger one is a choice intended to facilitate retention through mnemonics.

2.2.2.1 Hyperplane separation as a function of angular separation

By the definition of the random matrix $A \in \mathbb{R}^{m\times n}$, the row vectors $\mathbf{a}_i^\top$ are independent *(standard) Gaussian vectors*, which is to say, they are independent vector valued random variables and $\mathbf{a}_i \sim \mathcal{N}(\mathbf{0}, I_n)$ for each $i \in \{1, 2, \ldots, n\}$.

Given a pair points $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n \backslash \mathbf{0}_n$, let $\tilde{\mathbf{x}} := \mathbf{x}/\|\mathbf{x}\|_2$ and $\tilde{\mathbf{y}} := \mathbf{y}/\|\mathbf{y}\|_2$. We have already noted that the separation of $\mathbf{x}$ and $\mathbf{y}$ by a particular $\mathbf{a}_i$ is independent of the vector magnitudes—$\operatorname{sign}\big(\langle \mathbf{a}_i, \mathbf{x}\rangle\big) \cdot \operatorname{sign}\big(\langle \mathbf{a}_i, \mathbf{y}\rangle\big) < 0$ if and only if $\big\langle \mathbf{a}_i/\|\mathbf{a}_i\|_2, \tilde{\mathbf{x}}\big\rangle \cdot \big\langle \mathbf{a}_i/\|\mathbf{a}_i\|_2, \tilde{\mathbf{y}}\big\rangle < 0$. Now, let $E \subset \mathbb{S}^{n-1}$ be the subarc of the great circle containing $\tilde{\mathbf{x}}$ and $\tilde{\mathbf{y}}$ whose end points are $\pm\tilde{\mathbf{x}}$, and denote the subarc of E having endpoints $\tilde{\mathbf{x}}$ and $\tilde{\mathbf{y}}$ as E_0. With probability 1, the hyperplane induced by the $\mathbf{a}_i$ intersects E exactly once.

Since the the multivariate random variable $\mathbf{g} \sim \mathcal{N}(\mathbf{0}, I_n)$ is rotationally invariant, we have that the normalized vectors $\mathbf{a}_i/\|\mathbf{a}_i\|_2$ are uniformly distributed on the Euclidean sphere, $\mathbb{S}^{n-1}$. It follows that if E_1 and E_2 are subarcs of E having the same arc length,

$$\mathbb{P}\Big\{\mathbf{a}_i^\top \mathbf{z} \text{ for some } \mathbf{z} \in E_1\Big\} = \mathbb{P}\Big\{\mathbf{a}_i^\top \mathbf{z} \text{ for some } \mathbf{z} \in E_2\Big\},$$

since $\{\mathbf{q} \in \mathbb{S}^{n-1} : \mathbf{q}^\top \mathbf{z} \text{ for some } \mathbf{z} \in E_1\} \cong \{\mathbf{q} \in \mathbb{S}^{n-1} : \mathbf{q}^\top \mathbf{z} \text{ for some } \mathbf{z} \in E_2\}$. From this, it follows that the probability that $\mathbf{a}_i$ separates $\mathbf{x}$ and $\mathbf{y}$ is the ratio of the arc length of E_0 to the arc length of E, or $\cos^{-1}\big(\langle \tilde{\mathbf{x}}, \tilde{\mathbf{y}}\rangle\big)/\pi$—which is exactly $\mathrm{d_g}(\mathbf{x}, \mathbf{y})$.

By independence, the expected number of separating hyperplanes is also $\mathrm{d_g}(\mathbf{x}, \mathbf{y})$. More explicitly, given $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, and standard random hyperplane tessellation $\Phi : \mathbb{R}^n \to \mathbb{R}^m$, the expected *fraction* of entries in which the encoded vectors $\Phi(\mathbf{x})$ and $\Phi(\mathbf{y})$ differ is the normalized geodesic distance between the original vectors:

$$\mathbb{E}\left[\frac{1}{m}\mathrm{d_H}\big(\Phi(\mathbf{x}), \Phi(\mathbf{y})\big)\right] = \mathrm{d_g}(\mathbf{x}, \mathbf{y}) \equiv \frac{1}{\pi}\cos^{-1}\left(\frac{\langle \mathbf{x}, \mathbf{y}\rangle}{\|\mathbf{x}\|_2\|\mathbf{y}\|_2}\right). \tag{2.2}$$

We may reframe this simple connection between the normalized geodesic distance in the domain and Hamming distance in the image of a random hyperplane tessellation in terms of the component probabilities, for example, as in [33, Lemma 3.2]:

$$\mathbb{P}\Big\{\operatorname{sign}\big(\langle \mathbf{a}_i, \mathbf{x}\rangle\big) \neq \operatorname{sign}\big(\langle \mathbf{a}_i, \mathbf{y}\rangle\big)\Big\} = \frac{1}{\pi}\cos^{-1}\big(\langle \mathbf{x}, \mathbf{y}\rangle\big)$$

for $i \in \{1, 2, \ldots, n\}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{S}^{n-1}$.

Since the probabilities $\mathbb{P}\big\{(\Phi x)_i \neq (\Phi y)_i\big\}$ are independent and each equal to $\mathrm{d_g}(\mathbf{x}, \mathbf{y})$, the following corollary is immediate:

Corollary 2.2.6. *Given a standard random hyperplane tessellation $\Phi : \mathbb{R}^n \to \mathbb{R}^m$ and vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, the random variable $\mathrm{d_H}\big(\Phi(\mathbf{x}), \Phi(\mathbf{y})\big)$ follows the binomial distribution $B\big(m, \mathrm{d_g}(\mathbf{x}, \mathbf{y})\big)$.*

Of course, this fact is fundamental in formulating concentration bounds regarding hyperplane separation, such as found in [63],[62], and here in Chapter 3. To be explicit, given random variable $X \sim B(m, p)$, Hoeffding's inequality[8] provides the concentration bound $\mathbb{P}\big\{|X - mp| \leq \epsilon m\big\} \geq 1 - 2e^{-2\epsilon^2 m}$. It becomes clear, then, how well random hyperplane tessellations preserve normalized geodesic distance:

Corollary 2.2.7. *Given Φ, $\mathbf{x}$, and $\mathbf{y}$ as in Corollary 2.2.6 and $\epsilon > 0$,*

$$\mathbb{P}\left\{\left|\frac{1}{m}\mathrm{d_H}\big(\Phi(\mathbf{x}), \Phi(\mathbf{y})\big) - \mathrm{d_g}(\mathbf{x}, \mathbf{y})\right| \leq \epsilon\right\} \geq 1 - 2e^{-2\epsilon^2 m} \tag{2.3}$$

This subsection closes with a couple more observations regarding distances and hyperplane tessellations. Before moving on to examples of random binary codes, let us note an equivalence that arises when we apply a standard random hyperplane tessellation to a pair of vectors in Q_n; it turns out that we can express the expected Hamming distance between images under Φ in terms of the Hamming distance between the original vectors:

Lemma 2.2.8. *Given a standard random hyperplane tessellation $\Phi : \mathbb{R}^n \to \mathbb{R}^m$ and vectors $\mathbf{x}, \mathbf{y} \in Q_n$,*

$$\mathbb{E}\Big[\mathrm{d_H}\big(\Phi(\mathbf{x}), \Phi(\mathbf{y})\big)\Big] = \frac{m}{\pi}\cos^{-1}\left(1 - \frac{2}{n}\mathrm{d_H}(\mathbf{x}, \mathbf{y})\right).$$

Proof. For $x, y \in Q_n$, we relate the inner product with the Hamming distance:

$$\begin{aligned}\langle \mathbf{x}, \mathbf{y}\rangle &= \overbrace{(n - \mathrm{d_H}(\mathbf{x}, \mathbf{y}))}^{\#\text{ of matching entries}} - \overbrace{\mathrm{d_H}(\mathbf{x}, \mathbf{y})}^{\#\text{ of mismatches}} \\ &= n - 2\mathrm{d_H}(\mathbf{x}, \mathbf{y})\,.\end{aligned}$$

Noting that $\|x\|_2 = \sqrt{n}$ for all $x \in Q_n$, equation (2.2) becomes

$$\mathbb{E}\left[\frac{1}{m}\mathrm{d_H}\big(\Phi(\mathbf{x}), \Phi(\mathbf{y})\big)\right] = \frac{1}{\pi}\cos^{-1}\left(\frac{n - 2\mathrm{d_H}(\mathbf{x}, \mathbf{y})}{n}\right),$$

which yields the claimed equality upon multiplication by m, by the linearity of the expected value. □

[8] Wassily Hoeffding's (first) inequality ([41]) is more general than presented here, giving the upper tail bound $\mathbb{P}\Big\{\sum_{i=1}^m x_i - \mathbb{E}\big[\sum_{i=1}^m x_i\big] \geq \epsilon m\Big\} \leq e^{-2\epsilon^2 m}$ for sums of independent random variables $x_i \in [0, 1]$.

Remark 2.2.9. The underlying implied equality

$$\mathrm{d_g}(\mathbf{x},\mathbf{y}) = \frac{1}{\pi}\cos^{-1}\left(\frac{n-2\mathrm{d_H}(\mathbf{x},\mathbf{y})}{n}\right) \quad \text{for } \mathbf{x},\mathbf{y}\in Q_n \tag{2.4}$$

is one of a bounty of equivalences introduced by restrictions to different sets; Appendix A.1 provides tables and proofs of many such equivalences. These tables of "exchange rates" evolved rather organically in my notes, for example, when considering the minimum normalized geodesic distance of Q_n; since that distance is achieved by any pair $\mathbf{x},\mathbf{y}\in Q_n$ such that $\mathrm{d_H}(\mathbf{x},\mathbf{y})=1$, Eq. (2.4) above gives a quick result:

$$\mathrm{mindist_g}(Q_n) = \frac{1}{\pi}\cos^{-1}\left(\frac{n-2\mathrm{d_H}(\mathbf{x},\mathbf{y})}{n}\right) = \frac{1}{\pi}\cos^{-1}\left(1-\frac{2}{n}\right). \tag{2.5}$$

Remark 2.2.10 (Asymptotic results and families of codes)**.** In the context of the research presented in the coming chapters, random hyperplane tessellations exist in asymptotic regimes; that is to say, wherever the tool is used, the probability distributions relating to the images under random hyperplane tessellations are considered as the dimensions of both the domain and range grow without bound. In particular, the families of such maps considered take the form $\Phi:\mathbb{R}^n\to\mathbb{R}^{\lceil\beta n\rceil}$ for some fixed positive constant β.

Where the language of binary codes is relevant in these regimes, we are therefore considering *families of codes*. We will be interested in the information rates of these families, which is just the appropriately defined limit of the rates of the composing codes.

2.3 Block codes

Whereas a random hyperplane tessellation can be seen as the mapping of an arbitrary given set in $\mathbb{R}^n$ into a binary code space $Q_m\in\mathbb{R}^m$, a binary *block code* maps a whole code space $\{a,b\}^n$ into a (larger) code space $\{a',b'\}^m$. The dimension of the code space, m, is called the *block length*. The narrative illustration below (Section 2.3.1) follows the approach R. G. Gallager takes in his 1968 monograph ([30]) where the motivation begins with some specifying details among the components of Shannon communications model.

2.3.1 Motivation in a restricted communications model

As with the general model, we begin with output from an information source. This output—whatever its nature—is passed to a *source encoder* for conversion into a binary string. A *channel encoder* receives what appears to be a continuous stream of bits from the source encoder and processes it n bits at a time, thus treating the stream as a succession of binary *messages* of length n. The channel encoder in this model is a *block encoder*, which is to

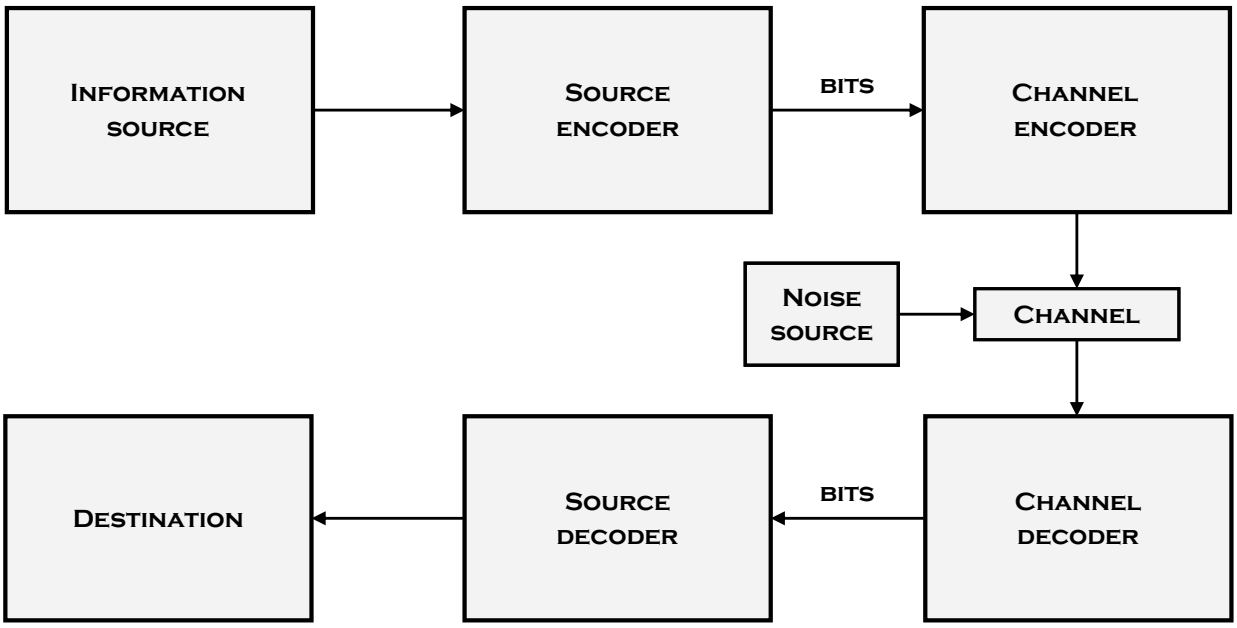

Figure 2.2: Restricted communications model from [30].

say it performs a block code assignment for each message; the resulting code words are its output. A (presumably) noisy channel carries the code word to a *channel decoder*, whose role it is to give the *source decoder* the same stream of bits that the channel encoder received; we call it a *block decoding error* any time the channel decoder fails to convert a received block into its originating n-bit message. The source decoder, naturally, acts as an inverse to the source encoder, and is responsible for converting the channel decoder's output into the original source output for the destination.

Remark 2.3.1 (From symbol-sequence mapping to $i \mapsto \mathbf{x}_i$)**.** In this model, the nature of the messages is such that the block code *necessarily* assigns code words to each of the 2^n, as there is no *a priori* knowledge of the structure of the input strings. It is worth noting that a convenient indexing of n-bit messages—and, by extension, an indexing of code words—arises from having a domain of $\{a, b\}^n$: reassigning the symbols to be the integers 0 and 1, the lexicographical ordering of the vectors may be read as the binary expansions of the naturally ordered integers 0 through $2^n - 1$. We may thus define a block code in terms of the image of these indices.

2.3.2 Illustrative examples: The glory and shortcomings of two random block codes

These examples provide context for addressing some of the quantifiable attributes of families of (block) codes. In addition to addressing asymptotic behaviors like information rates, error

rates and robustness, we will get a glimpse at how a block code's construction can affect the its inverse function (the source decoding). The two block codes incidentally provide examples of block code evaluation from the perspectives of a *probabalistic noise model* and an *adversarial noise model*, which are addressed in Remark 2.3.2.

2.3.2.1 Block codes from coin flipping

In 1973, R. G. Gallager demonstrated that *[t]he random coding bound is tight for the average code*[9][31]. There is more to unpack in that statement than fits the scope of this manuscript,[10] but the relevance to this example is that asymptotically, the expected error rate of a random binary code with information rate R vanishes exponentially with respect to the block size. To make this precise, let us clarify what is meant by a "random code" in this context.

Given $p \in (0,1)$, let ε be a Bernoulli random variable which takes the value 1 with probability p and 0 with probability $1-p$. Next, given natural numbers $n < m$, let C be a random $m \times 2^n$ matrix whose entries are given by independent copies of ε. Each realization of C provides a binary m-code of order 2^n whose code words are the columns $\{\mathbf{c}_i\}_{i=1}^{2^n}$ of the matrix, so we may consider C to be a binary code valued random variable. Furthermore, each realization induces a block code by the assignment $i \mapsto \mathbf{c}_{i+1}$, as described in Remark 2.3.1. In the language of [30], this interpretation of C makes it an *ensemble of* (m, R) *block codes*, where $R := \frac{n}{m}$ is the code rate.[11]

The bound-meeting ensembles of binary block codes in Gallager's aforementioned result have an underlying Bernoulli probability $p = \frac{1}{2}$ (see [30]), and the noisy channel is assumed to induce bit flips in entries independently with probability $\epsilon > 0$. Under these conditions, let i be a message in $0, 1^n$; then the expected value of the probability that a random block coding of i results in a decoding error is given by

$$\overline{P}_{\text{err},i} = \frac{g_\epsilon}{\sqrt{m}} \exp[-b_{\epsilon,R} \cdot m],$$

where g_ϵ and $b_{\epsilon,R}$ are positive constants depending only on ϵ and R. As noted earlier, the probability $\overline{P}_{\text{err},i}$ decays exponentially in the block length for a fixed rate.

As attractive as this family of codes may be, considering how well it appears to survive the channel, it bears a shortcoming. The matter of recovering the original stream is not addressed in the assignment of random code words to messages—we have guarantees on the recovery of the encoded signal, but decoding is left to a lookup table. The codes in the next example will have the capacity for efficient channel decoding, but we will see shortly that the rate suffers.

[9] The emphasized text is, in fact, the title of the paper.

[10] To begin with, the result does not restrict itself to *binary* block codes.

[11] In [30] and [31], this rate is given by $\ln(2^n)/m$, read "nats per bit". Our convention for rate as "bits per bit" does not qualitatively change the the result.

Remark 2.3.2 (Probabilistic vs. adversarial viewpoints)**.** We may describe our perspective in this example as one concerned about the likelihood of a decoding error, in the sense that however close our random code words may be, and however noise-corrupted our signals *could* become, the probabilistic qualities of the regime are such that—in expectation—we should have very few errors when we pick a random code. In contrast, the next example studies a particular random block code with a question of how well we might expect to pick a code that is "sufficiently robust" for a given channel—what is the probability that a code guarantees *zero* decoding errors? To make sense of this, we shall assume an upper bound on the fraction of bit flips a channel may induce in any bit sequence, rather than considering entry corruptions as independent random variables. Here, we consider the noise to be *adversarial* in nature, as though an actual adversary had access to the channel and would hand pick which bits to flip in order to cause the greatest disruption to our communications (within the "noise ratio" bound). As adversarial bit flips will induce a decoding error by pushing a signal closer to some "wrong" code word, robustness in this regime is measured by the minimum Hamming distance of a code—or, perhaps more intuitively, its minimum *normalized* Hamming distance.

2.3.2.2 Random hyperplane tessellations as bad *block* codes

As previously mentioned, random hyperplane tessellations provide another method of producing a random binary code—this is just a consequence of the definition. In fact, considering Q_n as a code space, a standard random hyperplane tessellation $\Phi : \mathbb{R}^n \to \mathbb{R}^m$ is automatically a block code. The conversation in Section 2.2.1 noted that Φ offers feasible recovery of its image, so the current example starts on that positive note. As it turns out, though, the robustness of the family of codes we are about to investigate decreases to zero asymptotically under the constraint of a fixed information rate.

To facilitate direct comparison with results in the previous example, let us fix an (asymptotic) code rate $R > 0$, inducing a family of block codes

$$\Phi_m : \mathbb{R}^{\lceil mR \rceil} \to \mathbb{R}^m$$

indexed by $m \in \mathbb{N}$. For a fixed m, set $n = \lceil mR \rceil$ so that $\left|\Phi_m(Q_n)\right| = 2^n$, note that $R \leq \frac{n}{m} \leq R + \frac{1}{m}$. We assume a noisy channel with an upper bound on the fraction of bit flips it imparts on any string it carries; let $\rho \in (0, \frac{1}{2})$ give this bound.

Recalling the discussion on what it means for a code to be robust against the noise ratio ρ (Remark 2.1.9 and Definition 2.1.10), a code C is considered successful in this regime if $\frac{1}{2}\text{mindist}_{\text{h}}(C) > \frac{\lfloor \rho m \rfloor}{m}$, or, equivalently, if $\text{mindist}_{\text{H}}(C) > 2\lfloor \rho m \rfloor$. An evaluation of the quality of the family of codes induced by a rate R, then, may be determined by the probability that the standard random hyperplane tessellation Φ_m embeds Q_n into $\mathbb{R}^m$ with sufficient minimum Hamming distance.

Suppressing the subscript on Φ_m for the time being, denote $\Phi(Q_n) =: C$ and let us consider

the distribution of the random variable $\delta_C := \text{mindist}_{\text{h}}(C)$. Applying Markov's inequality[12] to bound the probability of robustness yields

$$\mathbb{P}\left\{\frac{1}{2}\delta_C > \frac{\lfloor \rho m \rfloor}{m}\right\} \equiv \mathbb{P}\left\{m\delta_C > 2\lfloor \rho m \rfloor\right\} \leq \frac{m}{2\lfloor \rho m \rfloor}\mathbb{E}[\delta_C]\,, \tag{2.6}$$

leaving us to bound the expected value of the minimum d_{h}-distance of the tessellated Q_n. Since $\mathbb{E}\Big[\text{d}_{\text{H}}\big(\Phi(\mathbf{x}), \Phi(\mathbf{y})\big)\Big] = m\text{d}_{\text{g}}(\mathbf{x}, \mathbf{y})$ for $\mathbf{x}, \mathbf{y} \in Q_n$, it follows that

$$\mathbb{E}[\delta_C] \equiv \mathbb{E}\left[\min_{\substack{\mathbf{x},\mathbf{y}\in Q_n \\ \mathbf{x}\neq\mathbf{y}}} \text{d}_{\text{h}}\big(\Phi(\mathbf{x}), \Phi(\mathbf{y})\big)\right] \leq \min_{\substack{\mathbf{x},\mathbf{y}\in Q_n \\ \mathbf{x}\neq\mathbf{y}}} \text{d}_{\text{g}}(\mathbf{x}, \mathbf{y}) \equiv \text{mindist}_{\text{g}}(Q_n),$$

which, as noted in Eq. (2.5), is equal to $\frac{1}{\pi}\cos^{-1}\big(1 - \frac{2}{n}\big)$. Since this value decreases to zero in n (and m), we have our result: Given code rate $R > 0$, the family of block codes given by the standard random hyperplane tessellations

$$\Phi_m : \mathbb{R}^{\lceil mR \rceil} \to \mathbb{R}^m$$

has a vanishing robustness in this setting.

Remark 2.3.3 (A note on intuition: why this *should* have gone this way)**.** Since random hyperplane tessellations tend to conserve normalized geodesic distance as normalized Hamming distance,[13] the issue here is immediate: d_{h}-distance between Hamming neighbors in Q_n goes to zero as n goes to infinity.

Note, too, that before quantization, the map Φ is linear, and the nature of the underlying matrix A is such that any pair of its columns are orthogonal in expectation—their inner product is the sum of products of zero-mean independent random variables. Since A is a tall, thin matrix, it may also call to mind the submatrices of near isometry belonging to an RIP-matrix.

As Roman Vershynin states in [28], prior to demonstrating that the concentration of tall random matrices' singular values justifies the claim, "Tall matrices *should* act as approximate isometries."[14]

The rounding of A's image by Φ changes the the nature of the (scaled) near isometry from ℓ_2 distance preserving to the ebedding of d_{g} distances as d_{h} distance. The outcome, in either case, is that our signal set ends up as an approximate copy of the original cube, not taking advantage of all the extra space; in the next chapter, we develop methods which are intended to give our code access to that space.

[12] Markov's inequality states that, for nonnegative random variable X and positive constant a, $\mathbb{P}\{a \leq X\} \leq \mathbb{E}[X]/a$.

[13] (Recalling Section 2.2.2.1 and Corollary 2.2.7)

[14] Emphasis mine. Also, in context, Vershynin's statement is for the sake of heuristic—he also points out that such matrices *are* approximate isometries.

Chapter 3

A good code from random near-linear embeddings[†]

In light of the illustration in Section 2.3.2.2, we show the existence and explicit construction of a channel code of the Hamming cube Q_n that meets prescribed minimum distance requirements. The embedding takes advantage of the near isometry that a random hyperplane tessellation Φ provides between the normalized geodesic distance $\mathrm{d_g}$ and the normalized Hamming distance $\frac{1}{m}\mathrm{d_H}$ to effectively sparsify our signal.

3.1 Main result: A good code from random near-linear embeddings

Our embedding proceeds in two stages. In the first stage, an auxiliary ternary code of length M is constructed. In the second stage, the ternary code is converted into a binary code of length m by hyperplane tessellations.

3.1.1 The embedding Ψ

Stage 1. As a first step, we choose random subspaces of $\{-1, 0, 1\}^M$ with support size s. To this end, we obtain each support set $T \subset [\![M]\!]$ by performing Bernoulli experiments with a success probability that is chosen to guarantee at least s successes among M experiments.

[†]The mathematical content of this chapter appears as Section 3 of [6] (see Ch. 1 for details):
Bernhard G. Bodmann and Robert P. Mendez, "Binary block codes from Euclidean embeddings and random hyperplane tessellations," Proc. SPIE 10394, Wavelets and Sparsity XVII, 103940M (24 August 2017). DOI: http://doi.org/10.1117/12.2273917

The support set T is determined as a subset of the indices of the successes, and we repeat this procedure independently for L support sets.

For any index set J, let Σ_J denote the space of vectors in $\mathbb{R}^M$ supported on J. As a second step in this stage, for each support set T, we map an alphabet Q_{N_ρ} to a subset $\mathcal{X}_T$ in Σ_T; this is done in such a way that for each distinct pair $x, y \in \mathcal{X} := \bigcup_T \mathcal{X}_T$, we have $\mathrm{d_g}(x, y) \geq 3\rho$.

Stage 2. We perform a random hyperplane tessellation of the set $\mathcal{X}$ constructed in Stage 1 and obtain a Hamming distance bound on the embedded set given by $\mathrm{d_H}(x, y) \geq 2\lfloor \rho m \rfloor + 1$ for $x, y \in \Phi(\mathcal{X})$, $x \neq y$.

We shall use Ψ to denote the two-stage embedding described here.

Theorem 3.1.1. *Given $\rho \in (0, 1/9)$, $\alpha > 4$ and $\beta > 44$, set $N_\rho := \lfloor \frac{1}{\sin^2(\pi \sin^2(\frac{3\pi}{2}\rho))} \rfloor$ and let $n > 2N_\rho$. Let $\Psi : \{\pm 1\}^n \to \{\pm 1\}^m$ be an embedding based on random hyperplane tessellations as described in Section 3.1.1, setting $s := \lceil \alpha(n - N_\rho) \rceil$, $M := \lceil \beta s \rceil$, and $L := 2^{n - N_\rho}$.*

Then the probability that

$$\min_{\substack{x,y \in Q_n \\ x \neq y}} \mathrm{d_H}\big(\Psi(x), \Psi(y)\big) \geq 2\lfloor \rho m \rfloor + 1$$

is bounded below by

$$\left[1 - 2e^{\left(\log 2 - \frac{\alpha}{5}\right)l}\right] \cdot \left[1 - e^{\left(\log 4 - \frac{\alpha}{2}\log\frac{\beta}{22}\right)l}\right] \cdot \left[1 - e^{N_\rho \log 4 - \frac{\alpha l}{5}\sin^2\frac{3\pi\rho}{2}}\right] \cdot \left[1 - e^{n\log 4 - \frac{3\rho m}{20}}\right],$$

where $l := n - N_\rho$.

The proof of this theorem relies on the fact that the auxiliary ternary code described in the first stage of the embedding achieves a normalized geodesic separation of at least 3ρ with high probability; this fact is the content of Proposition 3.2.1, which Section 3.2 is devoted to proving. We may then make use of Lemma 3.3.1, which states that, with overwhelming probability, a random hyperplane tessellation of a set having 3ρ $\mathrm{d_g}$-separation provides an embedding into $\mathbb{R}^m$ with a Hamming separation of at least $2\lfloor \rho m \rfloor + 1$.

We precede the forthcoming propositions with a concentration bound for binomial random variables given by Corollary A.1.14 from Ref. [1], presented here as a lemma:

Lemma 3.1.2 (Corollary A.1.14 from Ref. [1])**.** *Given a binomial random variable X with mean μ, one has that $\mathbb{P}\{|X - \mu| > \epsilon\mu\} < 2\exp(-c_\epsilon \mu)$ for each $\epsilon > 0$, where $c_\epsilon := (1 + \epsilon)\log(1 + \epsilon) - \epsilon$.*

3.2 Auxiliary code separation: Stage 1

In this section, we produce an auxiliary code that meets a desired separation requirement. To the point, the proof of the following proposition demonstrates that the auxiliary ternary

code described in Section 3.1.1 has a normalized geodesic separation of at least 3ρ.

Proposition 3.2.1. *Given $\rho \in (0, 1/9)$, $\alpha > 4$ and $\beta > 44$, let $N_\rho := \left\lfloor \frac{1}{\sin^2(\pi \sin^2(\frac{3\pi}{2}\rho))} \right\rfloor$ and let $n > 2N_\rho$ and $l := n - N_\rho$.*

Let $\Psi : \{\pm 1\}^n \to \{\pm 1\}^m$ be an embedding based on random hyperplane tessellations as described in Section 3.1.1, setting $s := \lceil \alpha l \rceil$, $M := \lceil \beta s \rceil$, and $L := 2^{n-N_\rho} = 2^l$. Then the associated auxiliary ternary code $\mathcal{X}$ described as an embedding of $\{\pm 1\}^n$ into $\{\pm 1, 0\}^M$ achieves

$$\min_{\substack{x,y \in \mathcal{X} \\ x \neq y}} \mathrm{d_g}(x, y) \geq 3\rho$$

with probability not less than

$$\left[1 - 2e^{(\log 2 - \frac{\alpha}{5})l}\right] \cdot \left[1 - e^{\log 4 - \frac{\alpha}{2} \log \frac{\beta}{22})l}\right] \cdot \left[1 - e^{N_\rho \log 4 - \frac{\alpha l}{5} \sin^2 \frac{3\pi\rho}{2}}\right]$$

The lower bound in the statement of the proposition is the product of lower bounds of the probabilities of three events; we now provide those bounds in a sequence of propositions. For clarity and to facilitate forthcoming substitutions, the statements of these supporting propositions are written so that the variables are consistent with the supported proposition and with one another.

3.2.1 Controlling support size

We first show that our method of randomly selecting support sets provides, with high probability, a collection of sets each containing sufficiently many elements. Given that this event occurs, then for each set of M Bernoulli experiments yielding an index set T', a support set T of size s is chosen uniformly at random from T'. The vectors X'_j described below are thus nominally truncated to the vectors $X_j \in \mathcal{X} \cap \{0, 1\}^M$.

Proposition 3.2.2. *[Randomly selected supports of sufficient size] Given $l \in \mathbb{N}$, $\alpha > 4$, and $\beta > 44$, define $s := \lceil \alpha l \rceil$ and $M := \lceil \beta s \rceil$. For each $j \in [\![2^l]\!]$, let $X'_j \in \{0, 1\}^M \subset \mathbb{R}^M$ have its entries determined by an independent Bernoulli process with underlying probability $\frac{2s}{M} \approx \frac{2}{\beta}$. Then*

$$\mathbb{P}\left\{ \min_j \left\| X'_j \right\|_1 \geq s \right\} \geq 1 - 2\exp\left((\log 2 - \alpha/5)l\right).$$

Proof. Fixing $j \in [\![2^l]\!]$ and noting that $\mathbb{E}\left\|X'_j\right\|_1 = 2s$,

$$\begin{aligned}
\mathbb{P}\left\{\left\|X'_j\right\|_1 < s\right\} &\leq \mathbb{P}\left\{\left|\left\|X'_j\right\|_1 - 2s\right| > 2s - s\right\} \\
&\overset{\text{lem. 3.1.2}}{\leq} 2\exp(-c_{\frac{1}{2}} \cdot 2s) \\
&\leq 2\exp\left(-\frac{s}{5}\right) \\
&\leq 2\exp\left(-\frac{\alpha}{5}l\right).
\end{aligned}$$

Taking the union bound with 2^l vectors introduces the summand $l \log 2$ into the exponential:

$$\mathbb{P}\left\{\min_j \left\|X'_j\right\|_1 < s\right\} \overset{\text{union bound}}{\leq} 2^l \cdot 2\exp\left(-\frac{\alpha}{5}l\right) = 2\exp\left(l\log 2 - \frac{\alpha}{5}l\right).$$

The proposition is proven by taking the complementary probability. □

3.2.2 Event 2: The minimum $\mathrm{d_g}$-separation of the set of vectors determined by the sets *without* truncation is at least $\frac{1}{3}$

Next, we show that the set of "Bernoulli vectors" X'_j described above have adequate separation. The following lemma demonstrates that this separation implies, for sufficiently small ρ, that the vectors with support sets culled from the Bernoulli success sets will inherit adequate separation. We denote the support of a vector x as $\mathrm{supp}(x)$.

Lemma 3.2.3. *Given natural numbers $s < M$ and vectors $x', y' \in \{0,1\}^M \subset \mathbb{R}^M$ each having at least s nonzero entries and such that $\langle x', y'\rangle \leq s/2$, let $x, y \in \{0,1\}^M$ such that $\mathrm{supp}(x) \subset \mathrm{supp}(x')$ and $\mathrm{supp}(y) \subset \mathrm{supp}(y')$. If each of x and y have at least s non-zero entries, then*

$$\mathrm{d_g}(x, y) \geq \frac{1}{3}.$$

It is an obvious consequence that $\mathrm{d_g}(x, y) \geq 3\rho$ for $\rho \in [0, 1/9]$.

Proof. Assume the hypothesis, and note that $\langle x, y\rangle \leq \langle x', y'\rangle \leq \frac{s}{2}$. We have

$$\begin{aligned}
\mathrm{d_g}(x, y) := \frac{1}{\pi}\cos^{-1}\left(\frac{\langle x, y\rangle}{\|x\|_2\|y\|_2}\right) &\geq \frac{1}{\pi}\cos^{-1}\left(\frac{\langle x, y\rangle}{s}\right) \\
&\geq \frac{1}{\pi}\cos^{-1}\left(\frac{s}{2s}\right) = \frac{1}{3};
\end{aligned}$$

□

Proposition 3.2.4. *Under the same conditions of the preceding proposition (Prop 3.2.2), assume that* $\min_j \left\| X'_j \right\|_1 \geq s$. *Then*

$$\mathbb{P}\left\{ \text{mindist}_{\text{g}}(\{X'_j\}_{j=1}^{2^l}) > \frac{1}{3} \right\} \geq 1 - \exp\left(- \left(\frac{\alpha}{2} \log \frac{\beta}{22} - \log 4 \right) l \right),$$

and by the conditions on α *and* β, $\frac{\alpha}{2} \log \frac{\beta}{22} - \log 4 > 0$.

Proof. By the conditions of the hypothesis and Lemma 3.2.3, it is sufficient to show that $\left\langle X'_j, X^{j'} \right\rangle \leq s/2$ for all distinct j, j'.

For $j \neq j' \in [\![2^l]\!]$, we may consider $\left\langle X'_j, X'_{j'} \right\rangle$ as a binomial random variable with underlying probability $(\frac{2s}{M})^2$ and sample size M. Noting that $\mathbb{E}\left[\left\langle X'_j, X'_{j'} \right\rangle \right] = M \cdot \frac{4s^2}{M^2} = \frac{4s^2}{M}$,

$$\begin{aligned}
\mathbb{P}\left\{ \left\langle X'_j, X'_{j'} \right\rangle > \frac{s}{2} \right\} &\leq \mathbb{P}\left\{ \left| \left\langle X'_j, X'_{j'} \right\rangle - \frac{4s^2}{M} \right| > \frac{s}{2} - \frac{4s^2}{M} \right\} \\
&= \mathbb{P}\left\{ \left| \left\langle X'_j, X'_{j'} \right\rangle - \frac{4s^2}{M} \right| > \left(\frac{M}{8s} - 1 \right) \frac{4s^2}{M} \right\} \\
&\overset{\text{lem. 3.1.2}}{\leq} 2 \exp\left(- \left(\frac{M}{8s} \log \frac{M}{8s} - \frac{M}{8s} \right) \cdot \frac{4s^2}{M} \right) \\
&\leq 2 \exp\left(-\frac{s}{2} \left(\log \frac{M}{8s} - 1 \right) \right) \\
&\leq 2 \exp\left(-\frac{\alpha l}{2} \log \frac{\beta}{22} \right).
\end{aligned}$$

Applying the union bound, the probability that $\left\langle X'_j, X'_{j'} \right\rangle > \frac{m}{2}$ for some $j \neq j' \in [\![2^l]\!]$ is bounded above by $\binom{2^l}{2} \cdot 2 \exp\left(-\frac{\alpha l}{2} \log \frac{\beta}{22} \right) < \exp\left(-\frac{\alpha l}{2} \log \frac{\beta}{22} + l \log 4 \right)$. Factoring and taking the complementary probability completes the proof. □

3.2.3 Applying the random hyperplane tessellation

As previously discussed, the error parameter ρ induces an upper bound on the dimension of a Hamming cube that admits desirable separation traits under random hyperplane tessellation. Here, we give an explicit bound N_ρ on that dimension and show that for $n \leq N_\rho$, a random

hyperplane tessellation of Q_n provides an auxiliary code which *itself* provides a good code under random hyperplane tessellation with overwhelming probability.

Proposition 3.2.5 (Embedded $\mathrm{d_g}$-separation)**.** *Let $\rho \in [0, \frac{1}{6})$ and $\Phi : \mathbb{R}^n \to Q_s$ be a random hyperplane tessellation. Then if $n \leq [\sin^2(\pi \sin^2(\frac{3\pi}{2}\rho))]^{-1}$, we have*

$$\mathbb{P}\left\{ \min_{\substack{x,y \in Q_n \\ x \neq y}} \mathrm{d_g}\big(\Phi(x), \Phi(y)\big) \geq 3\rho \right\} \geq 1 - \exp\left(n \log 4 - \frac{1}{5} s \sin^2\big(3\pi\rho/2\big) \right).$$

Additionally, $\frac{s}{n} > \frac{1}{2\rho^2}$ is sufficient to ensure $n \log 4 - \frac{1}{5} s \sin^2\big(3\pi\rho/2\big) < 0$.

Proof. The inequality $\mathrm{d_g}\big(\Phi(x), \Phi(y)\big) \geq 3\rho$ is equivalent to

$$\mathrm{d_H}\big(\Phi(x), \Phi(y)\big) \geq \frac{s}{2}(1 - \cos(3\pi\rho)),$$

the righthand side of which equals $s \sin^2(3\pi\rho/2)$ by a half-angle identity. On the other hand, the condition $n \leq [\sin^2(\pi \sin^2(\frac{3\pi}{2}\rho))]^{-1} \equiv 2[1 - \cos(2\pi \sin^2(\frac{3\pi}{2}\rho))]^{-1}$ provides the following lower bound on the $\mathrm{d_g}$-separation of Q_n:

$$\begin{aligned}
\mathrm{mindist_g}(Q_n) :=& \frac{1}{\pi} \cos^{-1}\big(1 - 2\mathrm{mindist_H}(Q_n)/n\big) \\
=& \frac{1}{\pi} \cos^{-1}\big(1 - 2/n\big) \\
\geq& \frac{1}{\pi} \cos^{-1}\left(1 - \left[1 - \cos\left(2\pi \sin^2\big(3\pi\rho/2\big)\right)\right]\right) \\
=& 2\sin^2(3\pi\rho/2) \quad \text{(since } \rho < 1/6\text{)}.
\end{aligned}$$

It follows that $\mathbb{E}\Big[\mathrm{d_H}\big(\Phi(x), \Phi(y)\big)\Big] \geq 2s \sin^2(3\pi\rho/2)$ for distinct $x, y \in Q_n$.

Next, we bound the probability that a pair of encoded vectors fails to meet the minimum distance requirement:

$$\begin{aligned}
&\mathbb{P}\Big\{\mathrm{d_g}\big(\Phi(x), \Phi(y)\big) < 3\rho\Big\} \\
&\qquad = \ \mathbb{P}\Big\{\mathrm{d_H}\big(\Phi(x), \Phi(y)\big) < s \sin^2(3\pi\rho/2)\Big\} \\
&\qquad \leq \ \mathbb{P}\Big\{\Big|\mathrm{d_H}\big(\Phi(x), \Phi(y)\big) - \mathrm{d_g}(x,y)\, s\Big| > \mathrm{d_g}(x,y)\, s - s \sin^2(3\pi\rho/2)\Big\} \\
&\qquad \leq \ \mathbb{P}\Big\{\Big|\mathrm{d_H}\big(\Phi(x), \Phi(y)\big) - 2s \sin^2(3\pi\rho/2)\Big| > s \sin^2(3\pi\rho/2)\Big\} \\
&\qquad \overset{\text{lem. } 3.1.2}{\leq} \ 2\exp\Big(-c_{\frac{1}{2}} \cdot 2s \sin^2(3\pi\rho/2)\Big),
\end{aligned}$$

where $c_{\frac{1}{2}} = \frac{3}{2}\log\frac{3}{2} - \frac{1}{2} \approx \frac{1}{9.2}$. Substituting $1/10$ for $c_{\frac{1}{2}}$ and taking the union bound over distinct pairs in Q_n yields

$$\begin{aligned}
\mathbb{P}\big\{\mathrm{mindist}_{\mathrm{g}}(\Phi Q_n) \geq 3\rho\big\} &\geq 1 - \tbinom{2^n}{2} \cdot 2\exp\left(-\frac{1}{5}s\sin^2\big(3\pi\rho/2\big)\right) \\
&= 1 - \frac{1}{2}2^n(2^n-1)\cdot 2\exp\left(-\frac{1}{5}s\sin^2\big(3\pi\rho/2\big)\right) \\
&> 1 - 2^{2n}\exp\left(-\frac{1}{5}s\sin^2\big(3\pi\rho/2\big)\right) \\
&= 1 - \exp\left(n\log 4 - \frac{1}{5}s\sin^2\big(3\pi\rho/2\big)\right).
\end{aligned}$$

Finally, we solve the inequality $0 > n\log 4 - \frac{1}{5}s\sin^2\big(3\pi\rho/2\big)$ in terms of $\frac{s}{n}$ to obtain the condition

$$\frac{s}{n} > \frac{10\log 2}{\sin^2(\frac{3\pi}{2}\rho)}.$$

The expression $10\log 2/\sin^2(\frac{3\pi}{2}\rho)$ is bounded above by $\frac{1}{2\rho^2}$ on an interval containing $(0, \frac{1}{6}) \ni \rho$, and so $\frac{s}{n} > \frac{1}{2\rho^2}$ implies the necessary condition. □

We now have sufficient mathematical results to prove auxiliary code separation claim, Proposition 3.2.1, but we shall first provide an explicit construction for the code in order to show existence.

3.2.4 Assembling $\mathcal{X} = \bigcup_T \mathcal{X}_T$.

Recall that for a set $T \subset [\![M]\!]$, Σ_T is the collection of vectors in $\mathbb{R}^M$ supported on T. In the second step of obtaining our auxiliary ternary code, we declare $\mathcal{X}$ to be the union of vector sets $\mathcal{X}_{T_1}, \mathcal{X}_{T_2}, \ldots, \mathcal{X}_{T_L}$, where each set $\mathcal{X}_{T_j} \subset \Sigma_{T_j}$ is the image of the alphabet Q_{N_ρ} under some map. Additionally, we claim that $\{\mathcal{X}_{T_j}\}_{j=1}^L$ is produced in such a way that the set $\bigcup_j \mathcal{X}_{T_j}$ is separated by at least 3ρ in normalized geodesic distance.

We make the sets $\mathcal{X}_{T_j}$ explicit by first defining, for each $T \in \{T_j\}_{j=1}^L$, the map $\iota_T : \mathbb{R}^s \to \Sigma_T$ as the natural inclusion of $\mathbb{R}^s$ into $\mathbb{R}^M$ onto the support given by T. We set $X_T := \iota_T(\Phi(Q_{N_\rho}))$, and in the proof below, demonstrate that this assignment provides the desired separation.

Proof of Proposition 3.2.1. Recall that the variables in the supporting propositions are consistent with those in the main proposition and with one another. Thus, we assume the parameters ρ, α, β, N_ρ, and n are given according to the hypothesis of Proposition 3.2.1, that the induced parameters $l := n - N_\rho$, $s := \lceil \alpha l \rceil$, $M := \lceil \beta s \rceil$ and $L := 2^l$ follow, and that each time we access a supporting proposition, the variables in that proposition are taken coincident with those having these defined names.

We must demonstrate that the ternary auxiliary code $\mathcal{X}$ obtained in the first stage of producing the embedding Ψ has a minimum $\mathrm{d_g}$-separation of at least 3ρ with probability not less than $p_1 p_2 p_3$, where

$$p_1 = 1 - 2\exp\left(\left(\log 2 - \frac{\alpha}{5}\right) l\right) = \mathbb{P}\{\text{Event 1}\} \text{ (see Prop. 3.2.2)}$$

$$p_2 = 1 - \exp\left(\left(\log 4 - \frac{\alpha}{2}\log\frac{\beta}{22}\right) l\right) = \mathbb{P}\big\{\text{Event 2}|\text{Event 1}\big\} \text{ (see Prop. 3.2.4)}$$

$$p_3 = 1 - \exp\left(N_\rho \log 4 - \frac{\alpha l}{5}\sin^2\frac{3\pi\rho}{2}\right) = \mathbb{P}\{\text{Event 3}\} \text{ (see Prop. 3.2.5).}$$

The construction of the set $\mathcal{X}$ requires that each of $L = 2^l$ support-inducing Bernoulli processes has at least s successes; according to Proposition 3.2.2, this occurs with probability not less than p_1 under the constraints given by our parameters. Provided this occurs, the likelihood that the induced vector set $X' := \{X'_j\}_{j=1}^L$ satisfies $\mathrm{mindist_g}(X') \geq \frac{1}{3} \geq 3\rho$ is bounded below by p_2 in Proposition 3.2.4. By the definition of conditional probability, it follows that Event 1 and Event 2 both happen is at least $p_1 p_2$.

For each $j \in [\![L]\!]$, define $T'_j := \mathrm{supp}(X'_j)$ and let $T_j \subset T'_j$ be support set of size s. By Lemma 3.2.3, the induced set $X := \{X_j\}_{j=1}^L \subset \{0,1\}^M$ given by $\mathrm{supp}(X_j) = T_j$ also satisfies the separation bound, $\mathrm{mindist_g}(X) \geq 3\rho$. Thus, the described method of obtaining s-sized support sets for the L vectors in $X \subset \{0,1\}^M$ in such a way that no two of the implied vectors violate our minimum separation requirement succeeds with probability not less than $p_1 p_2$.

Let $\mathcal{T} := \{T_j\}_{j=1}^L$.

Next, for each $T \in \mathcal{T}$, define $\mathcal{X}_T := \iota_T(\Phi(Q_{N_\rho}))$ as in the narrative immediately preceding this proof. By Proposition 3.2.5, the near-linear embedding of Q_{N_ρ} into Q_s by the random hyperplane tessellation Φ has a 3ρ $\mathrm{d_g}$-separation with at least probability p_3. The isometry ι_T preserves distance, so $\mathrm{mindist_g}(\mathcal{X}_T) = \mathrm{mindist_g}(\Phi(Q_{N_\rho}))$ for each $T \in \mathcal{T}$.

By independence, the probability that $\mathcal{T}$ provides a 3ρ $\mathrm{d_g}$-separating support and Φ provides a 3ρ $\mathrm{d_g}$-separated embedding is bounded below by the product $p_1 p_2 p_3$. It remains to show that $\mathcal{X}$ meets this separation requirement whenever this happens.

Assume that $\mathcal{X}$ is obtained from a successful construction of $\mathcal{T}$ and Φ, and suppose $x, y \in \mathcal{X}$ are distinct vectors having possibly common supports T_{j_x} and T_{j_y}, respectively, with $j_x, j_y \in [\![L]\!]$. If $T_{j_x} \cap T_{j_y}$ is empty, then $\langle x, y\rangle = 0$ and $\mathrm{d_g}(x,y) = \frac{1}{\pi}\cos^{-1}(0) = \frac{1}{2} > 3\rho$. If $T_{j_x} = T_{j_y}$, then the $\mathrm{d_g}$-separation of $\mathcal{T}$ implies $j_x = j_y$, from which the separation granted by Φ provides $\mathrm{d_g}(x,y) \geq 3\rho$.

Suppose, then, that T_{j_x} and T_{j_y} intersect but do not agree, and set $J := T_{j_x} \cap T_{j_y}$. As the sum of $|J|$ products $x_i \cdot y_i \in \{\pm 1\}$, the inner product $\langle x, y\rangle$ is bounded above by $|J|$;

when this bound is met, x and y agree on the intersection of their supports. It follows that $\langle x, y\rangle = \langle X_{j_x}, X_{j_y}\rangle$ and so $\mathrm{d_g}(x,y) = \mathrm{d_g}\big(X_{j_x} X_{j_y}\big)$, which is bounded below by 3ρ. We conclude that $\mathrm{mindist_g}(\mathcal{X}) \geq 3\rho$, and the proposition is proven. $\square$

3.3 Stage 2 and the embedding Ψ

3.3.1 Auxiliary code separation implies Hamming distance of hyperplane tessellation

Lemma 3.3.1 (Embedded $\mathrm{d_H}$-separation from $\mathrm{d_g}$-separation)**.** *Let $\rho > 0$ and $\Phi : \mathbb{R}^M \to Q_m$ be a standard random hyperplane tessellation. If $\mathcal{X} \subset \mathbb{R}^M$ has a minimum $\mathrm{d_g}$-separation of at least 3ρ, then*

$$\mathbb{P}\left\{ \min_{\substack{x,y\in\mathcal{X}\\ x\neq y}} \mathrm{d_H}\big(\Phi(x),\Phi(y)\big) \geq 2\rho m + 1 \right\} \geq 1 - \exp\left(2\log|\mathcal{X}| - \frac{3\rho m}{20}\right).$$

Proof. Let $x, y \in \mathcal{X}$ be distinct, and assume that $\mathrm{mindist_g}(\mathcal{X}) \geq 3\rho$. Since normalized geodesic distance is invariant under scaling of the arguments, we may assume without loss of generality that x and y are unit vectors.

Since $\mathbb{P}\big\{(\Phi x)_i \neq (\Phi y)_i\big\} = \mathrm{d_g}(x,y)$, the random variable $\mathrm{d_H}(\Phi x, \Phi y)$ follows the binomial distribution $B(m, \mathrm{d_g}(x,y))$. We consider the probability that Φ *fails* to sufficiently separate x and y:

$$\begin{aligned}
\mathbb{P}\big\{\mathrm{d_H}(\Phi x,\Phi y) \leq 2\rho m\big\} &\leq \mathbb{P}\Big\{\big|\mathrm{d_H}(\Phi x,\Phi y) - \mathrm{d_g}(x,y)\, m\big| > \mathrm{d_g}(x,y)\, m - 2\rho m\Big\} \\
&= \mathbb{P}\Big\{\big|\mathrm{d_H}(\Phi x,\Phi y) - 3\rho m\big| > \rho m\Big\} \\
&\overset{\text{lem. 3.1.2}}{\leq} 2\exp\left(-c_{\frac{1}{3}}\cdot 3\rho m\right),
\end{aligned}$$

with $c_{\frac{1}{3}} = \frac{4}{3}\log\frac{4}{3} - \frac{1}{3} \approx \frac{1}{19.9}$. We conclude that $\mathbb{P}\Big\{\mathrm{d_H}\big(\Phi(x),\Phi(y)\big) \geq 2\rho m + 1\Big\} \geq 1 - 2\exp(3\rho m/20)$.

Next, we apply the union bound over $\binom{|\mathcal{X}|}{2} = \frac{1}{2}|\mathcal{X}|\,(|\mathcal{X}|-1)$ distinct pairs in $\mathcal{X}$:

$$\begin{aligned}
\mathbb{P}\big\{\mathrm{mindist_H}(\Phi(\mathcal{X})) \geq 2\rho m + 1\big\} &\geq 1 - \frac{1}{2}|\mathcal{X}|\,(|\mathcal{X}|-1)\cdot 2\exp\left(-\frac{3\rho m}{20}\right) \\
&> 1 - |\mathcal{X}|^2 \exp\left(-\frac{3\rho m}{20}\right) \\
&= 1 - \exp\left(2\log|\mathcal{X}| - \frac{3\rho m}{20}\right),
\end{aligned}$$

and the proof is complete. □

With this lemma, we are now prepared to prove Theorem 3.1.1.

3.3.2 Proof of Ψ's success rate

Proof of Theorem 3.1.1. Let $\mathcal{X}$ denote the auxiliary code in Stage 1 of the construction of Ψ and Φ denote the random hyperplane tessellation invoked in Stage 2. According to Proposition 3.2.1, the parameters given in the theorem imply that $\mathcal{X}$ has a minimum $\mathrm{d_g}$-separation of 3ρ with probability

$$\left[1 - 2e^{\left(\log 2 - \frac{\alpha}{5}\right)l}\right] \cdot \left[1 - e^{\left(\log 4 - \frac{\alpha}{2}\log\frac{\beta}{22}\right)l}\right] \cdot \left[1 - e^{N_\rho \log 4 - \frac{\alpha l}{5}\sin^2\frac{3\pi\rho}{2}}\right]$$

Provided this occurs, Lemma 3.3.1 gives

$$\begin{aligned}\mathbb{P}\left\{\min_{\substack{x,y\in Q_n\\ x\neq y}} \mathrm{d_H}\big(\Psi(x),\Psi(y)\big) \geq 2\rho m + 1\right\} &= \mathbb{P}\left\{\min_{\substack{x,y\in \mathcal{X}\\ x\neq y}} \mathrm{d_H}\big(\Phi(x),\Phi(y)\big) \geq 2\rho m + 1\right\} \\ &\geq 1 - \exp\left(2\log(2^n) - \frac{3\rho m}{20}\right) \\ &\geq 1 - \exp\left(n\log 4 - \frac{3\rho m}{20}\right).\end{aligned}$$

Taking the product of the bound on the probability that $\mathcal{X}$ has adequate separation and the bound on the probability that the hyperplane tessellation Φ provides adequate separation provides the claimed bound. □

3.4 Conclusion

The intermediate embedding of the Hamming cube into a random constant weight binary code permitted the random hyperplane tessellation to induce the desired separation of points. Additional, incomplete results suggust we can improve the robustness against noise up to $\sim .16$ by an alternate method of selecting the intermediate code.

Chapter 4

Binary Parseval frames from group orbits[†]

The focus of this chapter is dominantly algebraic and frame-theoretic in nature, though we are still in pursuit of "good binary codes." Joining this shift from the analytic perspective are two subtler transitions that occur at this point in the manuscript:

1. In this chapter, binary **only** means 0's and 1's, and those numbers now satisfy $1 + 1 = 0$—the underlying field has changed.

2. Whereas the conversation up to this point has increasingly focused on asymptotics, this chapter's examples and applications are decidedly finite.

We proceed with some background and comparisons before setting definitions and terminology.

4.1 Background: Frames and binary frames

A *finite frame* is simply a spanning family in a vector space, with the underlying field $\mathbb{F}$ often specified with a modifier. In the case of *binary* frames, which we take to be finite frames by definition, that field is the Galois field with two elements, denoted here as GF(2) or $\mathbb{Z}_2$. Binary frames have much in common with their real and complex counterparts, which have been studied extensively in mathematics and engineering [18, 51, 52].

[†]The content of this chapter appears as [59] (see Ch.1): Robert P. Mendez, Bernhard G. Bodmann, Zachery J. Baker, Micah G. Bullock and Jacob E. McLaney, "Binary Parseval frames from group orbits," Linear Algebra and its Applications, Volume 556, 1 November 2018, pps 265-300

As a spanning set, a frame for $\mathbb{F}^n$ necessarily contains at least n vectors; if it exactly meets that minimum, it is simply a basis for the vector space. As such, we typically think of frames as including linear dependencies, and, in fact, make use of that property. Such a frame may be used to *expand* any given vector into a linear combination of frame vectors, of course, without the assertion of uniqueness. Nonetheless, for real and complex *Parseval* frames, there is a standard choice of expansions having the property that the coefficients in the expansion of a vector can be calculated efficiently, and recovering a vector from these coefficients is also straight forward. With an appropriate definition of a *binary* Parseval frame, this property holds, as well [5]. Now, in the former case, the coefficients are computed by taking inner products of the frame vectors with the vector to be expanded; $\mathbb{Z}_2^n$ does not admit an inner product [5], but the less restrictive *dot product* in place of the inner product endows binary Parseval frames with the same "coefficient computing" qualities as their real and complex counterparts [39, 43].

Where distinguishing qualities among frames are to be made, equivalence classes become useful in isolating particular qualities. In the real and complex cases, a number of equivalence relations have been used. Frames may be *similar*, for example, and Parseval frames are subject to unitary equivalence [40], projective unitary equivalence [22], and switching equivalence [7, 34]. As holds true for real and complex Parseval frames, each set of unitarily equivalent binary Parseval frames can be identified with a corresponding Gramian [5, Proposition 4.8]. This identification of Gramians with classes of frames extends to the three frame equivalence relations applied here (as will be shown), and so the Gramians of binary Parseval group frames[1] become a central focus of this chapter. Even with coarser partitions, the quantities of representatives grows quickly with the frame size and dimension, as demonstrated in Section 4.4; For exhaustive lists of various equivalence classes of binary Parseval frames (for the lowest dimensions), see in [2] and [5].

For all the similarities between binary frame theory and that of real and complex frames, there are, of course, differences. One striking distinction is in the characterization of their *Gram* matrices;[2] the Gram matrices of real or complex Parseval frames are characterized as symmetric or Hermitian idempotent[3] matrices. In the binary case, these properties are insufficient, and must be augmented with the condition of having at least one non-zero diagonal entry [2]. This condition is equivalent to having at least one *odd* column vector, meaning that a column contains an odd number of 1's. The underlying reason is the range of the Gram matrix of *any* Parseval frame consists precisely of its eigenspace corresponding to eigenvalue one [37]—a consequence of idempotence—which in the binary case necessarily contains only odd vectors [2]. If none of the column vectors were odd, then the span could not satisfy this requirement.

[1] (given in Definition 4.2.8)

[2] The i, k entry of the Gram matrix of a frame $\{f_j\}_{j\in J}$ is the inner product of f_i and f_k (or dot product, in the binary frame case).

[3] Recall, a matrix (or any map) G is *idempotent* if $G = G^2$. For the sake of completeness: a *symmetric* real matrix G satisfies $G = G^\top$, whereas a *Hermitian* complex matrix G satisfies $G = G^*$.

We shall continue comparing the structure of binary Parseval frames with their real or complex counterparts throughout the chapter, specializing to frames obtained from the orbit of a vector under a group representation.

Here, we study binary Parseval group frames, with special emphasis on the structure of the Gramians associated with them. Our first main result is that a binary Parseval frame is obtained from the action of a group if and only if its Gramian is in the group algebra.

For such group frames, the Gram matrix is shown to be a binary linear combination of elements of the right regular representation, thus associated with a binary function on the group. This function provides a concise characterization of binary Parseval group frames, allowing us to find structural constraints for such frames. We use these constraints to catalogue coarser equivalence classes of binary Parseval frames obtained from group representations. We specialize further to abelian groups and deduce more specific design constraints.

We leave the study and applications of non-abelian groups and their associated binary group frames for future work. In addition, one may use finite fields other than the Galois field with two elements. Here, the motivation for code design was a natural reason to restrict the discussion to binary numbers.

4.2 Preliminaries

Unless otherwise noted, the vectors and matrices in this paper are over the field $\mathbb{Z}_2$ containing the two elements 0 and 1. We write I_k to indicate the $k \times k$ identity matrix over $\mathbb{Z}_2$, occasionally suppressing the subscript when the dimension would not otherwise be noted. We shall refer to the number of nonzero entries of a vector $x \in \mathbb{Z}_2^n$ as the *weight* of x (sometimes written $\|x\|_0$), and we say that x is *odd* or *even* if it has an odd or even number of entries equal to 1, respectively. These labels extend naturally to the columns and rows of a matrix viewed as column and row vectors (for example, we may refer to an *odd* or *even column* of a matrix). The expression $T \in M_n(\mathbb{Z}_2)$ means that T is an $n \times n$ matrix over $\mathbb{Z}_2$, and, in keeping with the notation of real or complex frames, we denote the transpose of a binary matrix T as T^*.

Additionally, we may suppress the range of indices on sums and sets for simplicity of notation, as in writing $\sum_j c_j f_j$ for $\sum_{j \in J} c_j f_j$ or $\{f_j\}$ for $\{f_j\}_{j \in J}$ when the index set J is clear from the context.

4.2.1 Binary Frames

Although the dot product as defined below has the appearance of an inner product, it fails to be positive definite, so it is not: Note that taking the dot product of a (non-zero) even vector with itself gives zero.

Definition 4.2.1 ($\langle\cdot,\cdot\rangle$, the dot product on $\mathbb{Z}_2^n$)**.** We define the bilinear map $\langle\cdot,\cdot\rangle : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2$, called the *dot product* on $\mathbb{Z}_2^n$, by

$$\left\langle \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}, \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \right\rangle := \sum_{i=1}^{n} a_i b_i,$$

compactly expressed as $\langle a, b\rangle = b^* a$ for vectors $a = [a_i]_{i=1}^n, b = [b_i]_{i=1}^n$. Consistent with the language of inner products, we say that two vectors in $\mathbb{Z}_2^n$ are *orthogonal* if their dot product is equal to zero.

We began Section 4.1 by describing frames, in general, as spanning sets; in fact, real and complex frames are typically defined in terms of the inner product, motivated by a generalization of the "reconstruction identity" (4.1) below. The fact that a frame in that setting spans its ambient vector space is a characterizing feature of finite frames; The absence of an inner product motivated the authors of [5] to define binary frames according to that characterizing feature, and, as narrated earlier, with the selection of the dot product to replace the inner product, many of the desirable qualities of the classic frames followed.

Definition 4.2.2 (Binary frame, binary Parseval frame)**.** Let $\mathcal{F} = \{f_j\}_{j\in J}$ be a family of vectors in $\mathbb{Z}_2^n$, indexed by a finite set J. If $\mathcal{F}$ spans $\mathbb{Z}_2^n$, we call $\mathcal{F}$ a (binary) *frame*; if $\mathcal{F}$ satisfies the *reconstruction identity*

$$x = \sum_{j\in J} \langle x, f_j\rangle f_j \quad \text{for all } x \in \mathbb{Z}_2^n, \tag{4.1}$$

we say that $\mathcal{F}$ is a *binary Parseval frame*.

For other choices of indefinite bilinear form on vector spaces over $\mathbb{Z}_2$ and associated frames, see [43]. Here, we restrict ourselves to the canonical choice, the dot product.

Since any family of vectors satisfying (4.1) necessarily spans $\mathbb{Z}_2^n$, each Parseval frame $\{f_j\}_{j\in J}$ for $\mathbb{Z}_2^n$ is in fact a frame, and the index set necessarily has the size $|J| \geq n$. For classification purposes it is useful to introduce equivalence relations among Parseval frames as in [5].

Definition 4.2.3 (Unitary binary matrices, unitary equivalence, switching equivalence)**.** We say that a binary $n \times n$ matrix U is *unitary* if $UU^* = U^*U = I_n$. Given vector families $\mathcal{F} := \{f_j\}_{j\in J}$ and $\mathcal{F}' := \{f'_j\}_{j\in J}$ in $\mathbb{Z}_2^n$, we say that $\mathcal{F}$ is *unitarily equivalent* to $\mathcal{F}'$ if there exists a unitary $U \in M_n(\mathbb{Z}_2)$ such that $f'_j = Uf_j$ for all $j \in J$; we say that $\mathcal{F}$ is *switching equivalent* to $\mathcal{F}'$ (written $\mathcal{F} \cong_{\text{sw}} \mathcal{F}'$) if there exists a unitary $U \in M_n(\mathbb{Z}_2)$ and a permutation σ on J such that $f'_j = Uf_{\sigma(j)}$ for all $j \in J$.

By definition, unitary equivalence is a refinement of switching equivalence. The nature of unitary and permutation matrices makes verifying that these are both equivalence relations

a straightforward exercise. Now, from this point forward, we focus on frames indexed by elements of a group; in this context, a restricted version of switching equivalence becomes useful—one which limits the permutations to the subset preserving the group structure. In short, we require the permutations to be group automorphisms.

Definition 4.2.4 (Automorphic switching equivalence)**.** Let Γ be a group; we denote the automorphisms of Γ by $\mathrm{Aut}(\Gamma)$. Given Γ-indexed vector families $\mathcal{F} := \{f_g\}_{g\in\Gamma}$ and $\mathcal{F}' := \{f'_g\}_{g\in\Gamma}$, we say that $\mathcal{F}$ and $\mathcal{F}'$ are *automorphically switching equivalent* (written $\mathcal{F} \cong_{\mathrm{aut}} \mathcal{F}'$) if there exist a unitary $U \in M_n(\mathbb{Z}_2)$ and an automorphism $\sigma \in \mathrm{Aut}(\Gamma)$ such that $f_g = Uf'_{\sigma(g)}$ for all $g \in \Gamma$.

4.2.2 Operators associated with a frame

The following four operators are defined in the same manner as for finite frames over the fields $\mathbb{R}$ and $\mathbb{C}$. In each definition, $\mathcal{F} = \{f_j\}_{j\in J}$ is assumed only to be a frame for $\mathbb{Z}_2^n$.

Definition 4.2.5 ($\Theta_{\mathcal{F}}$, the analysis operator,$\Theta^*_{\mathcal{F}}$, the synthesis operator)**.** We denote the space of $\mathbb{Z}_2$-valued functions on a set J by $\mathbb{Z}_2^J$. The *analysis operator* for $\mathcal{F}$ is the map $\Theta_{\mathcal{F}} : \mathbb{Z}_2^n \to \mathbb{Z}_2^J$ given by $(\Theta_{\mathcal{F}}x)(j) = \langle x, f_j\rangle$. The adjoint of $\Theta_{\mathcal{F}}$, also called *synthesis operator*, maps $h \in \mathbb{Z}_2^J$ to $\Theta^*_{\mathcal{F}}h = \sum_{j\in J} h(j)f_j$.

Definition 4.2.6 ($S_{\mathcal{F}}$, the frame operator)**.** The *frame operator* for $\mathcal{F}$ is the $n \times n$ matrix

$$S_{\mathcal{F}} := \Theta^*_{\mathcal{F}}\Theta_{\mathcal{F}}.$$

Remark 4.2.7. We note that the reconstruction identity (equation (4.1)) may be written as $x = \Theta^*_{\mathcal{F}}\Theta_{\mathcal{F}}x$. The reconstruction property of a Parseval frame $\mathcal{F}$ for $\mathbb{Z}_2^n$ is equivalent to $S_{\mathcal{F}} = I_n$.

Definition 4.2.8 ($G_{\mathcal{F}}$, the Gramian)**.** The *Gramian* for $\mathcal{F}$, usually called the *Gram matrix* if $J = \{1, 2, \ldots, k\}$, is the linear map $G_{\mathcal{F}} : \mathbb{Z}_2^J \to \mathbb{Z}_2^J$

$$G_{\mathcal{F}} := \Theta_{\mathcal{F}}\Theta^*_{\mathcal{F}}.$$

Taking $\delta_j(k) = 1$ if $k = j$ and $\delta_j(k) = 0$ otherwise, $\{\delta_j\}_{j\in J}$ is the standard basis for $\mathbb{Z}_2^J$, and we use matrix notation to write $(G_{\mathcal{F}})_{i,j} = \langle\Theta_{\mathcal{F}}\Theta^*_{\mathcal{F}}\delta_j, \delta_i\rangle = \langle f_j, f_i\rangle$. It follows from the symmetry of $\langle\cdot,\cdot\rangle$ that $(G_{\mathcal{F}})_{i,j} = (G_{\mathcal{F}})_{j,i}$, and thus $G_{\mathcal{F}}$ is symmetric (i.e., $G_{\mathcal{F}} = G^*_{\mathcal{F}}$). Further, if $\mathcal{F}$ is a binary Parseval frame, then the Gramian is idempotent:

$$G^2_{\mathcal{F}} = (\Theta_{\mathcal{F}}\Theta^*_{\mathcal{F}})(\Theta_{\mathcal{F}}\Theta^*_{\mathcal{F}}) = \Theta_{\mathcal{F}}\underbrace{(\Theta^*_{\mathcal{F}}\Theta_{\mathcal{F}})}_{=S_{\mathcal{F}}=I_n}\Theta^*_{\mathcal{F}} = \Theta_{\mathcal{F}}\Theta^*_{\mathcal{F}} = G_{\mathcal{F}}\,. \tag{4.2}$$

For each of these matrices, we may suppress the subscript if doing so does not cause ambiguity, simply writing Θ ,Θ^*, S, and G.

4.2.3 Group frames for $\mathbb{Z}_2^n$

Recall that, given a finite group Γ and a vector space V, a *representation* of Γ on V is a group homomorphism

$$\rho : \Gamma \to \mathrm{GL}(V),$$

where $\mathrm{GL}(V)$ denotes the general linear group of V. In such a case, we say that Γ *acts on* V by ρ, and for any group element g we may interchangeably write $\rho(g)$ as ρ_g. We shall refer to the elements of $\{\rho_g\}_{g\in\Gamma}$ as the *matrices of the representation* ρ, or simply as representation matrices. Further, if each of the matrices ρ_g is unitary, then we call the representation itself unitary.

In the context of complex Hilbert spaces, given a finite group Γ, a *group frame* generated by Γ is any frame $\{f_g\}_{g\in\Gamma}$ that satisfies $\rho_g f_h = f_{gh}$ for all $g, h \in \Gamma$, for some representation ρ of Γ. If that representation is unitary, the frame is the orbit of a single vector [76]; it is this idea of a group generating a frame from a single vector that provides the basis of our definition.

Definition 4.2.9 (Binary Parseval group frame, Γ-frame)**.** Given a natural number n and a group Γ acting on the vector space $\mathbb{Z}_2^n$ by a representation ρ, let $\mathcal{F} := \{\rho_g f\}_{g\in\Gamma}$ denote the orbit of a vector $f \in \mathbb{Z}_2^n$ under ρ. If $\mathcal{F}$ spans $\mathbb{Z}_2^n$, then it is a frame which we call a *binary group frame*. If $\mathcal{F}$ is a Parseval frame, we say that it is a *binary Parseval group frame*. For a given group Γ, we abbreviate the description "group frame generated by Γ" as Γ-frame [75]. We shall index frame vectors by their inducing group elements, so that $f_e := f$ and $f_g := \rho(g)f = \rho_g f$ for $g \in \Gamma$.

We begin with examples of frames generated with groups of size 27 acting on $\mathbb{Z}_2^9$. These examples show that depending on the choice of f_e, a unitary group representation may lead to an orbit that is a Parseval frame or just a frame.

Examples 4.2.10 (Two binary cyclic $\mathbb{Z}_{27}$-frames)**.** Let $\Gamma = \mathbb{Z}_{27}$ be the group of integers $\{0, 1, \ldots, 26\}$ with addition modulo 27. Let S_9 be the cyclic shift on $\mathbb{Z}_2^9$, so for each canonical basis vector e_i with $i \leq 8$, $S_9 e_i = e_{i+1}$ and $S_9 e_9 = e_1$. Since S_9 is a permutation matrix, the map $\rho : i \mapsto S_9^i$ is a homomorphism from Γ to $\mathrm{GL}(\mathbb{Z}_2^9)$. Choosing $f_e = [1\,0\,1\,1\,1\,1\,1\,1\,0]^*$ gives that $\{f_j\}_{j\in\Gamma}$ spans $\mathbb{Z}_2^9$, but $\Theta_{\mathcal{F}}^*\Theta_{\mathcal{F}} \neq I_9$, so $\mathcal{F}$ is a frame but not Parseval.

Moreover, choosing $f_e = e_1$ shows that $\{f_i\}_{i\in\Gamma}$ with $f_i = S_9^i e_1 = e_{1+i(\mathrm{mod}\,9)}$ and $e_0 \equiv e_9$ repeats the sequence of canonical basis vectors three times. Consequently, the synthesis operator is $\Theta_{\mathcal{F}}^* = [I_9\, I_9\, I_9]$ and $\Theta_{\mathcal{F}}^*\Theta_{\mathcal{F}} = I_9$, so $\mathcal{F}$ is Parseval.

An exhaustive search of all Parseval frames obtained from group orbits under the action of $\mathbb{Z}_{27}$ on $\mathbb{Z}_2^9$ reveals that up to unitary equivalence, the second example is the only case of a Parseval $\mathbb{Z}_{27}$-frame for $\mathbb{Z}_2^9$. Such an exhaustive search is made feasible by methods developed in Section 4.3.4. In a preceding paper, the linear dependence among repeated

frame vectors, as is exhibited in the frame having synthesis operator $[I_9\, I_9\, I_9]$, has been called *trivial redundancy* [5]; In the next example, we show that another group of the same size generates frames as well as Parseval frames without the occurrence of repeated vectors in either case.

Example 4.2.11 (Two binary Gabor frames)**.** Let $a, b \in \mathrm{GL}(\mathbb{Z}_3^3)$ and the suggestively named $\rho_a, \rho_b \in \mathrm{GL}(\mathbb{Z}_2^9)$ be defined by

$$a := \begin{bmatrix} 1&0&0\\0&1&1\\0&0&1 \end{bmatrix}, \quad b := \begin{bmatrix} 1&1&0\\0&1&0\\0&0&1 \end{bmatrix}, \quad \rho_a := \begin{bmatrix} I_3 & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & X & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & Y \end{bmatrix}, \quad \rho_b := \begin{bmatrix} \mathbf{0} & I_3 & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & I_3\\ I_3 & \mathbf{0} & \mathbf{0} \end{bmatrix},$$

where $\mathbf{0}$ is the 3×3 matrix of zeros, $X = \begin{bmatrix} 0&0&1\\1&0&0\\0&1&0 \end{bmatrix}$, and $Y = X^2$.

The group generated by a and b under matrix multiplication is the nonabelian finite *Heisenberg-Weyl* group modulo 3, denoted HW_3. From the fact that products of powers of a and b give all upper triangular ternary matrices whose diagonal entries are fixed at 1, one can deduce that this group has order 27 (see also [70]). The matrices ρ_a and ρ_b generate a group isomorphic to HW_3 and have been chosen such that setting $\rho(a) := \rho_a$ and $\rho(b) := \rho_b$ extends to an isomorphism $\rho : HW_3 \to \mathrm{GL}(\mathbb{Z}_2^9)$. For compactness of notation, we designate a third group element[4] c and corresponding $\rho_c \in \mathrm{GL}(\mathbb{Z}_2^9)$

$$c := \begin{bmatrix} 1&0&1\\0&1&0\\0&0&1 \end{bmatrix} \quad \text{and} \quad \rho_c := \rho(c) = \begin{bmatrix} X & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & X & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & X \end{bmatrix},$$

and order the elements of HW_3 in the following sequence:

$$\begin{gathered} e,\ a,\ a^2,\ b,\ ab,\ a^2b,\ b^2,\ ab^2,\ a^2b^2,\\ c,\ ac,\ a^2c,\ bc,\ abc,\ a^2bc,\ b^2c,\ ab^2c,\ a^2b^2c,\\ c^2,\ ac^2,\ a^2c^2,\ bc^2,\ abc^2,\ a^2bc^2,\ b^2c^2,\ ab^2c^2,\ a^2b^2c^2. \end{gathered}$$

Choosing $f_e = [1\,1\,0\,1\,0\,0\,0\,0\,0]^*$ and $f'_e = [1\,1\,0\,1\,1\,0\,1\,0\,0]^*$ induces HW_3-frames $\{f_e\}$ and $\{f'_e\}$ whose synthesis operators $\Theta_1^* := [f_e|f_a|f_{a^2}|\cdots|f_{a^2b^2c^2}]$ and $\Theta_2^* := [f'_e|f'_a|f'_{a^2}|\cdots|f'_{a^2b^2c^2}]$ are given in Figure 4.1. One may verify that $\{f'_g\}_{g\in HW_3}$ is the only Parseval frame of the pair by calculating the corresponding frame operators.

4.2.4 Regular representations and group frames

Constructing a faithful unitary representation of a finite group Γ is always possible; if Γ has order k and given a k-dimensional vector space V, one can find a collection of $k \times k$ permutation matrices $\{P_g\}_{g\in\Gamma} \subset \mathrm{GL}(V)$ that form a group isomorphic to Γ. This is just a result of Cayley's theorem for groups based on the left or right regular representation, as given below. The challenge, of course, is to find vector spaces of *smaller* dimension carrying

[4]Note that $\{e, c, c^2\}$ is the center of HW_3.

$$\Theta_1^* = \begin{bmatrix}
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0\\
1&1&1&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0\\
1&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&1&1&0&1&0&0&0&0&1&1&0\\
0&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&1&1\\
0&0&1&0&0&0&0&1&1&0&1&0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&1\\
0&0&0&1&1&0&1&0&0&0&0&0&0&1&1&0&1&0&0&0&0&1&0&1&0&0&1\\
0&0&0&1&0&1&0&0&1&0&0&0&1&1&0&1&0&0&0&0&0&0&1&1&0&1&0\\
0&0&0&0&1&1&0&1&0&0&0&0&1&0&1&0&0&1&0&0&0&1&1&0&1&0&0
\end{bmatrix}$$

$$\Theta_2^* = \begin{bmatrix}
1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0\\
1&1&1&1&1&1&1&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&1&1&1&1&1&1&1&1&1\\
1&0&1&1&0&0&1&0&1&0&1&1&0&0&1&0&1&1&1&1&0&0&1&0&1&1&0\\
1&1&0&0&1&0&1&1&0&1&0&1&1&0&0&1&0&1&0&1&1&0&0&1&0&1&1\\
0&1&1&0&0&1&0&1&1&1&1&0&0&1&0&1&1&0&1&0&1&1&0&0&1&0&1\\
1&0&0&1&1&0&1&1&0&0&1&0&0&1&1&0&1&1&0&0&1&1&0&1&1&0&1\\
0&0&1&1&0&1&1&0&1&1&0&0&1&1&0&1&1&0&0&1&0&0&1&1&0&1&1\\
0&1&0&0&1&1&0&1&1&0&0&1&1&0&1&1&0&1&1&0&0&1&1&0&1&1&0
\end{bmatrix}$$

Figure 4.1: Synthesis operators of two binary Gabor frames (see Example 4.2.11)

a unitary representation and vectors whose orbits under the group action form a Parseval frame.

With this in mind, we recall that the *regular representations* of a finite group Γ over a field $\mathbb{K}$ act on $\mathbb{K}^\Gamma$, the vector space of $\mathbb{K}$-valued functions on Γ; the *left* regular representation $\Lambda = \{\Lambda_g\}_{g\in\Gamma}$ and *right* regular representation $R = \{R_g\}_{g\in\Gamma}$ act on $\varphi : \Gamma \to \mathbb{K}$ according to

$$\Lambda_g\varphi : h \mapsto \varphi(g^{-1}h) \quad \text{and} \quad R_g\varphi : h \mapsto \varphi(hg)$$

and hence define group isomorphisms. By associativity, $\Lambda_g R_h\varphi$ and $R_h\Lambda_g\varphi$ are well defined, and commutativity among operators of the regular representations follows from the chain of equalities

$$\big(\Lambda_g R_h\varphi\big)(x) = \big(R_h\varphi\big)(g^{-1}x) = \varphi(g^{-1}xh) = \big(\Lambda_g\varphi\big)(xh) = \big(R_h\Lambda_g\varphi\big)(x),$$

which holds for all $g, h, x \in \Gamma$ and $\varphi \in \mathbb{K}^\Gamma$.

Remark 4.2.12. For future use, we note that for each $g \in \Gamma$, the nonzero entries of the permutation matrix associated with Λ_g and the canonical basis are indexed by the set $\{(gh, h)\colon h \in \Gamma\}$, and R_g is nonzero exactly on index set $\{(hg^{-1}, h)\colon h \in \Gamma\}$. Written in terms of the Kronecker delta,

$$(\Lambda_g)_{a,b} = \delta^g_{ab^{-1}} \quad \text{and} \quad (R_g)_{a,b} = \delta^g_{a^{-1}b}, \qquad \text{where} \qquad \delta^\beta_\alpha := \begin{cases} 1 \text{ if } \alpha = \beta \\ 0 \text{ if } \alpha \neq \beta \end{cases}.$$

We close the section by showing that, as in the real or complex case [76], the group representations which generate binary Parseval group frames are unitary.

Proposition 4.2.13 (Binary Parseval group frames are generated by unitary representations)**.** *Given a finite group Γ, let $\mathcal{F}$ be a binary Γ-frame generated by a group representation ρ. If $\mathcal{F}$ is Parseval with analysis operator Θ, then ρ is a unitary representation with matrices explicitly given by $\rho_g = \Theta^* \Lambda_g \Theta$ for each $g \in \Gamma$.*

Proof. Let Γ, $\mathcal{F}$ and Θ be as in the hypothesis. For $g, h \in \Gamma$ and $x \in \mathbb{Z}_2^n$,

$$(\Lambda_g \Theta x)(h) = \Theta x(g^{-1}h) = \langle x, \rho_{g^{-1}} f_h \rangle = \langle \rho_{g^{-1}}^* x, f_h \rangle = (\Theta \rho_{g^{-1}}^* x)(h),$$

so the following diagram commutes:

$$\begin{array}{ccc} \mathbb{Z}_2[\Gamma] & \xrightarrow{\Lambda_g} & \mathbb{Z}_2[\Gamma] \\ {\scriptstyle\Theta}\uparrow & & \uparrow{\scriptstyle\Theta} \\ \mathbb{Z}_2^n & \xrightarrow{(\rho_{g^{-1}})^*} & \mathbb{Z}_2^n \end{array}$$

By the Parseval property and the demonstrated intertwining relationship, we have $\rho_{g^{-1}}^* = \Theta^* \Theta \rho_{g^{-1}}^* = \Theta^* \Lambda_g \Theta$. Replacing g with g^{-1} and taking the transpose, we then get $\rho_g = \Theta^* \Lambda_{g^{-1}}^* \Theta$. Next, the unitarity of Λ_g gives the claimed expression $\rho_g = \Theta^* \Lambda_g \Theta$. These equalities together imply that $\rho_g = \rho_{g^{-1}}^*$; we conclude that each ρ_g is unitary. □

Example 4.2.14 (A binary Parseval $\mathbb{Z}_3^2$-frame)**.** The family of vectors and matrix

$$\mathcal{F} = \left\{ \underset{f_{\binom{0}{0}}}{\begin{bmatrix}0\\1\\0\\0\\0\end{bmatrix}}, \underset{f_{\binom{0}{1}}}{\begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix}}, \underset{f_{\binom{0}{2}}}{\begin{bmatrix}0\\0\\0\\1\\0\end{bmatrix}}, \underset{f_{\binom{1}{0}}}{\begin{bmatrix}0\\1\\1\\0\\1\end{bmatrix}}, \underset{f_{\binom{1}{1}}}{\begin{bmatrix}0\\0\\1\\1\\1\end{bmatrix}}, \underset{f_{\binom{1}{2}}}{\begin{bmatrix}0\\1\\0\\1\\1\end{bmatrix}}, \underset{f_{\binom{2}{0}}}{\begin{bmatrix}1\\1\\0\\1\\0\end{bmatrix}}, \underset{f_{\binom{2}{1}}}{\begin{bmatrix}1\\1\\1\\0\\0\end{bmatrix}}, \underset{f_{\binom{2}{2}}}{\begin{bmatrix}1\\0\\1\\1\\0\end{bmatrix}} \right\} \text{ and } G = \begin{bmatrix} 1&0&0&1&0&1&1&1&0 \\ 0&1&0&1&1&0&0&1&1 \\ 0&0&1&0&1&1&1&0&1 \\ 1&1&0&1&0&0&1&0&1 \\ 0&1&1&0&1&0&1&1&0 \\ 1&0&1&0&0&1&0&1&1 \\ 1&0&1&1&1&0&1&0&0 \\ 1&1&0&0&1&1&0&1&0 \\ 0&1&1&1&0&1&0&0&1 \end{bmatrix}$$

are a binary Parseval $\mathbb{Z}_3^2$ frame and its Gramian. Denoting the left regular representation of $\mathbb{Z}_3$ as $\tilde{\rho}$ with $\tilde{\rho}(1) \equiv \tilde{\rho}_1 := \begin{bmatrix} 0&0&1 \\ 1&0&0 \\ 0&1&0 \end{bmatrix}$, the left regular representation matrices of $\mathbb{Z}_3^2$ are defined by the Kronecker products $\Lambda_{\binom{i}{j}} = \tilde{\rho}_i \otimes \tilde{\rho}_j$, recalling that $\tilde{\rho}_i = \tilde{\rho}_1^i$ for $i \in \mathbb{Z}_3$. The corresponding matrices $\rho\binom{i}{j} := \Theta^* \Lambda_{\binom{i}{j}} \Theta$ provide a representation of the group $\mathbb{Z}_3^2$ on the vector space $\mathbb{Z}_2^5$.

$$\rho\binom{0}{0} = \begin{bmatrix} 1&0&0&0&0 \\ 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \end{bmatrix}, \quad \rho\binom{0}{1} = \begin{bmatrix} 1&0&0&0&0 \\ 0&0&0&1&0 \\ 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&0&1 \end{bmatrix}, \quad \rho\binom{0}{2} = \begin{bmatrix} 1&0&0&0&0 \\ 0&0&0&1&0 \\ 0&0&0&1&0 \\ 0&1&0&0&0 \\ 0&0&0&0&1 \end{bmatrix},$$

$$\rho\binom{1}{0} = \begin{bmatrix} 0&0&0&0&1 \\ 1&1&0&1&0 \\ 1&1&1&0&0 \\ 1&0&1&1&0 \\ 0&1&1&1&0 \end{bmatrix}, \quad \rho\binom{1}{1} = \begin{bmatrix} 0&0&0&0&1 \\ 1&0&1&1&0 \\ 1&1&0&1&0 \\ 1&1&1&0&0 \\ 0&1&1&1&0 \end{bmatrix}, \quad \rho\binom{1}{2} = \begin{bmatrix} 0&0&0&0&1 \\ 1&1&1&0&0 \\ 1&0&1&1&0 \\ 1&1&0&1&0 \\ 0&1&1&1&0 \end{bmatrix},$$

$$\rho\binom{2}{0} = \begin{bmatrix} 0&1&1&1&0 \\ 0&1&1&0&1 \\ 0&0&1&1&1 \\ 0&1&0&1&1 \\ 1&0&0&0&0 \end{bmatrix}, \quad \rho\binom{2}{1} = \begin{bmatrix} 0&1&1&1&0 \\ 0&1&0&1&1 \\ 0&1&1&0&1 \\ 0&0&1&1&1 \\ 1&0&0&0&0 \end{bmatrix}, \quad \rho\binom{2}{2} = \begin{bmatrix} 0&1&1&1&0 \\ 0&0&1&1&1 \\ 0&1&0&1&1 \\ 0&1&1&0&1 \\ 1&0&0&0&0 \end{bmatrix}.$$

One may verify that the induced map $\rho : \mathbb{Z}_3^2 \to \mathrm{GL}(\mathbb{Z}_2^5)$ is a unitary representation and that $\mathcal{F}$ is in fact the orbit of $f_{\binom{0}{0}}$ under ρ.

4.3 The structure of the Gramian of a binary Parseval group frame

The Gramian captures geometric information about the structure of the associated frame, since it records every pairwise dot product among frame vectors. If the frame is a group frame, then it also reflects the group structure. As shown below, the Gramian of a binary Parseval group frame is an element of the algebra generated by the right regular representation.

Theorem 4.3.1 (Gramians of binary Parseval group frames as elements of the group algebra)**.** *Let Γ be a finite group with right regular representation $\{R_g\}_{g\in\Gamma}$ and associated group algebra $\mathbb{Z}_2[\{R_g\}]$, and suppose G is the Gramian of a binary Parseval Γ-frame $\mathcal{F} := \{f_g\}_{g\in\Gamma}$. Then the Gram matrix is in the group algebra. More explicitly, G is given by*

$$G = \sum_{g\in\Gamma} \eta(g) R_g, \tag{4.3}$$

where the function $\eta : \Gamma \to \mathbb{Z}_2$ is defined by $\eta(g) := \langle f_g, f_e \rangle$.

Proof. Let ρ be the frame-generating group representation, which by Proposition 4.2.13 is a unitary representation of Γ. Consider $H = \sum_{g\in\Gamma} \eta(g) R_g$ with η as in the statement of the theorem. We compute for $a, b \in \Gamma$ the value

$$\begin{aligned} H_{a,b} &= \sum_{g\in\Gamma} \eta(g)(R_g)_{a,b} \\ &= \sum_{g\in\Gamma} \eta(g)\delta^g_{a^{-1}b} = \eta(a^{-1}b) \\ &= \langle f_{a^{-1}b}, f_e \rangle \\ &= \langle \rho_b f_e, \rho^*_{a^{-1}} f_e \rangle \\ &= \langle f_b, f_a \rangle = G_{a,b}\,. \end{aligned}$$

In the last identity, we have used the unitarity, $\rho_{a^{-1}} = \rho_a^*$. □

Theorem 4.3.2 (Gramians of binary Parseval frames in a group algebra imply group frame structure)**.** *Let Γ be a finite group with regular representations Λ and R, and suppose $\mathcal{F} = \{f_g\}_{g\in\Gamma}$ is a binary Parseval frame with Gramian G and analysis operator Θ. If G is in the group algebra $\mathbb{Z}_2[\{R_g\}]$, then $\rho_g := \Theta^* \Lambda_g \Theta$ defines a unitary representation of Γ and $\{f_g\}_{g\in\Gamma}$ is a Γ-frame obtained from the orbit of f_e under the representation $\{\rho_g\}_{g\in\Gamma}$.*

Proof. Assume that $G = \Theta\Theta^* \in \mathbb{Z}_2[\{R_g\}]$. Since Λ_g and $R_{g'}$ commute for each $g, g' \in \Gamma$, so do Λ_g and G. From $\Theta^*\Theta\Theta^* = \Theta^*$, then, we have $\Theta^*\Lambda_g\Theta\Theta^*\Lambda_h\Theta = \Theta^*\Lambda_{gh}\Theta$ for each $g, h \in \Gamma$, and since $(\Theta^*\Lambda_g\Theta)^* = \Theta^*\Lambda_{g^{-1}}\Theta$, it follows that $\rho_g = \Theta^*\Lambda_g\Theta$ defines a unitary representation of Γ. Using these properties for ρ_g then shows that

$$\rho_g f_e = \Theta^*\Lambda_g\Theta\Theta^*\delta_e = \Theta^*\Theta\Theta^*\Lambda_g\delta_e = \Theta^*\delta_g = f_g\,,$$

so the frame vectors are obtained from the orbit under the unitaries $\{\rho_g\}_{g\in\Gamma}$. □

We summarize the preceding two theorems in a characterization of binary Parseval group frames.

Corollary 4.3.3 (Characterization of binary Parseval group frames in terms of Gramians)**.** *Let Γ be a finite group with right regular representation $\{R_g\}_{g\in\Gamma}$. A binary Parseval frame $\mathcal{F}$ indexed by Γ is a Γ-frame if and only if its Gramian is in the algebra $\mathbb{Z}_2[\{R_g\}_{g\in\Gamma}]$.*

4.3.1 Characterizing the structure of the Gramian

In order to facilitate a catalogue of binary Parseval group frames, we identify necessary and sufficient conditions for their Gramians.

In the real or complex case, each symmetric idempotent matrix is the Gram matrix of a Parseval frame. In the binary case, [2, Theorem 4.1] characterizes Parseval frames with the additional requirement that at least one row or column vector is odd. This condition is equivalent to the condition that the Gramian has at least one odd vector in its range, since the span of the column vectors of a matrix forms the range of the matrix; we use these statements interchangeably throughout this paper. This condition is *also* equivalent to that of having at least one nonzero entry on the diagonal, since the idempotence and symmetry of a Gramian G induce the identity between the dot product of a vector $G\delta_g$ with itself and the corresponding diagonal entry of the Gramian, $\langle G\delta_g, G\delta_g\rangle = G_{g,g}$ for all $g \in \Gamma$.

We next combine the results we obtained so far with the characterization of the Gramians of binary Parseval frames to characterize Gramians that belong to binary Parseval group frames.

Theorem 4.3.4 (The structure of Gramians of binary Parseval group frames)**.** *Given a finite group Γ with right regular representation R, a map $G : \mathbb{Z}_2^\Gamma \to \mathbb{Z}_2^\Gamma$ is the Gramian of binary Parseval Γ-frame if and only if G is symmetric and idempotent, $G \in \mathbb{Z}_2[\{R_g\}]$ and the range of G contains an odd vector.*

Proof. As noted above, [2, Theorem 4.1] characterizes the Gram matrices of binary Parseval frames as symmetric, idempotent matrices having at least one odd column. Thus, given a finite group Γ, the characterization in the current theorem reduces to Corollary 4.3.3, and is thereby proven. □

In short, this last theorem states that we can move back and forth between elements in the unitary equivalence class of a frame and the Gramian. Since we focus on the construction of Gramians hereafter, we summarize how to obtain a group frame from the corresponding Gramian more explicitly. To this end, we recall that if G is the Gramian of a binary Parseval frame, then it factors into $G = \Theta\Theta^*$ where the columns of Θ are orthonormal with respect to the dot product and form a basis for the range of G. This means the columns of Θ^* are in the space whose dimension is the rank of G, as expected. Moreover, for any such factorization of G, the columns of Θ^* form a binary Parseval frame in the unitary equivalence class associated with G. Factoring G can be achieved by performing a version of a Gram-Schmidt algorithm, as demonstrated in [2]. We summarize the most practically relevant consequences of these observations and the preceding theorems.

Corollary 4.3.5 (Gramian candidates in group algebra induce unitary class representative group frames)**.** *Let Γ be a finite group with left and right regular representations $\{\Lambda_g\}_{g\in\Gamma}$ and $\{R_g\}_{g\in\Gamma}$, respectively. If a map $G \in \mathbb{Z}_2[\{R_g\}_{g\in\Gamma}]$ is symmetric and idempotent and its range contains an odd vector, then it can be factored in the form $G = \Theta\Theta^*$ where $f_g = \Theta^*\delta_g$ defines a binary Parseval frame $\{f_g\}_{g\in\Gamma}$ for $\mathbb{Z}_2^k$ and k is the rank of G. Moreover, $\rho_g = \Theta^*\Lambda_g\Theta$ defines a unitary representation of Γ, and the vectors $\{f_g\}_{g\in\Gamma}$ are a binary Parseval Γ-frame obtained from the orbit of f_e under the representation $\{\rho_g\}_{g\in\Gamma}$.*

4.3.2 Additional properties of the Gramian

Since regular representation matrices are permutation matrices, a consequence of Theorem 4.3.1 is that each of the rows of the Gramian of a binary Parseval group frame has the same weight. Thus, if a Gramian is assumed to be that of a binary Parseval group frame, the condition that one column is odd is equivalent to the condition that *every* column is odd, which equates to the condition that every diagonal entry is a 1, or even simply that $\eta(e) = 1$. Continuing under the assumption that the Gramian may be written as $G = \Sigma_g \eta(g) R_g$, the quantity of 1's in a column is the quantity of elements $g \in \Gamma$ such that $\eta(g) = 1$; it follows that G has an odd column if and only if the sum $\Sigma_g \eta(g) = 1$.

Now, suppose Γ is a finite group of order k and that we wish to exhaustively search for Γ-frames. The characterization in Theorem 4.3.4 tells us that the candidate set of Gramians is a subset of

$$\left\{ H = \sum_{g\in\Gamma} \eta(g) R_g \;\middle|\; \begin{array}{l} \eta(e) = 1 \\ \eta(g) = \eta(g^{-1}) \text{ for all } g \in \Gamma \\ \sum_g \eta(g) = 1 \end{array} \right\}. \tag{4.4}$$

From a computational standpoint, the three necessary criteria are easy to check as properties of the coefficient function η; in fact, no matrix multiplication is required until we wish to check idempotence. The following proposition reduces the idempotence condition to a property of η as well.

Proposition 4.3.6 (Idempotence in group algebra characterized by convolution identity)**.** *Given a finite group Γ with right regular representation $\{R_g\}_{g\in\Gamma}$ and a binary function $\eta : \Gamma \to \mathbb{Z}_2$, the matrix $\sum_g \eta(g)R_g$ is idempotent if and only if η is invariant under convolution with itself; that is, if and only if $\eta(h) = \eta * \eta(h) := \sum_g \eta(g)\eta(g^{-1}h)$ for each $h \in \Gamma$.*

Proof. Let Γ and $\{R_g\}_{g\in\Gamma}$ be as given above and $\eta : \Gamma \to \mathbb{Z}_2$ be a binary function. We note that

$$\Big(\sum_{g\in\Gamma} \eta(g)R_g \Big)^2 = \sum_{g_1,g_2\in\Gamma} \eta(g_1)\eta(g_2)R_{g_1g_2} = \sum_{g,h\in\Gamma} \eta(g)\eta(g^{-1}h)R_h; \tag{4.5}$$

it follows that $\sum \eta(g)R_g = \big(\sum \eta(g)R_g\big)^2$ implies $\eta(h) = \sum_g \eta(g)\eta(g^{-1}h)$ for each $h \in \Gamma$. On the other hand, suppose $\eta : \Gamma \to \mathbb{Z}_2$ is convolution invariant. Then

$$\sum_{h\in\Gamma} \eta(h)R_h = \sum_{h\in\Gamma} \Big[\sum_{g\in\Gamma} \eta(g)\eta(g^{-1}h) \Big] R_h = \sum_{g,h\in\Gamma} \eta(g)\eta(g^{-1}h)R_h,$$

which by equation (4.5) is equal to $\big(\sum \eta(g)R_g\big)^2$, and the proof is complete. □

Example 4.3.7. Consider D_3, the dihedral group of order 6, described $\langle a, b : a^3 = 1, b^2 = 1, b^{-1}ab = a^{-1}\rangle$; ordering the elements $1, a, a^2, b, ab, a^2b$, then the right regular representation matrices of D_3 are given by

$$\underset{R_1}{\begin{bmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1 \end{bmatrix}}, \underset{R_a}{\begin{bmatrix} 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 1&0&0&0&0&0\\ 0&0&0&0&0&1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0 \end{bmatrix}}, \underset{R_{a^2}}{\begin{bmatrix} 0&0&1&0&0&0\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&0&0&1&0\\ 0&0&0&1&0&0\\ 0&0&0&0&0&1 \end{bmatrix}}, \underset{R_b}{\begin{bmatrix} 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0 \end{bmatrix}}, \underset{R_{ab}}{\begin{bmatrix} 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 0&0&0&1&0&0\\ 0&0&1&0&0&0\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0 \end{bmatrix}}, \underset{R_{a^2b}}{\begin{bmatrix} 0&0&0&0&0&1\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 1&0&0&0&0&0 \end{bmatrix}}.$$

A quick check for convolution invariance among the twelve coefficient functions satisfying the conditions in (4.4) shows that only I_6 and $G_1 := R_1 + R_a + R_{a^2}$ give suitable Gramians. Synthesis matrices for the two classes are given by $\Theta^*_{G_1} := \left[\begin{smallmatrix} 1&1&1&0&0&0\\ 0&0&0&1&1&1 \end{smallmatrix}\right]$ and $\Theta^*_{I_6} = I_6$.

It follows from Proposition 4.3.6 that the coefficient function of the Gramian of a binary Parseval group frame is always convolution invariant, but convolution invariance of such a function does not ensure matrix symmetry:

Example 4.3.8. Let $\{R_j\}_{j=0}^6$ be the right regular representation matrices for the group $\mathbb{Z}_7$, noting that $R_j^* = R_j^{-1} = R_{-j}$. Consider the coefficient function given by

$$\eta(x) = \begin{cases} 1 & \text{if } x \in \{0,1,2,4\} \\ 0 & \text{if } x \in \{3,5,6\} \end{cases},$$

which is easily verified to satisfy $\eta = \eta * \eta$. It is clear, however, that the matrix $G = \sum_{j=0}^6 \eta(j)R_j$ is not symmetric (since $\eta(1) \neq \eta(6)$, for example), so G is not the Gramian of any frame.

Adding idempotence under convolution to the conditions in (4.4) removes the need to require that the coefficient function sums to 1, which is then implicit in $\eta(e) = 1$. We conclude a characterization of the coefficient functions of binary Parseval group frames.

Theorem 4.3.9 (Gramians of binary Parseval Γ-frames characterized by η)**.** *Given a finite group Γ with right regular representation matrices $\{R_g\}_{g\in\Gamma}$ and $G = \sum_g \eta(g)R_g$, then G is the Gramian of a binary Parseval Γ-frame if and only if $\eta(e) = 1$, η is symmetric under inversion of its argument and idempotent under convolution.*

Proof. Since $G = \sum_g \eta(g)R_g$ and $R_g^* = R_{g^{-1}}$ for all $g \in \Gamma$, it follows that G is symmetric if and only if η is. Further, Proposition 4.3.6 equates the idempotence of G with that of η. Now, $\eta(e) = 1$ if and only if $\eta(g) = 1$ for all $g \in \Gamma$, if and only if G has at least one odd column.

Theorem 4.3.4 provides four conditions which characterize the Gramians of binary Parseval group frames, three of which we have just demonstrated are equivalent to conditions on η. Since G automatically satisfies the remaining condition as an element of the group algebra $\mathbb{Z}_2[\{R_g\}]$, it follows that $G = \sum_g \eta(g)R_g$ is the Gramian of a binary Parseval Γ-frame if and only if $\eta(e) = 1$, $\eta = \eta * \eta$, and $\eta(g) = \eta(g^{-1})$ for all $g \in \Gamma$. □

In light of the last theorem, we can replace the necessary conditions (4.4) with necessary and sufficient conditions for G being the Gramian of a binary Parseval Γ-frame $\mathcal{F}$,

$$G \in \left\{ \sum_{g\in\Gamma} \eta(g)R_g \;\middle|\; \begin{array}{l} \eta(e) = 1 \\ \eta(g) = \eta(g^{-1}) \text{ for all } g \in \Gamma \\ \eta = \eta * \eta \end{array} \right\}, \tag{4.6}$$

where η is assumed to be a $\mathbb{Z}_2$-valued function on Γ.

4.3.3 Binary Parseval frames from orbits of abelian groups

Next, we focus on the special case of abelian groups.

Lemma 4.3.10 (Idempotence from square root condition for abelian groups)**.** *Given a finite abelian group Γ and function $\eta : \Gamma \to \mathbb{Z}_2$, η is idempotent under convolution if and only if*

$$\eta(g) = \sum_{h^2=g} \eta(h) \quad \textit{for all} \quad g \in \Gamma.$$

Proof. Fix $g \in \Gamma$ and partition Γ into $K_g := \{h \in \Gamma : h^2 = g\}$ and $B := \Gamma \backslash K_g$. Since Γ is abelian and by the definition of B, we have that for each element $x \in B$ there is a unique element $x^{-1}g = gx^{-1} \in B$, and $x \neq x^{-1}g$. We refine our partition on Γ by separating B

into disjoint sets B_1 and B_2 such that no two elements $x, y \in B_i$ multiply to g, arbitrarily assigning one element from each pair $\{x, x^{-1}g\}$ to B_1 and the other to B_2.

The idempotence under convolution is thus expressed

$$\begin{aligned}
\eta(g) &= \sum_{h\in\Gamma} \eta(h)\eta(h^{-1}g) \\
&= \sum_{h\in K_g} \eta(h)\eta(\underbrace{h^{-1}g}_{=h}) + \sum_{x\in B_1} \eta(x)\eta(x^{-1}g) + \sum_{y\in B_2} \eta(y)\eta(y^{-1}g) \\
&= \sum_{h\in K_g} \eta(h)\eta(h) + \sum_{x\in B_1} \left[\eta(x)\eta(x^{-1}g) + \eta(x^{-1}g)\eta(\underbrace{x}_{=(x^{-1}g)^{-1}g})\right] \\
&= \sum_{h\in K_g} \eta(h) + 2\sum_{x\in B_1} \eta(x)\eta(x^{-1}g) \\
&= \sum_{h\in K_g} \eta(h),
\end{aligned}$$

where the last two identities follow from noting $z^2 = z$ and $2z = 0$ for all $z \in \mathbb{Z}_2$. □

Example 4.3.11 (Binary Parseval group frames of $\mathbb{Z}_6$)**.** We use the preceding lemma to classify the binary Parseval group frames generated by the (abelian) additive group $\Gamma := \mathbb{Z}_6$. Suppose $G = \sum \eta(g)R_g$ is the Gramian of a binary Parseval $\mathbb{Z}_6$-frame $\mathcal{F}$; in the notation of the proof of Lemma 4.3.10, we have $K_1 = K_3 = K_5 = \emptyset$, for which the "square root condition" asserts $\eta(1) = \eta(3) = \eta(5) = 0$. By the coefficient function characterization of the Gramian, $\eta(0) = 1$, and since $2 + 2 = 4$, we have that either $\eta(2) = \eta(4) = 1$ or G is the identity matrix. It follows, noting that both options induce idempotent matrices, that any binary Parseval $\mathbb{Z}_6$-frame has a Gram matrix that is either I_6 or $G := R_0 + R_2 + R_4$,

$$\underbrace{\begin{bmatrix} 1&0&1&0&1&0\\ 0&1&0&1&0&1\\ 1&0&1&0&1&0\\ 0&1&0&1&0&1\\ 1&0&1&0&1&0\\ 0&1&0&1&0&1 \end{bmatrix}}_{G} = \underbrace{\begin{bmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1 \end{bmatrix}}_{R_0} + \underbrace{\begin{bmatrix} 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0 \end{bmatrix}}_{R_2} + \underbrace{\begin{bmatrix} 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0 \end{bmatrix}}_{R_4}.$$

To complete the classification, we note that G and I_6 represent distinct classes, since the Gramians of switching equivalent binary Parseval frames have the same number of nonzero entries. Synthesis matrices for the two classes are given by $\Theta_G^* := \left[\begin{smallmatrix} 1&0&1&0&1&0\\ 0&1&0&1&0&1 \end{smallmatrix}\right]$ and $\Theta_{I_6}^* = I_6$.

In the special case that every element in a group has exactly one square root, an even stronger consequence holds for η. This "unique square root" property is determined solely by the parity of a group's order (see, for example, Proposition 2.1 in [54]), and we recall part of this characterization in the following lemma.

Lemma 4.3.12. *A finite group of odd order has unique square roots.*

Proof. Let Γ be a group such that $|\Gamma| = 2n-1$ for some integer $n \geq 2$, and suppose $a^2 = b^2$ for some $a, b \in \Gamma$. Then $a^{2n-1} = e$, so $a = a \cdot a^{2n-1} = a^{2n} = b^{2n} = b$. □

Theorem 4.3.13 (Odd-ordered abelian groups and η)**.** *Let Γ be a finite abelian group of odd order. Then the map $g \mapsto \{g' \in \Gamma : g^{2^m} = g' \text{ for some } m \in \mathbb{N}\}$ partitions Γ, and a function $\eta : \Gamma \to \mathbb{Z}_2$ is idempotent under convolution if and only if η is constant on these sets.*

Proof. Since Γ has odd order, the unique square root property reduces the condition

$$\eta(g) = \sum_{h^2=g} \eta(h) \quad \text{for all} \quad g \in \Gamma$$

to

$$\eta(g^2) = \eta(g) \quad \text{for all} \quad g \in \Gamma;$$

thus, it remains only to show that the map defined in the hypothesis partitions Γ. Let $g \in \Gamma$, and for $j \in \mathbb{N}$, define $\gamma_j := g^{2^j}$. Since Γ finite, we may take N to be the least positive integer such that $\gamma_{N+1} \in \{\gamma_j\}_{j=1}^N$. By Γ's unique square roots, it follows that $\gamma_{N+1} = \gamma_1$, or $g = g^{2^N}$. Now, let $h \in \Gamma$ be distinct from g, and similarly define a sequence by $\hat{\gamma}_j := h^{2^j}$, with minimal M such that $h = h^{2^M}$. It follows that either $\{\gamma_j\}_{j\in\mathbb{N}} = \{\hat{\gamma}_j\}_{j\in\mathbb{N}}$ or $\{\gamma_j\}_{j\in\mathbb{N}} \cap \{\hat{\gamma}_j\}_{j\in\mathbb{N}} = \emptyset$, and the claim is shown. □

Example 4.3.14 (Classes of $\mathbb{Z}_{17}$-frames)**.** Suppose $G = \sum_g \eta(g) R_g \in \mathbb{Z}_2[\mathbb{Z}_{17}]$ is the Gramian of a binary Parseval $\mathbb{Z}_{17}$-frame. $\mathbb{Z}_{17}$ satisfies the conditions of Theorem 4.3.13 and η is idempotent under convolution (by Theorem 4.3.9, the "coefficient characterization" theorem), so we know that η is constant on each of the sets $\Delta_1 := \{1, 2, 4, 8, 16, 15, 13, 9\}$ and $\Delta_3 := \{3, 6, 12, 7, 14, 11, 5, 10\}$. Since Δ_1 and Δ_3 are closed under inversion (taking negatives, in this case), η may take different values on the sets. Thus, G is one of exactly four operators, given by

$$I_{17}, \quad I_{17} + \textstyle\sum_{j\in\Delta_1} R_j, \quad I_{17} + \sum_{j\in\Delta_3} R_j, \quad \text{and } \sum_{j\in\mathbb{Z}_{17}} R_j.$$

In illustrating an application of Theorem 4.3.13, this example also motivates us to introduce some additional notation.

Definition 4.3.15 (Symmetric doubling orbit, symmetric doubling orbit partition, $R_{[g]}$)**.** Let Γ be a finite abelian group having unique square roots. For any element $g \in \Gamma$, the *symmetric doubling orbit* of g is the set

$$[g] := \{g^{2^m} : m \in \mathbb{N}\} \cup \{(g^{-1})^{2^m} : m \in \mathbb{N}\}.$$

We define

$$R_{[g]} := \sum_{h\in[g]} R_h$$

and say that the collection $\Gamma' = \{[g]\}_{g\in J}$ is the *symmetric doubling orbit partition* of Γ (indexed by representatives $J \subset \Gamma$) if $\bigcup_{g\in J} [g] = \Gamma$ and for distinct $g, h \in J$ we have $[g] \neq [h]$.

Remark 4.3.16. We comment on our terminology. Since Γ is abelian, let us momentarily consider it as an additive group and express it as $\Gamma \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i}$. Modifying the notation in Definition 4.3.15 accordingly, we have

$$[g] := \{h \in \Gamma : 2^m g = h \text{ for some } m \in \mathbb{N}\} \cup \{h \in \Gamma : 2^m(-g) = h \text{ for some } m \in \mathbb{N}\},$$

which is equivalent to $\{\rho_m g\}_{m=1}^{L} \cup \{\rho_m(-g)\}_{m=1}^{L}$ for some $L \in \mathbb{N}$, where $\rho_m := 2^m I_k$.

It is easy to verify that the matrices $\{2^m I_k\}_{m=1}^{L}$ are representation matrices for the multiplicative subgroup generated by 2 in $\mathbb{Z}_L$, which motivates the "doubling orbit" part of the name *symmetric doubling orbit*: $\{\rho_m g\}_{m=1}^{L}$ is, in fact, the orbit of g under the action of $\langle 2\rangle_{\mathbb{Z}_L}^{\times}$.

We proceed with two results making use of the new notation. The first may be considered a corollary of Theorems 4.3.9 and 4.3.13, and the second uses the symmetric doubling orbit partitioning to provide a count of the binary Parseval Γ-frame unitary equivalence classes for our specified groups Γ.

Theorem 4.3.17 (Characterization of binary Parseval Γ-frames for odd order, abelian Γ)**.** *Let Γ be an odd-ordered abelian group with right regular representation R and symmetric doubling orbit partition $\{[g]\}_{g\in J}$. Let G be a linear map $G : \mathbb{Z}_2^{\Gamma} \to \mathbb{Z}_2^{\Gamma}$, then G is the Gramian of a binary Parseval Γ-frame if and only if $G = \sum_{g\in J} \nu([g])R_{[g]}$ for some $\nu : \Gamma' \to \mathbb{Z}_2$ with $\nu([e]) = 1$.*

Proof. Assume G is the Gramian of a binary Parseval Γ-frame, so that it may be written $G = \sum_{g\in\Gamma} \eta(g)R_g$; then η is idempotent under convolution (by Theorem 4.3.9) and thus constant on symmetric doubling orbits (by Theorem 4.3.13). It follows that $\nu([g]) := \eta(g)$ is well defined and satisfies $G = \sum_{[g]\in J} \nu([g])R_{[g]}$ and $\nu([e]) = 1$.

Conversely, assume $G = \sum_{g\in J} \nu([g])R_{[g]}$ for some ν such that $\nu([e]) = 1$, and define $\eta : \Gamma \to \mathbb{Z}_2$ by assigning $\eta(g) = \nu([g])$, then the conditions of Theorem 4.3.13 are met and η is idempotent under convolution. Noting that $\eta(e) = 1$, the conditions of Theorem 4.3.9 hold as well, and G is thereby the Gramian of a binary Parseval Γ-frame. □

Corollary 4.3.18 (Enumerating unitary equivalence classes of binary Parseval Γ-frames)**.** *Let the group Γ and the set Γ' be as above and define $k := |\Gamma|$, $k' := |\Gamma'|$, then the number of Gramians of unitarily inequivalent binary Parseval Γ-frames is $2^{k'-1} \leq 2^{\frac{1}{2}(k-1)}$.*

Proof. The value $2^{|\Gamma'|-1}$ is the number of functions $\nu : \Gamma' \to \mathbb{Z}_2$ having the property that $\nu([e]) = 1$, thus enumerating the functions delineated in Theorem 4.3.17. The quantity $2^{\frac{1}{2}(k-1)}$ is achieved if $\Gamma = \mathbb{Z}_3^2$, as well as any other case such that $\big|[g]\big| = 2$ for all $g \in \Gamma\backslash\{e\}$. Exceeding this bound implies the existence of $h \in \Gamma\backslash\{e\}$ such that $\big|[h]\big| = 1$, which implies $h = h^2$. Since the only idempotent element of a group is the identity element, such an h does not exist. □

Results in [4] justify the use of Gramians as class representatives of binary Parseval frames. For a group of size k, the naive upper bound of 2^{k^2} binary matrices thereby drops to $2^{\frac{1}{2}(k^2-1)}$ symmetric binary matrices with at least one odd column. Theorem 4.3.1 in this dissertation puts our Gramians in $\mathbb{Z}_2[\{R_g\}]$, a set of order 2^k. In the case of abelian Γ with unique square roots, Corollary 4.3.18 gives the number of distinct Gramians of binary Parseval Γ-frames exactly as $2^{|\Gamma'|-1}$, where $|\Gamma'| \leq \frac{1}{2}(k+1)$ is the quantity of symmetric doubling orbits of Γ. Thus, for a given abelian group Γ of odd order k, the unitary equivalence classes of binary Parseval frames are classified by computing the ranks of $2^{|\Gamma'|-1} \leq 2^{\frac{1}{2}(k-1)}$ Gramians.

Writing the elements of $\mathbb{Z}_p^q$ as vectors suggests plotting subsets of the group for visualization purposes. Noting that inverse elements are obtained by multiplying by $-1 \mod p$, the fact that each symmetric doubling orbit is a collection of scalar multiples of a single element puts each of the points of a given symmetric doubling orbit on a line in $\mathbb{Z}_p^q$ containing the origin.

For many odd-prime/natural-number pairs p, q, in fact, the nontrivial symmetric doubling orbits of $\mathbb{Z}_p^q$ are each identical to that line, minus the origin; this property holds any time the multiplicative subgroup of $\mathbb{Z}_p$ generated by 2 is $\mathbb{Z}_p\backslash\{0\}$, as in the cases of $p \in \{3, 5, 11, 13\}$. It also occurs when $\left|\langle 2\rangle_{\mathbb{Z}_p}^{\times}\right| = \frac{1}{2}(p-1)$ and $(-1) \notin \langle 2\rangle_{\mathbb{Z}_p}^{\times}$, since the *symmetric* part completes the set; the smallest p for which this occurs is 7.

The work in this paper shows that any Gramian in the group algebra of the regular representations yields a binary Parseval $\mathbb{Z}_p^q$-frame for $q \in \mathbb{N}$ and odd prime p if the group elements represented in the sum are the union of a collection of these linear subspaces. However, the converse of this statement is not true, as each Mersenne prime (that is, having the form $2^n - 1$) greater than 7 provides a counter example, as does every Fermat prime (i.e., of the form $2^n + 1$) greater than 5. We illustrate this in Fig. 4.2 with plots of the symmetric doubling orbits of $\mathbb{Z}_p^2$ for the smallest value that demonstrates this behavior, $p = 17$. Each plot shows a pair of orbits (one in red, one in black) that partition a line into two subsets. Any of the 2^{36} linear combinations of coefficients that are constant on these symmetric doubling orbits represents a distinct Gramian of a binary Parseval $\mathbb{Z}_{17}^2$-frame.

4.3.4 An algorithm for classifying binary Parseval Γ-frames for abelian Γ of odd order

For groups of smallest order, the unitary equivalence classes are manageable. However, even for $\mathbb{Z}_3^3$ the enumeration of Parseval frames becomes too tedious to do by hand. One reason is that group automorphisms may lead to different Gramians. The resulting set could be reduced to one representative without losing structural information. We recall that switching offers a coarser equivalence relation that is suitable for removing copies obtained by group automorphisms.

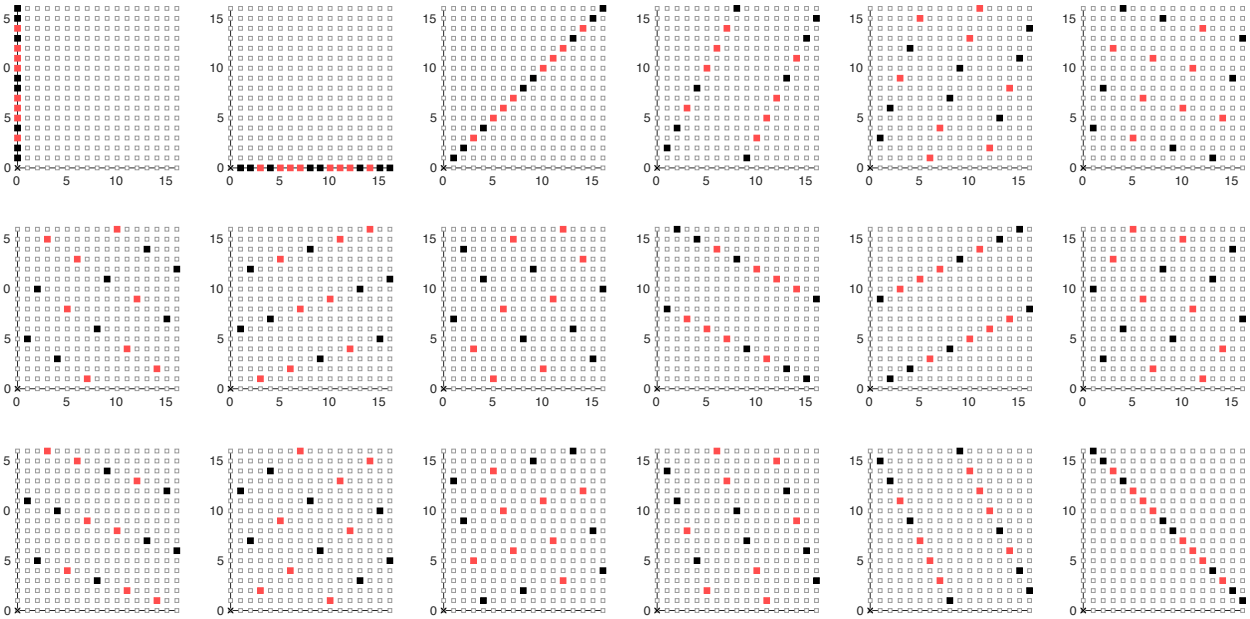

Figure 4.2: Symmetric doubling orbits of $\mathbb{Z}_{17}^2$, plotted in pairs that are complements in one-dimensional subspaces of $\mathbb{Z}_{17}^2$.

Proposition 4.3.19 (Automorphisms on Γ and automorphic switching equivalence)**.** *Let Γ be a finite group with right regular repesentation matrices $\{R_g\}_{g\in\Gamma}$, and let $\mathcal{F} := \{f_g\}_{g\in\Gamma}$ be a binary Parseval Γ-frame with Gramian $G := \sum_g \eta(g)R_g$, then an operator H is the Gramian of a binary Parseval Γ-frame that is automorphically switching equivalent to $\mathcal{F}$ if and only if $H = \sum_g \eta(\sigma(g))R_g$ for some $\sigma \in \mathrm{Aut}(\Gamma)$.*

Proof. Let ρ be the group representation that induces $\mathcal{F}$; we first show that the composition of the coefficent function η with an automorphism induces the Gramian of an automorphically switching equivalent frame.

Let $\sigma \in \mathrm{Aut}(\Gamma)$ and define $H := \sum_g \eta(\sigma(g))R_g$. From $\rho\circ\sigma$ being a group homomorphism, it follows that $\{\rho_{\sigma(g)}f_e\}_{g\in\Gamma}$ is a binary Parseval Γ-frame that is automorphically switching equivalent to $\mathcal{F}$. By Corollary 4.3.3, the Gramian G' of $\{\rho_{\sigma(g)}f_e\}_{g\in\Gamma}$ admits a coefficient function ν such that $G' = \sum_g \nu(g)R_g$. It remains only to prove that $\nu = \eta\circ\sigma$, so that $G' = H$.

Recall from the proof of Theorem 4.3.1 that for $a, b \in \Gamma$, $G_{a,b} = \eta(a^{-1}b)$ and $G'_{a,b} = \nu(a^{-1}b)$. We conclude

$$\begin{aligned}\nu(a^{-1}b) &= \left\langle \rho_{\sigma(b)}f_e, \rho_{\sigma(a)}f_e \right\rangle \\ &= G_{\sigma(a),\sigma(b)} \\ &= \eta\left(\sigma(a)^{-1}\sigma(b)\right) \\ &= \eta\left(\sigma(a^{-1}b)\right),\end{aligned}$$

this last identity following from the fact that σ is an automorphism.

Conversely, suppose $\mathcal{F}' := \{f'_g\}_{g\in\Gamma}$ is a Γ-frame that is automorphically switching equivalent to a frame $\mathcal{F}$ induced by a representation ρ. Let the unitary U and $\sigma \in \mathrm{Aut}(\Gamma)$ give $f'_g = Uf_{\sigma(g)} = U\rho_{\sigma(g)}f_e$ for all $g \in \Gamma$. Let the Gramians of $\mathcal{F}$ and $\mathcal{F}'$ be $G = \sum_g \eta(g)R_g$ and $H = \sum_g \nu(g)R_g$, respectively. We equate

$$\begin{aligned}\nu(a^{-1}b) &= \left\langle f'_b, f'_a \right\rangle \\ &= \left\langle U\rho_{\sigma(b)}f_e, U\rho_{\sigma(a)}f_e \right\rangle \\ &= \left\langle \rho_{\sigma(b)}f_e, \rho_{\sigma(a)}f_e \right\rangle \\ &= \eta\left(\sigma(a^{-1}b)\right),\end{aligned}$$

and we see that $H = \sum_g \eta(\sigma(g))R_g$ has the claimed form. □

Next, we study how symmetric doubling orbits behave under automorphisms. Let $g, h \in \Gamma$ and $a \in \mathbb{N}$ such that $g = h^{2^a}$. Under an automorphism $\sigma \in \mathrm{Aut}(\Gamma)$, we identify $\sigma(g) = \sigma(h^{2^a}) = \sigma(h)^{2^a}$. Consequently, if $g \in [h]$, then $\sigma(g) \in \big[\sigma(h)\big]$. This means the action of σ on Γ passes to an action on the symmetric doubling orbits.

Definition 4.3.20. For a finite abelian group Γ partitioned into symmetric doubling orbits $\Gamma' = \{[g]\}_{[g]\in J}$ and an automorphism σ, we let $\tilde{\sigma}$ be the associated bijection on Γ' such that $\tilde{\sigma}([g]) = \big[\sigma(g)\big]$.

Corollary 4.3.21 (Automorphisms on Γ and symmetric doubling orbits)**.** *Let Γ, $\{R_g\}$, $\mathcal{F}$, G and η be as above, and suppose Γ is abelian of odd order. Let Γ' be the symmetric doubling orbit partition of Γ, and $G = \sum_{[g]\in\Gamma'} \tilde{\eta}([g])R_{[g]}$ with $\tilde{\eta} : \Gamma' \to \mathbb{Z}_2$, then an operator H is the Gramian of a binary Parseval Γ-frame that is automorphically switching equivalent to $\mathcal{F}$ if and only if $H = \sum_{[g]\in\Gamma'} \tilde{\eta}(\tilde{\sigma}([g]))R_{[g]}$ for some $\sigma \in \mathrm{Aut}(\Gamma)$.*

Proof. Let $\sigma \in \mathrm{Aut}(\Gamma)$ and $\tilde{\sigma}$ be the associated bijection on Γ'. Let $\eta(g) = \tilde{\eta}([g])$ for each $g \in \Gamma$. Consequently, $\sum_{[g]\in\Gamma'} \tilde{\eta}(\tilde{\sigma}([g]))R_{[g]} = \sum_{g\in\Gamma} \eta(\sigma(g))R_g$. Applying Proposition 4.3.19 completes the proof. □

By identifying Gramians in the group algebra with functions on the group, Corollary 4.3.3 reduces the search for Gram matrices associated with a given Γ to a search over a subset of $\mathbb{Z}_2$-valued coefficient functions on Γ; Theorem 4.3.9 specifies that subset. Proposition 4.3.19 allows a classification of the valid coefficient functions in terms of the automorphism group on Γ. Specialized results for abelian groups summarized in Corollary 4.3.21 provide us with a concrete method for obtaining all binary Parseval group frames for abelian, odd-ordered groups. The following result provides theoretical justification for an algorithm guaranteed to produce a list of Gram matrices that contains exactly one representative from each automorphic switching equivalence class.

Theorem 4.3.22. *Given an odd-ordered abelian group Γ and a set $\mathcal{M}$ which generates the automorphism group of Γ, the algorithm described in the Practitioner's Guide below partitions the Gramians of binary Parseval Γ-frames under automorphic switching equivalence.*

Proof. Let Γ' be the symmetric doubling orbit partitioning of Γ. Corollary 4.3.21 reduces the theorem's partitioning to the comparison of symmetric doubling orbit coefficient functions. In particular, two binary Parseval Γ-frames are automorphically switching equivalent if and only if their Gramians $\sum_{[g]\in\Gamma'} \eta([g])R_{[g]}$ and $\sum_{[g]\in\Gamma'} \nu([g])R_{[g]}$ have the property that $\eta([g]) = \nu(\tilde{\sigma}([g]))$ for all $g \in \Gamma$ and $\tilde{\sigma}$ determined by the action of some $\sigma \in \mathrm{Aut}(\Gamma)$ on the symmetric doubling orbits. Given a coefficient function η, the algorithm does one of two things each time it accesses the multiplication table: it either identifies another coefficient function belonging to the same partition as η, or it terminates the search for coefficient functions in that partition. It thus remains to show that the algorithm exhausts the partition for any such η.

Let $\eta : \Gamma \to \mathbb{Z}_2$ be constant on symmetric doubling orbits. Enumerate $\mathcal{M} = \{M_i\}_{i=1}^N$ and define $M_0 := Id \in \mathrm{Aut}(\Gamma)$, and let $\Omega_0 := \{S_\eta\}$, where $S_\eta := \eta^{-1}(1)$. For $j \in \mathbb{N}$, define the set collection

$$\Omega_j := \{M_i(S) : i = 0, 1, \ldots, N \text{ and } S \in \Omega_{j-1}\}.$$

Note that $\Omega_{j-1} \subseteq \Omega_j$ for all $j \in \mathbb{N}$, since $S \in \Omega_{j-1}$ implies that $M_0(S) \in \Omega_j$. The algorithm produces each Ω_j sequentially and terminates the search for elements in η's partition at the end of identifying the elements of Ω_j if $\Omega_j = \Omega_{j-1}$. Now, if $\nu(g) = \eta(\sigma(g))$ for all $g \in \Gamma$ and some $\sigma \in \mathrm{Aut}(\Gamma)$, then there is a finite sequence $l_1, l_2, \ldots, l_k$ such that $\sigma = M_{l_k} M_{l_{k-1}} \cdots M_{l_1}$. It follows that the partition reprepresented by η is the set Ω_L for some $L \in \mathbb{N}$; thus, the algorithm produces the partition of η if and only if there is an integer j_η such that

$$\Omega_1 \subsetneq \Omega_2 \subsetneq \cdots \subsetneq \Omega_{j_\eta} = \Omega_{j_\eta+i} \quad \text{for all } i \in \mathbb{N}. \tag{4.7}$$

Let $j_0 \in \mathbb{N}$ be such that $\Omega_{j_0-1} = \Omega_{j_0}$; existence follows from the finiteness of $\mathbb{Z}_2[\Gamma]$. To prove that such j_η exists, it is enough to show that the equality $\Omega_{j_0} = \Omega_{j_0-1}$ implies $\Omega_{j_0} = \Omega_{j_0+i}$ for all $i \in \mathbb{N}$.

Let $S' \in \Omega_{j_0+1}$. By the inclusion $\Omega_{j_0} \subseteq \Omega_{j_0+1}$, it is left to show that $S' \in \Omega_{j_0}$. By the definition of Ω_{j_0+1}, we have $S' = M_i(S)$ for some $i \in \{0, 1, \ldots, N\}$ and some $S \in \Omega_{j_0} = \Omega_{j_0-1}$. Since $S \in \Omega_{j_0-1}$, it follows that $S' = M_i(S) \in \Omega_{j_0}$, and the proof is complete. □

A Practitioner's Guide to Generating Gramians of Binary Parseval Γ-Frames for abelian Γ of Odd Order

1. Produce a set J so that $\{e\} \cup J$ indexes the symmetric doubling orbit partition Γ' of Γ.
2. Select $\mathcal{M} \subset \mathrm{Aut}(\Gamma)$ to seed a multiplication table. If $\mathcal{M}$ generates $\mathrm{Aut}(\Gamma)$, this algorithm provides a partition of Γ-frames into automorphic switching equivalence classes. *(See Remark 4.3.23)*
3. Produce the automorphism multiplication table containing a row for each $M_i \in \mathcal{M}$, with entry (i, j) giving $M_i(\llbracket g_j \rrbracket)$.
4. For each $m \leq \frac{1}{2}|\Gamma'|$, apply the method described in Example 4.3.24 to partition subsets of the collection $\{\bigcup_{g\in K} [g] : K \subset J, |K| = m\}$. For $m > \frac{1}{2}|\Gamma'|$, use the fact that for given indexing sets K, K', the sets $\bigcup_{g\in K} [g]$ and $\bigcup_{g\in K'} [g]$ represent the same class if and only if $\bigcup_{g\in J\setminus K} [g]$ and $\bigcup_{g\in J\setminus K'} [g]$ do.

Remark 4.3.23 (Sampling $\mathrm{Aut}(\Gamma)$)**.** Choosing $\mathcal{M} = \mathrm{Aut}(\Gamma)$ guarantees accurate partitioning, although $\mathrm{Aut}(\Gamma)$ may be difficult to calculate. Theorem 4.3.22 tells us that we can obtain this partitioning as long as $\mathcal{M}$ is a generating set for $\mathrm{Aut}(\Gamma)$. If $\mathcal{M}$ is not known to generate $\mathrm{Aut}(\Gamma)$, the potential undersampling of the automorphism group may simply lead to the case that some classes are represented multiple times; the number of Gramians is still smaller than $2^{|\Gamma'|-1}$.

The following example demonstrates how the algorithm works.

Example 4.3.24 (Classifying binary Parseval $\mathbb{Z}_3^2$-frames)**.** Let the symmetric doubling orbit partition of $\mathbb{Z}_3^2$ given by set $\Gamma' = \{[g] : g \in \{e\} \cup J\}$ with $J := \{\binom{1}{0}, \binom{1}{1}, \binom{0}{1}, \binom{1}{2}\}$. We shall classify binary Parseval $\mathbb{Z}_3^2$-frames up to automorphic switching equivalence by identifying suitable Gramian representatives for each class. These Gramians have the form $I + \sum_{i=1}^{m} R_{[g_i]}$ for some $m \in \{0, 1, 2, 3, 4\}$ and distinct g_i's, and we proceed by considering one value of m at a time. We make use of the fact that for any finite vector space V, $\mathrm{Aut}(V) \equiv \mathrm{GL}(V)$.

$\mathbf{m = 0}$: The cases of $m = 0$ and $m = 4$ are trivial and listed in the summary.

$\mathbf{m = 1}$: The matrix $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right] \in \mathrm{GL}(\mathbb{Z}_3^2)$ gives

$$\left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right] \left\llbracket \binom{1}{0} \right\rrbracket = \left\{ \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right] \binom{1}{0}, \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right] \binom{2}{0} \right\} = \left\{ \binom{1}{1}, \binom{2}{2} \right\} = \left\llbracket \binom{1}{1} \right\rrbracket ;$$

applying the preceding corollary, $I + R_{\left\llbracket \binom{1}{0} \right\rrbracket}$ and $I + R_{\left\llbracket \binom{1}{1} \right\rrbracket}$ are thus Gramians of automorphically switching equivalent binary Parseval $\mathbb{Z}_3^2$-frames. With this in mind, consider the multiplication table given in Table 4.1. The first row shows that for $g, h \in J$, $[g] = \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right]^a [h]$ for some integer a. It follows that the four operators $I + R_{[g]}$ represent the same automorphic switching equivalence class.

Table 4.1: Multiplication table for selected $M \in \mathrm{GL}(\mathbb{Z}_3^2)$

	$\left[\binom{1}{0}\right]$	$\left[\binom{1}{1}\right]$	$\left[\binom{1}{2}\right]$	$\left[\binom{0}{1}\right]$
$\left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]$	$\left[\binom{1}{1}\right]$	$\left[\binom{1}{2}\right]$	$\left[\binom{0}{1}\right]$	$\left[\binom{1}{0}\right]$
$\left[\begin{smallmatrix}2&1\\1&0\end{smallmatrix}\right]$	$\left[\binom{1}{2}\right]$	$\left[\binom{0}{1}\right]$	$\left[\binom{1}{1}\right]$	$\left[\binom{1}{0}\right]$
$\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$	$\left[\binom{1}{0}\right]$	$\left[\binom{1}{2}\right]$	$\left[\binom{0}{1}\right]$	$\left[\binom{1}{1}\right]$

$\mathbf{m = 2}$: Similarly, the first two entries in the first row give

$$\left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]\left(\left[\binom{1}{0}\right]\cup\left[\binom{1}{1}\right]\right)=\left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]\left[\binom{1}{0}\right]\cup\left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]\left[\binom{1}{1}\right]=\left[\binom{1}{1}\right]\cup\left[\binom{1}{2}\right],$$

implying

$$I+R_{\left[\binom{1}{0}\right]}+R_{\left[\binom{1}{1}\right]}\quad\text{and}\quad I+R_{\left[\binom{1}{1}\right]}+R_{\left[\binom{1}{2}\right]}$$

are representatives of the same equivalence class. Proceeding down the first two columns, we find that Gramians $I+R_{\left[\binom{1}{2}\right]}+R_{\left[\binom{0}{1}\right]}$ and $I+R_{\left[\binom{1}{0}\right]}+R_{\left[\binom{1}{2}\right]}$ represent that same class.

Reentering the table with the index pair $\binom{1}{2},\binom{0}{1}$, we find the sets $\left[\binom{0}{1}\right]\cup\left[\binom{1}{0}\right]$ and $\left[\binom{0}{1}\right]\cup\left[\binom{1}{1}\right]$; it follows that each of the six distinct Gramians $I+\sum_{i=1}^{2}R_{[g_i]}$ represent the same class. *Note: If this step had not exhausted the "$m = 2$" case, we would continue to reenter the multiplication table with each new equivalent $\bigcup g_i$ until the class stops growing.*

$\mathbf{m = 3}$: We make use of set complements. Fixing $g, h \in J$, let a satisfy $[g] = \left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]^a[h]$. It follows that $\bigcup_{g'\neq g}[g'] = \left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]^a\bigcup_{h'\neq h}[h']$, since each $M \in \mathrm{GL}(\mathbb{Z}_3^2)$ is a bijection on $\bigcup_{g'\in J}[g']$. We conclude that each of the sums $I+\sum_{i=1}^{3}R_{[g_i]}$ represents the same equivalence class, since g and h were chosen arbitrarily.

Summary: Binary Parseval $\mathbb{Z}_3^2$-frames partition into five automorphic switching equivalence classes, with representative Gramians given by the identity operator, the 9×9 matrix of 1's, and three more representatives

$$I+R_{\left[\binom{1}{0}\right]},\quad I+R_{\left[\binom{1}{0}\right]}+R_{\left[\binom{0}{1}\right]},\ \text{and}\quad I+R_{\left[\binom{1}{0}\right]}+R_{\left[\binom{1}{1}\right]}+R_{\left[\binom{0}{1}\right]}.$$

Hence, the nontrivial Gramians turn out to have ranks 3 ($m = 1$), 5 ($m = 2$), and 7 ($m = 3$). The Gram matrices belonging to a given rank are equivalent, so we partitioned the fourteen nontrivial Gramians $I+\sum_{i=1}^{m}R_{[g_i]}$ into three equivalence classes.

4.4 Binary Parseval group frames as codes

One motivating application of binary Parseval group frames is their use as codes. The range of the analysis operator Θ is the so-called code book in $\mathbb{Z}_2^k$. Each codeword y in this codebook

is the image of a unique vector $x \in \mathbb{Z}_2^n$ which is obtained by $x = \Theta^* y$.

When $k > n$, the redundancy introduced by the embedding Θ makes it possible to accurately recover x from a *corrupted* codeword $\tilde{y} := E\Theta x + \epsilon$, provided the diagonal error matrix E and error vector ϵ are known to meet certain specified conditions.

For our binary case, we consider two types of errors: *erasures* ($\tilde{y} = E\Theta x$, $E_{i,i} \in \{0, 1\}$) and *bit-flips* ($\tilde{y} = \Theta x + \epsilon$, $\epsilon \in \mathbb{Z}_2^J$). We say that a binary Parseval frame $\mathcal{F}$ is *robust to m erasures* if for every diagonal binary matrix E having at most m zeros on the diagonal, the operator $E\Theta$ admits a left inverse. This is equivalent to the condition that the Hamming distance between any two vectors in the image of Θ (or, equivalently, of the Gramian of $\mathcal{F}$) is at least $m + 1$, since any pair of vectors that differ in only m entries are indistinguishable if those entries are "erased." By the linearity of Θ, this is also equivalent to the condition that each nonzero vector in $\Theta\mathbb{Z}_2^n$ has weight exceeding m.

On the other hand, we say that $\mathcal{F}$ is *robust to m bit-flips* if $\|\Theta x_1 - \Theta x_2\|_0 \geq 2m + 1$ for all $x_1, x_2 \in \mathbb{Z}_2^n$, $x_1 \neq x_2$. This notion of "robustness to error" implies the ability to identify each vector in the set $B := \{\Theta x + \epsilon : x \in \mathbb{Z}_2^n, \|\epsilon\|_0 \leq m\}$ as the (corrupted) image of a unique vector in $\mathbb{Z}_2^n$. Note that if $\|\Theta x_1 - \Theta x_2\|_0 = 2m$ for some pair $x_1, x_2 \in \mathbb{Z}_2^n$, then there exist m-weighted error vectors ϵ_1 and ϵ_2 such that $\Theta x_1 + \epsilon_1 = \Theta x_2 + \epsilon_2$. Now suppose that for any distinct $y_1, y_2 \in \Theta\mathbb{Z}_2^n$, we have $\|y_1 - y_2\|_0 \geq 2m + 1$, and let $\tilde{y} \in B$; by the triangle inequality, there is exactly one point $y \in \Theta\mathbb{Z}_2^n$ such that $\|y - \tilde{y}\|_0 \leq m$. Thus, we may recover the intended signal y by identifying the nearest point in $\Theta\mathbb{Z}_2^n$ to $\tilde{y}$, and recovery of $x = \Theta^* y$ follows.

Again appealing to the linearity of Θ, both robustness conditions are expressed in terms of the minimum weight among nonzero vectors in the range of Θ. For Parseval frames, the range of the analysis operator coincides with that of the Gramian, so it can be stated equivalently in terms of the range of the Gramian.

Definition 4.4.1 (Code weight of a Gramian or frame)**.** Given an operator $G : \mathbb{Z}_2^J \to \mathbb{Z}_2^J$, the *code weight* of G is the value $\min_{y \in G(\mathbb{Z}_2^J) \setminus \{0\}} \|y\|_0$.

In the following section, we compare $\mathbb{Z}_p^q$-frames with $\mathbb{Z}_{p^q}$-frames. The final major result in this paper is a proof that every binary Parseval $\mathbb{Z}_{p^q}$-frame is switching equivalent to a $\mathbb{Z}_p^q$-frame. We also include a number of examples in which the classes of Z_{p^q}-frames are mapped to their switching equivalent $\mathbb{Z}_p^q$ frames for select p's and q's and show that in addition to subsuming binary Parseval $\mathbb{Z}_{p^q}$-frames, there are examples of $\mathbb{Z}_p^q$-frames that outperform them as codes.

4.4.1 Comparing frames generated with $\mathbb{Z}_{p^q}$ vs. $\mathbb{Z}_p^q$

Fix $m \in \mathbb{N}$, and let $\mathcal{F}_1$ and $\mathcal{F}_2$ be switching equivalent binary Parseval frames. Theorem 4.9 in [4] establishes that this equivalence implies that $\mathcal{F}_1$ is robust to m erasures if and only if

$\mathcal{F}_2$ is. By the Gramian code weight characterization of robustness to each type of error, it follows that $\mathcal{F}_1$ is robust to m bit-flips if and only if $\mathcal{F}_2$ is. Theorem 4.11 in [5] characterizes switching equivalence between binary Parseval frames as permutation equivalence between their Gramians G_1 and G_2:

$$\mathcal{F}_1 \cong_{\text{sw}} \mathcal{F}_2 \quad \text{if and only if} \quad G_1 = P^* G_2 P \text{ for some permutation matrix } P.$$

Hence, for the purposes of evaluating binary Parseval group frames as codes, whether we are concerned about erasures or bit-flips, we may restrict our attention to permutation equivalence classes of the Gramians of such frames.

Applying the techniques in this paper, we have classified binary Parseval group frames for each of the groups below, using Gramians as class representatives. Recalling that the quantity of vectors in a group frame is given by the size of the group, and that the rank of the Gramian is the dimension of the inducing frame, we can directly compare the performance of several frames as error-correcting codes. To facilitate comparing $\mathbb{Z}_{p^q}$ and $\mathbb{Z}_p^q$ for a given pair p, q, we combine details for the two groups in a single table; in each of the comparisons below, $\mathbb{Z}_p^q$-frames perform at least as well as $\mathbb{Z}_{p^q}$-frames, and they often outperform their $\mathbb{Z}_{p^q}$ counterparts. In fact, the exhaustive search of best performing codes associated with binary Parseval frames generated with $\mathbb{Z}_p^q$ is guaranteed to be at least as good as the best codes generated with $\mathbb{Z}_{p^q}$, as shown in Theorem 4.4.6 below.

We now provide a sequence of results which culmintate in the proof of Theorem 4.4.6, which states that, given an odd prime p and $q \in \mathbb{N}$, any binary Parseval $\mathbb{Z}_{p^q}$-frame is switching equivalent a binary Parseval $\mathbb{Z}_p^q$-frame. Practically, this reduces to showing that the Gramian of a binary Parseval $\mathbb{Z}_{p^q}$-frame satisfies the Gram characterization for a $\mathbb{Z}_p^q$-frame for some reindexing. We accomplish this by showing that the symmetric doubling orbits of $\mathbb{Z}_{p^q}$ partition those of $\mathbb{Z}_p^q$, in the sense that for each $n \in \mathbb{Z}_{p^q}$, the matrix $R_{[n]}$ can be written as the sum of matrices in $\{R_{[g]}\}_{g \in \mathbb{Z}_p^q}$.

The map which produces this reindexing is the inverse of the function $\phi : \mathbb{Z}_p^q \to \mathbb{Z}_{p^q}$ given by

$$\phi(g) := \sum_{i=1}^{q} p^{i-1} g_i, \tag{4.8}$$

where the arithmetic is carried out in $\mathbb{Z}_{p^q}$; this mapping is akin to converting from numbers written in base p. It is worth noting that for a given $i \in \{1, 2, \ldots, q-1\}$ and $g \in \mathbb{Z}_p^q$, we have that p^i divides $\phi(g)$ if and only if the first i entries of g are zero; if p^i divides $\phi(g)$ and p^{i+1} does not, then the j-th entry of g, denoted g_j, is nonzero.

We recall a few fundamental properties of finite multiplicative groups in the context of this work. For a given $n \in \mathbb{N}$, we may consider $\mathbb{Z}_n$ as the ring $(\mathbb{Z}_n, \cdot, +)$, in which case the subset of elements having multiplicative inverses forms the multiplicative group $\mathbb{Z}_n^\times := (\mathbb{Z}/n\mathbb{Z})^\times$. The elements of $\mathbb{Z}_n$ that provide elements in $\mathbb{Z}_n^\times$ are those coprime with n.

Here we shall denote the multiplicative subgroup of $\mathbb{Z}_n^\times$ generated by element k as $\langle k\rangle_n^\times := \langle k\rangle_{\mathbb{Z}_n}^\times$.

Proposition 4.4.2. *Let $p, q, k \in \mathbb{N}$ with p prime and $1 < k < p$. Then $\left|\langle k\rangle_{p^q}^\times\right| = p^{q-1}\left|\langle k\rangle_p^\times\right|$ and $x \in \langle k\rangle_{p^q}^\times$ if and only if $x \pmod p \in \langle k\rangle_p^\times$.*

Proof. Note that $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$, since each nonzero element of $\mathbb{Z}_p$ is coprime with p. Recalling that a finite cyclic group of order mn is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$ if m and n are coprime, we have that

$$\mathbb{Z}_{p^q}^\times \cong \mathbb{Z}_{p^{q-1}(p-1)} \cong \mathbb{Z}_{p^{q-1}} \times \mathbb{Z}_{p-1} \cong \mathbb{Z}_{p^{q-1}} \times \mathbb{Z}_p^\times.$$

It follows that $\left|\mathbb{Z}_p^\times\right| = p-1$ and $\left|\mathbb{Z}_{p^q}^\times\right| = p^{q-1}(p-1)$. We consider now the subgroups $\langle k\rangle_p^\times \leq \mathbb{Z}_p^\times$ and $\langle k\rangle_{p^q}^\times \leq \mathbb{Z}_{p^q}^\times$.

Note that $x \in \langle k\rangle_{p^q}^\times$ implies that $x \pmod p \in \langle k\rangle_p^\times$, so that each element in $\langle k\rangle_{p^q}^\times$ may be written in the form $mp + t$ for some $m \in \{0, 1, \ldots, p^{q-1} - 1\}$ and some $t \in \langle k\rangle_p^\times$ considered as an element of $\mathbb{Z}$. It follows that $\left|\langle k\rangle_{p^q}^\times\right| \leq p^{q-1}\left|\langle k\rangle_p^\times\right|$. We shall show equality holds by demonstrating that the reverse inequality holds; the resulting equality will imply that *every* element of $\mathbb{Z}_{p^q}^\times$ of the form $mp + t$ as above is an element of $\langle k\rangle_{p^q}^\times$, completing the characterization $\langle k\rangle_p^\times = \{x \pmod p \mid x \in \langle k\rangle_p^\times\}$.

Let

$$\begin{aligned} \gamma_q : \langle k\rangle_{p^q}^\times &\to \mathbb{Z}_{p^{q-1}} \times \langle k\rangle_p^\times \\ k^j &\mapsto j \times k^j, \end{aligned}$$

where we consider $\mathbb{Z}_{p^{q-1}} \times \langle k\rangle_p^\times$ as a group in the natural way, inheriting its group operation componentwise. For $i, j \in \mathbb{N}$, we have

$$\gamma_q(k^i k^j) = \gamma_q(k^{i+j}) = (i + j, k^{i+j}) = (i, k^i)(j, k^j) = \gamma_q(k^i)\gamma_q(k^j),$$

and thus γ_q is a group homomorphism. Since the orders of the cyclic groups $\mathbb{Z}_{p^{q-1}}$ and $\langle k\rangle_p^\times$ are coprime, it follows that γ_q exhausts its range and that $\left|\gamma_q(\langle k\rangle_{p^q}^\times)\right| = \left|\mathbb{Z}_{p^{q-1}}\right|\left|\langle k\rangle_p^\times\right|$. This implies $\left|\langle k\rangle_{p^q}^\times\right| \geq p^{q-1}\left|\langle k\rangle_p^\times\right|$. We conclude that $\left|\langle k\rangle_{p^q}^\times\right| = p^{q-1}\left|\langle k\rangle_p^\times\right|$ and that $x \in \langle k\rangle_{p^q}^\times$ if and only if $x \pmod p \in \langle k\rangle_p^\times$. □

Corollary 4.4.3. *Let $p, q, k \in \mathbb{N}$ with p prime and $1 < k < p$. Then for each $y \in \mathbb{Z}_{p^q}^\times$,*

$$\left|y\langle k\rangle_{p^q}^\times\right| = p^{q-1}\left|\langle k\rangle_p^\times\right|$$

and $x \in y\langle k\rangle_{p^q}^\times$ if and only if $x \pmod p \in y\langle k\rangle_p^\times \pmod p$.

Proof. Fix $y \in \mathbb{Z}_{p^q}^\times$. Since the cosets of a subgroup partition a group into equal sized sets, the preceding proposition yields $\left|y\langle k\rangle_{p^q}^\times\right| = \left|\langle k\rangle_{p^q}^\times\right| = p^{q-1}\left|\langle k\rangle_p^\times\right|$.

Now, if $x \in y\langle k\rangle_{p^q}^\times$, then $x(\mathrm{mod}\, p) \in y\langle k\rangle_p^\times$. Since

$$\left|\{x \in \mathbb{Z}_{p^q}^\times : x(\mathrm{mod}\, p) \in y\langle k\rangle_p^\times\}\right| = p^{q-1}\left|\langle k\rangle_p^\times\right|,$$

it follows that

$$y\langle k\rangle_{p^q}^\times = \{x \in \mathbb{Z}_{p^q}^\times : x(\mathrm{mod}\, p) \in y\langle k\rangle_p^\times\},$$

and the proof is complete. □

Theorem 4.4.4. *Given $p, q, k \in \mathbb{N}$ with p prime and $1 < k < p$, let $x, y \in \mathbb{Z}_{p^q}$ and define nonnegative integers x', y', j_x, j_y such that $x = x'p^{j_x}$, $y = y'p^{j_y}$, and p divides neither x' nor y'. Then $x \in y\langle k\rangle_{p^q}^\times$ if and only if $j_x = j_y$ and $x'(\mathrm{mod}\, p) \in y'\langle k\rangle_p^\times(\mathrm{mod}\, p)$.*

Proof. Suppose $x \in y\langle k\rangle_{p^q}^\times$, so that $x'p^{j_x} = k^l y'p^{j_y}$ for some $l \in \mathbb{N}$. Then $j_x = j_y$, since k and p are coprime and p is coprime with each of x' and y'. Next, set $r := j_x = j_y$ and write

$$x'p^r \equiv k^l y'p^r(\mathrm{mod}\, p^q). \tag{4.9}$$

Since x and y may be seen as elements in $p^r\mathbb{Z}_{p^p} \cong \mathbb{Z}_{p^{q-r}}$, we may also identify x' and y' as elements of $\mathbb{Z}_{p^{q-r}}^\times \leq Z_{p^{q-r}}$ and note that congruence (4.9) implies

$$x' \equiv k^l y'(\mathrm{mod}\, p^{q-r}).$$

Then, using $y' \in \mathbb{Z}_{p^{q-r}}^\times$, Corollary 4.4.3 yields $x'(\mathrm{mod}\, p) \in y'\langle k\rangle_p^\times(\mathrm{mod}\, p)$.

Conversely, assume $j_x = j_y =: r$ and $x'(\mathrm{mod}\, p) \in y'\langle k\rangle_p^\times(\mathrm{mod}\, p)$. Then the conditions of Corollary 4.4.3 are met for $x, y \in \mathbb{Z}_{p^{q-r}}^\times$ and $x' \equiv k^{l'}y' \pmod{p^{q-r}}$ for some $l' \in \mathbb{N}$. Embedding $y'\langle k\rangle_{p^{q-r}}^\times$ into Z_{p^q} by $g \mapsto p^r g$ for $g \in y'\langle k\rangle_{p^{q-r}}^\times$, we have that $x = x'p^r \equiv 2^{l'}y'p^r \pmod{p^q} = 2^{l'}y$. □

The following lemma makes precise the claim that the map ϕ given by (4.8) maps the doubling orbits of $\mathbb{Z}_p^q$ into those of $\mathbb{Z}_{p^q}$.

Lemma 4.4.5. *Given $p, q \in \mathbb{N}$ with p an odd prime, let $x \in \mathbb{Z}_{p^q}$. If $g \in \phi^{-1}(x\langle 2\rangle_{p^q}^\times)$, then for $h \in \mathbb{Z}_p^q$, we have that $\phi(g\langle 2\rangle_p^\times + h) \subseteq x\langle 2\rangle_{p^q}^\times + \phi(h)$. As a consequence, $\phi(\phi^{-1}(x\langle 2\rangle_{p^q}^\times) + h) = x\langle 2\rangle_{p^q}^\times + \phi(h)$.*

Proof. We begin by proving the lemma for the case that $h = 0$. Let x, p and q be as in the hypothesis, and let $g = \phi^{-1}(x)$. Since $\langle 2\rangle_p^\times$ is cyclic, it suffices to show that for each $g' \in \phi^{-1}(x\langle 2\rangle_{p^q}^\times)$ there exists $k \in \mathbb{N}$ such that $\phi(2g') = 2^k x$; since $\langle 2\rangle_{p^q}^\times$ is cyclic, it suffices to demonstrate this for the case $g' = g$.

If $x = 0$ then $g = (0)_{i=1}^{q}$, and the claim is shown; assume, then, that $x \neq 0$ and define nonnegative integers x' and r such that $x = x'p^r$ and p does not divide x'. Note that r gives the quantity of leading zeros in the sequence $(g_i)_{i=1}^{q}$.

Expressing this equality in terms of the definition of ϕ,

$$\sum_{i=1}^{q} p^{i-1}(2g_i \,(\mathrm{mod}\, p)) \equiv 2^k x \,(\mathrm{mod}\, p^q),$$

where $2g_i \,(\mathrm{mod}\, p)$ is considered as an element of $\mathbb{Z}$. For each $i \in [\![q]\!]$, we may express $2g_i \,(\mathrm{mod}\, p)$ as $2g_i - \delta_i p$ for some $\delta_i \in \{0, 1\}$, since the value is either $2g_i$ or $2g_i - p$. Since $i \leq r$ implies $g_i = 0$, it follows that $\delta_i = 0$ for such i. Thus

$$\begin{aligned}
\phi(2g) &\equiv \sum_{i=1}^{q} p^{i-1}(2g_i - \delta_i p) \pmod{p^q} \\
&\equiv 2\sum_{i=1}^{q} p^{i-1} g_i - \sum_{i=1}^{q} \delta_i p^i \pmod{p^q} \\
&\equiv 2\phi(g) - \sum_{i=r+1}^{q} \delta_i p^i \pmod{p^q}.
\end{aligned}$$

It follows that $2\phi(g) - \sum_{i=r+1}^{q} \delta_i p^i \equiv 2\phi(g) \,(\mathrm{mod}\, p^r)$. The conditions given in Theorem 4.4.4 are thus satisfied for x and $\phi(2g)$, implying $\phi(2g) \in 2\phi(g)\langle 2\rangle_{p^q}^{\times} = 2x\langle 2\rangle_{p^q}^{\times} = x\langle 2\rangle_{p^q}^{\times}$. We conclude that $\phi(2^j g) \in x\langle 2\rangle_{p^q}^{\times}$ for all $j \in \mathbb{N}$.

We now consider the general case, letting $h \in \mathbb{Z}_p^q$. Again, since $\langle 2\rangle_p^{\times}$ and $\langle 2\rangle_{p^q}^{\times}$ are cyclic, we may assume that $g = \phi^{-1}(x)$. We must show that $\phi(g + h) = 2^j x + \phi(h)$ for some j. Similar to the $h = 0$ case, we define δ_i' so that $g_i + h_i - \delta_i' p \in \{0, 1, \ldots, p-1\}$ for each $i \in [\![q]\!]$. Recalling that the value r gives the number of leading zeros of g, we note that $\delta_i = \delta_i' = 0$ for $i \leq r$. Then

$$\begin{aligned}
\phi(g + h) &\equiv \sum_{i=1}^{q} p^{i-1}(g_i + h_i - \delta_i' p) \pmod{p^q} \\
&\equiv \phi(g) + \phi(h) - \sum_{i=1}^{q} \delta_i' p^i \pmod{p^q} \\
&\equiv x - \sum_{i=r+1}^{q} \delta_i' p^i + \phi(h) \pmod{p^q} \\
&\in x\langle 2\rangle_{p^q}^{\times} + \phi(h)
\end{aligned}$$

by Theorem 4.4.4, since $x - \sum_{i=r+1}^{q} \delta_i' p^i \equiv x \,(\mathrm{mod}\, p^r)$. We conclude that $\phi(g\langle 2\rangle_p^{\times} + h) \subseteq x\langle 2\rangle_{p^q}^{\times} + \phi(h)$ for all $g \in \phi^{-1}(x\langle 2\rangle_{p^q}^{\times})$ and $h \in \mathbb{Z}_p^q$.

It follows that $\phi(\phi^{-1}(x\langle 2\rangle_{p^q}^{\times}) + h) \subseteq x\langle 2\rangle_{p^q}^{\times} + \phi(h)$. Set equality follows from the fact that ϕ is a bijection, since both sides of the inclusion have the same number of elements. $\square$

We are ready to prove the section's main result. We wish to show that for each Gramian of a binary Parseval $\mathbb{Z}_{p^q}$-frame, the corresponding Gramian indexed by $\mathbb{Z}_p^q$, as obtained from the reindexing given by ϕ^{-1}, is in the group algebra $\mathbb{Z}_2[\mathbb{Z}_p^q]$; this is sufficient to show that the underlying frame is a binary Parseval $\mathbb{Z}_p^q$-frame, since the Gramian retains idempotence, symmetry and the weights of range vectors under switching.

Theorem 4.4.6. *Let $p, q \in \mathbb{N}$ with p an odd prime and define $\phi : \mathbb{Z}_p^q \to \mathbb{Z}_{p^q}$ by $\phi(g) := \sum_{i=1}^{q} p^{i-1} g_i$, carrying out the arithmetic in $\mathbb{Z}_{p^q}$. If $\mathcal{F} = \{f_x\}_{x \in \mathbb{Z}_{p^q}}$ is a binary Parseval $\mathbb{Z}_{p^q}$-frame for $\mathbb{Z}_2^n$, then $\mathcal{F}' := \{f_{\phi^{-1}(x)}\}_{x \in \mathbb{Z}_{p^q}}$ is a binary Parseval $\mathbb{Z}_p^q$-frame.*

Proof. Let $\mathcal{F} = \{f_x\}_{x \in \mathbb{Z}_{p^q}}$ be a binary Parseval $\mathbb{Z}_{p^q}$-frame for $\mathbb{Z}_2^n$. Denote the frame's analysis matrix and Gramian by $\Theta_{\mathcal{F}}$ and G, respectively, and let $\Theta_{\mathcal{F}'}$ and G' denote those of $\mathcal{F}'$. Since G and G' are switching equivalent, G' inherits symmetry, idempotence and column weights from G. By the characterization of binary Parseval group frames given by Theorem 4.3.4, it is then left to show that G' is a element of the group algebra of the right regular representation of $\mathbb{Z}_p^q$, denoted $\mathbb{Z}_2[\{R'_g\}]$.

Let $R := \{R_x\}_{x \in \mathbb{Z}_{p^q}}$ be the right regular representation of $\mathbb{Z}_{p^q}$ and let η be the binary coefficient function such that $G = \sum_{x \in \mathbb{Z}_{p^q}} \eta(x) R_x$, as guaranteed by Theorem 4.3.9. Since $\mathbb{Z}_{p^q}$ is an odd-ordered abelian group and η is idempotent under convolution, Theorem 4.3.13 provides that η is constant on cosets of the the multiplicative subgroup $\langle 2 \rangle_{p^q}^{\times}$. We shall demonstrate that ϕ induces an isomorphism between the sets $\{\sum_{y \in x\langle 2 \rangle_{p^q}^{\times}} R_y\}_{x \in \mathbb{Z}_{p^q}}$ and $\{\sum_{y \in x\langle 2 \rangle_{p^q}^{\times}} R'_{\phi^{-1}(y)}\}_{x \in \mathbb{Z}_{p^q}}$.

Let $\Phi : \mathbb{Z}_2^{Z_p^q} \to \mathbb{Z}_2^{Z_{p^q}}$ be defined on standard basis elements by $\Phi e'_g = e_{\phi(g)}$, where we use the $'$ (prime) to distinguish basis elements of the domain from those in the range. We wish to show that for each $x, z \in \mathbb{Z}_{p^q}$, the following holds:

$$\sum_{y \in x\langle 2 \rangle_{p^q}^{\times}} R_y e_z = \Phi\Bigg(\sum_{y \in x\langle 2 \rangle_{p^q}^{\times}} R'_{\phi^{-1}(y)} e'_{\phi^{-1}(z)} \Bigg). \tag{4.10}$$

As described in Section 4.2.4, we may explicitly express the image a function φ under R_y by $R_y\varphi : z \mapsto \varphi(y + z)$, and Eq. (4.10) becomes

$$\begin{aligned} \sum_{y \in x\langle 2 \rangle_{p^q}^{\times}} e_{y+z} &= \Phi\Bigg(\sum_{y \in x\langle 2 \rangle_{p^q}^{\times}} e'_{\phi^{-1}(y)+\phi^{-1}(z)} \Bigg) \\ &= \sum_{y \in x\langle 2 \rangle_{p^q}^{\times}} e'_{\phi(\phi^{-1}(y)+\phi^{-1}(z))}. \end{aligned}$$

Thus, we are left to show that $x\langle 2 \rangle_{p^q}^{\times} + z = \phi(\phi^{-1}(x\langle 2 \rangle_{p^q}^{\times}) + \phi^{-1}(z))$ for any $x, z \in \mathbb{Z}_{p^q}$. Taking $h := \phi^{-1}(z)$, this is exactly the content of Lemma 4.4.5, and the proof is complete. □

We illustrate this statement with some examples. It is worth noting ahead of the examples that there is an important distinction between the symmetric doubling orbit partitionings of $\mathbb{Z}_p^q$ and $\mathbb{Z}_{p^q}$. For an odd prime p, it is a simple exercise to show that each $[x]$ in $\mathbb{Z}_p^q$ that is not $[e]$ has the same order as the symmetric doubling orbit of 1 in $\mathbb{Z}_p$. In contrast, according to Theorem 4.4.4, $\mathbb{Z}_{p^q}$ partitions into kq nontrivial orbits for some $k \in \mathbb{N}$, k of each of q different sizes. Since automorphisms preserve symmetric doubling orbits (Proposition 4.3.19), they also preserve orbit size; it follows that the computational savings offered by applying Corollary 4.3.21 as in Example 4.3.24 do not apply or are significantly reduced when the group under consideration is $\mathbb{Z}_{p^q}$. In fact, for the values of p and q we explore here, the 2^q binary Parseval $\mathbb{Z}_{p^q}$-frame unitary equivalence classes promised by Corollary 4.3.18 coincide with automorphic switching equivalence classes. As we note in our closing remarks regarding $\mathbb{Z}_{17^q}$, this does not hold in general. Of course, the number of symmetric doubling orbits of $\mathbb{Z}_{p^q}$ grows linearly in q and may be considered as subsets of symmetric doubling orbits of Z_p^q (Theorem 4.4.6), whose number grows exponentially as $(p^q - 1)/\big|[g]\big|$ for any $g \in \mathbb{Z}_p^q \backslash \{e\}$.

The next step is to compute the code weight of each of the Gramians. We pause to reflect on the computational savings made available by the methods developed thus far. Results in [4] justify the use of Gramians as class representatives of binary Parseval frames as codes; for a group of size k, the naive upper bound of 2^{k^2} binary matrices thereby drops to $2^{\frac{1}{2}k(k-1)}(2^k - 1)$ symmetric binary matrices with at least one odd column. Theorem 4.3.1 in this paper puts our Gramians in $\mathbb{Z}_2[\{R_g\}]$, a set whose size is of order 2^k. In the case of abelian Γ with unique square roots, Corollary 4.3.18 gives the number of Gramians of binary Parseval Γ-frames exactly as $2^{|\Gamma'|-1}$, where $|\Gamma'| \leq \frac{1}{2}(k+1)$ is the quantity of symmetric doubling orbits of Γ. Thus, for a given abelian group Γ of odd order k, we must process no more than $2^{|\Gamma'|-1} \leq 2^{\frac{1}{2}(k-1)}$ Gramians to determine code weights, and these matrices can be computed directly. We may process even fewer Gramians if we reduce the set to representatives of automorphic switching equivalence classes. Note that in determining the code weight of a $k \times k$ Gramian G, the $2^{\operatorname{rank}(G)}$ vectors in the operator's range may be obtained by taking all linear combinations of up to $\operatorname{rank}(G)$ columns of G, for a total $\sum_{i=1}^{\operatorname{rank}(G)} \binom{k}{i}$ operations; comparing this combinatorial problem with the algorithm above, it is evident that computational savings result from any reduction in the quantity of Gramians we are to process.

Let us first consider the work for $\mathbb{Z}_3^2$ and $\mathbb{Z}_3^3$ to illustrate this.

Example 4.4.7. The nontrivial Gramians in Example Example 4.3.24 turn out to have ranks 3 ($m = 1$), 5 ($m = 2$), and 7 ($m = 3$), and thus require $\binom{9}{3}$, $\binom{9}{5}$, and $\binom{9}{7}$ computations to exhaust linear combinations of columns as described. For the cost of producing a 3×4 multiplication table and a computing a handful of table look-ups and comparisons, we partitioned the fourteen nontrivial Gramians $I + \sum_{i=1}^{m} R_{[g_i]}$ into three classes; the return on that cost in the form of having fewer Gramians to weight-check was the reduction from $4 \cdot \binom{9}{3} + 6 \cdot \binom{9}{5} + 4 \cdot \binom{9}{7} = 1236$ computations to $\binom{9}{3} + \binom{9}{5} + \binom{9}{7} = 246$.

The group $\mathbb{Z}_3^3$ has 14 symmetric doubling orbits, including $[e]$. The characterization of automorphic switching equivalence classes given by Corollary 4.3.21 provides that the 2^{13}

unique Gramians of binary Parseval $\mathbb{Z}_3^3$-frames reduce to only thirty representatives. The resulting computational savings are substantial even before taking into account the cost of finding code weights, which has grown to $\sum_{i=1}^{\operatorname{rank}(G)} \binom{27}{i}$ operations per Gramian.

4.4.1.1 Format of comparison tables

Each comparison table contains representatives of switching equivalence classes of binary Parseval Γ-frames for each of the groups we compare. For each such class, we provide the rank and code weight of the representing Gramian. After the first table, we exclude the trivial Gramians given by the identity and the matrix of all ones; the Gramians themselves are encoded as indexing elements of their symmetric doubling orbit summands. Whenever a class in $\mathbb{Z}_{p^q}$ matches the performance of a class in $\mathbb{Z}_p^q$, the two classes are described in the same row of the associated table. In many such cases, the two classes represent switching equivalent frames.

In the comparison of $\mathbb{Z}_3^2$ and $\mathbb{Z}_9$, for example, the Gramians given by $G_1 = \sum_{g\in J_1} R_{[g]}$ with $J_1 = \{\binom{0}{0},\binom{1}{0},\binom{1}{1},\binom{0}{1}\} \subset \mathbb{Z}_3^2$ and $G_2 = \sum_{g\in J_2} R_{[g]}$ with $J_2 = \{0,1\} \subset \mathbb{Z}_9$ each have rank 7 and code weight 2, and thus are listed in the same row.

Example 4.4.8 ($\mathbb{Z}_9$ vs. $\mathbb{Z}_3^2$)**.** The symmetric doubling orbit partitioning of $\mathbb{Z}_9$ consists of $[0]$, $[3] = \{3,6\}$, and $[1] = \{1,2,4,5,7,8\}$. In this case, each of the four binary Parseval $\mathbb{Z}_9$-frames is switching equivalent to one of the five binary Parseval $\mathbb{Z}_3^2$-frames delineated in Example 4.3.24. Apart from the trivial cases of the Gramian being the identity matrix or the matrix of all 1's, this correspondence

$$I + R_{\left[\binom{1}{0}\right]} = I + R_{[3]} \text{ and } \quad I + R_{\left[\binom{1}{0}\right]} + R_{\left[\binom{1}{1}\right]} + R_{\left[\binom{0}{1}\right]} = I + R_{[1]},$$

assumes an appropriate identification of group elements. Table 4.2 provides the implications for the performance of codes.

Table 4.2: Comparing Parseval frames with Gramians $G = \sum_{g\in J} R_{[g]}$ obtained from groups $\mathbb{Z}_3^2$ and $\mathbb{Z}_9$, together with their code weights. See Example 4.4.8 for details.

Gram rank	Code weight	$J \subset \mathbb{Z}_3^2$	$J \subset \mathbb{Z}_9$
1	1	$\{\binom{0}{0},\binom{1}{0},\binom{1}{1},\binom{0}{1},\binom{1}{2}\}$	$\{0,1,3\}$
3	3	$\{\binom{0}{0},\binom{1}{0}\}$	$\{0,3\}$
5	3	$\{\binom{0}{0},\binom{1}{0},\binom{1}{1}\}$	–
7	2	$\{\binom{0}{0},\binom{1}{0},\binom{1}{1},\binom{0}{1}\}$	$\{0,1\}$
9	1	$\{\binom{0}{0}\}$	$\{0\}$

Table 4.3: Comparing Parseval frames with Gramians $G = \sum_{g \in J} R_{[g]}$ obtained from groups $\mathbb{Z}_3^3$ and $\mathbb{Z}_{27}$, together with their code weights. See Example 4.4.9.

Gram rank	Code weight	$J \subset \mathbb{Z}_3^3$	$J \subset \mathbb{Z}_{27}$
3	9	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{1}, \binom{0}{2}\right\}$	{0,3,9}
5	9	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{0}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{2}{0}\right\}$	–
7	6	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{1}, \binom{2}{0}, \binom{2}{1}\right\}$	{0,1,9}
7	9	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{1}, \binom{1}{1}\right\}$	–
9	3	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}\right\}$	{0,9}
9	6	$\left\{\binom{0}{0}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{1}, \binom{1}{1}\right\}$	–
9	8	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{1}, \binom{2}{0}\right\}$	–
11	3	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{1}, \binom{2}{1}\right\}$	–
11	6	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}\right\}$	–
11	6	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{2}, \binom{2}{0}\right\}$	–
13	3	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{2}, \binom{2}{0}\right\}$	–
13	4	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{2}, \binom{2}{0}, \binom{2}{1}\right\}$	–
13	6	$\left\{\binom{0}{0}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}\right\}$	–
13	6	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{1}, \binom{1}{2}, \binom{2}{0}\right\}$	–
15	3	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}\right\}$	–
15	3	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{2}{0}\right\}$	–
15	4	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{2}{0}\right\}$	–
15	5	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{1}, \binom{1}{0}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{1}, \binom{2}{0}, \binom{2}{1}\right\}$	–
17	3	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}\right\}$	–

Continued on next page

Table 4.3 – *Continued from previous page*

Gram rank	Code weight	$J \subset \mathbb{Z}_3^3$	$J \subset \mathbb{Z}_{27}$
17	3	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{1}, \binom{1}{2}\right\}$	–
17	4	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}\right\}$	–
19	2	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{1}, \binom{1}{2}, \binom{2}{0}, \binom{2}{1}\right\}$	{0,1,3}
19	3	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{1}, \binom{1}{0}, \binom{1}{1}\right\}$	–
19	3	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{2}, \binom{2}{0}\right\}$	–
21	2	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{2}\right\}$	{0,3}
21	3	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{1}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{2}{0}\right\}$	–
23	2	$\left\{\binom{0}{0}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{1}\right\}$	–
25	2	$\left\{\binom{0}{0}, \binom{0}{0}, \binom{0}{1}, \binom{0}{1}, \binom{0}{2}, \binom{1}{0}, \binom{1}{0}, \binom{1}{1}, \binom{1}{1}, \binom{2}{0}, \binom{2}{1}\right\}$	{0,1}

Example 4.4.9 ($\mathbb{Z}_{27}$ vs. $\mathbb{Z}_3^3$, see Table 4.3)**.** The symmetric doubling orbit partitioning of $\mathbb{Z}_{27}$ consists of $[0]$, $[9] = \{9, 18\}$, $[3] = \{3, 6, 12, 15, 21, 24\}$, and $[1] = \mathbb{Z}_{27} \backslash ([0] \cup [9] \cup [3])$. The eight resulting Gramians each represent a distinct automorphic switching equivalence class of binary Parseval $\mathbb{Z}_{27}$-frames. The group $\mathbb{Z}_3^3$, as mentioned in Example 4.4.7, has 13 nontrivial symmetric doubling orbits and generates 30 automorphic switching equivalence classes of binary Parseval group frames.

Example 4.4.10 ($\mathbb{Z}_{125}$ vs. $\mathbb{Z}_5^3$, see Table 4.5)**.** The symmetric doubling orbit partitioning of $\mathbb{Z}_{125}$ consists of $[0]$ and three orbits, having orders $\big|[25]\big| = 4$, $\big|[5]\big| = 20$, $\big|[1]\big| = 100$. As with with the other $\mathbb{Z}_{p^q}$ cases thus far, the symmetric doubling orbits of $\mathbb{Z}_{125}$ are invariant under automorphism on $\mathbb{Z}_{125}$. It follows that the eight distinct Gramians induced by the three nontrivial symmetric doubling orbits represent eight distinct classes of binary Parseval $\mathbb{Z}_{125}$-frames.

The symmetric doubling orbit partitioning of $\mathbb{Z}_5^3$ consists of $[e]$ and 31 orbits of order 4. The 2^{31} distinct Gramians, each representing a distinct unitary equivalence class of binary Parseval $\mathbb{Z}_5^3$-frames, reduce to 7152 automorphic switching equivalence classes. Obtained by applying the algorithm described in this paper implemented in Matlab [58], Table 4.4 gives a breakdown of the these classes by the size of J:

Table 4.4: Number of nonzero terms $|J|$ summed in $\sum_{g\in J} R_{[g]}$ and number $\mathbf{N_{|J|}}$ of resulting automorphic switching equivalence classes.

$\|J\|$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mathbf{N_{\|J\|}}$	**1**	**1**	**1**	**2**	**3**	**5**	**12**	**22**	**42**	**92**	**174**	**296**	**476**	**669**	**832**	**948**
$\|J\|$	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16

The $\overline{\frac{0}{1}}$ entry corresponds to the identity matrix and the $\overline{\frac{31}{1}}$ entry, the matrix of all 1's. The counting the bottom row, which gives the total number of automorphically switching equivalent classes per quantity of nontrivial symmetric doubling orbit summands, sums to 7152.

For obvious reasons, we do not list representatives from each of the 7152 automorphism equivalence classes. Instead, the comparisons in Table 4.5 place each of the six nontrivial Gramians of binary Parseval $\mathbb{Z}_{125}$-frames next to a $\mathbb{Z}_5^3$ representative of the same rank and having maximal code weight among binary Parseval $\mathbb{Z}_5^3$-frames of the same dimension.

Table 4.5: Comparing groups $\mathbb{Z}_5^3$ and $\mathbb{Z}_{125}$ as generators of binary Parseval frames, best performers for each given rank of the Gramian. See Example 4.4.10.

$J \subset \mathbb{Z}_5^3$	Code weight	**Gram rank**	Code weight	$J \subset \mathbb{Z}_{125}$
$\left\{\binom{0}{0}_5, \binom{0}{0}_5, \binom{1}{1}_5, \binom{1}{1}_5, \binom{1}{2}_5, \binom{1}{3}_5, \binom{1}{4}_5\right\}$	25	**5**	25	{0,5,25}
$\left\{\binom{0}{0}_5, \binom{0}{0}_5, \binom{1}{0}_5, \binom{1}{0}_5, \binom{1}{0}_5, \binom{1}{0}_5, \binom{1}{3}_5, \binom{1}{3}_5, \binom{1}{4}_5, \binom{1}{2}_5, \binom{1}{2}_5, \binom{1}{3}_5\right\}$	25	**21**	10	{0,1,25}
$\left\{\binom{0}{0}_5, \binom{0}{1}_5, \binom{0}{1}_5, \binom{1}{0}_5, \binom{1}{0}_5, \binom{1}{1}_5, \binom{1}{1}_5, \binom{1}{2}_5, \binom{1}{2}_5, \binom{1}{3}_5\right\}$	25	**25**	5	{0,25}
$\left\{\binom{0}{0}_5, \binom{0}{0}_5, \binom{0}{1}_5, \binom{1}{0}_5, \binom{1}{3}_5, \binom{1}{2}_5, \binom{1}{3}_5\right\}$	5	**101**	2	{0,1,5}
$\left\{\binom{0}{0}_5, \binom{0}{1}_5, \binom{0}{1}_5, \binom{0}{1}_5, \binom{0}{1}_5, \binom{0}{1}_5, \binom{1}{0}_5, \binom{1}{1}_5, \binom{1}{1}_5, \binom{1}{2}_5, \binom{1}{2}_5, \binom{1}{2}_5, \binom{1}{3}_5, \binom{1}{3}_5, \binom{1}{3}_5, \binom{1}{4}_5, \binom{1}{4}_5, \binom{1}{4}_5, \binom{1}{4}_5\right\}$	5	**105**	2	{0,5}
$\left\{\binom{0}{0}_5, \binom{0}{1}_5, \binom{0}{1}_5, \binom{0}{1}_5, \binom{0}{1}_5, \binom{0}{1}_5, \binom{1}{0}_5, \binom{1}{0}_5, \binom{1}{0}_5, \binom{1}{0}_5, \binom{1}{0}_5, \binom{1}{0}_5, \binom{1}{2}_5, \binom{1}{2}_5, \binom{1}{2}_5, \binom{1}{2}_5, \binom{1}{3}_5, \binom{1}{3}_5, \binom{1}{3}_5, \binom{1}{3}_5, \binom{1}{4}_5, \binom{1}{4}_5, \binom{1}{4}_5, \binom{1}{4}_5\right\}$	2	**121**	2	{0,1}

Appendix A

Distance conversions

A.1 Exchange rates: formulas relating metrics

The proof of Lemma 2.2.8 demonstrates and uses the fact that $\langle \mathbf{x}, \mathbf{y} \rangle = n - 2\mathrm{d_H}(\mathbf{x}, \mathbf{y})$ for $\mathbf{x}, \mathbf{y} \in Q_n$. Indeed, sets of binary vectors offer a number of potentially useful reformulations of the distances between elements. The following tables of "exchange rates" provide a useful reference when restricting attention to certain binary we shall see in later chapters. NOTE: For compactness and consistency of notation, especially within the following tables, the symbols d_1 and d_2 represent the ℓ_1 and ℓ_2 metrics, respectively. That is, for a vector space V,

$$\begin{aligned} \mathrm{d}_1 : V \times V &\to \mathbb{R} \\ \mathbf{x} \times \mathbf{y} &\mapsto \|\mathbf{x} - \mathbf{y}\|_1 \end{aligned} \qquad \begin{aligned} \mathrm{d}_2 : V \times V &\to \mathbb{R} \\ \mathbf{x} \times \mathbf{y} &\mapsto \|\mathbf{x} - \mathbf{y}\|_2 \ . \end{aligned}$$

A.1.1 Formulas on $Q_n := \{-1, 1\}^n \subset \mathbb{R}^n$

Normalizing factors: For $\mathbf{x} \in Q_n$, we have

$$\|\mathbf{x}\|_0 = n, \quad \|\mathbf{x}\|_1 = n, \quad \|\mathbf{x}\|_2 = \sqrt{n}.$$

Distances between vectors: For $\mathbf{x}, \mathbf{y} \in Q_n$, we have just noted that Lemma 2.2.8 yields $\langle \mathbf{x}, \mathbf{y} \rangle = n - 2\mathrm{d_H}(\mathbf{x}, \mathbf{y})$. Additionally, combining the d_2 normalization factor on Q_n (i.e., $\|\mathbf{z}\|_2 = \sqrt{n}$ for all $\mathbf{z} \in Q_n$) with the definition $\mathrm{d_g}(\mathbf{x}, \mathbf{y}) := \frac{1}{\pi} \cos^{-1}\left(\frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\|_2 \|\mathbf{y}\|_2}\right)$ yields the equivalence $\langle \cdot, \cdot \rangle \equiv n \cos(\pi \mathrm{d_g})$ on Q_n. Applying the trigonometric identity $\sin^2 \frac{\theta}{2} = \frac{1}{2} - \frac{1}{2} \cos\theta$, we have

$$2\mathrm{d_H} \ \equiv \ n - \langle \cdot, \cdot \rangle \ \equiv \ n - n\cos(\pi \mathrm{d_g}) \ \equiv \ 2n \sin^2(\pi \mathrm{d_g}/2) \quad \text{on } Q_n. \tag{A.1}$$

Still considering $\mathbf{x}, \mathbf{y} \in Q_n$, we note that $|x_i - y_i| \in \{0, 2\}$ for each index i and that $\mathrm{d_H}(\mathbf{x}, \mathbf{y}) = \big|\{i : x_i - y_i \neq 0\}\big|$. From this, we deduce that $\|\mathbf{x} - \mathbf{y}\|_1 = 2\mathrm{d_H}(\mathbf{x}, \mathbf{y})$ and that $\|\mathbf{x} - \mathbf{y}\|_2^2 =$

$2^2 \mathrm{d_H}(\mathbf{x}, \mathbf{y})$, or, compactly, that

$$4\mathrm{d_H} \equiv 2\mathrm{d_1} \equiv \mathrm{d_2^2} \quad \text{on } Q_n. \tag{A.2}$$

The balance of the details in Table A.1 may be obtained from simple manipulations of the equivalences given in Eqs. (A.1) and (A.2) above.

Table A.1: Equivalences among pairwise comparisons for vectors in Q_n, as demonstrated in Appendix A.1.1. The equality $\mathrm{d_H} = \frac{1}{2}\mathrm{d_1}$ means $\mathrm{d_H}(\mathbf{x}, \mathbf{y}) = \frac{1}{2}\|\mathbf{x} - \mathbf{y}\|_1$ for $\mathbf{x}, \mathbf{y} \in Q_n$.

$$\begin{array}{rcccccccc}
\mathrm{d_H} & = & n\mathrm{d_h} & = & \frac{1}{2}\mathrm{d_1} & = & \frac{1}{4}\mathrm{d_2^2} & = \frac{1}{2}(n - \langle \cdot, \cdot \rangle) = & n\sin^2(\frac{\pi}{2}\mathrm{d_g}) \\
\frac{1}{n}\mathrm{d_H} & = & \mathrm{d_h} & = & \frac{1}{2n}\mathrm{d_1} & = & \frac{1}{4n}\mathrm{d_2^2} & = \frac{1}{2} - \frac{1}{2n}\langle \cdot, \cdot \rangle = & \sin^2(\frac{\pi}{2}\mathrm{d_g}) \\
2\mathrm{d_H} & = & 2n\mathrm{d_h} & = & \mathrm{d_1} & = & \frac{1}{2}\mathrm{d_2^2} & = n - \langle \cdot, \cdot \rangle = & 2n\sin^2(\frac{\pi}{2}\mathrm{d_g}) \\
4\mathrm{d_H} & = & 4n\mathrm{d_h} & = & 2\mathrm{d_1} & = & \mathrm{d_2^2} & = 2(n - \langle \cdot, \cdot \rangle) = & 4n\sin^2(\frac{\pi}{2}\mathrm{d_g}) \\
n - 2\mathrm{d_H} & = & n - 2n\mathrm{d_h} & = & n - \mathrm{d_1} & = & n - \frac{1}{2}\mathrm{d_2^2} & = \langle \cdot, \cdot \rangle = & n\cos(\pi \mathrm{d_g}) \\
1 - \frac{2}{n}\mathrm{d_H} & = & 1 - 2\mathrm{d_h} & = & 1 - \frac{1}{n}\mathrm{d_1} & = & 1 - \frac{1}{2n}\mathrm{d_2^2} & = \frac{1}{n}\langle \cdot, \cdot \rangle = & \cos(\pi \mathrm{d_g})
\end{array}$$

A.1.2 Formulas on $\Sigma_s^n := \{\mathbf{x} \in \Sigma^n : \|\mathbf{x}\|_1 = s\}$

When we examine the distances between $\{0, 1\}$-binary vectors in later sections, the vectors will have the same *sparsity*—that is, they will have the same quantity of nonzero entries.

Normalizing factors: For $\mathbf{x} \in \Sigma_s^n$, we have

$$\|\mathbf{x}\|_0 = s, \quad \|\mathbf{x}\|_1 = s, \quad \|\mathbf{x}\|_2 = \sqrt{s}.$$

Distances between vectors: Recall that $\|\cdot\|_0 \equiv \mathrm{d_H}$ on any vector space. Now, given $\mathbf{x}, \mathbf{y} \in \Sigma_s^n$, we have that $|x_i - y_i| \in \{0, 1\}$ for $i \in \{1, 2, \ldots, n\}$; together these facts yield

$$\|\mathbf{x} - \mathbf{y}\|_1 = \sum_{i=1}^{n} |x_i - y_i| = \|\mathbf{x} - \mathbf{y}\|_0 = \mathrm{d_H}(\mathbf{x}, \mathbf{y}) \quad \text{for } \mathbf{x}, \mathbf{y} \in \Sigma_s^n. \tag{A.3}$$

Furthermore, since $\|\mathbf{x} - \mathbf{y}\|_2^2 = \sum_{i=1}^n |x_i - y_i|^2 = \sum_{i=1}^n |x_i - y_i|$, we may extend the equivalences in Eq. (A.3) to read $\mathrm{d_1} \equiv \mathrm{d_H} \equiv \mathrm{d_2^2}$ on Σ_s^n.

Next, we can partition the set of "mismatched entries" between $\mathbf{x}$ and $\mathbf{y}$ by

$$\begin{aligned}
\{i : x_i - y_i \neq 0\} &= \{i : x_i - y_i = -1\} \cup \{i : x_i - y_i = 1\} \\
&= \{i : x_i = 0, y = 1\} \cup \{i : x_i = 1, y_i = 0\},
\end{aligned}$$

allowing us to derive the exchange between $\mathrm{d_H}$ and the inner product:

$$\underbrace{\mathrm{d_H}(\mathbf{x},\mathbf{y})}_{\#\text{ of mismatched entries}} = \underbrace{\overbrace{s}^{|\{i:x_i=1\}|} - \overbrace{\langle \mathbf{x},\mathbf{y}\rangle}^{|\{i:x_i=1=y_i\}|}}_{\#\text{ of mismatches where } x=1} + \underbrace{\overbrace{s}^{|\{i:y_i=1\}|} - \overbrace{\langle \mathbf{x},\mathbf{y}\rangle}^{|\{i:x_i=1=y_i\}|}}_{\#\text{ of mismatches where } y=1} = 2(s - \langle \mathbf{x},\mathbf{y}\rangle).$$

Finally, applying the $\mathrm{d_2}$ normalizing factor on Σ_s^n within the definition of $\mathrm{d_g}$ yields $\langle\cdot\rangle = s\cos(\pi \mathrm{d_g})$, and the equivalences in Table A.2 can be filled in through algebraic manipulation.

Table A.2: Equivalences among pairwise comparisons for vectors in Σ_s^n, as demonstrated in Appendix A.1.2.

$$\begin{array}{ccccccccc}
\mathrm{d_H} & = & n\mathrm{d_h} & = & \mathrm{d_1} & = & \mathrm{d_2^2} & = 2s - 2\langle\cdot,\cdot\rangle & = 4s\sin^2(\frac{\pi}{2}\mathrm{d_g}) \\
s - \frac{1}{2}\mathrm{d_H} & = & s - \frac{n}{2}\mathrm{d_h} & = & s - \frac{1}{2}\mathrm{d_1} & = & s - \frac{1}{2}\mathrm{d_2^2} & = \langle\cdot,\cdot\rangle & = s\cos(\pi \mathrm{d_g}) \\
1 - \frac{1}{2s}\mathrm{d_H} & = & 1 - \frac{n}{2s}\mathrm{d_h} & = & 1 - \frac{1}{2s}\mathrm{d_1} & = & 1 - \frac{1}{2s}\mathrm{d_2^2} & = \frac{1}{s}\langle\cdot,\cdot\rangle & = \cos(\pi \mathrm{d_g})
\end{array}$$

Appendix B

Some technical lemmata

In the context of approximating binomial coefficients—and, in particular, sums of term with binomial coefficient factors—it can be useful to resolve the induced bounding inequalities in the safety of an appendix. In addition to reducing clutter in the main narrative, there is, perhaps, less guilt associated with adding in a little extra information.

B.1 Estimates involving binomial coefficients

The Stirling-Robbins estimate for the factorial,

$$\sqrt{2\pi}\sqrt{n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi}\sqrt{n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}} \quad \text{for } n \in \mathbb{N}, \tag{B.1}$$

provides bounds on the accuracy of the estimate $n! \approx \sqrt{2\pi n}(n/e)^n$ via the factors $e^{\frac{1}{12n}} > e^{\frac{1}{12n+1}} > 1$. These bounds are fundamental in the first two results in this section, which are derived in support of any effort which benefits from being able to ignore the first couple summands in an expression.

To accomplish this, we declare $\epsilon_n \approx \sqrt{2\pi}$ to be the exact correction factor such that $n! = \epsilon_n\sqrt{n}(n/e)^n$, absorbing the constant; these factors naturally aggregate to provide a correction factor $\epsilon(n,k) \approx 1/\sqrt{2\pi}$ (assigned in Lemma B.1.1) for the binomial coefficient estimate $\sigma(n,k)$. As can be seen below in Eq. (B.3), $\epsilon(n,k)$ falls between $1/3$ and $1/\sqrt{2\pi}$ for all $k < n$; the following lemma uses the intermediate upper bound to demonstrate that for a particular relevant summation, the amount accumulated by rounding $\sigma(n,k)$ up to $1/\sqrt{2\pi}$ exceeds the total of the first few summands, which can thus be disregarded in the rounding. Let us proceed.

Lemma B.1.1 (Bounding the binomial coefficient approximation error)**.** *For all $n \in \mathbb{N}$, let*

$\epsilon_n := \frac{n!}{\sqrt{n}}(\frac{e}{n})^n$, *and for* $k, n \in \mathbb{N}$ *such that* $k < n$, *define the functions*

$$\epsilon(n,k) := \frac{\epsilon_n}{\epsilon_k \epsilon_{n-k}} \quad \textit{and} \quad \sigma(n,k) := \sqrt{\frac{n}{k(n-k)}}\frac{n^n}{k^k(n-k)^{n-k}}. \tag{B.2}$$

Then $\binom{M}{k} = \epsilon(n,k) \cdot \sigma(n,k)$ *and*

$$\frac{1}{3} < \frac{1}{\sqrt{2\pi}} \frac{e^{\frac{1}{12n+1}}}{e^{\frac{1}{12k}+\frac{1}{12(n-k)}}} < \epsilon(n,k) < \frac{\exp\left[\frac{1}{12n}\right]}{\exp\left[\frac{1}{12k+1}+\frac{1}{12(n-k)+1}\right]\sqrt{2\pi}} < \frac{1}{\sqrt{2\pi}}. \tag{B.3}$$

Proof. The equality $\binom{n}{k} = \epsilon(n,k)\cdot\sigma(n,k)$ follows from the definitions of the functions therein. To prove the claimed bounds for $\epsilon(n,k)$, we begin with Stirling's approximation as given in Eq. (B.1). Dividing by $\sqrt{n}(n/e)^n$ yields $\sqrt{2\pi}e^{\frac{1}{12n+1}} < \epsilon_n < \sqrt{2\pi}e^{\frac{1}{12n}}$, and the interior inequalities within (B.3) follow directly from applications of these bounds to each of ϵ_n, ϵ_k, and ϵ_{n-k} in $\epsilon(n,k)$. For the outer inequalities, we use the following easily verified properties of the bounding factors $e^{\frac{1}{12n+1}-\frac{1}{12k}-\frac{1}{12(n-k)}}$ and $e^{\frac{1}{12n}-\frac{1}{12k+1}-\frac{1}{12(n-k)+1}}$: they are symmetric about $n/2$, they are increasing in k on the interval $1 < k < n/2$, and they are increasing in n.

It follows that $(k,n) = (1,2)$ satisfies

$$\arg \inf_{\substack{0<k<n \\ k,n\in\mathbb{N}}} \left\{ \frac{1}{\sqrt{2\pi}} e^{\frac{1}{12n+1}-\frac{1}{12k}-\frac{1}{12(n-k)}} \right\}$$

and that

$$\sup_{\substack{0<k<n \\ k,n\in\mathbb{N}}} \left\{ \frac{1}{\sqrt{2\pi}} e^{\frac{1}{12n}-\frac{1}{12k+1}-\frac{1}{12(n-k)+1}} \right\} = \lim_{n\to\infty} \frac{1}{\sqrt{2\pi}} e^{\frac{1}{12n}-\frac{1}{12\frac{n}{2}+1}-\frac{1}{12(n-\frac{n}{2})+1}} = \frac{1}{\sqrt{2\pi}}.$$

Thus,

$$\frac{1}{3} < \frac{\overbrace{e^{-\frac{19}{150}}}^{\substack{\text{evaluation of} \\ \text{lower bound} \\ \text{at } k=1,n=2}}}{\sqrt{2\pi}} \leq \frac{\overbrace{e^{\frac{1}{12n+1}-\frac{1}{12k}-\frac{1}{12(n-k)}}}^{\substack{\text{lower bound induced} \\ \text{by lower bound for } \epsilon_n}}}{\sqrt{2\pi}} < \epsilon(n,k) \tag{B.4}$$

and

$$\epsilon(n,k) < \frac{\overbrace{e^{\frac{1}{12n}-\frac{1}{12k+1}-\frac{1}{12(n-k)+1}}}^{\substack{\text{upper bound induced} \\ \text{by upper bound for } \epsilon_n}}}{\sqrt{2\pi}} \leq \frac{\overbrace{e^{-\frac{18n-1}{12n(6n+1)}}}^{\substack{\text{evaluation of} \\ \text{upper bound} \\ \text{at } k=\frac{n}{2}}}}{\sqrt{2\pi}} < \frac{1}{\sqrt{2\pi}}, \tag{B.5}$$

thereby completing the proof. □

The next lemma provides conditions under which we may ignore the first two terms in our sum $\sum_{j=0}^{k} \binom{s}{j}\binom{M-s}{j}/\binom{M}{s}$ as a consequence of rounding the Stirling error factor $\epsilon(s,2)\epsilon(M-s,2)/\epsilon(M,s)$ up to $1/\sqrt{2\pi}$.

Lemma B.1.2 (Subsuming initial terms)**.** *Let $\sigma(\cdot,\cdot)$ be the Stirling approximation function given by equation* (B.2)*, and let $s, M \in \mathbb{N}$ such that $10 \le s < \frac{1}{2}M$. Then*

$$\sum_{j=0}^{2} \binom{s}{j}\binom{M-s}{j}\binom{M}{s}^{-1} < \frac{1}{\sqrt{2\pi}} \frac{\sigma(s,2)\sigma(M-s,2)}{\sigma(M,s)}. \tag{B.6}$$

Proof. We shall factor $\binom{s}{2}\binom{M-s}{2}\binom{M}{2}^{-1} \equiv \frac{\epsilon(s,2)\epsilon(M-s,2)}{\epsilon(M,s)} \frac{\sigma(s,2)\sigma(M-s,2)}{\sigma(M,s)}$ from the left hand side of the claimed inequality and use an upper bound on the error factor $\frac{\epsilon(s,2)\epsilon(M-s,2)}{\epsilon(M,s)}$ to prove the lemma. Applying the bounds on $\epsilon(\cdot,\cdot)$ given by (B.3) in the preceding lemma,

$$\begin{aligned}
\frac{\epsilon(s,2)\epsilon(M-s,2)}{\epsilon(M,s)} &< \frac{1}{\sqrt{2\pi}} \exp\left[\left(\frac{1}{12s} - \frac{1}{25} - \frac{1}{12s-23}\right)\right. \\
&\qquad + \left(\frac{1}{12(M-s)} - \frac{1}{25} - \frac{1}{12(M-s)-23}\right) \\
&\qquad \left. - \left(\frac{1}{12M+1} - \frac{1}{12s} - \frac{1}{12(M-s)}\right)\right] \\
&= \frac{1}{\sqrt{2\pi}} \exp\left[-\frac{2}{25} + \frac{1}{12s}\left(2 - \frac{1}{1-\frac{23}{12s}} + \frac{2}{\frac{M}{s}-1}\right.\right. \\
&\qquad \left.\left. - \frac{1}{\frac{M}{s}-1-\frac{23}{12s}} - \frac{1}{\frac{M}{s}+\frac{1}{12s}}\right)\right] \\
&< \frac{1}{\sqrt{2\pi}} \exp\left[-\frac{2}{25} + \frac{1}{12s}\left(1 + \frac{1}{\frac{M}{s}-1} - \frac{1}{\frac{M}{s}+1}\right)\right] \\
&< \frac{1}{\sqrt{2\pi}} \exp\left[-\frac{2}{25} + \frac{1}{6s}\right] \qquad \text{(since } M/s > 2\text{).}
\end{aligned}$$

Thus, we have that

$$\begin{aligned}
\sum_{j=0}^{2}\binom{s}{j}\binom{M-s}{j}\binom{M}{s}^{-1} &= \sum_{j=0}^{2}\frac{\binom{s}{j}\binom{M-s}{j}}{\binom{s}{2}\binom{M-s}{2}}\cdot\frac{\binom{s}{2}\binom{M-s}{2}}{\binom{M}{s}} \\
&= \left(\frac{4+4s(M-s)}{s(s-1)(M-s)(M-s-1)}+1\right) \\
&\qquad \cdot\frac{\epsilon(s,2)\epsilon(M-s,2)}{\epsilon(M,s)}\frac{\sigma(s,2)\sigma(M-s,2)}{\sigma(M,s)} \\
&< \left(\frac{4+4s(M-s)}{(s-1)^2(M-s-1)^2}+1\right) \\
&\qquad \cdot\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{2}{25}+\frac{1}{6s}\right)\frac{\sigma(s,2)\sigma(M-s,2)}{\sigma(M,s)}
\end{aligned}$$

and since $M-s>s\geq 10$,

$$\begin{aligned}
&< \left(\frac{4+4s^2}{(s-1)^2(s-1)^2}+1\right) \\
&\qquad \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{2}{25}+\frac{1}{6s}\right)\frac{\sigma(s,2)\sigma(M-s,2)}{\sigma(M,s)}.
\end{aligned}$$

Noting that $\left(\frac{4+4s^2}{(s-1)^4}+1\right)\exp\left(-\frac{2}{25}+\frac{1}{8s}\right)$ decreases monotonically to $\exp(-\frac{2}{25})<1$ and is less than 1 for $s\geq 10$,

$$\sum_{j=0}^{2}\binom{s}{j}\binom{M-s}{j}\binom{M}{s}^{-1} < \frac{1}{\sqrt{2\pi}}\frac{\sigma(s,2)\sigma(M-s,2)}{\sigma(M,s)}$$

for $s\geq 10$, and inequality (B.6) is proven. □

B.2 Estimating sums of exponentials

Given a sum of the form sum $\sum_{xM=h}^{k}\exp(ax^2+bx+c)$ allows us to bound using a standard[1] approximation of $\int_x^\infty \exp(-t^2)dt$ (see, e.g., [45]),

$$\frac{e^{-x^2}}{x+\sqrt{x^2+2}} \leq \int_x^\infty e^{-t^2}dt \leq \frac{e^{-x^2}}{x+\sqrt{x^2+1}} \qquad \text{for } x>0\ . \tag{B.7}$$

[1]This *Mills' ratio* bounding inequality, widely attributed to Yusaku Komatsu (1955), is typically expressed in terms of $e^{\frac{x^2}{2}}$, as in $2[x+\sqrt{x^2+4}]^{-1} < \exp(-\frac{x^2}{2})\int_x^\infty \exp(-\frac{t^2}{2})dt < 2[x+\sqrt{x^2+2}]^{-1}$.

When the arguments of the expression $\sum_{xM=n}^{k} \exp(ax^2 + bx + c)$ meet certain simple constraints, the corresponding estimate admits a compact expression. We offer this result as the content of the following proposition:

Lemma B.2.1. *Given the quadratic function $g : \mathbb{R} \to \mathbb{R}$ defined by*

$$g(x) := -A(x - B)^2 + D$$

with $A, B > 0$, let $h, k, M \in \mathbb{N}$ satisfy $h < k \leq BM$. Then, setting

$$\gamma_l(x) := \frac{e^{g(x)}}{A(B - x) + \sqrt{A^2(B - x)^2 + 2A}}$$

and

$$\gamma_u(x) := \frac{e^{g(x)}}{A(B - x) + \sqrt{A^2(B - x)^2 + A}},$$

we have

$$\begin{aligned}\gamma_l\left(\frac{k-1}{M}\right) - \gamma_u\left(\frac{h-1}{M}\right) &< \frac{1}{M}\sum_{xM=h}^{k-1} e^{g(x)} \\ &< \int_{\frac{h}{M}}^{\frac{k}{M}} e^{g(x)}dx < \gamma_u\left(\frac{k}{M}\right) - \gamma_l\left(\frac{h}{M}\right) < \frac{\exp\Big(g\big(\frac{k}{M}\big)\Big)}{2A\left(B - \frac{k}{M}\right)}.\end{aligned}$$

Proof. The proof resolves to demonstrating the following string of inequlities:

$$\begin{aligned}\gamma_l\left(\frac{k-1}{M}\right) - \gamma_u\left(\frac{h-1}{M}\right) &< \int_{\frac{h-1}{M}}^{\frac{k-1}{M}} e^{g(x)}dx \\ &< \frac{1}{M}\sum_{xM=h}^{k-1} e^{g(x)} \\ &< \int_{\frac{h}{M}}^{\frac{k}{M}} e^{g(x)}dx < \gamma_u\left(\frac{k}{M}\right) - \gamma_l\left(\frac{h}{M}\right) \\ &< \gamma_u\left(\frac{k}{M}\right) \\ &< \frac{\exp\Big(g\big(\frac{k}{M}\big)\Big)}{2A\left(B - \frac{k}{M}\right)}.\end{aligned}$$

Since $e^{g(x)}$ is increasing on the interval $(-\infty, B)$, for $n_0 \in [h, BM - 1]$ we have

$$\int_{\frac{n_0-1}{M}}^{\frac{n_0}{M}} e^{g(x)}dx \leq \frac{1}{M}\exp\Big(g\big(\frac{n_0}{M}\big)\Big) \leq \int_{\frac{n_0}{M}}^{\frac{n_0+1}{M}} e^{g(x)}dx.$$

It immediately follows that

$$\int_{\frac{h-1}{M}}^{\frac{k-1}{M}} e^{g(x)}dx < \frac{1}{M}\sum_{xM=h}^{k-1} e^{g(x)} < \int_{\frac{h}{M}}^{\frac{k}{M}} e^{g(x)}dx.$$

Now, for $0 < a < b \leq \frac{k}{M}$,

$$\int_a^b e^{g(x)}dx = \frac{e^D}{\sqrt{A}}\int_{b_t}^{a_t} e^{-t^2}dt = \frac{e^D}{\sqrt{A}}\left(\int_{b_t}^{\infty} e^{-t^2}dt - \int_{a_t}^{\infty} e^{-t^2}dt\right), \tag{B.8}$$

where the substitution $t^2 := A(x-B)^2$ results in $b_t = \sqrt{A}(B-b) < a_t = \sqrt{A}(B-a)$. Bounding expression (B.8) above we see

$$\begin{aligned}
\int_a^b e^{g(x)}dx &= \frac{e^D}{\sqrt{A}}\int_{b_t}^{a_t} e^{-t^2}dt \\
&< \frac{e^D}{\sqrt{A}}\left(\frac{\exp(-b_t^2)}{b_t+\sqrt{b_t^2+1}} - \frac{\exp(-a_t^2)}{a_t+\sqrt{a_t^2+2}}\right) \\
&= \frac{e^D}{\sqrt{A}}\left(\frac{\exp(-A(B-b)^2)}{\sqrt{A}(B-b)+\sqrt{A(B-b)^2+1}}\right. \\
&\qquad\qquad \left. -\frac{\exp(-A(B-a)^2)}{\sqrt{A}(B-a)+\sqrt{A(B-a)^2+2}}\right) \\
&= \frac{\exp(g(b))}{A(B-b)+\sqrt{A^2(B-b)^2+A}} - \frac{\exp(g(a))}{A(B-a)+\sqrt{A^2(B-a)^2+2A}} \\
&= \gamma_u(b) - \gamma_l(a) \\
&< \gamma_u(b).
\end{aligned}$$

That $\gamma_u(b) < \exp(g(b))/[2A(B-b)]$ follows from $A(B-b) < \sqrt{A^2(B-b)^2+A}$. Setting $a := \frac{h}{M}$ and $b := \frac{k}{M}$ in the preceding chain of inequalities produces the sequence of upper bounds claimed by the lemma.

Applying the same technique, the value $\int_{(h-1)/M}^{(k-1)/M} e^{g(x)}dx$ is bounded below by $\gamma_l(\frac{k-1}{M}) - \gamma_u(\frac{h-1}{M})$, and the proof is complete. □

Bibliography

[1] Noga Alon and Joel H. Spencer. *Appendix A: Bounding of Large Deviations*. John Wiley & Sons, Inc., 2008.

[2] Zachery J. Baker, Bernhard G. Bodmann, Micah G. Bullock, Samantha N. Branum, and Jacob E. McLaney. What is odd about binary parseval frames? *Involve, a Journal of Mathematics*, 11(2):219–233, 2017.

[3] Anton Betten, Michael Braun, Harald Fripertinger, Adalbert Kerber, Axel Kohnert, and Alfred Wassermann. *Error-correcting linear codes: Classification by isometry and applications*, volume 18. Springer Science & Business Media, 2006.

[4] Bernhard G. Bodmann, Bijan Camp, and Dax Mahoney. Binary frames, graphs and erasures. *Involve*, 7(2):151–169, 2014.

[5] Bernhard G. Bodmann, My Le, Letty Reza, Matthew Tobin, and Mark Tomforde. Frame theory for binary vector spaces. *Involve*, 2(5):589–602, 2009.

[6] Bernhard G. Bodmann and Robert P. Mendez. Binary block codes from Euclidean embeddings and random hyperplane tessellations. In Dimitri Van De Ville Yue M. Lu and Manos Papadakis, editors, *Proceedings of SPIE 10394, Wavelets and Sparsity XVII*. ACM Press, August 2017.

[7] Bernhard G. Bodmann and Vern I. Paulsen. Frames, graphs and erasures. *Linear Algebra and its Applications*, 404:118–146, 2005.

[8] Petros T. Boufounos and Richard G. Baraniuk. 1-bit compressive sensing. In *42nd Annual Conference on Information Sciences and Systems*, pages 16–21. IEEE, 2008.

[9] Jameson Cahill and Dustin G. Mixon. Robust width: A characterization of uniformly stable and robust compressed sensing. *CoRR*, abs/1408.4409, 2014.

[10] Emmanuel J. Candès. The restricted isometry property and its implications for compressed sensing. *Comptes Rendus Mathematique*, 346(9):589 – 592, 2008.

[11] Emmanuel J. Candès, Yonina C. Eldar, Deanna Needell, and Paige Randall. Compressed sensing with coherent and redundant dictionaries. *Applied and Computational Harmonic Analysis*, 31(1):59–73, 2011.

[12] Emmanuel J. Candès and Justin Romberg. Quantitative robust uncertainty principles and optimally sparse decompositions. *Foundations of Computational Mathematics*, 6(2):227–254, 2006.

[13] Emmanuel J. Candès and Justin Romberg. Sparsity and incoherence in compressive sampling. *Inverse Problems*, 23(3):969, 2007.

[14] Emmanuel J. Candès, Justin Romberg, and Terence Tao. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. *IEEE Transactions on Information Theory*, 52(2):489–509, 2006.

[15] Emmanuel J. Candès and Terence Tao. Decoding by linear programming. *IEEE Transactions on Information Theory*, 51(12):4203–4215, 2005.

[16] Emmanuel J. Candès and Terence Tao. Near-optimal signal recovery from random projections: Universal encoding strategies? *IEEE Transactions on Information Theory*, 52(12):5406–5425, 2006.

[17] Emmanuel J. Candès and Michael B. Wakin. An introduction to compressive sampling. *IEEE Signal Processing Magazine*, 25(2):21–30, 2008.

[18] Peter G. Casazza and Gitta Kutyniok, editors. *Finite Frames*. Applied and Numerical Harmonic Analysis. Birkhäuser Boston, 2013.

[19] Venkat Chandrasekaran, Benjamin Recht, Pablo A. Parrilo, and Alan S. Willsky. The convex geometry of linear inverse problems. *Foundations of Computational Mathematics*, 12(6):805–849, 2012.

[20] Scott Shaobing Chen, David L. Donoho, and Michael A. Saunders. Atomic decomposition by basis pursuit. *SIAM Review*, 43(1):129–159, 2001.

[21] Tuan-Yow Chien and Shayne Waldron. A classification of the harmonic frames up to unitary equivalence. *Applied and Computational Harmonic Analysis*, 30(3):307–318, 2011.

[22] Tuan-Yow Chien and Shayne Waldron. A characterization of projective unitary equivalence of finite frames and applications. *SIAM Journal of Discrete Mathematics*, 30(2):976–994, 2016.

[23] Cornelis de Vroedt. On the maximum cardinality of binary constant weight codes with prescribed distance. *Discrete Mathematics*, 97(1-3):155–160, 1991.

[24] David L. Donoho. Compressed sensing. *IEEE Transactions on Information Theory*, 52(4):1289–1306, 2006.

[25] David L. Donoho. For most large underdetermined systems of linear equations the minimal ℓ_1-norm solution is also the sparsest solution. *Communications on Pure and Applied Mathematics: A Journal Issued by the Courant Institute of Mathematical Sciences*, 59(6):797–829, 2006.

[26] Joakim Ekberg. *Geometries of Binary Constant Weight Codes*. PhD thesis, Karlstad University, 2006.

[27] Salim Y. El Rouayheb, Costas N. Georghiades, Emina Soljanin, and Alex Sprintson. Bounds on codes based on graph theory. In *2007 IEEE International Symposium on Information Theory*, pages 1876–1879. IEEE, 2007.

[28] Yonina C. Eldar and Gitta Kutyniok. *Compressed sensing: theory and applications*. Cambridge University Press, 2012.

[29] Tuvi Etzion and Alexander Vardy. A new construction for constant weight codes. In *2014 International Symposium on Information Theory and its Applications*, pages 338–342. IEEE, 2014.

[30] Robert G. Gallager. *Information Theory and Reliable Communication*. John Wiley & Sons, Inc., New York, NY, USA, 1968.

[31] Robert G. Gallager. The random coding bound is tight for the average code. *IEEE Transactions on Information Theory*, IT-19:244–246, 1973.

[32] James Gleick. *The Information: A History, a Theory, a Flood*. Pantheon Books, New York, NY, USA, 2011.

[33] Michel X. Goemans and David P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM*, 42:1115–1145, 1995.

[34] Vivek K. Goyal, Jelena Kovačević, and Jonathan A. Kelner. Quantized frame expansions with erasures. *Applied and Computational Harmonic Analysis*, 10(3):203–233, 2001.

[35] Ron Graham and Neil Sloane. Lower bounds for constant weight codes. *IEEE Transactions on Information Theory*, 26(1):37–43, 1980.

[36] Ronald L. Graham and Neil James Alexander Sloane. On constant weight codes and harmonious graphs. Technical report, Stanford University, Department of Computer Science, 1979.

[37] John I. Haas. *The geometry of structured Parseval frames and frame potentials*. PhD thesis, Ph. D. dissertation, University of Houston, 2015.

[38] Richard W. Hamming. Error detecting and error correcting codes. *The Bell System Technical Journal*, 29(2):147–160, 1950.

[39] Deguang Han, Keri Kornelson, David R. Larson, and Eric Weber. *Frames for undergraduates*, volume 40. American Mathematical Society, 2007.

[40] Deguang Han and David R. Larson. *Frames, Bases and Group Representations*, volume 147 of *American Mathematical Society: Memoirs of the American Mathematical Society*. American Mathematical Society, 2000.

[41] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

[42] Roderick B. Holmes and Vern I. Paulsen. Optimal frames for erasures. *Linear Algebra and its Applications*, 377:31–51, 2004.

[43] Ryan Hotovy, David R. Larson, and Sam Scholze. Binary frames. *Houston Journal of Mathematics*, 41(3):875–899, 2015.

[44] William Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2010.

[45] Kiyosi Itō and Henry P. McKean, Jr. *Diffusion Processes and Their Sample Paths*. Die Grundlehren der mathematischen Wissenschaften. Academic Press, 1965.

[46] Laurent Jacques, Jason N. Laska, Petros Boufounos, and Richard G. Baraniuk. Robust 1-bit compressive sensing via binary stable embeddings of sparse vectors. *IEEE Transactions on Information Theory*, 59(4):2082–2102, 2013.

[47] Selmer Johnson. On upper bounds for unrestricted binary-error-correcting codes. *IEEE Transactions on Information Theory*, 17(4):466–478, 1971.

[48] Selmer Johnson. Upper bounds for constant weight error correcting codes. *Discrete Mathematics*, 3(1-3):109–124, 1972.

[49] Deepti Kalra. Complex equiangular cyclic frames and erasures. *Linear Algebra and its Applications*, 419(2-3):373–399, 2006.

[50] Karin Knudson, Rayan Saab, and Rachel Ward. One-bit compressive sensing with norm estimation. *IEEE Trans. Information Theory*, 62(5):2748–2758, 2016.

[51] Jelena Kovačević and Amina Chebira. Life beyond bases: The advent of frames (part i). *IEEE Signal Processing Magazine*, 24(4):86–104, 2007.

[52] Jelena Kovačević and Amina Chebira. Life beyond bases: The advent of frames (part ii). *IEEE Signal Processing Magazine*, 24(5):115–125, 2007.

[53] Shu Lin and E.J. Weldon. Long BCH codes are bad. *Information and Control*, 11(4):445–451, 1967.

[54] Maria Silva Lucido and Mohammad Reza Pournaki. Elements with square roots in finite groups. *Algebra Colloquium*, 12(4):677–690, 2005.

[55] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*. Elsevier, 1977.

[56] Thomas G. Marshall. Coding of real-number sequences for error correction: A digital signal processing problem. *IEEE Journal on Selected Areas in Communications*, 2(2):381–392, 1984.

[57] Thomas G. Marshall. Fourier transform convolutional error-correcting codes. In *Twenty-Third Asilomar Conference on Signals, Systems and Computers*, volume 2, pages 658–662. IEEE, 1989.

[58] Robert P. Mendez. Supporting matlab programs repository. `http://math.uh.edu/~rpmendez/binaryParsevalGroupFrames/`. Verified October 13, 2018.

[59] Robert P. Mendez, Bernhard G. Bodmann, Zachery J. Baker, Micah G. Bullock, and Jacob E. McLaney. Binary parseval frames from group orbits. *Linear Algebra and its Applications*, 556:265–300, 2018.

[60] Roberto Montemanni and Derek H. Smith. Heuristic construction of constant weight binary codes. *Technical Report No. IDSIA-12-07*, 2007.

[61] Yaniv Plan and Roman Vershynin. Robust 1-bit compressed sensing and sparse logistic regression: A convex programming approach. *CoRR*, abs/1202.1212, 2012.

[62] Yaniv Plan and Roman Vershynin. One-bit compressed sensing by linear programming. *Communications on Pure and Applied Mathematics*, 66(8):1275–1297, 2013.

[63] Yaniv Plan and Roman Vershynin. Dimension reduction by random hyperplane tessellations. *Discrete & Computational Geometry*, 51(2):438–461, 2014.

[64] Yaniv Plan, Roman Vershynin, and Elena Yudovina. High-dimensional estimation with geometric constraints. *Information and Inference: A Journal of the IMA*, 6(1):1–40, 2017.

[65] Vera Pless. A classification of self-orthogonal codes over GF(2). *Discrete Mathematics*, 3(1-3):209–246, 1972.

[66] Gagan Rath and Christine Guillemot. Performance analysis and recursive syndrome decoding of DFT codes for bursty erasure recovery. *IEEE Transactions on Signal Processing*, 51(5):1335–1350, 2003.

[67] Gagan Rath and Christine Guillemot. Frame-theoretic analysis of DFT codes with erasures. *IEEE Transactions on Signal Processing*, 52(2):447–460, 2004.

[68] Holger Rauhut, Justin Romberg, and Joel A. Tropp. Restricted isometries for partial random circulant matrices. *Applied and Computational Harmonic Analysis*, 32(2):242–254, 2012.

[69] Mark Rudelson and Roman Vershynin. On sparse reconstruction from Fourier and Gaussian measurements. *Communications on Pure and Applied Mathematics*, 61(8):1025–1045, 2008.

[70] Julian Schwinger. Unitary operator bases. In *Proceedings of the National Academy of Sciences of the United States of America*, pages 570–579, 1960.

[71] Claude Elwood Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948.

[72] Derek H. Smith, Lesley A. Hughes, and Stephanie Perkins. A new table of constant weight codes of length greater than 28. *The Electronic Journal of Combinatorics*, 13(1):2, 2006.

[73] A. A. Tietavainen. An asymptotic bound on the covering radii of binary BCH codes. *IEEE Transactions on Information Theory*, 36(1):211–213, 1990.

[74] Richard Vale and Shayne Waldron. Tight frames and their symmetries. *Constructive Approximation*, 21(1):83–112, 2004.

[75] Richard Vale and Shayne Waldron. Tight frames generated by finite nonabelian groups. *Numerical Algorithms*, 48(1):11–27, 2008.

[76] Shayne Waldron. *Group Frames*, pages 171–191. Birkhäuser Boston, Boston, 2013.

[77] Shayne Waldron and Nick Hay. On computing all harmonic frames of n vectors in cd. *Applied and Computational Harmonic Analysis*, 21(2):168–181, 2006.

[78] Rachel Ward. Compressed sensing with cross validation. *IEEE Transactions on Information Theory*, 55(12):5773–5782, 2009.

[79] Stephen B. Wicker and Vijay K. Bhargava, editors. *Reed-Solomon Codes and Their Applications*. John Wiley & Sons, Inc., New York, NY, USA, 1999.

Index